

HP Network Automation

소프트웨어 버전: 9.10

사용 설명서

문서 릴리스 날짜: 2011년 3월
소프트웨어 릴리스 날짜: 2011년 3월



법적 고지

보증

HP 제품 및 서비스에 대한 모든 보증 사항은 해당 제품 및 서비스와 함께 제공되는 명시적 보증서에 규정되어 있습니다. 여기에 수록된 어떤 내용도 추가 보증을 구성하는 것으로 해석될 수 없습니다. HP는 여기에 수록된 기술적 또는 편집상의 오류나 누락에 대해 책임지지 않습니다.

본 정보는 예고 없이 변경될 수 있습니다. 022311

제한된 권리 범례

기밀 컴퓨터 소프트웨어입니다. 소유, 사용 또는 복사하기 위해서는 HP로부터 유효한 라이선스를 확보해야 합니다. FAR 12.211 및 12.212에 의거하여 상용 컴퓨터 소프트웨어, 컴퓨터 소프트웨어 설명서 및 상용 품목에 대한 기술 데이터는 공급업체의 표준 상용 라이선스에 따라 미국 정부에 사용 허가되었습니다.

저작권 고지

© Copyright 2011 Hewlett-Packard Development Company, L.P.

상표권 고지

Adobe®는 Adobe Systems Incorporated의 상표입니다.

Java™는 Sun Microsystems, Inc.의 미국 상표입니다.

승인

ANTLR, Apache, Bouncy Castle, GNU, Jaxen, Jython, Netaphor, MetaStuff, Radius, Sleepcat, TanukiSoftware

문서 업데이트

이 설명서의 제목 페이지에는 다음과 같은 식별 정보가 포함되어 있습니다

- 소프트웨어 버전 번호: 소프트웨어 버전을 나타냅니다.
- 문서 릴리스 날짜: 문서가 업데이트될 때마다 변경됩니다.
- 소프트웨어 릴리스 날짜: 이 소프트웨어 버전의 릴리스 날짜를 나타냅니다.

최신 업데이트를 확인하거나 문서의 최신 버전을 사용하고 있는지 확인하려면 다음 사이트로 이동하십시오.

<http://h20230.www2.hp.com/selfsolve/manuals>

이 사이트를 이용하려면 HP Passport ID를 등록하고 로그인해야 합니다. HP Passport ID를 등록하려면 다음 사이트로 이동하십시오.

<http://h20229.www2.hp.com/passport-registration.html>

또는 HP Passport 로그인 페이지에서 **New users - please register** 링크를 클릭하십시오.

또한 적절한 제품 지원 서비스에 가입하면 업데이트된 버전이나 새 버전을 받을 수 있습니다. 자세한 내용은 HP 판매 담당자에게 문의하십시오.

지원

HP Software Support Online 웹 사이트를 방문할 수 있습니다.

이 웹 사이트에서는 연락처 정보뿐만 아니라 HP Software에서 제공하는 제품, 서비스 및 지원에 대한 세부 정보를 제공합니다.

HP Software Support Online에서는 고객에게 자가 해결 기능을 제공합니다. 또한 비즈니스 관리에 필요한 대화식 기술 지원 도구에 신속하고 효율적으로 액세스할 수 있는 방법도 제공합니다. 중요한 지원 고객의 경우 HP Software Support 웹 사이트를 사용하면 다음과 같은 장점이 있습니다.

- 관심 있는 지식 문서 검색
- 지원 케이스와 기능 향상 요청 제출 및 추적
- 소프트웨어 패치 다운로드
- 지원 계약 관리
- HP 지원 연락처 조회
- 사용 가능한 서비스에 대한 정보 검토
- 다른 소프트웨어 고객과 토론 시작
- 소프트웨어 교육 조사 및 등록

대부분의 지원 영역을 이용하려면 HP Passport 사용자로 등록하고 로그인해야 하며 대부분의 영역에서는 지원 계약도 요구됩니다.

액세스 수준에 대한 추가 정보를 보려면 다음 사이트로 이동하십시오.

http://h20230.www2.hp.com/new_access_levels.jsp

HP Passport ID를 등록하려면 다음 사이트로 이동하십시오.

<http://h20229.www2.hp.com/passport-registration.html>

1장: 시작하기	19
제품 개요	20
NA 7.50 기능	21
NA 7.60 기능	22
NA 9.0 기능	24
NA 9.10 기능	26
기본 메뉴 모음	28
도움말 메뉴 옵션	29
NA 홈 페이지	30
명령 창 열기	31
설명서 액세스	31
HP Network Automation 9.10 사용 설명서	32
고객 지원 센터에 문의	34
문제 해결 보내기 페이지 필드	35
최신 소프트웨어 버전 보기	36
라이선스 정보 보기	36
시스템 구성 보기 페이지	37
2장: 관리 설정 구성	39
관리 설정 탐색	40
시작하기	41
구성 관리	42
구성 관리 페이지 필드	43
변경 감지	51
Syslog 메시지	52
사용자 특성 세부사항 페이지 필드	53
사전 작업 및 사후 작업 스냅샷 구성	54
장치 액세스	55
장치 액세스 페이지 필드	56
작업별 자격 증명	65
서버	67
서버 페이지 필드	68
워크플로	77
워크플로 페이지 필드	77
사용자 인터페이스	80
사용자 인터페이스 페이지 필드	80
HP 로그인 페이지 사용자 지정	84
텔넷/SSH	85
텔넷/SSH 페이지 필드	86

보고	90
보고 페이지 필드	91
사용자 인증	97
인증 장애 조치	98
LDAP 인증	99
SecurID 인증	99
TACACS+ 인증	99
RADIUS 인증	100
HP SA(HP Server Automation)	101
HP OO(HP Operations Orchestration)	101
사용자 인증 페이지 필드	102
LDAP 외부 인증 설정	106
LDAP SSL 구성	108
서버 모니터링	110
서버 모니터링 페이지 필드	111
타사 통합	115
타사 통합 페이지 필드	115
모니터링 결과 보기	117
시스템 상태 페이지 필드	117
모니터 메시지	118
서비스 시작 및 중지	123
서비스 시작/중지 페이지 필드	123
로깅	125
로그 수준	125
로그 이름	126
세션 로그	127
작업 로그	128
서버 로그	129
로그 관리	129
문제 해결 페이지 필드	130
드라이버 검토	131
드라이버 페이지 필드	131

3장: 장치 및 장치 그룹 추가..... 133

장치 추가로 이동	134
시작하기	135
장치 그룹 명명 규칙	136
장치 추가	137
새 장치 페이지 필드	138
장치 편집 페이지 필드	146
Bare Metal 프로비전	153
장치 템플릿	155

장치 템플릿 페이지 필드	155
장치 템플릿 세부사항 페이지 필드.....	157
템플릿 구성 편집 페이지	159
새 장치 템플릿 추가.....	161
새 장치 템플릿 페이지 필드.....	161
장치별 템플릿 페이지.....	164
새 장치 마법사 사용.....	165
새 장치 마법사 페이지 필드.....	165
장치 가져오기	167
CSV 장치 및 암호 데이터 파일 생성.....	168
장치 암호 규칙 생성.....	170
장치 암호 규칙 페이지 필드.....	171
장치 암호 규칙 페이지 필드.....	172
장치 그룹 추가	175
새 그룹 페이지 필드.....	177
상위 그룹 추가	178
새 상위 그룹 페이지 필드.....	178
상위 그룹 페이지 필드	179
동적 장치 그룹	180
동적 장치 그룹 생성.....	180
동적 장치 그룹 계산.....	182
장치 선택기.....	183
장치 선택	183
장치 그룹 선택	184
장치 선택기 버튼	184
장치 그룹 보기	186
장치 그룹 페이지 필드	187
장치 그룹 세부사항 페이지 필드	188
장치 및 사용자 세분화	191
로컬 영역	193
로컬 영역 및 NAT 액세스	193
로컬 영역 및 콘솔 액세스.....	193
로컬 영역 및 배스천 호스트 액세스.....	194
로컬 영역 추가	194
오버랩되는 IP 네트워크.....	194
HP 게이트웨이 설정.....	195
게이트웨이 목록 페이지 필드	198
게이트웨이 편집 페이지 필드	200
파티션	201
파티션 페이지 필드.....	202
새 파티션 페이지	203
파티션 편집 페이지 필드	204
파티션에 장치 추가.....	205
파티션 세부사항 보기.....	206

장치 그룹 편집	207
그룹 페이지 편집 필드	207
장치 일괄 편집	209
장치 일괄 편집 페이지 필드	209
장치 드라이버 검색	212
텔넷을 사용한 장치 액세스	213
SSH를 사용한 장치 액세스	214
텔넷/SSH 세션 나열	215
텔넷/SSH 세션 목록 페이지 필드	215
텔넷/SSH 프록시를 사용하여 구성 변경	217
배스천 호스트 사용	218

4장: 장치 구성 관리 221

장치 구성 변경으로 이동	221
시작하기	222
장치 구성 변경 보기	223
장치 구성 페이지 필드	224
장치 구성 세부사항 페이지 필드	227
장치 구성 데이터 편집	230
장치 구성 비교	231
장치 구성 비교 페이지 필드	231
장치 구성 배포	233
구성 배포 작업 페이지 필드	234

5장: 장치 보기 239

장치 정보 탐색	240
장치 보기	241
인벤토리 페이지 필드	241
장치 그룹 보기	244
장치 그룹 페이지 필드	244
장치 예약	246
활동 캘린더	247
장치 세부사항 보기	249
장치 세부사항 페이지 필드	250
NA/SA 통합	254
NA/SA 권한	255
장치 하드웨어 정보	256
방화벽을 통해 NA에 연결	256
포트 변경	258
잘못된 포트 개수	259

메뉴 옵션 보기	261
장치 이벤트 페이지 필드	266
장치 인터페이스 페이지 필드	267
인터페이스 세부사항 페이지 필드	269
인터페이스 편집 세부사항 페이지 필드	271
서브넷의 인터페이스 페이지 필드	273
장치 IP 주소 페이지 필드	274
장치 MAC 주소 페이지 필드	276
VLAN(가상 로컬 영역 네트워크)	278
장치 VLAN 페이지 필드	280
VLAN 생성 및 편집	282
VLAN 세부사항 페이지 필드	283
VTP 세부사항 페이지 필드	285
VTP 도메인 페이지 필드	287
VTP 도메인 페이지	288
장치 블레이드/모듈 페이지 필드	289
장치 정책 페이지 필드	290
서버 페이지 필드	292
장치 소프트웨어 이미지 권장 사항 페이지 필드	293
장치 작업 페이지 필드	297
장치 관계 페이지 필드	299
장치 소프트웨어 이력 페이지 필드	301
장치 세션 페이지 필드	303
편집 메뉴 옵션	304
장치에서 관리되는 IP 주소 페이지 필드	307
새 IP 주소 페이지(배스천 호스트)	309
새 IP 주소 페이지(사용자 지정 IP 주소)	310
새 IP 주소 페이지(콘솔 서버)	311
새 IP 주소 페이지(홉 상자)	312
새 IP 주소 페이지(새 통과 연결)	313
프로비전 메뉴 옵션	314
연결 메뉴 옵션	316

6장: 사용자 관리 317

사용자 관리 탐색	318
사용자 추가	319
모든 사용자 페이지 필드	320
로그온한 사용자 페이지 필드	321
전자 메일 알림	322
새 사용자 페이지 필드	323
사용자 암호 구성	326
사용자 시나리오 1	326
사용자 시나리오 2	327
사용자 시나리오 3	327

암호 만료.....	328
암호 재사용.....	329
사용자 그룹 추가	330
사용자 그룹 페이지 필드	330
새 사용자 그룹 페이지 필드.....	331
사용자 역할 추가	335
사용자 역할 및 권한 페이지 필드	335
새 사용자 역할 페이지 필드	337
사용자 설정 편집	338
내 설정	338
내 프로필 페이지 필드	339
내 작업 공간 페이지 필드.....	341
내 기본 설정 페이지 필드.....	341
내 권한 페이지 필드.....	343
암호 변경 페이지 필드	344
빠른 시작이란?.....	345
빠른 시작을 구성하는 방법	345
빠른 시작 관리.....	346
빠른 시작 사용	346
샘플 빠른 시작 표시	347
NA 홈 페이지 사용자 지정	349
내 홈 페이지 탭 필드	350
통계 대시보드 탭 필드	353
검색/연결 기능.....	354

7장: 작업 예약 355

작업 페이지로 이동.....	357
작업이란?	358
임시 장치 그룹에 대한 작업 실행.....	358
작업 예약	359
용어.....	359
라운드 로빈 그룹 작업	360
작업 템플릿.....	361
NA 작업.....	364
Syslog 구성 작업 페이지 필드	366
암호 배포 작업 페이지 필드	370
드라이버 검색 작업 페이지 필드	375
장치 재부팅 작업 페이지 필드	379
ICMP 테스트 실행 작업 페이지 필드	383
명령 스크립트 실행 작업 페이지 필드	389
진단 실행 작업 페이지 필드	397
스냅샷 작성 작업 페이지 필드	403
시작 및 실행 동기화 작업 페이지 필드	408

장치 소프트웨어 업데이트 작업 페이지 필드	413
배포 테이블	418
가져오기 작업 페이지 필드	421
네트워크 장치 감지 작업 페이지 필드	426
스캔 방식	427
IP 주소 범위 정의	428
중복 방지 작업 페이지 필드	433
OS 분석 작업 페이지 필드	436
포트 스캔 페이지 필드	440
장치 프로비전 작업 페이지 필드	444
장치 컨텍스트 추가 작업 페이지 필드	448
VLAN 작업 페이지 필드	452
트렁크 포트 구성	455
Cisco.com에서 이미지 다운로드 작업 페이지	456
장치 소프트웨어 백업 작업 페이지 필드	459
정책 준수 확인 작업 페이지 필드	462
요약 보고서 생성 작업 페이지 필드	466
전자 메일 보고서 작업 페이지 필드	469
원격 에이전트 배포 페이지 필드	472
FQDN 확인 작업 페이지 필드	475
데이터 정리 작업 페이지 필드	478
외부 응용 프로그램 실행 작업 페이지 필드	481
멀티 태스킹 프로젝트 예약	485
하위 작업 경고 상태	485
멀티 태스킹 프로젝트 페이지 필드	487
멀티 태스킹 프로젝트를 구성하는 방법	489
내 작업 보기	491
내 작업 페이지 필드	491
예정된 작업 보기	495
예정된 작업 페이지 필드	495
실행 중인 작업 보기	498
작업 실행 중 페이지 필드	498
최근 작업 보기	500
최근 작업 페이지 필드	500
작업 정보 페이지 필드	503
작업 로드 보기	506
작업 로드 페이지	506

8장: 정책 보증 관리	507
정책 보증으로 이동	508
시작하기	509

NA 정책 관리자의 작업 방식	510
정책 생성	511
정책 페이지 필드	512
새 정책 페이지 필드	514
새 규칙 페이지 필드	518
정책 가져오기/내보내기	524
정책 가져오기/내보내기 페이지 필드	524
정책 편집	525
정책 편집 페이지 필드	525
규칙 예외 추가	529
새 규칙 예외 페이지 필드	530
적용된 정책 보기	531
정책 활동 보기	532
정책 활동 페이지 필드	532
정책 준수 보기	534
정책 준수 테스트 페이지 필드	534
장치에 적용되는 구성 정책 페이지 필드	536
새 소프트웨어 수준 추가	537
소프트웨어 수준 추가 페이지 필드	537
소프트웨어 수준 페이지 필드	540
소프트웨어 수준 편집	543
소프트웨어 수준 편집 페이지 필드	543
정책 준수 테스트	545
정책 준수 테스트 페이지 필드	545
정책 테스트 페이지 필드	546

9장: 소프트웨어 배포 547

소프트웨어 이미지 탐색	547
시작하기	548
소프트웨어 이미지	551
소프트웨어 이미지 페이지 필드	551
이미지 집합 추가	553
소프트웨어 이미지 집합 추가 페이지 필드	553
소프트웨어 이미지 편집 페이지 필드	555
소프트웨어 배포	556
새 소프트웨어 수준 추가	557
소프트웨어 수준 추가 페이지 필드	557
장치 소프트웨어 버전 보기	560

10장: 이벤트 알림 규칙 561

이벤트 알림 규칙 탐색	562
시작하기	563
이벤트 규칙 추가	569
이벤트 알림 및 응답 규칙 페이지 필드	570
새 이벤트 알림 및 응답 규칙 페이지 필드	571
이벤트 규칙 변수	577
장치 이벤트 변수	577
장치 구성 이벤트에 대한 변수	578
장치 진단 이벤트에 대한 변수	578
모든 이벤트에 대한 변수	579

11장: 검색 수행 581

검색 페이지로 이동	582
장치 검색	583
장치 검색 페이지 필드	584
장치 검색 결과 페이지 필드	590
인터페이스 검색	593
인터페이스 검색 페이지 필드	593
인터페이스 검색 결과 페이지 필드	596
모듈 검색	597
모듈 검색 페이지 필드	597
모듈 검색 결과 페이지 필드	600
정책 검색	601
정책 검색 페이지 필드	601
정책 검색 결과 페이지 필드	604
정책, 규칙 및 준수 검색	605
정책, 규칙 및 준수 검색 페이지 필드	606
정책, 규칙 및 준수 검색 결과 페이지 필드	608
구성 검색	610
구성 검색 페이지 필드	610
구성 검색 결과 페이지 필드	614
진단 검색	616
진단 검색 페이지 필드	617
진단 검색 결과 페이지 필드	620
작업 검색	622
작업 검색 페이지 필드	622
작업 검색 결과 페이지 필드	628
세션 검색	630
세션 검색 페이지 필드	631
세션 검색 결과 페이지 필드	634

이벤트 검색.....	636
이벤트 검색 페이지 필드	636
이벤트 검색 결과 페이지 필드	639
이벤트 설명.....	640
사용자 검색.....	648
사용자 검색 페이지.....	648
사용자 검색 결과 페이지	650
ACL 검색	651
ACL 검색 페이지 필드.....	652
ACL 검색 결과 페이지 필드.....	655
MAC 주소 검색	657
MAC 주소 검색 페이지 필드	658
MAC 주소 검색 결과 페이지 필드.....	660
IP 주소 검색	661
IP 주소 검색 페이지 필드	661
IP 주소 검색 결과 페이지 필드.....	664
VLAN 검색.....	665
VLAN 검색 페이지 필드	665
VLAN 검색 결과 페이지 필드	667
장치 템플릿 검색	668
장치 템플릿 검색 페이지 필드	668
장치 템플릿 검색 결과 페이지 필드.....	670
단일 검색	671
단일 검색 페이지 필드	671
단일 검색 결과 페이지 필드.....	673
고급 검색	674
고급 검색 페이지 필드	674
샘플 고급 검색	677

12장: 진단 및 이벤트 관리..... 679

진단 및 단일 보기 탐색	679
이벤트 통합 보기(단일 보기).....	680
단일 보기 페이지 필드	681
진단.....	684
진단 페이지 필드	684
새 진단 페이지 필드.....	686
사용자 지정 진단 추가 및 편집	687

13장: 사용자 지정 데이터 설정

사용자 지정 데이터 설정 탐색	691
사용자 지정 데이터 설정 탐색	692

시작하기	693
사용자 지정 데이터 설정 페이지 필드	694
향상된 사용자 지정 필드 설정	699
새 사용자 지정 데이터 필드 페이지.....	700

14장: 구성 템플릿 생성 701

구성 템플릿 탐색	701
시작하기	702
구성 템플릿 보기	703
구성 템플릿 페이지 필드	703
새 구성 템플릿 생성.....	706
새 구성 템플릿 페이지 필드.....	706
구성 템플릿 보기 페이지 필드	708

15장: 명령 스크립트 관리..... 711

명령 스크립트로 이동	712
시작하기	713
HP OO(HP Operations Orchestration) 흐름	713
Bare Metal 프로비전 스크립트.....	714
명령 스크립트 보기.....	717
명령 스크립트 페이지 필드.....	717
스크립트/진단 가져오기/내보내기 페이지 필드	719
명령 스크립트 추가.....	720
새 명령 스크립트 페이지 필드	722
자동 수정 스크립트 생성	726
자동 수정 스크립트 구문	726
자동 수정 스크립트 변수 명명 규칙.....	727
자동 수정 스크립트 예	729
명령 스크립트 실행.....	738
구성 템플릿에서 스크립트 생성	739

16장: 보고서 741

보고서 탐색.....	742
시작하기	743
사용자 및 시스템 보고서	744
사용자 및 시스템 보고서 필드	747
네트워크 상태 보고서	748

네트워크 상태 보고서 필드	749
모범 사례 보고서	752
모범 사례 보고서 필드	753
장치 상태 보고서	755
장치 상태 보고서 필드	755
통계 대시보드	757
다이어그램 작성	758
다이어그램 작성 페이지 필드	764
appserver.rcx 파일 편집	768
장치 소프트웨어 보고서	770
장치 소프트웨어 보고서 필드	770
소프트웨어 수준 보고서	772
소프트웨어 수준 보고서 필드	772
소프트웨어 취약점 보고서	774
소프트웨어 취약점 보고서 필드	774
이미지 동기화 보고서	776
이미지 동기화 보고서 필드	776
시스템 및 네트워크 이벤트 보고서	778
시스템 및 네트워크 이벤트 보고서 필드	778
소프트웨어 취약점 이벤트 세부사항 보고서	780
요약 보고서	782
요약 보고서 설명	783
전자 메일 보고서	786

17장: SecurID 사용 787

시작하기	788
설치 필요 조건	789
RSA 서버 인증 관리자	789
사용자 인증	789
네트워크 장치 액세스	790
SecurID 소프트웨어 토큰 추가	793
새 SecurID 토큰 페이지	793
SecurID를 통한 로그인	794
로그인 방법 1: 시스템 PIN 사용	796
로그인 방법 2: 새 PIN 사용	797
SecurID 문제점 해결	798

18장: 준수 센터 801

준수 센터 탐색	802
시작하기	803

준수 센터 홈 페이지.....	804
COBIT 준수 상태 보고서	805
COBIT 준수 상태 페이지 필드	806
COSO 준수 상태 보고서.....	816
COSO 준수 상태 페이지 필드.....	817
ITIL 준수 상태 보고서	820
ITIL 준수 상태 페이지 필드.....	820
GLBA 준수 상태 보고서	825
GLBA 준수 상태 페이지 필드.....	826
HIPAA 준수 상태 보고서	829
HIPAA 준수 상태 페이지 필드	829
Visa CISP(PCI 데이터 보안 표준) 준수 상태 보고서.....	838
Visa CISP(PCI 데이터 보안 표준) 준수 상태 페이지 필드	839

19장: 워크플로 생성 853

워크플로 탐색	854
시작하기	855
워크플로 마법사	856
내 작업	859
내 작업 페이지 필드	859
승인 요청	863
승인 요청 페이지 필드	863
작업 승인	866
작업 정보 페이지 필드	866
전자 메일 알림	869

20장: ACL 작업 871

ACL 탐색	872
시작하기	873
ACL 보기	874
장치 ACL 페이지 필드	874
ACL 보기 페이지 필드	876
명령 스크립트 실행.....	878
ACL 생성	879
ACL 응용 프로그램 변경	880
ACL 라인 일괄 삽입.....	881
ACL 라인 일괄 삭제.....	882
ACL 주석 처리 및 ACL 핸들 생성	884

ACL 템플릿 생성	885
ACL 편집	886
ACL 삭제	887
ACL 삭제 작업 페이지	888

21장: 문제 해결 893

드라이버 검색 실패.....	894
장치 스냅샷 실패	895
Syslog를 통한 실시간 변경 감지 없음	896
세션 로그	897
SWIM 오류 메시지.....	898

부록 A: 명령줄 참조..... 915

부록 B: 명령 권한 917

명령 권한 허가	917
명령 목록	918
명령 권한 정의	920

부록 C: 샘플 스크립트 931

샘플 PERL 스크립트 #1.....	931
샘플 PERL 스크립트 #2.....	933
샘플 Expect 스크립트	934

용어집..... 935

색인 939

1장: 시작하기

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
제품 개요	20페이지의 "제품 개요"
NA 7.50 기능	21페이지의 "NA 7.50 기능"
NA 7.60 기능	22페이지의 "NA 7.60 기능"
NA 9.0 기능	24페이지의 "NA 9.0 기능"
NA 9.10 기능	26페이지의 "NA 9.10 기능"
기본 메뉴 모음	28페이지의 "기본 메뉴 모음"
메뉴 모음 옵션	29페이지의 "도움말 메뉴 옵션"
NA 홈 페이지	30페이지의 "NA 홈 페이지"
명령 창 열기	31페이지의 "명령 창 열기"
설명서 액세스	31페이지의 "설명서 액세스"
고객 지원 센터에 문의	34페이지의 "고객 지원 센터에 문의"
최신 소프트웨어 버전 보기	36페이지의 "최신 소프트웨어 버전 보기"
라이선스 정보 보기	36페이지의 "라이선스 정보 보기"
시스템 구성 보기 페이지	37페이지의 "시스템 구성 보기 페이지"

제품 개요

네트워크는 계속 확장되므로 네트워크 토폴로지가 점점 더 복잡해지고 있습니다. 또한 다수의 네트워크에서 이제 규정과 보안 모범 사례를 준수해야 합니다. 이로 인해 여러 프로토콜, 기술 및 공급업체가 포함된 복잡한 인프라를 지원하게 됩니다.

네트워크 인프라를 안전하고 자동화된 중앙 관리 방식으로 중점적으로 관리하는 작업은 추가 보안 취약점에서부터 전체 정지에 이르기까지 모든 성능에 극히 중대한 영향을 끼치게 되었으며, 이러한 모든 영향으로 인해 부채가 증가하고, 매출이 떨어지고, 생산성이 저하될 수도 있습니다.

HP NA(Network Automation)는 라우터, 스위치, 방화벽, 로드 밸런서 및 무선 액세스 지점에서의 구성과 소프트웨어 변경 사항을 추적하고 규제하는 엔터프라이즈급 솔루션을 제공합니다. 또한 IT 직원이 준수 문제, 보안 위험 및 재해 복구 위험을 줄이는 동안 문제를 발생시킬 수 있는 추세를 식별 및 수정할 수 있도록 네트워크 변경 사항을 표시합니다. NA는 각각의 장치 변경에 대한 전체 감사 추적 정보를 캡처하기도 합니다.

네트워크 엔지니어는 NA를 사용하여 다음 사항을 정확히 나타낼 수 있습니다.

- 변경된 장치 구성
- 구성 시 정확히 변경된 사항
- 변경을 수행한 사람
- 변경을 수행한 이유

또한 NA는 구성이 미리 정의된 표준을 준수하는지 확인하여 보안 및 규정 정책을 네트워크 수준에서 적용할 수 있습니다. 그 결과 결국에는 표준 및 규정을 준수하는, 탄력적이고 유지 보수가 가능한 네트워크를 구현할 수 있습니다.

NA는 HP, Cisco, Nortel, F5 Networks 및 Extreme을 비롯하여 업계를 선도하는 공급업체의 장치를 다수 지원하여 네트워크 변경 프로세스에 대한 식견을 얻을 수 있게 합니다. NA의 확장 가능한 아키텍처를 사용하면 최고 공급업체들의 가장 뛰어난 장치를 통합하여 도구 하나만으로도 모든 장치를 지원할 수 있게 됩니다.

참고: NA 9.10 설치 또는 NA 9.10으로 업그레이드에 대한 자세한 내용은 *Network Automation 9.10 업그레이드 및 설치 설명서*를 참조하십시오.

NA 7.50 기능

NA 7.50에는 다음과 같은 새로운 기능이 포함되었습니다.

- Bare Metal 프로비전 — 기본 제공 상태로 장치를 프로비전합니다. Bare metal 드라이버를 사용하면 Bare metal 장치에 대해 스크립트를 실행하여 완전히 구성된 장치를 프로덕션 네트워크에 제공할 수 있습니다.
- 네트워크 장치 템플릿 — 실제 장치를 제공하지 않고 구성 템플릿을 만듭니다. 네트워크 장치 템플릿을 사용하여 준수 확인, 정책 규칙 만들기, 구성 보기 및 비교(템플릿과 실제 장치 간에도 적용), 암호 규칙 설정 등을 수행한 후 프로덕션 네트워크에 장치를 추가할 수 있습니다.
- 보안 파티션 — 파티션별로 NA 객체 집합을 설정하여 보다 세부적인 권한을 지정합니다. NA 객체에는 장치, 사용자, 명령 스크립트, 장치 암호 규칙, 정책, 소프트웨어 이미지 등이 포함될 수 있습니다. 보안 파티션은 권한 모델, 그룹 계층, NA 코어 간 장치 배포 및 네트워크 다이어그램과 결합될 수 있습니다.
- 자동 수정 스크립트 — 위반된 정책 규칙의 정규 표현식 패턴 그룹에서 데이터를 참조하는 변수를 스크립트에 정의합니다. 자동 수정 팝업 창에서는 정책 규칙 페이지의 데이터에 액세스하여 변수 매핑을 표시하고, 샘플 코드를 생성하며, 스크립트를 저장하기 전에 검증할 수 있습니다. 표준 명령 스크립트와 달리 자동 수정 스크립트에서는 새로운 언어 구문을 사용하여 일치하는 항목을 반복합니다. 자동 수정 스크립트는 네트워크 장치에서 실행되는 명령 스크립트로 처리되고 변환됩니다.
- NNMi 통합 — NA를 NNMi와 통합하여 단일 서버에 상주하도록 합니다. 따라서 다음을 수행할 수 있습니다.
 - NNMi에서 장치 정책 준수 보고서 시작
 - NNMi 명령 스크립트 및 진단 시작
 - NNMi로 기본 제공 명령 스크립트 및 진단에 연결
 - 변경 작업을 수행 중인 장치에 대해 서비스 중지 지정
 - 변경된 커뮤니티 문자열을 NNMi에 자동 전파
 - 필요한 NNMi 관리 설정에 대해 새 장치 자동 구성
 - 이종 및 속도 불일치 상태에 대해 사용자에게 경고

- VoIP 지원 — VoIP 관리의 주요 요소는 다음과 같습니다.
 - 네트워크 장치 내에서 VoIP, MPLS, PoE 및 BGP 구성 요소 자동 검색
 - 특정 인터페이스에 대한 인터페이스 구성 요약에서 인터페이스 QoS 및 ACL 구성 섹션을 자동으로 구문 분석 및 표시
 - 구성 준수 확인 및 기본 장치 진단이 가능한 Cisco CallManager용 장치 드라이브
- 게이트웨이 서버의 SWIM(소프트웨어 이미지 관리) 프로세스 — 원격 장치에 대해 SWIM 중심 데이터를 표시합니다. 그러나 원격 장치는 NA 게이트웨이를 통해서만 연결할 수 있는 장치로 정의됩니다.
- HP OO(Operations Orchestration) 통합 — NA에서 타사 공급업체의 호스트와 상호 작용할 수 있습니다.

NA 7.60 기능

NA 7.60에는 다음과 같은 새로운 기능이 포함되었습니다.

- Solaris 64비트 지원 - Solaris 플랫폼에 NA를 설치하는 경우 NA에서 64비트 JVM(Java Virtual Machine)이 사용됩니다. 따라서 NA에서는 더 많은 메모리를 사용할 수 있습니다.
- 향상된 작업 예약 - 작업을 생성하거나 업데이트할 때 다른 작업보다 더 높은 우선 순위로 실행되도록 지금 작업에 대한 우선 순위를 설정할 수 있습니다. 작업 우선 순위 수준에는 1 ~ 5가 있습니다. 1은 최고 작업 우선 순위 수준입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 또한 그룹 작업에서 새 라운드-로빈 알고리즘을 사용할 수 있습니다. 예를 들어 라운드-로빈 알고리즘을 사용하여 오전 10시에 10,000대 장치에 대해 그룹 작업을 시작하고 나서 오전 10시 5분에 10대 장치에 대한 그룹 작업을 시작한 경우 두 번째 그룹 작업이 시작되기 전에 첫 번째 그룹 작업이 완료될 때까지 더 이상 기다릴 필요가 없습니다.
- 향상된 장치 선택기와 장치 그룹 탐색기 - 향상된 장치 선택기와 장치 그룹 탐색기를 사용하면 그룹 트리를 쉽게 탐색하여 다양한 응용 프로그램의 장치 및 장치 그룹을 선택할 수 있습니다.

- 포트 지원당 다중 VLAN — NA에서는 네트워크 스위치의 VLAN을 보고 프로비전할 수 있습니다. NA를 사용하여 다음을 수행할 수 있습니다.
 - 장치 VLAN의 전체 목록 보기
 - 특정 VLAN 세부사항 보기
 - VLAN에 할당된 포트 목록 보기
 - 트렁크 포트 보기
 - 트렁크 포트의 VLAN 목록 보기
 - 트렁크 포트의 기본 VLAN 보기(트렁크 포트의 트래픽에 태그가 지정되지 않은 VLAN)
 - 네트워크 스위치의 VTP 설정 보기
 - 네트워크 스위치의 새 VLAN 작성
 - VLAN에 할당된 포트 변경(포트 추가/정리)
 - VLAN 삭제
 - 포트를 트렁크 포트 구성(태그 지정 사용하는 여러 VLAN)
 - 트렁크 포트 VLAN(VLAN 멤버십) 변경
 - 트렁크 포트 기본 VLAN 변경
 - 트렁크 포트를 비 트렁크로 구성
- 가상 장치 및 가상 컨텍스트 지원 — 이제 NA에서는 VMware의 Infrastructure(ESX) 및 Cisco Nexus 1000V 시리즈 스위치를 통해 사용할 수 있는 VMware의 vSwitch(Virtual Switch) 기술을 비롯하여 가상 장치에 대한 지원을 제공합니다. 이러한 새로운 가상 장치는 레거시 장치와는 별도로 관리할 수 있으므로 중앙 지원을 제공합니다. 가상 장치는 물론, Cisco FWSM(Firewall Services Module) 및 Cisco ACE Application Control Engine Module 등 가상 컨텍스트를 지원하는 장치에서 비 IP 주소 컨텍스트에 대한 관리를 제공하는 장치 관계 향상과 실제 하드웨어와 가상 컨텍스트 간 기본 관계 파악을 활용할 수 있습니다.
- 장치 관계 — 장치 관계는 상위, 피어 및 하위 장치에 대한 데이터를 유지합니다. 장치 종속성은 새로운 장치 관계 API를 통해 정의할 수 있습니다.

- 연결 집계 지원 — 연결 집계 지원을 통해 NA는 장치의 특정 포트와 연관된 모든 링크 또는 연결을 나열할 수 있습니다. 이 정보는 향상된 진단이나 새 장치 컨텍스트 정보에서 수집됩니다. 연결 집계를 사용하면 여러 연결을 물리적 포트에 할당하는 가상 컨텍스트를 사용하여 장치를 관리할 수 있습니다.
- 연결 경로 향상 — 이제는 기본 IP 주소를 통해 장치 액세스를 활성화 또는 비활성화할 수 있습니다.
- API 향상 프로비전 및 스크립팅 — 이제는 장치 관계 API를 사용하여 장치 템플릿을 나열하고 장치 템플릿 구성을 표시하며 장치 템플릿 구성을 수정하고 장치를 프로비전할 수 있습니다.

NA 9.0 기능

다음은 NA 9.0에 포함된 기능입니다.

- 빠른 시작 — 이제는 작업을 사용자 지정하고 현재 페이지에서 탐색할 필요 없이 미리 작성된 데이터로 작업을 빨리 시작할 수 있습니다.
- 작업 템플릿 — 작업 템플릿을 사용하면 작업 정의를 저장할 수 있으므로 처음부터 다시 시작하지 않더라도 새로운 작업과 기존 작업을 쉽게 구성 및 실행할 수 있습니다.
- 간소화된 정책 관리자 — 이제 장치에 적용되는 정책을 볼 수 있습니다. 따라서 다음을 수행할 수 있습니다.
 - 현재 정책이 장치에 적용되었는지 확인
 - 정책 통과/실패 여부 보기
 - 장치가 NA에 추가될 때 장치에 적용되는 정책 보기
 - 장치에 적용된 정책에 대한 예외 보기

- Nmap 포트 스캔 — 이제 네트워크 장치 탐색 시 Nmap을 사용할 수 있습니다. Nmap은 장치의 포트를 검색하고 열린 포트와 해당 포트에서 제공하는 서비스에 대한 세부 사항을 반환하는 데 사용할 수 있습니다. 포트 스캔 작업을 실행하여 다음을 수행할 수 있습니다.
 - 장치에서 열려 있거나 닫힌 포트가 어느 것인지 쉽게 확인
 - TCP 스택, OS 검색 및 기타 Nmap 제공 서비스에 따라 장치의 취약성 파악
- 구성 파일 구문 분석 — 쉬운 탐색을 위해 구성 텍스트 바로 위에 구성 파일의 섹션에 대한 구문을 쉽게 분석할 수 있도록 하는 링크가 있습니다. 예를 들어 구성 파일에 Access List 섹션이 포함된 경우 구성 파일의 맨 위에 있는 Access List 링크를 클릭하여 해당 섹션으로 바로 이동할 수 있습니다. 현재는 Cisco IOS 일반 드라이버에서만 섹션 구문 분석을 지원합니다.
- SecurID 사용자 장치 인증 — 설치 시 NA 설치 프로그램은 *NA_DIRECTORY/jre* 디렉터리에 *rsa_api.properties* 파일을 설치합니다. RSA 서버 인증 관리자를 통해 생성되는 RSA conf 파일의 위치와 NA가 상주하는 서버의 IP 주소를 포함하도록 이 파일을 편집할 수 있습니다.
- FTP 서버 지원 — NA에는 통합된 FTP 서버가 있으며 NA에서는 일반적으로 CLI를 통해 장치에 액세스하여 장치와의 데이터 전송을 설정합니다.
- 장치 작동 시간 — 감지 장치 부팅 진단이 장치에 대해 마지막으로 실행된 시점과 장치 작동 시간을 검색할 수 있습니다.
- NA 사용자 암호 만료 — 다음 옵션은 새 사용자 프로필을 작성하거나 기존 사용자 프로필을 편집할 때 NA 시스템 관리자의 새 사용자 페이지 및 사용자 편집 페이지에 표시됩니다.
 - 사용자는 다음 로그인 시에 암호를 변경해야 함
 - 사용자는 암호를 변경할 수 없음
 - 암호 만료 안 함
 - 계정이 잠김
- NA 9.0에서는 더욱 쉬운 탐색과 업데이트된 내 작업 공간 영역을 위한 새로운 기본 메뉴 드롭다운 메뉴 등 보다 직관적인 사용자 인터페이스를 제공합니다.

- CLI/API에서 사용자 지정 데이터 필드 설정 — 이전에 몇몇 CLI 명령에는 customname 및 customvalue 옵션 사용을 통해 사용자 지정 필드를 수정할 수 있는 기능이 있었습니다. 하지만 한 번에 한 필드만 조작할 수 있었습니다. 이러한 제한이 여러 필드를 수정해야 하는 경우에는 다소 불편하기도 했습니다. 따라서 새로운 customnames 및 customvalues 값을 사용하면 여러 필드를 동시에 수정할 수 있습니다.
- 새 검색 및 보고 아키텍처 — 새 검색 및 보고 아키텍처를 사용하면 NA에서 검색 결과를 좀더 신속하게 표시할 수 있습니다. 또한 새 데이터 유형 필드를 쉽게 추가, 삭제 또는 수정할 수도 있습니다.
- 향상된 로깅 및 문제 해결 — 이제는 문제 해결 정보를 보고할 때 서버 로그, 작업 로그 및 랩퍼 로그 정보를 제공할 수 있습니다.
- NA 9.0에는 다음 플랫폼에 대한 지원이 포함됩니다.
 - Windows 2008 64비트
 - Oracle 11g
 - 64비트 Linux
 - MS SQL 2008

NA 9.10 기능

다음은 NA 9.10에 포함된 기능입니다.

- Autopass — NA 9.10 라이선스에는 두 가지 유형이 있습니다.
 - InstantOn - InstantOn NA 9.10 라이선스는 제품과 함께 제공됩니다. 각 InstantOn 라이선스는 제품 설치 후 250대 장치 및 60일 사용 기간으로 제한됩니다.
 - 영구 — 영구 NA 9.10 라이선스는 HP License Key Delivery Service를 통해 얻어야 합니다. 영구 NA 9.10 라이선스에는 만료일이 없으며 Horizontal Scalability 또는 다중 마스터 분산 시스템과 같은 NA 추가 기능과 함께 사용할 수 있습니다. NA 라이선스에 대한 자세한 내용은 *Network Automation 9.10 업그레이드 및 설치 설명서*를 참조하십시오.

- 장치 그룹 보기 — 이제는 상위 구조 내 상위 그룹 관점에서 장치 목록을 볼 수 있습니다. 이 기능을 사용하면 원하는 상위 그룹의 관점에서 장치를 일괄적으로 편집할 수 있습니다. 또한 이제 장치 그룹 페이지가 트리로도 표현됩니다. 이 트리는 이전 다중 페이지 드릴다운 탐색 디자인을 대체합니다.
- 전자 메일 알림 — 이제 로그인한 NA 사용자와 전자 메일을 주고 받을 수 있습니다.
- 정책 관리자 API — 이제 NA API를 사용하여 정책을 만들 수 있습니다. 이제 정책 생성, 정책 내 규칙 생성, 규칙에 대한 수정 스크립트 생성, 기존 정책 수정 등 CLI 명령이 제공됩니다. 자세한 내용은 *Network Automation 9.10 API Reference Guide*를 참조하십시오.
- 향상된 검색 — 구성이나 진단 데이터 등 텍스트 및/또는 LOB 열을 검색할 때 성능이 향상되었습니다. 이제 전체 텍스트 편집기를 사용하여 장치 구성을 빠르게 검색할 수 있습니다.
- NNMi-NA 통합 — NNMi-NA 통합 커넥터는 더 이상 NA 9.10에서 사용되지 않습니다. NNMi-NA 통합은 두 제품 간 WebServices 호출을 통해 발생합니다. 새로운 NNMi-NA 통합에는 다음이 포함됩니다.
 - 배포 간소화
 - 토폴로지 동기화 안정성 향상
 - NNMi와 NA 간 동기화 속도 향상
 모든 NNMi-NA 통합 구성이 NNMi UI에서 수행됩니다. 자세한 내용은 *NNMi 9.10 Deployment Reference*를 참조하십시오. 새로운 NNMi-NA 통합 아키텍처로 인해 NA 9.10은 NNMi 9.10만 지원합니다.
- 단일 사인온 — 이제 동일한 사용자 자격 증명을 사용하여 NA 및 NNMi에 로그인할 수 있습니다. NA-NNMi 통합에 대한 자세한 내용은 *HP NNMi 9.10 Deployment Reference*를 참조하십시오.
- SNMP v3 지원 — 장치 검색 시 SNMPv3을 사용하는 네트워크 장치를 검색할 수 있습니다. SNMPv3 프로토콜을 사용하는 경우 보안이 약한 네트워크 장치 검색 방법이 사용되지 않으므로 최신 SNMP 보안 메커니즘을 사용할 수 있습니다.

기본 메뉴 모음

HP Network Automation 로그아웃					
장치	작업	정책	보고서	관리	도움말
<ul style="list-style-type: none"> 인벤토리 그룹 새로 만들기 장치 템플릿 장치 그룹 상위 그룹 새 장치 마법사 	<ul style="list-style-type: none"> 내 작업 승인 요청 새 멀티 태스킹 프로젝트 작업 로드 활동 캘린더 작업 템플릿 예정된 작업 실행 중인 작업 최근 작업 	<ul style="list-style-type: none"> 정책 목록 새 정책 정책 가져오기 / 내보내기 정책 활동 정책 준수 정책 준수 테스트 소프트웨어 수준 정책 작업 정책 준수 확인 	<ul style="list-style-type: none"> 단일 보기 단일 검색 사용자 및 시스템 보고서 검색 대상 장치 인터페이스 모듈 정책 준수 구성 진단 작업 텔넷 / SSH 세션 이벤트 사용자 ACL MAC 주소 IP 주소 VLAN 장치 템플릿 고급 검색 준수 센터 네트워크 상태 모범 사례 장치 상태 통계 대시보드 다이어그램 작성 장치 소프트웨어 소프트웨어 취약점 이미지 동기화 보고서 시스템 및 네트워크 / 이벤트 요약 보고서 보고서 작업 요약 보고서 생성 전자 메일 보고서 	<ul style="list-style-type: none"> 사용자 사용자 그룹 새 사용자 새 사용자 그룹 로그온한 사용자 사용자 역할 및 권한 보안 파티션 게이트웨이 장치 암호 규칙 이벤트 알림 및 응답 규칙 사용자 지정 데이터 설정 LDAP 설정 워크플로 설정 관리 설정 구성 관리 장치 액세스 서버 워크플로 사용자 인터페이스 텔넷 / SSH 보고 사용자 인증 서버 모니터링 타사 통합 작업 로드 시스템 상태 서비스 시작 / 중지 문제 해결 드라이버 시스템 작업 가져오기 네트워크 장치 감지 중복 방지 OS 분석 원격 에이전트 배포 FQDN 확인 데이터 정리 외부 응용 프로그램 실행 	<ul style="list-style-type: none"> 문서 지원 HP Live Network HP Network Automation 정보
<ul style="list-style-type: none"> 구성 변경 장치 도구 명령 스크립트 구성 템플릿 장치 암호 규칙 장치 템플릿 진단 정책 소프트웨어 이미지 VTP 도메인 	<ul style="list-style-type: none"> 새 작업 Syslog 구성 암호 배포 드라이버 검색 장치 재부팅 ICMP 테스트 실행 명령 스크립트 실행 진단 실행 스냅샷 작성 시작 및 실행 동기화 장치 소프트웨어 업데이트 가져오기 네트워크 장치 감지 중복 방지 OS 분석 포트 스캔 템플릿에서 장치 프로비전 		<ul style="list-style-type: none"> 중급 검색 네트워크 상태 모범 사례 장치 상태 통계 대시보드 다이어그램 작성 장치 소프트웨어 소프트웨어 취약점 이미지 동기화 보고서 시스템 및 네트워크 / 이벤트 요약 보고서 보고서 작업 요약 보고서 생성 전자 메일 보고서 	<ul style="list-style-type: none"> 관리 설정 구성 관리 장치 액세스 서버 워크플로 사용자 인터페이스 텔넷 / SSH 보고 사용자 인증 서버 모니터링 타사 통합 작업 로드 시스템 상태 서비스 시작 / 중지 문제 해결 드라이버 시스템 작업 가져오기 네트워크 장치 감지 중복 방지 OS 분석 원격 에이전트 배포 FQDN 확인 데이터 정리 외부 응용 프로그램 실행 	
<ul style="list-style-type: none"> 장치 작업 정책 준수 확인 Syslog 구성 암호 배포 드라이버 검색 장치 재부팅 ICMP 테스트 실행 명령 스크립트 실행 진단 실행 스냅샷 작성 시작 및 실행 동기화 장치 소프트웨어 업데이트 가져오기 네트워크 장치 감지 중복 방지 OS 분석 템플릿에서 장치 프로비전 	<ul style="list-style-type: none"> 정책 준수 확인 요약 보고서 생성 전자 메일 보고서 원격 에이전트 배포 FQDN 확인 데이터 정리 외부 응용 프로그램 실행 		<ul style="list-style-type: none"> 중급 검색 네트워크 상태 모범 사례 장치 상태 통계 대시보드 다이어그램 작성 장치 소프트웨어 소프트웨어 취약점 이미지 동기화 보고서 시스템 및 네트워크 / 이벤트 요약 보고서 보고서 작업 요약 보고서 생성 전자 메일 보고서 	<ul style="list-style-type: none"> 관리 설정 구성 관리 장치 액세스 서버 워크플로 사용자 인터페이스 텔넷 / SSH 보고 사용자 인증 서버 모니터링 타사 통합 작업 로드 시스템 상태 서비스 시작 / 중지 문제 해결 드라이버 시스템 작업 가져오기 네트워크 장치 감지 중복 방지 OS 분석 원격 에이전트 배포 FQDN 확인 데이터 정리 외부 응용 프로그램 실행 	
<ul style="list-style-type: none"> ACL 삭제 ACL 라인 / 일괄 삽입 ACL 라인 / 일괄 제거 			<ul style="list-style-type: none"> 요약 보고서 보고서 작업 요약 보고서 생성 전자 메일 보고서 	<ul style="list-style-type: none"> 관리 설정 구성 관리 장치 액세스 서버 워크플로 사용자 인터페이스 텔넷 / SSH 보고 사용자 인증 서버 모니터링 타사 통합 작업 로드 시스템 상태 서비스 시작 / 중지 문제 해결 드라이버 시스템 작업 가져오기 네트워크 장치 감지 중복 방지 OS 분석 원격 에이전트 배포 FQDN 확인 데이터 정리 외부 응용 프로그램 실행 	

도움말 메뉴 옵션

다음 옵션은 도움말 드롭다운 메뉴에서 사용할 수 있습니다.

- 문서 — HP Network Automation 설명서 페이지를 엽니다. 상황에 맞는 온라인 도움말 정보는 각 NA 페이지의 도움말 링크에서 사용할 수 있습니다.
- 지원 — HP 고객 지원 센터 페이지를 엽니다. 이 사이트에서는 HP 고객에게 가장 최근의 패치 릴리스 및 설명서를 제공합니다. 또한 문제를 확인하고 해결하기 위해 파일을 업로드 할 수 있습니다.
- HP Live Network — HP Live Network 페이지를 엽니다. 이 페이지에서 보안 주의 서비스 데이터 및 기타 NA 콘텐츠 서비스 자료를 다운로드할 수 있습니다. HP Live Network는 HP Network Automation에 통합된 추가 콘텐츠 제공 서비스이며 네트워크 보안 및 준수 콘텐츠 업데이트를 정기적으로 제공합니다.

또한 HP Live Network 포털은 다음을 호스팅합니다.

- 드라이버 팩
- 전문화된 NDS 드라이버 개발 포럼
- 일반 NA 커뮤니티 포럼

HP Live Network 보안 및 준수 서비스를 통해 네트워크 보안 및 정책 위반을 즉시 평가할 뿐만 아니라 자동화된 수정 옵션을 제공할 수 있습니다. HP Live Network에서는 중요한 무료 콘텐츠 및 가입 서비스를 제공합니다. 자세한 내용은 [774페이지의 "소프트웨어 취약점 보고서"](#)를 참조하십시오.

참고: HP Live Network 서비스 설치에 대한 자세한 내용은 *HP Network Automation 9.10 업그레이드 및 설치 설명서*를 참조하십시오.

- HP Network Automation 정보 — HP Network Automation 정보 페이지를 엽니다. 이 페이지에서는 HP Network Automation에 대한 정보를 볼 수 있습니다. HP Network Automation 정보 페이지에 대한 자세한 내용은 [36페이지의 "최신 소프트웨어 버전 보기"](#)를 참조하십시오.

NA 홈 페이지

NA에 로그인할 때마다 NA 홈 페이지가 열립니다. 또한 각 페이지의 왼쪽 위 모서리에 있는 홈 링크를 클릭하여 NA 홈 페이지로 돌아갈 수 있습니다.

NA 홈 페이지에는 두 개 프레임이 포함되어 있습니다. 왼쪽 프레임에는 다음 항목이 포함됩니다.

- 검색 — 검색 옵션을 사용하면 호스트 이름이나 IP 주소별로 장치를 찾고 텔넷이나 SSH를 통해 이러한 장치에 연결할 수 있습니다. 자세한 내용은 [354페이지의 "검색/연결 기능"](#)을 참조하십시오.
- 내 작업 공간 — 내 작업 공간 영역에는 다음 섹션이 포함되어 있습니다.
 - 현재 장치/현재 장치 그룹(기본값은 인벤토리)
 - 내 즐겨찾기
 - 빠른 시작
 - 내 설정

내 작업 공간 영역의 옵션 구성에 대한 자세한 내용은 [338페이지의 "사용자 설정 편집"](#)을 참조하십시오.

오른쪽 프레임은 과거 24시간 동안의 최근 구성 변경, 다양한 시스템 이벤트 및 사용자의 승인이 필요한 작업의 스냅샷을 포함하도록 사용자 지정할 수 있습니다. 자세한 내용은 [349페이지의 "NA 홈 페이지 사용자 지정"](#)을 참조하십시오.

명령 창 열기

명령 창을 열려면 화면의 왼쪽에 있는 검색 탭에서 장치 IP 주소나 호스트 이름을 입력하고 연결 버튼을 클릭합니다. 또한 연결 메뉴를 사용하여 장치 세부사항 페이지에서 명령 창을 열 수도 있습니다. 명령 창 내에서 복사할 텍스트를 선택하고 Enter 키를 누르면 됩니다. 강조 표시된 텍스트가 복사 버퍼에 저장됩니다. 다음에는 이 텍스트를 다른 응용 프로그램으로 붙여 넣을 수 있습니다. 작업을 완료한 후 `exit`를 입력하여 창을 닫습니다.

참고: 텔넷/SSH 프록시를 사용하여 장치에 직접 연결하는 경우 장치를 종료해도 텔넷/SSH 프록시에 남아 있습니다. 다시 `exit`를 입력하지 않는 한 CLI 명령을 입력하여 다른 장치에 연결할 수 있습니다.

CLI 명령에 대한 도움말을 보려면 `help`를 입력하여 모든 명령 목록을 표시합니다. 특정 명령에 대해 자세한 도움말을 보려면 `help <명령 이름>`을 입력합니다.

설명서 액세스

핵심 NA 설명서 집합에 포함되는 문서는 다음과 같습니다.

- *HP Network Automation 9.10 사용 설명서* — PDF 버전을 보려면 로그인한 후 도움말 드롭다운 메뉴에서 문서를 클릭합니다. HP Network Automation 설명서 페이지가 열리면 목록에서 *HP Network Automation 9.10 사용 설명서*를 선택합니다.
- 온라인 도움말 파일 — 온라인 도움말 파일을 보려면 로그인한 후 NA 페이지 맨 위에 있는 도움말 링크를 클릭합니다.
- *HP Network Automation 9.10 업그레이드 및 설치 설명서* — PDF 버전을 보려면 로그인한 후 도움말 드롭다운 메뉴에서 문서를 클릭합니다. HP Network Automation 설명서 페이지가 열리면 목록에서 *HP Network Automation 9.10 업그레이드 및 설치 설명서*를 선택합니다.
- *HP Network Automation 9.10 릴리스 노트* — PDF 버전을 보려면 로그인한 후 도움말 드롭다운 메뉴에서 문서를 클릭합니다. HP Network Automation 설명서 페이지가 열리면 목록에서 *HP Network Automation 9.10 릴리스 노트*를 선택합니다.

아래 나열된 문서를 포함하여 추가 NA 간행물을 보려면 NA 지원 사이트로 이동하십시오.

- *NA 9.10 Multimaster Distributed System on Oracle User's Guide*
- *NA 9.10 Multimaster Distributed System on SQL Server User's Guide*
- *NA 9.10 Horizontal Scalability User's Guide*
- *NA 9.10 Satellite User's Guide*

HP Network Automation 9.10 사용 설명서

HP Network Automation 9.10 사용 설명서에 포함된 내용은 다음과 같습니다.

- 시스템 설정 및 구성
- 장치 및 장치 그룹 추가 및 구성
- 사용자, 그룹 및 역할 추가
- 워크플로 생성
- SecurID, TACACS+ 및 RADIUS를 사용하여 네트워크 장치에 액세스
- LDAP에서 사용자 및 사용자 그룹 가져오기
- ACL(액세스 제어 목록) 관리
- 준수 센터 사용
- 정보 검색, 사용자 지정 보고서 생성 및 요약 보고서 실행
- 구성 배포
- VLAN 보기 및 프로비전
- 장치 관계 구성
- 이벤트 규칙 및 이벤트 알림 생성
- 기본 진단 보기
- 진단 및 명령 스크립트 생성 및 실행
- 일관성 유지를 위해 회사 전체의 정책 규칙 생성
- 중앙 리포지토리에서 장치 소프트웨어 배포
- 텔넷 및 SSH를 사용하여 장치 연결

- 명령줄 인터페이스(CLI) 실행
- Java 및 PERL API을 사용하여 다른 IT 응용 프로그램과 데이터 교환
- 온라인 도움말 사용, 고객 지원 센터에 문의 및 소프트웨어 라이선스 업데이트

참고: *HP Network Automation 9.10 사용 설명서*는 NA 시스템 관리자가 사용할 수 있는 모든 옵션에 대한 정보를 제공합니다. 사용 권한에 따라 일부 NA 메뉴 옵션이 회색으로 표시될 수 있습니다.

다음 표에서는 *HP Network Automation 9.10 사용 설명서*에서 사용되는 규칙에 대해 설명합니다.

규칙	설명/작업
<i>기울임꼴</i>	시스템 메시지, 경로, 파일 이름 및 Web URL에 사용됩니다. 예를 들면 <code>C:\hp\sdk\docs</code> 와 같습니다.
링크	문서 내 한 위치에서 다른 위치로 이동하거나, 웹 페이지를 열거나 또는 새 전자 메일 메시지를 엽니다. 사용 설명서에서 상호 참조는 따옴표 안에 포함되고 페이지 번호가 있으며, URL 및 전자 메일 주소로 링크하는 동안 텍스트가 밑줄로 표시됩니다.
Enter	다음에 나오는 텍스트 또는 명령을 입력하고 키보드의 Enter 키를 눌러야 함을 나타냅니다.
< >	제공해야 하는 이름 또는 폴더와 같은 변수 정보를 나타냅니다. 자리 표시자를 바꿀 때 꺾쇠 괄호가 포함되면 안 됩니다.

고객 지원 센터에 문의

HP Software Support Online 웹 사이트를 방문할 수 있습니다.

<http://www.hp.com/go/hpsoftwaresupport>

이 웹 사이트에서는 연락처 정보뿐만 아니라 HP Software에서 제공하는 제품, 서비스 및 지원에 대한 세부 정보를 제공합니다.

문제를 보고하려면 가능한 많은 컨텍스트를 포함하십시오.

HP에서 다르게 동의하지 않는 한 HP는 HP Software Supported Version Policy에 따라 현재 주 릴리스의 현재 및 이전 부 버전과 이전 주 릴리스의 최신 부 버전에 대한 지원을 제공합니다.

제품의 새로운 주 버전을 사용할 수 있게 되는 경우:

- 새로운 주 버전 및 현재 주 버전에 대한 지원이 제공됩니다.
- 현재 주 버전보다 두 버전 아래의 주 버전에 대한 마지막 부 버전에 대해서는 EOS(End-of-Support)가 발생합니다.

예를 들어 NA 9.10이 릴리스되면

NA 7.50 및 NA 7.60과 함께 해당 버전도 지원됩니다. 그러나 NA 7.00은 더 이상 지원되지 않습니다.

문제 해결 보내기 페이지 필드

고객 지원 센터에 문제 해결 정보를 보내려면

1. 관리 아래에 있는 메뉴 모음에서 문제 해결을 클릭합니다. 문제 해결 페이지가 열립니다.
2. 페이지의 맨 위에 있는 문제 해결 정보 보내기 링크를 클릭합니다. 문제 해결 정보 보내기 페이지가 열립니다.

참고: 로그 파일에 액세스하려면 관리 권한이 있어야 합니다.

필드	설명/작업
받는 사람	전자 메일 주소가 표시되지 않으면 전자 메일 주소를 입력합니다.
제목	제목 라인으로, "HP Network Automation 정보"가 표시됩니다.
문제 번호	해당하는 경우 열려 있는 티켓과 관련된 문제 번호를 입력합니다.
주석	문제에 대한 설명을 입력합니다. 회신 전자 메일 주소 및 직통 전화(또는 휴대폰 번호)를 포함해야 합니다. 파일에 있는 연락처 정보의 대상은 문제가 있는 사람이 아닐 수도 있습니다.
포함	다음 옵션 중 하나 이상을 선택합니다. <ul style="list-style-type: none"> • 지난 < >시간 동안의 서버 로그 — 보내려는 로그를 저장한 시간을 입력합니다. 기본값은 4입니다. • 관리 설정 — NA 서버에 유효한 관리 설정 및 옵션 모음을 포함합니다. • 시스템 상태 파일 — 시스템 상태 정보를 제공하기 위해 생성한 파일입니다. • 래퍼 로그 — 요청 시 Jboss_Wrapper 로그 파일이 전송됩니다. • 작업 로그 — 사용할 수 있는 작업 로그 파일 목록입니다. 각 파일에는 작업 유형, 작업 ID, 장치(해당하는 경우) 및 작업 완료 시간이 나열되어 있습니다.

완료되면 보내기를 클릭해야 합니다.

참고: 문제 해결 정보 다운로드 페이지에서 문제 해결 정보를 다운로드할 수 있습니다. 받는 사람, 제목, 문제 번호 또는 설명 필드가 없는 경우를 제외하고, 이 페이지는 문제 해결 보내기 페이지와 동일합니다. 또한 보내기 버튼은 다운로드로 나타납니다.

최신 소프트웨어 버전 보기

HP Network Automation 정보 페이지를 보려면 도움말 드롭다운 메뉴에서 HP Network Automation 정보를 클릭합니다. HP Network Automation 정보 페이지가 열립니다.

현재 NA 소프트웨어 버전에 대한 자세한 내용을 볼 수 있습니다. 또한 이 페이지에 포함되는 링크는 다음과 같습니다.

- 드라이버 업데이트 패키지 다운로드 — HP BSA Essentials Network 웹 사이트를 표시합니다.
- 최신 릴리스 노트 보기 — HP Passport 로그인 페이지를 표시합니다.
- 라이선스 정보 보기 — 자세한 내용은 [36페이지의 "라이선스 정보 보기"](#)를 참조하십시오.
- 고객 지원 센터에 문의 — Software Support Online 웹 사이트를 표시합니다.
- 시스템 구성 보기 — 자세한 내용은 [37페이지의 "시스템 구성 보기 페이지"](#)를 참조하십시오.

또한 시스템에 설치된 장치 드라이버 목록을 제공합니다. 지원되는 장치에 대한 자세한 내용은 DRS(장치 릴리스 서비스) 설명서를 참조하십시오. DRS는 자동화된 새로운 드라이버 릴리스 및 전달 시스템입니다.

라이선스 정보 보기

라이선스 정보 페이지에서는 다음 사항을 확인할 수 있습니다.

- 제품 라이선스 소유자
- 라이선스에 포함된 노드 수
- 사용 중인 노드 수
- 라이선스 만료 시기

이 페이지에서 라이선스를 업데이트할 수도 있습니다.

라이선스 정보 페이지를 보려면

1. 도움말 드롭다운 메뉴에서 HP Network Automation 정보를 클릭합니다. HP Network Automation 정보 페이지가 열립니다.
2. 라이선스 정보 보기 링크를 클릭합니다. 라이선스 정보 페이지가 열립니다.

필드	설명/작업
제품	사용이 허가된 소프트웨어 버전을 표시합니다.
라이선스 부여 대상	회사 또는 부서 이름을 표시합니다.
라이선스가 부여된 노드 수	소프트웨어에서 인식할 수 있는 노드 수를 표시합니다. Cisco 6500과 같은 일부 장치에는 별도의 노드로 작동하는 카드가 포함되어 있음에 주의하십시오.
사용 중인 노드 수	NA에서 활성화된 노드 수를 표시합니다.
라이선스 만료	소프트웨어 라이선스 만료 시기를 표시합니다.
라이선스 업데이트 버튼	소프트웨어 라이선스를 업데이트 할 시기가 되면 HP에서는 사용자에게 새 라이선스 텍스트를 보냅니다. 새 라이선스를 설치하려면 입력란에 해당 텍스트를 붙여넣은 다음 라이선스 업데이트를 클릭합니다.

시스템 구성 보기 페이지

분산 시스템이 활성화되고 NA 코어를 구성한 경우 시스템 구성 보기 페이지에서 다음 사항을 확인할 수 있습니다.

- NA 코어 구성 수
- 파티션 구성 수


IP 네트워크와 제한된 장치 및 사용자 보기 오버랩에 대한 자세한 내용은 [191페이지의 "장치 및 사용자 세분화"](#)를 참조하십시오. 다중 마스터 분산 시스템 설치 및 구성에 대한 자세한 내용은 *HP Network Automation 9.10 Multimaster Distributed System on Oracle User's Guide* 또는 *HP Network Automation 9.10 Multimaster Distributed System on SQL Server User's Guide*를 참조하십시오.

2장: 관리 설정 구성

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	41페이지의 "시작하기"
구성 관리	42페이지의 "구성 관리"
장치 액세스	56페이지의 "장치 액세스 페이지 필드"
서버	67페이지의 "서버"
워크플로	77페이지의 "워크플로"
사용자 인터페이스	80페이지의 "사용자 인터페이스"
텔넷/SSH	85페이지의 "텔넷/SSH"
보고	90페이지의 "보고"
사용자 인증	97페이지의 "사용자 인증"
LDAP 인증 설정	106페이지의 "LDAP 외부 인증 설정"
서버 모니터링	110페이지의 "서버 모니터링"
타사 통합	115페이지의 "타사 통합"
모니터링 결과 보기	117페이지의 "모니터링 결과 보기"
서비스 시작 및 중지	123페이지의 "서비스 시작 및 중지"
로깅	125페이지의 "로깅"
드라이버 검토	131페이지의 "드라이버 검토"

관리 설정 탐색

 HP Network Automation 로그아웃					
장치 ▾	작업 ▾	정책 ▾	보고서 ▾	관리 ▾	도움말 ▾
▼					
<div style="border: 1px solid black; padding: 5px;"> <ul style="list-style-type: none"> 사용자 사용자 그룹 새 사용자 새 사용자 그룹 로그온한 사용자 </div>					
<div style="border: 1px solid black; padding: 5px;"> <ul style="list-style-type: none"> 사용자 역할 및 권한 </div>					
<div style="border: 1px solid black; padding: 5px;"> <ul style="list-style-type: none"> 보안 파티션 게이트웨이 장치 암호 규칙 이벤트 알림 및 응답 규칙 </div>					
<div style="border: 1px solid black; padding: 5px;"> <ul style="list-style-type: none"> 사용자 지정 데이터 설정 향상된 사용자 지정 데이터 설정 LDAP 설정 워크플로 설정 </div>					
<div style="border: 1px solid black; padding: 5px;"> <ul style="list-style-type: none"> 관리 설정 ▶ 구성 관리 장치 액세스 서버 워크플로 사용자 인터페이스 텔넷 /SSH 보고 사용자 인증 서버 모니터링 타사 통합 </div>					
<div style="border: 1px solid black; padding: 5px;"> <ul style="list-style-type: none"> 작업 로드 시스템 상태 서비스 시작 / 중지 문제 해결 드라이버 </div>					
<div style="border: 1px solid black; padding: 5px;"> <ul style="list-style-type: none"> 시스템 작업 ▶ </div>					

시작하기

시스템 관리자는 HP NA(Network Automation) 운영에 영향을 주는 구성 가능한 설정에 대한 값을 정의할 수 있습니다. 이러한 설정은 설치 중 초기 값을 수신하지만, 사용자가 값을 변경하여 기능을 사용자 지정할 수 있습니다. 예를 들어, 다양한 운영과 연관된 간격에 대한 기본값을 변경하거나, 스크립트 작성 언어에 대한 지원을 구성할 수 있습니다. 또한 특정 페이지의 모양과 내용을 사용자 지정할 수 있습니다.

구성 옵션을 검토하고 변경 작업을 하려면 관리 아래의 메뉴 모음에서 관리 설정을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다.

- 구성 관리
- 장치 액세스
- 서버
- 워크플로
- 사용자 인터페이스
- 텔넷/SSH
- 보고
- 사용자 인증
- 서버 모니터링
- 타사 통합

구성 관리

구성 관리 페이지에서 다음을 구성할 수 있습니다.

- 구성 변경 감지
- 사용자 ID
- 시작 및 실행 구성
- ACL 구문 분석 및 편집
- 구성 정책 확인
- 사전 작업 및 사후 작업 스냅샷
- 진단
- 플래시 저장 공간
- 부팅 감지
- 사용자 지정 서비스 유형

구성 관리 페이지를 보려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 구성 관리를 클릭합니다. 구성 관리 페이지가 열립니다. 변경 사항을 저장하려면 저장을 클릭해야 합니다.

구성 관리 페이지 필드

필드	설명/작업
변경 감지	
변경 감지	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •사용함 — 변경 사항이 감지될 때마다 NA가 장치 구성 스냅샷을 가져옵니다(기본값). •폴링만 — NA가 장치 그룹 스냅샷 도중에는 장치 구성 스냅샷을 가져오지만 변경 사항이 감지될 때는 스냅샷을 가져오지 않습니다. •사용 안 함 — 감지된 변경 사항에 대한 응답으로 또는 장치 그룹 스냅샷 도중 구성 스냅샷을 가져오지 않습니다. <p>변경 감지에 대한 자세한 내용은 51페이지의 "변경 감지"를 참조하십시오.</p>
변경 감지 간격	<p>변경 감지와 스냅샷 간의 지연 간격(분)을 입력합니다. 기본값은 10분입니다. NA가 변경 사항을 감지할 때 여기에 지정된 간격 동안 장치 스냅샷이 지연됩니다. 후속 스냅샷은 간격 중 전송된 모든 변경 알림을 반영합니다.</p>
Syslog 감지 패턴	<p>NA가 제공한 기본 패턴에 패턴을 추가하려면 오른쪽 상자에 패턴을 입력하고 패턴 추가 <<를 클릭합니다. 왼쪽 상자에서 패턴을 선택하고 패턴 삭제를 클릭하여 패턴을 삭제할 수 있습니다. NA가 Syslog 서버에서 이러한 패턴과 일치하는 항목을 찾습니다. NA가 일치 항목을 찾으면 구성 변경을 나타내고 장치 구성의 스냅샷을 가져옵니다(위에서 이 기능을 활성화한 경우). (참고: HP는 Syslog 서버를 제공합니다. NA를 설치할 때 현재 Syslog 서버를 유지한 경우에도 NA Syslog 서버를 설치하고 Syslog 메시지를 NA Syslog 서버로 중계해야 합니다.)</p> <p>Syslog 메시지 패턴에 대한 자세한 정보는 52페이지의 "Syslog 메시지"를 참조하십시오.</p>
무시할 Syslog 패턴	<p>패턴을 무시하려면 오른쪽 상자에 패턴을 입력하고 패턴 추가 <<를 클릭합니다. 왼쪽 상자에서 패턴을 선택하고 패턴 삭제를 클릭하여 패턴을 삭제할 수 있습니다.</p>

필드	설명/작업
보조 IP 유형	<p>보조 IP 유형을 선택합니다. 기본적으로 기본 및 대체 유형이 선택됩니다. 보조 IP 유형은 보조 IP 주소에 대한 변경 감지 Syslog 이벤트 처리에 사용됩니다. 모든 보조 IP 주소가 Syslog 이벤트 처리에 포함됩니다. 다음 옵션 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 기본 • 대체 • 콘솔 • 홉 상자 • NAT • 통과 연결 • 내부 통과 • 내부 직접 <p>진단 관리에 대한 자세한 내용은 307페이지의 "장치에서 관리되는 IP 주소 페이지 필드"를 참조하십시오.</p>
Syslog 메시지의 보낸 사람 IP 주소 사용	이 옵션을 선택하면 Syslog 메시지 보낸 사람의 IP 주소가 사용됩니다.
변경 감지 시 무시할 사용자	Syslog 또는 AAA 변경 이벤트를 처리할 때 무시할 사용자를 나타냅니다. 사용자를 추가하려면 오른쪽 상자에 사용자 이름을 입력하고 사용자 이름 추가 <<를 클릭합니다. 반면, 사용자를 삭제하려면 왼쪽 상자에서 사용자 이름을 선택하고 사용자 이름 삭제를 클릭합니다.
사용자 ID 변경	
사용자 자동 생성	이 옵션을 선택하면 NA가 구성 변경 작성자를 인식하지 못할 경우 새 사용자를 생성합니다.
자동 생성 사용자 접미사	자동 생성 기능에 따라 NA가 새 사용자에게 추가하는 접미사를 입력합니다. 기본값은 _auto입니다.
Syslog 사용자 ID	이 옵션을 선택하면 NA가 Syslog 메시지에서 사용자 식별을 시도합니다.

필드	설명/작업
Syslog 사용자 패턴	<p>Syslog 사용자 패턴은 Java 정규 표현식입니다. 캡처 그룹을 추가하여 정규 표현식에서 사용자 이름의 위치를 나타낼 수 있습니다. 예를 들면 다음과 같습니다.</p> <ul style="list-style-type: none"> • User (\S+) authenticated • session opened for user (\S+) • Login successful for user (\S+) on <p>NA는 이러한 패턴을 사용하여 구성 변경을 담당하는 사용자를 확인합니다.</p> <p>오른쪽 상자에 패턴을 입력하고 패턴 추가 <<를 클릭합니다. 오른쪽 상자에서 패턴을 선택하고 패턴 삭제를 클릭하여 패턴을 삭제할 수 있습니다. NA가 Syslog에서 이러한 정규 표현식과 일치하는 항목을 찾습니다. NA는 일치 항목을 찾으면 텍스트를 사용자로 캡처합니다. 일반적으로 장치 드라이버가 이러한 패턴을 채웁니다.</p>
Syslog에서 워크스테이션 IP 주소 확인	<p>이 옵션을 선택하면 NA는 Syslog 메시지에서 IP 주소를 확인하고 도메인 이름을 관련된 구성 변경을 담당하는 사용자 이름으로 취급합니다. 이 방법은 Syslog 메시지에서 다른 방법으로 사용자 이름을 확인할 수 없는 경우에만 사용됩니다.</p>
확인되지 않은 IP 주소 저장	<p>이 옵션을 선택하면 DNS를 사용하는 호스트 이름을 확인할 수 없을 때 NA는 IP 주소를 사용자 이름으로 취급합니다. 점은 대시로 대체됩니다. 예를 들어, 10.10.1.1은 사용자 10-10-1-1이 됩니다.</p>
Syslog에서 사용자 자동 생성	<p>이 옵션과 사용자 자동 생성을 선택하면 NA는 Syslog 메시지에서 식별된 사용자를 기존 사용자와 일치시키려고 합니다. 기존 사용자가 없으면 새 사용자가 생성됩니다.</p>

필드	설명/작업
시작/실행 구성	
시작 구성 캡처	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 끄기 — NA가 각 시작 구성을 캡처하지 않습니다. • 감지만 — NA가 각 시작 구성을 캡처하고 실행 구성과 비교하지만 시작 구성을 저장하지 않습니다. • 켜기(기본값) — NA는 각 시작 구성을 캡처하고 실행 구성과 비교하며 시작 구성을 저장합니다. 일부 공급업체 및 장치는 시작 구성의 개념을 지원하지는 않음에 주의하십시오.
ACL 구문 분석	
각 스냅샷을 사용하여 ACL 데이터 구문 분석	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 사용함 — NA가 각 스냅샷을 사용하여 ACL 데이터를 구문 분석하고 저장합니다. • 사용 안 함 — NA가 각 스냅샷을 사용하여 ACL 데이터를 구문 분석하지 않습니다. <p>이 옵션은 새 장치를 추가할 때 이 기능의 기본 상태만 설정합니다. 일괄 편집을 사용하여 장치 그룹에 대한 ACL 구문 분석을 켜고 끌 수 있습니다. (참고: 이 옵션으로 인해 장치별로 오버라이드될 수 있습니다.)</p>
ACL 편집	
응용 프로그램 사전 편집 스크립트 표시	<p>이 옵션을 선택하면 ACL을 편집하거나 생성할 때 ACL 응용 프로그램을 사전 처리하기 위한 스크립트가 표시됩니다. 사전 응용 프로그램 스크립트는 장치에 있는 ACL의 기존 응용 프로그램을 취소합니다. 신규이거나 업데이트된 ACL 스크립트가 편집된 ACL을 장치에 추가합니다.</p>
편집 준비 스크립트 표시	<p>이 옵션을 선택하면 ACL을 편집하거나 생성할 때 편집 준비 스크립트가 표시됩니다. 편집 준비 스크립트는 편집한 ACL을 승인하도록 장치를 준비하는 데 필요한 스크립트 작성 작업을 수행합니다.</p>
응용 프로그램 스크립트 표시	<p>이 옵션을 선택하면 ACL을 편집하거나 생성할 때 ACL 응용 프로그램 스크립트가 표시됩니다. 응용 프로그램 스크립트는 ACL을 적용하는 데 (예: VTY 연결) 사용되는 스크립트 작성의 부분입니다. 응용 프로그램 스크립트는 ACL을 다시 적용합니다.</p>

필드	설명/작업
구성 정책 확인	
기본적으로 배포 전 확인	이 옵션을 선택하면 NA가 배포 전 정의된 구성 정책을 기준으로 편집한 구성을 확인합니다.
패턴 시간 초과	패턴을 구성과 일치시키는 데 소요되는 최대 시간(초)을 입력합니다. 기본값은 30초입니다.
자동 수정 스크립트 실행	이 옵션을 선택하면 규칙을 준수하지 않음이 발견될 경우 자동 수정 스크립트의 자동 실행을 허용할지 여부를 제어합니다. 자동 수정 스크립트에 대한 자세한 내용은 726페이지의 "자동 수정 스크립트 생성" 을 참조하십시오.
가져온 정책을 인벤토리 그룹에 자동 적용	이 옵션을 선택하면 가져온 정책은 모두 인벤토리 그룹에 적용됩니다.
사전 작업 및 사후 작업 스냅샷	
사용자가 사전/사후 작업 스냅샷 오버라이드	이 옵션을 선택하면 사용자가 개별 작업을 실행할 때 기본 사전 작업 및 사후 작업 스냅샷 설정을 오버라이드할 수 있습니다. 오버라이드가 허용된 경우 사전 및 사후 작업 스냅샷 옵션이 해당되는 새 작업 페이지에 표시됩니다. 오버라이드가 허용되지 않으면 기본 설정이 사용됩니다. (자세한 내용은 54페이지의 "사전 작업 및 사후 작업 스냅샷 구성" 을 참조하십시오.)
스크립트당 사전/사후 작업 스냅샷 설정 힌트 허용	이 옵션을 선택하면 개별 스크립트에서 사전 작업 및 사후 작업 스냅샷 설정을 오버라이드할 수 있습니다.
	<p>참고: 사전 작업 스냅샷 설정을 오버라이드하려면 스크립트 설명에 "tc_pre_snapshot=true" 텍스트를 포함하여 사전 작업 스냅샷을 요청하거나 "tc_pre_snapshot=false" 텍스트를 포함하여 사전 작업 스냅샷 없음을 요청하십시오. 사후 작업 스냅샷 설정을 오버라이드하려면 스크립트 설명에 tc_post_snapshot=true 텍스트를 포함하여 사후 작업 스냅샷을 작업의 일부로 요청하거나, tc_post_snapshot=task 텍스트를 포함하여 사후 작업 스냅샷을 별도 작업으로 요청하거나, tc_post_snapshot=false 텍스트를 포함하여 사후 작업 스냅샷 없음을 요청하십시오.</p> <p>자세한 내용은 54페이지의 "사전 작업 및 사후 작업 스냅샷 구성"을 참조하십시오.</p>

필드	설명/작업
명령 스크립트 실행 전 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음(기본값) •작업에 포함됨
명령 스크립트 실행 후 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨(기본값) •별도 작업으로 예정됨
구성 배포 전 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨(기본값)
구성 배포 후 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨(기본값) •별도 작업으로 예정됨
장치 프로비전 후 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨(기본값) •별도 작업으로 예정됨
진단 실행 전 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음(기본값) •작업에 포함됨
진단 실행 후 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음(기본값) •작업에 포함됨 •별도 작업으로 예정됨

필드	설명/작업
ACL 삭제 전 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨(기본값)
ACL 삭제 후 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨(기본값) •별도 작업으로 예정됨
시작/실행 동기화 후 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음(기본값) •작업에 포함됨 •별도 작업으로 예정됨
사후 작업 스냅샷 지연	별도 스냅샷 작업(있는 경우)으로 실행하는 사후 작업 스냅샷에 대한 지연을 입력합니다. 기본값은 30초입니다.
진단	
토폴로지 데이터 수집 빈도	네트워크 성능을 보존하기 위해 조정해야 하는 새로운 클래스의 진단에 토폴로지 데이터가 포함되어 있습니다. 토폴로지 데이터는 네트워크 다이어그램을 렌더링하는 데 사용됩니다. 토폴로지 데이터를 수집하면 NA 서버에 대한 부하가 상당히 증가하므로 가능한 자주 수행하지는 마십시오. 토폴로지 데이터 수집 간 허용되는 최소 간격(시간)을 입력합니다. 기본값은 168시간입니다.
저장된 토폴로지 데이터	현재 데이터베이스에 저장된 토폴로지 데이터의 허용 가능한 기간(시간)을 입력합니다. 저장된 데이터가 이 값보다 오래된 경우, 장치에서 데이터를 직접 검색합니다. 그렇지 않으면 저장된 데이터가 사용됩니다. 기본값은 72시간입니다.
이중 데이터 수집 빈도	네트워크 성능을 보존하기 위해 조정해야 하는 새로운 클래스의 진단에 이중 불일치 데이터가 있습니다. 이중 불일치 데이터는 공통적인 엔드 투 엔드(end-to-end) 성능 문제를 식별하는 데 사용됩니다. 종종 이중 불일치는 한 시스템은 전이중 방식으로 설정되고 다른 시스템은 반이중 방식으로 설정될 때 발생합니다. 이중 불일치 데이터를 수집하면 NA 서버에 대한 부하가 상당히 증가하므로 가능한 자주 수행하지는 마십시오. 이중 데이터 수집 간 허용되는 최소 간격(시간)을 입력합니다. 기본값은 168시간입니다.

필드	설명/작업
저장된 이중 데이터	현재 데이터베이스에 저장된 이중 데이터의 허용 가능한 기간(시간)을 입력합니다. 저장된 데이터가 이 값보다 오래된 경우, 장치에서 데이터를 직접 검색합니다. 그렇지 않으면 저장된 데이터가 사용됩니다. 기본값은 72시간입니다.
플래시 저장 공간	
적은 플래시 이벤트	이 옵션을 선택하면 감지된 사용 가능한 플래시 저장 공간이 적을 경우 이벤트가 생성됩니다.
적은 플래시 임계값	공간이 적은 이벤트가 생성되기 전에 채워야 하는 플래시 저장 공간의 백분율을 입력합니다. 기본값은 90%입니다.
부팅 감지	
오류 마진 계수	장치 부팅을 감지할 때 허용할 시계 편차(6시간당 초 수)를 입력합니다. 장치를 확인하는 최소 빈도를 6시간마다 한 번으로 하는 것이 좋습니다.
사용자 지정 서비스 유형	
사용자 지정 서비스 유형	서비스 유형을 추가하거나 삭제합니다. 서비스 유형에서는 장치에 대해 VoIP, BGP, MPLS 등을 지정할 수 있습니다. 이 값을 사용하여 장치의 용도를 식별할 수 있습니다. 서비스 유형에 대한 자세한 내용은 249페이지의 "장치 세부사항 보기" 를 참조하십시오.

변경 감지

NA는 다음을 포함하여 장치 구성에 대한 변경 사항을 감지하기 위한 여러 가지 방법을 사용합니다.

- Syslog 메시지
- AAA 로그 읽기
- 내부 프록시

이러한 방법에서 NA는 다양한 많은 입력을 사용하여 장치에서 실제로 변경을 수행한 사용자를 확인합니다. 이 정보에서는 변경을 담당한 가능성이 가장 많은 사용자가 제공 됩니다. 우선 순위의 순서대로 다음 정보가 사용됩니다.

- 장치에서 실행된 암호 변경을 예약한 사용자
- 장치에서 실행된 소프트웨어 업데이트를 예약한 사용자
- 장치에 구성을 배포한 사용자
- 장치에서 스크립트를 실행한 사용자
- NA의 프록시를 통해 장치에 연결한 사용자
- AAA 로그에서 수집한 사용자 정보
- syslog 메시지에서 구문 분석된 사용자 정보

NA가 우선 순위 목록에서 상위에 있는 장치 인터랙션에 변경 속성을 할당합니다. 예를 들어 한 사용자가 다른 사용자가 장치에 대해 프록시 설정한 동일한 시간에 암호 변경을 예약하고, 변경 사항이 감지되면 해당 변경 사항은 암호 변경을 예약한 사용자에게 할당 됩니다.

장치의 구성 변경을 보려면

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다. 현재 관리되는 모든 장치 목록이 열립니다.
2. 구성 변경을 확인할 장치를 클릭합니다. 장치 세부사항 페이지가 열립니다.
3. 보기 드롭다운 메뉴에서 구성 변경을 클릭합니다.
4. 변경한 사람 열에서 세부사항 링크를 클릭합니다. 사용자 특성 세부사항 페이지가 열립니다.

Syslog 메시지

NA Core Syslog 서버는 Syslog 메시지를 시스템에서 사용 중인 드라이버에 대한 Syslog 패턴 목록과 일치하는 NA Core로 전달합니다. 드라이버 검색 작업이 실행되는 경우 Syslog 메시지 패턴 목록이 업데이트되고 나서 NA Syslog 서버에 Syslog 메시지 패턴 목록을 업데이트하라는 지시가 전달됩니다.

NA Satellite Syslog 서버도 동일한 작업을 수행합니다. 이 서버는 사용 중인 장치에 대한 Syslog 메시지 패턴 목록을 포함하며 이러한 패턴 중 하나와 일치하는 NA Core로만 메시지를 전달합니다. 따라서 원격 에이전트 배포 작업을 실행하면 `Initialized Satellite with N syslog change detection patterns from Core`. 메시지가 표시됩니다.

초기 NA Satellite가 현재 Syslog 메시지 패턴 목록을 수신합니다. 후속 드라이버 검색 작업은 새 장치가 검색되어 새 Syslog 패턴이 필요할 경우 NA Core Syslog 서버와 NA Satellite Syslog 서버에 모두 알립니다.

사용자 특성 세부사항 페이지 필드

참고: 모든 구성 변경이 사용자의 특성이 될 수 있는 것은 아니며 해당 안 됨으로 표시될 수도 있습니다.

필드	설명/작업
이벤트 세부사항 변경	
사용자	변경 사항을 작성한 사용자의 이름을 표시합니다.
날짜	변경 사항이 작성된 날짜를 표시합니다.
장치 인터랙션	변경 사항을 감지하는 데 사용된 방법(예: Syslog)을 표시합니다.
추가 세부사항	변경 사항에 대한 추가 세부사항(예: 콘솔에서 변경이 수행된 경우)을 표시합니다.

사전 작업 및 사후 작업 스냅샷 구성

사전 작업 및 사후 작업 스냅샷을 구성하여 다음 작업을 수행할 수 있습니다.

- 다양한 작업 유형에 대한 사전 및 사후 스냅샷 동작 정의
- 사후 스냅샷을 별도 작업으로 실행
- 특정 작업을 실행할 때 기본 사전 작업 및 사후 작업 스냅샷 동작 오버라이드

다음 작업에 대한 사전 작업 및 사후 작업 스냅샷 옵션을 표시할 수 있습니다.

- 구성 배포(234페이지의 "구성 배포 작업 페이지 필드" 참조)
- 진단 실행(397페이지의 "진단 실행 작업 페이지 필드" 참조)
- ACL 삭제(888페이지의 "ACL 삭제 작업 페이지" 참조)
- 동기화된 시작 및 실행(408페이지의 "시작 및 실행 동기화 작업 페이지 필드" 참조)
- 명령 스크립트 실행(389페이지의 "명령 스크립트 실행 작업 페이지 필드" 참조)
- ACL 라인 일괄 삽입(881페이지의 "ACL 라인 일괄 삽입" 참조)
- ACL 라인 일괄 제거(882페이지의 "ACL 라인 일괄 삭제" 참조)

명령 스크립트에 스냅샷 힌트를 제공할 때 특별 태그를 명령 스크립트에 추가하여 해당 스크립트를 실행할 때마다 사전 또는 사후 작업 스냅샷 동작을 지정할 수 있습니다. 예를 들어, 실제로 장치에 연결하거나 장치를 수정하지 않는 고급 스크립트를 사용한다고 가정하면 고급 스크립트는 NA API만을 사용하여 장치에 대한 정보를 추출하고 보고서를 생성합니다. 이 경우 작업이 실행되고 나면 스냅샷을 가져올 필요가 없으므로 고급 스크립트에는 사후 스냅샷이 필요 없음을 나타내는 태그가 포함될 수 있습니다.

장치 그룹에 대해 실행할 스크립트를 두 개 이상 선택하고 힌트를 포함하는 스크립트가 두 개 이상일 경우 지정된 동작 중 가장 안정적인 동작이 사용됩니다.

장치 액세스

장치 액세스 페이지를 사용하여 다음 작업을 수행할 수 있습니다.

- 장치 연결 방법 지정
- 네트워크 장치 감지 작업 설정 구성
- 배스천 호스트 설정 구성
- SecurID 장치 액세스 구성
- SSH 장치 액세스 구성
- 사전 작업 기준으로 장치에 액세스할 때 사용되는 자격 증명 지정
- Nortel BayRS MIB/OS 버전 지정
- 게이트웨이 메시 정보 입력

종종 네트워크 환경은 네트워크 방화벽에 의해 보호됩니다. NA는 방화벽을 통해 장치에 액세스하는 네 가지 방법을 제공합니다.

- 방화벽을 통해 직접 액세스를 엽니다.
- 방화벽에 NAT(네트워크 주소 변환)를 생성하고 NAT를 사용하여 장치에 액세스하도록 NA를 구성합니다. NAT 주소는 NAT를 사용하는 장치의 장치 구성에는 나타나지 않습니다.
- 방화벽의 먼 쪽에 있는 기존 배스천 호스트를 사용하여 관리 요청을 프록시하도록 NA를 구성합니다. 배스천 호스트에서는 이미 방화벽을 통해 액세스할 수 있으므로, 배스천 호스트 구성을 사용하여 배스천 호스트의 프록시 연결을 통해 장치를 관리할 수 있습니다.
- 게이트웨이 메시 사용. 자세한 내용은 *HP Network Automation 9.10 Satellite User's Guide*를 참조하십시오.

콘솔 서버는 직렬 링크를 사용하여 장치에 대한 물리적 연결을 유지합니다. 이러한 링크는 텔넷을 통해 서버에서 호스트하는 특정 IP 포트 번호에 제공됩니다. 네트워크 장치가 네트워크와 연결되지 않은 경우에도 콘솔 서버 연결을 사용할 수 있습니다.

장치 액세스 페이지를 보려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 장치 액세스를 클릭합니다. 그러면 장치 액세스 페이지가 열립니다.

장치 액세스 페이지 필드

필드	설명/작업
장치 연결 방법	
암호 선택	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none">• 항상 마지막으로 성공한 암호를 먼저 사용합니다. 이 옵션을 선택하면 NA는 이전의 장치 액세스에서 마지막으로 성공한 암호를 먼저 사용합니다. 마지막으로 성공한 암호가 작업 중간에 변경될 경우 마지막으로 성공한 이 새로운 암호는 나머지 작업에도 사용된다는 보장이 없습니다. 또한 마지막으로 사용된 규칙 변경됨 이벤트가 계속 생성됩니다. 따라서 장치가 예상 암호 규칙을 사용하지 않는 시기를 확인할 수 있습니다.• 항상 정의된 순서대로 암호를 사용합니다. 이 옵션을 선택하면 NA가 항상 정의된 순서대로 암호를 사용합니다. NA는 장치와의 그 다음 통신 주기에서 가장 최근에 사용된 인증 자격 증명을 추적합니다. 이 옵션을 통해 장치 암호 규칙을 이용하면서 각 장치에 대한 연결 시도 횟수를 최소화할 수 있습니다. 자세한 내용은 170 페이지의 "장치 암호 규칙 생성"을 참조하십시오.

필드	설명/작업
기본 연결 방법	<p>다음 방법을 사용하여 장치에 연결할 수 있습니다. 이러한 방법은 새 장치 페이지 및 장치 추가 마법사에서 기본적으로 선택되어 나타납니다. 다음 옵션 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none"> • 텔넷 • SSH • RLogin • SNMP • SCP • FTP • TFTP <p>참고: NA에는 통합된 TFTP 서버가 있으므로 일반적으로 SNMP 또는 CLI를 통해 장치에 액세스하여 이 장치와의 송수신을 설정합니다. 자체 TFTP 서버가 있는 장치의 경우 NA는 TFTP 클라이언트 역할을 수행합니다. 일반적으로 SCP는 CLI와 함께 사용되어야 합니다. SCP에서 SSH를 사용하려면 장치가 활성화되어야 합니다. 장치에서 SSH 서버가 실행되고 있지 않는 경우에는 SCP를 실행할 수 없습니다. NA는 통합된 FTP 서버를 제공하고 일반적으로 CLI를 통해 장치에 액세스하여 이 장치와의 송수신을 설정합니다.</p>
잘못된 로그인 시도 지연	<p>장치 시간을 복구할 수 있도록 잘못된 로그인 시도 후 지연되는 시간(초)을 입력합니다. 기본값은 5초입니다.</p>
SNMP 시간 초과	<p>장치가 config 로드와 같은 SNMP 명령 집합에서 작동할 때까지 대기하는 시간(초)을 입력합니다. 기본값은 40초입니다.</p>
최대 암호 시도 수	<p>허용된 최대 암호 시도 수를 입력합니다. 영(0)은 제한 없음을 나타냅니다. 10개의 암호 규칙이 있을 때 3을 입력하면 NA는 처음 3번의 암호 규칙을 시도한 후 중지됩니다. 이 설정은 3번 로그인 시도 실패 후 TACACS 서버가 사용자 이름을 잠글 경우 유용합니다. 암호 규칙을 한 번만 시도하려면 1을 입력할 수 있습니다. 이 설정은 한 번만 암호 규칙이 작동하는 경우 유용합니다.</p>
최대 저장 규칙	<p>시도할 최대 저장 암호 규칙 수를 입력합니다. 기본값은 3입니다. 이 옵션을 사용하지 않으려면 0을 입력합니다.</p>

필드	설명/작업
네트워크 감지 장치 작업 설정 및 포트 스캔 작업 설정	
NMAP 유틸리티 경로	네트워크 장치를 검색하기 위한 Nmap 유틸리티의 경로를 입력합니다. (참고: Nmap에서는 네트워크를 검색하여 가동되는 포트와 이러한 포트에서 제공하는 서비스를 확인할 수 있습니다. 자세한 Nmap 내용은 www.Insecure.Org 를 참조하십시오.) Nmap 설치에 대한 자세한 내용은 <i>Network Automation 9.10 업그레이드 및 설치 설명서</i> 를 참조하십시오.
Nmap 포트 스캔 허용	선택한 경우 적당한 권한을 가진 사용자가 Nmap을 사용하여 네트워크 장치를 검색할 수 있습니다. Nmap 사용에 대한 자세한 내용은 440페이지의 "포트 스캔 페이지 필드" 를 참조하십시오.
Nmap 포트 스캔 옵션	Nmap을 사용하여 네트워크 장치를 검색할 때 기본 옵션을 표시합니다. Nmap은 장치 검색이 수행되는 방식을 제어합니다. 기본적으로 NA는 -PO를 Nmap에 전달하여 Nmap에 UDP 대신에 IP로 작업하도록 지시합니다. 전체 옵션 목록은 Nmap 설명서를 참조하십시오. Nmap 사용에 대한 자세한 내용은 440페이지의 "포트 스캔 페이지 필드" 를 참조하십시오.
작업 당 검색할 최대 주소 수	검색할 최대 IP 주소 수를 입력합니다. 네트워크 장치 감지 작업을 검색할 최대 주소 수(1024가 기본값임)로 제한하여 네트워크 트래픽을 줄여야 합니다.
최대 SNMP 스캐너 스레드 수	SNMP 검색 방법을 사용하여 장치 검색 중 네트워크 장치 감지 작업이 생성할 최대 SNMP 스캐너 스레드 수를 입력합니다. 기본값은 79입니다. 이론적으로 최대 SNMP 스캐너 스레드 수가 높을수록 작업 실행이 빨라집니다. 그러나 SNMP 스캐너 스레드 수가 너무 많으면 각 SNMP 스캐너 스레드에 필요한 CPU 오버헤드 및 네트워크 트래픽으로 인해 시스템 성능이 저하될 수 있습니다. (참고: 네트워크 장치 감지 작업을 구성할 때 네트워크 장치 감지 작업이 SNMP를 사용하여 장치를 감지하도록 하는 옵션을 사용할 수 있습니다. 그 결과, 작업은 SNMP를 통해 장치에 전달하는 많은 SNMP 스캐너 스레드를 생성합니다. 다른 검색 방법에 대한 내용은 426페이지의 "네트워크 장치 감지 작업 페이지 필드" 를 참조하십시오.)

필드	설명/작업
네트워크 검색 IP 또는 CIDR 범위 제외	오른쪽 상자에 IP 주소 또는 CIDR(Classless Inter-Domain Routing) 범위 제외(예: 192.168.1.0-192.168.2.0 또는 192.168.31.0/24)를 입력하고 패턴 추가 << 버튼을 클릭하면 범위가 포함됩니다. 패턴을 삭제하려면 왼쪽 상자에서 패턴을 선택하고 패턴 삭제 버튼을 클릭합니다.
SNMP 시간 초과	각 SNMP SysOID 프로브에 대한 SNMP 시간 초과 값(밀리초)을 입력합니다. 기본값은 500밀리초입니다.
배스천 호스트 설정	
기본적으로 배스천 호스트 사용	이 옵션을 선택하면 새 장치가 텔넷 및 SSH 액세스 시 배스천 호스트를 사용합니다. (참고: 장치별로 배스천 호스트 설정을 오버라이드할 수 있습니다.)
기본 배스천 호스트	텔넷 및/또는 SSH 액세스에 사용할 배스천 호스트의 호스트 이름 또는 IP 주소를 입력합니다.
기본 배스천 호스트 사용자 이름	텔넷 및/또는 SSH 액세스에 사용할 배스천 호스트의 사용자 이름을 입력합니다.
기본 배스천 호스트 암호	텔넷 및/또는 SSH 액세스에 사용할 배스천 호스트의 암호를 입력합니다.
SecurID 장치 액세스	
SecurID 라이선스 사용	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 사용자당 고유 토큰 사용 — 이 옵션을 선택하면(기본값) 각 장치 액세스는 작업 또는 텔넷/SSH 프록시 연결을 시작한 사용자에게 해당하는 초기값만 사용합니다. • 소프트웨어 토큰 풀 사용자 이름 — 이 옵션을 선택하면 일반 사용 소프트웨어 토큰 초기값 풀이 제공되고 최대 성능을 발휘하도록 가능한 효율적으로 사용됩니다. SecurID 소프트웨어 토큰 풀이 연결된 사용자 이름을 입력합니다. <p>사용자별로 고유한 소프트웨어 토큰을 사용할 경우, 더 많은 토큰이 필요하고 토큰 유지 보수가 증가합니다. 일반 사용자를 포함한 풀에서 소프트웨어 토큰을 사용하면 필요한 토큰 수가 줄어들고 잠재적으로 작업 처리량이 증가합니다.</p>

필드	설명/작업
최대 소프트웨어 토큰 수	실행 중인 NA로 가져온 최대 소프트웨어 토큰 라이선스 수를 입력합니다. 기본값은 1024입니다.
암호 코드 수명	소프트웨어 토큰 암호 코드의 수명을 입력합니다. 기본값은 60초입니다.
FTP 및 SSH 장치 액세스	
FTP/SSH 사용자	<p>FTP 또는 SSH 사용자를 입력합니다. FTP 또는 SSH 사용자 이름은 장치 연결을 통해 FTP 또는 SSH 서버에 액세스할 때 사용됩니다. 이 사용자 이름이 시스템 FTP 또는 SSH 서버에 없는 경우 자동으로 생성됩니다.</p> <p>참고: Linux 또는 Solaris 플랫폼에서 SCP를 사용하는 경우 대체 포트에서 실행되도록 시스템의 SSHD(SSH 데몬)를 수정하고 SSHD 서비스를 다시 시작해야 합니다. 포트 8022가 권장됩니다. SCP 및 SSH가 제대로 작동하도록 하려면 장치별 설정을 구성해야 합니다. 또한 SCP에 NA SSH 서버를 사용하려면 장치 및 장치 드라이버에서 SCP를 지원해야 합니다.</p>
FTP/SSH 암호	FTP 또는 SSH 암호를 입력합니다. FTP 또는 SSH 암호는 장치 연결을 통해 FTP 또는 SSH 서버에 액세스할 때 사용됩니다.

필드	설명/작업
작업 자격 증명	
표준 장치 자격 증명 허용	<p>다음 작업 중 하나 이상을 선택합니다. 기본적으로 모든 작업이 선택되어 있습니다.</p> <ul style="list-style-type: none"> • Syslog 구성 • ACL 삭제 • 구성 파일 배포 • 암호 배포 • 드라이버 검색 • 장치 재부팅 • 명령 스크립트 실행 • 진단 실행 • ICMP 테스트 실행 • 시작 및 실행 동기화 • 스냅샷 작성 • 장치 소프트웨어 업데이트 <p>위의 작업을 사용하여 사용자는 장치별 암호 및/또는 네트워크 전체 암호 규칙을 사용하는 표준 처리를 선택할 수 있습니다. 작업별 자격 증명에 대한 자세한 내용은 65페이지의 "작업별 자격 증명"을 참조하십시오. 암호 규칙에 대한 내용은 172페이지의 "장치 암호 규칙 페이지 필드"를 참조하십시오.</p>

필드	설명/작업
작업별 장치 자격 증명 허용	<p>다음 작업 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none">• Syslog 구성• ACL 삭제• 구성 파일 배포• 드라이버 검색• 암호 배포• 장치 재부팅• 명령 스크립트 실행• 진단 실행• ICMP 테스트 실행• 시작 및 실행 동기화• 스냅샷 작성• 장치 소프트웨어 업데이트 <p>이 옵션을 선택하면 위의 작업 시 해당 작업에 특정한 일회용 장치 자격 증명을 입력해야 합니다. 작업별 자격 증명에 대한 자세한 내용은 65페이지의 "작업별 자격 증명"을 참조하십시오.</p>

필드	설명/작업
사용자 AAA 자격 증명 허용	<p>다음 작업 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none"> • Syslog 구성 • ACL 삭제 • 구성 파일 배포 • 드라이버 검색 • 암호 배포 • 장치 재부팅 • 명령 스크립트 실행 • 진단 실행 • ICMP 테스트 실행 • 시작 및 실행 동기화 • 스냅샷 작성 • 장치 소프트웨어 업데이트 <p>이 옵션을 선택하면 위의 작업을 사용하여 사용자가 작업을 실행할 때 사용할 작업 소유자의 AAA 자격 증명을 선택할 수 있습니다. (참고: 사용자는 올바른 AAA 자격 증명을 정의해야 합니다.) 작업별 자격 증명에 대한 자세한 내용은 65페이지의 "작업별 자격 증명"을 참조하십시오.</p>
플백 관리 사용자	알 수 없는 사용자로 작업에 AAA 자격 증명을 사용할 관리 사용자를 입력합니다.
Nortel 검색	
Nortel BayRS MIB/OS 버전	BayRS 드라이버를 검색할 추가 BayRS MIB 버전/수정 버전 목록을 표시합니다. 세로 막대로 구분된 <MIB 버전>/<수정 버전> 순서를 사용합니다(예: 14.00/1D12 14.20/).
게이트웨이 메시	
로컬 게이트웨이 호스트	NA 코어와 동일한 범위에 있는 게이트웨이 시스템의 호스트 이름 또는 IP 주소 및 포트를 입력합니다(예: gw-vlan10:3001). 게이트웨이 메시에 대한 내용은 194페이지의 "오버랩되는 IP 네트워크"를 참조하십시오.

필드	설명/작업
로컬 게이트웨이 프록시 포트	NA 코어와 동일한 범위에 있는 게이트웨이 시스템의 포트 이름을 입력합니다(예: gw-vlan10:3001). 기본값은 3002입니다. 게이트웨이 메시에 대한 내용은 194페이지의 "오버랩되는 IP 네트워크" 를 참조하십시오.
로컬 게이트웨이 관리 포트	로컬 영역의 게이트웨이에 대한 관리 포트 번호를 입력합니다. 이 포트 번호는 게이트웨이 메시에서 영역 이름을 반입하는 데 사용됩니다. 기본값은 9090입니다.
게이트웨이 관리 개인 키 파일 이름	<p>관리 포트에 연결하는 데 필요한 게이트웨이의 개인 키 파일 이름을 입력합니다. 이 파일 이름은 절대 경로 또는 상대 경로일 수 있습니다. 상대 경로는 NA 설치 경로의 루트(일반적으로 C:\NA)에 상대적입니다. 게이트웨이의 개인 키는 게이트웨이가 설치될 때 생성됩니다.</p> <p>NA 독립형 게이트웨이를 사용할 때 개인 키 파일 이름은 opswgw-mngt-server.pkcs8입니다. NA 게이트웨이를 설치한 <i>saOPSWgw*/certificates</i> 디렉터리에서 이 파일을 복사해야 합니다. NA 설치의 루트(일반적으로 C:\Rendition)에 이 파일을 복사합니다. HP SA와 NA를 통합할 경우 NA에서는 HP SA 게이트웨이 메시지를 사용합니다. 이 경우에는 HP SA 호스트의 spog.pkcs 파일을 NA 설치 루트(일반적으로 C:\Rendition)에 복사합니다. 관리 설정에서 파일 이름을 spog.pkcs8로 변경해야 합니다.</p> <p>참고: .pkcs8 파일은 공용 키 암호화 체계에서 사용된 개인 키를 포함하는 PKCK#8 형식 파일입니다. 게이트웨이 메시지를 보안하려면 개인 키를 사용하여 게이트웨이 메시지를 관리해야 합니다. NA는 게이트웨이 메시지 관리 기능을 사용하여 게이트웨이 메시에서 지원되는 범위 이름을 나열합니다.</p> <p>게이트웨이 관리 설정을 테스트하려면 새 장치 페이지를 열고 연결 정보 섹션으로 이동하여 범위 이름 목록이 있는지 확인합니다.</p>
게이트웨이 메시지 지연	게이트웨이 메시지를 통해 원격 범위에 접근하는 지연 시간(초)을 입력합니다. 기본값은 5초입니다. 이 수는 원격 장치와 통신할 때 사용되는 시간 초과에 추가됩니다.

변경 사항을 저장하려면 저장을 클릭해야 합니다.

작업별 자격 증명

작업별 자격 증명 구성 작업을 통해 장치에 액세스하는 작업의 고유한 자격 증명 처리를 지정하여 장치에 액세스하는 데 사용되는 자격 증명을 지정할 수 있습니다. 다음 작업을 수행할 수 있습니다.

- 작업 소유자의 AAA 자격 증명을 사용하여 작업 실행
- 작업을 생성할 때 지정한 일회용 자격 증명을 사용하여 작업 실행
- 어떤 유형의 작업에 어떤 유형의 자격 증명에 필요한지 구성

일반적으로 보안 환경에서는 CiscoSecure ACS TACACS+ 서버와 같이, 각 사용자가 각 장치에서 실행할 수 있는 명령을 제한하는 AAA 서버를 구현했을 수 있습니다.

예를 들어, 사용자 A와 사용자 B 모두 권한을 가지는 특정 명령을 사용하여 명령 스크립트를 실행할 수 있다고 가정하면 사용자 A와 사용자 B 모두 NA가 구현되고 난 후 명령 스크립트를 실행할 수 있어야 합니다. 하지만 사용자 A와 사용자 B 모두 자격 증명을 유지 보수하여 권한이 있는 명령만 실행하도록 해야 할 수 있습니다.

따라서 작업별 자격 증명을 사용할 때 명령 스크립트를 실행하는 권한이 있는 사용자 A와 사용자 B에 대해 새로운 정적 NA 계정을 설정하지 않아도 됩니다. 각 사용자는 현재 권한으로 명령 스크립트를 실행할 수 있습니다. 사용자 A 또는 사용자 B가 권한이 없는 명령을 사용할 경우 NA는 오류를 반환합니다.

AAA 자격 증명을 사용할 때 NA는 다음을 수행합니다.

- 마지막으로 성공한 자격 증명, 장치별 자격 증명, 암호 규칙 및 장치 저장 암호를 포함하여 모든 표준 자격 증명 처리를 시도합니다.
- 각 시도에서 NA는 사용자 이름과 암호를 작업 소유자의 AAA 사용자 이름과 암호로 바꿉니다. 시도가 실패할 경우 NA는 사용자의 AAA 암호를 실행 암호 및 활성화 암호로 사용하여 다시 시도합니다. 모든 AAA 로그인 시도가 실패할 경우 작업이 실패합니다.

참고: .RCX 파일에 설정할 수 있는 숨은 config 설정 프록시/auth_fallback_for_aaa_task가 있습니다. 이 설정을 true로 설정하면 NA는 폴백하고 표준 암호 처리를 시도합니다.

일회용 자격 증명을 구성할 때 NA는 작업 유형에 따라 지정된 유형의 자격 증명 처리를 사용합니다. 예를 들어, 스냅샷 작업에 AAA 자격 증명만 허용되는 경우 모든 스냅샷 작업은 AAA 자격 증명을 사용합니다. 지정된 작업 유형에 둘 이상의 자격 증명 유형이 허용될 경우 사용자는 사용할 자격 증명 유형을 선택할 수 있습니다.

지정된 작업이 일회용 자격 증명을 사용하도록 선택된 경우 NA는 작업을 생성할 때 사용자가 지정한 자격 증명을 사용합니다. 일회용 자격 증명에 실패하면 작업이 실패합니다.

참고: 일회용 자격 증명에 성공하면 NA는 장치에 대해 마지막으로 성공한 자격 증명 정보를 업데이트하지 않습니다.

서버

서버 페이지를 사용하여 다음 작업을 수행할 수 있습니다.

- TFTP, FTP 및 SMTP 서버 지정
- NA 작업 제한 설정
- Syslog 구성
- 장치 가져오기 간격 구성
- 기본 IP 주소 재할당 및 중복 방지 설정 구성
- 도메인 이름 확인 구성
- 감사 로그 사용
- 데이터베이스 정리 구성
- 고급 스크립팅 성능 구성
- HTTP 프록시 서버 구성
- 동적 장치 그룹 재계산 구성
- 소프트웨어 이미지 관리 구성
- 확장 드라이버의 디렉터리에 대한 절대 경로 지정
- 서버 성능 정리 구성
- 이벤트 차별화 크기 임계값 구성
- 비 관리 NA 코어에서 Syslog 변경 감지 무시

서버 페이지를 보려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 서버를 클릭합니다. 서버 페이지가 열립니다.

서버 페이지 필드

필드	설명/작업
서버	
FTP/TFTP 서버 IPv4 주소	NA에서 사용하는 FTP/TFTP 서버(기본적으로 NA 서버 자체)의 IPv4 주소를 입력합니다.
FTP/TFTP 서버 IPv6 주소	NA에서 사용하는 FTP/TFTP 서버(기본적으로 NA 서버 자체)의 IPv6 주소를 입력합니다. IPv6 지원에 대한 자세한 내용은 <i>Network Automation 9.10 업그레이드 및 설치 설명서</i> 를 참조하십시오.
FTP/TFTP 파일 경로	FTP/TFTP 서버가 구성 파일을 작성할 경로 및 폴더를 입력합니다. NA에서 이 폴더에 대한 읽기/쓰기 권한이 필요합니다. 기본값은 <code>C:\<설치 디렉터리>\server\ext\tftp\tftpdroot</code> 입니다.
Syslog 서버 IPv4 주소	NA에서 사용하는 Syslog 서버의 IPv4 주소를 입력합니다. (참고: 이 옵션이 지정되어 있지 않으면 NA 서버의 첫 번째 비루프백 IPv4 주소가 사용됩니다.)
Syslog 서버 IPv6 주소	NA에서 사용하는 Syslog 서버의 IPv6 주소를 입력합니다. (참고: 이 옵션이 지정되어 있지 않으면 NA 서버의 첫 번째 비루프백 IPv6 주소가 사용됩니다.)
SMTP 서버	NA가 전자 메일 알림을 보내기 위해 사용하는 SMTP 서버의 호스트 이름 또는 IP 주소를 입력합니다.
SMTP 발신 주소	NA가 전자 메일에 사용하는 발신 주소를 입력합니다.
작업	
최대 동시 작업 수	<p>동시에 실행할 수 있는 최대 작업 수를 입력합니다. 이 설정은 동시에 실행할 수 있는 비 그룹 작업 수를 제한합니다. NA는 동시 비 그룹 작업 수를 제한하여 시스템 및 네트워크 성능 저하를 피합니다. 기본값은 20개 동시 비 그룹 작업입니다. 데이터베이스 연결 풀에서는 데이터베이스 연결 수가 제한됩니다. 따라서 최대 동시 작업 수는 50 이하여야 합니다.</p> <p>참고: NA는 사용할 수 있는 메모리가 충분하지 않으면 최대 동시 작업을 실행하지 않습니다. 따라서 최대 동시 작업이 200으로 설정되면 NA는 200개 동시 작업 모두를 실행할 수 없습니다.</p>

필드	설명/작업
최대 동시 그룹 작업 수	<p>동시에 실행할 수 있는 최대 그룹 작업 수를 입력합니다. 장치 인벤토리에 대해 실행된 스냅샷과 같은 그룹 작업은 하위 작업(그룹의 각 장치당 작업 하나)을 예약합니다.</p> <p>참고: 최대 동시 그룹 작업 수를 최대 동시 작업 수 값보다 낮게 설정하면 대규모 그룹 운영 중 NA는 시간이 중요한 독립적인 작업을 실행할 수 있습니다. 예를 들어, 대규모 그룹 범위의 암호 변경 작업 중에도 NA는 시기적절하게 실시간 변경 감지로 실행되는 스냅샷 작업을 실행합니다.</p>
최대 작업 길이	<p>작업이 중지되고 실패 상태로 되기 전에 작업이 실행될 수 있는 최대 시간을 입력합니다. 기본값은 3,600초(1시간)입니다. 지정된 작업에 대해 최대 작업 길이 시간에 도달할 경우 NA는 작업을 중지합니다. 하지만 실제로 안전하게 중지할 수 있는 지점에 도달할 때까지는 처리가 중지되지 않습니다. 일부 작업의 경우 이 시점에 도달하기까지 상당한 시간이 소요될 수도 있습니다.</p>
Syslog 구성	
기본적으로 syslog 구성	<p>이 옵션을 선택하면 NA는 자동으로 새 장치에 Syslog 변경 감지를 구성합니다.</p>
기본 Syslog 릴레이	<p>새 장치에 대한 릴레이 호스트의 기본 호스트 이름 또는 IP 주소를 입력합니다.</p>
장치 가져오기	
기존 장치 덮어쓰기	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 예 — NA는 NA 데이터베이스에 저장된 기존 장치 데이터를 가져온 데이터로 덮어씁니다(기본값). 가져오기에 포함되지 않은 장치에는 영향을 주지 않습니다. 아니요 — NA는 NA 데이터베이스에 저장된 기존 장치 데이터를 가져온 데이터로 덮어쓰지 않습니다.
누락 장치 간격	<p>이 간격보다 긴 시간 동안 가져오기 소스에서 누락된 장치는 누락/액세스 불가능 장치 작업별로 삭제되거나, 비활성으로 표시되거나, 변경되지 않은 상태로 유지됩니다. 기본값은 45일입니다.</p>
액세스 불가능 장치 간격	<p>NA가 이 간격으로 액세스할 수 없는 장치는 누락/액세스 불가능 장치 작업별로 삭제되거나, 비활성으로 표시되거나, 변경되지 않은 상태로 유지됩니다. 기본값은 45일입니다.</p>

필드	설명/작업
누락/액세스 불가능 장치 작업	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •장치 삭제 — 데이터베이스에서 누락되거나 액세스할 수 없는 장치를 삭제합니다. •장치를 비활성으로 표시 — 누락되거나 액세스 불가능한 장치를 비활성으로 표시합니다(기본값). 일반적으로 데이터베이스에서 장치를 삭제하는 것보다 장치를 비활성으로 변경하여 구성 이력을 보존하는 것이 좋습니다. •작업 없음 — 누락되거나 액세스 불가능한 장치에 대해 아무런 작업을 수행하지 않습니다.
기본 IP 재할당 및 중복 방지 설정	
기본 IP 주소 재할당	이 옵션을 선택하면 NA는 기본 IP 주소를 포함하여 장치와 연결된 모든 IP 주소를 살펴보고(장치와 연관된 다른 모든 인터페이스 추가), 제공된 정규 표현식 또는 다른 규칙과 일치하는 기본 IP 주소를 설정합니다.
인터페이스 이름 재할당 정규 표현식 패턴	오른쪽 상자 정규 표현식 패턴을 입력하고 패턴 추가 << 패턴을 클릭합니다. 정규 표현식은 IP 주소가 준수해야 하는 인터페이스 이름을 지정하는 특수 텍스트 문자열(예: Loopback.*)입니다. 패턴을 삭제하려면 왼쪽 상자에서 패턴을 선택하고 패턴 삭제 버튼을 클릭합니다.
IP 주소 재할당 정규 표현식 패턴	오른쪽 상자 정규 표현식 패턴을 입력하고 패턴 추가 << 버튼을 클릭합니다. 정규 표현식은 사용 가능한 인터페이스의 IP 주소와 일치하는 특수 텍스트 문자열입니다(예: 10\.\.1\.*). 패턴을 삭제하려면 왼쪽 상자에서 패턴을 선택하고 패턴 삭제 버튼을 클릭합니다.
IP 재할당 순서	<p>둘 이상의 IP 주소가 인터페이스 이름 또는 IP 주소 패턴과 일치할 경우 다음 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •가장 낮은 IP 주소를 선택하여 기본 IP 주소로 지정(기본값) •가장 높은 IP 주소를 선택하여 기본 IP 주소로 지정

필드	설명/작업
중복 감지	중복이 감지될 때 장치에 대해 다음 옵션 중 하나를 선택합니다. 참고: 장치의 인터페이스와 IP 주소 정보가 동일할 경우 장치는 중복으로 간주됩니다. <ul style="list-style-type: none"> •중복 유지 •중복 비활성화(기본값) •중복 삭제
도메인 이름 확인	
기존 도메인 이름 덮어쓰기	이 옵션을 선택하면 NA가 FQDN 확인 작업을 실행할 때 수동 FQDN 항목을 DNS에서 확인된 FQDN 항목으로 덮어씁니다. 작업이 실행될 때 장치 도메인 이름과 장치 호스트 이름은 모두 바뀔에 주의하십시오.
감사 로그	
감사 로깅	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •사용함 — NA는 사용자 작업의 감사 로그를 저장합니다. 로그를 보려면 감사 로그 보기를 클릭합니다. •사용 안 함 — NA는 사용자 작업의 감사 로그를 저장하지 않습니다(기본값).
데이터베이스 정리	
구성	데이터베이스에 구성을 저장할 기간(일)을 입력합니다. 기본값은 365일입니다.
진단	데이터베이스에 진단을 저장할 기간(일)을 입력합니다. 기본값은 45일입니다.
이벤트	데이터베이스에 이벤트를 저장할 기간(일)을 입력합니다. 기본값은 45일입니다.
작업	데이터베이스에 작업을 저장할 기간(일)을 입력합니다. 기본값은 365일입니다.
세션	데이터베이스에 프록시 텔넷/SSH 세션을 저장할 기간(일)을 입력합니다. 기본값은 45일입니다.
로그 파일	서버 로그 파일을 저장할 기간(일)을 입력합니다. 기본값은 30일입니다. 로그 파일은 매우 커질 수 있으므로 파일을 정리하여 서버에서 디스크 공간을 확보하는 것이 중요할 수 있습니다.

필드	설명/작업
임시 드라이버 파일	임시 드라이버 파일을 저장할 기간(일)을 입력합니다. 기본값은 30일입니다.
작업 로그 파일	작업 로그 파일이 보유될 기간(일)을 입력합니다. 기본값은 7일입니다.
토폴로지 데이터	토폴로지 데이터를 저장할 기간(일)을 입력합니다. 기본값은 45일입니다.
다이어그램 파일	다이어그램 파일을 저장할 기간(일)을 입력합니다. 기본값은 1일입니다.
ACL 데이터	ACL 데이터를 저장할 기간(일)을 입력합니다. 기본값은 365일입니다.
장치 인증 데이터	장치 인증 데이터를 저장할 기간(일)을 입력합니다. 기본값은 45일입니다.
고급 스크립팅	
스크립팅 언어 1	<p>고급 스크립팅을 사용하여 네트워크에서 사용되는 스크립팅 언어로 작성된 사용자 지정 스크립트를 실행할 수 있습니다. 각 언어에 대한 언어 해석기를 설치한 다음 고급 스크립팅 설정을 통해 해석기 경로를 언어 옵션과 연결시켜야 합니다.</p> <p>여기에서 지정한 스크립팅 언어는 고급 스크립팅 옵션을 선택할 때 새 명령 스크립트 페이지의 선택 목록에 나타납니다. 기본적으로 이 설정은 Expect에 대해 미리 구성되어 있습니다. 이 페이지에서 해당하는 해석기 경로 [#] 설정에 이 언어에 대한 해석기 경로를 지정해야 합니다.</p> <p>최대 5개 언어에 대한 고급 스크립팅 성능을 구성할 수 있고, 미리 구성된 기본값을 사용하지 않을 경우 기본 언어를 덮어쓸 수 있습니다. 명령줄에서 실행한 언어만 지원됩니다(예: JScript 및 Python).</p> <p>참고: Expect 및 Perl에 대해 슬롯 1과 2가 미리 구성되어 있습니다. 그러나 NA는 Expect에 대한 해석기만 설치합니다. 여기서 지정하는 각 언어로 작성된 스크립트를 실행하려면 각 언어에 대한 해석기를 설치하고 해당 해석기 경로를 구성해야 합니다.</p>
해석기 경로 1	스크립팅 언어 1에 지정된 언어를 실행하는 해석기 경로를 입력합니다.

필드	설명/작업
스크립팅 언어 [2-5]	<p>여기에서 지정한 언어는 고급 스크립팅 옵션을 선택할 때 새 명령 스크립트 페이지의 언어 선택 목록에 표시됩니다. 해당하는 해석기 경로 [#] 설정에 이 언어에 대한 해석기 경로를 지정해야 합니다.</p> <p>참고: 기본적으로 스크립팅 언어 2가 Perl에 대해 미리 구성되어 있지만 이 설정을 작동하게 하려면 Perl 해석기를 설치해야 합니다.</p>
해석기 경로 [2-5]	<p>연결된 스크립팅 언어 [#] 상자에 지정한 언어를 실행하는 해석기 경로를 입력합니다.</p> <p>참고: Windows 환경의 경우 기본적으로 해석기 경로 2는 Perl에 대해 미리 구성되어 있지만 NA는 Perl 해석기를 설치하지 않습니다. 이 설정이 기능 하려면 Perl을 설치하고 경로를 구성해야 합니다.</p>
동적 그룹	
동적 그룹 자동 재계산	<p>시스템이 모든 동적 그룹의 구성원 장치를 재계산하는 빈도를 입력합니다. 기본값은 60분입니다. 자동 재계산을 사용하지 않으려면 0을 입력합니다. (참고: 동적 그룹 구성원을 다시 계산하는 작업은 NA가 다양한 쿼리를 수행하여 그룹의 규칙 및/또는 필터를 기준으로 동적 그룹에 속하는 장치를 확인함을 의미합니다.)</p>
이벤트 구동 재계산	<p>이 옵션을 선택하면 장치 변경 이벤트가 발생할 때마다 시스템이 모든 동적 그룹 구성원을 다시 계산합니다.</p>
장치 변경 이벤트	<p>동적 그룹 구성원 재계산을 트리거할 장치 변경 이벤트를 선택합니다. 이 설정은 이벤트 구동 재계산 옵션이 사용될 때만 적용됩니다. 장치 변경 이벤트의 예는 다음과 같습니다.</p> <ul style="list-style-type: none"> •장치 추가됨 •장치 구성 변경 •장치 삭제됨 •장치 편집됨 •장치 소프트웨어 변경 •장치 관리되지 않음

필드	설명/작업
소프트웨어 이미지 관리	
SNMP 재시도	처음 실패 후 시도할 횟수를 입력합니다. 최대값은 5입니다.
SNMP 시간 초과	SNMP 패킷에 대한 시간 초과(초)를 입력합니다. 기본값은 5초입니다.
텔넷 시간 초과	소켓 시간 초과 값(초)을 입력합니다. 기본값은 10입니다.
HTTP 프록시 서버	HTTP 프록시 서버를 입력합니다. 프록시 서버는 직접 액세스가 작동되지 않는 경우 HTTP를 통해 Cisco.com에 액세스하는 데 사용됩니다.
HTTP 프록시 서버 포트	HTTP 프록시 서버 포트를 입력합니다.
소프트웨어 이미지 관리 서비스 호스트	소프트웨어 이미지 관리 서비스를 실행 중인 시스템의 호스트 이름 또는 IP 주소를 입력합니다.
소프트웨어 이미지 관리 서비스 포트	소프트웨어 이미지 관리 서비스 포트를 입력합니다. 이것은 소프트웨어 이미지 관리 서비스가 수신하는 포트입니다. 일반적으로 포트 6099입니다.
드라이버	
드라이버 확장 디렉터리	NA가 추가 드라이버를 찾는 디렉터리를 입력합니다. 드라이버 개발에 대한 내용은 DDK(Driver Development Kit) 문서를 참조하십시오.
성능 조정	
이벤트 목록은 563페이지 의 "시작하기"를 참조하십시오.	필터할 각 이벤트에 대한 확인란을 클릭합니다. 이 확인란을 선택하여 시스템 성능을 조정할 수 있습니다. 또한 대규모 구성을 위해 이벤트 차별화와 라인별 마스킹을 제한하고, 대규모 작업 세션 로그의 저장 및 표시를 제한할 수도 있습니다.
특수 성능 설정	
대규모 구성을 위한 이벤트 차별화 제한	대규모 구성의 경우 이벤트 전자 메일에서 구성 차이 보고서를 생성하는 프로세스에는 시스템 리소스가 많이 소비될 수 있습니다. 이 옵션을 활성화하고 크기 제한(아래 참조)을 설정하면 구성 크기가 지정된 임계값보다 큰 이벤트에 대해 구성 차이 보고서를 건너뛰게 됩니다.

필드	설명/작업
이벤트 차별화 크기 임계값	크기 제한을 설정하면 구성 크기가 지정한 임계값보다 큰 이벤트에 대해 구성 차이 보고서를 건너뛰게 됩니다.
대규모 구성에 대한 라인별 마스킹 제한	대규모 구성의 경우 두 구성 간 라인별 차이를 표시하는 프로세스에는 많은 양의 시스템 리소스가 소비될 수 있습니다. 이 옵션을 활성화하고 크기 제한(아래 참조)을 설정하면 지정된 임계값보다 크기가 큰 구성에 대해 추가 강조 표시 또는 라인 번호 매기기 없이 구성 차이 페이지에 두 구성이 나란히 표시됩니다.
라인별 마스킹 크기 임계값	크기 제한을 설정하면 지정된 임계값보다 크기가 큰 구성에 대해 추가 강조 표시 또는 라인 번호 매기기 없이 구성 차이 페이지에 두 구성이 나란히 표시됩니다.
대규모 작업 세션 로그에 대한 저장 및 표시 제한	작업 세션 로그는 작업 결과의 일부로 저장됩니다. 일부 장치는 많은 양의 데이터를 세션 로그로 덤프하므로 데이터베이스에서 작업 테이블의 크기가 크게 증가합니다. 이 옵션을 활성화하고 크기 제한(아래 참조)을 설정하면 지정된 임계값이 충족되고 나서 세션 로그가 잘리므로 해당 세션이 과도하게 커지지 않습니다.
작업 세션 로그 크기 임계값	크기 제한을 설정하면 지정된 임계값이 충족되고 나서 세션 로그가 잘리므로 세션 로그가 과도하게 커지지 않습니다.
비 관리 코어에서 Syslog 변경 감지 무시	분산 시스템에서 여러 NA 코어에 Syslog 메시지를 보내도록 장치가 설정된 경우 두 NA 코어에서 동시에 동일한 장치에 대해 스냅샷 작업을 예약하려 할 때 데이터베이스 복제 충돌이 발생할 수 있습니다. 이 옵션을 활성화하면 NA 코어에서 Syslog 메시지를 무시하고 스냅샷 작업을 예약하지 않습니다. 분산 시스템에 대한 내용은 <i>Network Automation 9.10 Multimaster Distributed System on Oracle User's Guide</i> 를 참조하십시오.
메시의 코어가 해당 코어에서 생성된 모든 작업을 로컬로 실행하도록 허용	이 옵션은 지정된 장치에 대한 작업이 임의의 NA 코어에서 실행될 수 있도록 로컬 NA 코어에 지시하므로 한 번에 한 작업만 장치에서 실행됩니다. 이 NA 코어는 다른 NA 코어와 통신하여 실행 중인 작업을 확인해야 합니다. 분산 시스템에 대한 내용은 <i>Network Automation 9.10 Multimaster Distributed System on Oracle User's Guide</i> 를 참조하십시오.

필드	설명/작업
이 코어에서 생성된 모든 작업을 로컬로 실행하도록 허용	이 옵션은 사용자가 생성한 작업이 이 NA 코어에 기록되어 현재 NA 코어에 작업이 할당되도록 합니다. 따라서 장치가 속하는 사이트에 대한 관리하는 NA 코어가 무시됩니다. 분산 시스템에 대한 내용은 <i>Network Automation 9.10 Multimaster Distributed System on Oracle User's Guide</i> 를 참조하십시오.

변경 사항을 저장하려면 저장을 클릭해야 합니다.

워크플로

워크플로 페이지에서 다음 작업을 수행할 수 있습니다.

- 워크플로 사용
- 이벤트 알림 및 응답 규칙 구성
- 장치 예약 시스템 구성
- 텔넷/SSH 프록시에 대한 장치 예약 구성

워크플로 페이지를 보려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 워크플로를 클릭합니다. 워크플로 페이지가 열립니다.

워크플로 페이지 필드

필드	설명/작업
워크플로	
워크플로 사용	이 옵션을 선택하면 승인 규칙이 정의된 작업에 대해 승인이 필요합니다.
우선 순위 값	승인이 필요한 작업에 설정할 수 있는 우선 순위를 정의합니다. 기본값은 다음과 같습니다. <ul style="list-style-type: none">•낮음•중간•높음 값을 입력하고 값 추가 << 버튼을 클릭하여 긴급, 보통 등과 같은 다른 값을 추가할 수 있습니다. 값을 선택하고 값 삭제 버튼을 클릭하여 값을 삭제할 수 있습니다. 참고: NA 스케줄러는 값을 살펴보지 않습니다. 이것은 기본적으로 시기 적절하게 승인이 필요한 작업을 확인하기 위해 표시되는 대기열입니다.

필드	설명/작업
이벤트 알림 및 응답 규칙	
작업 실행	이 항목을 선택하면(기본값) 이벤트 규칙으로 인해 예정된 모든 작업을 승인해야 합니다. 예를 들어 구성 정책 비준수 이벤트가 발생하고 그로 인해 수정 조치를 위한 작업이 트리거되는 경우 해당 작업은 배포 전에 승인해야 합니다.
장치 예약 시스템	
장치 예약 시스템	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •사용함 — 장치 예약 시스템을 활성화합니다(기본값). 장치 예약 시스템에 대한 내용은 246페이지의 "장치 예약"을 참조하십시오. •사용 안 함 — 장치 예약 시스템을 비활성화합니다.
기본 기간	장치 및/또는 장치 그룹이 예약 상태를 유지할 수 있는 기간(분)을 입력합니다. 기본값은 60분입니다.
활동 캘린더의 최대 열 수	활동 캘린더의 최대 열 수를 설정합니다. 기본값은 1024입니다. 활동 캘린더에 대한 내용은 247페이지의 "활동 캘린더" 를 참조하십시오.
30분 동안 최소 오버랩	30분 동안 예약됨으로 활동 캘린더에 표시하기 위해 예약을 연장해야 하는 최소 시간(분)을 30분으로 설정합니다. 기본값은 5분입니다.

필드	설명/작업
텔넷/SSH 프록시 예약	
<p>텔넷/SSH 프록시에 대한 장치 예약</p>	<p>NA 텔넷/SSH 프록시를 사용하여 장치에 액세스하고 구성할 수 있습니다. 이 옵션은 액세스 제어, 키스트로크 세션 로깅 및 인라인 주석 성능을 제공합니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 무시 — 텔넷/SSH 프록시를 통해 장치에 액세스할 때 장치 예약을 무시합니다(기본값). 장치 예약 시스템에 대한 내용은 246페이지의 "장치 예약"을 참조하십시오. • 경고 — 텔넷/SSH 프록시를 통해 장치에 액세스할 때 승인된 장치 예약이 없을 경우 사용자에게 경고합니다. • 방지 — 승인된 장치 예약이 없을 경우 사용자가 텔넷/SSH 프록시를 통해 장치에 연결하지 못하도록 합니다. 사용자가 오버라이드 권한을 가지는 경우 장치에 대한 비액세스를 오버라이드할지 여부를 묻습니다. <p>경고 또는 금지를 선택하면 NA가 사용자, 장치 및 장치 그룹을 포함하여 일치하는 장치 예약과 예약이 승인된 경우 멀티 태스킹 프로젝트에 대해 예정된 시간을 찾습니다.</p>
장치 예약 경고 메시지 없음	승인된 장치 예약이 없을 때 표시할 경고 메시지를 입력합니다. 기본 경고 메시지는 <i>경고: 지금 이 장치에 대해 승인된 예약이 없습니다</i> 입니다. 기본 경고 메시지를 삭제하는 옵션을 사용할 수 있습니다.

사용자 인터페이스

사용자 인터페이스 페이지에서 다음 작업을 수행할 수 있습니다.

- 로그인 보안 구성
- 모든 페이지에 표시된 날짜 형식 설정
- NA 메뉴 사용자 지정
- 모듈 보기/편집 페이지에 대한 슬롯 추가
- 새 템플릿/템플릿 편집 페이지에서 역할 추가 및 삭제
- 명령 스크립트 및 진단 편집 페이지의 텍스트 상자 크기 사용자 지정
- 장치 선택기 표시 사용자 지정
- 향상된 사용자 지정 필드 사용
- 빠른 시작 작업 작업 구성

사용자 인터페이스 페이지를 보려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 사용자 인터페이스를 클릭합니다. 사용자 인터페이스 페이지가 열립니다. 완료되면 저장을 클릭해야 합니다.

사용자 인터페이스 페이지 필드

필드	설명/작업
보안	
세션 시간 초과	비활성 웹 세션을 종료하기 전에 NA가 기다리는 시간(초)을 입력합니다. 기본값은 1800초입니다. 변경 사항은 다음 로그인까지 적용되지 않습니다.
장치 구성을 보기 위한 장치 권한 확인	이 옵션을 선택하면 사용자에게 해당 장치 권한이 있을 경우에만 장치 구성을 볼 수 있습니다. 변경 사항을 적용하려면 NA를 다시 시작해야 합니다.
사용자 이름 및 암호 자동 완성	이 옵션을 선택하면 NA 로그인 페이지에서 브라우저의 자동 완성 기능이 '사용'으로 설정됩니다.
스택 추적 표시	이 옵션을 선택하면 웹 UI 오류 페이지에서 예외 스택 추적을 볼 수 있습니다.

필드	설명/작업
사이트 간 스크립팅 확인	이 옵션을 선택하면 NA가 사용자 입력을 확인하여 <script>, <object>, , <input> 등과 같은 잠재적인 사이트 간 스크립팅 요소를 필터링합니다. 즉, 이 옵션을 사용하여 스크립트에서 잠재적인 악성 Javascript 코드를 제거할 수 있습니다. 악성 Javascript 코드가 발견되면 오류가 반환됩니다.
날짜/시간 표시	
날짜 형식	이 설정은 웹 인터페이스 전체에 날짜가 나타나는 방식을 제어합니다. 기본 형식은 MMM-dd-yy HH:mm:ss입니다. 날짜 및 시간 요소의 순서를 다양하게 설정하고, 날짜 및 시간을 교체하고, 4자리수 연도(yyyy)를 입력하고, 월을 2자리수 값(MM)으로 변경할 수 있습니다. 요소는 대소문자를 구분합니다. 예를 들어 HH는 24시간 시계를 나타내는 반면, hh는 12시간 시계를 나타냅니다.
메뉴 사용자 지정	
사용자 지정 메뉴 링크 표시	이 옵션을 선택하면 정보 옵션 위에 사용자가 정의한 이름이 나타납니다. 티켓팅 응용 프로그램의 홈 페이지와 같은 HTML 페이지에 대한 메뉴 제목과 링크를 제공할 수 있습니다.
사용자 지정 메뉴 제목	표시할 이름을 입력합니다.
사용자 지정 메뉴 페이지	사용자 지정 메뉴 링크 표시를 선택하면 사용자가 메뉴 제목을 클릭하면 표시되는 HTML 페이지의 URL을 입력합니다. 이것은 다른 HTML 응용 프로그램 내 페이지일 수 있습니다.
구성 비교	
시각적 비교를 위한 컨텍스트 라인 수	두 구성을 비교할 때 각 변경 위 및 아래에 표시할 라인 수를 입력합니다. 기본값은 3입니다.
전자 메일 비교를 위한 컨텍스트 라인	두 구성을 전자 메일의 텍스트로 비교할 때 각 변경 위 및 아래에 표시할 라인 수를 입력합니다. 기본값은 3입니다.
소프트웨어 센터	
슬롯	모듈 보기/편집 페이지에 나타나는 슬롯(카드/블레이드/모듈에 대한 새시 슬롯)을 추가 및 삭제합니다. 슬롯을 추가하려면 오른쪽 상자에 슬롯을 입력하고 슬롯 추가 <<를 클릭합니다. 슬롯을 삭제하려면 왼쪽 상자에서 슬롯을 선택하고 슬롯 삭제를 클릭합니다.

필드	설명/작업
파일 준수 수준 표시	이미지 집합의 각 이미지 파일에 대한 준수 수준을 표시하려면 확인란을 선택합니다.
장치 모델	장치 모델을 입력하고 나서 모델 추가 버튼을 클릭합니다. 장치 모듈 버튼을 사용하면 장치 모듈을 삭제할 수 있습니다.
프로세서 유형	프로세서 유형을 입력하고 나서 프로세서 추가 버튼을 클릭합니다. 프로세서 삭제 버튼을 사용하면 프로세서 유형을 삭제할 수 있습니다.
장치 BootROM	장치 BootROM을 입력하고 나서 장치 BootROM 추가 버튼을 클릭합니다. BootROM 삭제 버튼을 사용하면 장치 BootROM을 삭제할 수 있습니다.
템플릿	
템플릿 역할	새 템플릿/템플릿 편집 페이지에서 템플릿 작성자가 선택하는 역할을 추가 및 삭제합니다. 역할은 테두리 또는 코어와 같은 네트워크에서 장치가 수행하는 역할을 설명할 수 있습니다. 역할을 추가하려면 오른쪽 상자에 역할을 입력하고 역할 추가 <<를 클릭합니다. 역할을 삭제하려면 왼쪽 상자에서 역할을 선택하고 역할 삭제를 클릭합니다.
스크립트	
스크립트 텍스트 높이	명령 스크립트 편집 및 진단 편집 페이지의 텍스트 상자 크기(높이)를 입력합니다. 기본값은 12행입니다.
스크립트 텍스트 너비	명령 스크립트 편집 및 진단 편집 페이지의 텍스트 상자 크기(너비)를 입력합니다. 기본값은 60자입니다.
고급 사용자 지정 필드	
향상된 사용자 지정 필드 사용	이 옵션을 선택하면 일부 데이터 집합에 대해 향상된 사용자 지정 필드를 구성할 수 있습니다. 사용자 지정 데이터 필드를 사용하여 특정 장치, 구성, 사용자 등에 유용한 데이터를 할당할 수 있습니다. 자세한 내용은 694페이지의 "사용자 지정 데이터 설정 페이지 필드" 를 참조하십시오.
기타	
작업 페이지 새로 고침 간격	작업 목록 페이지를 새로 고치는 간격(초)을 입력합니다. 기본값은 60초입니다.

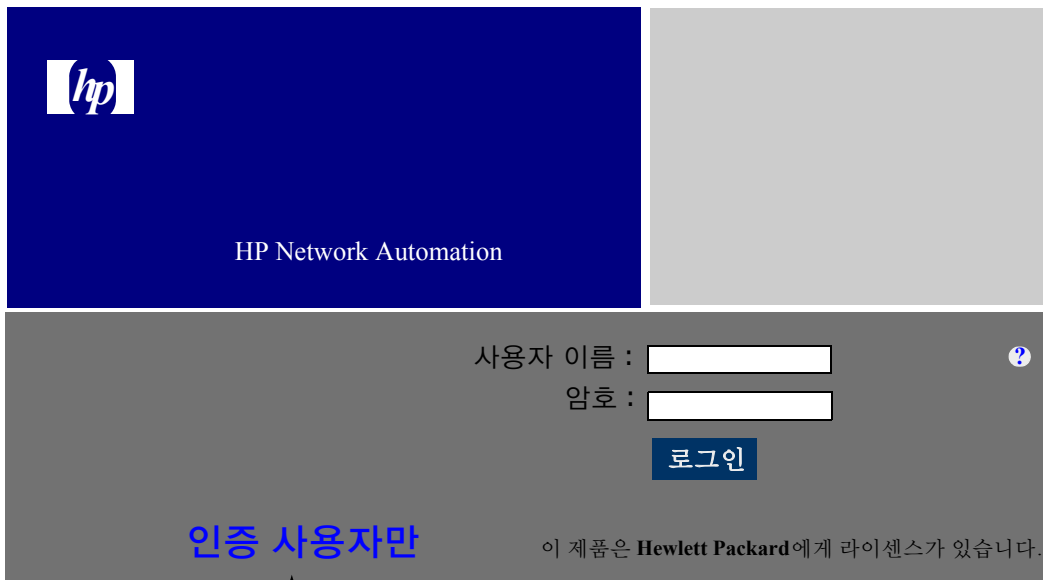
필드	설명/작업
일반 텍스트로 표시하기 위한 구성 크기 임계값	구성을 일반 텍스트로 표시하기 위한 구성 크기 임계값을 입력합니다. 기본값은 200,000바이트입니다. 일부 구성은 규모가 너무 커서 막대한 양의 서버 및 브라우저 리소스를 소모하지 않고 라인 번호 매김과 같은 특수 처리를 제공할 수 없습니다. 구성이 기본값을 초과할 때 구성은 <pre> 및 </pre> 태그를 사용하여 일반 텍스트로 표시됩니다.
커뮤니티 문자열 마스크	이 옵션을 선택하면 웹 UI의 커뮤니티 문자열이 일반 텍스트로 표시되지 않습니다. 이 옵션은 NA에 표시된 커뮤니티 문자열 전용입니다. 구성에 포함된 커뮤니티 문자열은 드라이버별 중요 데이터 마스크 구현에 따라 마스크됩니다.
숨겨진 스택 추적 출력 사용 안 함	이 옵션을 선택하면 숨겨진 스택 추적이 비활성화됩니다. 이 옵션을 선택하지 않으면 서버 오류가 발생할 때 NA는 서버 로그 외에 추가로 스택 추적을 숨겨진 텍스트로 HTML 페이지에 출력합니다. (참고: 전체 Java 스택 추적은 기본적으로 지원 호출에 도움이 되도록 숨겨진 HTML로 제공됩니다. 숨겨진 HTML이 잠재적인 보안 취약점이 될 수 있다고 생각되면 이 옵션을 선택하십시오.)
자세한 예외 메시지 출력 사용 안 함	이 옵션을 선택하면 자세한 예외 메시지 출력이 사용되지 않습니다. 이 옵션을 선택하지 않으면 서버 오류가 발생할 때 NA는 자세한 예외 메시지를 서버 로그 외에 HTML 페이지에 출력합니다.

HP 로그인 페이지 사용자 지정

HP NA(Network Automation) 로그인 페이지를 사용자 지정하여 경고 메시지 또는 회사별 정보와 같은 정보를 표시할 수 있습니다.

HP 로그인 페이지를 사용자 지정하려면

1. `$NA_install_dir/resource` 디렉터리에서 `customer_banner.html` 파일을 엽니다. 파일이 없으면 해당 이름으로 파일을 생성합니다. (참고: `resource` 디렉터리를 생성해야 할 수도 있습니다.)
2. 텍스트 편집기로 파일을 열고(HTML이 허용됨) HP 로그인 페이지에 표시할 텍스트를 입력합니다.
3. 파일을 저장하고 NA에 로그인합니다. 로그인 상자 아래에 텍스트가 표시됩니다. 표시할 수 있는 단어 수에 대한 제한은 없습니다. 하지만 페이지에 적절하게 맞춰지도록 화면 표시를 확인해야 합니다. 다음은 샘플 로그인 페이지입니다.



사용자 지정 배너

텔넷/SSH

텔넷/SSH 페이지에서 다음 설정을 구성할 수 있습니다.

- 텔넷/SSH 로깅
- 텔넷/SSH 프록시
- 장치 단일 사인온
- 텔넷 클라이언트
- 텔넷 서버
- SSH 서버

텔넷/SSH 페이지를 보려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 텔넷/SSH를 클릭합니다. 텔넷/SSH 페이지가 열립니다.

장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버그하는 첫 번째 단계로 세션 로그를 확인해야 합니다. 세션 로그는 CLI, SNMP 및 작업 중 수행한 모든 전송 프로토콜 작업에 대한 세부사항을 제공합니다.

텔넷/SSH 페이지 필드

필드	설명/작업
텔넷/SSH 세션 로깅	
명령 기록	이 옵션을 선택하면 텔넷 또는 SSH 세션 실행 시 명령이 저장됩니다. 명령을 보려면 장치 정보 페이지에서 텔넷/SSH 세션 보기를 클릭한 다음 명령만 보기를 클릭합니다. 이 페이지의 스크립트로 변환 링크를 사용하여 나중에 사용하기 위해 세션의 명령을 스크립트에 빨리 캡처할 수 있습니다. 자세한 내용은 720페이지의 "명령 스크립트 추가" 를 참조하십시오.
응답 기록	이 옵션을 선택하면 텔넷 또는 SSH 세션을 실행할 때 전체 세션 로그를 저장합니다. 로그를 보려면 장치 정보 페이지에서 텔넷/SSH 세션 보기 및 전체 세션 보기를 클릭합니다. 이 페이지의 스크립트로 변환 링크를 사용하여 나중에 사용하기 위해 세션의 명령을 스크립트에 빨리 캡처할 수 있습니다. 자세한 내용은 720페이지의 "명령 스크립트 추가" 를 참조하십시오.
로깅 강제 시행	이 옵션을 선택하면 API 사용 도중 각 텔넷/SSH 세션에 대한 장치 명령 및 응답을 강제로 로깅합니다.
텔넷/SSH 프록시	
텔넷/SSH 서버 사용	텔넷/SSH 프록시를 사용하여 장치에 액세스하고 구성할 수 있습니다. 이 옵션은 액세스 제어, 키스트로크 세션 로깅 및 인라인 주석 성능을 제공합니다. 이 옵션을 선택하면(기본값) NA가 텔넷/SSH 서버로 작동할 수 있습니다.
서버 비활성 시간 초과	유휴 상태의 텔넷 또는 SSH 세션이 연결 끊김으로 전환되기 전에 NA 텔넷/SSH 서버에 연결되는 최대 시간을 입력합니다. NA에 연결된 텔넷/SSH 클라이언트가 이 시간 동안 활성화되지 않는 경우 세션 시간이 초과됩니다. 기본값은 30분입니다.

필드	설명/작업
기본 연결 방법	<p>단일 사인온 없이 장치에 연결하려면 텔넷 또는 SSH를 선택합니다. 이 방법은 <code>-method</code> 옵션이 포함되지 않을 때 텔넷/SSH 프록시 연결 명령에서 사용되는 연결 방법입니다. 단일 사인온 사용을 선택하고 장치 편집 페이지의 지원 목록에 동일한 연결 방법이 포함된 경우가 아니면 이 방법이 무시됩니다.</p> <p>참고: NA가 외부 인증을 위해 SecurID를 사용하도록 구성되었을 때는 NA 프록시에 연결할 때 단일 사인온 기능이 활성화되지 않습니다. SecurID 암호 코드는 다시 사용될 수 없으므로 SecurID 자격 증명을 사용하여 다시 인증해야 합니다.</p>
장치 비활성 시간 초과	연결을 닫기 전에 NA가 유휴 상태 장치 세션을 열어 두는 시간(분)을 입력합니다. 기본값은 30분입니다.
SSH 로그인 시간 초과	NA 프록시에서 <code>-login</code> 스위치를 사용하여 SSH 로그인의 시간 초과에 대한 시간(초)을 입력합니다. 기본값은 15초입니다.
동시 세션에 대한 주의	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 동시 세션 경고 — 이 옵션을 선택하면(기본값) 두 번째 사용자가 장치에 연결하려고 할 때 경고가 발생합니다. 이 옵션은 한 사용자가 다른 사용자의 변경을 실수로 덮어쓰지 않도록 하는 데 유용합니다. 관리 권한이 있는 사용자만 경고를 오버라이드할 수 있습니다. • 동시 세션 금지 — 이 옵션을 선택하면 NA는 모든 사용자에 대한 동시 세션을 금지합니다. • 작업 없음 — 이 옵션을 선택하면 NA는 동시 세션을 무시합니다.
분산 시스템에 대한 동시 세션 처리	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 비로컬 장치에 대한 세션 허용. 동시 세션 경고(위의 설명 참조)와 비로컬 장치에 대한 세션 허용을 둘 다 선택한 경우 경고가 표시되지 않습니다. • 비로컬 장치에 대한 세션 금지 <p>분산 시스템에 대한 내용은 <i>Network Automation 9.10 Multimaster Distributed System on Oracle User's Guide</i>를 참조하십시오.</p>
알 수 없는 장치에 연결	이 옵션을 선택하면(기본값) NA를 사용하여 관리되지 않는 장치에 연결할 수 있습니다.

필드	설명/작업
최대 장치 연결 목록	와일드카드 검색에 기반한 장치에 연결할 때 일치하는 장치가 여러 개 발견되는 경우 표시되는 최대 장치 수를 입력합니다. 기본값은 20입니다. 더 많은 장치가 반환될 수 있는 경우 와일드카드 표현식을 제한할 것을 요청합니다.
장치 단일 사인온	
단일 사인온 사용	이 옵션을 선택하면(기본값) NA는 자동으로 사용자를 한 번 인증한 다음 사용자가 장치 수정 권한을 가지는 장치에 기록합니다. 참고: NA가 외부 인증을 위해 SecurID를 사용하도록 구성되었을 때는 NA 프록시에 연결할 때 단일 사인온 기능이 활성화되지 않습니다. SecurID 암호 코드는 다시 사용될 수 없으므로 SecurID 자격 증명을 사용하여 다시 인증해야 합니다.
장치 권한을 수정하지 않을 때 단일온 모드	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •로그인 프롬프트 제공 •제한된 액세스 모드로 로그인 •로그인 거부
로그인 배너 표시	이 옵션을 선택하면(기본값) NA는 장치에 로그인할 때 로그인 배너를 표시합니다.
단일 사인온에 대한 AAA 로그인 사용	이 옵션을 선택하면 NA는 AAA 로그인 정보를 사용합니다. 이 옵션은 새 사용자/사용자 편집 페이지의 프록시 인터페이스에 AAA 로그인 사용 섹션으로 안내합니다.
AAA 로그인 실패 시 HP Network Automation 로그인 사용	이 옵션을 선택하면(기본값) AAA 사용자 이름 및 암호 정보가 실패할 경우 NA 로그인 정보가 사용됩니다.

필드	설명/작업
텔넷 클라이언트	
텔넷 클라이언트	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • NA의 통합 텔넷 클라이언트 사용(기본값)(참고: 단일 사인온을 지원하는 유일한 옵션입니다.) • NA의 텔넷 프록시에 표준 브라우저 telnet:// URL 사용 • 표시된 장치에 직접 표준 브라우저 telnet:// URL 사용
텔넷 서버(이러한 설정을 변경하면 텔넷/SSH 서버가 다시 시작됨)	
텔넷 사용	이 옵션을 선택하면(기본값) NA는 텔넷 서버로 작동합니다.
텔넷 서버 포트	NA가 클라이언트 연결을 승인하는 포트를 입력합니다. Windows의 경우 기본값은 23이고, Unix의 경우 기본값은 8023입니다.
최대 텔넷 연결	NA가 동시에 승인하는 최대 텔넷 클라이언트 연결 수를 입력합니다. 기본값은 50입니다.
SSH 서버(이러한 설정을 변경하면 텔넷/SSH 서버가 다시 시작됨)	
SSH 사용	이 옵션을 선택하면(기본값) NA는 SSH 서버로 작동합니다.
SSH 서버 포트	NA가 클라이언트 연결을 승인하는 포트를 입력합니다. 기본값은 22입니다.
최대 SSH 연결	NA가 동시에 승인하는 최대 SSH 클라이언트 연결 수를 입력합니다. 기본값은 50입니다.

변경 사항을 저장하려면 저장을 클릭해야 합니다.

보고

보고 페이지에서 다음을 포함하여 조직에 대한 네트워크 상태 보고서를 사용자 지정할 수 있습니다.

- 정책 규칙 위반
- 소프트웨어 준수 위반
- 시작 구성과 실행 구성 간 불일치
- 장치 액세스 실패
- 구성 변경
- 전자 메일 보고서
- 다이어그램 작성
- 이미지 동기화 보고서

각 보고 범주에 대해 위험 수준 색상 코드와 각 층에서 준수하지 않는 장치 백분율에 대한 임계값을 지정하는 매개변수를 조합하여 개별 장치(및 장치 그룹)에 대한 상태 표시기를 설정할 수 있습니다. 예를 들어, 외부 네트워크 액세스 및 원격 사무실을 제어하는 테두리 라우터 그룹에는 더 높은 점수를 할당하는 반면 LAN 장치는 기본값 그대로 유지할 수 있습니다.

네트워크에서 각 이벤트의 중요성을 가장 잘 반영하는 설정을 제공하면 문제점을 식별하고 네트워크가 설정된 모든 정책을 실제로 준수하는 데 도움이 될 수 있습니다.

또한 보고 페이지에는 사용자 정의 전자 메일 알림 작업을 통해 전송된 전자 메일 보고서의 형식 및 내용에 대한 옵션 및 보고서를 저장할 위치를 지정하는 옵션이 있습니다. 또한 다이어그램 매개변수를 설정할 수 있습니다. 다이어그램에 대한 내용은 **764페이지의 "다이어그램 작성 페이지 필드"**를 참조하십시오.

참고: 비준수 장치의 상태(위험 수준)가 그룹의 상태를 결정합니다. 예를 들어, 단일 비준수 장치의 위험 수준을 노란색으로 설정할 때 그룹의 한 장치가 위반 상태에 있으면 위반 장치 수에 대한 임계값에 도달할 때 장치 그룹은 상태를 노란색으로 표시됩니다.

보고 페이지를 보려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 보고를 클릭합니다. 보고 페이지가 열립니다.

보고 페이지 필드

필드	설명/작업
정책 규칙 위반	
장치 상태 색상	<p>장치 그룹의 단일 장치가 구성 정책 규칙을 위반할 때 표시할 색상을 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 빨강(기본값) • 노랑 • 녹색
범주 상태 색상	<p>다음 장치 상태 색상에 대한 구성 정책 위반 장치의 임계값(백분율)을 입력합니다.</p> <ul style="list-style-type: none"> • 노랑 — 기본값이 1%입니다. • 빨강 — 기본값이 2%입니다.
소프트웨어 수준 위반	
장치 상태 색상	<p>장치 그룹의 단일 장치에 대한 소프트웨어가 준수하지 않을 때 표시할 색상을 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 빨강(기본값) • 노랑 • 녹색 <p>다음 준수 수준은 위반으로 간주됩니다.</p> <ul style="list-style-type: none"> • 보안 위험 • 사전 프로덕션 • 사용되지 않음 • 브론즈 • 실버 • 골드 • 플래티늄
범주 상태 색상	<p>소프트웨어 수준 위반이 있는 장치의 임계값(백분율)을 입력합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 노랑 — 기본값이 1%입니다. • 빨강 — 기본값이 2%입니다.

필드	설명/작업
시작 구성과 실행 구성 간 불일치	
장치 상태 색상	<p>장치 그룹에 있는 단일 장치의 시작 구성이 실행 구성과 일치하지 않을 때 표시할 색상을 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 빨강 • 노랑(기본값) • 녹색
범주 상태 색상	<p>시작과 실행이 불일치하는 장치의 임계값(백분율)을 입력합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 노랑 — 기본값이 1%입니다. • 빨강 — 기본값이 2%입니다.
장치 액세스 실패	
장치 상태 색상	<p>장치 그룹의 단일 장치가 장치 액세스 실패를 보고할 때 표시할 색상을 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 빨강 • 노랑(기본값) • 녹색
범주 상태 색상	<p>액세스가 실패된 장치의 임계값(백분율)을 입력합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 노랑 — 기본값이 1%입니다. • 빨강 — 기본값이 2%입니다.
구성 변경	
장치 상태 색상	<p>장치 그룹에 있는 단일 장치의 구성이 변경했을 때 표시할 색상을 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 빨강 • 노랑(기본값) • 녹색

필드	설명/작업
범주 상태 색상	<p>구성 변경을 가지는 장치의 임계값(백분율)을 입력합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 노랑 — 기본값이 1%입니다. • 빨강 — 기본값이 2%입니다.
전자 메일 보고서	
전자 메일 보고서 형식	<p>검색 결과를 전자 메일 보고서로 보낼 때 사용할 전자 메일 형식을 선택합니다. 이 옵션은 네트워크 상태 보고서에는 적용되지 않습니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • HTML 메일(기본값) • CSV 파일 첨부 • 일반 텍스트 • HTML 전자 메일(링크 포함 안 함)
전자 메일 보고서에 작업 결과 포함	<p>이 옵션을 선택하면 전체 작업 세부사항이 CSV(침표로 분리된 값) 파일 형식으로 작업 검색 결과를 포함하는 전자 메일 보고서에 포함됩니다. 이 옵션은 네트워크 상태 보고서에는 적용되지 않습니다.</p>
전자 메일 링크	<p>전자 메일 보고서의 HTML 링크 주소 형식을 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 호스트 이름(확인 가능한 경우) • IP 주소 • 정규 이름(확인 가능한 경우, FQDN) (기본값) • 사용자 정의 — 전자 메일 링크에 사용할 사용자 정의 서버 주소를 입력합니다.

필드	설명/작업
단일 보기	
추적할 장치 변경 이벤트	<p>추적할 장치 변경 이벤트를 선택합니다. 이 설정은 단일 보기 페이지에 표시할 기본 이벤트 집합을 결정합니다. 681페이지의 "단일 보기 페이지 필드"를 참조하십시오. 이벤트는 다음과 같습니다.</p> <ul style="list-style-type: none"> •장치 구성 변경 •장치 부팅됨 •장치 진단 변경됨 •장치 암호 변경 •모듈 추가됨 •모듈 변경됨 •모듈 제거됨 •소프트웨어 변경 •사용자 메시지
추적할 진단	<p>추적할 진단을 선택합니다. 이 설정은 단일 보기 페이지에서 해당 이벤트 유형을 선택하면 표시되는 장치 진단 변경됨 이벤트를 결정합니다. 681페이지의 "단일 보기 페이지 필드"를 참조하십시오. 기본 진단 유형은 다음과 같습니다.</p> <ul style="list-style-type: none"> •하드웨어 정보 •메모리 문제 해결 •NA 감지 장치 부팅 •NA 장치 파일 시스템 •NA 플래시 저장 공간 •NA 인터페이스 •NA 모듈 상태 •NA OSPF 인접 환경 •NA 라우팅 테이블 <p>참고: 진단에 대한 자세한 내용은 261페이지의 "메뉴 옵션 보기"를 참조하십시오.</p>

필드	설명/작업
다이어그램 작성	
최대 노드	다이어그램에 표시할 최대 노드 수를 입력합니다. 기본값은 250개 노드입니다. 다이어그램 생성으로 인해 메모리 부족 오류가 발생할 경우 이 값을 낮출 수 있습니다. 많은 노드를 포함하는 다이어그램은 대용량 이미지로 만듭니다. 이미지가 JPEG 형식으로 출력되기 전에 압축되지 않은 형태로 메모리에 생성됩니다. 다이어그램에 추가 노드를 포함하려면 값을 증가시킬 수 있지만, 메모리 부족 상태를 초래할 수 있습니다.
레이블 글꼴 크기	다이어그램의 레이블 글꼴 크기를 입력합니다. 기본값은 8입니다. 이 값을 증가시키면 노드 크기에 비해 레이블의 크기가 증가하여, 잠재적으로 레이블의 가독성이 좀 더 높아집니다.
최대 레이아웃 기간	레이아웃 알고리즘을 실행할 최대 시간을 입력합니다. 기본값은 30초입니다. 레이아웃 알고리즘은 이 최대 시간 후 정지합니다. 이 제한에 도달해도 정확한 다이어그램이 생성됩니다. 하지만 다이어그램이 가장 최적의 상태로 배치되지 않을 수 있습니다.
다이어그램 압축성	0~100 범위에서 노드 간 공간을 입력합니다. 기본값은 95입니다. 이 값은 다이어그램의 분포 형태를 제어합니다. 압축성이 낮은 다이어그램의 노드가 읽기 편합니다. 압축성이 높은 다이어그램일수록 공간을 적게 차지하는 반면 압축 다이어그램은 읽기 힘들 수 있습니다. 또한 레이아웃은 더 오래 걸리는 경향이 있으므로 압축 다이어그램은 실행하는 데 시간이 조금 더 걸릴 수 있습니다.
품질-시간 비율	0~100 범위에서 기본 레이아웃 비율을 입력합니다. 기본값은 100입니다. 값이 높을수록 다이어그램 외형이 선명해지지만 레이아웃하는 데 더 많은 시간이 걸리고 더 많은 CPU 주기가 사용됩니다.
기본 가장자리 길이	0~100 범위에서 기본 가장자리 길이 값을 입력합니다. 기본값은 100입니다. 일반적으로 가장자리가 길수록 다이어그램에서 노드 간 공간이 커지지만 필요에 따라 레이아웃 알고리즘이 이 설정을 오버라이드합니다. 값이 클수록 다이어그램은 넓게 분포되어 메모리 소비가 높아집니다. 값이 높을수록 가장자리에서 노드 및 레이블을 오버랩하기 않으므로 다이어그램이 읽기 쉬워집니다.
기본 최소 노드 거리	0~100 범위에서 기본 최소 노드 거리 값을 입력합니다. 기본값은 20입니다. 이 값은 연결이 없는 노드 간의 간격을 제어합니다. 값이 작을수록 다이어그램 압축성은 커집니다.

필드	설명/작업
이미지 동기화 보고서	
이미지 동기화 보고서 파일	이미지 동기화 보고서 파일을 입력하고 파일 추가 버튼을 클릭합니다. 파일 삭제 버튼을 사용하면 이미지 동기화 보고서 파일을 삭제할 수 있습니다. 이미지 동기화 보고서를 사용하면 NA 소프트웨어 이미지 리포지토리에 상주하지 않는 장치 또는 장치 그룹에서 현재 실행 중인 소프트웨어 이미지 또는 백업 소프트웨어 이미지를 볼 수 있습니다. 이미지 동기화 보고서에 대한 자세한 내용은 776페이지의 "이미지 동기화 보고서 필드" 를 참조하십시오.
기타	
Excel CSV 형식 사용	이 옵션을 선택하면(기본값) 검색 결과를 CSV(쉼표로 분리된 값) 파일로 내보낼 때 Microsoft Excel CSV 형식이 사용됩니다.
전자 메일 보고서 파일 내보내기 위치	모든 보고서 파일을 저장할 NA 서버의 위치 경로를 입력합니다. 사용자가 전자 메일 보고서 작업을 정의할 때 파일에 이 보고서 저장 옵션을 선택할 경우 모든 보고서는 자동으로 이 위치에 저장됩니다. 기본 위치는 <code>C:\<설치 디렉터리>/addins</code> 입니다.

사용자 인증

사용자 인증을 사용하면 사용자 인증을 한 곳에서 관리하여 여러 개의 데이터베이스를 유지 보수하지 않아도 됩니다. 사용할 수 있는 사용자 인증 옵션은 다음과 같습니다.

- LDAP(Lightweight Directory Access Protocol)
- SecurID
- TACACS+
- RADIUS
- HP SA(HP Server Automation)
- HP OO(HP Operations Orchestration)

외부 인증이 실패하면 NA는 다음의 경우 로컬 사용자 자격 증명에 폴백을 시도합니다.

- 외부 인증 서비스가 중단되거나 액세스될 수 없는 경우
- 외부 인증 방법을 통해 성공적으로 로그인하지 않은 정적 사용자 계정인 경우
- 기본 제공된 관리 사용자 계정인 경우

참고: NA가 로컬 인증으로 장애 조치를 실행하도록 하려면 사용자 계정에 대해 이 성능을 활성화해야 합니다. 기본적으로 NA는 로컬 인증으로 장애 조치하지 않습니다. 자세한 내용은 [98페이지](#)의 "인증 장애 조치" 및 [323페이지](#)의 "새 사용자 페이지 필드"를 참조하십시오.

또한 사용자 인증을 사용하여 NA에서 기본 제공된 사용자에게 대해 다음 보안 정책을 구성할 수 있습니다.

- 최소 암호 길이 정의
- 암호 복잡성 규칙 정의
- 구성된 연속 로그인 시도 실패 횟수 후 사용자 잠금

사용자 인증 페이지를 보려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 사용자 인증을 클릭합니다. 사용자 인증 페이지가 열립니다. 자세한 내용은 [102페이지](#)의 "사용자 인증 페이지 필드"를 참조하십시오.

인증 장애 조치

TACACS와 같은 단순 인증의 경우 로그인 실패 시 로컬 인증에 대한 장애 조치가 발생합니다. LDAP 인증의 경우, 사용자가 외부적으로 존재하지 않은 경우 또는 LDAP 연결 오류가 있는 경우에만 장애 조치가 발생합니다.

모든 인증 방법에 대해 장애 조치는 다음 조건에 대해서만 발생할 수 있습니다.

- 사용자가 장애 조치로 구성되어 있습니다.
- 기본 관리 사용자(UID = 1)가 사용됩니다.

장애 조치는 다음 알고리즘을 사용합니다.

1. 외부 인증 방법 시도
2. 실패 모드 테스트

외부 인증 서버에 대한 연결 오류가 있는 경우:

- 관리 사용자(UID = 1)인 경우 로컬 인증을 시도합니다.
- 관리 사용자가 아닌 경우 장애 조치가 사용되는지 확인합니다. 사용하는 경우 로컬 인증을 시도합니다. 사용하지 않는 경우 일반 인증 오류를 반환합니다.
- 일반 인증 실패가 있는 경우 관리 사용자(UID = 1)이면 로컬 인증을 시도합니다. 관리 사용자가 아니면 일반 인증 오류를 반환합니다.

LDAP 인증

조직이 Microsoft Active Directory 또는 LDAP(Lightweight Directory Access Protocol)를 사용할 경우 그룹과 사용자를 모두 NA에 가져올 수 있습니다. NA는 LDAP 데이터베이스와의 활성 접속을 유지하여 응용 프로그램에 로그인할 수 있고 로그인할 수 없는 현재 사용자를 그대로 유지합니다.

외부 사용자 인증이 활성화되면 네트워크 문제로 인해 LDAP 서버에 연결할 수 없게 되더라도 NA에 로그인할 수 있습니다. NA가 지정된 LDAP 서버에 연결할 수 없는 경우 이전에 NA에 로그인한 사용자는 NA 사용자 암호를 사용하여 NA에 로그인할 수 있습니다. 내 프로필 페이지에서 NA 암호를 설정할 수 있습니다. 자세한 내용은 [339페이지의 "내 프로필 페이지 필드"](#)를 참조하십시오.

LDAP 사용자가 NA 시스템 관리자와 동일한 사용자 이름을 가지는 LDAP 사용자가 없음을 확인하십시오. 기본 시스템 관리자의 사용자 이름은 admin이지만, 변경될 수 있습니다. 기본 관리자와 다른 LDAP 사용자 간에 이름 충돌이 발생할 경우 기본 관리자는 NA에 로그인하지 못할 수 있습니다.

NA에 사용자가 생성되고 LDAP에서 삭제되면 해당 사용자는 (LDAP 암호가 아닌) NA 암호를 사용하여 NA에 다시 로그인할 수 있습니다.

LDAP에 대한 외부 인증 설정에 관한 자세한 내용은 [106페이지의 "LDAP 외부 인증 설정"](#)을 참조하십시오.

SecurID 인증

RSA SecurID 솔루션은 인증된 사용자에게만 네트워크 리소스에 대한 액세스를 부여하여 조직을 보호할 수 있도록 설계되었습니다. 일반적으로 SecurID는 두 개로 나뉜 인증 체계로, 암호/PIN과 함께 토큰이 필요합니다. 토큰은 60초마다 변경됩니다. 자세한 내용은 [793페이지의 "SecurID 소프트웨어 토큰 추가"](#)를 참조하십시오.

TACACS+ 인증

Cisco IOS 소프트웨어는 현재 TACACS+를 포함하여 TACACS(Terminal Access Controller Access Control System) 보안 프로토콜의 여러 버전을 지원합니다. TACACS+는 인증 및 허가 프로세스에 대한 상세한 계정 정보 및 유연한 관리 제어를 제공합니다.

TACACS+ 서버(일반적으로 CiscoSecure ACS)를 사용하여 사용자를 인증할 경우 다음과 같은 이점이 있습니다.

- 필요한 NA 사용자만 단일 사용자 이름과 암호를 기억합니다.
- NA 사용자 관리를 한 곳에서 관리할 수 있습니다.
- TACACS+ 암호 제한을 쉽게 적용할 수 있습니다.

TACACS+ 서버를 사용하여 NA에 사용자를 인증하면 다음 작업을 수행할 수 있습니다.

- TACACS+ 서버를 사용하여 사용자 로그인을 인증하도록(즉, 사용자가 유효한 사용자 이름/암호 쌍을 입력했음을 확인) NA를 구성합니다.
- 텔넷/SSH 프록시에 대한 TACACS+ 인증을 지원합니다.
- NA에서 개별 사용자에게 풀백 암호를 할당합니다.
- TACACS+ 서버에 액세스할 수 없을 때만 TACACS+ 사용자의 풀백 암호가 사용되도록 TACACS+ 사용자를 식별합니다(관리 사용자가 아닌 사용자가 잘못된 TACACS+ 암호를 입력한 경우에는 아님).
- 장애 조치 목적을 위한 여러 개의 TACACS+ 서버를 구성합니다.

NA는 TACACS+에서 다른 모든 라우터와 유사한 인증 장치로 특정 사용자 이름과 함께 정의되어야 합니다. 이렇게하면 사용자는 NA에 로그인하고 NA는 사용자의 네트워크 장치에 로그인할 수 있습니다.

참고: TACACS+는 인증/허가를 위해서는 사용되지 않습니다. 즉 TACACS+를 통해 사용자를 인증하려면 사용자를 직접 NA에 추가하고 사용자에게 적절한 권한을 할당해야 합니다. 사용자가 NA에서 TACACS+ 사용자로 식별되면 이 지정을 제거할 수 없습니다.

RADIUS 인증

RADIUS(Remote Authentication Dial-In User Service)를 사용할 경우

- 네트워크 액세스 서버가 RADIUS 클라이언트로 작동할 수 있습니다. RADIUS 클라이언트가 정보를 지정된 RADIUS 서버로 전달한 다음 반환된 응답에 대처할 수 있습니다.
- RADIUS 서버가 연결 요청을 수신하고, 사용자를 인증한 다음 적절한 연결을 위해 필요한 모든 클라이언트 구성 정보를 반환할 수 있습니다.
- RADIUS 서버가 다른 RADIUS 서버 또는 다른 서버의 인증 서버에 대한 프록시 클라이언트로 작동할 수 있습니다.

참고: RADIUS는 인증/허가를 위해 사용되지 않습니다. 이것은 RADIUS+를 통해 사용자를 인증하려면 사용자를 직접 NA에 추가하고 사용자에게 적절한 권한을 할당해야 함을 의미합니다. 사용자가 NA에서 RADIUS 사용자로 식별되면 이 지정을 제거할 수 없습니다.

TACAC+ 또는 RADIUS 인증을 사용하려면 관리 아래에 있는 메뉴 모음에서 관리 설정을 선택하고 사용자 인증 탭을 클릭합니다. 사용자 인증 페이지가 열립니다. 완료되면 저장을 클릭해야 합니다.

HP SA(HP Server Automation)

HP Server Automation 옵션을 사용하여 NA 시스템은 사용자 인증을 위해 HP SA 시스템을 사용할 수 있습니다. 따라서 HP SA 사용자는 HP SA 자격 증명을 사용하여 NA에 로그인할 수 있습니다. 또한 이 옵션을 사용하여 네트워크 다이어그램에 HP SA 서버를 표시하고 MAC 주소에서 HP SA 서버로 연결할 수 있습니다. 자세한 내용은 [254페이지의 "NA/SA 통합"](#)을 참조하십시오.

HP OO(HP Operations Orchestration)

IT 조직은 수행 중인 작업의 감사 추적 기능을 제공하지 않는 오래된 문제 해결 안내서를 사용하여 수동으로 문제 해결 작업을 수행하기도 합니다. IT 조직이 스크립트를 자동화 솔루션으로 배포할 때도 스크립트는 유지 보수하기 힘들고 감사 추적을 제공하지 않습니다.

HP OO 옵션을 사용하여 NA 웹 UI에서 직접 안내 모드로 HP OO 흐름을 시작할 수 있습니다. 무인 HP OO 흐름을 실행하려면 언어 흐름에 대한 명령 스크립트를 생성해야 합니다. 무인 흐름 실행에 대한 자세한 내용은 [713페이지의 "HP OO\(HP Operations Orchestration\) 흐름"](#)을 참조하십시오.

일반적으로 HP OO를 사용하여 NA 내 모든 루틴 선택, 문제 해결 및 유지 보수 작업을 중앙 집중화할 수 있습니다. 사용 가능한 HP OO 흐름을 정의한 후 다음을 수행할 수 있습니다.

- 자동 HP OO 흐름을 실행하여 하나 또는 여러 개의 장치 IP 주소가 지정된 타사 시스템에서 데이터를 수집하고 나타낼 수 있습니다. 자세한 내용은 [713페이지의 "HP OO\(HP Operations Orchestration\) 흐름"](#)을 참조하십시오.
- 사전 정의된 소프트웨어 업그레이드 관리 흐름을 실행할 수 있습니다. 이 HP OO 흐름은 모니터링 시스템에서 라우터를 제거하고 OSPF 메시에서 라우터를 제거하고 IOS 이미지를 업그레이드한 다음 장치를 OSPF 메시에 다시 삽입하고 모니터링 시스템에 다시 추가합니다. 프로세스 자동화 옵션에 대한 자세한 내용은 [304페이지의 "편집 메뉴 옵션"](#)을 참조하십시오.

HP OO에 대한 자세한 내용은 *HP Operation Orchestration Users Guide* 및 *HP Operation Orchestration Software Development Kit Guide*를 참조하십시오.

사용자 인증 페이지 필드

필드	설명/작업
사용자 암호 보안	
최소 사용자 암호 길이	암호가 포함해야 하는 최소 문자 수를 입력합니다. 이 문자 수보다 적은 수의 암호는 유효하지 않음으로 간주됩니다.
사용자 암호가 대문자와 소문자를 포함해야 함	이 옵션을 선택하면 사용자는 소문자와 대문자를 모두 포함하는 암호를 선택해야 합니다.
추가 사용자 암호 제한	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 추가 제한 없음(기본값) • 영문자가 아닌 숫자 또는 특수 문자를 하나 이상 포함해야 함 • 숫자 및 특수 문자를 각각 하나 이상 포함해야 함

필드	설명/작업
최대 연속 로그인 실패 수	최대로 허용된 연속 사용자 인증 실패 수를 입력합니다. 이 최대 수를 넘으면 사용자는 비활성화됩니다. 0(영) 값은 이 확인을 건너뛴을 나타냅니다. (참고: 이 설정은 기본 제공 사용자 인증에만 적용되고 외부 인증 방법에는 적용되지 않습니다.)
외부 인증 유형	
외부 인증 유형	<p>사용할 외부 인증 유형을 선택합니다. 다음과 같은 옵션이 있습니다.</p> <ul style="list-style-type: none"> • 없음(로컬 인증) • HP Server Automation • HP Server Automation & TACACS+ • TACACS+ • RADIUS • SecurID • LDAP <p>TACACS+ 또는 RADIUS를 선택할 경우 아래 섹션에서 구성할 수 있습니다. LDAP를 선택하면 LDAP 설정 링크를 클릭합니다. 자세한 내용은 106 페이지의 "LDAP 외부 인증 설정"을 참조하십시오. SecurID에는 추가 외부 인증 옵션이 없습니다.</p>
TACACS+/RADIUS 인증	
기본 TACACS+ 또는 RADIUS 서버	기본 TACACS+ 또는 RADIUS 서버의 호스트 이름 또는 IP 주소를 입력합니다.
보조 TACACS+ 또는 RADIUS 서버	보조 TACACS+ 또는 RADIUS 서버의 호스트 이름 또는 IP 주소를 입력합니다. 이 필드는 선택 사항입니다.
TACACS+ 또는 RADIUS 암호	TACACS+ 또는 RADIUS 서버에 구성된 NA 호스트의 공유 암호를 입력합니다. TACACS+ 또는 RADIUS 암호는 TACACS+ 또는 RADIUS 클라이언트(NA)가 TACACS+ 또는 RADIUS 서버와 통신을 암호화하는 데 사용하는 키(암호)입니다. 클라이언트와 서버는 서버가 통신을 암호 해독할 수 있도록 암호에 동의해야 합니다.

필드	설명/작업
TACACS+ 또는 RADIUS 인증 방법	NA와 TACACS+ 또는 RADIUS 서버 간 통신을 암호화하는 데 사용되는 다음 인증 방법 중 하나를 선택합니다. <ul style="list-style-type: none"> •PAP(Password Authentication Protocol) •CHAP(Challenge Handshake Authentication Protocol) •MSCHAP(Microsoft Challenge Handshake Authentication Protocol) •ARAP(TACACS+만) •ASCII(TACACS+만)
기본 NAS-ID 대신 RADIUS NAS-IP 사용	이 옵션을 사용하면 기본 NAS-ID 필드 대신 NA 코어 정보를 사용하여 RADIUS NAS-IP 필드를 보냅니다. 이것은 NA 코어에 대해 찾는 첫 번째 비루프백 IP 주소를 보냅니다. (참고: 이 설정의 NAS는 NA 제품에서 제공된 것이 아닙니다. 이것은 RADIUS 인증에 해당됩니다.)
고정 RADIUS NAS-IP 문자열	발견된 기본 IP 주소 대신 RADIUS NAS-IP 필드로 사용할 상수 문자열을 입력합니다. 이 옵션은 NA가 기본값을 사용하지 않고, NAS-IP 필드에 사용할 IP 주소를 NA에 알릴 때 사용할 수 있습니다. 이 옵션은 다중 네트워크 인터페이스 카드 시스템에 대해서만 필요하거나 필드를 서버에 바인딩되지 않은 IP 주소로 설정할 경우에만 필요합니다. (참고: 이 설정의 NAS는 NA 제품에서 제공된 것이 아닙니다. 이것은 RADIUS 인증에 해당됩니다.)

HP Server Automation 인증

Twist 서버	HP Twist 서버의 호스트 이름 또는 IP 주소를 입력합니다. 자세한 내용은 <i>HP Server Automation User's Guide</i> 를 참조하십시오.
Twist 포트 번호	HP Twist 서버에 연결할 Twist 포트 번호(일반적으로 1032)를 입력합니다. 자세한 내용은 <i>HP Server Automation User's Guide</i> 를 참조하십시오.
Twist 사용자 이름	Twist 웹 서비스 API(wsapi) 사용자 이름(일반적으로 <i>wsapiReadUser</i>)을 입력합니다.
Twist 암호	Twist 웹 서비스 API(wsapi) 암호를 입력합니다.

필드	설명/작업
OCC 서버	연결된 서버로 링크하기 위한 HP Command Center(OCC) 호스트 이름을 입력합니다. OCC 서버는 HP SA(HP Server Automation) 웹 UI 클라이언트입니다. NA는 HP SA에 대한 하이퍼링크를 생성할 수 있습니다. 따라서 NA 서버 페이지에서 HP SA 서버 페이지로 바로 이동할 수 있습니다. 자세한 내용은 292페이지의 "서버 페이지 필드" 를 참조하십시오.
기본 사용자 그룹	드롭다운 메뉴에서 HP SA 인증 사용자를 추가할 수 있는 사용자 그룹의 이름을 선택합니다. 이 그룹을 사용하여 HP SA 사용자에 대한 기본 권한을 설정할 수 있습니다. 자세한 내용은 254페이지의 "NA/SA 통합" 을 참조하십시오.
HP Operations Orchestration 인증	
HP OO 호스트 이름	HP OO 서버의 호스트 이름 또는 IP 주소를 입력합니다.
HP OO 포트	HP OO 서버에 연결할 HP OO 포트 번호를 입력합니다.
HP OO 서비스	HP OO 서비스에 대한 다음 연결 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •https:// •http:// <p>HP OO 서비스는 SSL 또는 일반 텍스트를 사용합니다.</p>
HP OO 사용자 이름	HP OO 사용자 이름을 입력합니다.
HP OO 암호	HP OO 암호를 입력합니다.
가이드 흐름 이름	오른쪽 상자에 가이드 흐름 이름을 입력하고 패턴 추가 <<를 클릭합니다. 흐름은 모든 장치군에 적용됩니다. 예를 들어, 가이드 흐름 이름 앞에 <i>Cisco IOS:flow 1</i> 을 붙이면 가이드 흐름이 Cisco IOS 장치군에 속하는 모든 장치에 적용됩니다. 왼쪽 상자에서 가이드 흐름 이름을 선택한 다음 패턴 삭제를 클릭하여 가이드 흐름 이름을 삭제할 수 있습니다. <p>흐름 구성에 대한 자세한 내용은 <i>HP Operations Orchestration User's Guide</i>를 참조하십시오. HP OO에 로그인하는 방법에 대한 자세한 내용은 304페이지의 "편집 메뉴 옵션"을 참조하십시오.</p>

LDAP 외부 인증 설정

LDAP 외부 인증을 활성화하려면

1. 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 사용자 인증을 클릭합니다. 관리 설정 - 사용자 인증 페이지가 열립니다.
2. 외부 인증 유형 필드로 이동합니다.
3. 외부 인증 유형 필드에서 LDAP를 선택하고 저장을 클릭합니다.
4. LDAP 설정 링크를 클릭합니다. LDAP 설정 마법사가 열립니다. 이전에 LDAP 인증을 설정한 경우 다음 정보가 표시됩니다.
 - LDAP 인증 상태
 - LDAP 서버 호스트
 - 포트 번호
 - 연결 사용자 이름
 - 연결 사용자 암호
 - 검색 기반
 - 보안 연결을 사용하는 경우
 - 서버 시간 초과

참고: NA는 사용자가 로그인할 때마다 필드가 동일한지 확인합니다. 필요할 경우 NA는 사용자 필드 정보를 LDAP의 해당 정보로 업데이트합니다. 예를 들어 NA 관리자가 NA의 사용자 A를 수동으로 업데이트하고 사용자 A의 전자 메일 주소를 변경하는 경우 다음 번에 사용자 A가 로그인할 때 NA에서 사용자 A의 전자 메일 주소를 LDAP에 있는 값으로 자동 변경합니다.

다음 표는 설정 프로세스를 안내합니다.

단계	작업
----	----

- | | |
|----------|--|
| 1 | <p>LDAP 설치 마법사 시작 페이지에서 다음을 클릭합니다. 다음 정보를 입력하고 다음을 클릭합니다.</p> <ul style="list-style-type: none"> • 서버 유형 — 서버 유형(Active Directory(기본값) 또는 일반 LDAP)을 선택합니다. • 서버 이름 — LDAP 또는 Active Directory 서버의 호스트 이름 즉, AD/도메인 컨트롤러의 호스트 이름 또는 IP 주소를 입력합니다. • 포트 — LDAP 요청 포트 번호를 입력합니다. 모든 Windows 2000 AD 도메인 컨트롤러는 포트 389에서 LDAP 요청을 수신합니다. 단일 도메인 구성에는 포트 389 또는 포트 636(SSL을 사용하는 경우)을 사용해야 합니다. 그러나 다중 도메인 AD 환경에서는 포트 3268 또는 포트 3269(SSL을 사용하는 경우)를 사용합니다. • 연결 유형 — 정기 연결(기본값) 또는 보안 연결(SSL)을 선택합니다. 디렉터리 서버에 연결할 때는 보안 연결을 선택해야 합니다. (참고: 이 옵션을 활성화하고 디렉터리 서버/도메인 컨트롤러 서버 인증서가 인증된 CA 중 하나에 의해 서명되지 않은 경우에는 NA가 실행 중인 서버로 인증서를 수동으로 가져와야 합니다.) LDAP SSL 구성에 대한 자세한 내용은 108페이지의 "LDAP SSL 구성"을 참조하십시오. • 서버 시간 초과 — LDAP 운영에 대해 시간 초과를 밀리초 단위로 입력합니다. LDAP 운영이 이 값보다 길게 소요되면 작동이 중단됩니다. |
| 2 | <p>다음 정보를 입력하고 다음을 클릭합니다.</p> <ul style="list-style-type: none"> • 연결 사용자 이름 — 연결 사용자 이름을 입력합니다. AD 서버에서 사용자 정보를 쿼리하려면 NA가 도메인 사용자 계정(DN)을 가지는 AD 서버로 바인드해야 합니다. DN은 Windows 2000 LDAP 형식이거나 Windows 2000 User Principal Name(UPN) 형식일 수 있습니다. Windows 2000 UPN 형식은 LDAP 트리에서 DN을 고유하게 식별하는 속기 표기법입니다. 사용자 계정과 각 도메인 모두 UPN에 포함되어 있습니다. Windows 2000 UPN DN의 예가 <i>jsmith@hp.com</i>입니다. • 연결 사용자 암호 — 연결 사용자 암호를 입력합니다. • 검색 기준 — 검색 기준을 입력합니다. 검색 기준은 LDAP 검색을 위한 LDAP 디렉터리의 시작점입니다. 검색 기준을 전체 AD의 루트 도메인으로 설정하는 것이 좋습니다. 이렇게 하면 NA가 전체 Windows 2000 AD를 쿼리할 수 있습니다. 검색 기준이 특정 OU 수준으로 설정되어 있는 경우에는 해당 특정 OU의 하위 객체만 쿼리할 수 있습니다. 이와 비슷한 경우로 검색 기준이 특정 도메인 수준으로 설정되어 있는 경우에는 해당 특정 도메인의 하위 객체만 쿼리할 수 있습니다. 이러한 이유로 인해 검색 기준은 가능한 한 일반적이어야 합니다. |

단계	작업
3	NA에 액세스할 수 있는 보안 그룹을 나타냅니다. 찾기 옵션을 사용하여 LDAP에서 사용자 그룹을 찾고 다음을 클릭할 수 있습니다.
4	사용자 이름과 암호를 입력하여 외부 인증 설정을 확인한 다음 로그인 테스트 버튼을 클릭할 수 있습니다. 설정 정보를 저장하려면 저장 버튼을 클릭해야 합니다. 오류가 없으면 다음 메시지가 표시되고 외부 인증 설정 요약 페이지가 업데이트됩니다. Successfully updated External Authentication settings.

LDAP SSL 구성

LDAP SSL 구성의 경우

1. Windows 2000 또는 Windows 2003 서버에 엔터프라이즈 인증 기관을 설치합니다. 모든 도메인 컨트롤러가 자동으로 등록되고 적절한 인증서를 설치합니다.
2. 그룹 정책 편집기를 사용하여 기본 도메인 컨트롤러 정책을 엽니다.
3. 컴퓨터 구성 아래 Windows 설정을 클릭합니다.
4. 보안 설정을 클릭한 다음 공용 키 정책을 클릭합니다.
5. 인증서 자동 요청 설정을 클릭합니다.
6. 마법사를 사용하여 도메인 컨트롤러에 대한 정책을 추가합니다.

자세한 내용은 Microsoft 기술 자료 Q247078을 참조하십시오.

인증서 가져오기:

1. 시작 → 프로그램 → 관리 도구 → 인증 기관을 클릭하여 인증 기관 관리 콘솔(일반적으로 LDAP 서버에 있음)을 시작합니다.
2. 인증 기관 로컬 아래에서 도메인 컨트롤러에 대한 인증서를 발행하는 인증서 기관(CA)을 찾습니다.
3. CA를 마우스 오른쪽 버튼으로 클릭하고 등록 정보를 선택합니다.
4. 일반 탭에서 인증서 보기를 클릭합니다.
5. 자세히 탭을 선택하고 파일에 복사를 선택합니다.
6. 마법사를 사용하여 인증서를 Base64 인코드 파일로 내보냅니다.

7. 이 파일을 NA 서버에 복사합니다.
8. Windows 명령 프롬프트에서 다음으로 이동합니다.
`<install directory>\jre\bin`
9. `keytool -import -file PATH_TO_THE_CERT_FILE -alias ADSCert -keystore ../../server/ext/jboss/server/default/conf/truecontrol.keystore`를 입력합니다.

키 저장소 암호는 "sentinel"입니다.

`PATH_TO_THE_CERT_FILE`을 7단계에서 생성한 파일의 절대 경로로 바꿉니다.

10. 서비스 애플릿 또는 Solaris나 Linux에서 `/etc/init.d/truecontrol` 스크립트를 사용하여 NA를 다시 시작합니다. UI에서 NA를 다시 시작하는 경우 키 저장소 변경이 로드되지 않습니다.

서버 모니터링

서버 모니터링을 사용하여 NA 서버의 전체 상태를 확인할 수 있습니다. 오류가 발견될 때 경고 알림 및 이벤트 로깅이 트리거됩니다. 모든 서버 모니터는 미리 패키징되어 NA와 함께 배송됩니다.

모니터가 오류를 수신할 경우 NA 모니터 오류 이벤트가 트리거되고 시스템 관리자에게 오류 알림을 보냅니다. 시스템은 나중에 해당 모니터를 확인할 때 모니터가 여전히 오류 상태에 있더라도 해당 모니터에 대한 모니터 오류 이벤트를 계속해서 보내지 않습니다. 모니터가 오류 상태에 있고 그 영향으로 이벤트가 트리거되고 나서 상태가 정상으로 변경될 때 시스템은 모니터 정상 이벤트만 보냅니다.

참고: 시스템을 다시 시작해도 오류 상태가 계속되면 새 모니터 오류 이벤트가 트리거됩니다. 데이터베이스에 액세스할 수 없는 경우 시스템은 관리자에게 이 사실을 전자 메일로 알립니다.

서버 모니터링 페이지에서 서버 모니터를 구성할 수 있습니다. 모든 서버 모니터 또는 특정 서버 모니터만 활성화하는 옵션을 사용할 수도 있습니다. 최근 모니터 실행 결과는 모니터 로그 파일에 저장되고 시스템 상태 페이지에서 볼 수 있습니다. 시스템 상태 페이지에 대한 내용은 [111페이지의 "서버 모니터링 페이지 필드"](#)를 참조하십시오.

참고: 관리자만 모니터링 작업 설정을 변경하는 권한을 가집니다. 모든 사용자는 모니터링 결과를 볼 수 있습니다.

서버 모니터링 페이지를 보려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 서버 모니터링을 클릭합니다. 서버 모니터링 페이지가 열립니다.

서버 모니터링 페이지 필드

필드	설명/작업
서버 모니터링	
서버 모니터링 사용	이 옵션을 선택하면(기본값) 서버 모니터링이 활성화됩니다. NA 오류가 생성되면 알람을 전자 메일로 보냅니다. 최근 결과는 모니터 로그 파일에 저장되고 시스템 상태 페이지에서 볼 수 있습니다. 확인되지 않은 경우 예정된 모니터 검사가 더 이상 실행되지 않습니다. 하지만 서버 모니터를 여전히 수동으로 실행할 수 있습니다.
모니터링을 시작하기 전 시작 시 지연 간격	시작 후 서버 모니터링 시작을 지연하는 시간(분)을 입력합니다. 기본값은 2분입니다.
모니터링 실행 간 지연 간격	모니터링 실행 간 지연 시간(분)을 입력합니다. 기본값은 360분입니다.
ConfigMonitor 사용	이 옵션을 선택하면 구성 모니터가 활성화됩니다. 이 모니터는 설치된 .rcx 파일 및 기타 구성 파일이 정상임을 확인합니다. 이 모니터는 초기 설치된 .rcx 파일의 백업을 만들고 설치된 .rcx 파일의 백업을 오류 없는 최신 버전으로 유지합니다.
DatabaseDataMonitor 사용	이 옵션을 선택하면 데이터베이스 데이터 모니터가 활성화됩니다. 이 모니터는 모든 중요 시스템 구성 요소가 데이터베이스에 있음을 확인합니다. 예를 들어 관리 사용자가 존재하는지, 암호 작성 키가 하나만 있는지, 일시 중지되었거나 보류 중인 인벤토리 스냅샷 작업이 하나 존재하는지 등을 확인합니다. 이 모니터는 암호 작성 키의 백업과 관리 전자 메일 주소(데이터베이스 서버가 중단된 경우 사용)를 만듭니다.
DatabaseMonitor 사용	이 옵션을 선택하면 데이터베이스 모니터가 활성화됩니다. 이 모니터는 데이터베이스 연결을 확인합니다. 예를 들어, 잘못된 자격 증명이 있는지 또는 연결이 너무 많은지를 확인합니다.
DiskMonitor 사용	이 옵션을 선택하면 디스크 모니터가 활성화됩니다. 이 모니터는 디스크 공간 부족 상태를 확인합니다.
DynamicDeviceGroup 모니터 사용	이 옵션을 선택하면 DynamicDeviceGroup 모니터가 활성화됩니다. 이 모니터는 동적 장치 그룹 수를 계산합니다.
FTPMonitor 사용	이 옵션을 선택하면 FTP 모니터가 활성화됩니다. 이 모니터는 타임스탬프와 함께 FTP 파일을 로컬 시스템으로 보낸 다음 파일 시스템을 확인하여 올바르게 작성되었음을 확인합니다.

필드	설명/작업
HTTPMonitor 사용	이 옵션을 선택하면 HTTP 모니터가 활성화됩니다. 이 모니터는 NA 웹 서버가 올바르게 실행 중임을 확인합니다.
LDAPMonitor 사용	이 옵션을 선택하면 LDAP 모니터가 활성화됩니다. 이 모니터는 LDAP 서버가 사용 가능한지 확인합니다.
LicenseMonitor 사용	이 옵션을 선택하면 LicenseMonitor가 활성화됩니다. 이 모니터는 사용 가능한 라이선스가 관리되는 장치의 백분율 이하로 떨어지거나 만료될 다음 라이선스가 지정된 일 수 이내에 있는지 확인합니다. 자세한 내용은 아래 "모니터 구성" 섹션을 참조하십시오.
LogMonitor 사용	이 옵션을 선택하면 LogMonitor가 활성화됩니다. LogMonitor는 로그 설정 관리를 담당합니다. 너무 긴 로그에 대해 로그 수준이 추적 또는 디버깅으로 유지되면 시스템 성능이 저하될 수 있습니다. LogMonitor는 이러한 낮은 수준으로 유지된 로그를 정기적으로 확인하여 오류로 재설정합니다.
MemoryMonitor 사용	이 옵션을 선택하면 메모리 모니터가 활성화됩니다. 이 모니터는 메모리 부족 상태를 확인합니다.
RMIMonitor 사용	이 옵션을 선택하면 RMI 모니터가 활성화됩니다. 이 모니터는 NA EJB에 대한 RMI 액세스가 작동 중임을 확인합니다. 이것은 일부 다른 EJB 컨테이너(Java 응용 프로그램 서버)에 RMI 포트가 없도록 합니다.
RunExternalTaskMonitor 사용	이 옵션을 선택하면 외부 작업 실행 모니터가 활성화됩니다. 이 모니터는 NA 서버가 외부 .bat 또는 .sh 파일을 실행할 수 있도록 합니다.
위성 모니터 사용	이 옵션을 선택하면 위성 모니터가 활성화됩니다. 이 모니터는 Syslog와 TFTP가 실행 중인지 여부와 위성이 NA 코어와 동일한 버전인지 확인합니다. NA 위성 구성에 대한 자세한 내용은 <i>Network Automation 9.10 Satellite Users Guide</i> 를 참조하십시오.
SMTPMonitor 사용	이 옵션을 선택하면 SMTP 모니터가 활성화됩니다. 이 모니터는 구성된 메일 서버에서 포트 23에 텔넷 연결을 설정하고, SMTP QUIT 명령을 보내고 적절한 221 응답 코드를 대기합니다.
SSHMonitor 사용	이 옵션을 선택하면 SSH 모니터는 활성화됩니다. 이 모니터는 NA에 내장된 SSH 서버에 대한 연결을 테스트합니다.

필드	설명/작업
SoftwareImageManagementMonitor 사용	이 옵션을 선택하면 SoftwareImageManagementMonitor가 활성화됩니다. SWIM이 활성화되면 이 모니터는 SWIM 서버와 통신할 수 있는지 확인합니다.
SyslogMonitor 사용	이 옵션을 선택하면 Syslog 모니터가 활성화됩니다. 이 모니터는 Syslog 메시지를 NA로 보내고 NA 관리 엔진이 이 메시지를 수신하도록 합니다.
TelnetMonitor 사용	이 옵션을 선택하면 텔넷 모니터가 활성화됩니다. 이 모니터는 NA에 내장된 텔넷 서버가 올바르게 실행 중임을 확인합니다.
TFTPMonitor 사용	이 옵션을 선택하면 TFTP 모니터가 활성화됩니다. 이 모니터는 타임스탬프와 함께 TFTP 파일을 로컬 시스템으로 보낸 다음 파일 시스템을 확인하여 올바르게 작성되었음을 확인합니다.
모니터 구성	
DatabaseDataMonitor에서 인벤토리 스냅샷 확인	이 옵션을 선택하면 데이터베이스 데이터 모니터의 인벤토리 스냅샷이 확인됩니다.
사용 가능 공간에 대한 경고 임계값	사용 가능한 디스크 공간 경고 메시지를 트리거할 임계값을 입력합니다. 기본값은 20MB입니다.
사용 가능 공간에 대한 오류 임계값	사용 가능 디스크 공간 오류 메시지를 트리거할 임계값을 입력합니다. 기본값은 10MB입니다.
디스크 공간을 모니터링할 드라이브	오른쪽 상자에 드라이브를 입력한 다음 드라이브 추가 <<를 클릭합니다. 드라이브를 삭제하려면 왼쪽 상자에서 드라이브를 선택하고 드라이브 삭제를 클릭합니다.
관리되는 장치 수에 대한 경고 임계값	총 라이선스의 백분율을 입력합니다. 사용 가능한 라이선스가 이 백분율 아래로 떨어지면 경고가 발생합니다. 장치 수 임계값은 10%로 기본 지정됩니다.
라이선스 만료에 대한 경고 임계값	기간(일)을 입력합니다. 지정된 기간(일) 내 다음 라이선스가 만료될 경우 경고가 발생합니다. 만료일 임계값의 기본값은 30일로 지정됩니다.
로그 모니터가 문제를 감지할 때 로그를 자동으로 ERROR로 재설정하고 작업 로그를 닫습니다.	이 옵션은 기본적으로 선택되어 있습니다. 이 옵션을 선택했을 때 로그 모니터가 로그가 너무 오랫동안 낮은 수준이나 설정되었음을 감지하면 자동으로 해당 로그 수준을 오류로 재설정합니다.

필드	설명/작업
TRACE 수준을 설정하기 위해 설정된 로그가 너무 오랫동안 열림 상태로 보고되지 않는 시간	기본값은 48시간입니다. 로그 모니터가 너무 오랫동안 너무 낮게 설정되었음을 감지하지 않고 로그가 TRACE 수준에 있을 수 있는 시간입니다.
DEBUG 수준을 설정하기 위해 설정된 로그가 너무 오랫동안 열림 상태로 보고되지 않는 시간	기본값은 48시간입니다. 로그 모니터가 너무 오랫동안 너무 낮게 설정되었음을 감지하지 않고 로그가 DEBUG 수준에 있을 수 있는 시간입니다.
활성 작업 로그가 너무 오랫동안 열림 상태로 보고되지 않는 시간	기본값은 6시간입니다. 활성 작업 로그가 너무 오랫동안 열림 상태로 보고되지 않는 시간입니다.
사용 가능 RAM에 대한 경고 임계값	사용 가능 RAM 경고 메시지를 트리거할 임계값을 입력합니다. 기본값은 20MB입니다.
사용 가능 RAM에 대한 오류 임계값	사용 가능 RAM 오류 메시지를 트리거할 임계값을 입력합니다. 기본값은 10MB입니다.
SSH 스레드 확인 지연 간격	SSH 스레드 확인 간격을 입력합니다. 기본값은 15000밀리초입니다.
TFTP 파일 확인 간격	TFTP 파일 확인 간격을 입력합니다. 기본값은 5000밀리초입니다.
FTP 파일 확인 간격	FTP 파일 확인 간격을 입력합니다. 기본값은 5000밀리초입니다.
표시할 Syslog 메시지별 지연 간격	Syslog 메시지를 표시할 간격을 입력합니다. 기본값은 45000밀리초입니다.

변경 사항을 저장하려면 저장을 클릭해야 합니다.

타사 통합

HP NNMi(Network Node Manager)는 NNMi와 NA 소프트웨어가 이미 실행 중인 시스템에서 다음과 같은 기능 및 장점을 제공합니다.

- 통합 알람
- HP NNMi에서 NA 구성 이력에 액세스
- 운영 효율성

NA-NNMi 통합에 대한 자세한 내용은 *HP NNMi 9.10 Deployment Reference*의 HP Network Automation 장을 참조하십시오.

타사 통합 페이지에는 NA에서 NNMi로의 통신 구성과 관련된 매개 변수가 포함되어 있습니다. NNMi-NA 통합 구성 양식에서 통합을 사용하면 필드가 설정됩니다.

타사 통합 페이지를 사용하면 NNMi 장치 재검색 트리거, 서비스 중지 트리거 및 SNMP 커뮤니티 문자열 전파에 대한 NNMi-NA 통합 동작을 변경할 수 있습니다.

타사 통합 페이지를 보려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 타사 통합을 클릭합니다. 타사 통합 페이지가 열립니다.

타사 통합 페이지 필드

필드	설명/작업
타사 통합	
타사 통합	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •사용함 •사용 안 함(기본값)
NNMi 통합	
NA 사용자	NA-NNMi 통합 사용자 이름을 입력합니다.
NA 파티션	NA-NNMi 통합 파티션 이름을 입력합니다. NA 파티션 생성에 대한 정보는 201페이지의 "파티션" 을 참조하십시오.

필드	설명/작업
NNMi호스트	NNMi 서버 호스트 이름 또는 IP 주소를 입력합니다.
NNMi HTTP 포트	NNMi HTTP 포트 번호를 입력합니다. 기본값은 포트 80입니다.
NNMi 사용자	NNMi 로그인 사용자 이름을 입력합니다.
NNMi 암호	NNMi 로그인 암호를 입력합니다.
작업 후 호스트 재검색	<p>목록에서 작업을 선택합니다. 선택한 작업으로 인해 작업이 성공적으로 실행된 경우 NNMi가 장치를 재검색합니다. 기본 작업은 다음과 같습니다.</p> <ul style="list-style-type: none"> •장치 소프트웨어 업데이트 •암호 배포 •장치 재부팅 •드라이버 검색
서비스 중지 이벤트	<p>목록에서 작업을 선택합니다. 작업이 시작되면 NA에서 NNMi 웹 서비스를 호출하여 장치를 "서비스 중지"로 지정합니다. 따라서 NNMi는 일시적으로 장치를 더 이상 관리하지 않습니다. 작업이 완료된 후 NA는 NNMi 웹 서비스를 호출하고 장치를 관리됨으로 지정합니다. 기본 작업은 다음과 같습니다.</p> <ul style="list-style-type: none"> •장치 소프트웨어 업데이트 •암호 배포 •장치 재부팅
장치 작업에 실패할 경우	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •서비스에서 장치 다시 설정(기본값) •서비스에서 장치 다시 설정 안 함
작업이 완료된 후 장치 준수 확인에 실패할 경우	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •서비스에서 장치 다시 설정(기본값) •서비스에서 장치 다시 설정 안 함
SNMP 커뮤니티 문자열 전파	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •사용함 •사용 안 함(기본값)

모니터링 결과 보기

시스템 상태 페이지는 최근 모니터 실행 결과를 표시합니다. 시스템 상태 페이지를 보려면 관리 아래의 메뉴 모음에서 시스템 상태를 클릭합니다. 시스템 상태 페이지가 열립니다.

시스템 상태 페이지 필드

필드	설명/작업
모두 실행 링크	나열된 모니터를 모두 실행합니다.
서버 모니터링 구성 링크	서버 모니터링 페이지를 엽니다. 자세한 내용은 111페이지의 "서버 모니터링 페이지 필드" 를 참조하십시오.
모니터 이름	모니터 이름을 표시합니다. 각 모니터는 모니터 중인 하위 시스템에 대한 다양한 메시지를 반환할 수 있습니다. 118페이지의 "모니터 메시지" 를 참조하십시오.
상태	다음에 포함된 모니터 상태를 표시합니다. <ul style="list-style-type: none"> • 정상 • 경고 • 오류 • 사용 안 함
마지막 확인	모니터를 마지막으로 실행한 날짜 및 시간을 표시합니다.
결과	결과에 대한 정보를 표시합니다.
작업	선택할 수 있는 옵션은 다음과 같습니다. <ul style="list-style-type: none"> • 지금 실행 — 모니터를 즉시 실행합니다. • 세부사항 보기 — 모니터에 대한 설명, 상태, 결과 및 추가 진단 정보를 포함하여 모니터에 대한 세부사항을 볼 수 있는 모니터 세부사항 페이지를 엽니다. • 서비스 시작/중지 — 서비스 시작/중지 페이지를 엽니다. 자세한 내용은 123페이지의 "서비스 시작 및 중지"를 참조하십시오.

모니터 메시지

각 모니터는 모니터 중인 하위 시스템에 대한 다양한 메시지를 반환할 수 있습니다. 이 섹션에서는 이러한 몇 가지 메시지와 가능한 수정 작업을 자세히 설명합니다.

모니터	설명/해결
BaseServerMonitor	<threadname>이 실행되고 있지 않음 — 적절한 NA 기능에 필요한 스레드가 알 수 없는 이유로 인해 실패했습니다. NA 관리 엔진을 다시 시작해야 할 수 있습니다.
ConfigMonitor	<ul style="list-style-type: none"> • <filename>.rcx 파일 누락 — NA의 필수 구성 파일 중 하나가 누락되었습니다. 지원 센터에 문의하십시오. • <filename>.rcx에서 필수 구성을 가져오는 중 오류 발생 — NA의 구성 파일 중 하나가 손상되었습니다. 지원 센터에 문의하십시오. • rcx 파일: <filename> 구문 분석 중 예외 발생 — NA의 구성 파일 중 하나가 손상되었습니다. 지원 센터에 문의하십시오.
MySQL의 DatabaseMonitor	<ul style="list-style-type: none"> • <servername>:3306의 MySQL 서버에 연결할 수 없음 — NA가 연결을 시도 중인 위치에서 실행 중인 MySQL 서버가 없습니다. MySQL 서비스를 다시 시작하거나 NA 연결 정보가 올바른지 확인할 수 있습니다. • 통신 링크 실패: java.io.IOException — MySQL 서버에 대한 연결이 끊어졌습니다. NA 관리 엔진을 다시 시작하거나 MySQL 서비스를 다시 시작해야 할 수 있습니다. • <database_name> 데이터베이스에 대한 <username> 사용자의 액세스 거부 — NA가 잘못된 데이터베이스에 연결을 시도 중이거나 기존 데이터베이스에 몇 가지 권한 문제가 있습니다. NA 연결 정보가 올바른지 확인합니다. • 잘못된 인증 사양: <username> 사용자의 액세스 거부(암호 사용: 예) — NA가 잘못된 사용자 이름 또는 암호를 사용하여 연결을 시도합니다. NA 데이터베이스 사용자 이름 및 암호를 올바른 값으로 재설정합니다. • 일반 오류: NA.RN_CRYPTO_KEY 테이블이 존재하지 않음 — NA는 지정된 자격 증명을 사용하여 데이터베이스에 연결할 수 있지만, 데이터베이스가 NA 데이터베이스가 아니거나 손상되었습니다(예:RN_CRYPTO_KEY 테이블 누락). NA 연결 정보가 올바른지 확인합니다.

모니터	설명/해결
Oracle의 DatabaseMonitor	<ul style="list-style-type: none"> • 소켓 설정 중 오류가 발생했습니다. 연결이 거부됨: 연결 — NA가 연결을 시도 중인 위치에서 실행 중인 Oracle 서버가 없습니다. Oracle 서비스를 다시 시작해야 하거나 NA 연결 정보가 올바른지 확인해야 할 수 있습니다. • 피어에 의한 연결 재설정: 소켓 쓰기 오류 — Oracle 서버에 대한 연결이 끊겼습니다. NA 관리 엔진을 다시 시작하거나 Oracle을 다시 시작해야 할 수 있습니다. • ORA-12505 연결이 거부되었습니다. 지정된 SID(<database_name>)가 Oracle 서버에 의해 인식되지 않았습니다. — NA가 잘못된 데이터베이스 이름에 연결을 시도 중입니다. NA 연결 정보가 올바른지 확인합니다. • ORA-01017: 사용자 이름/암호가 잘못되었습니다. 로그인이 거부되었습니다. — NA가 잘못된 사용자 이름 또는 암호를 사용하여 연결을 시도 중입니다. NA 데이터베이스 사용자 이름 및 암호를 올바른 값으로 재설정합니다. • ORA-00942: 테이블 또는 보기가 존재하지 않습니다. — NA가 지정된 자격 증명을 사용하여 데이터베이스에 연결하지만 데이터베이스가 NA 데이터베이스가 아니거나 손상되었습니다(예: RN_CRYPT0_KEY 테이블 누락). NA 연결 정보가 올바른지 확인합니다.
SQLServer의 DatabaseMonitor	<ul style="list-style-type: none"> • 소켓 설정 중 오류가 발생했습니다. — NA가 연결을 시도 중인 위치에서 실행 중인 SQLServer가 없습니다. SQLServer 서비스를 다시 시작하거나 NA 연결 정보가 올바른지 확인합니다. • 피어에 의한 연결 재설정: 소켓 쓰기 오류 — SQLServer에 대한 연결이 끊겼습니다. NA 관리 엔진을 다시 시작하거나 SQLServer를 다시 시작하십시오. • 로그인 <database_name>에서 요청된 데이터베이스를 열 수 없습니다. 로그인이 실패합니다. — NA가 잘못된 데이터베이스 이름에 연결을 시도하거나 기존 데이터베이스에 몇 가지 권한 문제가 있습니다. NA 연결 정보가 올바른지 확인합니다. • <username> 사용자에게 대한 로그인이 실패했습니다. — NA가 잘못된 사용자 이름 또는 암호를 사용하여 연결을 시도합니다. NA 데이터베이스 사용자 이름 및 암호를 올바른 값으로 재설정합니다. • 객체 이름 RN_CRYPT0_KEY가 잘못되었습니다. — NA가 지정된 자격 증명을 사용하여 데이터베이스에 연결하지만, 데이터베이스가 NA 데이터베이스가 아니거나 손상되었습니다(예: RN_CRYPT0_KEY 테이블 누락). NA 연결 정보가 올바른지 확인합니다.

모니터	설명/해결
DatabaseDataMonitor	<ul style="list-style-type: none"> • 관리 사용자를 찾을 수 없습니다. — NA에 구성된 관리 사용자가 없습니다. 지원 센터에 문의하십시오. • 여러 개의 암호 작성 키가 있습니다. — NA의 데이터베이스에 여러 개의 암호 작성 키가 있습니다. 지원 센터에 문의하십시오. • 현재 키가 저장된 키와 일치하지 않습니다. — NA는 현재 다른 암호 작성 키를 사용 중입니다. 지원 센터에 문의하십시오. • 암호 작성 키가 두 개 이상입니다. — NA는 현재 다른 암호 작성 키를 사용 중입니다. 지원 센터에 문의하십시오. • 인벤토리 그룹 스냅샷을 찾을 수 없습니다. — NA에 시스템의 모든 장치에서 구성을 수집하는 작업이 없습니다. 인벤토리 그룹에 대한 스냅샷 작업을 생성합니다. • 보고서 작업을 찾을 수 없습니다. — NA에 요약 보고서를 생성하는 작업이 없습니다. 요약 보고서 생성 작업을 생성합니다. • 정리 작업을 찾을 수 없습니다. — NA에 데이터베이스에서 오래된 데이터를 정리하는 작업이 없습니다. 데이터베이스 정리 작업을 생성합니다.
DiskMonitor	<p>디스크/파일 시스템 <filesystem>은 <space>바이트만 사용할 수 있습니다. 오류 임계값은 <limit>바이트입니다. — NA 서버가 디스크 드라이브 공간을 거의 다 채웠습니다. 디스크 드라이브에서 불필요한 파일을 삭제합니다.</p>
HTTPMonitor	<p>NA 로그인 페이지를 가져올 수 없습니다. — 응용 프로그램이 구성된 HTTP/HTTPS 포트에서 실행 중이지만, NA 웹 서버로 나타나지 않습니다. NA 서버에서 실행 중인 다른 모든 웹 서버(예: IIS)를 중지한 다음 NA 관리 엔진을 다시 시작합니다.</p>
LDAPMonitor	<ul style="list-style-type: none"> • ActiveDirectory가 사용 중이 아닙니다. — 이것은 NA 서버가 LDAP를 사용하도록 구성되지 않았음을 나타내는 정보용 메시지입니다. • LDAPMonitor에서 예외 발생: javax.naming.CommunicationException: <hostname>:389 — <hostname> 호스트가 없습니다. 외부 인증을 위한 서버 이름 설정을 수정합니다. • LDAPMonitor에서 예외 발생: javax.naming.CommunicationException: <hostname>:389 — <hostname> 호스트가 있지만 LDAP 포트(389)에서 연결을 승인하지 않습니다. 서버 이름 설정이 올바른지 확인합니다. 올바른 경우 LDAP 서버가 해당 호스트에서 실행 중인지 확인합니다. • LDAPMonitor에서 예외 발생: javax.naming.AuthenticationException — 외부 인증을 위한 연결 사용자 이름 또는 연결 사용자 암호 설정이 잘못되었습니다. 이러한 설정이 올바른지 확인합니다.

모니터	설명/해결
LicenseMonitor	<p>"라이선스 만료 임박" 또는 "장치 수가 사용 가능한 라이선스의 현재 임계값을 초과함"과 같은 경고가 결과 열에 표시됩니다. 경고가 표시되지 않으면 사용 가능한 장치 라이선스 수가 표시됩니다(예: "3454/3600개의 장치 라이선스 남음"). 세부사항 보기 링크를 클릭하여 사용된 라이선스와 사용 가능한 라이선스 및 라이선스 만료일과 같은 라이선스에 대한 세부사항을 확인합니다. (참고: 여러 개의 라이선스가 사용되는 경우 만료일은 다음으로 만료될 라이선스의 날짜입니다.)</p>
MemoryMonitor	<p><bytes>바이트 사용 가능. — 이것은 시스템에서 사용할 수 있는 메모리 양입니다. 오류 상태 발생 시 시스템이 적절하게 작동하는 데 필요한 메모리 양이 부족해집니다. 지원 센터에 문의하십시오.</p>
RMIMonitor	<p>RMI 포트 1099에 연결할 수 없습니다. — 다른 응용 프로그램이 NA에서 NA의 클라이언트 및 API가 적절하게 작동하려면 필요한 포트 1099를 사용하고 있습니다. 포트 1099를 사용 중인 응용 프로그램을 중지하고 NA 관리 엔진을 다시 시작합니다. 이 작업이 가능하지 않으면 지원 센터에 문의하십시오.</p>
RunExternalTask Monitor	<ul style="list-style-type: none"> • CreateProcess: <path>\tc_test.bat error=5 — NA에 테스트 스크립트 (및 가능한 다른 스크립트)에 액세스할 권한이 없습니다. NA의 디렉터리에 대한 파일 시스템 권한을 확인합니다. • CreateProcess: <path>\tc_test.bat error=2 — NA가 테스트 스크립트를 찾을 수 없습니다. 지원 센터에 문의하십시오. • Running <path>\tc_test.bat from directory <path> Got result code: 0 Got output: <text> — 테스트 스크립트가 손상되었습니다. 지원 센터에 문의하십시오.
SMTPMonitor	<ul style="list-style-type: none"> • SMTP 서버 이름이 공백입니다. — NA의 SMTP 서버 이름 관리 설정이 공백입니다. 메일 서버가 관리 설정 페이지에 설정되었는지 확인합니다. • <hostname> 25에 텔넷 연결을 열 수 없습니다. — NA가 <hostname>에 연결할 수 없거나 호스트가 SMTP 포트(25)에서 연결을 수신하지 않습니다. 올바른 메일 서버가 관리 설정 페이지에 설정되었는지 확인합니다. NA 서버가 해당 서버의 포트 25에 액세스할 수 있는지 확인합니다. • 예상 대기 시간 초과: 220 수신. — 응용 프로그램이 구성된 메일 서버의 포트 23에서 실행 중이지만 적절한 SMTP 코드로 응답하지 않으므로 SMTP 응용 프로그램으로 나타나지 않습니다. 올바른 메일 서버가 관리 설정 페이지에 설정되었는지 확인합니다.

모니터	설명/해결
SSHMonitor	SSH 서버에 연결하는 중 알 수 없는 문제가 발생했습니다. — NA SSH 서버가 올바르게 작동하지 않습니다. NA가 사용 중인 SSH 포트를 수신하는 다른 응용 프로그램이 없는지 확인하고 NA 관리 엔진을 다시 시작합니다.
SyslogMonitor	테스트 syslog 메시지가 처리되지 않았습니다. — NA에서 기본 제공된 Syslog 서버가 실행되고 있지 않거나 몇 가지 문제가 있습니다. 지원 센터에 문의하십시오.
TelnetMonitor	<ul style="list-style-type: none"> • <hostname> 23에 텔넷 연결을 열 수 없습니다. — NA 텔넷 서버가 올바르게 작동하지 않습니다. NA 관리 엔진을 다시 시작합니다. 이렇게 해서 문제가 해결되지 않으면 지원 센터에 문의하십시오. • 예상 대기 시간 초과: HP 로그인: 수신. — 응용 프로그램이 구성된 텔넷 포트에서 실행 중이지만 NA 텔넷 서버로 나타나지 않습니다. NA 텔넷 서버 수신 포트를 수정합니다.
FTPMonitor	<ul style="list-style-type: none"> • FTP 서버에 대한 연결 시간이 초과되었습니다. — FTP 서버가 실행되고 있지 않거나 연결을 승인하지 않습니다. FTP 서버를 다시 시작합니다. • 테스트 FTP 파일이 작성되었으나 읽을 수 없습니다. FTP 경로 설정을 확인합니다. — FTP 파일이 성공적으로 FTP 서버에 작성되었지만, 이후 파일 시스템에서 읽을 수 없습니다. FTP 경로 설정이 NA 관리 엔진에서 올바른지 확인합니다. • 검사점 파일을 찾았으나 타임스탬프가 최신 상태가 아닙니다. — 최근 파일 쓰기 시도가 실패했지만 시스템에 이전 검사점 시도가 있습니다. 이는 FTP 서버가 과거의 특정 지점에서는 작동했지만 지금은 작동하고 있지 않음을 의미합니다. FTP 서버를 다시 시작합니다.
TFTPMonitor	<ul style="list-style-type: none"> • TFTP 서버에 대한 연결 시간이 초과되었습니다. — TFTP 서버가 실행되고 있지 않거나 연결을 승인하지 않습니다. TFTP 서버를 다시 시작합니다. • 테스트 TFTP 파일이 작성되었으나 읽을 수 없습니다. TFTP 경로 설정을 확인합니다. — TFTP 파일이 성공적으로 TFTP 서버에 작성되었지만, 이후 파일 시스템에서 읽을 수 없습니다. TFTP 경로 설정이 NA 관리 엔진에서 올바른지 확인합니다. • 검사점 파일을 찾았으나 타임스탬프가 최신 상태가 아닙니다. — 최근 파일 쓰기 시도가 실패했지만 시스템에 이전 검사점 시도가 있습니다. 이는 TFTP 서버가 과거의 특정 지점에서는 작동했지만 지금은 작동하고 있지 않음을 의미합니다. TFTP 서버를 다시 시작합니다.

서비스 시작 및 중지

다음은 NA의 네 가지 기본 기능 장치입니다.

- NA 관리 엔진
- HP Live Network
- TFTP, FTP 및 Syslog 서버
- 소프트웨어 이미지 관리 서버

일반적으로 고객 지원 센터와 작업할 때는 서비스를 중지, 시작 또는 다시 시작할 수만 있습니다.

서비스를 시작/중지하거나 드라이버를 다시 로드하려면 관리 아래의 메뉴 모음에서 서비스 시작/중지를 클릭합니다. 서비스 시작/중지 페이지가 열립니다.

참고: 웹 사용자 인터페이스를 사용하여 NA 서비스를 시작 및 중지할 때 이전 페이지를 탐색하지 못할 수도 있습니다. 뒤로 버튼을 클릭하면 텍스트가 null인 페이지가 나타납니다. 이 경우 대신 브라우저의 뒤로 버튼을 클릭합니다.

서비스 시작/중지 페이지 필드

필드	설명/작업
관리 엔진	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 중지 — 관리 엔진(NA 서버라고도 함)을 중지합니다. 이 옵션은 NA 내 기본 서비스입니다. • 다시 시작 — 관리 엔진을 다시 시작합니다.
HP Live Network	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 드라이버 다시 로드 — 새 장치를 추가할 때 NA 드라이버를 사용할 수 있도록 NA 드라이버를 다시 로드할 수 있습니다. 다시 로드 버튼은 드라이버를 검색하지 않습니다. • 콘텐츠 다시 로드 — 콘텐츠는 제품 업그레이드가 필요 없이 HP에서 사용할 수 있는 NA의 향상 기능 및 확장 제품군입니다. 일부 콘텐츠 서비스는 등록해야 할 수 있습니다. 예를 들어, NA는 HP 보안 서비스를 통해 소프트웨어 수준 정책의 콘텐츠 가져오기를 지원합니다. HP 보안 서비스의 일부로 HP에서 소프트웨어 수준 정책을 다운로드하여 네트워크 무결성 관리를 지원할 수 있습니다. 자세한 내용은 540페이지의 "소프트웨어 수준 페이지 필드"를 참조하십시오.

필드	설명/작업
TFTP 서버	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 시작 — TFTP 서버를 시작합니다. NA는 주로 이 옵션을 사용하여 구성을 검색하고 배포합니다. (참고: TFTP는 최상의 성능을 제공합니다. TFTP를 사용할 수 없는 경우 NA는 텔넷 또는 SSH를 사용하여 구성을 처리합니다.) • 중지 — TFTP 서버를 중지합니다. • 다시 시작 — TFTP 서버를 다시 시작합니다.
FTP 서버	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 시작 — FTP 서버를 시작합니다. NA는 주로 이 옵션을 사용하여 구성을 검색하고 배포합니다. (참고: FTP를 사용할 수 없는 경우 NA는 TFTP, 텔넷 또는 SSH를 사용하여 구성을 처리합니다.) • 중지 — FTP 서버를 중지합니다. • 다시 시작 — FTP 서버를 다시 시작합니다.
Syslog 서버	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 시작 — Syslog 서버를 시작합니다. NA가 유일한 Syslog 서버일 수 있거나, 다른 Syslog 서버가 NA에 메시지를 전달할 수 있습니다. NA는 Syslog 메시지를 사용하여 실시간 변경 이벤트를 감지하고 사용자에게 돌려 보냅니다. • 중지 — Syslog 서버를 중지합니다. • 다시 시작 — Syslog 서버를 다시 시작합니다.
소프트웨어 이미지 관리 서버	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 시작 — 소프트웨어 이미지 관리 서버를 시작합니다. 소프트웨어 이미지 관리 서버는 Cisco.com에서 이용 가능한 소프트웨어 이미지를 기본 권장 사항과 함께 제공합니다. 장치 소프트웨어 이미지 권장 사항 페이지에 대한 자세한 내용은 293페이지의 "장치 소프트웨어 이미지 권장 사항 페이지 필드"를 참조하십시오. • 시작 — 소프트웨어 이미지 관리 서버를 중지합니다. • 다시 시작 — 소프트웨어 이미지 관리 서버를 다시 시작합니다.

로깅

로깅은 NA에서 기능을 수행할 때 수행되는 기능에 대한 정보를 얻는 방법입니다. 시스템 고장 시 로깅은 잘못된 점을 식별하는 기본 수단이며, 문제를 해결하는 방법입니다.

로그 수준

로그는 시스템에서 발생하는 이벤트를 기록하는 일련의 메시지 형식으로 제공됩니다. 기본적으로 이러한 메시지는 오류, 예상치 못한 상황 또는 잠재적인 불량 데이터의 경우와 같은 중요 이벤트만 기록합니다. 이것을 오류 로깅 수준이라고 합니다. 로깅 수준은 시스템 측면에 대해 기록되는 정보의 양을 나타내는 방법입니다. 수준이 낮을수록 기록되는 메시지는 많아집니다.

NA 로그 수준은 다음과 같습니다.

- 치명적 – 메시지는 치명적 오류가 발견된 경우에만 기록되며, 가장 높은 로깅 수준입니다.
- 오류 – 메시지는 주로 오류 경로를 표시하기 위해 기록되며, 기본 로깅 수준입니다.
- 디버그 – 메시지는 특정 오류가 발생한 이유를 식별하는 데 도움을 주기 위해 기록되며, 중간 로깅 수준입니다.
- 추적 – 메시지는 시스템의 일반 작동에 대해 기록되며, 가장 낮은 로깅 수준입니다.

참고: 많은 로그로 설정하면 시스템 성능이 크게 저하될 수 있습니다. 대부분의 경우 고객 지원 센터에서 지시할 때만 로깅 수준을 조정해야 합니다.

로그 이름

로그에 지정되는 이름을 통해 로그와 관련된 시스템의 부분에 대해 알 수 있습니다. 로그 이름은 계층적이므로 한 로그가 다양한 하위 로그를 포함할 수 있습니다. NA는 다음과 같은 상위 로그를 제공합니다.

- API – 표준 웹 인터페이스가 아닌 다른 방법을 통해 NA와의 인터랙션과 관련된 로깅입니다.
- 캐시 공급자 – 데이터베이스 캐싱 성능 향상 추적과 관련된 로깅입니다.
- DDK – DDK와 관련된 로깅입니다.
- 장치 – 주로 장치와의 인터랙션과 관련된 로깅입니다.
- 외부 – TFTP, FTP, Syslog 서버 및 타사 응용 프로그램에 대한 커넥터와 같은 외부 유틸리티와 관련된 로깅입니다.
- 기능 – 특정 NA 기능과 관련된 로깅입니다.
- FlexUI – Flex 사용자 인터페이스 구성 요소(예: 장치 선택기)에 대한 문제 추적과 관련된 로깅입니다.
- 시스템 – NA 시스템 및 서버의 내부 기능과 관련된 로깅입니다.
- 웹 UI – 웹 인터페이스를 통해 NA와의 인터랙션과 관련된 로깅입니다.

이러한 광범위한 각 범주 아래에는 많은 하위 로그가 있습니다. 예를 들어, 장치 로그 아래에 액세스, 세션 및 데이터 하위 로그가 있습니다. 이러한 하위 로그는 장치에 대한 액세스, 장치와의 인터랙션 및 검색된 데이터 각각에 중점을 두고 보다 전문화된 로깅을 포함합니다. 이러한 각 하위 로그에는 필요한 경우 더 전문화된 하위 로그가 있습니다.

하위 로그는 포함 로그 이름과 슬래시 다음에 하위 로그를 표시하여 나타냅니다. 예를 들면 다음과 같습니다.

- 장치
- 장치/세스
- 장치/액세스/인증 규칙
- 장치/세션
- 장치/세션/SSH
- 장치/세션/SNMP

로그 수준은 해당 로그에 대해 설정된 가장 낮은 수준과 같거나 포함 로그의 수준입니다. 따라서 장치/세션/SNMP 로그가 오류 수준으로 설정되었지만 장치/세션 로그가 디버그 수준으로 설정된 경우 장치/세션/SNMP 로그도 DEBUG 수준으로 설정된 것처럼 취급됩니다.

낮은 수준에서 많은 로그를 활성화하면 시스템 성능이 저하될 수 있으므로 광범위한 컨테이너 로그를 낮은 수준으로 설정할 경우 주의하십시오. 포함된 로그도 모두 자동으로 해당 수준으로 설정되기 때문입니다.

참고: 로그 이름을 통해 로그와 관련된 시스템의 부분에 대해 알 수 있더라도 로그 설정을 조작하기 전에는 항상 고객 지원 센터에 문의하십시오.

세션 로그

세션 로그는 작업 중 NA가 장치와 인터랙션하는 방식을 나타내는 데 사용되는 특수 유형의 로그입니다. 이것은 실제로 장치와 인터랙션하는 작업에만 사용될 수 있습니다. 이 로그의 출력은 자동으로 작업 결과에 삽입됩니다.

세션 로그는 각 장치별 작업 생성 페이지에 제공된 확인란을 통해 활성화됩니다. 대부분의 경우 작업을 다시 실행하면 작업을 처음 실행했을 때 세션 로그가 활성화되지 않았더라도 자동으로 세션 로그가 활성화됩니다. 작업 생성에 대한 자세한 내용은 [355페이지의 "7장: 작업 예약"](#)을 참조하십시오.

세션 로그는 연결 실패, 인증 실패 또는 스크립팅 오류와 같은 공통적인 장치 인터랙션 문제로 인해 발생하는 문제를 식별하는 데 도움을 줍니다. 또한 NA가 장치에서 특정 결과를 얻기 위해 하는 작업을 보여주고 실제로 그러한 작업이 올바른 것인지를 확인하기 위해서도 이 세션 로그를 사용할 수 있습니다.

세션 로그는 다음 사항에 대한 정보를 표시합니다.

- 작업 프로세스 단계(이 정보는 NA에 해당하는 정보로, 로그를 구성하는 데 유용하게 사용됨)
- 다양한 프로토콜을 통한 연결 시도
- 연결 해제 및 연결 실패
- 장치로 보낸 명령

- 장치에서 수신한 결과
- 장치에서 예상한 결과(있는 경우)

참고: 많은 오류는 예상된 특정 결과로 명령이 전송되기 때문에 발생합니다. 따라서 장치가 다른 결과로 응답할 때 작업이 실패합니다.

세션 로그를 검토할 때 NA는 가능한 모든 방법으로 작업을 완료하려고 합니다. 따라서 작업이 성공적으로 완료될 경우에도 세션 로그에는 실패로 표시될 수 있습니다. 예를 들어, 세션 로그에 TFTP 업로드 시도 실패가 표시되더라도 구성 스냅샷은 성공할 수 있습니다. 이렇게 실패한 시도가 장치에 대한 TFTP 연결에 문제가 있음을 나타낼 수 있지만, 실패로 인해 NA는 다른 방법으로 구성을 얻으려고 합니다. 이러한 다른 방법이 성공할 경우 작업은 TFTP 실패에도 불구하고 성공합니다.

작업 로그

작업 로그는 하나의 특정 작업과 관련된 시스템 활동을 추적하는 데 생성된 일반 목적의 로그입니다. 작업 로깅은 (반복 일정이 아닌) 한 번 실행된 작업으로 제한됩니다. 뿐만 아니라 작업이 장치와 관련된 경우 단일 장치를 기준으로 실행할 때만 작업 로그를 사용할 수 있습니다. NA의 모든 작업 유형이 작업 로그를 지원하지는 않습니다. 예를 들어, 작업 로그는 작업에 대한 새 이벤트 알림 및 응답 규칙을 생성할 때 사용할 수 없습니다.

참고: 모든 NA 사용자가 작업별 로그를 만들 수 있지만, 관리 권한을 가진 사용자만 이러한 로그를 보고 다운로드할 수 있습니다. 로그를 보고 다운로드할 수 있는 적절한 사용 권한이 없으면 NA 시스템 관리자에게 문의하거나 필요할 경우 로그 정보를 제공하도록 지원 센터에 요청하십시오.

작업에 작업 로깅을 사용할 수 있는 경우 작업 로깅 섹션이 작업 생성 페이지에 제공됩니다. 생성 중인 작업이 작업 로깅에 적절하지 않은 경우(장치 그룹 또는 반복 일정을 기준으로 실행되므로) 작업 로깅 인터페이스는 응답하지 않습니다.

작업에 대한 작업 로깅을 활성화하는 작업은 확인란을 선택하고 하나 이상의 로그 이름을 선택하는 작업으로 이루어집니다. 사용 가능한 모든 로그 이름 목록이 제공됩니다. 이 목록은 생성 중인 작업에 적절한 기본 로그 세트의 항목을 포함할 수 있습니다. 기본 세트를 포함하거나 제외하여, 원하는 만큼 로그를 선택할 수 있습니다. 목록에서 선택된 로그 이름은 자동으로 작업 로그에 대해 TRACE 수준으로 설정됩니다.

작업을 실행할 때 해당 작업에 특정한 로그가 파일로 생성되고 NA 서버 로그와 함께 저장됩니다. 어떤 이유로 해서 작업 로그 파일을 생성할 수 없는 경우 작업은 즉시 오류 메시지가 표시되면서 실패합니다. 작업 로그에 대한 정보는 작업 결과 페이지에 제공되지 않습니다.

서버 로그

서버 로그는 전체 NA 시스템에 대한 로그로, 한 위치의 모든 작업과 기타 모든 프로세스 활동을 기록하는 메시지를 포함합니다. 서버 로그는 문제 해결 페이지에서 활성화됩니다. 자세한 내용은 [130페이지의 "문제 해결 페이지 필드"](#)를 참조하십시오.

참고: 서버 로그는 고객 지원부의 지시에 따라야 합니다.

로그 관리

다양한 유형의 로그를 활성화하고 비활성화할 뿐만 아니라 NA는 로그 파일의 보유 기간을 관리하고 성능 관리 기술을 제공하여 오랜 시간 이후 로그 수준을 재설정합니다. 로그 파일 보유 기간 관리에 대한 자세한 내용은 [68페이지의 "서버 페이지 필드"](#)를 참조하십시오. NA에서 로그 수준을 자동으로 재설정하는 방법 및 설정을 수정하는 방법 등 성능 관리 기술에 대해서는 [110페이지의 "서버 모니터링"](#)을 참조하십시오.

문제 해결 페이지 필드

문제 해결 페이지를 보려면 관리 아래의 메뉴 모음에서 문제 해결을 클릭합니다. 문제 해결 페이지가 열립니다.

필드	설명/작업
문제 해결 정보 보내기 링크	전자 메일을 작성하고 시스템 정보 및 로그를 고객 지원 센터로 보낼 수 있는 문제 해결 정보 보내기 페이지를 엽니다. 자세한 내용은 35페이지의 "문제 해결 보내기 페이지 필드" 를 참조하십시오.
문제 해결 정보 다운로드 링크	문제 해결 정보를 다운로드할 수 있습니다. 자세한 내용은 35페이지의 "문제 해결 보내기 페이지 필드" 를 참조하십시오.
관리 사용자에게 테스트 전자 메일 보내기 링크	시스템 관리자에게 전자 메일을 보냅니다. 이 옵션은 NA의 전자 메일 시스템이 올바르게 구성되도록 확인하고 전자 메일(특히 문제 해결 전자 메일)을 가져올 수 없는 문제를 해결할 경우 사용됩니다.
로그 활성화 대상	로그를 활성화할 하나 이상의 구성 요소를 선택합니다. 로그에 대한 자세한 내용은 125페이지의 "로그" 을 참조하십시오.
추가 대상	목록에 없는 추가 소프트웨어 구성요소를 입력합니다.
수준 < > 이상	로그 수준을 선택합니다. 옵션은 다음과 같습니다. <ul style="list-style-type: none"> • 치명적(가장 적은 메시지) • 오류(기본값) • 디버그 • 추적(가장 많은 메시지) 자세한 내용은 125페이지의 "로그 수준" 을 참조하십시오.
로그 보존 기간 < >일	로그 데이터를 보존할 기간을 입력합니다. 기본값은 2일입니다. (참고: 로그 데이터는 디스크 공간을 많이 차지할 수 있습니다.)
재설정	이 옵션을 선택하면 제출 버튼을 클릭할 때 모든 로그가 기본 로그 수준(오류)으로 재설정됩니다.

드라이버 검토

드라이버 페이지는 시스템에 설치된 드라이버 목록과 현재 사용 중인 드라이버 수를 표시합니다. 드라이버 페이지에서 HP에서 기본적으로 제공하거나 보증한 NA 드라이버를 판별할 수 있으므로 결과는 HP에서 지원됩니다.

드라이버 페이지를 보려면 관리 아래의 메뉴 모음에서 드라이버를 클릭합니다. 드라이버 페이지가 열립니다.

드라이버 페이지 필드

필드	설명/작업
드라이버 다시 로드 링크	NA에 대한 드라이버를 추가, 제거 또는 업데이트했을 때 드라이버를 다시 로드할 수 있습니다.
설명	드라이버 이름을 표시합니다.
내부 이름	드라이버 식별에 사용된 고유 드라이버 이름을 표시합니다. 이것은 지원 센터에서 사용합니다.
패키지 이름	드라이버 패키지 이름을 표시합니다.
버전	드라이버 버전을 표시합니다.
빌드 번호	현재 NA 빌드 번호를 표시합니다.
작성자	드라이버를 작성한 사람의 이름을 표시합니다. 지정되지 않은 경우에는 드라이버가 HP에서 기본적으로 제공되었음을 암시합니다.
인증됨	드라이버가 인증된 경우 표시합니다. 인증된 드라이버는 HP에서 생성한 NA 드라이버이거나 타사에서 생성하고 HP에서 보증한 NA 드라이버입니다.
사용 중	드라이버가 현재 사용 중인 경우 표시합니다.

3장: 장치 및 장치 그룹 추가

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	135페이지의 "시작하기"
장치 추가	137페이지의 "장치 추가"
장치 편집	146페이지의 "장치 편집 페이지 필드"
Bare Metal 프로비전	153페이지의 "Bare Metal 프로비전"
새 장치 템플릿 추가	161페이지의 "새 장치 템플릿 추가"
장치 추가 마법사 사용	165페이지의 "새 장치 마법사 사용"
장치 가져오기	167페이지의 "장치 가져오기"
장치 암호 규칙 생성	170페이지의 "장치 암호 규칙 생성"
장치 그룹 추가	175페이지의 "장치 그룹 추가"
동적 그룹	180페이지의 "동적 장치 그룹"
장치 선택기	183페이지의 "장치 선택기"
장치 그룹 보기	186페이지의 "장치 그룹 보기"
장치 및 사용자 세분화	191페이지의 "장치 및 사용자 세분화"
HP 게이트웨이 설정	195페이지의 "HP 게이트웨이 설정"
장치 그룹 편집	207페이지의 "장치 그룹 편집"
장치 배치 편집	209페이지의 "장치 일괄 편집"
장치 드라이버 검색	212페이지의 "장치 드라이버 검색"
텔넷/SSH 세션 나열	215페이지의 "텔넷/SSH 세션 나열"
배스천 호스트 사용	218페이지의 "배스천 호스트 사용"

장치 추가로 이동

HP Network Automation		로그아웃			
장치	작업	정책	보고서	관리	도움말
<ul style="list-style-type: none"> 인벤토리 그룹 새로 만들기 <ul style="list-style-type: none"> 장치 장치 템플릿 장치 그룹 상위 그룹 새 장치 마법사 	<ul style="list-style-type: none"> 구성 변경 장치 도구 <ul style="list-style-type: none"> 명령 스크립트 구성 템플릿 장치 암호 규칙 장치 템플릿 진단 정책 소프트웨어 이미지 장치 작업 <ul style="list-style-type: none"> 정책 준수 확인 Syslog 구성 암호 배포 드라이버 검색 장치 재부팅 ICMP 테스트 실행 명령 스크립트 실행 진단 실행 스냅샷 작성 시작 및 실행 동기화 장치 소프트웨어 업데이트 가져오기 <ul style="list-style-type: none"> 네트워크 장치 감지 중복 방지 OS 분석 템플릿에서 장치 프로비전 ACL 삭제 <ul style="list-style-type: none"> ACL 라인 일괄 삽입 ACL 라인 일괄 삭제 	<ul style="list-style-type: none"> 사용자 사용자 그룹 새 사용자 새 사용자 그룹 로그온한 사용자 	<ul style="list-style-type: none"> 사용자 역할 및 권한 보안 파티션 <ul style="list-style-type: none"> 게이트웨이 장치 암호 규칙 이벤트 알림 및 응답 규칙 사용자 지정 데이터 설정 LDAP 설정 워크플로 설정 관리 설정 작업 로드 <ul style="list-style-type: none"> 시스템 상태 서비스 시작 / 중지 문제 해결 드라이버 시스템 작업 		

시작하기

장치를 추가하면 HP NA(Network Automaton)에서는 다음 작업이 수행됩니다.

1. 올바른 장치 드라이버를 자동으로 검색 및 할당하여 장치와의 통신을 활성화합니다. 이 프로세스를 드라이버 검색이라고 합니다.
2. 장치 스냅샷을 작성하여 시스템 정보 및 초기 구성을 수집합니다.
3. "NA 인터페이스" 및 "NA 라우팅 테이블"과 같은 핵심 진단 집합을 실행합니다. 전체 진단 목록은 [261페이지의 "메뉴 옵션 보기"](#)를 참조하십시오.

장치를 성공적으로 검색하고 스냅샷을 작성하기 위해 NA에서는 장치에 완전히 액세스할 수 있어야 하며 장치에 대한 SNMP 읽기 액세스 권한도 필요할 수 있습니다.

콘솔 서버는 현재 IP 네트워크에 연결할 수 없는 장치에 액세스할 수 있도록 하는 데 사용되며, 하드웨어 장애가 있는 장치, 보호된 네트워크에 있는 장치 또는 IP 프로토콜 (IPX, ATM 등)을 실행하지 않는 장치 등과 같이 장치의 콘솔 포트 상의 직렬 연결을 통해서만 연결할 수 있습니다.

Cisco AS5xxx와 같이 SSH 인증을 사용하는 표준 콘솔 서버를 사용하려는 경우 적절한 포트 번호로 콘솔 서버 루프백에 대해 Telnet을 실행하여 콘솔 서버에서 대상 장치에 연결할 수 있습니다. 이를 위해 다음을 수행해야 합니다.

- SSH 연결 방법을 사용하도록 원하는 장치를 구성합니다.
- 배스천 호스트 액세스를 사용하도록 원하는 장치를 구성합니다. 배스천 호스트로서의 콘솔 서버에 대한 주소 및 자격 증명을 제공해야 합니다.
- 장치별 자격 증명을 사용하도록 장치를 설정합니다(이 경우 각 장치는 다른 대상 포트를 가짐).
- 영향 받은 각 장치에서 해당 액세스 변수를 구성합니다. 이러한 변수는 다음을 포함할 수 있습니다.
 - hop_prompt = >(Cisco 콘솔 서버 프롬프트)
 - hop_target_connect_protocol = telnet(Telnet을 사용하여 콘솔 서버에서 대상 장치로 연결)
 - hop_telnet_cmd_host = <루프백 IP>(콘솔 서버에 있는 루프백의 IP 주소)
 - hop_telnet_cmd_port = <장치 포트>(콘솔 서버에 있는 대상 장치의 포트 번호)

참고: 단순 인증을 사용하는 텔넷 콘솔 서버(대상 장치가 포트로 지정)는 액세스 변수 console_xxx 집합을 사용하여 지원할 수 있습니다. 보다 복잡한 텔넷 콘솔 서버 구성은 사용자 지정된 배스천 호스트 액세스를 사용해야 할 수 있습니다.

배스천 호스트는 대부분의 다른 호스트가 액세스할 수 없는 보호된 네트워크 섹션에 액세스하기 위한 승격된 권한을 갖는 호스트입니다. 이를 통해 관리 시스템은 배스천 호스트가 권한을 갖는 보호된 네트워크의 요소를 관리할 때 배스천 호스트를 "홉"으로 사용할 수 있습니다. 일반적으로 배스천 호스트는 인터넷 및 DMZ 라우터/스위치, 엑스트라넷 파트너, 보안 및/또는 사설 네트워크에 사용됩니다.

이러한 두 가지 경우에서 NA는 텔넷, SSH, FTP/TFTP 및 SNMP와 같은 다른 액세스 방법을 사용할 수 없을 때 콘솔 서버 및 배스천 호스트를 장치 액세스 수단으로 사용하여 (일반적으로 CLI 사용) 일반적인 관리 기능을 수행합니다.

참고: 모든 액세스 방법이 활성화되면 NA는 SSH, 텔넷, SNMP 및 콘솔을 순서대로 사용하여 장치에 액세스합니다. 또한 NA에서는 화면 스크래핑(예: SSH+SCP, SSH+TFTP, SSH+화면 스크래핑, 텔넷+SCP, 텔넷+TFTP, 텔넷+화면 스크래핑, SNMP+TFTP 및 콘솔+화면 스크래핑) 전에 파일 전송을 수행합니다.

장치 그룹 명명 규칙

정책과 연관된 시스템 생성 장치 그룹을 참조할 때 장치 그룹 명명 규칙이 업데이트되었습니다. 예를 들어 이전 릴리스에서 DynamicCfgPolicyxxxx(여기서 xxxx는 정책을 적용할 장치 그룹을 생성하는 데 사용되는 장치 그룹의 이름)으로 명명된 장치 그룹이 이제는 Config Policy Group - CONFIGPOLICYNAME - TIMESTAMP로 명명되었습니다(여기서 CONFIGPOLICYNAME은 장치 그룹이 생성된 구성 정책의 이름이며 TIMESTAMP는 장치 그룹이 생성된 시간).

장치 추가

새 장치를 추가하려면 장치 아래의 메뉴 모음에서 새로 만들기를 선택하고 장치를 클릭합니다. 새 장치 페이지가 열립니다. 완료되면 저장 버튼이나 저장 및 다른 항목 추가 버튼을 클릭할 수 있습니다.

참고: 네트워크 장치 감지 작업을 사용하면 NA에서 관리하려는 장치를 네트워크에서 찾을 수 있습니다. IP 주소 범위를 제공하면 NA에서는 네트워크를 검색하여 장치를 찾습니다. 자세한 내용은 [426페이지의 "네트워크 장치 감지 작업 페이지 필드"](#)를 참조하십시오.

새 장치 페이지 필드

필드	설명/작업
마법사 사용 링크	장치 추가 마법사를 엽니다. (참고: 장치가 없으면 장치 추가 마법사가 자동으로 열립니다.) 새 장치 마법사 사용에 대한 자세한 내용은 165페이지의 "새 장치 마법사 사용" 을 참조하십시오.
IP 주소(또는 DNS 이름)	장치의 IP 주소 또는 DNS 호스트 이름을 입력합니다.
호스트 이름	적용 가능한 경우 장치의 호스트 이름을 입력합니다.
사이트 <이름>	<p>드롭다운 메뉴에서 파티션을 선택합니다. 이 필드는 하나 이상의 보안 파티션을 구성한 경우에만 표시됩니다.) 또한 필드 이름을 파티션 페이지에서 수정할 수 있습니다. (자세한 내용은 202페이지의 "파티션 페이지 필드"를 참조하십시오.)</p> <p>일반적으로 보안 파티션이란 고유한 IP 주소를 갖는 장치의 그룹입니다. 단일 NA 코어로 여러 보안 파티션을 관리할 수 있습니다. 설치된 NA 서버의 NA 코어는 단일 관리 엔진, 연관된 서비스 및 단일 데이터베이스로 구성되어 있습니다.</p> <p>참고: 장치/장치 그룹에 보안 파티션이 적용되면 각 보안 파티션에 대해 추가 드롭다운 메뉴가 제공될 수 있습니다. (보안 파티션에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화"를 참조하십시오.)</p>
그룹에 속함	장치가 구성원으로 속하는 그룹이 표시됩니다. 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기를 사용하는 방법에 대한 자세한 내용은 183페이지의 "장치 선택기" 를 참조하십시오.
변경 감지 및 폴링	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 사용함 — 이 옵션을 선택하면(기본값) NA에서는 정규 폴링 작업의 일부로 장치의 변경을 폴링하거나 변경 이벤트를 감지할 때 폴링합니다. • 폴링만 — 이 옵션을 선택하면 NA는 정규 폴링 작업의 일부로만 장치의 변경을 폴링합니다. • 사용 안 함 — 이 옵션을 선택하면 NA에서는 장치와 관련된 변경 이벤트를 무시합니다. 또한 NA에서는 장치의 변경을 정규 폴링 작업의 일부로 확인하지 않습니다. 일상적인 유지 관리 중에 이 장치를 정규 폴링 작업에서 제외하려면 이 옵션을 선택하는 것이 좋습니다.

필드	설명/작업
관리 상태	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 활성 — 이 옵션을 선택하면(기본값) NA에서는 장치에 대한 변경을 기록합니다. • 사전 프로덕션 — 이 옵션을 선택하면 장치가 사전 프로덕션 장치로 지정됩니다. 사전 프로덕션 장치는 프로덕션 네트워크에서 아직 활성화되지 않은 장치입니다. 사전 프로덕션 장치는 포함되도록 명시적으로 선택하지 않는 한 검색에 포함되지 않으며 네트워크 상태의 보고서에 포함되지 않습니다. (참고: Bare metal 장치는 사전 프로덕션 상태를 사용해야 합니다.) • 비활성 — 이 옵션을 선택하면 NA에서는 장치에 대한 변경을 기록하지 않습니다. 이 옵션은 장치가 지원되지 않거나 활성 상태가 아닌 경우에 선택하는 것이 좋습니다. 장치를 비활성 상태로 만들면 네트워크 트래픽이 줄어들고 리소스를 사용할 수 있게 됩니다.
장치 드라이버	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 드라이버 자동 검색 — 이 옵션을 선택하면(기본값) NA는 SNMP 또는 텔넷을 사용하여 장치를 쿼리하고 가장 적합한 장치 드라이버를 할당합니다. (참고: 기존 장치를 편집하는 경우 이 옵션이 드라이버 재검색으로 바뀝니다.) • 드라이버 지정 — 이 옵션을 선택하면 현재 장치에 할당된 드라이버가 표시되거나 드롭다운 메뉴의 사용 가능한 드라이버 목록 중에서 선택할 수 있습니다.
주석	장치에 대한 주석을 입력합니다.
암호 정보	
네트워크 전체 암호 규칙 사용	<p>이 옵션을 선택하면(기본값) NA에서는 장치에 적용되는 네트워크 전체 장치 암호 규칙을 사용합니다. 네트워크 전체 암호 규칙을 사용하는 것은 확장성이 뛰어난 장치 자격 증명 설정 방법입니다.</p> <p>참고: 장치 그룹이 동일한 자격 증명을 공유하는 대규모 네트워크의 경우 장치 암호 규칙을 사용하십시오. 이렇게 하면 장치 자격 증명을 한 장소에 통합하여 쉽게 관리할 수 있습니다. 장치 암호 규칙 생성에 대한 자세한 내용은 170페이지의 "장치 암호 규칙 생성"을 참조하십시오.</p>
이 암호 규칙을 먼저 사용	이 옵션을 선택하면 NA에서는 드롭다운 메뉴에서 선택한 암호 규칙을 먼저 사용합니다.

필드	설명/작업
장치별 암호 정보 사용	<p>이 옵션을 선택하면 NA에서는 장치에 고유하게 적용되는 인증 자격 증명을 사용합니다. 장치별 암호 규칙을 구현하려면 다음 정보를 입력하십시오.</p> <ul style="list-style-type: none"> • 사용자 이름 — 필요한 경우 장치 액세스에 사용되는 사용자 이름을 입력합니다. 장치가 AAA 솔루션(예: TACACS+ 또는 RADIUS)을 사용하도록 구성된 경우 AAA 사용자 계정을 생성하고 해당 AAA 자격 증명을 장치 자격 증명으로 사용하십시오. • 암호 — NA에서 장치 액세스에 사용하는 암호를 입력합니다. • 암호 확인 — 확인을 위해 암호를 다시 입력합니다. • 활성화 암호 — NA에서 권한이 부여된 모드에 액세스하는 데 필요한 활성화 암호를 입력합니다. 대부분의 구성 변경 작업에는 활성화 암호가 필요합니다. (참고: Nortel ASN/ARN과 같은 일부 장치에는 권한이 부여된 모드에 액세스하기 위해 암호가 필요하지 않을 수 있습니다. 또한 일부 장치는 권한이 부여된 모드에 대한 암호를 비활성화하도록 구성될 수 있습니다. 네트워크 관리자에게 사이트별 구성을 확인하십시오.) • 활성화 암호 확인 — 활성화 암호를 다시 입력합니다. • SNMP 읽기 전용 커뮤니티 문자열 — NA에서 SNMP 값을 읽는 데 사용하는 SNMP 암호를 입력합니다. • SNMP 읽기/쓰기 커뮤니티 문자열 — NA에서 SNMP 값을 읽고 쓰는 데 사용하는 SNMP 암호를 입력합니다. • SNMPv3 사용자 이름 — 장치 액세스에 사용되는 SNMPv3 사용자 이름을 입력합니다. • SNMPv3 인증 암호 — NA에서 장치 액세스에 사용하는 SNMPv3 인증 암호를 입력합니다. • SNMPv3 인증 암호 확인 — 확인을 위해 SNMPv3 인증 암호를 다시 입력합니다. • SNMPv3 암호화 암호 — SNMPv3 암호화 암호를 입력합니다. • SNMPv3 암호화 암호 확인 — 확인을 위해 SNMPv3 암호화 암호를 다시 입력합니다.

필드	설명/작업
장치 액세스 설정	
장치 액세스 설정	<p>NA는 대부분의 네트워크 및 네트워크 장치에서 작동하도록 고안되었습니다. 그러나 고유한 장치 구성이 특정 장치를 관리하는 NA의 기능에 영향을 줄 수 있습니다. 장치 액세스 설정을 사용하여 네트워크 구성에 맞게 NA를 조정할 수 있습니다. 장치 액세스 설정은 장치 암호 정보와 연결되어 있습니다. 입력한 장치별 설정은 장치별 암호를 사용하도록 선택한 경우에만 적용됩니다. 네트워크 전체 장치 설정을 암호 규칙에 추가할 수 있습니다. TACACS+ 인증에 대한 자세한 내용은 99페이지의 "TACACS+ 인증"을 참조하십시오. SecurID 사용에 대한 자세한 내용은 794페이지의 "SecurID를 통한 로그인"을 참조하십시오.</p> <p>참고: 장치 액세스 설정 사용 방법에 대한 자세한 내용을 보려면 "장치 액세스 설정 사용 방법" 링크를 클릭하십시오. 액세스 변수 도움말 파일은 새 브라우저 창에서 열립니다.</p>
NAT 정보	
NAT IP 주소	<p>장치의 내부적으로 구성된 IP 주소가 NA에서 장치 액세스에 사용하는 기본 IP 주소와 다른 경우 이 주소를 입력합니다. (참고: NAT를 사용하는 경우 페이지 맨 위의 장치 IP 상자에 NA가 장치 액세스에 사용할 IP 주소를 입력해야 합니다.)</p>
TFTP 서버 IP 주소	<p>장치에 로컬인 NA 서버의 NAT IP 주소를 입력합니다.</p>
FTP 서버 IP 주소	<p>장치에 로컬인 NA 서버의 NAT IP 주소를 입력합니다.</p>

필드	설명/작업
연결 정보	
연결 방법	<p>NA는 다음 프로토콜 조합을 사용하여 네트워크 장치와 통신할 수 있습니다. 사용하려는 하나 이상의 프로토콜을 선택합니다. NA는 사용자가 선택한 프로토콜 중에서 언제든지 가장 효율적인 프로토콜을 선택합니다.</p> <ul style="list-style-type: none"> •SNMP •SNMPv1 또는 SNMPv2c(커뮤니티 문자열 인증) •SNMPv3(사용자 인증) — SNMPv3을 사용하는 경우 noAuthNoPriv(사용자 이름만), authNoPriv(사용자 이름, 인증 암호), authPriv(사용자 이름, 인증 및 암호화 암호) 옵션이 제공됩니다. 인증 방법에는 SHA(Secure Hash Algorithm) 및 MD5(Message Digest Algorithm)가 포함되며, 암호화 방법에는 DES(Data Encryption Standard), AES(Advanced Encryption Standard), AES192 및 AES256이 포함됩니다. •RLogin •텔넷 •SSH(SSH1 또는 SSH2(기본값), SSH1만 또는 SSH2만 중에서 선택할 수 있음) •콘솔 서버(텔넷 통합) 확인란 — NA에서는 표준 네트워크 연결 외에 콘솔 서버를 통해 장치에 연결할 수 있습니다. 또한 표준 연결이 실패하면 텔넷/SSH 프록시는 사용자를 장치에 연결할 때 자동으로 콘솔 설정으로 장애 조치됩니다. 이 옵션을 선택한 경우 포트 번호와 함께 콘솔 서버의 IP 주소 또는 호스트 이름을 입력하십시오. •콘솔 서버만 사용 확인란 — 기본적으로 하나 이상의 연결 방법을 선택해야 합니다. 텔넷이 기본값으로 사용됩니다. 이 옵션을 선택하면 위의 연결 방법 중 하나를 선택할 수 없습니다.
전송 프로토콜	<p>다음 전송 프로토콜 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none"> •SCP •SFTP •FTP •TFTP

필드	설명/작업
배스천 호스트	<p>"텔넷 및 SSH 액세스의 경우 Unix 또는 Linux 배스천 호스트 사용" 확인란을 선택한 경우 다음을 입력합니다.</p> <ul style="list-style-type: none"> • 배스천 호스트의 IP 주소 또는 호스트 이름 • 배스천 호스트에 액세스하는 데 사용되는 사용자 이름(일반적으로 root) • 배스천 호스트에 액세스하는 데 사용되는 암호 • 확인을 위해 암호 다시 입력 <p>(참고: 배스천 호스트 정보를 수정하려면 307페이지의 "장치에서 관리되는 IP 주소 페이지 필드"로 이동하십시오.)</p>

Syslog 구성

구성 변경 감지를 위한 장치에 Syslog 구성

이 옵션을 선택하고(기본값) 드라이버 검색을 수행하거나 각 장치에 드라이버를 할당한 경우 NA에서는 장치별로 다음 단계를 수행합니다.

1. 구성의 스냅샷을 작성합니다.
2. 구성을 업데이트하여 Syslog 메시지를 NA로 보냅니다.
3. 장치가 변경 감지를 활성화하도록 자동 구성되었음을 나타내는 주석을 구성에 작성합니다.
4. 최종 스냅샷을 작성합니다.

다음 옵션 중 하나를 선택할 수 있습니다.

- NA Syslog 서버에 기록할 장치 설정 — 구성 변경 감지를 위한 장치에 Syslog 구성 확인란을 선택한 경우 기본적으로 선택됩니다.
- 장치가 Syslog 릴레이에 로그되므로 올바른 로깅 수준 설정 — 릴레이 호스트의 호스트 이름 또는 IP 주소를 입력합니다. 이전에 릴레이 호스트가 입력된 경우 기본적으로 여기에 나타납니다.

ACL 구문 분석

다음 옵션 중 하나를 선택합니다.

- 사용함 — 이 옵션을 선택하면(기본값) 각 스냅샷 시 장치에 대한 ACL 데이터가 저장됩니다. 스냅샷이 작성될 때까지 ACL은 로드되지 않습니다.
- 사용 안 함 — 이 옵션을 선택하면 각 스냅샷 시 장치에 대한 ACL 데이터가 저장되지 않습니다.

필드	설명/작업
추가 정보	<p>NA에서는 장치 스냅샷 프로세스의 다음 필드 일부를 자동으로 채웁니다. 이러한 필드를 수동으로 채울 경우 장치가 폴링될 때마다 데이터가 덮어쓰여집니다.</p>
장치 설명	장치 식별에 사용할 설명을 입력합니다.
모델	장치의 제조업체 모델 번호를 입력합니다.
FQDN	장치가 속한 도메인을 입력합니다. 이 도메인은 FQDN 확인 관리 옵션이 선택되어 있으면 감지됩니다.
일련 번호	장치의 제조업체 일련 번호를 입력합니다.
공급업체	장치 공급업체(예: Cisco 또는 Nortel)를 입력합니다.
자산 태그	장치의 회사 자산 태그 번호를 입력합니다.
위치	네트워크에서의 장치의 물리적 또는 논리적 위치를 입력합니다.
계층 레이어	<p>계층 레이어는 장치 속성입니다. 장치를 추가하거나 편집할 때 장치의 계층 레이어를 설정할 수 있습니다. 따라서 네트워크 다이어그램을 구성할 때 필터링할 계층 레이어를 선택할 수 있습니다. 예를 들어 전체 네트워크(인벤토리)를 다이어그램으로 작성하도록 선택한 후 계층 레이어가 코어로 설정된 코어 장치만 가져오도록 "코어"에 대해 필터링을 적용할 수 있습니다. 네트워크 다이어그램 작성에 대한 자세한 내용은 758페이지의 "다이어그램 작성"을 참조하십시오.</p> <p>참고: 아래에 제공된 옵션은 기본 계층 레이어입니다. 사용자 지정 계층 레이어에 대한 자세한 내용은 768페이지의 "appserver.rcx 파일 편집"을 참조하십시오.</p> <p>드롭다운 메뉴에서 계층 레이어를 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> •레이어가 설정되지 않음 •코어 •배포 •액세스 •가장자리

필드	설명/작업
사용자 지정 서비스 유형	서비스 유형을 입력합니다. 서비스 유형에서는 VoIP, BGP, MPLS 등을 지정할 수 있습니다. 이 값을 사용하여 장치의 용도를 식별할 수 있습니다. 이러한 값으로 장치 서비스에 태그를 지정하면 그룹(정적 또는 동적)에서 해당 서비스를 쉽게 검색하거나 볼 수 있습니다.

장치 편집 페이지 필드

필드	설명/작업
IP 주소(또는 DNS 이름)	장치 IP 주소 또는 DNS 호스트 이름을 표시합니다.
호스트 이름	해당되는 경우 장치 호스트 이름을 표시합니다.
사이트 <이름>	<p>사이트 이름을 표시합니다. 파티션 페이지에서 필드 이름을 수정할 수 있습니다. (자세한 내용은 202페이지의 "파티션 페이지 필드"를 참조하십시오.) 일반적으로 보안 파티션이란 고유한 IP 주소를 갖는 장치의 그룹입니다. 단일 NA 코어로 여러 보안 파티션을 관리할 수 있습니다. 설치된 NA 서버의 NA 코어는 단일 관리 엔진, 연관된 서비스 및 단일 데이터베이스로 구성되어 있습니다.</p> <p>참고: 장치/장치 그룹에 보안 파티션이 적용되면 각 보안 파티션에 대해 추가 드롭다운 메뉴가 제공될 수 있습니다. (보안 파티션에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화"를 참조하십시오.)</p>
그룹에 속함	장치가 구성원으로 속하는 그룹이 표시됩니다. 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기를 사용하는 방법에 대한 자세한 내용은 183페이지의 "장치 선택기" 를 참조하십시오.
변경 감지 및 폴링	<p>옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 사용함 — 이 옵션을 선택하면(기본값) NA에서는 정규 폴링 작업의 일부로 장치의 변경을 폴링하거나 변경 이벤트를 감지할 때 폴링합니다. • 폴링만 — 이 옵션을 선택하면 NA는 정규 폴링 작업의 일부로만 장치의 변경을 폴링합니다. • 사용 안 함 — 이 옵션을 선택하면 NA에서는 장치와 관련된 변경 이벤트를 무시합니다. 또한 NA에서는 장치의 변경을 정규 폴링 작업의 일부로 확인하지 않습니다. 일상적인 유지 관리 중에 이 장치를 정규 폴링 작업에서 제외하려면 이 옵션을 선택하는 것이 좋습니다.

필드	설명/작업
관리 상태	<p>옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 활성 — 이 옵션을 선택하면(기본값) NA에서는 장치에 대한 변경을 기록합니다. • 사전 프로덕션 — 이 옵션을 선택하면 장치가 사전 프로덕션 장치로 지정됩니다. 사전 프로덕션 장치는 프로덕션 네트워크에서 아직 활성화되지 않은 장치입니다. 사전 프로덕션 장치는 포함되도록 명시적으로 선택하지 않는 한 검색에 포함되지 않으며 네트워크 상태의 보고서에 포함되지 않습니다. (참고: Bare metal 장치는 사전 프로덕션 상태를 사용해야 합니다.) • 비활성 — 이 옵션을 선택하면 NA에서는 장치에 대한 변경을 기록하지 않습니다. 이 옵션은 장치가 지원되지 않거나 활성 상태가 아닌 경우에 선택하는 것이 좋습니다. 장치를 비활성 상태로 만들면 네트워크 트래픽이 줄어들고 리소스를 사용할 수 있게 됩니다.
장치 드라이버	<p>옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 드라이버 재검색 — 이 옵션을 선택하면(기본값) NA는 SNMP 또는 텔넷을 사용하여 장치를 쿼리하고 가장 적합한 장치 드라이버를 할당합니다. • 드라이버 지정 — 이 옵션을 선택하면 현재 장치에 할당된 드라이버가 표시되거나 드롭다운 메뉴의 사용 가능한 드라이버 목록 중에서 선택할 수 있습니다.
주석	장치에 대한 주석을 표시합니다.
암호 정보	
네트워크 전체 암호 규칙 사용	<p>이 옵션을 선택하면(기본값) NA에서는 장치에 적용되는 네트워크 전체 장치 암호 규칙을 사용합니다. 네트워크 전체 암호 규칙을 사용하는 것은 확장성이 뛰어난 장치 자격 증명 설정 방법입니다.</p> <p>참고: 장치 그룹이 동일한 자격 증명을 공유하는 대규모 네트워크의 경우 장치 암호 규칙을 사용하십시오. 이렇게 하면 장치 자격 증명을 한 장소에 통합하여 쉽게 관리할 수 있습니다. 장치 암호 규칙 생성에 대한 자세한 내용은 170페이지의 "장치 암호 규칙 생성"을 참조하십시오.</p>
이 암호 규칙을 먼저 사용	이 옵션을 선택하면 NA에서는 드롭다운 메뉴에서 선택한 암호 규칙을 먼저 사용합니다.

필드	설명/작업
장치별 암호 정보 사용	<p>이 옵션을 선택하면 NA에서는 장치에 고유하게 적용되는 인증 자격 증명을 사용합니다. 장치별 암호 규칙을 구현하려면 다음 정보를 입력하십시오.</p> <ul style="list-style-type: none"> • 사용자 이름 — 필요한 경우 장치 액세스에 사용되는 사용자 이름을 입력합니다. 장치가 AAA 솔루션(예: TACACS+ 또는 RADIUS)을 사용하도록 구성된 경우 AAA 사용자 계정을 생성하고 해당 AAA 자격 증명을 장치 자격 증명으로 사용하십시오. • 암호 — NA에서 장치 액세스에 사용하는 암호를 입력합니다. • 암호 확인 — 확인을 위해 암호를 다시 입력합니다. • 활성화 암호 — NA에서 권한이 부여된 모드에 액세스하는 데 필요한 활성화 암호를 입력합니다. 대부분의 구성 변경 작업에는 활성화 암호가 필요합니다. (참고: Nortel ASN/ARN과 같은 일부 장치에는 권한이 부여된 모드에 액세스하기 위해 암호가 필요하지 않을 수 있습니다. 또한 일부 장치는 권한이 부여된 모드에 대한 암호를 비활성화하도록 구성될 수 있습니다. 네트워크 관리자에게 사이트별 구성을 확인하십시오.) • 활성화 암호 확인 — 활성화 암호를 다시 입력합니다. • SNMP 읽기 전용 커뮤니티 문자열 — NA에서 SNMP 값을 읽는 데 사용하는 SNMP 암호를 입력합니다. • SNMP 읽기/쓰기 커뮤니티 문자열 — NA에서 SNMP 값을 읽고 쓰는 데 사용하는 SNMP 암호를 입력합니다. • SNMPv3 사용자 이름 — 장치 액세스에 사용되는 SNMPv3 사용자 이름을 입력합니다. • SNMPv3 인증 암호 — NA에서 장치 액세스에 사용하는 SNMPv3 인증 암호를 입력합니다. • SNMPv3 인증 암호 확인 — 확인을 위해 SNMPv3 인증 암호를 다시 입력합니다. • SNMPv3 암호화 암호 — SNMPv3 암호화 암호를 입력합니다. • SNMPv3 암호화 암호 확인 — 확인을 위해 SNMPv3 암호화 암호를 다시 입력합니다.
마지막으로 사용한 암호 규칙 재설정	선택한 경우 NA가 마지막으로 사용한 암호 규칙을 재설정합니다.

필드	설명/작업
장치 액세스 설정	
장치 액세스 설정	<p>NA는 대부분의 네트워크 및 네트워크 장치에서 작동하도록 고안되었습니다. 그러나 고유한 장치 구성이 특정 장치를 관리하는 NA의 기능에 영향을 줄 수 있습니다. 장치 액세스 설정을 사용하여 네트워크 구성에 맞게 NA를 조정할 수 있습니다. 장치 액세스 설정은 장치 암호 정보와 연결되어 있습니다. 입력한 장치별 설정은 장치별 암호를 사용하도록 선택한 경우에만 적용됩니다. 네트워크 전체 장치 설정을 암호 규칙에 추가할 수 있습니다. TACACS+ 인증에 대한 자세한 내용은 99페이지의 "TACACS+ 인증"을 참조하십시오. SecurID 사용에 대한 자세한 내용은 794페이지의 "SecurID를 통한 로그인"을 참조하십시오.</p> <p>참고: 장치 액세스 설정 사용 방법에 대한 자세한 내용을 보려면 "장치 액세스 설정 사용 방법" 링크를 클릭하십시오. 액세스 변수 도움말 파일은 새 브라우저 창에서 열립니다.</p>
NAT 정보	
NAT IP 주소	<p>장치의 내부적으로 구성된 IP 주소가 NA에서 장치 액세스에 사용하는 기본 IP 주소와 다른 경우 이 주소를 표시합니다. (참고: NAT를 사용하는 경우 페이지 맨 위의 장치 IP 상자에 NA가 장치 액세스에 사용할 IP 주소를 입력해야 합니다.)</p>
TFTP 서버 IP 주소	<p>장치에 로컬인 NA 서버의 NAT IP 주소를 표시합니다.</p>

필드	설명/작업
연결 정보	
연결 방법	<p>NA는 다음 프로토콜 조합을 사용하여 네트워크 장치와 통신할 수 있습니다. 사용 중인 하나 이상의 프로토콜을 표시합니다. NA는 사용자가 선택한 프로토콜 중에서 언제든지 가장 효율적인 프로토콜을 선택합니다.</p> <ul style="list-style-type: none"> •SNMP •SNMPv1 또는 SNMPv2c(커뮤니티 문자열 인증) •SNMPv3(사용자 인증) — SNMPv3을 사용하는 경우 noAuthNoPriv(사용자 이름만), authNoPriv(사용자 이름, 인증 암호), authPriv(사용자 이름, 인증 및 암호화 암호) 옵션이 제공됩니다. 인증 방법에는 SHA(Secure Hash Algorithm) 및 MD5(Message Digest Algorithm)가 포함되며, 암호화 방법에는 DES(Data Encryption Standard), AES(Advanced Encryption Standard), AES192 및 AES256이 포함됩니다. •RLogin •텔넷 •SSH(SSH1 또는 SSH2(기본값), SSH1만 또는 SSH2만 중에서 선택할 수 있음) •콘솔 서버(텔넷 통합) 확인란 — NA에서는 표준 네트워크 연결 외에 콘솔 서버를 통해 장치에 연결할 수 있습니다. 또한 표준 연결이 실패하면 텔넷/SSH 프록시는 사용자를 장치에 연결할 때 자동으로 콘솔 설정으로 장애 조치됩니다. 이 옵션을 선택한 경우 포트 번호와 함께 콘솔 서버의 IP 주소 또는 호스트 이름을 입력하십시오. 기존 장치를 편집할 때 콘솔 서버 정보를 수정하려면 307페이지의 "장치에서 관리되는 IP 주소 페이지 필드"로 이동하십시오. <p>참고: Cisco ASA 하위 장치와의 연결이 상위 장치를 통과할 수 있습니다. 하지만 Cisco ASA 하위 장치의 텔넷 및 SSH 연결 방법이 상위 장치의 연결 방법과 일치하지 않을 경우 하위 장치의 연결 방법 설정이 상위 장치의 연결 방법 설정을 오버라이드하지 않으므로 일부 통신이 실패할 수 있습니다.</p>
전송 프로토콜	<p>전송 프로토콜은 다음과 같습니다.</p> <ul style="list-style-type: none"> •SCP •SFTP •FTP •TFTP

필드	설명/작업
----	-------

배스천 호스트 배스천 호스트 정보를 수정하려면 307페이지의 "장치에서 관리되는 IP 주소 페이지 필드"로 이동하십시오.

ACL 구문 분석

옵션은 다음과 같습니다.

- 사용함 — 이 옵션을 선택하면(기본값) 각 스냅샷 시 장치에 대한 ACL 데이터가 저장됩니다. 스냅샷이 작성될 때까지 ACL은 로드되지 않습니다.
- 사용 안 함 — 이 옵션을 선택하면 각 스냅샷 시 장치에 대한 ACL 데이터가 저장되지 않습니다.

추가 정보

NA에서는 장치 스냅샷 프로세스의 다음 필드 일부를 자동으로 채웁니다. 이러한 필드를 수동으로 채울 경우 장치가 폴링될 때마다 데이터가 덮어쓰여집니다.

장치 설명	장치에 대한 설명을 표시합니다.
모델	장치의 제조업체 모델 번호를 표시합니다.
FQDN	장치가 속하는 FQDN(정규화된 도메인 이름)을 입력합니다. 이 도메인은 FQDN 확인 관리 옵션이 선택되어 있으면 감지됩니다.
일련 번호	장치의 제조업체 일련 번호를 표시합니다.
공급업체	장치 공급업체(예: Cisco 또는 Nortel)를 표시합니다.
자산 태그	장치의 회사 자산 태그 번호를 표시합니다.
위치	네트워크에서의 장치의 물리적 또는 논리적 위치를 표시합니다.

필드	설명/작업
계층 레이어	<p>계층 레이어는 장치 속성입니다. 장치를 추가하거나 편집할 때 장치의 계층 레이어를 설정할 수 있습니다. 따라서 네트워크 다이어그램을 구성할 때 필터링할 계층 레이어를 선택할 수 있습니다. 예를 들어 전체 네트워크(인벤토리)를 다이어그램으로 작성하도록 선택한 후 계층 레이어가 코어로 설정된 코어 장치만 가져오도록 "코어"에 대해 필터링을 적용할 수 있습니다. 네트워크 다이어그램 작성에 대한 자세한 내용은 758페이지의 "다이어그램 작성"을 참조하십시오.</p> <p>참고: 아래에 제공된 옵션은 기본 계층 레이어입니다. 사용자 지정 계층 레이어에 대한 자세한 내용은 768페이지의 "appserver.rcx 파일 편집"을 참조하십시오.</p> <p>드롭다운 메뉴에서 계층 레이어를 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 레이어가 설정되지 않음 • 코어 • 배포 • 액세스 • 가장자리
사용자 지정 서비스 유형	<p>서비스 유형에서는 VoIP, BGP, MPLS 등을 지정할 수 있습니다. 이 값을 사용하여 장치의 용도를 식별할 수 있습니다. 이러한 값으로 장치 서비스에 태그를 지정하면 그룹(정적 또는 동적)에서 해당 서비스를 쉽게 검색하거나 볼 수 있습니다.</p>

Bare Metal 프로비전

Bare Metal 프로비전은 장치를 기본 제공 상태에서 가져와 프로덕션 네트워크에서 작동할 수 있는 상태로 설정하는 프로세스입니다. Bare metal 장치는 NA와 제대로 인터랙션할 수 있는 위치로 아직 설정되지 않았습니다. bare metal 장치에 가장 일반적인 시나리오는 대화식 CLI 세션처럼 표준 NA 인터랙션에 적절히 응답할 위치로 장치를 구성하는 초기화 절차가 아직 수행되지 않은 경우입니다.

참고: Bare metal 장치는 처음으로 부팅되어 몇 가지 형태의 "부트스트랩" OS를 실행하기도 하는 장치입니다. NA는 bare metal 드라이버를 사용할 때 매우 제한된 방식으로만 장치와 인터랙션할 수 있습니다.

일반적으로 bare metal 프로비전 프로세스는 다음과 같습니다.

- **준비** — 준비 중에 장치는 시스템으로 보내져 구성, 펌웨어, OS 등을 승인할 수 있는 위치로 설정됩니다. 이러한 장치는 네트워크에 임시 위치를 지정할 수 있지만 네트워크 내에서 원하는 위치와 일치하는 IP 정보로 설정되지 않습니다. 준비 단계의 목표는 NA에서 프로비전하려고 하는 데이터 유형을 승인할 수 있는 확인된 정상 상태로 장치를 설정하는 것입니다. 따라서 장치는 구성 배포, OS 배포 및 사용자 지정 스크립팅을 처리할 수 있습니다.
- **프로토타입** — 프로토타입은 장치 템플릿을 정의하고 유지 관리하는 프로세스입니다. 장치 템플릿은 NA의 다른 장치와 유사한 메커니즘을 통해 조작되지만 장치 템플릿과 연관된 실제 장치는 없습니다. 프로토타입 단계의 목표는 장치를 작동시키지 않고 장치 구성 및 기타 프로비전 정보를 정의할 수 있도록 하는 것입니다. 보조 목표는 정보를 정의, 유지 관리 및 다시 사용하는 방법을 제공하는 것입니다.

참고: 장치 템플릿은 구성, OS/파일 사양 및 기타 장치별 정보를 정의한 다음 기존 장치에 적용할 수 있는 기능을 제공합니다. 장치 템플릿에는 정책 확인처럼 테스트할 실제 장치가 없어도 특정 장치 운영을 지원하는 기능도 있습니다. 자세한 내용은 [161페이지의 "새 장치 템플릿 추가"](#)를 참조하십시오.

- **프로비전** — 프로비전 중에는 추상적인 장치 템플릿이 실제 장치(일반적으로 사전 프로덕션 장치)에 적용됩니다. 이 적용 과정은 장치 템플릿의 프로비전 정보 가져 오기 및 적절히 장치에 적용하기로 구성됩니다. 장치 템플릿 구성의 경우 이 단계는 구성을 배포하는 프로세스가 됩니다. 프로비전에는 장치 템플릿의 프로비전 정보를 해당 장치에 맞게 사용자 지정할 특정 정보를 제공하는 기능도 포함됩니다. 이 정보는 사용자 지정 스크립트에 변수 값을 제공하는 것과 유사합니다. 프로비전 단계의 목표는 장치 구성 및 기타 장치 템플릿의 프로비전 정보를 실제 장치에 적용할 수 있도록 하는 것입니다.

다음은 간략하게 요약된 bare metal 프로비전 단계입니다.

1. NA에 사전 프로덕션 장치를 추가합니다. [137페이지의 "장치 추가"](#)를 참조하십시오. 사전 프로덕션 장치는 프로덕션 네트워크에서 아직 활성화되지 않은 장치입니다. 사전 프로덕션 장치는 포함되도록 명시적으로 선택하지 않는 한 검색에 포함되지 않으며 네트워크 상태의 보고서에 포함되지 않습니다.

참고: 장치 템플릿을 구성하기 전에 사전 프로덕션 장치를 NA에 추가할 필요는 없습니다. 그러나 사전 프로덕션 장치에 장치 템플릿을 배포하려면 NA에서 해당 장치를 관리해야 합니다.

2. 장치 템플릿을 구성합니다. 장치 템플릿은 다른 장치에 제공할 수 있는 OS/파일 시스템 및 구성 정보를 포함한 추상적인 장치 구성입니다. [161페이지의 "새 장치 템플릿 추가"](#)를 참조하십시오.
3. bare metal 장치에 연결합니다. Bare metal 장치는 사전 프로덕션 장치의 한 형태입니다. 기능은 텔넷 또는 SSH 프록시 연결 설정, 장치에 대해 스크립트 실행, 드라이버 검색 및 장치 설정 편집으로 매우 제한적입니다. [714페이지의 "Bare Metal 프로비전 스크립트"](#)를 참조하십시오.
4. 장치 템플릿에서 장치를 프로비전합니다. [444페이지의 "장치 프로비전 작업 페이지 필드"](#)를 참조하십시오. 장치 템플릿은 검색할 수 있습니다. [668페이지의 "장치 템플릿 검색"](#)을 참조하십시오.

장치 템플릿

장치 템플릿을 사용하면 구성, OS/파일 사양 및 기타 장치별 정보를 정의한 다음 기존 장치에 적용할 수 있습니다. 장치 템플릿에는 정책 확인처럼 테스트할 실제 장치가 없어도 특정 장치 운영을 지원하는 기능도 있습니다. bare metal 프로비전 프로세스에 대한 자세한 내용은 [153페이지의 "Bare Metal 프로비전"](#)을 참조하십시오.

참고: 장치 템플릿은 장치에 배포하여 기존 데이터를 완전히 덮어쓸 수 있는 전체 구성 파일입니다.

장치 템플릿 페이지에 액세스하려면 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 장치 템플릿을 클릭합니다. 장치 템플릿 페이지가 열립니다.

장치 템플릿 페이지 필드

필드	설명/작업
새 장치 템플릿 링크	새 장치 템플릿 페이지가 열립니다. 161페이지의 "새 장치 템플릿 추가" 를 참조하십시오.
확인란	왼쪽의 확인란을 통해 장치 템플릿을 삭제할 수 있습니다. 장치 템플릿을 선택한 후 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 장치 템플릿을 선택하거나 선택 취소할 수 있습니다.
호스트 이름	장치 템플릿의 호스트 이름을 표시합니다. 호스트 이름을 클릭하면 템플릿에 대한 추가 정보를 볼 수 있는 장치 템플릿 세부사항 페이지가 열립니다. 자세한 내용은 157페이지의 "장치 템플릿 세부사항 페이지 필드" 를 참조하십시오.
장치 공급업체	장치 공급업체(예: Cisco 또는 Nortel)를 표시합니다.
장치 모델	장치의 제조업체 모델 번호를 표시합니다.
파티션	보안 또는 비즈니스상의 이유로 파티션을 생성한 경우 특정 파티션의 각 장치에 대해 장치 암호 규칙을 파티셔닝할 수 있습니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.

필드	설명/작업
작업	<p>선택할 수 있는 작업은 다음과 같습니다.</p> <ul style="list-style-type: none">• 편집 — 장치 템플릿 편집 페이지가 열립니다. 155페이지의 "장치 템플릿 페이지 필드"를 참조하십시오.• 구성 보기 — 구성 보기 페이지가 열립니다. 227페이지의 "장치 구성 세부 사항 페이지 필드"를 참조하십시오.• 정책 준수 테스트 — 정책 준수 테스트 페이지를 엽니다. 자세한 내용은 545페이지의 "정책 준수 테스트 페이지 필드"를 참조하십시오.

장치 템플릿 세부사항 페이지 필드

장치 템플릿 페이지에서 장치를 선택하면 해당 장치에 대한 장치 템플릿 세부사항 페이지가 열립니다.

메뉴 옵션	설명/작업
보기 메뉴	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 장치 템플릿 홈 — 장치 템플릿 페이지를 엽니다. 155페이지의 "장치 템플릿 페이지 필드"를 참조하십시오. • 장치 템플릿 세부사항 — 세부사항을 볼 특정 장치 템플릿을 선택할 수 있습니다. • 현재 구성 — 현재 이 템플릿에 대해 설정된 구성을 보고 설명을 추가할 수 있는 현재 구성 페이지가 열립니다. "장치에 배포" 옵션을 클릭하면 구성 배포를 예약하거나 구성 배포를 즉시 시작할 수 있습니다. • 구성 이력 — 구성 변경을 볼 수 있는 장치 구성 페이지가 열립니다. 224페이지의 "장치 구성 페이지 필드"를 참조하십시오. • ACL — ACL(액세스 제어 목록)에 대한 정보를 볼 수 있는 장치 ACL 페이지를 엽니다. 자세한 내용은 874페이지의 "ACL 보기"를 참조하십시오. • 인터페이스 — 장치 인터페이스에 대한 정보를 볼 수 있는 장치 인터페이스 페이지를 엽니다. 자세한 내용은 267페이지의 "장치 인터페이스 페이지 필드"를 참조하십시오.

메뉴 옵션	설명/작업
편집 메뉴	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 구성 편집 — 구성을 편집한 다음 배포할 수 있는 구성 편집 페이지가 현재 구성으로 열립니다. 자세한 내용은 159페이지의 "템플릿 구성 편집 페이지"를 참조하십시오. • 장치 템플릿 편집 — 장치 템플릿 편집 페이지가 열립니다. 161페이지의 "새 장치 템플릿 페이지 필드"를 참조하십시오. • 장치 템플릿 삭제 — 장치 템플릿을 삭제할 수 있습니다. • 새 템플릿으로 저장 — 현재 장치 템플릿을 새 장치 템플릿으로 저장할 수 있습니다. 155페이지의 "장치 템플릿 페이지 필드"를 참조하십시오. • 프로세스 자동화 — HP Operations Orchestration에 로그인하여 HP Operations Orchestration 흐름을 안내 모드로 시작할 수 있는 HP Operations Orchestration 로그인 페이지가 열립니다. HP Operations Orchestration에 대한 자세한 내용은 <i>HP Operations Orchestration User's Guide</i>를 참조하십시오.
프로비전 메뉴	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 템플릿에서 장치 프로비전 — 장치에 대한 장치 템플릿 페이지가 열려 현재 장치 템플릿으로 다양한 장치를 프로비전할 수 있습니다. 164페이지의 "장치별 템플릿 페이지"를 참조하십시오.
주석	장치에 대한 설명을 표시합니다.
공급업체	장치 제조업체의 이름을 표시합니다.
모델	장치 모델 명칭을 표시합니다.
드라이버 이름	장치에 할당된 드라이버를 표시합니다.
장치 유형	라우터, 스위치, 방화벽 등의 장치 유형을 표시합니다.
장치 원본	장치를 NA로 가져왔고 소스에 이름이 지정된 경우 가져오기 소스의 이름을 표시합니다. 가져오기 소스에 이름이 지정되지 않은 경우 <날짜>에 NA에 추가됨으로 표시됩니다. 장치가 수동으로 추가된 경우 "<사용자 이름>에 의해 <날짜>에 수동으로 추가함"으로 표시됩니다.
마지막 구성 변경	장치 구성이 마지막으로 변경된 날짜와 시간을 표시합니다.

메뉴 옵션	설명/작업
관리 상태	장치 템플릿이 실제 장치가 아니어서 활성화 또는 비활성으로 지정할 수 없기 때문에 장치 템플릿이 표시됩니다.

템플릿 구성 편집 페이지

기본적으로 장치 템플릿의 구성은 장치의 전체 구성 파일을 대체하는 데 사용할 수 있는 스크립트입니다. 따라서 구성은 부팅 시 장치에서 사용할 수 있는 완전한 작업 구성 파일이어야 합니다.

처음부터 구성을 생성하는 대신 "새 템플릿으로 저장" 명령을 사용하여 네트워크에 이미 있는 장치에서 구성을 복사할 수 있습니다. 자세한 내용은 [304페이지의 "편집 메뉴 옵션"](#)을 참조하십시오.

변수를 사용하여 구성을 사용자 지정할 수 있습니다. '\$' 문자는 변수 이름에 사용하도록 예약되었습니다. 장치 템플릿에 상수 '\$'를 입력해야 할 경우 이스케이프 시퀀스 \x24를 사용하십시오.

참고: tc_로 시작하는 변수는 특수한 용도로 예약된 것입니다. 해당 문자 시퀀스로 시작되는 변수는 정의할 수 없습니다.

\$MyVar\$와 같은 사용자 지정 변수에는 Pull 변수 버튼을 사용하여 해당 변수에 대해 정의된 프롬프트가 있습니다. Pull 변수 버튼은 장치 템플릿에 사용된 변수별로 입력 필드를 페이지 맨 아래에 추가하면서 페이지를 새로 고칩니다. 변수를 위한 사용자 지정 프롬프트를 정의하고 각 프롬프트에서 허용하는 값을 제한할 때 이 필드를 사용합니다.

- 값에 라인을 여러 개 허용합니다.
- 값을 다음으로 제한: (첫 번째, 마지막, 끝에서 두 번째)
- 암호(이 옵션을 선택하면 NA는 명령 스크립트 실행 작업 페이지에서 값 프롬프트가 표시될 때 암호를 에코하지 않음)

\$tc_device_hostname\$과 같은 예약된 변수는 프로비전할 장치의 값으로 자동으로 채워집니다. 장치 템플릿 자체의 값은 이러한 변수에 사용되지 않습니다.

참고: 사용자 지정 변수를 CSV 파일로 제공하려는 경우 기존의 scriptField1, scriptFiled2 등과 같은 헤더를 장치 템플릿의 사용자 지정 변수 이름으로 대체할 수 있습니다. CSV 파일을 사용하면 장치 템플릿에서 여러 장치를 한 번에 프로비전할 수 있습니다. 프로비전할 각 장치에 대한 변수 값을 장치 템플릿을 사용하여 제공해야 합니다.

장치의 기본 IP 주소 변경

장치 템플릿 프로비전 프로세스의 일부로 장치의 기본 IP 주소를 변경하려는 경우 `$tc_device_primary_ip$` 변수는 이 용도로 특별히 예약되어 있으며 장치 템플릿에만 사용됩니다. 다른 예약된 변수와 달리 이 변수의 값은 장치 프로비전 작업이 실행될 때 사용자가 제공하거나 CSV 파일에서 제공합니다. CSV 데이터 파일에는 이 변수가 열로 포함되어 있습니다.

장치 템플릿의 구성에 `$tc_device_primary_ip$`를 포함하면 장치 프로비전 작업이 완료된 후 NA에서는 장치에 액세스하는 데 사용된 기본 IP 주소를 이 새 값으로 업데이트합니다. NA에서는 모든 보고서 및 검색에서 장치를 식별하도록 새로운 기본 IP 주소를 표시합니다.

새 장치 템플릿 추가

새 장치 템플릿 페이지에서는 새 장치 템플릿을 추가할 수 있습니다.

새 장치 템플릿을 추가하려면 장치 아래의 메뉴 모음에서 새로 만들기를 선택하고 장치 템플릿을 클릭합니다. 장치 템플릿 페이지의 새 장치 템플릿 링크에서도 이 페이지에 액세스할 수 있습니다. 새 장치 템플릿 페이지가 열립니다.

새 장치 템플릿 페이지 필드

새 장치 템플릿 페이지에서는 장치 템플릿을 구성할 수 있습니다.

참고: 장치 템플릿 편집 페이지는 필드가 채워져 있다는 점을 제외하면 새 장치 템플릿 페이지와 동일합니다.

필드	설명/작업
이름	장치 템플릿의 이름을 입력합니다.
파티션	적용 가능한 경우 드롭다운 메뉴에서 파티션을 선택합니다. 새 장치 템플릿은 파티션에 있는 장치에만 적용됩니다. 파티션 생성에 대한 자세한 내용은 191 페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
장치 드라이버	드롭다운 메뉴의 사용 가능한 드라이버 목록에서 드라이버를 선택합니다.
주석	장치에 대한 주석을 입력합니다.

연결 정보(장치 템플릿은 실제 장치가 아니기 때문에 템플릿 자체에 연결할 수는 없지만 장치 템플릿에서 프로비전된 장치는 해당 연결 설정을 상속할 수 있습니다. 자세한 내용은 [155페이지의 "장치 템플릿"](#)을 참조하십시오.

필드	설명/작업
연결 방법	<p>NA는 다음 프로토콜 조합을 사용하여 네트워크 장치와 통신할 수 있습니다. 사용하려는 하나 이상의 프로토콜을 선택합니다. NA는 사용자가 선택한 프로토콜 중에서 언제든지 가장 효율적인 프로토콜을 선택합니다.</p> <ul style="list-style-type: none"> •SNMP •SNMPv1 또는 SNMPv2c(커뮤니티 문자열 인증) •SNMPv3(사용자 인증) — SNMPv3을 사용하는 경우 noAuthNoPriv(사용자 이름만), authNoPriv(사용자 이름, 인증 암호), authPriv(사용자 이름, 인증 및 암호화 암호) 옵션이 제공됩니다. 인증 방법에는 SHA(Secure Hash Algorithm) 및 MD5(Message Digest Algorithm)가 포함되며, 암호화 방법에는 DES(Data Encryption Standard), AES(Advanced Encryption Standard), AES192 및 AES256이 포함됩니다. •RLogin •텔넷 •SSH(SSH1 또는 SSH2(기본값), SSH1만 또는 SSH2만 중에서 선택할 수 있음)
전송 프로토콜	<p>다음 전송 프로토콜 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none"> •SCP •FTP •TFTP
ACL 구문 분석	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •사용함 — 이 옵션을 선택하면(기본값) 각 스냅샷 시 장치에 대한 ACL 데이터가 저장됩니다. 스냅샷이 작성될 때까지 ACL은 로드되지 않습니다. •사용 안 함 — 이 옵션을 선택하면 각 스냅샷 시 장치에 대한 ACL 데이터가 저장되지 않습니다.
추가 정보	<p>NA에서는 장치 스냅샷 프로세스의 다음 필드 일부를 자동으로 채웁니다. 이러한 필드를 수동으로 채울 경우 장치가 폴링될 때마다 데이터가 덮어쓰여집니다.</p>
장치 설명	장치 식별에 사용할 설명을 입력합니다.

필드	설명/작업
모델	장치의 제조업체 모델 번호를 입력합니다. FQDN 확인 작업을 통해 장치의 기본 IP 주소에서 역방향 DNS 조회를 실행하여 시스템의 각 장치에 대한 FQDN(정규화된 도메인 이름)을 설정할 수 있습니다.
공급업체	장치 공급업체(예: Cisco 또는 Nortel)를 입력합니다.
계층 수준	<p>계층 레이어는 장치 속성입니다. 장치를 추가하거나 편집할 때 장치의 계층 레이어를 설정할 수 있습니다. 따라서 네트워크 다이어그램을 구성할 때 필터링할 계층 레이어를 선택할 수 있습니다. 예를 들어 전체 네트워크(인벤토리)를 다이어그램으로 작성하도록 선택한 후 계층 레이어가 코어로 설정된 코어 장치만 가져오도록 "코어"에 대해 필터링을 적용할 수 있습니다. 네트워크 다이어그램 작성에 대한 자세한 내용은 758페이지의 "다이어그램 작성"을 참조하십시오.</p> <p>참고: 아래에 제공된 옵션은 기본 계층 레이어입니다. 사용자 지정 계층 레이어에 대한 자세한 내용은 768페이지의 "appserver.rcx 파일 편집"을 참조하십시오.</p> <p>드롭다운 메뉴에서 계층 레이어를 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 레이어가 설정되지 않음 • 코어 • 배포 • 액세스 • 가장자리
사용자 지정 서비스 유형	서비스 유형을 입력합니다. 서비스 유형에서는 VoIP, BGP, MPLS 등을 지정할 수 있습니다. 이 값을 사용하여 장치의 용도를 식별할 수 있습니다. 이러한 값으로 장치 서비스에 태그를 지정하면 그룹(정적 또는 동적)에서 해당 서비스를 쉽게 검색하거나 볼 수 있습니다.

작업이 완료된 경우에는 저장 버튼을 클릭하고 다른 장치 템플릿을 추가하려는 경우에는 저장 및 다른 항목 추가 버튼을 클릭해야 합니다.

장치별 템플릿 페이지

장치 템플릿 세부사항 페이지의 프로비전 메뉴에서 템플릿에서 장치 프로비전 옵션을 선택하면 해당 장치에 대한 장치 템플릿 페이지가 열립니다. 이 페이지에는 장치 템플릿에 할당된 드라이버와 일치하는 장치 목록이 표시되며, 장치 템플릿에서 프로비전할 수 있습니다.

필드	설명/작업
장치 표시	<p>풀다운 메뉴에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •모두 •활성 •사전 프로덕션
호스트 이름	장치의 호스트 이름을 표시합니다. 호스트 이름을 클릭하면 장치 및 해당 구성 내역에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
장치 IP	장치의 IP 주소를 표시합니다. 빨간색으로 표시된 장치는 마지막 스냅샷 시도에서 실패한 장치입니다. 비활성 장치는 IP 주소 옆의 아이콘으로 표시됩니다. IP 주소를 클릭하면 장치 및 해당 구성 내역에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
장치 공급업체	장치 제조업체 이름이 표시됩니다.
장치 모델	지정된 장치 모델이 표시됩니다.
파티션	적용 가능한 경우 드롭다운 메뉴에서 파티션을 선택합니다. 새 장치 템플릿은 파티션에 있는 장치에만 적용됩니다. 파티션 생성에 대한 자세한 내용은 191 페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
작업	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> •장치 프로비전 — 새 작업 - 장치 프로비전 페이지가 열려 장치를 프로비전할 수 있습니다. 444페이지의 "장치 프로비전 작업 페이지 필드"를 참조하십시오. •구성 비교 — 장치 구성 비교 페이지가 열립니다. 231페이지의 "장치 구성 비교 페이지 필드"를 참조하십시오.

새 장치 마법사 사용

새 장치 마법사를 사용하여 장치를 추가하려면 장치 아래의 메뉴 모음에서 새 장치 마법사를 클릭합니다. 새 장치 마법사가 열립니다.

새 장치 마법사 페이지 필드

단계	설명/작업
1단계: 장치 생성	<p>다음 정보를 입력합니다.</p> <ul style="list-style-type: none"> • 호스트 이름 또는 IP — 장치의 호스트 이름이나 IP 주소를 입력합니다. • 주석 — 장치에 대한 주석을 입력합니다. • 관리 상태 — 활성 또는 비활성을 선택합니다. (참고: 사전 프로덕션 장치는 새 장치 마법사를 통해 추가할 수 없습니다.) <p>완료되면 다음 중 하나를 클릭합니다.</p> <ul style="list-style-type: none"> • 다음 — 인증 페이지가 열립니다. 아래를 참조하십시오. • 완료 — 장치가 성공적으로 추가되면 장치 추가 마법사 축하 페이지가 열립니다. 이 페이지에는 검색 문제에 대한 정보가 표시됩니다.

단계	설명/작업
2단계: 장치 인증	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 네트워크 전체 암호 규칙 사용 — 이 옵션을 선택하면(기본값) NA는 장치에 적용되는 네트워크 전체 장치 암호 규칙을 사용합니다. 만들기 링크를 클릭하여 네트워크 전체 암호 규칙을 생성할 수 있습니다. 170페이지의 "장치 암호 규칙 생성"을 참조하십시오. • 장치별 암호 사용 — 이 옵션을 선택한 경우 장치에 대해 사용자 이름, 암호, 활성화 암호(적용 가능한 경우), SNMP 읽기 커뮤니티 문자열 및 SNMP 쓰기 커뮤니티 문자열을 입력합니다. SNMPv3의 경우 인증 및 암호화 정보를 입력합니다. <p>완료되면 다음 중 하나를 클릭합니다.</p> <ul style="list-style-type: none"> • 뒤로 — 장치 생성 단계로 돌아갑니다. • 다음 — 구성 페이지가 열립니다. 아래를 참조하십시오. • 완료 — 장치가 성공적으로 추가되면 장치 추가 마법사 축하 페이지가 열립니다. 이 페이지에는 검색 문제에 대한 정보가 표시됩니다.
3단계: 장치 구성	<p>NA에서는 장치 공급업체 및 모델을 검색하려고 합니다. 검색이 성공적으로 수행되면 장치 구성을 가져와 저장합니다. 그러면 변경 감지를 위해 장치가 구성됩니다. 변경 감지를 위해 장치를 구성하지 않으려면 장치에 대한 Syslog 구성 업데이트 상자를 선택 취소합니다. 이 상자를 선택한 경우 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • HP Network Automation Syslog 서버에 기록 — 장치에 대한 Syslog 구성 업데이트 상자를 선택하면 이 옵션이 기본적으로 선택됩니다. • 기존 Syslog 릴레이 호스트에 기록 — 릴레이 호스트의 호스트 이름 또는 IP 주소를 입력합니다. (참고: NA에서는 변경 감지를 위해 올바른 로깅 수준을 설정합니다.) <p>완료를 클릭합니다. 장치가 성공적으로 추가되면 장치 추가 마법사 축하 페이지가 열립니다. 이 페이지에는 검색 문제에 대한 정보가 표시됩니다.</p>

장치 가져오기

CSV(쉼표로 구분된 값) 파일에서 장치를 가져오려면 다음과 같은 방법을 사용할 수 있습니다.

- 장치 암호 규칙(일반적으로 그룹에 할당) 및 CSV 파일 사용
- 장치 데이터를 한 CSV 파일에 가져오고 장치 암호 정보를 다른 CSV 파일에 가져오기

CSV 파일을 사용하여 장치를 가져오려면 장치 아래의 메뉴 모음에서 장치 작업을 선택하고 가져오기를 클릭합니다. 가져오기 작업 페이지가 열립니다. [421페이지의 "가져오기 작업 페이지 필드"](#)를 참조하십시오.

CSV 파일에서 정기적으로 장치를 가져오도록 NA를 구성할 수 있습니다. 장치를 처음 가져올 때 다음을 수행해야 합니다.

- 장치 암호 규칙을 설정한 후 인벤토리 그룹에 적용합니다(모든 장치). [170페이지의 "장치 암호 규칙 생성"](#)을 참조하십시오.
- 기본 연결 방법을 구성합니다. [56페이지의 "장치 액세스 페이지 필드"](#)를 참조하십시오.
- 장치 가져오기 파일(Device.csv)을 준비합니다. Device.csv 파일을 편집하거나 Excel과 같은 프로그램에 로드할 수 있습니다. [168페이지의 "CSV 장치 및 암호 데이터 파일 생성"](#)을 참조하십시오.

참고: 네트워크 장치 감지 작업을 사용하면 NA에서 관리하려는 장치를 네트워크에서 찾을 수 있습니다. IP 주소 범위를 제공하면 NA에서는 네트워크를 검색하여 장치를 찾습니다. 자세한 내용은 [426페이지의 "네트워크 장치 감지 작업 페이지 필드"](#)를 참조하십시오.

CSV 장치 및 암호 데이터 파일 생성

CSV 장치 데이터 파일(device.csv)에서 첫 번째 행에는 가져오는 데이터에 대한 NA 데이터베이스 열 이름이 포함되어 있습니다. 가장 일반적으로 사용되는 열 이름은 아래에 나와 있습니다. 열 이름은 대소문자를 구분합니다.

열 이름	설명/작업
primaryIPAddress	장치의 기본 IP 주소. 유일한 필수 필드입니다.
deviceDriver	장치 드라이버의 이름
deviceGroupName	장치가 들어 있는 그룹의 이름
hostName	장치의 호스트 이름
consoleIPAddress	장치와 연결된 콘솔의 IP 주소
consolePort	콘솔의 포트 번호. 장치 액세스를 위해 콘솔 서버를 사용할지 여부를 지정합니다. (참고: 콘솔 서버 액세스에는 텔넷만 사용됩니다.)
accessMethods	<p>장치에 대한 액세스 방법. accessMethods는 access_methods[+connect_methods[+console]]로 구성됩니다. 예를 들면 다음과 같습니다.</p> <ul style="list-style-type: none"> • CLI:TFTP+ssh+console • CLI:FTP+ssh:telnet • SNMP:TFTP <p>access_methods는 CLI, SNMP, TFTP 또는 FTP일 수 있으며 둘 이상의 액세스 방법이 지원될 경우 콜론으로 구분됩니다. (참고: connect_methods는 CLI가 지원될 경우에만 적용되며, SSH 또는 텔넷일 수 있으며, 둘 이상의 방법이 지원될 경우 콜론으로 구분됩니다.)</p>
managementStatus	<p>장치가 활성화(관리됨), 비활성(관리되지 않음), 사전 프로덕션(아직 완전히 구성되지 않음) 또는 장치 템플릿인지를 나타냅니다. 숫자 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 0 — 활성화(기본값) • 1 — 비활성 • 2 — 장치 템플릿 • 3 — 사전 프로덕션
assetTag	이 장치의 자산 태그 문자열

열 이름	설명/작업
siteName	장치가 속한 사이트의 이름
comments	장치에 대한 설명
deviceCustom1	사용자 지정 데이터 페이지의 장치 섹션에서 최대 6개의 사용자 지정 필드를 생성할 수 있습니다. 데이터를 가져오기 전에 필드를 생성해야 합니다.

NA에서는 장치 구성의 다음 필드를 자동으로 채웁니다. 장치 데이터를 가져올 때 이러한 필드를 수동으로 채우는 경우 관리 설정 - 서버 페이지의 "기존 장치 덮어쓰기" 옵션이 예로 설정되어 있으면 장치를 가져올 때마다 데이터를 덮어씁니다. 자세한 내용은 [67페이지의 "서버"](#)를 참조하십시오.

- 호스트 이름
- 일련 번호
- 위치
- 공급업체
- 모델
- 운영 체제

참고: 열을 채우지 않을 경우에는 열 이름을 포함하지 마십시오. 장치가 이미 있는 경우 빈 값이 기존 데이터를 덮어씁니다.

그룹 및 장치 암호 규칙을 사용하여 장치를 가져오려면 다음이 있어야 합니다.

1. 가져올 장치의 정의된 그룹: [175페이지의 "장치 그룹 추가"](#)를 참조하십시오.
2. 각 그룹의 정의된 네트워크 전체 암호 규칙: [170페이지의 "장치 암호 규칙 생성"](#)을 참조하십시오.
3. 각 장치가 속하는 그룹을 포함하는 가져온 장치: [167페이지의 "장치 가져오기"](#)를 참조하십시오.
4. 가져온 장치에 대해 검색된 드라이버: [212페이지의 "장치 드라이버 검색"](#)을 참조하십시오. 지원되는 장치에 대한 자세한 내용은 DRS(장치 릴리스 서비스) 설명서를 참조하십시오. DRS는 자동화된 새로운 드라이버 릴리스 및 전달 시스템입니다.

장치 암호 규칙 생성

장치 암호 규칙을 사용하면 동일한 사용자 이름, 암호 및 SNMP 커뮤니티 문자열을 장치 그룹, IP 주소 범위 또는 호스트 이름에 적용할 수 있습니다.

참고: 장치 암호 규칙을 공용 장치 그룹에만 적용할 수 있습니다. 개인 장치 그룹에는 암호 규칙을 적용할 수 없습니다.

장치에 로그인하려고 할 때 NA는 적용 가능한 장치 암호 규칙 목록을 로그인이 성공할 때까지 순서대로 적용한 다음 해당 규칙을 장치 로그인으로 설정합니다. 이후의 로그인 시도에서 규칙이 실패하면 NA는 유효한 새 로그인을 찾을 때까지 적용 가능한 규칙을 순서대로 다시 시도합니다. 이 설정은 장치 액세스 페이지에서 구성할 수 있습니다. 자세한 내용은 [56페이지의 "장치 액세스 페이지 필드"](#)를 참조하십시오.

참고: 장치 암호를 생성할 때 "항상 마지막으로 성공한 암호를 먼저 사용합니다" 및 "항상 정의된 순서대로 암호를 사용합니다" 옵션을 설정할 수 있습니다. 자세한 내용은 [56페이지의 "장치 액세스 페이지 필드"](#)를 참조하십시오.

장치 암호 규칙을 생성하려면 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 장치 암호 규칙을 클릭합니다. 장치 암호 규칙 페이지가 열립니다.

참고: 규칙 순서는 중요합니다. NA는 장치 암호 규칙 페이지에 표시된 순서대로 규칙을 적용합니다. 스냅샷을 작성할 때 성능 문제가 계속 나타날 경우 가장 일반적으로 사용되는 규칙이 맨 위에 오도록 규칙의 순서를 다시 지정하는 것을 고려하십시오. 또한 더 적은 수의 그룹이나 더 작은 IP 범위로 규칙을 제한해야 합니다.

장치 암호 규칙 페이지 필드

필드	설명/작업
새 암호 규칙 링크	암호 규칙 정의 페이지가 열립니다. 이 페이지에서 장치 암호 규칙을 생성 및 편집할 수 있습니다. 자세한 내용은 172페이지의 "장치 암호 규칙 페이지 필드" 를 참조하십시오.
확인란	왼쪽의 확인란을 사용하여 장치 암호 규칙을 삭제할 수 있습니다. 규칙을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 규칙을 선택하거나 선택을 취소할 수 있습니다.
변경 날짜	규칙이 마지막으로 변경된 날짜와 시간이 표시됩니다.
규칙 이름	규칙의 이름이 표시됩니다.
유형	다음과 같은 규칙 유형이 표시됩니다. <ul style="list-style-type: none"> •IP 범위 •호스트 이름 •장치 그룹
파티션	보안 또는 비즈니스상의 이유로 파티션을 생성한 경우 특정 파티션의 각 장치에 대해 장치 암호 규칙을 파티셔닝할 수 있습니다. 특정 파티션의 특정 장치뿐만 아니라 모든 파티션의 모든 장치에서 공유할 장치 암호 규칙을 구성할 수 있습니다. 장치 암호 규칙을 모든 파티션에서 사용할 수 있는 경우 [공유]라는 레이블이 붙습니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오. <p>참고: 장치 암호 규칙을 생성할 때 드롭다운 메뉴에서 파티션을 선택할 수 있습니다. 자세한 내용은 172페이지의 "장치 암호 규칙 페이지 필드"를 참조하십시오.</p>
장치	규칙의 호스트 이름, IP 주소 또는 그룹 이름을 표시합니다.
생성자	규칙을 수정한 사람의 로그인 이름이 표시됩니다. NA는 해당 이름을 사용할 수 없음을 의미합니다.
작업	각 규칙에 대해 다음 작업을 선택할 수 있습니다. <ul style="list-style-type: none"> •편집 — 규칙을 편집할 수 있는 장치 암호 규칙 페이지가 열립니다. 자세한 내용은 172페이지의 "장치 암호 규칙 페이지 필드"를 참조하십시오. (참고 장치 암호 규칙은 우선 순위의 순서대로 나열됩니다. 화살표를 사용하여 목록에서 규칙을 위 또는 아래로 이동할 수 있습니다.)

장치 암호 규칙 페이지 필드

참고: 암호 및 SNMP 커뮤니티 문자열은 AES 256비트 키로 암호화된 NA 데이터베이스에 저장됩니다. 각 NA 설치에 대해 고유 키가 생성됩니다.

필드	설명/작업
규칙 정의	
네트워크 전체 암호 규칙	이 옵션을 선택하면(기본값) NA에서는 규칙의 모든 장치에 적용되는 네트워크 전체 장치 암호 규칙을 사용합니다. 네트워크 전체 암호 규칙을 사용하는 것은 확장성이 뛰어난 장치 자격 증명 설정 방법입니다.
규칙 이름	규칙 이름을 입력합니다.
파티션	적용 가능한 경우 드롭다운 메뉴에서 파티션을 선택합니다. 장치 암호 규칙은 파티션에 있는 장치에만 적용됩니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
다음 이전에 삽입	드롭다운 메뉴에서 이 규칙이 위에 삽입될 기존 규칙 이름을 선택합니다.
IP 범위	이 옵션을 선택한 경우 규칙이 적용될 범위의 첫 번째 및 마지막 IP 주소를 입력합니다. 와일드카드(* 또는 ?)를 사용하면 관련 장치 집합에 이 규칙을 적용할 수 있습니다.
호스트 이름	이 옵션을 선택한 경우 이 규칙이 적용될 호스트 이름을 입력합니다. 와일드카드(* 또는 ?)를 사용하면 관련 장치 집합에 이 규칙을 적용할 수 있습니다.
장치 그룹	이 옵션을 선택한 경우 장치 선택기를 사용하여 이 규칙이 적용될 그룹 이름 하나를 선택합니다. 규칙을 모든 장치에 적용하려면 인벤토리를 선택합니다. 장치 암호 규칙은 단일 장치 그룹에만 할당할 수 있습니다.
장치별 암호 정보	선택한 경우 장치 IP 주소를 입력합니다. NA에서 이 페이지에 있는 현재 인증 정보를 사용하고 저장 버튼을 클릭할 때 지정된 장치에 복사합니다.

필드	설명/작업
암호 정보	
사용자 이름	NA에서 장치 액세스에 사용할 사용자 이름을 입력합니다. 장치가 AAA 솔루션(예: TACACS+)을 사용하도록 구성된 경우 NA에 대한 AAA 사용자 계정을 생성하고 해당 AAA 자격 증명을 장치 자격 증명으로 사용하십시오.
암호	NA에서 장치 액세스에 사용할 암호를 입력합니다.
암호 확인	확인을 위해 암호를 다시 한 번 입력합니다.
활성화 암호	NA에서 권한이 부여된 모드에 액세스하는 데 필요한 활성화 암호를 입력합니다. 대부분의 구성 변경 작업에는 활성화 암호가 필요합니다. (참고: Nortel ASN/ARN과 같은 일부 장치에는 권한이 부여된 모드에 액세스하기 위해 암호가 필요하지 않을 수 있습니다. 또한 일부 장치는 권한이 부여된 모드에 대한 암호를 비활성화하도록 구성될 수 있습니다. 네트워크 관리자에게 사이트별 구성을 확인하십시오.)
활성화 암호 확인	확인을 위해 활성화 암호를 다시 입력합니다.
SNMP 읽기 전용 커뮤니티 문자열	SNMP 읽기 전용 커뮤니티 문자열을 입력합니다.
SNMP 읽기/쓰기 커뮤니티 문자열	SNMP 읽기/쓰기 커뮤니티 문자열을 입력합니다.
SNMPv3 사용자 이름	장치 액세스에 사용되는 SNMPv3 사용자 이름을 입력합니다.
SNMPv3 인증 암호	NA에서 장치 액세스에 사용할 SNMPv3 인증 암호를 입력합니다.
SNMPv3 인증 암호 확인	확인을 위해 SNMPv3 인증 암호를 다시 입력합니다.
SNMPv3 암호화 암호	SNMPv3 암호화 암호를 입력합니다.
SNMPv3 암호화 암호 확인	확인을 위해 SNMPv3 암호화 암호를 다시 입력합니다.

필드	설명/작업
장치 액세스 설정 표시	<p>NA는 대부분의 네트워크 및 네트워크 장치에서 작동하도록 고안되었습니다. 그러나 고유한 장치 구성이 특정 장치를 관리하는 NA의 기능에 영향을 줄 수 있습니다. 장치 액세스 설정을 사용하여 네트워크 구성에 맞게 NA를 조정할 수 있습니다. 장치 액세스 설정은 장치 암호 정보와 연결되어 있습니다. 입력한 장치별 설정은 장치별 암호 정보를 사용하도록 선택한 경우에만 적용됩니다. 네트워크 전체 장치 설정을 암호 규칙에 추가할 수 있습니다. 예를 들면 다음과 같습니다.</p> <ul style="list-style-type: none"> • 실행 모드 프롬프트 • 구성 모드 프롬프트 • 관리 프롬프트 <p>참고: 장치 암호 규칙을 정의할 때 각 장치 액세스 설정에 대한 여러 값을 정의할 수 있어도 장치 액세스 설정당 하나의 값만 지정해야 합니다. 장치 액세스 설정을 두 번 이상 지정하면 값 중 하나만 사용되며 사용될 값에 대한 특정 결정 기준은 없습니다. 장치 액세스 설정 사용 방법에 대한 자세한 내용을 보려면 "장치 액세스 설정 사용 방법" 링크를 클릭하십시오.</p>

완료되면 저장 버튼을 클릭해야 합니다. 그러면 새 규칙이 장치 암호 규칙 목록에 표시됩니다.

장치 그룹 추가

장치 그룹을 생성하면 조직에 적합한 방식으로 장치를 분류할 수 있습니다. 장치는 다음 스키마 중 하나를 사용하여 이미 구성되어 있을 수 있습니다.

- 지리적/물리적 위치(예: 시애틀 및 뉴욕)
- 비즈니스 단위/부서(예: 판매, 구매 및 제조)
- 네트워크 아키텍처에서의 역할(예: 코어, 가장자리, 배포, 액세스)

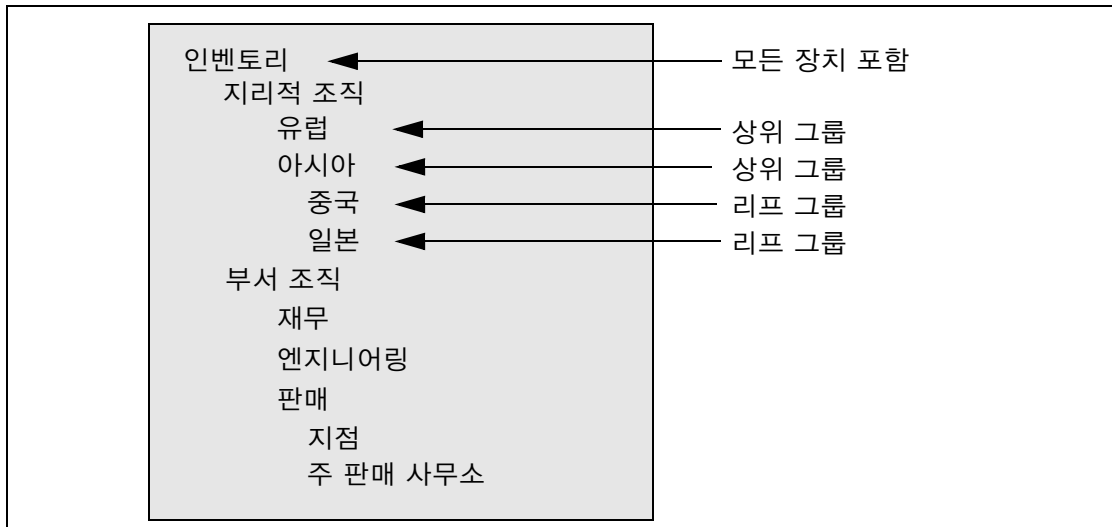
초기 장치 그룹 페이지에는 하나의 시스템 그룹인 인벤토리 그룹이 포함되어 있습니다. 인벤토리 그룹에는 NA에 추가된 모든 장치가 포함되어 있습니다. 그러나 사용자가 생성하는 사용자 정의 그룹도 이 페이지에 나타납니다.

NA의 장치 그룹 계층은 상위 그룹 및 리프 그룹으로 구성됩니다.

- 상위 그룹에는 상위 항목이 하나만 포함될 수 있습니다. 상위 그룹을 새 상위 그룹의 하위 그룹으로 추가하면 이전 연관이 덮어쓰여집니다. 또한 상위 그룹은 장치가 아닌, 장치 그룹만 포함할 수 있습니다.
- 리프 그룹은 다른 장치 그룹이 아닌, 장치만 포함할 수 있습니다.

기본 인벤토리 그룹은 특수하게 취급되며, 상위 그룹이기도 하고 리프 그룹이기도 합니다. 여기에는 시스템의 모든 장치가 포함되어 있습니다. 상위 그룹에 속하지 않는 모든 리프 그룹은 인벤토리 그룹에 포함됩니다.

장치 그룹 계층을 생성하면 장치 그룹 집합에 대해 작업 및 보고서를 쉽게 실행할 수 있습니다. 장치 그룹 계층의 예는 아래와 같습니다.



예를 들어 이 장치 그룹 계층을 사용하여 일본 장치 또는 아시아 장치(중국 및 일본 장치 모두 포함)에 대해 작업 및 보고서를 실행할 수 있습니다.

새 그룹 페이지 필드

새 장치 그룹을 추가하려면 장치 아래의 메뉴 모음에서 새로 만들기를 선택하고 장치 그룹을 클릭합니다. 새 그룹 페이지가 열립니다.

참고: NA 관리자가 아니면 사용자 그룹에 보기 관리 또는 파티션 관리 권한을 부여할 수 없습니다.

필드	설명/작업
그룹 이름	그룹 이름을 입력합니다.
설명	그룹에 대한 설명을 입력합니다.
사이트 <이름>	적용 가능한 경우 드롭다운 메뉴에서 파티션을 선택합니다. 필드 이름은 파티션 페이지에서 수정할 수 있습니다. (자세한 내용은 202페이지의 "파티션 페이지 필드" 를 참조하십시오.)
소유자	드롭다운 메뉴에서 이름을 선택합니다. Admin이 기본값입니다.
공유	공용 또는 개인을 선택합니다. 공용 그룹은 모든 사용자가 볼 수 있지만 개인 그룹은 그룹의 소유자와 시스템 관리자만 볼 수 있습니다. 참고: 개인 장치 그룹을 사용하면 여러 사용자가 자체 장치 그룹을 설정할 수 있습니다. 사용자는 NA에 로그인하면 자신의 장치 그룹과 공용 장치 그룹을 볼 수 있습니다. 따라서 쉽게 사용하고 확장할 수 있도록 NA를 사용자 지정할 수 있습니다.
상위 장치 그룹	드롭다운 메뉴에 인벤토리 그룹이 나타나지만 다른 그룹을 선택할 수 있습니다. 그룹을 개인 그룹으로 설정하면 선택한 사항은 무시됩니다. 개인 그룹은 그룹 계층의 일부가 될 수 없습니다.
장치	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> 고정 장치 집합(정적 그룹)을 선택하려면 장치 선택기를 사용하십시오. — 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. 동적 장치 집합(동적 그룹)을 정의하려면 필터를 사용하십시오. — 자세한 내용은 180페이지의 "동적 장치 그룹"을 참조하십시오.

상위 그룹 추가

새 상위 그룹을 추가하려면

1. 장치 아래의 메뉴 모음에서 그룹을 클릭합니다. 장치 그룹 페이지가 열립니다.
187페이지의 "장치 그룹 페이지 필드"를 참조하십시오.
2. 페이지 맨 위에 있는 새 상위 그룹 링크를 클릭합니다. 새 상위 그룹 페이지가 열립니다.

참고: 상위 그룹을 생성하려면 올바른 사용 권한이 있어야 합니다. 또한 장치 그룹 계층이 공유되며 모든 상위 그룹은 공용이어야 합니다.

새 상위 그룹 페이지 필드

필드	설명/작업
그룹 이름	상위 그룹의 이름을 입력합니다.
설명	다른 그룹과 차별화하는 상위 그룹에 대한 설명을 입력합니다.
사이트 <이름>	드롭다운 메뉴에서 파티션을 선택합니다. 필드 이름은 파티션 페이지에서 수정할 수 있습니다. (자세한 내용은 202페이지의 "파티션 페이지 필드" 를 참조하십시오.)
공유	상위 그룹은 항상 공용입니다.
상위 장치 그룹	기본적으로 드롭다운 메뉴에서 인벤토리가 표시됩니다.
하위 장치 그룹	<ul style="list-style-type: none"> • 모든 장치 그룹 — 모든 현재 장치 그룹 목록이 표시됩니다. 상위 그룹에 하위 항목으로 포함할 장치 그룹을 선택하고 복사 >>를 클릭합니다. 그룹은 한 상위 그룹의 하위 그룹만 될 수 있습니다. 그룹이 이미 상위 그룹에 속해 있으면 해당 그룹은 이전 상위 그룹에서 제거됩니다. • 이 그룹의 하위 — 상위 그룹에 하위 항목으로 할당된 장치 그룹 목록이 표시됩니다. 이 그룹에서 제거할 하위 그룹을 선택하고 << 제거를 클릭합니다.

완료되면 저장 버튼을 클릭합니다. 상위 그룹이 열립니다.

상위 그룹 페이지 필드

필드	설명/작업
새 그룹 링크	새 장치 그룹을 생성할 수 있는 새 그룹 페이지가 열립니다. 자세한 내용은 175페이지의 "장치 그룹 추가" 를 참조하십시오.
새 상위 그룹 링크	새 상위 그룹을 추가할 수 있는 새 상위 그룹 페이지를 엽니다. 자세한 내용은 178페이지의 "새 상위 그룹 페이지 필드" 를 참조하십시오.
그룹 이름	장치 그룹의 사용자 정의 이름을 표시합니다. 그룹 이름을 클릭하면 장치 그룹 세부사항 페이지가 열립니다. 자세한 내용은 188페이지의 "장치 그룹 세부사항 페이지 필드" 를 참조하십시오.
설명	다른 그룹과 차별화하는 그룹에 대한 설명을 입력합니다.
장치 수	그룹에 있는 장치의 수를 표시합니다.
소유자	장치 그룹을 생성한 사용자 이름을 표시합니다.
공유	그룹이 공용 그룹인지 또는 개인 그룹인지가 표시됩니다. 공용 그룹은 모든 사용자가 볼 수 있지만 개인 그룹은 그룹의 소유자와 시스템 관리자만 볼 수 있습니다.
작업	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 보기 — 선택한 장치 그룹에 포함된 장치를 표시합니다. 장치는 이 장치가 리프 장치 그룹인 경우 이 장치 그룹의 직접 하위 항목이거나 장치 그룹이 상위 장치 그룹인 경우 하위 장치 그룹의 하위 항목일 수 있습니다. 보기 옵션에 대한 자세한 내용은 186페이지의 "장치 그룹 보기"를 참조하십시오. • 그룹 편집 — 사용자 정의 그룹에 대한 이름 및 주석을 변경할 수 있는 그룹 편집 페이지가 열립니다. 또한 그룹에서 장치를 추가 및 삭제할 수도 있습니다. 자세한 내용은 207페이지의 "그룹 페이지 편집 필드"를 참조하십시오. • 삭제 — 그룹을 영구적으로 삭제합니다. • 다이어그램 — 다이어그램 작성 페이지가 열립니다. 758페이지의 "다이어그램 작성"을 참조하십시오. • 공용/개인 그룹으로 변경 — 장치 그룹의 공용 및 개인 모드 간을 전환합니다.

동적 장치 그룹

동적 장치 그룹은 포함된 장치가 고정되지 않는다는 점을 제외하고 정적 장치 그룹과 매우 유사합니다. 시스템은 그룹과 연결된 미리 정의된 기준을 사용하여 쿼리를 수행함으로써 동적 장치 그룹에 포함되는 장치를 확인합니다.

정적 장치 그룹과 마찬가지로, 동적 장치 그룹은 장치 작업 실행 페이지, 검색 페이지, 다이어그램, 장치 소프트웨어 보고서 등을 비롯한 모든 그룹 목록에 표시됩니다. 다음 표에서는 정적 및 동적 장치 그룹 간의 차이를 알기 쉽게 보여 줍니다.

정적 장치 그룹	동적 장치 그룹
장치를 선택하여 만듭니다. 177페이지의 "새 그룹 페이지 필드" 를 참조하십시오.	검색 기준 및/또는 규칙 집합을 정의하여 만듭니다. 최대 검색 기준은 10개입니다. 동적 장치 그룹 생성 단계는 아래와 같습니다.
수동으로 추가 또는 제거하지 않으면 장치는 고정 상태로 남아 있습니다.	네트워크 및/또는 장치 구성 이벤트가 발생할 때 장치가 변경될 수 있습니다.
그룹에서 장치를 수동으로 제거할 수 있습니다.	그룹에서 장치를 수동으로 제거할 수 없습니다.

참고: 동적 그룹은 그룹 계층에서 하위 그룹만 될 수 있습니다. 또한 장치가 속하는 그룹을 지정할 수 있는 장치 편집 페이지나 장치 가져오기 작업 페이지에는 동적 그룹이 나타나지 않습니다.

동적 장치 그룹 생성

동적 장치 그룹은 다음 두 가지 방법으로 생성할 수 있습니다.

- 장치 검색 결과 페이지 사용
- 새 그룹 페이지 사용

장치 검색 페이지를 사용하여 동적 그룹을 생성하려면

1. 보고서 아래의 메뉴 모음에서 검색 대상을 선택하고 장치를 클릭합니다. 장치 검색 페이지가 열립니다.
2. 검색 기준을 입력합니다. 예를 들어 장치 공급업체 필드를 선택하고 Cisco를 입력합니다.
3. 검색 버튼을 클릭합니다. 장치 검색 결과 페이지가 열리고 모든 Cisco 장치가 표시됩니다.
4. 노란색 "검색 기준" 섹션이 보일 때까지 페이지 아래로 스크롤합니다.
5. 동적 그룹의 이름을 입력하고 "동적 그룹으로 작성" 옵션을 선택한 후 그룹 생성 버튼을 클릭합니다.
6. 장치 검색 결과 페이지 맨 위에 "새 장치 그룹이 성공적으로 생성됨: <이름>" 메시지가 표시됩니다.

새 그룹 페이지를 사용하여 동적 그룹을 생성하려면

1. 장치 아래의 메뉴 모음에서 새로 만들기를 선택하고 장치 그룹을 클릭합니다. 새 그룹 페이지가 열립니다.
2. 그룹 이름 필드에 동적 그룹의 이름을 입력합니다.
3. 필요에 따라 설명, 파티션 이름(해당되는 경우), 소유자, 상위 장치 그룹 및 장치 필드를 작성합니다. 이러한 필드에 대한 자세한 내용은 [177페이지의 "새 그룹 페이지 필드"](#)를 참조하십시오.
4. 장치 필드 아래로 스크롤합니다.
5. "동적 장치 집합(동적 그룹)을 정의하려면 필터를 사용하십시오" 옵션을 클릭합니다. 다음을 수행할 수 있게 화면이 변경됩니다.
 - 하나 이상의 검색 기준(예: 장치 IP, 도메인 이름, 정책 준수 등)을 사용하여 검색을 구성합니다. (**참고:** 동적 장치 그룹을 생성하기 위한 검색 필터 및/또는 규칙을 하나 이상 지정해야 합니다.)
 - 필요한 경우 부울 식(그리고/또는)을 사용하여 검색을 필터링합니다.
 - 장치 그룹으로 검색을 제한합니다. 이 옵션을 사용하면 다른 그룹을 기반으로 동적 그룹을 생성할 수 있습니다.
6. 동적 장치 그룹을 정의한 후에 저장 버튼을 클릭합니다. 새 동적 장치 그룹이 표시됩니다.

동적 장치 그룹을 정적 장치 그룹으로 변경하려면 그룹 편집 페이지를 열고 장치 필드 아래로 스크롤합니다. "고정 장치 집합(정적 그룹)을 선택하려면 장치 선택기를 사용하십시오" 옵션을 클릭합니다. 동적 장치 그룹을 정적 장치 그룹으로 변경하면 현재 장치가 새 정적 장치 그룹의 구성원이 됩니다.

동적 장치 그룹 계산

동적 장치 그룹 구성원은 다음과 같은 경우에 계산됩니다.

- 먼저 동적 장치 그룹을 구성합니다.
- 동적 장치 그룹 페이지에서 "장치 목록 업데이트" 링크를 클릭합니다.
- 백그라운드 프로세스가 모든 동적 장치 그룹을 주기적으로 다시 계산합니다.
- 미리 정의한 장치 변경 이벤트가 발생합니다.

동적 그룹 자동 재계산 및 이벤트 구동 재계산 매개 변수에 대한 자세한 내용은 [67페이지](#)의 "서버"를 참조하십시오.

장치 선택기

장치 선택기에는 두 가지 옵션이 포함됩니다.

- 장치 선택 – 그룹 트리를 쉽게 탐색하여 다양한 용도(예를 들면 장치에서 작업을 예약하는 경우)로 장치를 선택할 수 있습니다.
- 장치 그룹 선택 – 그룹 트리를 쉽게 탐색하여 다양한 용도(예를 들면 장치 그룹을 편집하는 경우)로 장치를 선택할 수 있습니다.

이러한 각각의 선택기는 장치와 장치 그룹을 탐색할 수 있는 창을 엽니다.

장치 선택

기본적으로 장치 선택기가 닫혀 있습니다. IP 주소, 호스트 이름 또는 장치 그룹 이름의 처음 몇 자를 입력하여 고정 장치 또는 장치 그룹을 빠르게 검색할 수 있습니다. 첫 글자를 입력하자마자 검색 결과가 즉시 표시됩니다.

자동 완성 목록에서 선택하려면

- 단일 항목의 경우 – 항목을 클릭하거나 아래쪽 화살표를 눌러서 항목을 강조 표시한 다음 Enter 키를 누릅니다.
- 여러 항목의 경우 – Ctrl 키를 누른 다음 원하는 항목을 선택하고 Enter 키를 누릅니다.

자동 완성 목록에서 선택을 취소하려면

- 단일 항목의 경우 – 항목 오른쪽에 표시된 빨간색 X 아이콘을 클릭합니다.
- 여러 항목의 경우 – Ctrl 키를 누르고 원하는 항목을 선택한 다음 항목 오른쪽에 표시되는 빨간색 X 아이콘을 클릭합니다.

파티션 이름(예: Default Site:10.255.1.10)에 접두사를 지정하여 검색하려는 경우 전체 이름이 입력될 때까지 자동 완성 목록에 파티션 이름만 표시됩니다. 예를 들어 Def를 입력하는 경우 전체 파티션 이름을 입력할 때까지 전체 파티션 이름(Default Site:10.255.1.10)을 볼 수 없습니다.

장치 그룹 선택

장치 그룹을 검색하려면 돋보기 아이콘을 클릭합니다. 장치 그룹 선택기 창이 열리고 인벤토리 장치 그룹이 첫 번째로 나열되어 있는 장치 그룹 계층이 표시됩니다.

기본적으로 장치 그룹 계층은 축소되어 있습니다. 더하기(+) 기호를 클릭하여 계층을 확장할 수 있습니다. 장치 그룹을 한 번 클릭하면 해당 그룹 내 모든 장치가 표시됩니다. 표시할 수 있는 항목 수가 더 많으면 수직 스크롤 막대가 표시됩니다.

장치 그룹의 모든 장치 목록을 보려면 그룹 그룹의 이름을 클릭합니다. 다음 정보가 표시됩니다.

필드	설명/작업
필터	장치 그룹을 신속히 검색할 수 있습니다.
호스트 이름	장치의 호스트 이름을 표시합니다.
장치 IP	장치의 IP 주소를 표시합니다.
장치 공급업체	장치 제조업체 이름이 표시됩니다.
장치 모델	지정된 장치 모델이 표시됩니다.
파티션	장치 그룹이 속해 있는 파티션을 표시합니다. 파티션은 NA 객체 집합입니다. 파티션은 권한 모델, 그룹 계층, NA 코어의 장치 분산 및 네트워크 다이어그램과 함께 사용될 수 있습니다. 자세한 내용은 201페이지의 "파티션" 을 참조하십시오.

장치 선택기 버튼

다음 장치 선택기 버튼을 사용합니다.

- 적용 버튼 – 하나 이상의 장치 또는 장치 그룹을 선택하려면 화면에서 원하는 항목 (강조 표시됨)을 클릭하고 "적용" 버튼을 클릭합니다. 선택한 항목이 추가되고 장치 선택기 또는 장치 그룹 선택기 창이 열린 상태로 유지됩니다. 선택한 장치 또는 장치 그룹 중 하나가 허용되지 않는 경우 적용 버튼이 회색으로 표시됩니다.

- 확인 버튼 – 현재 선택한 항목을 추가하고 장치 선택기 또는 장치 그룹 선택기 창을 닫습니다. 선택한 장치 또는 장치 그룹 중 하나가 허용되지 않는 경우 확인 버튼이 회색으로 표시됩니다.
- 취소 버튼 – 변경 내용을 저장하지 않고 장치 선택기 또는 장치 그룹 선택기 창을 닫습니다.

참고: 장치 선택기 및 장치 그룹 선택기 창의 맨 위 오른쪽 모서리에는 크기 조정 아이콘이 있습니다. 각각의 최대화 및 원래 크기로 복원 옵션을 사용할 수 있습니다.

장치 그룹 보기

처음에는 장치 그룹 페이지에 하나의 시스템 그룹, 즉 인벤토리 그룹이 포함됩니다. 인벤토리 그룹에는 모든 장치가 포함되어 있습니다. 그러나 사용자가 생성하는 사용자 정의 그룹도 이 페이지에 나타납니다.

보기 작업 링크는 선택한 장치 그룹에 포함된 장치를 표시합니다. 장치는 장치 그룹이 리프 장치 그룹인 경우 해당 장치 그룹의 직접 하위 장치일 수 있으며, 장치 그룹이 상위 장치 그룹인 경우 하위 그룹의 하위 장치일 수 있습니다.

이전 NA 릴리스에서는 장치 그룹의 이름을 클릭하여 리프 그룹의 장치를 보는 것만 가능했습니다. 이제는 보기 작업 링크를 클릭하여 상위 구조 내 상위 그룹 관점에서 장치 목록을 볼 수 있습니다. 이 기능을 사용하면 원하는 상위 그룹의 관점에서 장치를 일괄적으로 편집할 수 있습니다.

예를 들면 시/도, 국가 및 도시별로 장치 그룹이 구성된 경우 이제는 시/도 수준에서 모든 장치에 대해 일괄 편집을 수행할 수 있지만, 예전에는 도시 수준에서만 장치에 대한 일괄 편집을 수행할 수 있었습니다. 장치 그룹 추가에 대한 자세한 내용은 [175페이지의 "장치 그룹 추가"](#)를 참조하십시오.

장치 그룹을 보려면 장치 아래의 메뉴 모음에서 그룹을 클릭합니다. 장치 그룹 페이지가 열립니다. 공용 장치 그룹은 모든 사용자에게 표시됩니다. 개인 장치 그룹은 그룹 소유자 및 NA 관리자에게만 표시됩니다.

장치 그룹 페이지 필드

필드	설명/작업
새 그룹 링크	새 장치 그룹을 생성할 수 있는 새 그룹 페이지가 열립니다. 자세한 내용은 175페이지의 "장치 그룹 추가" 를 참조하십시오.
새 상위 그룹 링크	새 상위 그룹을 추가할 수 있는 새 상위 그룹 페이지를 엽니다. 자세한 내용은 178페이지의 "새 상위 그룹 페이지 필드" 를 참조하십시오.
그룹 이름	장치 그룹의 사용자 정의 이름을 표시합니다. 상위 그룹은 다른 상위 그룹의 하위가 아닌 이상 들여쓰기로 표시되지 않습니다. 상위 그룹에 속해 있는 그룹은 상위 아래에 들여쓰기로 표시됩니다. 그룹 이름을 클릭하면 장치 그룹에 대한 자세한 정보를 볼 수 있는 장치 그룹 페이지가 열립니다. 자세한 내용은 188페이지의 "장치 그룹 세부사항 페이지 필드" 를 참조하십시오.
설명	그룹에 대한 설명이 표시됩니다.
장치 수	그룹에 있는 장치의 수를 표시합니다.
소유자	장치 그룹을 생성한 사용자 이름을 표시합니다.
공유	그룹이 공용 그룹인지 또는 개인 그룹인지가 표시됩니다. 공용 장치 그룹은 모든 사용자가 볼 수 있지만 개인 장치 그룹은 그룹의 소유자와 NA 관리자만 볼 수 있습니다.
작업	인벤토리 그룹에 대한 작업 필드는 사용자가 그룹 이름을 선택할 때까지 비어 있습니다. 사용자 정의 그룹은 다음 작업을 표시합니다. <ul style="list-style-type: none"> • 보기 — 선택한 장치 그룹에 포함된 장치를 표시합니다. 장치는 이 장치가 리프 장치 그룹인 경우 이 장치 그룹의 직접 하위 항목이거나 장치 그룹이 상위 장치 그룹인 경우 하위 장치 그룹의 하위 항목일 수 있습니다. • 편집 — 사용자 정의 그룹에 대한 이름 및 주석을 변경할 수 있는 그룹 편집 페이지가 열립니다. 또한 그룹에서 장치를 추가 및 삭제할 수도 있습니다. 자세한 내용은 207페이지의 "그룹 페이지 편집 필드"를 참조하십시오. • 삭제 — 그룹을 영구히 삭제합니다. • 다이어그램 — 다이어그램 작성 페이지가 열립니다. 758페이지의 "다이어그램 작성"을 참조하십시오. • 공용/개인 그룹으로 변경 — 장치 그룹의 공용 및 개인 모드 간을 전환합니다.

장치 그룹의 트리에는 장치 그룹 파티션 멤버십을 표시하는 도구 설명이 포함되어 있습니다. 이 정보를 사용하여 중복 장치 그룹 이름 간에 차별화하거나 장치 그룹 파티션을 설정할 수 있습니다.

예를 들어 이러한 파티션에 대해 보기 권한이 설정되어 있는 여러 파티션 및 여러 사용자 그룹을 만들려는 경우 장치 그룹 페이지를 볼 때 두 장치 그룹이 동일한 이름일 수 있습니다. 툴팁을 사용하여 장치 그룹이 속하는 파티션 이름(예: 파티션1: 에지 라우터와 파티션2: 에지 라우터)을 볼 수 있습니다. 파티션 구성에 대한 자세한 내용은 [201페이지](#)의 "파티션"을 참조하십시오.

장치 그룹에 대한 자세한 정보를 보려면

1. 장치 아래의 메뉴 모음에서 그룹을 클릭합니다. 장치 그룹 페이지가 열립니다.
2. 자세한 정보를 보려는 그룹 이름을 클릭합니다. 장치 그룹 세부사항 페이지가 열립니다.

장치 그룹 세부사항 페이지 필드

필드	설명/작업
그룹 링크	모든 장치 그룹을 볼 수 있는 장치 그룹 페이지가 열립니다. 자세한 내용은 187페이지 의 "장치 그룹 페이지 필드"를 참조하십시오.
새 장치 링크	새 장치를 추가할 수 있는 새 장치 페이지가 열립니다. 자세한 내용은 137페이지 의 "장치 추가"를 참조하십시오.
새 장치 그룹 링크	새 그룹을 추가할 수 있는 새 그룹 페이지가 열립니다. 자세한 내용은 175페이지 의 "장치 그룹 추가"를 참조하십시오.
새 상위 그룹 링크	새 상위 그룹을 추가할 수 있는 새 상위 그룹 페이지를 엽니다. 자세한 내용은 178페이지 의 "상위 그룹 추가"를 참조하십시오.
그룹 편집 링크	장치 그룹을 편집할 수 있는 그룹 편집 페이지가 열립니다. 자세한 내용은 207페이지 의 "그룹 페이지 편집 필드"를 참조하십시오.
장치 목록 업데이트 링크	페이지를 새로 고치고 장치 그룹 멤버십을 다시 계산합니다.

필드	설명/작업
현재 작업 그룹	현재 작업 그룹이 드롭다운 메뉴에 표시됩니다. 드롭다운 메뉴에서 다른 그룹을 선택할 수 있습니다.
활성 장치만 나열 확인란	이 옵션을 선택하면 장치 목록이 능동적으로 관리되는 장치로 제한됩니다.
그룹에서 실행할 작업	이 그룹에서 실행할 작업을 드롭다운 메뉴에서 선택할 수 있습니다. 작업 실행에 대한 자세한 내용은 358페이지의 "작업이란?" 을 참조하십시오.
확인란	<p>왼쪽의 확인란을 사용하여 장치를 관리할 수 있습니다. 장치를 선택한 후에 작업 드롭다운 메뉴를 클릭합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> •활성화 — 선택한 장치를 관리하도록 NA에 지시합니다. •비활성화 — 선택한 장치를 관리하지 않도록 NA에 지시합니다. •일괄 편집 — 선택한 모든 장치에 대한 드라이버를 할당하고 연결 방법을 설정할 수 있는 장치 일괄 편집 페이지가 열립니다. 자세한 내용은 209페이지의 "장치 일괄 편집 페이지 필드"를 참조하십시오. •다이어그램 — 다이어그램 작성 페이지가 열립니다. 758페이지의 "다이어그램 작성"을 참조하십시오. •삭제 — 선택한 장치를 삭제합니다. •장치 그룹에 대해 실행할 작업을 선택합니다. <p>인접한 선택 드롭다운 메뉴를 통해 모든 장치를 선택하거나 선택 취소할 수 있습니다.</p>
호스트 이름	장치의 호스트 이름을 표시합니다. 호스트 이름을 클릭하면 장치 및 해당 구성 내역에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
장치 IP	장치의 IP 주소를 표시합니다. 빨간색으로 표시된 장치는 마지막 스냅샷 시도에서 실패한 장치입니다. 비활성 장치는 IP 주소 옆의 아이콘으로 표시됩니다. IP 주소를 클릭하면 장치 및 해당 구성 내역에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
장치 공급업체	장치 제조업체 이름이 표시됩니다.
장치 모델	지정된 장치 모델이 표시됩니다.

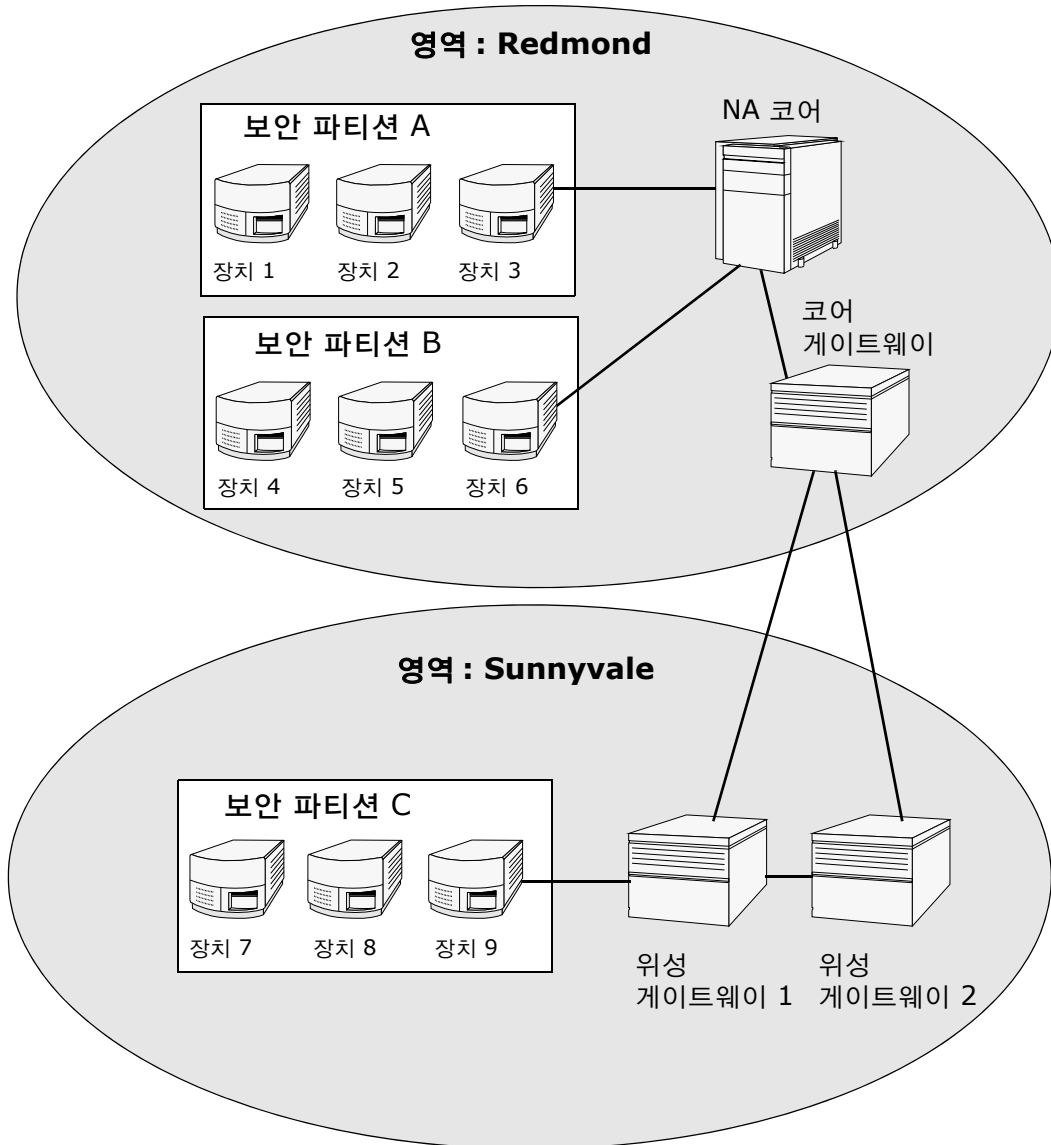
필드	설명/작업
파티션	장치가 속해 있는 파티션을 표시합니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다.)
마지막으로 변경된 시간	장치 구성이 마지막으로 변경된 날짜와 시간을 표시합니다.
작업	선택할 수 있는 작업은 다음과 같습니다. <ul style="list-style-type: none">• 편집 — 이 장치에 대한 정보를 편집할 수 있는 장치 편집 페이지를 엽니다. 자세한 내용은 146페이지의 "장치 편집 페이지 필드"를 참조하십시오.• 텔넷 — 텔넷 창을 엽니다.• SSH — SSH 창을 엽니다.• 구성 보기 — 최신 구성을 보고 주석을 추가할 수 있는 현재 구성 페이지를 엽니다.

장치 및 사용자 세분화

NA는 오버랩되는 IP 네트워크를 관리하고 장치(및 장치 그룹) 및 사용자(및 사용자 그룹)를 모두 파티셔닝하는 기능을 제공합니다. 이 섹션에서 사용되는 용어는 다음과 같습니다.

- **NA 코어** — 단일 NA 관리 엔진, 관련 서비스(Syslog 및 TFTP) 및 단일 데이터베이스입니다. NA 코어는 여러 파티션(장치 집합)을 관리할 수 있습니다. 여러 NA 코어를 분산 시스템 구성에 연결할 수 있습니다. 분산 시스템 설치 및 구성에 대한 자세한 내용은 *Network Automation 9.10 Multimaster Distributed System on Oracle User's Guide* 또는 *Network Automation 9.10 Distributed System on SQL Server User's Guide*를 참조하십시오.
- **보안 파티션** — 파티션의 일부인 NA 객체 집합입니다. NA 객체에는 장치, 사용자, 명령 스크립트, 장치 암호 규칙, 정책, 소프트웨어 이미지 등이 포함됩니다. 파티션은 권한 모델, 그룹 계층, NA 코어의 장치 분산 및 네트워크 다이어그램과 함께 사용될 수 있습니다.
- **기본 사이트 파티션** — 기본 파티션(이름이 지정된 기본 사이트)입니다. NA를 처음 사용하는 경우 파티션만 기본 파티션으로 사용할 수 있습니다. 기본 사이트 파티션은 시스템에서 게이트웨이 메시지를 통해 장치에 연결하는 데 필요합니다. 현재 NA에서 관리되는 모든 장치가 포함됩니다. 기본 사이트 파티션 이름은 바꿀 수 있지만 등록 정보는 수정할 수 없습니다. (**참고:** 이전 버전의 NA에서 여러 파티션을 구성한 경우 해당 파티션을 편집할 수 있습니다. 그러나 파티션을 추가하거나 삭제할 수는 없습니다.)
- **영역** — 네트워크 세그먼트. 일반적으로 영역은 고유한 IP 주소 집합으로 식별됩니다. 예를 들어 영역에는 10.255.111.128로 번호가 매겨진 두 개의 장치가 포함될 수 없습니다. 대신 장치는 별도의 영역으로 분리되어야 합니다. 파티션은 관리하는 NA 코어와 같은 영역에 있을 필요가 없습니다. 영역은 여러 파티션을 포함할 수 있는 큰 부분입니다. 영역에는 NA 코어가 포함될 필요가 없지만 일반적으로 NA 코어는 로컬 영역의 장치를 관리합니다. NA 코어는 게이트웨이 메시지를 통해 원격 영역의 장치를 관리할 수 있습니다. 게이트웨이 메시지는 영역 간에 IP 트래픽을 프록시하는 데 사용됩니다.

다음 그림에서는 여러 보안 파티션 구성의 다양한 구성 요소를 보여 줍니다. 그림에 나와 있는 것처럼 영역 및 파티션은 중복될 수 없으며 하나의 장치가 둘 이상의 영역에 있을 수 없습니다. 그러나 하나의 영역에 여러 파티션과 NA 코어가 있을 수 있습니다. 또한 하나의 영역에 여러 게이트웨이가 있을 수도 있습니다.



로컬 영역

장치가 로컬 영역에 있는 경우 NA는 NA 게이트웨이 메시지를 통과하지 않고 직접 장치에 연결합니다.

NA에서 장치에 연결할 때 해당 장치가 로컬 코어와 같은 영역에 있으면 NA는 장치에 직접 연결합니다. 그렇지 않으면 NA에서는 로컬 코어 게이트웨이에 연결하고 지정된 영역의 장치에 연결하도록 코어 게이트웨이에 요청하여 게이트웨이 메시지를 통해 장치에 연결합니다.

참고: 로컬 영역은 코어 영역의 별칭입니다. 장치가 코어 영역 또는 로컬 영역에 있는 경우 NA는 해당 장치에 직접 연결합니다.

로컬 영역 및 NAT 액세스

NA의 장치에 NAT IP 주소를 할당하면 NA는 NAT IP 주소를 사용하여 장치에 연결합니다. NAT IP 주소에는 연관된 영역이 있으므로 동일한 규칙이 적용됩니다. NAT IP 주소 영역이 로컬(코어의 영역 또는 정의된 로컬 영역)이면 직접 액세스할 수 있습니다. 그렇지 않으면 게이트웨이 메시지를 통해 액세스합니다.

NA에서 모든 NAT 액세스가 로컬이라고 가정할 경우 영역을 NAT IP 주소에 연결할 수 있으면 장치의 한 인터페이스가 다른 L3 클라우드에 있다는 사실을 NA L3 네트워크 다이어그램에 정확하게 반영할 수 있습니다.

로컬 영역 및 콘솔 액세스

NA의 장치에 대해 콘솔 서버가 정의되어 있으면 NA는 콘솔 서버를 사용하여 연결합니다. 콘솔 서버의 IP 주소에도 연관된 영역 이름이 있으며, 위의 NAT 액세스와 동일하게 처리됩니다.

로컬 영역 및 배스천 호스트 액세스

장치에 대해 배스천 호스트가 정의되어 있으면 NA는 배스천 호스트를 사용합니다. 배스천 호스트 IP 주소에는 영역을 할당할 수 없습니다. NA는 배스천 호스트에 항상 로컬로 액세스합니다. 따라서 원격 장치에 대해 배스천 호스트 액세스가 가능한 경우 게이트웨이 메시지를 사용하지 않고 로컬 영역을 사용하여 다양한 원격 영역의 장치를 관리할 수 있습니다. 배스천 호스트 액세스에서는 장치에 대한 CLI 액세스만 허용합니다. 따라서 SNMP 및 TFTP를 사용할 수 없습니다. TFTP를 사용할 수 없으므로 배스천 호스트 액세스를 사용하는 장치에 대해서는 소프트웨어 업데이트를 사용할 수 없습니다.

로컬 영역 추가

로컬 영역을 추가하려면

1. `$HPNA/jre/adjustable_options.rcx` 파일을 편집합니다. 여기서 `$HPNA`는 NA 설치의 루트(일반적으로 Windows의 `C:\Rendition`)입니다.
2. 다음과 같이 `gateway/mesh/local_realms`에 대한 주석을 제거하고 로컬 영역 이름을 추가합니다.

```
<!--Gateway Mesh: define realms that do not use the Gateway Mesh-->
<array name="gateway/mesh/local_realms">
  <value>Local Realm 1</value>
  <value>Local Realm 2</value>
</array>
```

3. NA를 다시 시작합니다.

오버랩되는 IP 네트워크

모든 파티션에는 관리하는 NA 코어가 있어야 합니다. 그러나 앞의 그림에 나와 있는 것처럼 관리하는 NA 코어는 해당 코어가 관리 중인 파티션과 같은 영역에 포함될 필요가 없습니다.

장치에 액세스할 때 NA 코어가 동일한 영역(예: 장치 3)에 있는 경우 NA에서는 해당 장치에 직접 연결하여 관리합니다. NA 코어가 관리 중인 장치와 다른 영역(예: 장치 9)에 있는 경우 NA에서는 해당 영역의 위성 게이트웨이 1에 연결한 후 다른 게이트웨이를 통해 장치 9와 통신합니다.

게이트웨이 모음을 *게이트웨이 메시*라고 합니다. NA 코어와 같은 영역에 있는 게이트웨이를 *코어 게이트웨이*라고 하고 NA 코어가 없는 영역의 게이트웨이를 *위성 게이트웨이*라고 합니다. 게이트웨이 메시지를 통해 NA 코어는 다양한 영역의 장치를 관리할 수 있습니다. 게이트웨이 메시지 구성에 대한 자세한 내용은 [56페이지의 "장치 액세스 페이지 필드"](#)를 참조하십시오.

HP 게이트웨이의 설치와 구성은 중복되거나 오버랩되는 IP 주소를 사용하는 장치 및 네트워크를 관리하려는 경우에만 필요합니다. HP 게이트웨이는 독립 실행형 제품이며 NA에 번들로 묶여 있지 않습니다.

다음과 같은 여러 항목을 구성할 수 있습니다.

- 영역 — 오버랩되는 IP 주소를 사용할 수 있도록 합니다. 즉, 같은 IP 주소를 갖는 둘 이상의 장치를 사용할 수 있습니다.
- 같은 영역의 보안 파티션 — 사용자의 보기 액세스 권한을 같은 영역에 있는 장치로 제한할 수 있도록 합니다. 파티션이 삭제되면 모든 객체가 기본 파티션(이름이 지정된 기본 사이트)에 자동으로 배치됩니다.
- 같은 영역의 게이트웨이 — 한 게이트웨이가 실패할 경우 가동 시간을 향상시킬 수 있습니다.
- 같은 영역의 NA 코어 — NA 시스템의 장치 정보에 대한 액세스를 공유할 수 있도록 합니다. Oracle의 NA 분산 시스템은 게이트웨이 메시의 각 NA 코어 데이터를 다른 모든 NA 코어에서 액세스할 수 있는 다중 마스터 시스템입니다. 따라서 NA 코어가 중단된 경우 중복 데이터 및 장애 조치가 허용될 수 있습니다. 자세한 내용은 *Network Automation 9.10 Distributed System on Oracle User's Guide*를 참조하십시오.

HP 게이트웨이 설정

이 섹션에서 사용되는 용어는 다음과 같습니다.

- **게이트웨이** — IP 트래픽을 다른 게이트웨이로 라우팅하는 응용 프로그램
- **게이트웨이 메시지** — 서로 간에 트래픽을 라우팅하는 게이트웨이 모음
- **코어 게이트웨이** — NA 코어와 같은 영역에서 실행되는 게이트웨이

- **위성 게이트웨이** — NA 코어가 없는 영역에서 실행되는 게이트웨이
- **IP 공간** — 오버랩되는 IP 주소가 없는 하나 이상의 영역

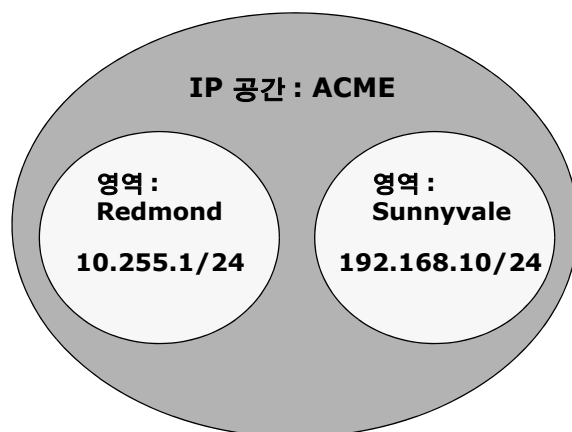
NA와 함께 HP 게이트웨이를 사용하면 오버랩되는 IP 주소(예: 같은 IP 주소를 갖는 여러 장치)를 지원할 수 있습니다. 또한 관리되는 장치와 같은 LAN에 NA 원격 에이전트를 설치하여, 장치를 로컬로 관리하는 데 Syslog 및 TFTP를 사용할 수 있습니다. 자세한 내용은 [472페이지의 "원격 에이전트 배포 페이지 필드"](#)를 참조하십시오.

참고: 같은 LAN에 많은 NA 사용자가 있는 경우 NA 코어(NA 다중 마스터 분산 시스템)가 해당 LAN의 NA 원격 에이전트에 적합할 수 있습니다. 자세한 내용은 *Network Automation 9.10 Multimaster Distributed System on Oracle User's Guide*를 참조하십시오.

일반적으로 HP 게이트웨이를 사용하여 NA 코어는 하나 이상의 NAT 사용 장치 또는 방화벽 이면에 있는 서버를 관리할 수 있습니다. 이 작업은 게이트웨이 인스턴스 사이에 SSH 터널과 같은 지속형 TCP 터널을 생성하여 수행합니다. 또한 HP 게이트웨이는 대역폭 관리를 제공합니다. 이러한 기능은 터널이 저대역폭 연결을 통해 전송되며 대역폭의 사용을 최대 연결 속도보다 작은 고정 크기로 제한해야 하는 경우에 중요합니다.

참고: 위성 구성 설치에 대한 자세한 내용은 *HP Network Automation 9.10 Satellite User's Guide*를 참조하십시오.

HP SA(HP Server Automation)는 각 설치에 게이트웨이 메시지를 사용합니다. 그러나 NA는 오버랩되는 IP 주소를 처리해야 하는 경우에만 게이트웨이 메시지를 사용합니다. NA/HP SA 통합을 사용하면 영역은 아래와 같이 오버랩되는 IP 주소가 없는 네트워크 모음이 될 수 있습니다. 따라서 IP 공간을 오버랩되는 IP 주소가 없는 하나 이상의 영역으로 정의할 수 있습니다.



NA 코어는 NAT 사용 환경에서 다른 IP 공간에 있을 수 있습니다. NA 코어가 같은 IP 공간에 있는 경우 NA 코어가 관리할 장치에 위상학적으로 가깝다면, 게이트웨이 메시지를 통과하지 않고 장치와 직접 통신하는 것이 더 효율적입니다. WAN 사용량을 줄이려면 NA 위성을 관리할 장치와 위상학적으로 가깝게 배치하는 것이 더 나을 수 있습니다.

HP 게이트웨이는 다음 플랫폼에서 지원됩니다.

- RedHat-Linux-3AS 및 4AS
- SuSE-Linux-9ES
- SunOS-5.9 및 5.10

HP 게이트웨이를 설정하려면 다음을 설치해야 합니다.

1. 각 NA 코어에 대한 코어 게이트웨이
2. 각 원격 영역에 대한 위성 게이트웨이

참고: HP SA 및 NA 간 게이트웨이를 공유할 경우에는 HP SA 설치 프로그램을 사용해야 합니다. NA 게이트웨이 설치 프로그램은 HP SA에 사용되는 게이트웨이를 설치할 수 없습니다. NA 게이트웨이 설치 프로그램은 NA 전용 게이트웨이 메시용으로 사용됩니다.

코어 게이트웨이 설치, 위성 게이트웨이 설치 및 게이트웨이 메시지를 사용하도록 NA 구성 작업을 위한 단계별 지침은 *HP Network Automation 9.10 Satellite User's Guide*를 참조하십시오. 게이트웨이 메시 구성에 대한 자세한 내용은 **56페이지의 "장치 액세스 페이지 필드"**를 참조하십시오.

게이트웨이 목록 페이지 필드

게이트웨이 목록 페이지는 현재 구성된 게이트웨이를 표시하며 게이트웨이 정보를 편집할 수 있도록 합니다. 자세한 내용은 **200페이지의 "게이트웨이 편집 페이지 필드"**를 참조하십시오.

게이트웨이 목록 페이지를 열려면 관리 아래의 메뉴 모음에서 게이트웨이를 클릭합니다. 게이트웨이 목록 페이지가 열립니다.

참고: 게이트웨이 메시지를 설치한 경우 각 위성 게이트웨이 호스트에 NA 원격 에이전트를 설치해야 합니다. 코어 게이트웨이가 있는 호스트에는 NA 원격 에이전트를 설치하지 마십시오.

필드	설명/작업
원격 에이전트 배포 링크	NA 원격 에이전트를 배포할 수 있는 원격 에이전트 배포 페이지가 열립니다. 자세한 내용은 472페이지의 "원격 에이전트 배포 페이지 필드" 를 참조하십시오.
위성 모니터 링크	모니터 상태를 볼 수 있는 모니터 세부사항 페이지가 열립니다.
IP 공간	IP 공간 이름이 표시됩니다. IP 공간은 오버랩되는 IP 주소가 없는 하나 이상의 영역입니다.

필드	설명/작업
영역	영역 이름을 표시합니다. 영역 이름은 게이트웨이에서 반환됩니다. 영역 이름은 게이트웨이가 설치될 때 설정되며 NA에서 수정할 수 없습니다. 영역 이름을 변경하려면 게이트웨이를 다시 설치해야 합니다. 자세한 지침은 <i>Network Automation 9.10 Satellite User's Guide</i> 를 참조하십시오.
게이트웨이	게이트웨이 이름이 표시됩니다. 게이트웨이 이름은 게이트웨이가 설치될 때 설정되며 NA에서 수정할 수 없습니다. 자세한 지침은 <i>Network Automation 9.10 Satellite User's Guide</i> 를 참조하십시오.
호스트	게이트웨이가 설치된 시스템의 호스트 이름 또는 IP 주소가 표시됩니다. 게이트웨이 호스트에 여러 IP 주소가 있으면 게이트웨이 호스트의 이 주소가 사용됩니다. 호스트 IP 주소는 둘 이상의 게이트웨이가 같은 영역에 설치되어 있는 경우에만 중요합니다. 참고: 중복성을 위해 같은 영역에 여러 위성 게이트웨이를 설치할 수 있습니다.
파티션	적용 가능한 경우 영역 이름과 연결된 파티션 이름이 표시됩니다. 자세한 내용은 201페이지의 "파티션" 을 참조하십시오.
코어	다중 마스터 분산 시스템 환경에서 코어 이름은 코어 편집 페이지에서 설정됩니다. 코어 편집 페이지의 영역 이름이 게이트웨이의 영역 이름과 일치하면 게이트웨이 목록 페이지에 해당 코어의 코어 이름이 표시됩니다. 코어 편집 페이지에 대한 자세한 내용은 <i>Network Automation 9.10 Multimaster Distributed System on Oracle Users Guide</i> 를 참조하십시오.
에이전트	위성 게이트웨이에 대한 NA 원격 에이전트 이름이 표시됩니다. NA 원격 에이전트 이름은 게이트웨이 편집 페이지에서 변경할 수 있습니다. 게이트웨이 메시지를 설치한 경우 각 위성 게이트웨이 호스트에 NA 원격 에이전트를 설치해야 합니다. 설치된 NA 원격 에이전트가 없으면 에이전트 열은 비어 있습니다. 자세한 내용은 472페이지의 "원격 에이전트 배포 페이지 필드" 를 참조하십시오.
작업	다음 옵션 하나만 제공됩니다. <ul style="list-style-type: none"> • 편집 — 게이트웨이 편집 페이지가 열립니다. 200페이지의 "게이트웨이 편집 페이지 필드"를 참조하십시오.

게이트웨이 편집 페이지 필드

NA에서는 영역 이름을 기반으로 IP 공간 이름을 자동으로 설정합니다. 그러나 두 영역이 같은 IP 공간에 있으며 이 영역을 L3 다이어그램에 올바르게 작성하려는 경우 게이트웨이를 편집하여 IP 공간 이름을 설정할 수 있습니다.

게이트웨이 편집 페이지를 열려면 게이트웨이 목록 페이지의 작업 열에서 편집 옵션을 클릭합니다.

필드	설명/작업
게이트웨이	게이트웨이 이름이 표시됩니다. 게이트웨이 이름은 게이트웨이가 설치될 때 설정되며 NA에서 수정할 수 없습니다.
영역	영역 이름을 표시합니다. 영역 이름은 게이트웨이에서 반환됩니다. 영역 이름은 게이트웨이가 설치될 때 설정되며 NA에서 수정할 수 없습니다.
IP 공간	IP 공간 이름이 표시됩니다. IP 공간은 오버랩되는 IP 주소가 없는 하나 이상의 영역입니다. 새 IP 공간 이름을 입력합니다.
호스트	게이트웨이가 설치된 시스템의 호스트 이름 또는 IP 주소가 표시됩니다. 새 호스트 이름 또는 IP 주소를 입력합니다.
위성	NA 코어가 없는 영역에서 실행되는 위성 게이트웨이가 표시됩니다. 적용 가능한 경우 위성 게이트웨이 이름을 입력합니다.

파티션

파티션은 NA 객체 집합입니다. NA 객체에는 장치, 사용자, 명령 스크립트, 장치 암호 규칙, 정책, 소프트웨어 이미지 등이 포함됩니다. 파티션은 권한 모델, 그룹 계층, NA 코어의 장치 분산 및 네트워크 다이어그램과 함께 사용될 수도 있습니다.

파티션은 항상 공용 그룹입니다. 장치 그룹 계층 내에 배치될 수 있습니다. 파티션에 추가되는 객체(예: 장치, 장치 그룹, 사용자 또는 사용자 그룹)는 이전에 속해 있던 파티션에서 자동으로 제거됩니다.

파티션이 삭제되면 모든 객체가 기본 파티션(이름이 지정된 기본 사이트)에 자동으로 배치됩니다. 따라서 모든 장치가 한 파티션에만 나타나게 됩니다. 명시적 파티션이 없는 IP 주소를 참조하면 기본 파티션이 사용됩니다. 파티션에 대한 자세한 내용은 [191페이지의 "장치 및 사용자 세분화"](#)를 참조하십시오.

NA에서는 다른 사용자를 볼 수 있는 사용자를 제한하는 기능을 제공합니다. 따라서 NA 시스템에서 사용자 및 사용자 그룹을 파티셔닝할 수 있습니다. 예를 들어 관리되는 서비스 공급자가 대규모 은행 기관을 관리하고 있는 경우 해당 관리되는 서비스 공급자를 위해 일하는 사용자를 은행 사용자가 볼 수 없도록 렌더링할 수 있습니다. 암호 규칙과 같은 사용자 객체를 파티셔닝하는 경우 모든 파티션에 대해 액세스 권한이 있는 사용자만 전역(또는 공유) 객체를 생성 및/또는 편집할 수 있습니다.

파티션 페이지 필드

파티션 페이지를 열려면 관리 아래의 메뉴 모음에서 보안 파티션을 클릭합니다. 파티션 페이지가 열립니다.

필드	설명/작업
파티션 기준	적용 가능한 경우 드롭다운 메뉴에서 파티션을 선택합니다. 기본 파티션은 이름이 지정된 사이트입니다. 기본 사이트 파티션은 시스템에서 게이트웨이 메시지를 통해 장치에 연결하는 데 필요합니다. 명시적 파티션이 없는 IP주소를 참조하면 기본 사이트 파티션이 사용됩니다.
이름 바꾸기 링크	파티션의 이름을 바꿀 수 있습니다. 이 이름은 새 장치, 새 장치 그룹 및 새 상위 장치 그룹 페이지에 표시됩니다. 자세한 내용은 138페이지의 "새 장치 페이지 필드" 를 참조하십시오.
새 파티션 링크	새 파티션을 생성할 수 있는 새 파티션 페이지가 열립니다. 자세한 내용은 203페이지의 "새 파티션 페이지" 를 참조하십시오.
파티션 이름	기본 사이트 파티션과 사용자가 생성한 다른 파티션을 표시합니다.
코어	분산 NA 설치에서 이 필드는 이 파티션의 장치를 관리하는 데 사용될 NA 코어를 지정합니다. 참고: NA 코어가 하나뿐이면 이 옵션이 표시되지 않습니다. 자세한 내용은 <i>Network Automation 9.10 Multimaster Distributed System on Oracle User's Guide</i> 또는 <i>Network Automation 9.10 Distributed System on SQL Server User's Guide</i> 를 참조하십시오.
영역 이름	드롭다운 메뉴에서 영역을 선택합니다. 이 필드는 이 파티션의 장치 및/또는 사용자가 속하는 영역을 지정합니다. 참고: 영역이 하나뿐인 경우(예: HP 게이트웨이 메시가 없는 경우)에는 이 옵션이 표시되지 않습니다. NA 코어가 같은 영역에 없는 경우 NA는 HP 게이트웨이 메시지를 사용하여 이 파티션의 장치에 연결합니다.
설명	파티션에 대한 설명이 제공됩니다.
장치 수	파티션에 포함된 장치의 수가 표시됩니다.
작업	<p>선택할 수 있는 작업은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 편집 — 파티션 편집 페이지가 열립니다. 자세한 내용은 204페이지의 "파티션 편집 페이지 필드"를 참조하십시오. • 삭제 — 파티션을 삭제할 수 있습니다. 기본 사이트 파티션은 삭제할 수 없습니다.

새 파티션 페이지

새 파티션을 추가하려면

1. 관리 아래의 메뉴 모음에서 보안 파티션을 클릭합니다. 파티션 페이지가 열립니다.
2. 페이지 맨 위에 있는 새 파티션 링크를 클릭합니다. 새 파티션 페이지가 열립니다.
3. 파티션 이름 및 설명을 입력합니다.
4. 장치 필드에서 장치 선택기를 사용하여 파티션에 넣을 장치를 선택합니다. 장치 선택기를 사용하는 방법에 대한 자세한 내용은 [183페이지의 "장치 선택기"](#)를 참조하십시오.

참고: 파티션은 장치 및 사용자에게 모두 적용할 수 있습니다. 파티션이 사용자에게 적용된 경우 사용자 편집 페이지에 파티션을 편집할 수 있는 옵션이 제공됩니다.

5. 저장 버튼을 클릭합니다. 파티션 페이지가 열리고 현재 파티션이 표시됩니다. *기본 사이트*라는 기본 파티션 하나가 있습니다. 이 파티션에는 네트워크에서 검색된 모든 장치가 포함되어 있습니다.

파티션 편집 페이지 필드

파티션을 편집하려면

1. 관리 아래의 메뉴 모음에서 보안 파티션을 클릭합니다. 파티션 페이지가 열립니다.
2. 편집하려는 파티션에 대해 작업 열에서 편집 옵션을 클릭합니다. 파티션 <이름> 편집 페이지가 열립니다. 다음 표에는 기본 사이트 파티션을 편집할 때 표시되는 필드가 나와 있습니다.

필드	설명/작업
파티션 이름	파티션 이름이 표시됩니다.
설명	파티션에 대한 설명이 제공됩니다.
코어	이 필드는 기본 파티션의 파티션에 대해서만 표시됩니다. 분산 NA 설치에서 이 필드는 이 파티션의 장치를 관리하는 데 사용될 NA 코어를 지정합니다. NA 코어에 대한 자세한 내용은 194페이지의 "오버랩되는 IP 네트워크" 를 참조하십시오.
영역 이름	이 필드는 기본 사이트 파티션의 파티션에 대해서만 표시됩니다. 드롭다운 메뉴에서 영역을 선택합니다. 이 필드는 이 파티션의 장치가 속하는 영역을 지정합니다. NA 코어가 같은 영역에 없는 경우 NA는 게이트웨이 메시지를 사용하여 이 파티션의 장치에 연결합니다.
장치	장치 선택기의 장치 상자에 장치 목록이 표시됩니다. 장치 선택기를 사용하는 방법에 대한 자세한 내용은 183페이지의 "장치 선택기" 를 참조하십시오. 파티션에 장치를 추가할 경우 해당 장치가 이전 파티션에서 자동으로 제거됩니다. 또한 파티션을 삭제하려면 먼저 모든 장치를 다른 파티션으로 이동해야 합니다. 그래야 해당 파티션이 삭제됩니다.

완료되면 저장 버튼을 클릭해야 합니다.

파티션에 장치 추가

파티션에 장치를 추가하려면

1. 관리 아래의 메뉴 모음에서 보안 파티션을 클릭합니다. 파티션 페이지가 열립니다.
2. 파티션 이름 열에서 편집할 파티션을 클릭합니다. 파티션 페이지가 열립니다. 이 페이지는 인벤토리 페이지와 비슷하여 파티션의 관리되는 장치 목록을 볼 수 있습니다. 그러나 페이지 맨 위에 그룹 편집과 파티션의 두 링크가 추가로 표시됩니다. 파티션 링크를 클릭하면 파티션 페이지로 돌아갑니다. (자세한 내용은 [241페이지](#)의 "인벤토리 페이지 필드"를 참조하십시오.)
3. 그룹 편집 링크를 클릭하면 파티션의 장치를 편집할 수 있는 파티션 편집 페이지가 열립니다. 완료되면 저장 버튼을 클릭해야 합니다. 파티션에 대한 자세한 내용은 [191페이지](#)의 "장치 및 사용자 세분화"를 참조하십시오.

필드	설명/작업
파티션 이름	파티션의 이름이 표시됩니다.
설명	파티션에 대한 설명이 표시됩니다.
장치	해당되는 경우 장치 목록이 표시됩니다. 장치 선택기를 사용하는 방법에 대한 자세한 내용은 183페이지 의 "장치 선택기"를 참조하십시오.

완료되면 저장 버튼을 클릭해야 합니다.

파티션 세부사항 보기

파티션은 장치 및/또는 사용자 집합이 될 수 있습니다. 장치 및/또는 사용자는 한 파티션에만 포함될 수 있습니다. 둘 이상의 파티션이 있으면 각 장치 및/또는 사용자가 유일한 단일 파티션에 위치합니다.

파티션 정보를 보거나 편집하려면

1. 관리 아래의 메뉴 모음에서 보안 파티션을 클릭합니다.
2. 정보를 원하는 파티션을 클릭합니다. 자세한 내용은 [241페이지의 "인벤토리 페이지 필드"](#)를 참조하십시오.

장치 그룹 편집

기존 장치 그룹을 편집하려면

1. 장치 아래의 메뉴 모음에서 그룹을 클릭합니다. 장치 그룹 페이지가 열립니다.
2. 편집할 장치 그룹에 대한 작업 열에서 편집을 클릭합니다. 그룹 편집 페이지가 열립니다. 완료되면 저장을 클릭해야 합니다.

그룹 페이지 편집 필드

필드	설명/작업
그룹 이름	장치 그룹의 이름이 표시됩니다.
설명	장치 그룹에 대한 설명이 표시됩니다.
파티션	드롭다운 메뉴에서 파티션을 선택합니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다.) 일반적으로 파티션이란 고유한 IP 주소를 갖는 장치의 그룹입니다. 단일 NA 코어로 여러 파티션을 관리할 수 있습니다. 설치된 NA 서버의 NA 코어는 단일 관리 엔진, 연관된 서비스 및 단일 데이터베이스로 구성되어 있습니다.
공유	편집할 장치 그룹이 공용인지 개인인지 또는 장치 그룹이 상위 그룹인지를 알려 줍니다. 리프 그룹을 편집하는 경우 장치 그룹에 상위 그룹이 있다는 정보가 표시됩니다.
상위 장치 그룹	드롭다운 메뉴에 상위 장치 그룹 이름이 표시됩니다.
장치	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 고정 장치 그룹(정적 그룹)을 선택하려면 장치 선택기를 사용하십시오. — 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. • 필터를 사용하여 동적 장치 집합(동적 그룹) 정의 — 하나 이상의 검색 기준을 사용하여 검색을 구성하거나, 부울 식(그리고/또는)을 사용하여 검색을 필터링하거나, 장치 그룹별로 검색을 제한할 수 있도록 화면이 바뀝니다.

필드	설명/작업
하위 장치 그룹	<ul style="list-style-type: none">• 모든 장치 그룹 — 모든 현재 장치 그룹 목록이 표시됩니다. 상위 그룹에 하위 항목으로 포함할 장치 그룹을 선택하고 복사 >>를 클릭합니다.• 이 그룹의 하위 — 상위 그룹에 하위 항목으로 할당된 장치 그룹 목록이 표시됩니다. 이 그룹에서 제거할 하위 그룹을 선택하고 << 제거를 클릭합니다.

장치 일괄 편집

일괄 편집 기능을 사용하여 장치 설정을 변경할 수 있습니다. 다음을 수행할 수 있습니다.

- 드라이버 할당
- 연결 명령(SNMP, SNMPv3, Telnet, SSH) 설정
- 전송 프로토콜(SCP, TFTP, FTP) 설정
- 배스천 호스트 정보 설정
- 마지막으로 사용한 암호 재설정
- ACL 구문 분석 설정

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다. 현재 관리되는 모든 장치 목록이 열립니다.
2. 하나의 일괄 운영으로 편집할 장치에 대한 확인란을 선택합니다.
3. 작업 드롭다운 메뉴에서 일괄 편집을 클릭합니다. 장치 일괄 편집 페이지가 열립니다. 완료되면 저장 버튼을 클릭해야 합니다.

장치 일괄 편집 페이지 필드

필드	설명/작업
장치	선택한 장치가 나열됩니다.
드라이버 할당	이 옵션을 선택한 경우 장치 배치에 할당할 드라이버를 선택합니다.

필드	설명/작업
연결 방법 설정	<p>이 옵션을 선택한 경우 다음 연결 방법 및 전송 프로토콜 중에서 일괄 편집을 위한 액세스 방법을 선택합니다.</p> <p>연결 방법:</p> <ul style="list-style-type: none"> •SNMP •SNMPv3(사용자 인증) — SNMPv3을 사용하는 경우 noAuthNoPriv(사용자 이름만), authNoPriv(사용자 이름, 인증 암호), authPriv(사용자 이름, 인증 및 암호화 암호) 옵션이 제공됩니다. 인증 방법에는 SHA(Secure Hash Algorithm) 및 MD5(Message Digest Algorithm)가 포함되며, 암호화 방법에는 DES(Data Encryption Standard), AES(Advanced Encryption Standard), AES192 및 AES256이 포함됩니다. •SNMPv1 또는 SNMPv2c(기본적으로 선택됨) •텔넷 •SSH — SSH1 또는 SSH2(기본값), SSH1만 또는 SSH2만 중에서 선택합니다. <p>전송 프로토콜(기본적으로 선택되어 있음):</p> <ul style="list-style-type: none"> •SCP •SFTP •FTP •TFTP
배스천 호스트 정보 설정	<p>이 옵션을 선택한 경우 다음 정보를 입력합니다.</p> <ul style="list-style-type: none"> •해당되는 경우 "텔넷 및 SSH 액세스의 경우 Unix 또는 Linux 배스천 호스트 사용" •배스천 호스트의 IP 주소 또는 호스트 이름 •배스천 호스트 사용자 이름 •배스천 호스트 암호 •암호 확인
마지막으로 사용한 암호 재설정	<p>이 옵션을 선택한 경우 마지막으로 사용한 암호를 재설정합니다.</p>

필드	설명/작업
ACL 구문 분석 설정	이 옵션을 선택한 경우 다음 옵션 중 하나를 선택할 수 있습니다. <ul style="list-style-type: none"> • 각 스냅샷을 사용하여 ACL을 구문 분석하고 저장함 • 각 스냅샷을 사용하여 ACL를 구문 분석하고 저장하지 않음
계층 레이어 설정	드롭다운 메뉴에서 계층 레이어를 선택합니다.
사용자 지정 서비스 유형 설정	이 옵션을 선택한 경우 서비스 유형을 선택합니다. 서비스 유형에서는 VoIP, BGP, MPLS 등을 지정할 수 있습니다. 이 값을 사용하여 장치의 용도를 식별할 수 있습니다. 이러한 값으로 장치 서비스에 태그를 지정하면 그룹(정적 또는 동적)에서 해당 서비스를 쉽게 검색하거나 볼 수 있습니다.
사용자 지정 데이터 필드 설정	이 옵션을 선택하면 장치에 할당된 사용자 지정 데이터를 편집할 수 있습니다. 자세한 내용은 699페이지의 "항상된 사용자 지정 필드 설정" 을 참조하십시오.

장치 드라이버 검색

검색을 수행하면 장치에 적합한 장치 드라이버를 찾습니다. 장치 드라이버는 각 장치에 대한 고유한 명령을 NA에서 이기종 네트워크 관리에 사용하는 범용 형식으로 변환합니다.

검색을 수행하면 SNMP 또는 텔넷/SSH를 사용하여 각각의 새 장치가 쿼리된 후 적절한 장치 드라이버가 할당됩니다. 이 프로세스가 실패하면 최근 작업 페이지에 결과가 표시됩니다. NA는 올바른 드라이버가 할당될 때까지 장치 구성을 능동적으로 관리할 수 없습니다. 드라이버 검색이 실패하면 드라이버를 수동으로 할당할 수 있습니다. 지원되는 장치에 대한 자세한 내용은 DRS(장치 릴리스 서비스) 설명서를 참조하십시오. DRS는 자동화된 새로운 드라이버 릴리스 및 전달 시스템입니다.

장치 드라이버 검색 프로세스를 시작하려면 장치 아래의 메뉴 모음에서 새 장치 작업을 선택하고 드라이버 검색을 클릭합니다. 새 작업 - 드라이버 검색 페이지가 열립니다. **375페이지의 "드라이버 검색 작업 페이지 필드"**를 참조하십시오. 장치 드라이버 검색은 소프트웨어 배포 작업에 의해서도 시작됩니다. 소프트웨어가 성공적으로 업로드되고, 장치가 재부팅되면(장치 재부팅 옵션을 선택한 경우) 장치 드라이버 검색 작업이 시작됩니다.

텔넷을 사용한 장치 액세스

NA에서 텔넷 및 SSH 세션을 시작하면 다음과 같은 이점을 얻을 수 있습니다.

- 로그인 간편화 — 사용자는 NA 계정을 사용하여 로그인합니다. NA에서 사용자의 권한을 확인합니다. 사용자는 NA CLI 명령을 입력하거나 장치에 직접 연결할 수 있습니다. 사용자는 한 세션 동안 한 장치에서 연결을 끊은 후 다른 장치에 연결할 수 있습니다. 사용자는 장치 공급업체, 종류 등에 관계없이 하나의 로그인만 기억하면 됩니다. 요청된 로그인 방법이 작동하지 않으면 NA는 백업 로그인 방법을 자동으로 시도합니다.
- 그룹 및 권한별 구성 — 장치를 그룹으로 구성하고 그룹별로 권한을 할당하면 사용자가 관심이 있고 권한이 있는 장치에만 액세스할 수 있게 됩니다.
- AAA가 없는 경우에도 구성 저장 — 텔넷/SSH 프록시는 수정된 구성, 인라인 주석, 변경을 수행한 사람을 저장할 수 있도록 합니다. 텔넷/SSH 프록시는 세션의 감사 로그를 구성에 자동으로 연결합니다.
- ACL 감소 — 장치당 하나의 ACL이 아니라 NA 서버에 대한 ACL(액세스 제어 목록)이 필요합니다.
- 보안 강화 — 네트워크에서 장치를 변경하는 사람을 파악하면 보다 쉽게 권한이 없는 사용자를 감지하고 무단 변경을 추적할 수 있습니다. 또한 NA를 사용하면 무단 변경 전에 저장된 안정적인 구성을 쉽게 배포할 수 있으므로 잠재적인 손상을 수정하고 네트워크 서비스를 빨리 복원할 수 있습니다.

뿐만 아니라 NA를 통해 텔넷/SSH 클라이언트를 장치에 연결하고 세션을 추적할 수 있습니다. 다른 클라이언트도 문제 없이 작동될 수 있지만, NA는 다음 클라이언트와의 연결에서 테스트되었습니다.

- SecureCRT
- Windows 텔넷
- Putty

텔넷/SSH 프록시 인터페이스와 관련된 다양한 관리 설정이 있습니다. 자세한 내용은 [85페이지의 "텔넷/SSH"](#)를 참조하십시오.

NA를 사용하여 텔넷 세션을 시작하려면 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다. 현재 관리되는 모든 장치 목록이 열립니다. 장치에 대한 작업 열에서 텔넷 옵션을 선택합니다. 장치에 로그인되며 텔넷 창에 장치 프롬프트가 표시됩니다.

참고: 컴퓨터에 JRE(Java Runtime Environment)가 아직 설치되어 있지 않으면, 브라우저는 텔넷이나 SSH를 처음 사용할 때 브라우저는 Sun 웹 사이트에서 다운로드를 시작합니다. 이것은 예상된 동작이며 JRE의 다운로드와 설치를 승인해야 합니다.

처음 NA에서 텔넷 또는 SSH 세션을 실행하면 HP에서 인증서를 다운로드할지 묻는 보안 창이 표시될 수 있습니다. 계속하려면 Grant always를 클릭합니다. 이렇게 하면 사용자가 HP의 콘텐츠를 신뢰하는지 확인합니다.

원하는 장치 명령을 입력할 수 있습니다. 완료되면 *quit*를 입력합니다. 이렇게 하면 텔넷 세션에서는 로그아웃되지만 NA 텔넷 프록시 세션에는 남아 있게 됩니다. 프록시 세션은 NA> 프롬프트를 사용합니다.

텔넷/SSH 프록시 세션에서 다른 장치에 연결하거나 NA CLI 명령을 입력할 수 있습니다. 페이지 맨 위에 있는 연결을 클릭하여 프록시 세션을 직접 시작할 수 있습니다.

참고: NA는 세션에서 모든 명령/응답 시퀀스를 분리하려고 하지만 이것은 간단한 작업이 아닙니다. 장치가 명령을 자동으로 완료하거나 장치가 추가 명령 매개 변수를 표시하면 명령/응답이 반드시 명확히 분리되지는 못합니다. 또한 이러한 종류의 대화식 바로 가기의 사용이 포함되는 세션은 고급 스크립트를 생성하는 데 적합하지 않을 수 있습니다.

SSH를 사용한 장치 액세스

SSH 세션을 시작하려면 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다. 현재 관리되는 모든 장치 목록이 열립니다. 장치에 대한 작업 열에서 SSH 옵션을 선택합니다. 원하는 장치 명령을 입력할 수 있습니다. 완료되면 *quit*를 입력합니다.

참고: 페이지 맨 위에 있는 연결을 클릭하여 프록시 세션을 직접 시작할 수 있습니다. SSH 프록시 세션에서 다른 장치에 연결하거나 NA CLI 명령을 입력할 수 있습니다.

텔넷/SSH 세션 나열

텔넷 및 SSH 세션을 나열하려면 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다. 현재 관리되는 모든 장치 목록이 열립니다. 장치를 클릭합니다. 해당 장치에 대한 장치 세부사항 페이지가 열립니다. 보기 드롭다운 메뉴에서 텔넷/SSH 세션을 클릭합니다. 텔넷/SSH 세션 페이지가 열리고 맨 위에 장치 호스트 이름이나 IP 주소가 표시됩니다.

텔넷/SSH 세션 목록 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 세션을 삭제할 수 있습니다. 세션을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 세션을 선택하거나 선택 취소할 수 있습니다.
시작 날짜	세션이 시작된 날짜와 시간이 표시됩니다.
상태	열림 또는 닫힘의 세션 상태가 표시됩니다.
유형	텔넷 또는 SSH의 세션 유형이 표시됩니다.
종료 날짜	세션이 끝난 날짜와 시간이 표시됩니다.
생성자	세션을 생성한 사람의 이름을 표시합니다.
<사용자 지정 필드>	텔넷/SSH 세션에 대해 정의된 모든 사용자 지정 필드가 이 페이지에 표시됩니다.
작업	다음 옵션 중에서 선택할 수 있습니다. <ul style="list-style-type: none"> • 전체 텔넷/SSH 세션 보기 — 세션 중에 입력한 명령과 장치 응답을 볼 수 있는 텔넷/SSH 세션 페이지를 엽니다. • 명령만 보기 — 세션 중에 입력한 명령을 볼 수 있는 텔넷/SSH 세션 페이지를 엽니다. 이 옵션은 이 장치나 다른 장치에서 재생할 스크립트를 기록할 때 유용합니다. 명령을 클릭하면 해당 명령에 대한 장치 응답이 표시됩니다.

참고: 왼쪽 마우스 버튼으로 텍스트를 선택하면 텍스트가 강조 표시됩니다. 그런 후 Enter 키를 눌러 텍스트를 클립보드로 붙여 넣을 수 있습니다. 텔넷/SSH 애플릿 내에서 오른쪽 마우스 버튼을 누르면 클립보드의 텍스트가 애플릿으로 붙여 넣어집니다.

connect를 사용할 때 바로 가기에서는 connect dev*와 같이 호스트 이름이나 IP 주소에 와일드카드가 추가됩니다. 이렇게 하면 장치 목록이나 검색 범위를 좁히기 위한 메시지로 돌아갑니다. 연결할 장치 번호를 입력합니다. 셸 인터페이스는 다음 컨트롤 문자를 지원합니다.

제어 문자	설명
^A	커서가 입력 라인 맨 처음으로 이동됩니다.
^B, 왼쪽 화살표	커서가 한 문자 뒤로 이동됩니다.
^C	입력 라인이 취소되고 새 프롬프트로 돌아갑니다.
^D	커서 아래의 문자가 지워집니다.
^F, 오른쪽 화살표	커서가 한 문자 오른쪽으로 이동됩니다.
^H, 백스페이스, Delete	커서 왼쪽 문자가 지워집니다.
^J, ^M	CRLF를 보냅니다.
^K	커서부터 라인 끝까지 종료되고 텍스트가 종료 버퍼에 추가됩니다.
^L, ^R	새 명령줄에서 명령을 에코합니다(화면 다시 그리기 시뮬레이션).
^N, 아래쪽 화살표	명령 이력의 다음 명령으로 이동됩니다.
^P, 위쪽 화살표	명령 이력의 이전 명령으로 이동됩니다.
^T	커서 아래의 문자와 이전 문자의 순서를 바꿉니다.
^U, ^X	커서부터 라인 처음까지 삭제되고 삭제된 문자가 종료 버퍼에 추가됩니다.
^W	커서부터 단어 처음까지 삭제되고 삭제된 문자가 종료 버퍼에 추가됩니다.
^Y	종료 버퍼부터 현재 위치까지 삭제됩니다.
^\	현재 장치 연결이 닫힙니다(콘솔 서버를 통해 액세스할 때 유용).
ESC-b	커서가 한 단어 뒤로 이동됩니다.
ESC-f	커서가 한 단어 앞으로 이동됩니다.

텔넷/SSH 프록시를 사용하여 구성 변경

텔넷/SSH 프록시를 통해 구성을 변경하려면 다음을 수행합니다.

1. NA 서버에 대해 텔넷 또는 SSH를 실행한 후 NA 자격 증명을 사용하여 로그인합니다.
2. `connect` 명령을 사용하여 장치에 연결합니다. NA를 통해 연결할 수 있는 장치를 보려면 `connect*`를 입력합니다. 너무 많은 장치가 표시되면 호스트 이름의 처음 몇 문자나 IP 주소의 숫자 몇 개를 입력하고 별표를 입력하여 필드 범위를 좁힙니다(예: `connect bor*`).
3. 연결할 장치의 텔넷/SSH 프록시에 표시되는 숫자 목록에 포함된 숫자를 하나 입력합니다. NA는 사용자의 액세스 자격 증명을 확인한 후에 사용자를 자동으로 장치에 로그인합니다.
4. Cisco IOS 장치인 경우 장치에 대해 `Config T` 모드에 들어가 변경을 수행하고 관련 설명을 추가합니다.
5. 터미널 구성 모드에서 빠져 나온 후 `Exit`를 입력합니다.
6. NA 텔넷/SSH 프록시를 끝내려면 프롬프트에 `Exit`를 입력합니다.

텔넷/SSH 프록시를 사용할 때는 장치에 로그인될 때 인라인 주석 처리가 진행됩니다.

배스천 호스트 사용

배스천 호스트는 사설 네트워크와 공용 네트워크 간의 게이트웨이입니다. 보안 방책으로 사용되는 배스천 호스트는 사설 네트워크와 공용 네트워크 사이에서 해커의 공격을 막기 위한 장벽으로 작용할 수 있습니다.

배스천 호스트를 NA와 함께 사용하면 텔넷 또는 SSH 세션에 잠금 기능을 사용할 수 있습니다. 다음 작업을 수행할 수 있습니다.

- 장치 기준으로 배스천 호스트를 지정합니다.
- 사용자 이름(선택 사항) 및 암호를 배스천 호스트에 대한 로그인 자격 증명으로 지정합니다.
- 배스천 호스트에 대해 텔넷 또는 SSH를 실행한 후 대상 장치에 대해 텔넷 또는 SSH를 실행합니다.

참고: 배스천 호스트를 사용할 경우 모든 CLI 액세스는 장치로 직접 진행되지 않고 배스천 호스트를 통해 진행됩니다. 배스천 호스트를 사용하도록 구성된 장치에 텔넷/SSH 프록시를 통해 연결하면 NA는 배스천 호스트를 통해 연결하고 지정된 사용자의 AAA 자격 증명을 배스천 호스트와 대상 장치 둘 다에 적용합니다.

배스천 호스트에 대한 액세스는 정상적인 NA 암호 규칙 처리를 거치지 않고 진행됩니다. 배스천 호스트 자격 증명에 올바르지 않으면 폴백이 없습니다. 배스천 호스트에 로그인한 후에는 배스천 호스트에서 장치에 액세스하면 NA에서 정상적인 암호 처리가 진행됩니다.

참고: 하나의 특정 장치에 대해 여러 배스천 호스트를 지정할 수 없습니다. 그러나 DNS 이름을 공유하는 여러 배스천 호스트 간에 로드 균형을 조정하여 이러한 상태를 시뮬레이션할 수 있습니다.

텔넷 및 SSH 액세스에 대해 Unix 또는 Linux 배스천 호스트를 지정하려면

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다. 현재 관리되는 모든 장치 목록이 열립니다.
2. 페이지 맨 위에 있는 새 장치 링크를 클릭합니다. 새 장치 페이지가 열립니다.
3. 페이지 중간으로 스크롤하여 연결 정보 섹션을 찾습니다. 자세한 내용은 [138페이지](#)의 "새 장치 페이지 필드"를 참조하십시오.

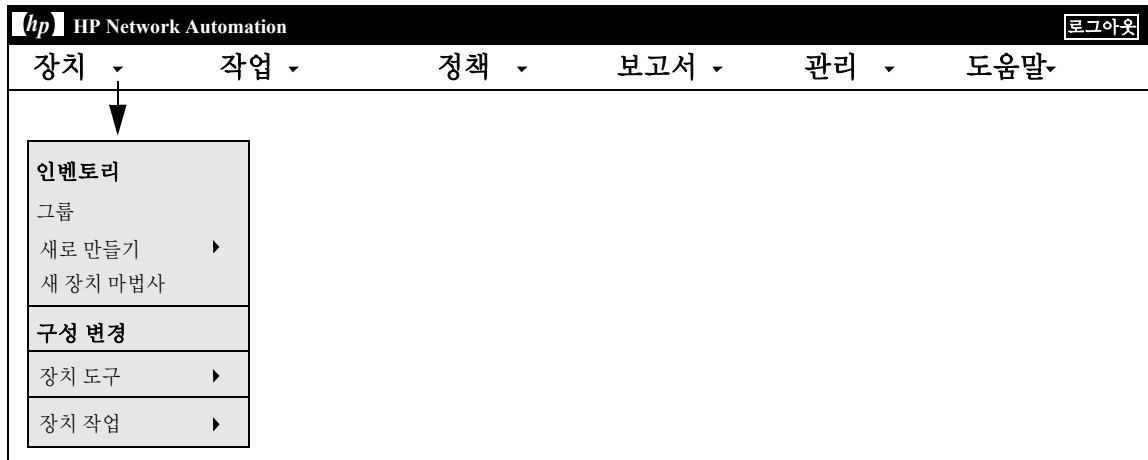
새 장치가 텔넷 및 SSH 액세스에 대해 기본적으로 배스천 호스트를 사용하도록 지정하려면 관리 아래의 메뉴 모음에서 관리 설정을 선택한 후 장치 액세스를 클릭합니다. 자세한 내용은 [56페이지의 "장치 액세스 페이지 필드"](#)를 참조하십시오.

4장: 장치 구성 관리

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	222페이지의 "시작하기"
장치 구성 변경 보기	223페이지의 "장치 구성 변경 보기"
장치 구성 비교	231페이지의 "장치 구성 비교"
장치 구성 배포	233페이지의 "장치 구성 배포"

장치 구성 변경으로 이동



시작하기

HP Network Automation(NA)은 장치 구성 변경을 감지하고 기록합니다. 장치 구성이 변경되면 NA는 구성을 중앙의 리포지토리로 다운로드합니다. NA는 수행된 변경과 수행한 사람을 즉시 확인할 수 있는 다중 실시간 변경 감지 및 경보 시스템을 지원합니다.

Cisco IOS 장치와 같이 Syslog를 통한 사용자 특성을 지원하는 장치의 경우 NA는 사용자 이름을 추출한 후 구성 변경에 연결합니다. NA가 사용자 이름을 NA 사용자에게 연결할 수 없으면 무작위로 생성된 암호를 사용하여 새 사용자 계정이 생성됩니다. 기본적으로 NA는 자동으로 생성된 사용자임을 나타내기 위해 새 사용자에게 용어 "_auto"를 붙입니다. 이를 통해 NA는 등록되지 않은 사용자가 변경한 내용을 비롯한 모든 변경 내용의 소유권을 보고할 수 있습니다. NA는 AAA 계정 로그, Syslog 메시지 및 프록시 로그를 비롯한 여러 방법을 사용하여 지정된 구성 변경의 작성자를 검색합니다.

ACL(액세스 제어 목록)은 여러 장치에 대한 구성의 일부입니다. 이 목록은 전달된 패킷이 라우터 인터페이스에서 수락될지 또는 차단될지를 제어하여 네트워크 트래픽을 필터링합니다.

일반적으로 ACL의 정의는 구성 명령문을 모아 놓은 것입니다. 이러한 명령문은 수락하거나 거부할 주소, 프로토콜 및 패턴을 정의합니다. ACL은 라우팅 업데이트의 콘텐츠를 제한하고 네트워크 보안을 제공하는 데 사용될 수 있습니다.

NA는 장치에서 구성 정보를 검색하고 구성에서 ACL 명령문 및 응용 프로그램을 추출합니다. 그런 후 NA는 구성과는 별도로 ACL을 저장합니다. ACL 생성에 대한 자세한 내용은 [879페이지의 "ACL 생성"](#)을 참조하십시오.

장치 구성 변경 보기

구성 변경 페이지에서 변경한 구성을 볼 수 있습니다. 빨간색 텍스트로 표시되는 장치는 최근 작업이 실패한 장치입니다. 비활성 장치는 IP 주소 옆에 아이콘이 표시됩니다.

구성 변경 사항이 서로 다른 색상으로 표시되면 두 구성을 쉽게 검색하고 변경된 영역을 빠르게 확인할 수 있습니다. NA를 사용하지 않고 있으므로 잘못 구성된 장치를 자동으로 식별해야 하는 장치 아래의 메뉴 모음에서 장치에 연결하고 구성을 불러온 후 구성에 이상한 부분이 있는지 확인해야 합니다.

최근 구성 변경의 전체 목록을 보려면 장치 아래의 메뉴 모음에서 구성 변경을 클릭합니다. 구성 변경 페이지가 열립니다. 장치를 클릭하여 특정 장치 구성 정보를 볼 수 있습니다.

특정 장치에 대한 구성 변경을 보려면

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다. 현재 관리되는 모든 장치 목록이 열립니다.
2. 구성 변경을 확인할 장치를 클릭합니다. 해당 장치에 대한 장치 세부사항 페이지가 열립니다.
3. 보기 드롭다운 메뉴에서 구성 변경을 클릭합니다. 장치 구성 페이지가 열립니다. 장치 구성 세부사항 페이지에 대한 내용은 [227페이지의 "장치 구성 세부사항 페이지 필드"](#)를 참조하십시오.

장치 구성 페이지 필드

필드	설명/작업
호스트 이름	장치 호스트 이름을 표시합니다. 장치의 호스트 이름을 클릭하면 이 장치에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
장치 IP	장치 IP 주소를 표시합니다. 장치 IP 주소를 클릭하면 이 장치에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
마지막 스냅샷 시도	장치에 마지막으로 액세스한 날짜와 시간이 표시됩니다.
마지막 스냅샷 결과	"구성이 변경되지 않음"과 같은 마지막 스냅샷 결과를 표시합니다.
보기 메뉴	자세한 내용은 261페이지의 "메뉴 옵션 보기" 를 참조하십시오.
편집 메뉴	자세한 내용은 304페이지의 "편집 메뉴 옵션" 을 참조하십시오.
프로비전 메뉴	자세한 내용은 314페이지의 "프로비전 메뉴 옵션" 을 참조하십시오.
연결 메뉴	자세한 내용은 316페이지의 "연결 메뉴 옵션" 을 참조하십시오.
장치에 대해 예정된 배포 링크	장치에 대해 예정된 배포가 있는지 확인할 수 있는 장치 검색 결과 페이지가 열립니다.
편집한 구성 링크	편집한 구성 검색 결과 페이지가 열립니다. 자세한 내용은 614페이지의 "구성 검색 결과 페이지 필드" 를 참조하십시오.
확인란	<p>왼쪽의 확인란을 사용하여 두 장치 구성을 비교하거나 장치 구성을 삭제할 수 있습니다. 장치를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음을 클릭합니다.</p> <ul style="list-style-type: none"> •비교 — 선택한 두 구성을 나란히 비교할 수 있는 장치 구성 비교 페이지가 열립니다. 차이점은 쉽게 확인할 수 있게 서로 다른 색상으로 강조 표시됩니다. •삭제 — 선택한 장치 구성이 삭제됩니다. <p>인접한 선택 드롭다운 메뉴를 통해 모든 장치 구성을 선택하거나 선택을 취소할 수 있습니다.</p>

필드	설명/작업
날짜	구성이 마지막으로 추가 또는 변경된 날짜와 시간이 표시됩니다.
변경한 사람	구성, 장치 또는 작업을 변경한 사람의 로그인 이름이 표시됩니다. N/A는 해당하는 사람이 없음을 의미합니다.
주석	구성에 대한 주석이 표시됩니다.
작업	<p>선택할 수 있는 작업은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 이전과 비교 — 선택한 구성과 이전 구성을 나란히 비교할 수 있는 장치 구성 비교 페이지가 열립니다. 차이점은 쉽게 확인할 수 있게 서로 다른 색상으로 강조 표시됩니다. • 구성 보기 — 장치 구성 세부사항 페이지가 열립니다. 이 페이지에서는 전체 구성을 확인하거나 구성을 실행 중인 장치에 이 버전의 구성을 배포하거나, 구성을 시작하고 재부팅(해당되는 경우)할 수 있습니다. 또한 구성을 편집하고 구성 텍스트 버전을 다운로드하며 구성을 전자 메일로 전송하고 현재의 구성을 이전 또는 다음 구성과 비교할 수도 있습니다. 자세한 내용은 227페이지의 "장치 구성 세부사항 페이지 필드"를 참조하십시오. • 진단 — 이 구성에 대한 진단 정보를 볼 수 있는 진단 페이지를 엽니다. 진단에는 기본 IP, 장치 정보, NA 감지 장치 부팅, NA 인터페이스, NA 모듈 상태, NA OSPF 인접 환경 및 NA 라우팅 테이블이 포함되어 있습니다. 진단에 대한 자세한 내용은 261페이지의 "메뉴 옵션 보기"를 참조하십시오.

시작 및 실행 구성이 다른 경우 장치 구성 페이지 맨 위에 다음 링크가 표시됩니다.

- 시작 보기 — 현재 시작 구성을 볼 수 있는 장치 구성 페이지가 열립니다. 자세한 내용은 [227페이지의 "장치 구성 세부사항 페이지 필드"](#)를 참조하십시오.
- 시작을 실행과 비교 — 시작 및 실행 구성을 비교할 수 있는 장치 구성 비교 페이지가 열립니다. 자세한 내용은 [231페이지의 "장치 구성 비교 페이지 필드"](#)를 참조하십시오.

- 동기화 — 시작 및 실행 구성을 동기화할 수 있는 새 작업 - 시작 및 실행 동기화 페이지가 열립니다. 자세한 내용은 408페이지의 "시작 및 실행 동기화 작업 페이지 필드"를 참조하십시오.

장치 구성 세부사항 페이지 필드

장치 구성 세부사항 페이지에서 다음 작업을 수행할 수 있습니다.

- 특정 구성의 세부사항을 검토합니다.
- 구성에 대한 주석을 입력합니다.
- 이 버전의 구성을 장치에 배포합니다. 예를 들어 안정적인 구성을 배포하여 장치의 잘못된 변경 사항을 롤백할 수 있습니다.

참고: 쉬운 탐색을 위해 구성 텍스트 바로 위에 구성 파일의 섹션에 대한 구문을 빠르게 분석할 수 있도록 하는 링크가 있습니다. 예를 들어 구성 파일에 Access List 섹션이 포함된 경우 구성 파일의 맨 위에 있는 Access List 링크를 클릭하여 해당 섹션으로 바로 이동할 수 있습니다. 현재는 Cisco IOS 일반 드라이버에서만 섹션 구문 분석을 지원합니다.

특정 장치에 대한 장치 구성 세부사항 페이지를 보려면

1. 장치 세부사항 페이지에서 보기 드롭다운 메뉴를 클릭한 후 구성 변경을 클릭합니다. 장치 구성 페이지가 열립니다.
2. 작업 열에서 구성 보기 링크 옵션을 클릭합니다. 장치 구성 세부사항 페이지가 열립니다.

필드	설명/작업
호스트 이름	장치 호스트 이름을 표시합니다. 장치의 호스트 이름을 클릭하면 이 장치에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
장치 IP	장치 IP 주소를 표시합니다. 장치 IP 주소를 클릭하면 이 장치에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
마지막 스냅샷 시도	장치에 마지막으로 액세스한 날짜와 시간이 표시됩니다.
마지막 스냅샷 결과	"구성이 변경되지 않음"과 같은 마지막 스냅샷 결과를 표시합니다.

필드	설명/작업
장치 관찰 링크	<p>장치 관찰 옵션을 처음 클릭하면, 장치를 포함하는 감시 그룹이 장치 관찰 이벤트 규칙과 함께 생성됩니다. 장치에 대한 변경 사항이 발생하면 장치를 감시하는 사용자에게 전자 메일 알림이 전송됩니다. 장치 관찰 이벤트 규칙은 다음과 같은 다양한 이벤트에 대해 전자 메일 알림을 전송합니다.</p> <ul style="list-style-type: none"> •장치 액세스 실패 •장치 부팅됨 •장치 구성 변경 •장치 삭제됨 •장치 진단 변경됨 •장치 편집됨 •장치 소프트웨어 변경 •소프트웨어 취약점이 감지됨 <p>참고: 장치 관찰 이벤트 규칙을 편집하여 이벤트를 변경할 수 있습니다. 앞으로 관찰하는 모든 장치는 동일한 이벤트 규칙 이름을 사용합니다. 571페이지의 "새 이벤트 알림 및 응답 규칙 페이지 필드"를 참조하십시오.</p> <p>감시 그룹에서 장치를 제거하려면 장치 관찰 중지를 클릭합니다.</p>
보기 메뉴	자세한 내용은 261페이지의 "메뉴 옵션 보기" 를 참조하십시오.
편집 메뉴	자세한 내용은 304페이지의 "편집 메뉴 옵션" 을 참조하십시오.
프로비전 메뉴	자세한 내용은 314페이지의 "프로비전 메뉴 옵션" 을 참조하십시오.
연결 메뉴	자세한 내용은 316페이지의 "연결 메뉴 옵션" 을 참조하십시오.
실행 중인 구성에 배포 링크	<p>구성을 실행 중인 구성에 배포할 수 있는 새 작업 - 구성 배포 페이지가 열립니다. (참고: 모든 장치에 이 작업을 사용할 수 있는 것은 아닙니다.) 자세한 내용은 234페이지의 "구성 배포 작업 페이지 필드"를 참조하십시오.</p>
시작 구성 배포 및 재부팅 링크	<p>시작 및 실행 구성이 동기화 상태가 되도록 해당 구성을 시작 구성에 배포하고 장치를 재부팅할 수 있는 새 작업 - 구성 배포 페이지가 열립니다. (참고: 모든 장치에 이 작업을 사용할 수 있는 것은 아닙니다.) 자세한 내용은 234페이지의 "구성 배포 작업 페이지 필드"를 참조하십시오.</p>

필드	설명/작업
바이너리 구성 배포 및 재부팅 링크	바이너리 구성을 장치에 배포하고 장치를 재부팅합니다.
텍스트 구성 보기 링크	클립보드로 복사된 후 다른 응용 프로그램으로 붙여 넣을 수 있도록 구성이 일반 텍스트로 새 브라우저 창에 표시됩니다.
텍스트 구성 다운로드 링크	다른 시스템으로 복사할 수 있도록 구성을 텍스트 형식으로 다운로드합니다.
바이너리 구성 다운로드 링크	다른 시스템으로 복사할 수 있도록 구성을 바이너리 형식으로 다운로드합니다.
텍스트 구성 전자 메일 보내기 링크	해당 구성을 전자 메일로 보낼 수 있습니다.
이전과 비교 링크	이전 구성과 새 구성을 나란히 확인할 수 있는 장치 구성 비교 페이지가 열립니다. 차이점은 쉽게 확인할 수 있게 서로 다른 색상으로 강조 표시됩니다. 참고: 이 구성이 첫 번째 구성이면 "이것은 첫 번째 구성입니다."라는 텍스트가 표시됩니다. 마지막 구성이면 "이것은 현재 구성입니다."라는 텍스트가 표시됩니다.
변경한 사람	스냅샷을 트리거한 변경을 수행한 사람의 로그인 이름 및 사용자 세부사항을 제공할 수 있는 "세부사항" 링크를 표시합니다.
생성 날짜	구성 변경을 캡처한 스냅샷의 날짜 및 시간이 표시됩니다.
<사용자 지정 필드>	장치 스냅샷 및 진단에 대해 정의된 사용자 지정 필드가 표시됩니다.
구성 주석	이 구성과 다른 구성(특히 이전 구성)을 구분하기 위한 주석을 입력합니다. 주석 편집을 클릭합니다. 주석 편집 옵션을 사용하여 이 구성에 대한 사용자 지정 필드 및 주석을 편집할 수 있습니다. 장치 구성 데이터 편집에 대한 자세한 내용은 230페이지의 "장치 구성 데이터 편집" 을 참조하십시오.
라인/구성 텍스트	구성 파일이 표시됩니다.

장치 구성 데이터 편집

편집 메뉴에서 인라인 구성 주석 편집 옵션을 클릭하여 구성 주석을 추가하거나 편집할 수 있습니다. 사용자 지정 데이터 추가에 대한 자세한 내용은 [694페이지의 "사용자 지정 데이터 설정 페이지 필드"](#)를 참조하십시오.

인라인 주석을 편집할 때는 다음이 적용됩니다.

- 구성의 라인이 변경될 때마다 해당 라인에 대한 주석이 제거됩니다. 예를 들어 호스트 이름을 변경하면 NA는 명령이 변경된 후에 주석이 계속 유효한지 확인할 수 없으므로 호스트 이름 명령 바로 위에 있는 주석을 모두 제거합니다.
- 빈 라인을 추가하거나 제거할 때는 주의하십시오. 빈 라인은 일부 장치에 중요할 수 있으므로 NA는 추가되거나 제거된 빈 라인을 구성 변경으로 취급합니다. 빈 주석 라인(! 또는 ##과 같은 이중 주석 문자로 시작하는 라인)을 추가할 수 있습니다.
- 인라인 주석은 구성 파일과 같은 방식으로 버전 관리되지 않습니다. 주석 블록은 구성의 다음 명령에 적용됩니다. 배포가 다음 명령줄에 영향을 미치지 않을 경우 주석은 변경되지 않습니다. 이전 구성을 배포하여 새 구성을 덮어쓰는 경우 최신 구성의 주석이 잘못된 위치에서 끝날 수 있더라도 배포된 구성에 적용될 수 있습니다.
- 많은 편집이 요구되는 파일에서 주석이 삭제될까 걱정되는 경우에는 필요할 때 주석을 복원할 수 있도록 구성 파일을 저장하기 전에 해당 파일을 주석과 함께 복사할 것을 권장합니다.

장치 구성 비교

장치 구성 비교 페이지에는 같은 장치에 대한 두 구성이 나란히 표시됩니다. 추가, 삭제 및 변경 사항은 왼쪽에 라인 번호가 붙은 두 열로 강조 표시됩니다. 각 구성은 고유한 IP 주소와 구성 스냅샷이 작성된 날짜/시간으로 식별됩니다.

서로 다른 장치에서 두 구성을 비교하려면

1. 장치 아래의 메뉴 모음에서 구성 변경을 클릭합니다. 구성 변경 페이지가 열립니다.
2. 왼쪽의 확인란을 사용하여 두 장치를 클릭합니다.
3. 작업 드롭다운 메뉴에서 비교를 클릭합니다. 장치 구성 비교 페이지가 열립니다.

장치 구성 비교 페이지 필드

필드	설명/작업
라인이 변경됨	라인 수가 연보라색으로 강조 표시됩니다.
라인이 삽입됨	삽입된 라인 수가 옅은 녹색으로 강조 표시됩니다.
라인이 삭제됨	삭제된 라인 수가 옅은 노란색으로 강조 표시됩니다.
컨텍스트와의 차이 표시	이 옵션을 선택하면(기본값) 각 변경의 이전 또는 이후 세 라인의 변경만 표시됩니다.
전체 텍스트 표시	이 옵션을 선택하면 완전한 구성 파일이 표시됩니다.
UNIX 스타일 차이 표시	이 옵션을 선택하면 구성 파일이 UNIX diff 형식으로 표시됩니다.
실행 중인 구성에 배포 링크	이 구성을 장치의 실행 중인 구성으로 배포할 수 있는 구성 배포 페이지가 열립니다. (참고: 모든 장치에 이 작업을 사용할 수 있는 것은 아닙니다.)
시작 구성 배포 및 재부팅	시작 및 실행 구성이 동기화 상태가 되도록 해당 구성을 시작 구성에 배포하고 장치를 재부팅할 수 있는 구성 배포 페이지가 열립니다. (참고: 모든 장치에 이 작업을 사용할 수 있는 것은 아닙니다.)

필드	설명/작업
구성 #1/구성 #2	구성 #1 또는 구성 #2 링크를 클릭하면 장치 구성 세부사항 페이지가 열립니다. 자세한 내용은 227페이지의 "장치 구성 세부사항 페이지 필드" 를 참조하십시오. 참고: 이 구성이 첫 번째 구성이면 "이것은 첫 번째 구성입니다."라는 텍스트가 표시됩니다. 마지막 구성이면 "이것은 현재 구성입니다."라는 텍스트가 표시됩니다.
장치	장치의 호스트 이름 또는 IP 주소가 표시됩니다. 장치의 호스트 이름 및 IP 주소를 클릭하면 장치 및 해당 구성 내역에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
날짜	구성 변경을 캡처한 스냅샷의 날짜 및 시간이 표시됩니다.

장치 구성 배포

다음 두 가지 방법으로 구성을 배포할 수 있습니다.

- 실행 중인 구성에 배포 — 구성을 배포할 때 장치를 재부팅할 때까지 구성 파일은 사용 중인 상태로 남아 있습니다. 장치를 재부팅하면 시작 구성이 실행 중인 구성을 덮어쓸 수 있습니다.
- 시작 구성에 배포 — 구성을 배포할 때 장치는 재부팅되고 새 구성이 실행 중인 구성도 되고 시작 구성도 됩니다.

구성을 배포하려면

1. 장치 아래의 메뉴 모음에서 구성 변경을 클릭합니다. 구성 변경 페이지가 열립니다.
2. 장치에 대한 작업 열에서 구성 보기를 클릭합니다. 장치 구성 세부사항 페이지가 열립니다. 다음 옵션 중 하나를 선택합니다(적용 가능한 경우).
 - 실행 중인 구성에 배포 — 이 구성을 장치의 실행 중인 구성에 배포할 수 있는 새 작업 - 구성 배포 페이지가 열립니다.
 - 시작 구성 배포 및 재부팅 — 시작 및 실행 구성이 동기화 상태가 되도록 해당 구성을 시작 구성에 배포하고 장치를 재부팅할 수 있는 새 작업 - 구성 배포 페이지가 열립니다.

구성 배포 작업 페이지 필드

필드	설명/작업
작업 이름	구성 배포를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
적용 대상	장치의 호스트 이름이나 IP 주소가 표시됩니다.
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 가능한 한 빨리 시작(기본값) • 시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
우선 순위	작업 우선 순위를 표시합니다. 1~5의 5가지 작업 우선 순위 수준이 있으며, 최고 작업 우선 순위는 1입니다. 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.
작업 옵션	
세션 로그	전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 장치와 인터랙션하는 대부분의 작업은 세션 로깅이 설정되어야만 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버그하는 첫 번째 단계로 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.)
확인란	"변경 사항이 장치에 적용되는 모든 정책을 준수하는지 확인합니다" 옵션은 기본적으로 선택되어 있습니다. 장치 유형에 따라 실행 중인 구성에 배포 또는 시작 구성 배포 및 재부팅을 선택할 수 있습니다.
구성	구성이 표시됩니다.
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.

필드	설명/작업
장치 자격 증명 옵션	
<p>서버 페이지의 관리 설정에서 구성한 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라, 장치 자격 증명 옵션이 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 68페이지의 "서버 페이지 필드"를 참조하십시오.</p>	
장치 자격 증명	<p>서버 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력하라는 메시지가 표시됩니다. 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명이 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
사전 작업/사후 작업 스냅샷 옵션	
<p>스냅샷 옵션은 시스템이 구성 관리 페이지의 관리 설정에서 사용자 오버라이드를 활성화하도록 구성된 경우에만 표시됩니다. (자세한 내용은 43페이지의 "구성 관리 페이지 필드"를 참조하십시오.)</p>	
사전 작업 스냅샷	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 없음(기본값) 작업에 포함됨
사후 작업 스냅샷	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 없음 작업에 포함됨(기본값) 별도 작업으로 예정됨
승인 옵션	
<p>승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.</p>	

필드	설명/작업
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.

필드	설명/작업
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < > 번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

완료되면 작업 저장을 클릭해야 합니다.

5장: 장치 보기

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
장치 보기	241페이지의 "장치 보기"
장치 그룹 보기	244페이지의 "장치 그룹 보기"
장치 예약	246페이지의 "장치 예약"
장치 세부사항 보기	249페이지의 "장치 세부사항 보기"
NA/SA 통합	254페이지의 "NA/SA 통합"
메뉴 옵션 보기	261페이지의 "메뉴 옵션 보기"
VLAN(가상 로컬 영역 네트워크)	278페이지의 "VLAN(가상 로컬 영역 네트워크)"
편집 메뉴 옵션	304페이지의 "편집 메뉴 옵션"
프로비전 메뉴 옵션	314페이지의 "프로비전 메뉴 옵션"
연결 메뉴 옵션	316페이지의 "연결 메뉴 옵션"

장치 정보 탐색

The screenshot shows the HP Network Automation web interface. At the top, there is a navigation bar with the HP logo and the text "HP Network Automation" on the left, and a "로그아웃" (Logout) button on the right. Below the navigation bar, there are several menu items: "장치" (Devices), "작업" (Jobs), "정책" (Policies), "보고서" (Reports), "관리" (Management), and "도움말" (Help). The "장치" menu is currently expanded, showing a dropdown list with the following items: "인벤토리" (Inventory), "그룹" (Groups), "새로 만들기" (New) with a right-pointing arrow, "새 장치 마법사" (New Device Wizard), "구성 변경" (Change Configuration), "장치 도구" (Device Tools) with a right-pointing arrow, and "장치 작업" (Device Actions) with a right-pointing arrow.

장치 보기

관리되는 장치 목록을 보려면 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다. 인벤토리는 기본 작업 그룹입니다. 현재 관리되는 모든 장치가 인벤토리에 나열되어 있습니다. 새 장치 추가에 대한 자세한 내용은 [137페이지의 "장치 추가"](#)를 참조하십시오.

인벤토리 페이지 필드

필드	설명/작업
그룹 링크	현재 장치 그룹 목록을 볼 수 있는 장치 그룹 페이지를 엽니다. 자세한 내용은 244페이지의 "장치 그룹 보기" 를 참조하십시오.
새 장치 링크	새 장치를 추가할 수 있는 새 장치 페이지를 엽니다. 자세한 내용은 137페이지의 "장치 추가" 를 참조하십시오.
새 장치 그룹 링크	새 장치 그룹을 추가할 수 있는 새 장치 그룹 페이지를 엽니다. 자세한 내용은 175페이지의 "장치 그룹 추가" 를 참조하십시오.
새 상위 그룹 링크	새 상위 그룹을 추가할 수 있는 새 상위 그룹 페이지를 엽니다. 자세한 내용은 178페이지의 "상위 그룹 추가" 를 참조하십시오.
현재 작업 그룹	기본 그룹인 인벤토리를 표시합니다. 드롭다운 메뉴에서 다른 그룹을 선택할 수 있습니다(해당되는 경우).
활성 장치만 나열 확인란	인벤토리 목록에 활성 장치만 포함하려면 이 확인란을 선택합니다. 비활성 장치는 능동적으로 관리되지 않습니다.
그룹에서 실행할 작업	이 그룹에서 실행할 작업을 드롭다운 메뉴에서 선택할 수 있습니다. 작업 실행에 대한 자세한 내용은 358페이지의 "작업이란?" 을 참조하십시오.
그룹 설명	시스템에 알려진 모든 장치의 목록입니다.

필드	설명/작업
확인란	<p>왼쪽의 확인란을 사용하여 장치를 관리할 수 있습니다. 장치를 선택한 후에 작업 드롭다운 메뉴를 클릭합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 활성화 — 선택한 장치를 관리하도록 NA에 지시합니다. • 비활성화 — 선택한 장치를 관리하지 않도록 NA에 지시합니다. • 일괄 편집 — 드라이버를 할당하고 선택한 모든 장치에 대해 동시에 연결 방법을 설정할 수 있는 장치 일괄 편집 페이지를 엽니다. 자세한 내용은 209페이지의 "장치 일괄 편집 페이지 필드"를 참조하십시오. • 다이어그램 — 다이어그램 작성 페이지가 열립니다. 758페이지의 "다이어그램 작성"을 참조하십시오. • 삭제 — 선택한 장치를 삭제합니다. • 확인된 장치에 대해 실행할 작업을 선택합니다. 자세한 내용은 358페이지의 "임시 장치 그룹에 대한 작업 실행"을 참조하십시오. <p>인접한 선택 드롭다운 메뉴를 통해 모든 장치를 선택하거나 선택 취소할 수 있습니다.</p>
호스트 이름	<p>장치의 호스트 이름을 표시합니다. 빨간색으로 표시된 장치는 마지막 스냅 샷 시도에서 실패한 장치입니다. 비활성 장치는 IP 주소 옆의 아이콘으로 표시됩니다. 호스트 이름 링크를 클릭하면 장치 및 장치의 구성 이력에 대한 기본 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다. 장치 세부사항 페이지에 대한 자세한 내용은 261페이지의 "메뉴 옵션 보기"를 참조하십시오.</p>
장치 IP	<p>장치의 IP 주소를 표시합니다. 장치 IP 링크를 클릭하면 장치 및 장치의 구성 이력에 대한 기본 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다. 장치 세부사항 페이지에 대한 자세한 내용은 261페이지의 "메뉴 옵션 보기"를 참조하십시오.</p>
장치 공급업체	<p>장치 제조업체의 이름을 표시합니다.</p>
장치 모델	<p>장치 모델 명칭을 표시합니다.</p>
파티션	<p>장치가 속해 있는 파티션을 표시합니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다.)</p>

필드	설명/작업
작업	각 장치에 대해 다음 작업을 선택할 수 있습니다. <ul style="list-style-type: none">• 편집 — 이 장치에 대한 정보를 편집할 수 있는 장치 편집 페이지를 엽니다. 146페이지의 "장치 편집 페이지 필드"를 참조하십시오.• 텔넷 — 텔넷 창을 엽니다.• SSH — SSH 창을 엽니다.• 구성 보기 — 마지막 구성을 보고, 실행 중인 구성에 배포하고, 주석을 추가할 수 있는 현재 구성 페이지를 엽니다.
페이지별 결과 표시 수	드롭다운 메뉴에서 페이지당 표시할 항목 수를 설정할 수 있습니다. 기본값은 25입니다.

장치 그룹 보기

장치 그룹은 조직의 상황에 맞게 장치를 범주화하는 방법입니다.

- 지리적/실제 위치
- 사업체/부서
- 네트워크 아키텍처에서의 역할
- 활성화 상태

작성한 장치 그룹은 검색, 규칙 인증, 암호 업데이트 등 다양한 기능 수행을 위해 사용할 수 있습니다. 장치 그룹 추가에 대한 자세한 내용은 [175페이지의 "장치 그룹 추가"](#)를 참조하십시오.

처음에는 장치 그룹 페이지에 하나의 시스템 그룹, 즉 인벤토리 그룹이 포함됩니다. 인벤토리 그룹에는 모든 장치가 포함되어 있습니다. 그러나 사용자가 생성하는 사용자 정의 그룹도 이 페이지에 나타납니다.

장치 그룹 목록을 보려면 장치 아래의 메뉴 모음에서 그룹을 클릭합니다. 장치 그룹 페이지가 열립니다. 공용 장치 그룹은 모든 사용자에게 표시됩니다. 개인 장치 그룹은 소유자 및 NA 관리자에게만 표시됩니다.

장치 그룹 페이지 필드

필드	설명/작업
새 그룹 링크	새 장치 그룹을 생성할 수 있는 새 장치 그룹 페이지를 엽니다. 새 장치 그룹 생성에 대한 자세한 내용은 175페이지의 "장치 그룹 추가" 를 참조하십시오.
새 상위 그룹 링크	새 상위 그룹을 추가할 수 있는 새 상위 그룹 페이지를 엽니다. 자세한 내용은 178페이지의 "상위 그룹 추가" 를 참조하십시오.

필드	설명/작업
그룹 이름	장치 그룹의 사용자 정의 이름을 표시합니다. 상위 그룹은 다른 상위 그룹의 하위가 아닌 이상 들여쓰기로 표시되지 않습니다. 상위 그룹에 속해 있는 그룹은 상위 아래에 들여쓰기로 표시됩니다. 그룹 이름을 클릭하면 장치 그룹에 대한 자세한 정보를 볼 수 있는 장치 그룹 페이지가 열립니다. 자세한 내용은 244페이지의 "장치 그룹 페이지 필드" 를 참조하십시오. (참고: 앞에 클라우드 아이콘이 나오는 그룹 이름은 파티션에 포함되어 있습니다. 파티션에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.)
설명	그룹에 대한 간단한 설명을 표시합니다.
장치 수	그룹에 있는 장치의 수를 표시합니다.
소유자	장치 그룹을 생성한 사용자 이름을 표시합니다.
공유	장치 그룹이 공용 그룹인지 개인 그룹인지를 표시합니다. 공용 장치 그룹은 모든 사용자가 볼 수 있지만 개인 장치 그룹은 소유자와 시스템 관리자만 볼 수 있습니다.
작업	<p>인벤토리 그룹에 대한 작업 필드는 사용자가 그룹 이름을 선택할 때까지 비어 있습니다. 사용자 정의 장치 그룹은 다음 작업을 표시합니다.</p> <ul style="list-style-type: none"> • 보기 — 선택한 장치 그룹에 포함된 장치를 표시합니다. 장치는 이 장치가 리프 장치 그룹인 경우 이 장치 그룹의 직접 하위 항목이거나 장치 그룹이 상위 장치 그룹인 경우 하위 장치 그룹의 하위 항목일 수 있습니다. 보기 옵션에 대한 자세한 내용은 187페이지의 "장치 그룹 페이지 필드"를 참조하십시오. • 편집 — 장치 그룹에 대한 정보를 편집할 수 있는 그룹 편집 페이지를 엽니다. • 삭제 — 장치 그룹을 삭제할 수 있습니다. • 다이어그램 — 다이어그램 작성을 수행하면 네트워크 장치에서 토폴로지 데이터를 수집할 수 있습니다. 자세한 내용은 758페이지의 "다이어그램 작성"을 참조하십시오. • 개인 그룹으로 변경/공용 그룹으로 변경 — 사용자가 장치 그룹을 공용 또는 개인으로 지정할 수 있습니다. 공용 장치 그룹은 모든 사용자가 볼 수 있지만 개인 장치 그룹은 소유자와 시스템 관리자만 볼 수 있습니다.

장치 예약

대규모 네트워크를 갖춘 조직에서는 누가 언제 어떤 장치로 작업하는가를 관리하는 일이 중요합니다. 장치 예약 시스템을 사용하면 특정 시간 동안 하나의 장치 또는 장치 그룹을 예약할 수 있습니다. 장치 예약 충돌 알림을 통해 사용자는 이미 유지 보수 중인 장치로 작업하는 경우를 피할 수 있으며, 대규모 IT 그룹은 제어되고 조직화된 방식으로 네트워크에서 예약 및 작업할 수 있습니다. 장치 예약 시스템 및 활동 캘린더 구성에 대한 자세한 내용은 [77페이지의 "워크플로"](#)를 참조하십시오.

멀티 태스킹 프로젝트에 속하는 하위 작업의 영향을 받는 장치 및/또는 장치 그룹은 업무 중에 자동으로 예약됩니다. 또한 멀티 태스킹 프로젝트가 승인되고 하나 이상의 예정된 작업에 다음 읽기-쓰기 작업(아래 나열됨)이 포함되어 있는 경우, 읽기-쓰기 작업이 현재 예정된 장치에만 영향을 주는지 확인하기 위한 검사가 수행됩니다. 그럴 경우 장치 예약 충돌 이벤트가 생성됩니다. 그러나 장치 예약 충돌은 사용자가 장치 또는 장치 그룹을 실행하지 못하게 합니다.

읽기/쓰기 작업에는 다음 항목이 포함됩니다.

- 구성 배포
- 명령 스크립트 실행
- 암호 배포
- 장치 재부팅
- 시작 및 실행 동기화
- 장치 소프트웨어 업데이트

멀티 태스킹 프로젝트에서 장치 또는 장치 그룹을 예약한 경우, 어떤 장치에서든 장치 구성 변경이 감지되면 이 내용이 사용자에게 알려집니다.

멀티 태스킹 프로젝트 설정에 대한 자세한 내용은 [485페이지의 "멀티 태스킹 프로젝트 예약"](#)을 참조하십시오.

활동 캘린더

활동 캘린더를 사용하면 네트워크에서 발생하는 활동을 볼 수 있습니다. 활동 캘린더는 다음을 비롯하여, 특정 날짜에 예정된 업무 및 장치 예약의 목록을 제공합니다.

- 특정 날짜에 실행하도록 예정된 모든 작업.
- 작업의 시작 시간 및 날짜.
- 작업의 지속 시간.
- 작업이 실행될 예정된 장치 및/또는 장치 그룹.
- 작업에 모호한 예약 충돌 이벤트가 있는지 여부.

모든 작업 블록은 정시 또는 30분을 경계로 시작되고 끝납니다. 따라서 특정 작업이 특정 시의 22분에 시작되면, 그 작업은 해당 시를 나타내는 행 내에 표시됩니다.

왼쪽 캘린더는 이번 달을 표시합니다. 오른쪽 캘린더는 다음 달을 표시합니다. 선택한 날은 해당 캘린더에서 강조 표시됩니다. 특정 날을 선택하려면 캘린더에 나열된 날을 클릭할 수 있습니다. 해당 날의 이벤트로 페이지가 다시 그려집니다.

오른쪽 창에 있는 달력 아래에 작업 세부사항이 표시됩니다. 다음과 같은 작업 정보가 제공됩니다.

- 시작 시간
- 기간
- 이벤트를 예약한 사용자 이름
- 이벤트 상태(예: 보류 중, 실행 중 및 성공)

활동 캘린더를 보려면 작업 아래의 메뉴 모음에서 활동 캘린더를 클릭합니다. 활동 캘린더가 열립니다. 다음 그림은 샘플 활동 캘린더를 보여줍니다.

활동 캘린더
즐거찾기에 추가 ◆ 도움말 ?

◀ 2009년 8월 14일 ▶

3 층 작업 / 예약 수

1000	스냅샷 작성	
2000		
3000		
4000		배포 압축
5000		
6000		
7000		
8000		
9000		
10000		

2009년 8월							2009년 9월							
주	일	월	화	수	목	금	주	일	월	화	수	목	금	토
30						1	35		1	2	3	4	5	
31	2	3	4	5	6	7	36	6	7	8	9	10	11	12
32	9	10	11	12	13	14	37	13	14	15	16	17	18	19
33	16	17	18	19	20	21	38	20	21	22	23	24	25	26
34	23	24	25	26	27	28	39	27	28	29	30			
35	30	31												

날짜 선택

작업

스냅샷 작성

시작 시간 : **2009년 8월 3일 10:45:05**

기간 : **7 시간**

예약자 : **Tad**

상태 : **보류 중**

lab-1000.w1
lab-6000-sw

나열된 2개 장치 또는 그룹
장치 / 그룹 목록 수정

셀에 표시된 링크를 클릭하면 작업 패널의 정보가 업데이트됩니다. 멀티 태스킹 프로젝트에 모호한 장치 예약 충돌이 있는 경우에는 셀이 노란색으로 강조 표시됩니다. 멀티 태스킹 프로젝트 구성에 대한 자세한 내용은 [485페이지의 "멀티 태스킹 프로젝트 예약"](#)을 참조하십시오.

장치 세부사항 보기

장치 세부사항 페이지에서는 장치 전용 작업을 수행할 수 있습니다. 장치 세부사항 페이지를 보려면

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다.
2. 인벤토리 페이지에서 장치를 클릭합니다. 해당 장치에 대한 장치 세부사항 페이지가 열립니다.(대부분의 다른 페이지에서 검색 기능을 사용하여 장치 세부사항 페이지를 볼 수도 있습니다.)

다음 그림은 장치 세부사항 페이지에서 수행할 수 있는 작업 개요를 보여줍니다. 메뉴 옵션은 보고 있는 장치에 따라 달라집니다.

보기	편집	프로비전	연결
장치 세부사항 ▶ 장치 홈 ACL 인터페이스 IP 주소 MAC 주소 VLAN VTP 정보 모듈 정책 서버 소프트웨어 업그레이드 / 권장 사항	스냅샷 작성 드라이버 검색 구성 편집 및 배포 인라인 구성 / 주석 편집	템플릿에서 장치 프로비전 정책 준수 확인 Syslog 구성 ACL 삭제 암호 배포 장치 재부팅 ICMP 테스트 실행 명령 스크립트 실행 진단 실행 시작 및 실행 동기화 장치 소프트웨어 업데이트 새 VLAN OS 분석 장치 컨텍스트 포트 스캔	텔넷을 사용하는 프록시를 통해 SSH 를 사용하는 프록시를 통해
단일 보기 현재 구성 구성 변경 진단 ▶ 모두 기본 IP 장치 정보 NA 감지 장치 부팅 NA 인터페이스 NA 모듈 상태 NA OSPF 인접 환경 NA 라우팅 테이블 NA 토폴로지 데이터 수집 NA VLAN 데이터 수집	장치 편집 관리되는 IP 주소 편집 장치 활성화 / 비활성화 장치 삭제 새 장치로 저장 새 템플릿으로 저장 새 메시지 프로세스 자동화		
장치 작업 장치 이벤트 장치 관계 소프트웨어 감사 추적 텔넷 /SSH 세션			

장치 세부사항 페이지 필드

필드	설명/작업
호스트 이름	장치 호스트 이름을 표시합니다. 장치의 호스트 이름을 클릭하면 이 장치에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
장치 IP	장치 IP 주소를 표시합니다. 장치 IP 주소를 클릭하면 이 장치에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
마지막 스냅샷 시도	장치 구성에 대한 스냅샷을 작성하기 위해 NA를 통해 마지막으로 장치에 액세스 한 날짜 및 시간을 표시합니다.
마지막 스냅샷 결과	이 장치 구성의 마지막 스냅샷 상태를 표시합니다. 스냅샷이 실패하면 해당 작업 결과 페이지에 대한 링크가 표시됩니다.
정보 링크	<p>해당되는 경우 장치에 대한 정보가 추가 정보에 대한 링크와 함께 표시됩니다. 예를 들어 장치가 하나 이상의 정책을 준수하지 않는 경우 정책 이벤트 링크를 클릭하여 정책 활동 페이지를 열 수 있습니다. NA에서 시작 구성과 실행 구성이 다른 것으로 확인되면 다음과 같은 링크가 표시됩니다.</p> <ul style="list-style-type: none"> • 시작 보기 — 장치 구성 페이지를 엽니다. • 시작을 실행과 비교 — 장치 구성 비교 페이지를 엽니다. • 동기화 — 새 작업 - 시작 및 실행 동기화 페이지를 엽니다.

필드	설명/작업
장치 관찰 링크	<p>장치 관찰 옵션을 처음 클릭하면, 장치를 포함하는 감시 그룹이 장치 관찰 이벤트 규칙과 함께 생성됩니다. 장치에 대한 변경 사항이 발생하면 장치를 감시하는 사용자에게 전자 메일 알림이 전송됩니다. 장치 관찰 이벤트 규칙은 다음과 같은 다양한 이벤트에 대해 전자 메일 알림을 전송합니다.</p> <ul style="list-style-type: none"> • 장치 액세스 실패 • 장치 부팅됨 • 장치 구성 변경 • 장치 삭제됨 • 장치 진단 변경됨 • 장치 편집됨 • 장치 소프트웨어 변경 • 소프트웨어 취약점이 감지됨 <p>참고: 장치 관찰 이벤트 규칙을 편집하여 이벤트를 변경할 수 있습니다. 앞으로 관찰하는 모든 장치는 동일한 이벤트 규칙 이름을 사용합니다. 571페이지의 "새 이벤트 알림 및 응답 규칙 페이지 필드"를 참조하십시오.</p> <p>감시 그룹에서 장치를 제거하려면 장치 관찰 중지를 클릭합니다.</p>
보기 메뉴	<p>보기 메뉴를 엽니다. 자세한 내용은 261페이지의 "메뉴 옵션 보기"를 참조하십시오.</p>
편집 메뉴	<p>편집 메뉴를 엽니다. 자세한 내용은 304페이지의 "편집 메뉴 옵션"를 참조하십시오.</p>
프로비전 메뉴	<p>프로비전 메뉴를 엽니다. 자세한 내용은 314페이지의 "프로비전 메뉴 옵션"를 참조하십시오.</p>
연결 메뉴	<p>연결 메뉴를 엽니다. 자세한 내용은 316페이지의 "연결 메뉴 옵션"를 참조하십시오.</p>
장치 설명	<p>장치의 사용자 정의 설명을 표시합니다(해당되는 경우).</p>
FQDN	<p>해당되는 경우 FQDN 정보를 표시합니다.</p>

필드	설명/작업
서비스 유형	서비스 유형에서는 VoIP, BGP, MPLS 등을 지정할 수 있습니다. 이 값을 사용하여 장치의 용도를 식별할 수 있습니다. 이러한 값으로 장치 서비스에 태그를 지정하면 그룹(정적 또는 동적)에서 해당 서비스를 쉽게 검색하거나 볼 수 있습니다. 참고: 장치 액세스 아래의 관리 설정을 통해 사용자 지정 서비스 유형을 생성할 수 있습니다. 43페이지의 "구성 관리 페이지 필드" 를 참조하십시오. 장치를 편집하여 이러한 값을 설정할 수도 있습니다.
주석	해당되는 경우 설명을 표시합니다.
공급업체	Nortel 또는 Cisco와 같은 장치 공급업체를 표시합니다.
모델	제조업체의 모델 번호를 표시합니다.
소프트웨어 버전	장치에서 실행 중인 운영 체제 소프트웨어의 버전을 표시합니다.
드라이버 이름	장치에 할당된 드라이버를 표시합니다.
장치 유형	라우터, 스위치, 방화벽 등의 장치 유형을 표시합니다.
일련 번호	장치의 제조업체 일련 번호를 표시합니다.
자산 태그	장치의 회사 자산 태그 번호를 표시합니다.
시스템 메모리	장치 시스템 메모리를 표시합니다.
위치	일반적으로 위치는 구성 파일에서 얻을 수 있습니다.
장치 원본	장치를 NA로 가져왔고 소스에 이름이 지정된 경우 가져오기 소스의 이름을 표시합니다. 가져오기 소스에 이름이 지정되지 않은 경우 <날짜>에 NA에 추가됨으로 표시됩니다. 장치가 수동으로 추가된 경우 "<사용자 이름>에 의해 <날짜>에 수동으로 추가함"으로 표시됩니다.
마지막으로 성공한 스냅샷	마지막으로 성공한 스냅샷의 날짜 및 시간을 표시합니다.
마지막 구성 변경	장치 구성이 마지막으로 변경된 날짜와 시간을 표시합니다.
마지막 액세스 시도	장치에 마지막으로 액세스를 시도한 날짜와 시간을 표시합니다.
마지막 액세스 성공	장치에 마지막으로 액세스한 날짜와 시간을 표시합니다.

필드	설명/작업
변경 감지 및 폴링	<p>다음 중 하나를 표시합니다.</p> <ul style="list-style-type: none"> • 사용함 — 장치의 실제 구성에 대해 저장된 구성을 확인하도록 NA가 장치를 주기적으로 폴링함을 나타냅니다. • 사용 안 함 — NA가 장치를 주기적으로 폴링하지 않거나 다른 방식으로도 장치를 관리하지 않음을 나타냅니다.
관리 상태	<p>다음 중 하나를 표시합니다.</p> <ul style="list-style-type: none"> • 활성 — NA가 장치 구성에 대한 변경 사항을 기록함을 나타냅니다. • 비활성 — NA가 변경 사항을 기록하지 않으며 NA를 통해 장치를 변경할 수 없음을 나타냅니다.
암호 규칙	암호 규칙 정보를 표시합니다.
VTP 도메인	해당되는 경우 VTP(VLAN Trunking Protocol) 도메인 이름을 표시합니다.
VTP 운영 모드	해당되는 경우 VTP(VLAN Trunking Protocol) 운영 모드를 표시합니다.
티켓 번호	티켓 번호를 표시합니다(해당되는 경우). NA 커넥터 중 하나를 설치한 경우 티켓 업데이트 버튼을 클릭하여 티켓을 업데이트할 수 있습니다.

NA/SA 통합

IT 환경에서 변경 사항을 구현하려면 네트워크 관리자와 시스템 관리자가 서로 협력해야 합니다. 서로 다른 운영 체제를 실행하는 서버 및 방화벽, 로드 밸런서, 스위치, 라우터 등을 포함하는 네트워크 장치가 있을 수 있습니다. 예를 들어, 몇몇 환경에서는 로드 밸런서와 방화벽 등 실제로 응용 프로그램의 일부인 네트워크 장치를 변경해야 합니다.

HP NA(Network Automation)를 HP SA(Server Automation)와 통합하면 다음을 수행할 수 있습니다.

- SA 서버와 NA 네트워크 장치 사이의 레이어 1 연결을 볼 수 있습니다. NA는 와이어링의 위치를 추론만 할 뿐입니다. NA는 발견적 방법(heuristics)을 최대한 사용하여 장치 및/또는 서버 사이의 물리적 연결을 확인합니다. SA에 대한 자세한 내용은 *HP Server Automation User's Guide*를 참조하십시오.
- SA 서버와 NA 네트워크 장치 사이의 레이어 2 연결을 볼 수 있습니다. NA는 네트워크 다이어그램을 더 쉽게 읽을 수 있도록 장치 및/또는 서버 사이의 데이터 링크 연결 수를 줄입니다. 종속적인 연결을 통해 추론할 수 있는 연결만 감소됩니다. 자세한 내용은 **758페이지의 "다이어그램 작성"**을 참조하십시오.
- 특정 NA 네트워크 장치에 표시되는 SA 서버에 대한 정보를 볼 수 있으며, 그 반대로 어떤 네트워크 장치에서 특정 SA 서버가 표시되는지를 볼 수 있습니다.

NA/SA 통합을 설정하려면 NA 토폴로지 데이터 수집 진단을 실행해야 합니다. 이 진단은 모든 스위치에 대한 MAC 주소를 수집하도록 NA에 지시합니다. MAC 주소는 레이어 2와 레이어 1 연결을 검색하여 추가해야 합니다.

레이어 1 연결(와이어링)을 레이어 2 연결(ARP 테이블)로부터 추론할 수 있는 경우도 있습니다. 이를 통해 이중 및 속도 설정과 같은 구성 불일치를 감지할 수 있습니다.

- NA/SA 통합 구성에 대한 자세한 내용은 **97페이지의 "사용자 인증"**을 참조하십시오.
- 네트워크 다이어그램 작성에 대한 자세한 내용은 **758페이지의 "다이어그램 작성"**을 참조하십시오.

- 이중 및 속도 설정을 비롯한 인터페이스 세부사항 보기에 대한 자세한 내용은 [269 페이지의 "인터페이스 세부사항 페이지 필드"](#)를 참조하십시오.
- SA 서버 보기에 대한 자세한 내용은 [292페이지의 "서버 페이지 필드"](#)를 참조하십시오.

NA/SA 권한

NA와 SA를 통합하면 동일한 사용자 이름과 암호를 사용하여 두 시스템에 로그인할 수 있습니다. 그러나 해당 사용자가 SA와 NA에서 어떤 SA 서버를 볼 수 있는가는 사용자의 SA 권한에 의해 제어됩니다. 마찬가지로 해당 사용자가 NA와 SA에서 어떤 네트워크 장치를 볼 수 있는가는 NA 사용자의 권한에 의해 제어됩니다.

NA를 구성할 때 SA 사용자 이름과 암호를 지정할 수 있습니다. [102페이지의 "사용자 인증 페이지 필드"](#) 정보를 참조하십시오. NA가 토폴로지 수집 진단을 통해 MAC 주소를 읽을 때 어떤 SA 서버가 발견될 것인지는 SA 사용자의 권한에 의해 제어됩니다. 사용자는 권한을 가지고 있는 SA 서버만 볼 수 있으므로, 모든 SA 서버를 볼 수 있는 SA 사용자를 지정하는 것이 좋습니다. 이렇게 하면 알려진 모든 SA 서버가 NA의 해당 MAC 주소로 매핑됩니다.

예를 들면 다음과 같습니다.

- Server1의 MAC 주소는 0060839488A1입니다.
- SA 사용자 A는 Server1을 볼 수 있습니다.
- SA 사용자 B는 Server1을 볼 수 없습니다.
- 스위치 S7은 Server1에 연결됩니다.

SA 사용자 A를 Twist 서버 사용자 이름으로 사용하도록 NA가 구성된 경우 토폴로지 수집 진단이 실행될 때 NA는 0060839488A1을 Server1에 매핑합니다. SA 사용자 A는 NA에 로그인할 경우 스위치 S7에 대한 서버 페이지(장치 세부사항 페이지)에서 Server1을 볼 수 있습니다. SA 사용자 B는 Server1을 볼 수 있는 권한이 없으므로 NA에 로그인할 경우 서버 페이지에서 Server1을 볼 수 없습니다.

장치 하드웨어 정보

NA와 SA를 통합하면 관리되는 SA 서버 및 NA 네트워크 장치에 대한 기본 하드웨어 세부사항 외에 네트워크 인터페이스의 다음 정보에 대한 보고서도 작성됩니다.

- 서버 측에서 볼 때 네트워크 인터페이스는 이더넷 인터페이스, MAC 주소, 연결된 장치, VLAN 이름, 이중 및 속도 설정 등을 식별합니다.
- 네트워크 장치 측에서 볼 때 네트워크 인터페이스는 이더넷 포트, 속도 및 이중 설정, 연결된 장치를 식별합니다. 자동 협상 모드가 NA의 네트워크 인터페이스에서 설정된 후 SA의 네트워크 카드에서 협상됩니다. 이 구성을 정의하는 정책을 생성할 수 있습니다(예: 이중을 전이중(자동)으로, 속도를 100(자동)으로 지정하는 정책).

자세한 내용은 [267페이지의 "장치 인터페이스 페이지 필드"](#)를 참조하십시오.

방화벽을 통해 NA에 연결

NA API(Application Program Interface)는 Java RMI(Java Remote Method Invocation)를 사용하여 NA 서버에 연결합니다. Java RMI는 여러 프로토콜에서 실행할 수 있습니다. NA는 JRMP(Java Remote Method Protocol)를 통한 Java RMI만 지원합니다. SA와 NA를 통합할 경우 SA는 NA API를 사용합니다. 그 결과 Java RMI와 JRMP는 다음 포트를 사용합니다.

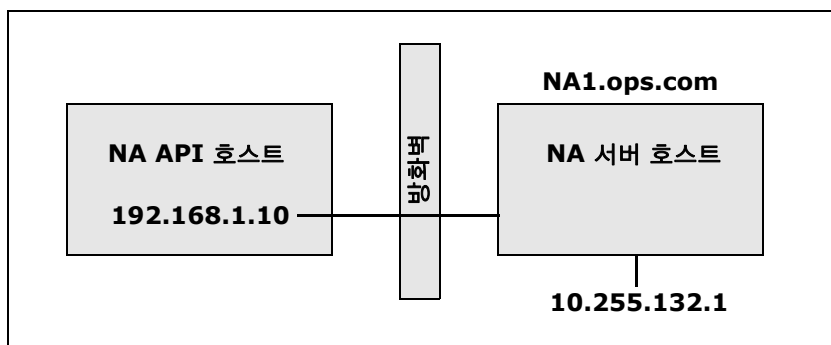
- JNDI(Java Naming and Directory Interface)(일반적으로 포트 1099)
- RMI(일반적으로 동적인 포트 1098)
- RMI Object(일반적으로 포트 4444)

방화벽을 통해 NA API를 사용하려면 다음을 수행합니다.

1. 포트 1098, 1099 및 4444를 허용하도록 방화벽을 구성합니다. NA 서버가 방화벽 양쪽에 동일한 IP 주소를 가지고 있으면 구성이 완료됩니다. NA 서버 호스트가 방화벽 외부에 다른 IP 주소를 가지고 있으면 2단계로 계속 진행합니다.
2. IP 주소 대신 RMI 서버 호스트 이름을 사용하도록 NA를 구성합니다. 이 작업을 수행하려면 `$NA/server/ext/jboss/server/default/conf/jnp.properties` 파일을 작성하여 `java.rmi.server.useLocalHostname=true`를 포함합니다.

3. 파일을 저장하고 NA 서버를 다시 시작합니다.
4. NA 서버 호스트와 NA API 호스트(SA와 NA를 통합한 경우 SA 서버 호스트)에서 호스트 이름 확인이 올바른지 확인합니다.

다음의 예에서 NA는 호스트 이름 NA1.ops.com 및 IP 주소 10.255.132.1에서 실행되고 있습니다. 방화벽 외부에서 NA1.ops.com에 액세스하려면 192.168.1.10을 사용해야 합니다. NA 서버 호스트(10.255.132.1)는 NA1.ops.com을 올바르게 확인해야 합니다. NA API 호스트에서 NA1.ops.com은 192.168.1.10을 올바르게 확인해야 합니다.



높은 수준에서, Java RMI/JRMP 프로토콜은 다음과 같이 수행됩니다.

1. 클라이언트는 호스트 192.168.1.10에서 JNDI 포트(1099)에 연결됩니다.
2. 클라이언트 쿼리: bean Connect는 어디에 있습니까?
3. 서버 응답: 호스트 na1.ops.com의 포트 1098에 있습니다.
4. 클라이언트는 na1.ops.com에 대한 IP 주소를 조회합니다.
5. 클라이언트는 호스트 192.168.1.10에서 포트 1098에 연결됩니다.
6. 클라이언트에서 새로운 Java.class 파일을 요구하면 클라이언트는 호스트 192.168.1.10에서 포트 4444에 연결됩니다.

포트 변경

JNDI 포트를 변경하려면 다음을 수행합니다.

1. 예를 들면 `$NA/server/ext/jboss/server/default/conf/jboss-service.xml` 파일을 편집하여 1099를 1199로 변경합니다.
2. 파일을 저장하고 NA 서버를 다시 시작합니다. (참고: JNDI 포트를 변경할 경우 NA API를 호출하는 코드도 변경해야 합니다. 예를 들면 NA API를 `na1.ops.com:1099`에 연결하는 대신 `na1.ops.com:1199`(또는 기타 구성된 포트)에 연결해야 합니다.)

RMI 포트를 변경하려면

1. 예를 들면 `$NA/server/ext/jboss/server/default/conf/jboss-service.xml` 파일을 편집하여 1098를 1198로 변경합니다.
2. 파일을 저장하고 NA 서버를 다시 시작합니다. (참고: RMI 포트에 대한 변경 사항은 클라이언트에 대해 투명합니다. 클라이언트 변경은 필요하지 않습니다.)

RMI Object 포트를 변경하려면

1. 예를 들면 `$NA/server/ext/jboss/server/default/conf/jboss-service.xml` 파일을 편집하여 4444를 4445로 변경합니다.
2. 파일을 저장하고 NA 서버를 다시 시작합니다. (참고: RMI Object 포트에 대한 변경 사항은 클라이언트에 대해 투명합니다. 클라이언트 변경은 필요하지 않습니다.)

잘못된 포트 개수

포트 개수가 잘못된 경우 다음을 수행하여 계산되는 포트 유형을 구성합니다.

1. NA를 중지합니다.
2. `$NA/adjustable_options.rcx` 파일을 업데이트하고 `<options>` 태그와 `</options>` 태그 사이에 다음 항목을 추가합니다.

```
<array name="PortCount/PortTypes">
<value>Ethernet</value>
<value>FastEthernet</value>
<value>GigEthernet</value>
<value>FDDI</value>
<value>Lex</value>
<value>TokenRing</value>
<value>VGAnyLan</value>
<value>Pos</value>
<value>Serial</value>
<value>HSSI</value>
<value>ATM</value>
<value>Dialer</value>
<value>BRI</value>
<value>DSL</value>
<value>TenGigabitEthernet</value>
<value>GigEthernetTrunk</value>
</array>
```

참고: 개수를 계산할 인터페이스/포트 유형에 적합하게 위의 목록을 편집합니다.

3. `$NA`를 `NA`가 설치된 위치(일반적으로 `/opt/na`)로 바꿉니다.
4. `$NA/adjustable_options.rcx` 파일을 업데이트하고 `<options>` 태그와 `</options>` 태그 사이에 다음 항목을 추가합니다.

```
<option name="snapshot/force_update_model_data">true</option>
```

참고: 이 옵션을 사용하면 `NA`가 구성 변경이 없어도 모든 검사점 스냅샷에서 포트 개수 및 기타 장치 데이터를 다시 계산합니다.

5. NA를 다시 시작합니다.
6. 인벤토리에 대해 스냅샷 작업을 실행하여 포트 개수를 업데이트합니다.
7. 새 작업 페이지에서 스냅샷을 검사점으로 만들기 옵션을 확인합니다. 이렇게 하면 기존 장치에 대한 포트 개수가 다시 계산됩니다.

참고: 참고: 스냅샷 작업을 실행한 후 *\$NA/adjustable_options.rcx* 파일에서 `<option name="snapshot/force_update_model_data">true</option>`을 제거해야 할 수도 있습니다.

메뉴 옵션 보기

메뉴 옵션	설명/작업
장치 세부사항	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none">• 장치 홈 — 해당 장치에 대한 장치 세부사항 페이지를 엽니다.• ACL — 이 장치와 연관된 모든 ACL의 목록을 볼 수 있는 장치 ACL 페이지를 엽니다. 자세한 내용은 874페이지의 "ACL 보기"를 참조하십시오.• 인터페이스 — 장치의 인터페이스, 각 인터페이스를 통해 연결되는 업스트림 및 다운스트림 장치의 목록을 볼 수 있는 장치 인터페이스 페이지를 엽니다. 연결된 장치를 능동적으로 관리할 경우 해당 장치에 대한 링크가 생성됩니다. 이 링크를 사용하면 문제 해결 시 네트워크 다이어그램을 조회할 필요 없이 레이어 3 토폴로지를 통과할 수 있습니다. (참고: 인터페이스 진단을 실행하면 장치 인터페이스 페이지가 업데이트됩니다. 기본적으로 NA가 구성 변경을 감지할 때 이 진단이 실행됩니다.) 자세한 내용은 267페이지의 "장치 인터페이스 페이지 필드"를 참조하십시오.• IP 주소 — 장치와 연관된 모든 IP 주소를 볼 수 있는 장치 IP 주소 페이지를 엽니다. 여기에는 장치에 대한 인터페이스의 IP 주소는 물론 장치에서 보이는 네트워크의 IP 주소도 포함됩니다. 자세한 내용은 274페이지의 "장치 IP 주소 페이지 필드"를 참조하십시오.• MAC 주소 — 장치와 연관된, NA에서 인식되는 모든 MAC 주소의 목록을 볼 수 있는 장치 MAC 주소 페이지를 엽니다. 자세한 내용은 276페이지의 "장치 MAC 주소 페이지 필드"를 참조하십시오.• VLAN — 장치에서 구성된 VLAN 정보를 볼 수 있는 VLAN 페이지를 엽니다. 자세한 내용은 280페이지의 "장치 VLAN 페이지 필드"를 참조하십시오.

메뉴 옵션	설명/작업
장치 세부사항(계속)	<ul style="list-style-type: none"> • VTP 정보 — VLAN에 대한 VTP 정보를 볼 수 있는 VTP 세부사항 페이지를 엽니다. 자세한 내용은 285페이지의 "VTP 세부사항 페이지 필드"를 참조하십시오. • 모듈 — 장치에 설치된 모듈(블레이드, 카드)의 목록을 볼 수 있는 장치 블레이드/모듈 페이지를 엽니다. 기본적으로 모듈 데이터는 매주 모듈 상태 진단에 의해 업데이트됩니다. 자세한 내용은 289페이지의 "장치 블레이드/모듈 페이지 필드"를 참조하십시오. • 정책 — 장치에 올바른 정책이 적용되었는지 확인할 수 있는 장치 정책 페이지를 열고, 정책의 통과 여부를 확인하며, 장치가 NA에 추가될 때 장치에 적용된 정책을 확인하고, 장치에 적용된 정책에 대한 예외 사항을 볼 수 있습니다. 자세한 내용은 290페이지의 "장치 정책 페이지 필드"를 참조하십시오. • 서버 — 장치에 연결된 HP SA(Server Automation) 서버 목록을 볼 수 있는 서버 페이지를 엽니다. 자세한 내용은 292페이지의 "서버 페이지 필드"를 참조하십시오. • 소프트웨어 업그레이드 권장 사항 — 모든 장치 소프트웨어 이미지 권장 사항을 볼 수 있는 소프트웨어 업그레이드 권장 사항 페이지를 엽니다. 단, 내 기본 설정 페이지에서 지정한 필터로 제거한 내용은 제외됩니다. 자세한 내용은 293페이지의 "장치 소프트웨어 이미지 권장 사항 페이지 필드"를 참조하십시오.
단일 보기	<p>단일 장치 또는 한 페이지의 모든 장치에 대한 변경 사항을 나타내는 이벤트를 추적할 수 있는 단일 보기 페이지를 엽니다. 자세한 내용은 680페이지의 "이벤트 통합 보기(단일 보기)"를 참조하십시오.</p>
현재 구성	<p>장치의 실행 구성에 대해 구성을 배포할 수 있는 현재 구성 페이지를 엽니다. 자세한 내용은 224페이지의 "장치 구성 페이지 필드"를 참조하십시오.</p>
구성 변경	<p>두 장치 구성을 나란히 볼 수 있는 장치 구성 페이지를 엽니다. 자세한 내용은 231페이지의 "장치 구성 비교"를 참조하십시오.</p>

메뉴 옵션	설명/작업
진단	<p>진단 목록에서 옵션을 선택합니다. 각 옵션은 장치에 대한 진단의 기록 목록을 보여줍니다. 가장 자주 사용되는 진단은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 모두 — 한 페이지에 대한 모든 진단을 표시합니다. • 기본 IP — 기본 게이트웨이, DNS 서버, 도메인 목록, 설치된 인터페이스에 할당된 IP 주소와 같은 기본 IP 정보를 표시합니다. • 메모리 문제 해결 — 이 진단은 일부 장치에 대해 구현되는 샘플 사용자 지정 진단이며, 장치 구성 변경 이후 표준 진단으로서 포함됩니다. • 장치 정보 — 소프트웨어 및 하드웨어 버전, 장치의 모델 및 호스트 이름, 인터페이스 설명과 같은 기본 장치 정보를 표시합니다. 이 정보는 기본 진단과 함께 나타나지만 NA가 장치에서 스냅샷 작업을 실행할 때에만 업데이트됩니다. • NA 감지 장치 부팅 — 장치가 마지막으로 부팅된 시기에 대한 정보를 표시합니다. • NA 장치 파일 시스템 — 현재 장치의 플래시 카드 또는 하드 드라이브에 있는 파일(일반적으로 소프트웨어 이미지 파일)을 기록합니다. 이 데이터는 소프트웨어 배포 작업에 사용됩니다.

메뉴 옵션	설명/작업
진단(계속)	<ul style="list-style-type: none"> • NA 이중 데이터 수집 — 인터페이스 보고서에 대한 현재 포트 설정 및 이중 설정 등 레이어 2 연결 데이터를 수집합니다. 일부 장치는 이 진단을 지원하지 않습니다. 또한 볼 수 있는 진단 출력이 없습니다. • NA 플래시 저장 공간 — 이 진단은 Nortel BayRS 장치에 대해서만 사용되는 특정 용도의 진단으로서, 낮은 플래시 공간 이벤트를 트리거한 다음 압축 스크립트를 실행합니다. • NA 인터페이스 — 상태, IP 주소, 오류, I/O 비율, VLAN 정보 등 장치에 대한 인터페이스 정보를 표시합니다. • NA 모듈 상태 — 이 장치에 대한 모듈 진단을 표시합니다. • NA OSPF 인접 환경 — NA 데이터베이스에 저장된 OSPF 인접 환경 테이블의 목록을 표시합니다. • NA 라우팅 테이블 — NA 데이터베이스에 저장된, 이 장치에 대한 모든 라우팅 테이블을 표시합니다. BGP가 실행 중인 경우 라우팅 테이블 요약 정보도 표시합니다(사용 가능한 경우). • NA 토폴로지 데이터 수집 — 이 진단은 다이어그램 작성 및 토폴로지 보고서에 사용되는 테이블을 채우는 데 사용됩니다. 볼 수 있는 진단 출력은 가지고 있지 않습니다. • NA VLAN 데이터 수집 — 이 진단은 최신 VLAN 정보를 수집하는 데 사용됩니다. 새 장치 VLAN 및 장치 편집 VLAN 페이지는 해당 장치에서 마지막으로 수집된 VLAN 데이터를 기반으로 합니다. VLAN 데이터를 최신 상태로 유지하려면 VLAN 데이터 수집 진단을 실행하여 NA를 최신 VLAN 데이터로 업데이트합니다. (참고: 이 진단을 수행해도 데이터베이스에 진단 텍스트가 저장되지 않습니다. 이 진단은 데이터베이스에서 특정 테이블만 업데이트합니다. 결과적으로 이 진단을 볼 수 없습니다. • NA 포트 스캔 — 이 진단은 Nmap을 사용하여 장치의 포트를 검색하고 열린 포트와 이러한 포트에서 제공하는 서비스에 대해 세부사항을 반환합니다.
장치 작업	<p>이 장치와 연관된 모든 작업 목록을 볼 수 있는 장치 작업 페이지를 엽니다. 또한 이 페이지에서 작업에 대한 세부사항을 보거나 작업을 다시 실행할 수도 있습니다. 장치 작업 페이지에 대한 자세한 내용은 297페이지의 "장치 작업 페이지 필드"를 참조하십시오.</p>

메뉴 옵션	설명/작업
장치 이벤트	성공/실패 상태 등 장치에 대한 최근 시스템 이벤트를 보고, 요약 필드에 있는 링크를 클릭하여 이벤트에 대한 자세한 정보에 액세스할 수 있는 장치 이벤트 페이지를 엽니다. 장치 이벤트 페이지 필드에 대한 자세한 내용은 266페이지의 "장치 이벤트 페이지 필드" 를 참조하십시오.
장치 관계	장치 관계 페이지를 엽니다. 장치 관계를 사용하면 장치 간에 관계를 설정하고 관계를 볼 수 있습니다. 장치 관계에 대한 자세한 내용은 299페이지의 "장치 관계 페이지 필드" 를 참조하십시오.
소프트웨어 감사 추적	장치에 어떤 소프트웨어가 로드되었는지를 볼 수 있는 장치 소프트웨어 이력 페이지를 엽니다. 장치에 로드된 소프트웨어 페이지 필드에 대한 자세한 내용은 301페이지의 "장치 소프트웨어 이력 페이지 필드" 를 참조하십시오.
텔넷/SSH 세션	장치와 연관된 텔넷 및 SSH 세션 목록을 볼 수 있는 장치 세션 페이지를 엽니다. 세션은 전체 세션에 대해 기록된 명령 또는 키 입력만 포함할 수 있습니다. 장치 세션 페이지 필드에 대한 자세한 내용은 303페이지의 "장치 세션 페이지 필드" 를 참조하십시오.

대부분의 NA 진단은 제품과 함께 제공되며 편집할 수 없는 표준 진단입니다. 단, 다음의 샘플 진단은 예외입니다.

- 메모리 문제 해결
- 하드웨어 정보

장치 이벤트 페이지 필드

장치 이벤트 페이지에서는 성공/실패 상태 등 장치에 대한 최근 시스템 이벤트를 보고, 이벤트에 대한 자세한 정보에 액세스할 수 있습니다.

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 이벤트를 삭제할 수 있습니다. 이벤트를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 이벤트를 선택하거나 선택 취소할 수 있습니다.
이벤트 날짜	이벤트가 발생한 날짜 및 시간을 표시합니다.
요약	이벤트에 대한 간단한 요약 표시합니다. 요약 링크를 클릭하면, 이벤트에 대한 자세한 정보를 볼 수 있는 이벤트 세부사항 페이지가 열립니다.
추가한 사람	이벤트를 시작한 사람 또는 프로세스를 표시합니다.

장치 인터페이스 페이지 필드

장치 인터페이스 페이지에서는 장치의 인터페이스 및 각 인터페이스를 통해 연결된 업스트림 장치와 다운스트림 장치의 목록을 볼 수 있습니다. 포트는 계층 2 조건이고 인터페이스는 계층 3 조건이지만 NA에서는 차이가 없습니다.

장치 인터페이스 페이지를 보려면 장치에 대한 보기 메뉴에서 장치 세부사항을 선택하고 인터페이스를 클릭합니다. 장치 인터페이스 페이지가 열립니다.

필드	설명/작업
포트 이름	Ethernet0 또는 Serial1과 같은 포트의 이름을 표시합니다.
포트 유형	FastEthernet이 같은 포트 유형의 이름을 표시합니다.
포트 상태	인터페이스가 작동하도록 구성(Configured Up)되었는지, 관리를 위해 작동이 중지(Administratively Down)되었는지를 표시합니다. (참고: 이것은 인터페이스의 프로토콜 상태를 나타내는 것이 아니라 구성된 상태만을 나타냅니다.)
실행 중인 포트 상태	포트의 레이어 2 연결을 지정합니다(위로 또는 아래로). 이 정보는 NA 이중 데이터 수집 진단에서 수집됩니다. 자세한 내용은 397페이지의 "진단 실행 작업 페이지 필드" 를 참조하십시오.
포트 IP	인터페이스의 기본 IP 주소를 표시합니다. NA는 장치 구성으로부터 IP 주소를 구문 분석합니다. 자세한 내용은 224페이지의 "장치 구성 페이지 필드" 를 참조하십시오.
설명	인터페이스에 대한 간단한 설명을 표시합니다. NA는 장치 구성으로부터 설명을 구문 분석합니다.
협상 이중	협상 이중(전이중 또는 반이중)을 표시합니다. 이 정보는 토폴로지 데이터 수집 진단을 통해 수집됩니다. 자세한 내용은 397페이지의 "진단 실행 작업 페이지 필드" 를 참조하십시오.

필드	설명/작업
작업	<p>각 인터페이스에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 인터페이스 편집 — 이 인터페이스 및 사용자 지정 데이터 필드에 대한 세부사항을 편집할 수 있는 인터페이스 편집 세부사항 페이지를 엽니다. 271페이지의 "인터페이스 편집 세부사항 페이지 필드"를 참조하십시오. • 인터페이스 보기 — 이 인터페이스와 사용자 지정 데이터에 대한 세부사항을 보고, 대체 IP 주소 및 연결된 서버를 보고, 주석을 보고 편집할 수 있는 인터페이스 세부사항 페이지를 엽니다. 269페이지의 "인터페이스 세부사항 페이지 필드"를 참조하십시오. SA 서버 관리에 대한 자세한 내용은 <i>HP Server Automation User's Guide</i>를 참조하십시오. • 서브넷의 인터페이스 — 이 인터페이스와 동일한 서브넷의 모든 인터페이스를 볼 수 있는 서브넷의 인터페이스 페이지를 엽니다. 장치들이 능동적으로 관리되는 한, 서브넷 내에 연결된 장치들을 통과할 수 있습니다. 273페이지의 "서브넷의 인터페이스 페이지 필드"를 참조하십시오.

인터페이스 세부사항 페이지 필드

인터페이스 세부사항 페이지에서는 특정 인터페이스에 대한 세부사항을 볼 수 있습니다. 포트는 레이어 2 용어이고 인터페이스는 레이어 3 용어지만 NA는 이 둘을 구분하지 않습니다.

필드	설명/작업
장치	장치의 이름 및 IP 주소를 표시합니다.
이름	인터페이스 이름을 표시합니다(예: Ethernet0/1).
유형	인터페이스 유형을 표시합니다(예: Ethernet).
상태	인터페이스 상태를 표시합니다(예: Configured Up).
연결 대상	인터페이스가 연결되어 있는 서버를 표시합니다.
기본 IP	인터페이스의 기본 IP 주소를 표시합니다. 서브넷의 인터페이스 링크를 클릭하면 이 인터페이스와 동일한 서브넷의 모든 인터페이스를 볼 수 있는 장치 인터페이스 페이지가 열립니다. 장치들이 능동적으로 관리되는 한, 서브넷 내에 연결된 장치들을 통과할 수 있습니다. 자세한 내용은 267페이지의 "장치 인터페이스 페이지 필드" 를 참조하십시오.
설명	인터페이스에 대한 설명을 표시합니다.
MAC 주소	인터페이스의 MAC 주소를 표시합니다(예: 00-50-10-F6-41).
멤버 VLAN	이 장치가 속해 있는 VLAN을 표시합니다. VLAN 이름 링크를 클릭하면 VLAN에 대한 VLAN 세부사항 페이지가 열립니다. 자세한 내용은 283페이지의 "VLAN 세부사항 페이지 필드" 를 참조하십시오. VLAN에 대한 자세한 내용은 278페이지의 "VLAN(가상 로컬 영역 네트워크)" 을 참조하십시오. 참고: 트렁크 포트에 기본 VLAN(태그 지정되지 않은 VLAN)이 없으면 기본 VLAN이 멤버 VLAN 목록 하단에 표시되지 않습니다.
이중	네트워크 인터페이스는 이더넷 포트, 속도, 이중 설정, 연결된 장치 및 VLAN 이름을 식별합니다. 자동 협상 모드가 NA의 네트워크 인터페이스에서 설정된 후 SA의 네트워크 카드에서 협상됩니다. 이중 불일치는 관리되는 서버와 연결된 네트워크 장치의 속도 및 이중 사이의 구성 불일치입니다.
속도	네트워크 인터페이스는 이더넷 포트, 속도, 이중 설정, 연결된 장치 및 VLAN 이름을 식별합니다. 자동 협상 모드가 NA의 네트워크 인터페이스에서 설정된 후 SA의 네트워크 카드에서 협상됩니다. 속도 불일치는 관리되는 서버와 연결된 네트워크 장치의 속도 및 이중 사이의 구성 불일치입니다.

필드	설명/작업
구성	인터페이스의 현재 구성을 표시합니다. 구성 보기 링크를 클릭하면 현재 구성 페이지가 열립니다. Configlet 구문 분석을 통해 파서는 인터페이스 관련 구성의 라인을 추출합니다.
VRF	<p>인터페이스와 연관된 VRF(가상 라우팅 및 전달)를 정의하는 장치 구성 섹션을 표시합니다. VRF를 사용하면 동일한 라우터 내에서 라우팅 테이블의 여러 인터페이스가 동시에 존재할 수 있습니다. 라우팅 인터페이스가 독립적이므로 서로 충돌 없이 동일 또는 중복 IP 주소를 사용할 수 있습니다.</p> <p>참고: 이 필드는 인터페이스에 연관된 VRF가 있고 장치 드라이버가 VRF 구문 분석을 지원하는 경우에만 표시됩니다.</p>
QoS	QoS(Quality of Service) 정보를 표시합니다. NA에서는 QoS 구성 명령문에 대한 인터페이스 구성을 구문 분석하고 해당 전역 구성 정보를 표시합니다. 즉, 인터페이스 구성과 관련되지만 해당 인터페이스 구성에 포함되지 않는 구성 부분이 표시됩니다. 여기에는 라우팅 맵, 정책 맵, 클래스 맵 및 ACL이 포함됩니다. 이러한 정보는 보다 광범위한 장치 구성 보기 및 네트워크가 현재 상태(패킷 손실, 특정 패킷 유형에 대한 긴 지연 등)로 수행되는 원인을 제공합니다.
ACL	인터페이스에 존재하는 것으로 확인된 ACL을 표시합니다.
마지막 수정일	인터페이스가 마지막으로 수정된 시점을 표시합니다.
주석	인터페이스에 대한 주석을 표시합니다.
편집 세부사항 링크	인터페이스 편집 세부사항 페이지가 열립니다. 271페이지의 "인터페이스 편집 세부사항 페이지 필드" 를 참조하십시오.

인터페이스 편집 세부사항 페이지 필드

인터페이스 편집 세부사항 페이지를 사용하면 인터페이스에 대한 세부사항과 사용자 지정 데이터 필드를 편집할 수 있습니다.

인터페이스 편집 세부사항 페이지로 이동하려면

1. 장치 세부사항 페이지에서 보기 메뉴를 선택합니다.
2. 보기 메뉴에서 장치 세부사항을 선택하고 인터페이스를 클릭합니다. 장치 인터페이스 페이지를 엽니다.
3. 작업 필드에서 편집하려는 포트에 대한 인터페이스 편집 링크를 클릭합니다. 인터페이스 편집 세부사항 페이지가 열립니다.

참고: 인터페이스 편집 세부사항 페이지에는 트렁크 포트를 구성하기 위한 섹션이 포함되어 있습니다. VLAN 트렁크 확인란을 사용하면 트렁크 포트를 설정할 수 있습니다. 이 섹션은 표에 설명된 것처럼 기본 VLAN ID 및 멤버 VLAN 등 선택한 경우에 표시되는 축소 가능한 필드 세트입니다.

필드	설명/작업
장치	장치의 이름 및 IP 주소를 표시합니다.
이름	인터페이스 이름을 표시합니다(예: Ethernet0/1).
유형	인터페이스 유형을 표시합니다(예: Ethernet).
상태	인터페이스 상태를 표시합니다(예: Configured Up).
연결 대상	인터페이스가 연결되어 있는 서버를 표시합니다.
기본 IP	인터페이스의 기본 IP 주소를 표시합니다. 서브넷의 인터페이스 링크를 클릭하면 이 인터페이스와 동일한 서브넷의 모든 인터페이스를 볼 수 있는 장치 인터페이스 페이지가 열립니다. 장치들이 능동적으로 관리되는 한, 서브넷 내에 연결된 장치들을 통과할 수 있습니다.
설명	인터페이스에 대한 설명을 표시합니다.
MAC 주소	인터페이스의 MAC 주소를 표시합니다(예: 00-50-10-F6-41).
멤버 VLAN	이 장치가 속해 있는 VLAN을 표시합니다. VLAN에 대한 자세한 내용은 278페이지 의 " VLAN(가상 로컬 영역 네트워크) "을 참조하십시오.

필드	설명/작업
이중	네트워크 인터페이스는 이더넷 포트, 속도, 이중 설정, 연결된 장치 및 VLAN 이름을 식별합니다. 자동 협상 모드가 NA의 네트워크 인터페이스에서 설정된 후 SA의 네트워크 카드에서 협상됩니다. 이중 불일치는 관리되는 서버와 연결된 네트워크 장치의 속도 및 이중 사이의 구성 불일치입니다.
속도	네트워크 인터페이스는 이더넷 포트, 속도, 이중 설정, 연결된 장치 및 VLAN 이름을 식별합니다. 자동 협상 모드가 NA의 네트워크 인터페이스에서 설정된 후 SA의 네트워크 카드에서 협상됩니다. 속도 불일치는 관리되는 서버와 연결된 네트워크 장치의 속도 및 이중 사이의 구성 불일치입니다.
VLAN 트렁크	<p>특정 포트를 트렁크 포트, 물리적 포트 및 포트 채널(집계된 링크)로 구성할 수 있습니다. VLAN 인터페이스용 포트와 루프백 포트를 트렁크로 구성할 수 없습니다. VLAN 트렁크의 선택을 취소하면 포트가 비 트렁크로 설정됩니다. 따라서 기본 VLAN ID 필드에 표시된 VLAN에 포트가 할당됩니다. VLAN 트렁크 포트 설정을 수정하면 장치에 변경 내용을 적용하기 위한 새 VLAN 작업이 생성됩니다. 자세한 내용은 452페이지의 "VLAN 작업 페이지 필드"를 참조하십시오.</p> <p>참고: 장치 드라이버에서 향상된 VLAN 기능을 지원하지 않는 경우 인터페이스 편집 세부사항 페이지에 VLAN 트렁크 필드가 표시되지 않습니다.</p>
기본 VLAN ID	기본 VLAN ID는 트렁크 포트에서 패킷에 태그가 지정되지 않은 VLAN입니다. 또한 해당 포트에서 수신되는 태그가 지정되지 않은 모든 패킷을 기본 VLAN의 패킷으로 간주됩니다. 기본 VLAN은 Cisco 용어입니다. 예를 들어 ProCurve에서는 기본 VLAN 용어를 사용하지 않습니다. ProCurve에서는 태그가 지정되지 않은 VLAN 멤버십 용어를 사용합니다. 트렁크 포트 하나에서 사용할 수 있는 태그가 지정되지 않은 VLAN 멤버십은 하나뿐입니다.
멤버 VLAN	VLAN 트렁크 포트는 선택한 VLAN의 트래픽을 전송합니다. 선택되지 않은 VLAN이 정리됩니다.
VLAN ID 지정	Cisco 장치의 경우 트렁크 포트에 대해 VLAN ID 또는 VLAN ID 범위를 지정할 수 있습니다. Cisco 장치의 트렁크 포트는 장치에 정의되지 않은 VLAN의 멤버일 수 있습니다. 이 필드는 비 Cisco 장치에는 표시되지 않습니다.
주석	인터페이스에 대한 주석을 표시합니다.

서브넷의 인터페이스 페이지 필드

서브넷의 인터페이스 페이지에서는 협상 이중 및 협상 속도 설정과 함께 서브넷의 인터페이스를 볼 수 있습니다. 레이어 3 인터페이스는 서브넷의 다른 인터페이스와 비교됩니다. 불일치가 있을 경우 일치하지 않는 포트의 값은 빨간색 텍스트로 굵게 표시됩니다.

필드	설명/작업
호스트 이름	인터페이스가 상주하는 호스트의 이름 또는 IP 주소를 표시합니다.
포트 이름	Ethernet0 또는 Serial1과 같은 포트의 이름을 표시합니다.
포트 상태	인터페이스가 작동하도록 구성(Configured Up)되었는지, 관리를 위해 작동이 중지(Administratively Down)되었는지를 표시합니다. (참고: 이것은 인터페이스의 프로토콜 상태를 나타내는 것이 아니라 구성된 상태만을 나타냅니다.)
포트 IP	인터페이스의 기본 IP 주소를 표시합니다. NA는 장치 구성으로부터 IP 주소를 구문 분석합니다.
설명	인터페이스에 대한 간단한 설명을 표시합니다. NA는 장치 구성으로부터 설명을 구문 분석합니다.
협상 이중	협상 이중(전이중 또는 반이중)을 표시합니다. 이 정보를 사용하면 스위치를 통과하는 트래픽이 전이중 100M 또는 반이중 10M에서 작동하는 다른 스위치의 영향을 받는지 확인할 수 있습니다. 예를 들어 일부 경로에서 발생하는 지연으로 인해 패킷을 강제로 대기열에 배치하는 스위치가 네트워크에 있을 수 있습니다.
협상 속도	100M와 같은 협상 속도를 표시합니다.
작업	<p>각 인터페이스에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 인터페이스 편집 — 이 인터페이스 및 사용자 지정 데이터 필드에 대한 세부사항을 편집할 수 있는 인터페이스 편집 페이지를 엽니다. • 인터페이스 보기 — 이 인터페이스와 사용자 지정 데이터에 대한 세부사항을 보고, 대체 IP 주소 및 연결된 서버를 보고, 주석을 보고 편집할 수 있는 인터페이스 세부사항 페이지를 엽니다. 269페이지의 "인터페이스 세부사항 페이지 필드"를 참조하십시오. SA 서버 관리에 대한 자세한 내용은 <i>HP Server Automation User's Guide</i>를 참조하십시오.

장치 IP 주소 페이지 필드

장치 IP 주소 페이지에서는 장치와 연관된 모든 IP 주소를 볼 수 있습니다. 여기에는 장치에 대한 인터페이스의 IP 주소는 물론 장치에서 보이는 네트워크의 IP 주소도 포함됩니다.

필드	설명/작업
포트 이름	장치의 IP 주소와 연관된 포트 이름을 표시합니다.
주소	IP 주소를 표시합니다.
주소 유형	IP 주소 유형(예: 포트 주소 또는 포트에서 표시됨)을 표시합니다.
VLAN	유형이 "포트 주소"인 경우 이 IP 주소를 포함하는 VLAN에 대한 링크(있는 경우)를 제공합니다.
설명	IP 주소에 대한 설명이 제공됩니다.
원격 위치	유형이 "포트에서 표시됨"인 경우 원격 위치에 대한 링크를 제공합니다. 원격 위치는 NA에서 인식되는 장치 및 포트입니다(또는 NA/SA 통합이 활성화된 경우 SA에서 인식되는 서버 및 인터페이스).
첫 번째로 표시됨	IP 주소가 처음 식별된 날짜 및 시간을 표시합니다.
마지막으로 표시됨	NA가 토폴로지 데이터를 수집한 마지막 시기에 IP 주소가 식별된 경우 "현재"가 표시됩니다. 현재가 아닌 경우에는 NA가 네트워크에서 IP 주소를 마지막으로 식별한 날짜 및 시간입니다. IP 주소는 네트워크에 더 이상 존재할 수 없습니다(예: 랩톱이나 기타 임시 장치의 IP 주소). 또한 IP 주소가 주요 흐름에 더 이상 존재할 수 없도록 라우팅 트래픽이 변경될 수 있습니다.
연관된 MAC	장치와 연관된, NA에서 인식되는 모든 MAC 주소의 목록을 볼 수 있는 장치 MAC 주소 페이지를 엽니다.

필드	설명/작업
작업	<p>각 장치에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none">• 세부사항 보기 — 장치, 장치 포트, IP 주소, MAC 주소, 유형, 첫 번째로 표시됨, 마지막으로 업데이트됨 등의 정보에 대한 세부사항을 볼 수 있는 IP 주소 세부사항 페이지를 엽니다.• MAC 보기 — 이 IP 주소와 상호 참조되는 MAC 주소 세부사항 페이지를 엽니다. 상호 참조란 NA가 데이터를 수집할 때 IP 주소와 MAC 주소가 동일한 소스에서 오는 것으로 표시되었음을 의미합니다. 이는 "포트에서 표시됨" 레코드에서만 이용 가능합니다.

장치 MAC 주소 페이지 필드

장치 MAC 주소 페이지에서는 장치와 연관된 모든 MAC 주소 목록을 볼 수 있습니다.

필드	설명/작업
포트 이름	장치의 IP 주소와 연관된 포트 이름을 표시합니다.
주소	장치 MAC 주소를 표시합니다.
주소 유형	MAC 주소에 대한 설명을 표시합니다(예: "포트 주소" 또는 "포트에서 표시됨").
VLAN	유형이 "포트 주소"인 경우 이 MAC 주소를 포함하는 VLAN에 대한 링크(있는 경우)를 제공합니다.
설명	MAC 주소에 대한 설명을 표시합니다.
원격 위치	유형이 "포트에서 표시됨"인 경우 원격 위치에 대한 링크를 제공합니다. 원격 위치는 NA에서 인식되는 장치 및 포트입니다. 또는 HP SA(Server Automation)에서 인식되는 서버 및 인터페이스일 수 있습니다. NA/SA 통합에 대한 자세한 내용은 254페이지의 "NA/SA 통합" 을 참조하십시오.
첫 번째로 표시됨	MAC 주소가 처음 식별된 날짜 및 시간을 표시합니다.
마지막으로 표시됨	NA가 토폴로지 데이터를 수집한 마지막 시기에 MAC 주소가 식별된 경우 "현재"가 표시됩니다. 현재가 아닌 경우에는 NA가 네트워크에서 MAC 주소를 마지막으로 식별한 날짜 및 시간입니다. MAC 주소는 네트워크에 더 이상 존재할 수 없습니다(예: 랩톱이나 기타 임시 장치의 MAC 주소). 또한 MAC 주소가 주요 흐름에 더 이상 존재할 수 없도록 라우팅 트래픽이 변경될 수 있습니다.
연관된 IP	장치와 연관된, NA에서 인식되는 모든 IP 주소의 목록을 볼 수 있는 장치 IP 주소 페이지를 엽니다.

필드	설명/작업
작업	<p>각 장치에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none">• 세부사항 보기 — 장치, 장치 포트, MAC 주소, 유형, 구성 조각, 첫 번째로 표시됨 및 마지막으로 업데이트됨 등의 정보에 대한 세부사항을 볼 수 있는 MAC 주소 세부사항 페이지를 엽니다.• IP 보기 — 장치, 장치 포트, IP 주소, MAC 주소, 유형, 첫 번째로 표시됨 및 마지막으로 업데이트됨 등의 정보에 대한 세부사항을 볼 수 있는 IP 주소 세부사항 페이지를 엽니다.• 이 필드는 IP 주소와 상호 참조됩니다. 상호 참조란 NA가 데이터를 수집할 때 IP 주소와 MAC 주소가 동일한 소스에서 오는 것으로 표시되었음을 의미합니다. 이는 "포트에서 표시됨" 레코드에서만 이용 가능합니다.

VLAN(가상 로컬 영역 네트워크)

VLAN(가상 로컬 영역 네트워크)은 패킷의 단일 브로드캐스트 도메인 역할을 하는 포트를 모아놓은 집합입니다. VLAN은 VLAN 태그로 이더넷 프레임을 수정하여 네트워크 스위치 간의 브로드캐스트 도메인 세분화와 그룹 장치를 제공하는 레이어 2(데이터 링크 레이어)에서 작동합니다. NA는 각 포트가 할당되어 있는 VLAN과 관리되는 장치에 정의된 VLAN에 대한 정보를 수집합니다.

일반적으로 VLAN은 네트워크 스위치에 있지 않더라도 최종 무선국을 함께 그룹화하기 위해 브로드캐스트 도메인을 세분화합니다. VLAN에서는 네트워크 스위치를 가상화할 수 있으므로 네트워크 스위치가 여러 네트워크 스위치에 걸친 LAN과 두 개 이상의 레이어 2 네트워크에 서비스를 제공할 수 있습니다.

VLAN은 세분화 서비스를 제공하므로 네트워크 라우터를 사용하지 않고도 레이어 2에서 보안, 확장성 및 네트워크 관리 문제를 해결합니다. 다양한 브로드캐스트 도메인은 한 도메인의 트래픽을 다른 도메인으로부터 분리하므로 조직 내에서 보안을 제공합니다.

예를 들어 엔터프라이즈 환경에서 재무부, 인사부 및 영업부마다 고유의 브로드캐스트 도메인이 있으므로 각 트래픽을 다른 부서에서 볼 수 없습니다. 또한 재무부의 직원은 다양한 시설에 근무할 수 있습니다. 따라서 VLAN은 이들이 동일 네트워크 스위치에 연결된 단일 물리적 위치에 있는 것처럼 이들을 하나로 그룹화하여 네트워크 확장성을 증가할 수 있습니다.

VLAN은 네트워크 스위치를 여러 브로드캐스트 도메인으로 세분화하고 여러 네트워크 스위치를 브로드캐스트 도메인에 포함시킬 수 있도록 함으로써 네트워크 스위치에 대한 가상화도 제공합니다. 따라서 조직 내 각 부서에 대해 개별 네트워크 스위치를 사용하지 않고, 대신에 VLAN을 사용하여 네트워크 스위치를 가상 네트워크 스위치로 구분함으로써 여러 부서에 서비스를 제공할 수 있습니다.

NA에서는 네트워크 스위치에서 VLAN을 확인하고 프로비전할 수 있습니다. NA를 사용하여 다음을 수행할 수 있습니다.

- 장치 VLAN의 전체 목록 보기
- 특정 VLAN 세부사항 보기
- VLAN에 할당된 포트 목록 보기
- 트렁크 포트 보기

- 트렁크 포트의 VLAN 목록 보기
- 트렁크 포트의 기본 VLAN 보기(트렁크 포트의 트래픽에 태그가 지정되지 않은 VLAN)
- 네트워크 스위치의 VTP 설정 보기
- 네트워크 스위치의 새 VLAN 작성
- VLAN에 할당된 포트 변경(포트 추가/정리)
- VLAN 이름 변경
- VLAN 삭제
- 포트를 트렁크 포트 구성(태그 지정에 사용하는 여러 VLAN)
- 트렁크 포트 VLAN(VLAN 멤버십) 변경
- 트렁크 포트 기본 VLAN 변경
- 트렁크 포트를 비 트렁크로 구성

장치 VLAN 페이지 필드

장치 VLAN 페이지에는 장치의 모든 VLAN 목록이 표시됩니다. VLAN에 대한 자세한 내용은 [278페이지의 "VLAN\(가상 로컬 영역 네트워크\)"](#)을 참조하십시오.

장치 VLAN 페이지로 이동하려면

1. 인벤토리 페이지에서 VLAN 세부사항을 표시할 장치를 선택합니다. 페이지의 검색 옵션을 사용하여 장치를 찾을 수도 있습니다. 장치 세부사항 페이지가 열립니다.
2. 장치 세부사항 페이지에서 보기 메뉴를 선택합니다.
3. 보기 메뉴에서 장치 세부사항 옵션을 선택하고 VLAN 옵션을 클릭합니다. 장치 VLAN 페이지가 열립니다.

참고: 장치 드라이버에서 향상된 VLAN 기능을 지원하지 않을 경우 프로비전 작업이 표시되지 않습니다.

필드	설명/작업
새 VLAN 링크	새 VLAN을 생성할 수 있는 새 장치 VLAN 페이지를 엽니다. 자세한 내용은 282 페이지의 "VLAN 생성 및 편집" 을 참조하십시오.
VLAN	VLAN 이름을 표시합니다.
VLAN 유형	VLAN 유형을 표시합니다. 이 필드는 공급업체마다 다릅니다.
VLAN ID	VLAN ID를 표시합니다.
VLAN 상태	활성 또는 일시 중단됨 등 VLAN 상태를 표시합니다.
마지막 수정일	장치에서 NA가 마지막으로 VLAN을 읽은 날짜 및 시간을 표시합니다. (이 날짜 및 시간 이후에도 NA가 장치에서 VLAN을 읽었을 수 있지만, 변경 사항이 없는 경우)
설명	장치에서 가져온 VLAN에 대한 정보를 표시합니다.

필드	설명/작업
작업	<p>각 VLAN에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none">• 보기 — VLAN 세부 정보를 볼 수 있는 VLAN 세부사항 페이지를 엽니다. VLAN 포트 정보는 장치 인터페이스 페이지와 연결되어 있습니다. 자세한 내용은 283페이지의 "VLAN 세부사항 페이지 필드"를 참조하십시오. 트렁크 포트가 VLAN의 멤버인 경우 트렁크 포트도 표시됩니다.• 편집 — VLAN 세부 정보를 보고 VLAN 이름, 설명 및 포트 멤버십을 편집할 수 있는 VLAN 편집 세부사항 페이지를 엽니다. 자세한 내용은 282페이지의 "VLAN 생성 및 편집"를 참조하십시오.• 삭제 — VLAN 삭제 확인 대화 상자를 엽니다.

VLAN 생성 및 편집

새 장치 VLAN 페이지에서는 VLAN 이름을 입력하고 새 VLAN에 할당할 포트를 확인할 수 있습니다. 장치 VLAN 편집 페이지에서는 VLAN 이름과 포트 멤버십 정보를 수정할 수 있습니다. VLAN에 대한 자세한 내용은 [278페이지의 "VLAN\(가상 로컬 영역 네트워크\)"](#)을 참조하십시오.

참고: 새 장치 VLAN 및 장치 편집 VLAN 페이지는 해당 장치에서 마지막으로 수집된 VLAN 데이터를 기반으로 합니다. 이러한 페이지에는 VLAN 데이터를 마지막으로 수집한 이후에 발생한 장치 변경 사항은 반영되지 않습니다. VLAN 데이터를 최신 상태로 유지하려면 VLAN 데이터 수집 진단을 실행하여 NA를 최신 VLAN 데이터로 업데이트합니다. 자세한 내용은 [397페이지의 "진단 실행 작업 페이지 필드"](#)를 참조하십시오.

필드	설명/작업
장치	장치의 호스트 이름 및/또는 IP 주소를 표시합니다. 장치 링크를 클릭하면 장치 세부사항 페이지가 열립니다. 249페이지의 "장치 세부사항 보기" 를 참조하십시오.
VLAN 이름	새 VLAN 이름을 입력하거나 기존 VLAN 이름을 편집합니다.
VLAN ID	VLAN ID를 입력합니다. VLAN ID가 입력 필드인 새 VLAN 작업과는 달리 새 VLAN 작업 VLAN ID 필드는 VLAN 편집 작업 전용 텍스트입니다.
VLAN 유형	VLAN 유형을 표시합니다. 이 필드는 공급업체마다 다릅니다. 이 정보는 장치에서 수집된 데이터에서 자동으로 입력됩니다.
VLAN 상태	활성 또는 일시 중단됨 등 VLAN 상태를 표시합니다. 이 정보는 장치에서 수집된 데이터에서 자동으로 입력됩니다.
VLAN MTU	VLAN에서 사용할 수 있는 VLAN 최대 전송 단위(패킷 크기)를 표시합니다. 이 필드는 공급업체마다 다릅니다. 이 정보는 장치에서 수집된 데이터에서 자동으로 입력됩니다.

필드	설명/작업
VLAN 포트	<p>VLAN 포트 목록을 표시합니다. 포트 이름은 해당 포트에 대한 인터페이스 세부 사항 페이지에 연결됩니다. 자세한 내용은 269페이지의 "인터페이스 세부사항 페이지 필드"를 참조하십시오.</p> <p>VLAN에 현재 할당된 포트가 선택됩니다. 현재 할당되지 않았지만 할당할 수 있는 사용 가능한 포트는 선택되어 있지 않습니다. 괄호 안에는 기본 VLAN 이름이 지정되어 있습니다. 포트가 트렁크 포트이면 상태가 해당 포트로 표시됩니다. 또한 포트가 PortChannel이면 집합 포트가 심볼로 구분된 목록에 표시됩니다.</p> <p>VLAN에 현재 할당된 포트는 확인란의 선택을 취소하여 VLAN에서 정리(제거)할 수 있습니다. 마찬가지로, 현재 VLAN에 할당되지 않은 포트는 해당 확인란의 선택을 취소하여 할당할 수 있습니다.</p>
VLAN 설명	VLAN의 설명을 표시합니다.

완료되면 저장 버튼을 클릭해야 합니다. 수정한 경우 VLAN 작업 페이지가 열립니다. 자세한 내용은 [452페이지의 "VLAN 작업 페이지 필드"](#)를 참조하십시오.

VLAN 세부사항 페이지 필드

장치 VLAN 페이지의 작업 필드에서 보기 옵션을 클릭하면 VLAN 세부사항 페이지가 열립니다.

필드	설명/작업
장치	장치의 호스트 이름 및/또는 IP 주소를 표시합니다. 장치 링크를 클릭하면 장치 세부사항 페이지가 열립니다. 자세한 내용은 249페이지의 "장치 세부사항 보기" 를 참조하십시오.
VLAN 이름	VLAN 이름을 표시합니다.
VLAN ID	VLAN ID를 표시합니다.
VLAN 유형	VLAN 유형을 표시합니다. 이 필드는 공급업체마다 다릅니다.
VLAN 상태	활성 또는 일시 중단됨 등 VLAN 상태를 표시합니다.

필드	설명/작업
VLAN MTU	VLAN에서 사용할 수 있는 VLAN 최대 전송 단위(패킷 크기)를 표시합니다. 이 필드는 공급업체마다 다릅니다.
VLAN 포트	VLAN 포트 목록을 표시합니다. 포트 링크를 클릭하면 해당 포트에 대한 인터페이스 세부사항 페이지가 열립니다. 트렁크 포트에 기본 VLAN(태그 지정되지 않은 VLAN)이 없으면 기본 VLAN이 멤버 VLAN 목록 하단에 표시되지 않습니다. 269페이지의 "인터페이스 세부사항 페이지 필드" 를 참조하십시오. 트렁크 포트의 경우 장치 인터페이스 페이지에 모든 VLAN이 나열됩니다. 자세한 내용은 267페이지의 "장치 인터페이스 페이지 필드" 를 참조하십시오.
VLAN 설명	장치에서 가져온 VLAN에 대한 정보를 표시합니다.
마지막 수정일	장치에서 NA가 마지막으로 VLAN을 읽은 날짜 및 시간을 표시합니다. (이 날짜 및 시간 이후에도 NA가 장치에서 VLAN을 읽었을 수 있지만, 변경 사항이 없는 경우)
편집 세부사항 링크	VLAN 편집 세부사항 페이지를 엽니다. 자세한 내용은 282페이지의 "VLAN 생성 및 편집" 을 참조하십시오.

VTP 세부사항 페이지 필드

VTP(VLAN Trunking Protocol)는 Cisco 스위치 간의 VLAN을 관리하는 Cisco 전용 프로토콜입니다. VTP는 VTP 도메인이라고 하는 관리 도메인을 정의합니다. VTP 도메인에서 하나 이상의 스위치는 서버로 구성되어 VLAN 구성을 배포하므로 VLAN을 수동으로 구성할 필요가 없습니다. 세 가지 참여 수준(작동 모드)이 있습니다.

- Server
- Client
- Transparent

VTP 도메인에서 서버로 구성된 스위치는 모든 VLAN 구성 변경 내용을 도메인 내 다른 스위치에 알립니다. VTP 패킷이 서버로 연결된 스위치로 전송됩니다. Client 모드에 있는 스위치는 VTP 패킷에 응답하고 그에 따라 고유의 VLAN 구성을 수정하고 나서 VTP 패킷을 도메인 내 다른 스위치로 중계합니다. Transparent 모드의 스위치는 VLAN 구성을 변경하지 않고 VTP 패킷을 다른 스위치로 중계합니다.

장치가 Cisco 스위치이고 장치가 VTP 도메인에 참여하는 경우 NA가 장치 VTP 정보를 표시합니다. VLAN에 대한 자세한 내용은 [278페이지의 "VLAN\(가상 로컬 영역 네트워크\)"](#)을 참조하십시오.

참고: NA에서는 VTP 설정을 프로비전하지 않습니다. NA VTP 지원은 읽기 전용이므로 NA가 표시를 위해 장치에서 VTP 정보만 수집합니다.

VTP 세부사항 페이지로 이동하려면

1. 인벤토리 페이지에서 VTP 세부사항을 표시할 장치를 선택합니다. 페이지의 검색 옵션을 사용하여 장치를 찾을 수도 있습니다. 장치 세부사항 페이지가 열립니다.
2. 장치 세부사항 페이지에서 보기 메뉴를 선택하고 VTP 정보 옵션을 클릭합니다. VTP 세부사항 페이지가 열립니다.

필드	설명/작업
장치	장치의 호스트 이름 및/또는 IP 주소를 표시합니다. 장치 링크를 클릭하면 장치 세부사항 페이지가 열립니다. 자세한 내용은 249페이지의 "장치 세부사항 보기" 를 참조하십시오.
VTP 버전	VTP 버전을 표시합니다.

필드	설명/작업
구성 버전	구성 버전 번호를 표시합니다.
도메인 이름	VTP 도메인 이름을 표시합니다. 이름은 VTP 도메인 페이지의 링크이며 이 페이지에서는 해당 도메인에 속하는 장치 목록을 볼 수 있습니다. 자세한 내용은 288페이지의 "VTP 도메인 페이지" 를 참조하십시오. (참고: 단일 따옴표 안에 포함된 VTP 도메인 이름을 사용하면 NA가 SQL 오류를 반환합니다.)
로컬로 지원되는 최대 VLAN 수	로컬로 지원되는 VLAN의 최대 개수를 표시합니다.
기존 VLAN 수	기존 VLAN 수를 표시합니다.
VTP 운영 모드	Server, Client, Transparent 또는 끄기 등 VTP 작동 모드를 표시합니다.
VTP 정리 모드	사용하는 경우 VTP 정리를 통해 알 수 없는 유니캐스트와 브로드캐스트에서 발생된 불필요한 트래픽을 제거할 수 있습니다.
VTP V2 모드	사용하는 경우 VTP 2 모드는 토큰 링 VLAN용으로 사용할 수 있습니다.
VTP 트랩 생성	사용하는 경우 문제 해결을 위해 VTP 트랩을 생성할 수 있습니다.
MD5 다이제스트	사용하는 경우 문제 해결을 위해 MD5 다이제스트를 사용할 수 있습니다. MD5 다이제스트는 VTP 암호(구성된 경우)와 VTP 도메인 이름의 조합에서 생성된 16바이트 워드(MD5 값)를 표시합니다.
이 도메인의 VTP	도메인의 장치를 표시합니다. 장치의 호스트 이름 및/또는 IP 주소는 장치 세부 사항 페이지의 링크입니다. 장치 세부사항 페이지에는 장치에 VTP 구성이 있는 경우 VTP 도메인 이름 및 작동 모드 정보가 포함됩니다. 자세한 내용은 250페이지의 "장치 세부사항 페이지 필드" 를 참조하십시오.
마지막으로 수정한 사람	VTP를 마지막으로 수정한 사람을 표시합니다.
마지막 수정일	VTP가 마지막으로 수정된 날짜를 표시합니다.

VTP 도메인 페이지 필드

VTP(VLAN Trunking Protocol) 도메인 페이지에는 NA에서 관리하는 하나 이상의 장치 네트워크에 있는 VTP 도메인이 나열됩니다. VLAN에 대한 자세한 내용은 [278페이지의 "VLAN\(가상 로컬 영역 네트워크\)"](#)을 참조하십시오.

VTP 도메인 페이지로 이동하려면 장치 메뉴에서 장치 도구를 선택하고 VTP 도메인 옵션을 클릭합니다. VTP 도메인 페이지가 열립니다.

필드	설명/작업
도메인 이름	도메인 이름을 표시합니다.
VTP 버전	VTP 버전을 표시합니다.
장치 수	NA가 도메인 내에서 인식하는 장치 수를 표시합니다.
작업	보기 링크를 클릭하면 VTP 도메인 페이지가 열립니다. 자세한 내용은 288페이지의 "VTP 도메인 페이지" 를 참조하십시오.

VTP 도메인 페이지

VTP 도메인 페이지에는 특정 도메인의 장치가 표시됩니다. VLAN에 대한 자세한 내용은 [278페이지의 "VLAN\(가상 로컬 영역 네트워크\)"](#)을 참조하십시오.

VTP 도메인(domain_name) 페이지로 이동하려면 VTP 도메인 페이지에서 장치 세부 정보를 표시할 도메인에 대한 작업 필드에 있는 보기 옵션을 클릭합니다. VTP 도메인 페이지가 열립니다.

필드	설명/작업
호스트 이름	장치의 호스트 이름을 표시합니다. 호스트 이름 링크를 클릭하면 장치 세부사항 페이지가 열립니다. 자세한 내용은 249페이지의 "장치 세부사항 보기" 를 참조하십시오.
장치 IP	장치 IP 주소를 표시합니다. 장치 IP 링크를 클릭하면 장치 세부사항 페이지가 열립니다. 자세한 내용은 249페이지의 "장치 세부사항 보기" 를 참조하십시오.
MD5 다이제스트	사용하는 경우 문제 해결을 위해 MD5 다이제스트를 사용할 수 있습니다.
작동 모드	서버, 클라이언트 투명 또는 끄기 등 VTP 작동 모드를 표시합니다.
파티션	장치가 속해 있는 파티션을 표시합니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다.)
작업	<p>선택할 수 있는 작업은 다음과 같습니다.</p> <ul style="list-style-type: none"> • VTP 보기 — VTP 세부사항 페이지를 엽니다. 자세한 내용은 285페이지의 "VTP 세부사항 페이지 필드"를 참조하십시오. • VLAN 보기 — 장치 VLAN 페이지가 열립니다. 자세한 내용은 280페이지의 "장치 VLAN 페이지 필드"를 참조하십시오.

장치 블레이드/모듈 페이지 필드

장치 블레이드/모듈 페이지에는 장치에 설치된 모듈(블레이드, 카드)이 나열됩니다. 기본적으로 모듈 데이터는 매주 모듈 상태 진단 작업에 의해 업데이트됩니다.

필드	설명/작업
모듈 슬롯	모듈이 설치된 장치의 슬롯을 표시합니다.
모듈 설명	모듈에 대한 간단한 설명을 표시합니다. NA는 장치 구성으로부터 설명을 구문 분석합니다.
모듈 모델	모델 식별자를 표시합니다.
모듈 일련 번호	모듈의 일련 번호를 표시합니다.
작업	<p>각 모듈에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> •모듈 편집 — 모듈 인벤토리 세부 정보를 보고 사용자 지정 데이터 필드를 편집할 수 있는 블레이드/모듈 세부사항 편집 페이지를 엽니다. •모듈 보기 — 모듈 인벤토리 세부사항을 보고 주석을 편집할 수 있는 블레이드/모듈 세부사항 페이지를 엽니다.

장치 정책 페이지 필드

장치 정책 페이지에서는 다음 작업을 수행할 수 있습니다.

- 현재 정책이 장치에 적용되었는지 확인
- 정책 통과/실패 여부 보기
- 장치가 NA에 추가될 때 장치에 적용되는 정책 보기
- 장치에 적용된 정책에 대한 예외 보기

정책 생성에 대한 내용은 [510페이지의 "NA 정책 관리자의 작업 방식"](#)을 참조하십시오. 적용된 정책을 보는 방법에 대한 자세한 내용은 [531페이지의 "적용된 정책 보기"](#)를 참조하십시오.

필드	설명/작업
정책 이름	정책 이름을 표시합니다.
규칙 이름	해당되는 경우 정책 규칙 이름을 표시합니다. 자세한 내용은 518페이지의 "새 규칙 페이지 필드" 를 참조하십시오.
설명	정책 설명(예: 암호 유지)을 표시합니다.
정책 규칙 예외	해당되는 경우 정책 규칙 예외를 표시합니다. 자세한 내용은 530페이지의 "새 규칙 예외 페이지 필드" 를 참조하십시오.
상태	다음에 포함된 정책 상태를 표시합니다. <ul style="list-style-type: none"> •활성 •비활성 •통과함 •실패함

필드	설명/작업
중요도	<p>위반된 규칙의 중요도를 나타내며, 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none">•정보용 — 일반적으로 응답이 필요하지 않은 이벤트•낮음 — 시간이 허용될 경우 응답이 필요할 수 있는 이벤트•중간 — 일반적으로 72시간 이내에 시기 적절한 응답이 필요한 이벤트•높음 — 일반적으로 24시간 이내에 신속한 응답이 필요한 이벤트•심각 — 즉각적인 응답이 필요한 이벤트
작업	<p>각 정책에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none">•정책 편집 — 정책을 편집할 수 있는 정책 편집 페이지를 엽니다. 자세한 내용은 525페이지의 "정책 편집 페이지 필드"를 참조하십시오.•정책 규칙 편집 — 정책 규칙을 편집할 수 있는 정책 규칙 편집 페이지를 엽니다. 자세한 내용은 518페이지의 "새 규칙 페이지 필드"를 참조하십시오.

서버 페이지 필드

서버 페이지는 세부사항을 표시하는 장치에 연결된 각 서버의 이름을 표시합니다. 서버의 호스트 이름을 클릭하면 서버 세부사항 페이지가 열립니다. SA 사용에 대한 자세한 내용은 *HP Server Automation User's Guide*를 참조하십시오.

NA는 레이어 1 와이어링의 위치를 추론만 할 뿐입니다. NA의 감소 알고리즘은 장치 및 /또는 서버 사이의 모든 연결을 최대한 줄입니다.

참고: HP SA(Server Automation) Command Center에 로그인하지 않은 경우 서버의 호스트 이름을 클릭하면 로그인하라는 창이 표시됩니다.

필드	설명/작업
네트워크 장치 인터페이스	서버에서 사용하는 네트워크 장치 인터페이스입니다(예: FastEthern1/0).
서버 호스트 이름	서버의 호스트 이름을 표시합니다. 서버의 호스트 이름을 클릭하면 서버 세부사항 페이지가 열립니다. 자세한 내용은 <i>HP Server Automation User's Guide</i> 를 참조하십시오.
서버 인터페이스	운영 체제에서 보고한 서버 인터페이스 이름입니다.
고객	고객 이름을 표시합니다.
설비	고객 설비를 표시합니다.
서버 사용	서버 사용을 표시합니다. 자세한 내용은 <i>HP Server Automation User's Guide</i> 를 참조하십시오.
배포 단계	배포 단계를 표시합니다. 자세한 내용은 <i>HP Server Automation User's Guide</i> 를 참조하십시오.

장치 소프트웨어 이미지 권장 사항 페이지 필드

소프트웨어 이미지 권장 사항 페이지는 Cisco.com에서 이용 가능한 소프트웨어 이미지를 기본 권장 사항과 함께 표시합니다. 소프트웨어 이미지에 대한 속성도 소프트웨어 이미지의 위치에 대한 정보와 함께 페이지에 표시됩니다. Cisco.com에서 NA 소프트웨어 리포지토리로 소프트웨어 이미지가 다운로드되고 이미지 집합이 작성됩니다.

내 기본 설정 페이지에서 권장 필터를 적용할 수 있습니다. 자세한 내용은 [341페이지의 "내 기본 설정 페이지 필드"](#)를 참조하십시오.

참고: Cisco 지원 장치 목록을 검토하려면 다음 URL을 참조하십시오. NA는 RME(Resource Manager Essentials)의 데이터를 사용합니다. 따라서 Cisco에서 장치를 지원해야 합니다. 그렇지 않으면 Cisco 소프트웨어 이미지를 다운로드할 수 없습니다.

http://cisco.com/en/US/products/sw/cscowork/ps2425/products_device_support_table09186a008086099b.html

다음 그림은 장치 소프트웨어 이미지 권장 사항 페이지의 샘플 섹션을 보여줍니다. 이 예에서는 공유 옵션이 선택되었습니다. 다운로드할 소프트웨어 이미지를 이미지 세부사항 섹션에서 클릭하면(이 경우 *rsp-isv56i-mz.121.bin*) 소프트웨어 이미지가 NA 리포지토리로 다운로드됩니다.

모듈 / 슬롯 / 유형 목록	버전 목록	기능 목록
BOOT_LOADER SYSTEM_SW	--- 기본 권장 --- 12.2.46 --- 일반 권장 --- 12.4.8c 12.4.8b	--- 기본 권장 --- IP/VIP IPSEC 56 --- 일반 권장 --- ENTERPRISE/VIP PLUS ENTERPRISE/VIP IPSEC 56
<h3>이미지 세부사항</h3> <p>Cisco.com 에서 다운로드할 작업 예약 rsp-isv56i-mz.121.bin 파일 크기 : 11483336 바이트 기능 : IP/VIP IPSEC 56 플래시 : 16MB RAM : 64MB 버전 : 12.2..46</p> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;"> <p>slot0</p> <p>여유 공간 크기 : 4900236 바이트 파티션 크기 : 1638400 바이트 경고 -SWIM10661: Cisco.com 에서 사용 가능한 이미지가 업그레이드를 위해 선택됨</p> </div> <div style="border: 1px solid black; padding: 5px;"> <p>bootflash</p> <p>여유 공간 크기 : 383824 바이트 파티션 크기 : 7602176 바이트 경고 -SWIM10661: Cisco.com 에서 사용 가능한 이미지가 업그레이드를 위해 선택됨</p> </div>		

장치 소프트웨어 이미지 권장 사항 페이지를 열려면

1. OS 분석을 지원하는 Cisco 장치를 선택합니다. 해당 장치에 대한 장치 세부사항 페이지가 열립니다.
2. 보기 메뉴에서 장치 세부사항을 선택하고 소프트웨어 업그레이드 권장 사항을 클릭합니다.

필드	설명/작업
호스트 이름	장치 호스트 이름을 표시합니다. 장치 호스트 이름을 클릭하면 장치에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
장치 IP	장치 IP 주소를 표시합니다. IP 주소를 클릭하면 해당 장치에 대한 자세한 내용을 볼 수 있는 장치 세부사항 페이지가 열립니다.
마지막 액세스 시간	장치에 마지막으로 액세스한(예: 스냅샷 작성) 날짜 및 시간을 표시합니다.
마지막 스냅샷 결과	장치 구성의 마지막 스냅샷 상태를 표시합니다. 스냅샷이 실패하면 작업 결과 페이지에 대한 링크가 표시됩니다.
보기 메뉴	보기 메뉴를 엽니다. 자세한 내용은 261페이지의 "메뉴 옵션 보기" 를 참조하십시오.
편집 메뉴	편집 메뉴를 엽니다. 자세한 내용은 304페이지의 "편집 메뉴 옵션" 을 참조하십시오.
프로비전 메뉴	프로비전 메뉴를 엽니다. 자세한 내용은 314페이지의 "프로비전 메뉴 옵션" 을 참조하십시오.
연결 메뉴	연결 메뉴를 엽니다. 자세한 내용은 316페이지의 "연결 메뉴 옵션" 을 참조하십시오.

필드	설명/작업
소프트웨어 이미지 다운로드	<p>다음 섹션은 선택 시 데이터가 채워집니다. 샘플 표시를 보려면 위 그림을 참조하십시오.</p> <ul style="list-style-type: none"> • 모듈/슬롯/유형 목록 — BOOT_LOADER(운영 체제를 시작하기 위해 소프트웨어를 로드하는 작은 프로그램) 및 SYSTEM_SW를 표시합니다. • 버전 목록 — BOOT_LOADER 또는 SYSTEM_SW를 선택하면 소프트웨어 이미지 버전 목록이 표시됩니다. • 기능 목록 — 소프트웨어 이미지 버전을 선택하면 해당 소프트웨어 이미지 버전에 대한 기능 목록이 표시됩니다. 기능을 선택하면 이미지 세부사항 섹션이 데이터로 채워집니다. NA 소프트웨어 리포지토리에 없는 소프트웨어 이미지의 경우 소프트웨어 이미지 이름을 클릭하여 Cisco.com에서 직접 소프트웨어 이미지를 다운로드할 수 있습니다. 이미지가 NA 소프트웨어 리포지토리에 이미 있는 경우 소프트웨어 이미지 링크를 클릭합니다. 장치 소프트웨어 작업 업그레이드 페이지가 열리는데, 여기서 장치를 선택한 소프트웨어 이미지로 업그레이드할 수 있습니다. 자세한 내용은 413페이지의 "장치 소프트웨어 업데이트 작업 페이지 필드"를 참조하십시오.
이미지 세부사항	파일 크기, 버전 상태, 플래시 등 소프트웨어 이미지에 대한 정보를 표시합니다. 장치의 슬롯 및 부트플래시에 대한 정보도 경고와 함께 표시됩니다.

장치 작업 페이지 필드

장치 작업 페이지는 장치와 연관된 모든 작업을 나열합니다. 또한 이 페이지에서 작업에 대한 세부사항을 보거나 작업을 다시 실행할 수도 있습니다.

필드	설명/작업
이 페이지를 60초마다 새로 고칩니다.	60초마다 표시를 새로 고치지 않으려면 이 상자의 선택을 취소합니다. 이 값 설정에 대한 자세한 내용은 80페이지의 "사용자 인터페이스 페이지 필드" 를 참조하십시오.
확인란	왼쪽의 확인란을 사용하여 선택한 작업을 삭제할 수 있습니다. 작업을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 작업을 선택하거나 선택 취소할 수 있습니다.
예약 날짜	작업이 실행된 또는 실행하도록 예정된 날짜 및 시간을 표시합니다.
작업 이름	작업 이름을 클릭하면 작업의 주관자, 작업이 작성된 시기, 작업의 영향을 받는 장치와 같은 작업 세부사항을 볼 수 있는 작업 정보 페이지가 열립니다. 또한 자세한 작업 이력 정보를 볼 수 있습니다.
작업 상태	작업의 상태를 표시합니다. 상태는 다음과 같습니다. <ul style="list-style-type: none"> • 성공함 — 작업이 성공했습니다. • 실패함 — 작업이 실패했습니다. • 중복 — 작업이 다른 작업과 중복되어 실행되지 않았습니다. • 건너뛴 — 이 작업의 실행 시간에 도달했을 때 이미 동일한 작업이 실행 중이어서 작업을 건너뛰었습니다. • 경고 — 그룹 작업에 일부 실패한 하위 작업이 포함되어 있지만, 모든 작업이 실패한 것은 아닙니다.
우선 순위	작업 우선 순위를 표시합니다. 1~5의 5가지 작업 우선 순위 수준이 있으며, 최고 작업 우선 순위는 1입니다. 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
예약자	작업을 예약한 사람(또는 작업을 수정한 마지막 사용자)의 로그인 이름을 표시합니다.
주석	작업에 대한 주석을 표시합니다.

필드	설명/작업
작업	<p>각 작업에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none">• 세부사항 — 작업에 대한 세부사항을 볼 수 있는 작업 세부사항 페이지를 엽니다.• 다시 실행 — 작업을 편집 및 다시 실행할 수 있는 작업 편집 페이지가 열립니다. 이 링크는 작업을 다시 실행할 수 있을 경우에만 나타납니다.

장치 관계 페이지 필드

장치 관계 페이지에서는 상위, 피어 및 하위 장치 관계를 볼 수 있습니다. 일반적으로 장치 관계는 상위, 피어 및 하위 장치 모두에 대한 데이터를 유지합니다.

장치 종속성은 장치 관계 API를 통해 정의됩니다. 예를 들어 두 장치가 컨텍스트 관계에 정의된 경우 해당 관계는 컨텍스트 관리 기능을 통해 유지됩니다. 컨텍스트 관리에 대한 자세한 내용은 [448페이지의 "장치 컨텍스트 추가 작업 페이지 필드"](#)를 참조하십시오. 장치 관계 API에 대한 자세한 내용은 *NA 9.10 API Reference Guide*를 참조하십시오.

관련된 두 장치는 장치 관계라고 하는 관계에 참여하게 됩니다. 예를 들어, 첫 번째 장치에 두 번째 장치를 통해서만 연결할 수 있는 첫 번째 장치는 하위 장치가 되며 두 번째 장치는 상위 장치가 됩니다. 따라서 상위 장치에 액세스할 수 없으면 하위 장치에 액세스할 수 없습니다.

현재 NA는 장치 관계 면에서 VMware ESX 서버만 지원합니다. CLI는 VMware ESX 서버에 액세스하는 데 사용됩니다. 하지만 서버 셸에서 VMware ESX 서버는 다른 Linux 서버와 매우 비슷해 보입니다.

VMware ESX 서버가 식별되고 나면 서버가 새 장치의 장치 세부사항 메뉴에 있는 모듈 옵션에서 제공됩니다. [250페이지의 "장치 세부사항 페이지 필드"](#)를 참조하십시오.

새 장치에서는 상위 항목을 통해 보유하고 있는 정보를 사용함으로써 정보에 액세스할 수 있습니다. 이 경우 vSwitch는 VMware ESX 서버에 의해 실행됨을 알고 있습니다. 따라서 스냅샷 작업이 실행될 때 vSwitch는 VMware ESX 서버에 대한 알려진 정보를 사용하여 액세스됩니다. 이는 VMware ESX 서버와의 직접 연결을 의미하거나 장치와의 직접 연결을 의미할 수도 있습니다. 가능할 경우 상위 장치에 포함된 장치가 실제 장치로 표시됩니다.

장치 관계 페이지를 열려면 보기 메뉴에서 장치 관계를 클릭합니다.

필드	설명/작업
상위 장치	상위 장치를 표시합니다.
피어 장치	피어 장치를 표시합니다.
하위 장치	하위 장치를 표시합니다.

상위, 피어 또는 하위 장치를 추가하거나 제거하려면 해당 열에 있는 추가 또는 삭제 링크를 클릭합니다. 장치 추가에 대한 내용은 [137페이지의 "장치 추가"](#)를 참조하십시오.

컨텍스트를 지원하는 장치의 경우 다음 정보가 장치 컨텍스트 페이지에 표시됩니다.

- 컨텍스트의 호스트 이름
- 컨텍스트 이름
- 컨텍스트 제거 링크
- 새 컨텍스트 추가 링크 자세한 내용은 [448페이지의 "장치 컨텍스트 추가 작업 페이지 필드"](#)를 참조하십시오.

참고: 컨텍스트를 추가/제거하는 데 필요한 특정 정보(예: 필요한 변수)가 드라이버 안에 포함되어 있습니다. 이러한 변수는 작업 추가/제거 페이지에 제공됩니다.

장치 소프트웨어 이력 페이지 필드

장치 소프트웨어 이력 페이지에서는 현재 장치에 로드된 소프트웨어를 볼 수 있습니다.

필드	설명/작업
호스트 이름	장치 호스트 이름을 표시합니다. 장치 호스트 이름을 클릭하면 장치에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
장치 IP	장치 IP 주소를 표시합니다. IP 주소를 클릭하면 해당 장치에 대한 자세한 내용을 볼 수 있는 장치 세부사항 페이지가 열립니다.
마지막 액세스 시간	장치에 마지막으로 액세스한(예: 스냅샷 작성) 날짜 및 시간을 표시합니다.
마지막 스냅샷 결과	장치 구성의 마지막 스냅샷 상태를 표시합니다. 스냅샷이 실패하면 작업 결과 페이지에 대한 링크가 표시됩니다.
보기 메뉴	보기 메뉴를 엽니다. 자세한 내용은 261페이지의 "메뉴 옵션 보기" 를 참조하십시오.
편집 메뉴	편집 메뉴를 엽니다. 자세한 내용은 304페이지의 "편집 메뉴 옵션" 을 참조하십시오.
프로비전 메뉴	프로비전 메뉴를 엽니다. 자세한 내용은 314페이지의 "프로비전 메뉴 옵션" 을 참조하십시오.
연결 메뉴	연결 메뉴를 엽니다. 자세한 내용은 316페이지의 "연결 메뉴 옵션" 을 참조하십시오.
변경 날짜	소프트웨어를 마지막으로 배포한 날짜 및 시간을 표시합니다.
변경한 사람	소프트웨어를 장치에 마지막으로 배포한 사람의 이름을 표시합니다.
변경 끝	장치에서 실행되고 있는 현재 소프트웨어 버전을 표시합니다.
장치 소프트웨어 버전	장치에서 실행되고 있는 현재 소프트웨어 버전을 표시합니다.
변경 시작	소프트웨어 배포 전에 장치에서 실행되고 있던 소프트웨어 버전을 표시합니다.

필드	설명/작업
소프트웨어 수준	소프트웨어 수준 등급을 표시합니다. 자세한 내용은 537페이지의 "새 소프트웨어 수준 추가"를 참조하십시오.
이미지 집합	장치에 배포된 마지막 이미지 집합의 이름을 표시합니다. 이미지 집합은 장치에 즉시 배포할 수 있는 이미지의 그룹입니다. 이미지 집합에는 하나 이상의 이미지가 포함될 수 있습니다.

장치 세션 페이지 필드

장치 세션은 장치와 연관된 텔넷 및 SSH 세션을 나열합니다. 세션은 전체 세션에 대해 기록된 명령 또는 키 입력만 포함할 수 있습니다.

필드	설명/작업
시작 날짜	세션이 시작된 날짜를 표시합니다.
상태	세션 상태가 열림인지 닫힘인지를 표시합니다.
유형	세션 유형(텔넷 또는 SSH)을 표시합니다.
종료 날짜	세션이 끝난 날짜를 표시합니다.
생성자	세션을 연 사람의 로그인 이름을 표시합니다.
작업	<p>각 세션에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 전체 텔넷/SSH 세션 보기 — 해당 세션의 명령 및 시스템 응답을 볼 수 있는 텔넷/SSH 세션 페이지가 열립니다. 이 세션에 의해 생성된 구성(있는 경우)에 대한 텍스트 표시도 있습니다. • 명령만 보기 — 텔넷/SSH 세션 페이지를 열지만, 세션 중 입력한 명령만 표시합니다. 이 옵션은 명령으로부터 스크립트를 작성하고자 할 경우 유용할 수 있습니다.

편집 메뉴 옵션

메뉴 옵션	설명/작업
스냅샷 작성	새 작업 — 스냅샷 페이지를 엽니다. 스냅샷 작업을 사용하면 스냅샷을 예약할 수 있습니다. 스냅샷은 장치 구성의 복사본 및 NA 데이터베이스에 저장된 관련 데이터를 새로 고칩니다. 특히 스냅샷은 저장된 구성이 장치에서 실행되는 구성과 일치하는지 확인합니다. 일치하지 않는 경우, 스냅샷 작업은 장치 구성의 복사본 및 NA 데이터베이스에 저장된 관련 데이터를 대체합니다. 자세한 내용은 403페이지의 "스냅샷 작성 작업 페이지 필드" 를 참조하십시오.
드라이버 검색	새 작업 — 검색 작업 페이지를 엽니다. 드라이버 검색은 장치에 드라이버가 할당되었는지를 확인하는 작업을 작성합니다. 할당되지 않은 경우 검색은 현재 드라이버를 NA 데이터베이스에 있는 가장 적합한 드라이버로 덮어씁니다. (참고 : NA에서 각 장치와 통신하려면 드라이버가 필요합니다.) 자세한 내용은 375페이지의 "드라이버 검색 작업 페이지 필드" 를 참조하십시오.
구성 편집 및 배포	구성을 편집한 다음 배포할 수 있는 구성 편집 페이지를 현재 구성으로 엽니다. "장치에 배포" 옵션을 클릭하면 구성 배포를 예약하거나 구성 배포를 즉시 시작할 수 있습니다. NA는 구성 변경 사항을 장치에 배포하고 결과 구성을 캡처합니다. 작업이 실행되는 동안 이 작업에 대한 작업 결과 페이지가 자동으로 새로 고쳐집니다. 자세한 내용은 234페이지의 "구성 배포 작업 페이지 필드" 를 참조하십시오.
인라인 구성 주석 편집	종종 두 개의 느낌표(!!)로 시작되는 주석을 입력할 수 있는 구성 편집 페이지를 엽니다. 지속적인 주석 문자는 두 글자뿐입니다. 그러나 일부 장치에서는 구분 기호로 여러 주석 문자를 사용합니다. 이 경우 주석 엔진이 지속적인 주석을 구문 분석하는 데 어려움을 겪을 수 있습니다.
장치 편집	장치에 대한 정보를 편집할 수 있는 장치 편집 페이지를 엽니다. 자세한 내용은 146페이지의 "장치 편집 페이지 필드" 를 참조하십시오.

메뉴 옵션	설명/작업
관리되는 IP 주소 편집	<p>관리되는 IP 주소 — 장치에 액세스하기 위해 사용할 수 있는 모든 IP 주소 정보를 보고 수정할 수 있는, 장치에서 관리되는 IP 주소 페이지를 엽니다. 각 장치를 고유하게 식별하는 하나의 기본 IP 주소가 있어야 합니다. 그러나 NA가 장치에 연결될 확률을 높이기 위해 대체 IP 주소를 추가할 수 있습니다. 대체 IP 주소는 관리 오버헤드를 줄이고 장치 데이터의 품질을 높입니다. (참고: NA는 기본 IP 주소로 장치에 액세스하지 못할 경우 나열된 순서에 따라 대체 주소로 액세스를 시도합니다. 네트워크 효율성을 위해 액세스 가능성이 가장 높은 IP 주소를 목록의 맨 위로 이동합니다.) 자세한 내용은 307페이지의 "장치에서 관리되는 IP 주소 페이지 필드"를 참조하십시오.</p>
장치 활성화/비활성화	<p>장치를 관리하거나 관리하지 않습니다.</p>
장치 삭제	<p>NA 데이터베이스에서 장치를 완전히 제거할지 확인할 수 있는 대화 상자를 엽니다. NA 데이터베이스에서 장치를 영구적으로 삭제하면 해당 장치에 대한 구성 이력을 손실하게 됩니다. 삭제 대신 장치를 비활성 상태로 만들면 구성 이력을 보존할 수 있습니다.</p>
새 장치로 저장	<p>기존 장치를 사용하여 다음 정보로 장치 추가 및 장치 템플릿 추가 페이지를 미리 채울 수 있습니다.</p> <ul style="list-style-type: none"> • 그룹 • 드라이버 • 암호 정보 • 연결 정보 • 모델 • 공급업체 <p>자세한 내용은 138페이지의 "새 장치 페이지 필드"를 참조하십시오.</p>

메뉴 옵션	설명/작업
새 템플릿으로 저장	<p>기존 장치를 사용하여 다음 정보로 장치 템플릿 추가 페이지를 미리 채울 수 있습니다.</p> <ul style="list-style-type: none"> • 구성 파일 • 드라이버 • 연결 정보 • 모델 • 공급업체 • 계층 레이어 <p>자세한 내용은 155페이지의 "장치 템플릿 페이지 필드"를 참조하십시오.</p>
새 메시지	<p>이 장치를 참조하는 모든 NA 사용자에게 메시지를 게시할 수 있는 새 메시지 페이지를 엽니다. 단일 보기를 사용하여 이벤트를 추적할 수도 있습니다. 자세한 내용은 680페이지의 "이벤트 통합 보기(단일 보기)"를 참조하십시오.</p>
프로세스 자동화	<p>HP Operations Orchestration에 로그인하여 HP Operations Orchestration 흐름을 안내 모드로 시작할 수 있는 HP Operations Orchestration 로그인 페이지를 엽니다. HP Operations Orchestration 사용자 인증 구성에 대한 자세한 내용은 97페이지의 "사용자 인증"을 참조하십시오. HP Operations Orchestration에 대한 자세한 내용은 <i>HP Operations Orchestration User's Guide</i>를 참조하십시오.</p>

장치에서 관리되는 IP 주소 페이지 필드

장치에서 관리되는 IP 주소 페이지에서는 장치에 액세스하는 데 사용될 수 있는 모든 IP 주소를 보고 수정할 수 있습니다. 각 장치를 고유하게 식별하는 하나의 기본 IP 주소가 있어야 합니다.

다음을 사용하여 장치에 연결할 수 있습니다.

- 기본 IP 주소
- 많은 보조 IP 주소(장치에서 제공하거나 수동으로 입력)
- 콘솔 서버 IP 주소 및 포트
- 배스천 호스트
- 홉 상자
- 다른 장치의 IP 주소

필드	설명/작업
배스천 호스트 정의 링크	장치에 배스천 호스트가 정의되어 있지 않으면 새 IP 주소 페이지가 열립니다. 자세한 내용은 309페이지의 "새 IP 주소 페이지(배스천 호스트)" 를 참조하십시오. 장치에 배스천 호스트가 정의되어 있으면 다음 두 링크가 추가로 표시됩니다. <ul style="list-style-type: none"> • 배스천 호스트 편집 • 배스천 호스트 삭제
새 IP 주소 링크	새 IP 주소 페이지를 엽니다. 자세한 내용은 310페이지의 "새 IP 주소 페이지(사용자 지정 IP 주소)" 를 참조하십시오. NAT 또는 기타 주소 지정 스키마를 사용할 때 NA에 의해 자동으로 감지되지 않는 IP 주소를 추가하는 것이 좋습니다. 여기서 추가하는 IP 주소에는 "custom"이란 레이블이 붙습니다.
새 콘솔 서버 링크	새 IP 주소 페이지를 엽니다. 자세한 내용은 311페이지의 "새 IP 주소 페이지(콘솔 서버)" 를 참조하십시오.
새 홉 상자 링크	새 IP 주소 페이지를 엽니다. 자세한 내용은 312페이지의 "새 IP 주소 페이지(홉 상자)" 를 참조하십시오.
새 통과 연결 링크	새 IP 주소 페이지를 엽니다. 자세한 내용은 313페이지의 "새 IP 주소 페이지(새 통과 연결)" 를 참조하십시오.

필드	설명/작업
마지막으로 사용한 IP 재설정 링크	마지막으로 사용한 IP 주소를 재설정할 수 있습니다.
포트 IP	장치의 포트 IP 주소, 즉 기본, 대체 또는 사용자 지정 주소를 표시합니다. 장치 구성을 구문 분석하여 채운 모든 IP 주소는 "대체" 주소로 나열됩니다.
장치 액세스에 사용됨	아니요 또는 예를 표시합니다. NA는 먼저 기본 IP 주소, 다음에는 콘솔 서버 주소(있는 경우), 그리고 마지막으로 이 필드에 "예"로 표시된 대체 IP 주소("아니요"가 기본값) 순서로 장치에 대한 액세스를 시도합니다.
유형	IP 주소 유형, 즉 기본, 대체 또는 사용자 지정 주소를 표시합니다. 새 장치/장치 편집 페이지의 IP 주소는 항상 기본 IP 주소입니다. 감지되는 추가 IP 주소는 대체 주소입니다. 새 IP 주소 링크를 사용하여 IP 주소를 추가하는 경우 이들은 사용자 지정 IP 주소로 간주됩니다.
영역 이름	영역 이름을 표시합니다. 영역 이름은 게이트웨이에서 반환됩니다. 영역 이름은 게이트웨이가 설치될 때 설정되며 NA에서 수정할 수 없습니다.
작업	<p>각 장치에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 편집 — 기본 IP 주소에 대한 장치 편집 페이지가 열려 IP 주소와 서브넷 마스크를 수정하고, 새로운 액세스 순서를 위해 기본 IP 주소 앞에 새 IP 주소를 삽입하고, 변경에 대한 설명을 추가할 수 있습니다. 이 페이지는 대체, NAT, TFTP 서버 및 사용자 지정 IP 주소에 대해 표시됩니다. 자세한 내용은 146페이지의 "장치 편집 페이지 필드"를 참조하십시오. 장치에 수동으로 추가한 IP 주소만 삭제하도록 선택할 수 있습니다. 다른 모든 IP 주소에 대해서는 새 IP 주소 페이지를 엽니다. 310페이지의 "새 IP 주소 페이지(사용자 지정 IP 주소)"를 참조하십시오. • 위로 이동 — 목록에 여러 대체 IP 주소가 나타날 때 이 옵션을 사용하면 목록에서 해당 IP 주소가 위로 이동합니다. NA는 나열된 순서에 따라 대체 주소 사용을 시도합니다. (참고: 이 옵션은 보조, 사용자 지정 및 홉 상자 IP 주소에만 사용할 수 있습니다. 기본 및 콘솔 IP 주소는 정렬할 수 없습니다.) • 아래로 이동 — 목록에 여러 대체 IP 주소가 나타날 때 이 옵션을 사용하면 목록에서 해당 IP 주소가 아래로 이동합니다. NA는 나열된 순서에 따라 대체 주소 사용을 시도합니다. (참고: 이 옵션은 보조, 사용자 지정 및 홉 상자 IP 주소에만 사용할 수 있습니다. 기본 및 콘솔 IP 주소는 정렬할 수 없습니다.)

새 IP 주소 페이지(배스천 호스트)

장치에서 관리되는 IP 주소 페이지에서 배스천 호스트 정의 링크를 클릭하면 새 IP 주소 페이지가 열립니다. 배스천 호스트는 Linux 또는 Solaris 시스템에서 사용할 수 있습니다.

참고: 배스천 호스트를 구성할 때 콘솔 서버 액세스를 포함한 모든 장치 액세스 시도에서는 먼저 "배스천 호스트"라는 중간 호스트에 로그인한 다음 장치 연결을 시도합니다.

필드	설명/작업
배스천 호스트 IP 주소 값	배스천 호스트의 IP 주소를 입력합니다. 호스트 이름을 입력하면 NA에서 IP 주소로 확인합니다.
사용자 이름	배스천 호스트 액세스에 사용할 사용자 이름을 입력합니다.
암호	배스천 호스트 액세스에 사용할 암호를 입력합니다.
암호 확인	확인용 암호를 재입력합니다.
장치 연결 방법	배스천 호스트에 로그인한 후 장치에 액세스할 방법, SSH 또는 텔넷을 입력합니다.
연결 스크립트 변수	변수 집합을 입력하여 연결 스크립팅을 사용자 지정합니다. NA가 중간 호스트에 연결되었는지 식별하기 위해 조회할 기본 프롬프트 패턴(정규 표현식)은 <code>(\x23 \x24 %)</code> 이며 '#', '\$' 또는 '%'로 변환됩니다. (참고: 필드를 비워 두면 기본 변수를 사용합니다. 기본 변수는 대부분의 배스천 호스트에서 작동해야 합니다.)
주석	필요한 경우 주석을 입력합니다.

새 IP 주소 페이지(사용자 지정 IP 주소)

장치에서 관리되는 IP 주소 페이지에서 새 IP 주소 링크를 클릭하면 새 IP 주소 페이지가 열립니다.

필드	설명/작업
사용자 지정 IP 주소 값	새 IP 주소를 입력합니다. 호스트 이름을 입력하면 NA에서 IP 주소로 확인합니다.
장치 액세스	장치 액세스를 사용하면 사용자 지정 IP 주소를 사용하여 장치에 액세스할 수 있습니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •아니요 — IP 주소를 사용하여 장치에 액세스하지 않습니다. •예 — IP 주소를 사용하여 장치에 액세스합니다. •전용 — 장치를 액세스할 때 이 IP 주소(경로)만 사용합니다. 다른 모든 장치에 대한 장치 액세스가 '아니요'로 설정됩니다.
주석	필요한 경우 주석을 입력합니다.

새 IP 주소 페이지(콘솔 서버)

장치에서 관리되는 IP 주소 페이지에서 새 콘솔 서버 링크를 클릭하면 새 IP 주소 페이지가 열립니다.

참고: 콘솔 서버는 텔넷 사용 콘솔 서버에서 포트에 따라 장치에 자동 통과를 제공할 때 사용됩니다. 이 옵션은 텔넷에만 적용됩니다. 콘솔 서버를 사용하면 장치에 텔넷이 자동으로 사용됩니다.

필드	설명/작업
콘솔 IP 주소 값	새 콘솔 IP 주소를 입력합니다. 호스트 이름을 입력하면 NA에서 IP 주소로 확인합니다.
콘솔 포트	콘솔 서버의 콘솔 포트를 입력합니다.
장치 액세스	장치 액세스를 사용하면 콘솔 서버를 사용하여 장치에 액세스할 수 있습니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none">•아니요 — IP 주소를 사용하여 장치에 액세스하지 않습니다.•예 — IP 주소를 사용하여 장치에 액세스합니다.•전용 — 장치를 액세스할 때 이 IP 주소(경로)만 사용합니다. 다른 모든 장치에 대한 장치 액세스가 '아니요'로 설정됩니다.
주석	필요한 경우 주석을 입력합니다.

새 IP 주소 페이지(홉 상자)

장치에서 관리되는 IP 주소 페이지에서 새 홉 상자 링크를 클릭하면 새 IP 주소 페이지가 열립니다.

홉 상자는 일반적으로 "배스천 호스트" 스크립팅을 사용하여 장치에 연결합니다. 배스천 호스트와 달린 홉 상자 옵션을 사용하려면 중간 호스트에 로그인한 후 사용할 IP 주소를 지정해야 합니다. 홉 상자 경로는 지정된 배스천 호스트(있는 경우)를 먼저 통과하지 않습니다.

필드	설명/작업
홉 상자 IP 주소 값	홉 상자의 IP 주소를 입력합니다. 호스트 이름을 입력하면 NA에서 IP 주소로 확인합니다.
대상 IP(홉 상자)	홉 상자에서 이동할 IP 주소를 입력합니다.
사용자 이름	홉 상자 액세스에 사용할 사용자 이름을 입력합니다.
암호	홉 상자 액세스에 사용할 암호를 입력합니다.
암호 확인	확인용 암호를 재입력합니다.
장치 연결 방법	홉 상자에 로그인한 후 장치에 액세스할 방법, SSH 또는 텔넷을 입력합니다.
연결 스크립트 변수	변수 집합을 입력하여 연결 스크립팅을 사용자 지정합니다. NA가 중간 호스트에 연결되었는지 식별하기 위해 조회할 기본 프롬프트 패턴(정규 표현식)은 <code>(\x23 \x24 %)</code> 이며 '#', '\$' 또는 '%'로 변환됩니다. (참고: 필드를 비워 두면 기본 변수를 사용합니다. 기본 변수는 대부분의 배스천 호스트에서 작동해야 합니다.)
주석	필요한 경우 주석을 입력합니다.

새 IP 주소 페이지(새 통과 연결)

장치에서 관리되는 IP 주소 페이지에서 새 통과 연결 링크를 클릭하면 새 IP 주소 페이지가 열립니다.

새 통과 연결 옵션을 사용하면 다른 장치를 통해 장치에 연결할 수 있습니다. 이 옵션은 CLI를 통해서만 지원됩니다. SNMP는 지원되지 않습니다.

참고: 새 통과 연결은 NA에 이미 존재하는 장치에 대해서만 사용할 수 있습니다.

텔넷 및 SSH를 사용 시 네 가지 조합을 사용할 수 있습니다.

- 장치 B(SSH)를 통해 장치 A(SSH)에 액세스
- 장치 B(텔넷)를 통해 장치 A(SSH)에 액세스
- 장치 B(SSH)를 통해 장치 A(텔넷)에 액세스
- 장치 B(텔넷)를 통해 장치 A(텔넷)에 액세스

따라서 장치 B를 통해 장치 A에 연결할 때 새 통과 연결에서 장치 B를 자동으로 추가합니다. 발견된 컨텍스트가 NA 모듈 상태 진단의 일부로서 장치로 모두 추가되며 연결 경로가 자동으로 구성됩니다. 장치 컨텍스트에 대한 자세한 내용은 [448페이지의 "장치 컨텍스트 추가 작업 페이지 필드"](#)를 참조하십시오.

필드	설명/작업
통과 연결 IP 주소 값	연결에 사용할 새 IP 주소를 입력합니다.
장치 액세스	장치 액세스를 사용하면 IP 주소를 사용하여 장치에 액세스할 수 있습니다. SCP를 사용할 수 없습니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 아니요 — IP 주소를 사용하여 장치에 액세스하지 않습니다. • 예 — IP 주소를 사용하여 장치에 액세스합니다. • 전용 — 장치를 액세스할 때 이 IP 주소(경로)만 사용합니다. 다른 모든 장치에 대한 장치 액세스가 '아니요'로 설정됩니다.
주석	필요한 경우 주석을 입력합니다.

프로비전 메뉴 옵션

메뉴 옵션	설명/작업
템플릿에서 장치 프로비전	이 장치에 대한 장치 템플릿을 볼 수 있는 장치 템플릿 페이지를 엽니다. 자세한 내용은 155페이지의 "장치 템플릿 페이지 필드" 를 참조하십시오.
정책 준수 확인	구성 및 소프트웨어가 현재 정책을 준수하는지 여부를 볼 수 있는 새 작업 - 정책 준수 확인 페이지를 엽니다. 462페이지의 "정책 준수 확인 작업 페이지 필드" 를 참조하십시오.
Syslog 구성	실시간 변경 감지를 위해 이 장치에서 Syslog를 구성할 수 있는 새 작업 - Syslog 구성 페이지를 엽니다. 366페이지의 "Syslog 구성 작업 페이지 필드" 를 참조하십시오.
ACL 삭제	ACL을 삭제할 수 있는 새 작업 - ACL 삭제 페이지를 엽니다. 887페이지의 "ACL 삭제" 를 참조하십시오.
암호 배포	장치에 암호 변경을 배포하는 작업을 설정할 수 있는 새 작업 - 암호 배포 페이지를 엽니다. 370페이지의 "암호 배포 작업 페이지 필드" 를 참조하십시오.
장치 재부팅	NA 데이터베이스에 있는 장치를 재부팅할 수 있는 새 작업 - 장치 재부팅 페이지를 엽니다. 379페이지의 "장치 재부팅 작업 페이지 필드" 를 참조하십시오.
ICMP 테스트 실행	한 장치에서 하나 이상의 다른 장치로 Ping 또는 Traceroute 테스트를 예약할 수 있는 새 작업 - ICMP 테스트 실행 페이지를 엽니다. 383페이지의 "ICMP 테스트 실행 작업 페이지 필드" 를 참조하십시오.
명령 스크립트 실행	장치에 대한 명령 스크립트를 편집 및 예약할 수 있는 새 작업 - 명령 스크립트 실행 페이지를 엽니다. 389페이지의 "명령 스크립트 실행 작업 페이지 필드" 를 참조하십시오.
진단 실행	장치에 대한 진단을 예약할 수 있는 새 작업 - 진단 실행 페이지를 엽니다. 397페이지의 "진단 실행 작업 페이지 필드" 를 참조하십시오.
시작 및 실행 동기화	장치에 대한 구성의 시작 및 실행을 동기화할 수 있는 새 작업 - 시작 및 실행 동기화 페이지를 엽니다. 408페이지의 "시작 및 실행 동기화 작업 페이지 필드" 를 참조하십시오.
장치 소프트웨어 업데이트	하나 이상의 장치에 대해 소프트웨어 배포를 예약할 수 있는 새 작업 - 장치 소프트웨어 업데이트 페이지를 엽니다. 413페이지의 "장치 소프트웨어 업데이트 작업 페이지 필드" 를 참조하십시오.

메뉴 옵션	설명/작업
새 VLAN	새 작업 - VLAN 페이지를 엽니다. 이 페이지에서는 네트워크 스위치의 VLAN을 구성할 수 있습니다. 자세한 내용은 452페이지의 "VLAN 작업 페이지 필드" 를 참조하십시오.
OS 분석	sysoid(장치 모델의 고유 식별자), OS 버전, 플래시 저장 옵션, 모듈 등의 정보와 같은 Cisco 장치에 대한 데이터를 수집하는 새 작업 - OS 분석 작업 페이지를 엽니다. 자세한 내용은 436페이지의 "OS 분석 작업 페이지 필드" 를 참조하십시오.
장치 컨텍스트	장치 컨텍스트를 만들 수 있는 새 작업 - 장치 컨텍스트 페이지를 엽니다. 컨텍스트란 장치 내부의 장치를 말합니다. 컨텍스트는 하드웨어(모듈 및 슬롯 포함) 또는 가상일 수 있습니다. NA에서는 장치 컨텍스트를 사용하여 상위 장치와 하위 장치 간 관계를 자동으로 추가합니다. NA에서는 컨텍스트에 IP 주소를 지정할 필요가 없습니다. 그보다는 컨텍스트와의 통과 경로 연결을 구성하여 NA에서 컨텍스트를 관리할 수 있습니다. 자세한 내용은 448페이지의 "장치 컨텍스트 추가 작업 페이지 필드" 를 참조하십시오.
포트 스캔	Nmap에서 네트워크 장치를 검색할 수 있는 새 작업 - 포트 스캔 페이지를 엽니다. Nmap은 장치의 포트를 검색하고 열린 포트와 해당 포트에서 제공하는 서비스에 대한 세부 사항을 반환하는 데 사용할 수 있습니다. 자세한 내용은 440페이지의 "포트 스캔 페이지 필드" 를 참조하십시오.

연결 메뉴 옵션

NA는 텔넷 또는 SSH 프로토콜을 사용하는 네트워크 장치에 대한 단일 사인온을 지원합니다. NA 서버는 텔넷/SSH 프록시로서 작동합니다. 전송된 데이터는 일반 텍스트 형식입니다.

NA 서버를 텔넷/SSH 프록시로 사용하지 않는 경우 안전한 URL을 통해 또는 표준 텔넷 명령을 사용하여 장치에 직접 로그인할 수 있습니다.

메뉴 옵션	설명/작업
텔넷을 사용하는 프록시를 통해	이 장치에 텔넷 명령을 입력할 수 있는 텔넷 창을 엽니다.
SSH를 사용하는 프록시를 통해	이 장치에 SSH 명령을 입력할 수 있는 SSH 창을 엽니다.

6장: 사용자 관리

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
사용자 추가	319페이지의 "사용자 추가"
전자 메일 알림	322페이지의 "전자 메일 알림"
사용자 암호 구성	326페이지의 "사용자 암호 구성"
사용자 그룹 추가	330페이지의 "사용자 그룹 추가"
새 사용자 역할 추가	335페이지의 "사용자 역할 추가"
사용자 설정 편집	338페이지의 "사용자 설정 편집"
빠른 시작	345페이지의 "빠른 시작이란?"
NA 홈 페이지 사용자 지정	349페이지의 "NA 홈 페이지 사용자 지정"
검색/연결 기능	354페이지의 "검색/연결 기능"

사용자 관리 탐색

The screenshot displays the HP Network Automation web interface. The top navigation bar includes the HP logo, the text 'HP Network Automation', and a '로그아웃' (Logout) button. The main navigation menu consists of several items: '장치' (Devices), '작업' (Jobs), '정책' (Policies), '보고서' (Reports), '관리' (Management), and '도움말' (Help). The '관리' (Management) menu is currently expanded, showing a list of sub-items:

- 사용자 (Users)
- 사용자 그룹 (User Groups)
- 새 사용자 (New Users)
- 새 사용자 그룹 (New User Groups)
- 로그온한 사용자 (Logged-in Users)
- 사용자 역할 및 권한 (User Roles and Permissions)
- 보안 파티션 (Security Partitions)
- 게이트웨이 (Gateways)
- 장치 암호 규칙 (Device Password Rules)
- 이벤트 알림 및 응답 규칙 (Event Notifications and Response Rules)
- 사용자 지정 데이터 설정 (Custom Data Settings)
- LDAP 설정 (LDAP Settings)
- 워크플로 설정 (Workflow Settings)
- 관리 설정 (Management Settings) ▶
- 작업 로드 (Job Load)
- 시스템 상태 (System Status)
- 서비스 시작 / 중지 (Start / Stop Services)
- 문제 해결 (Troubleshooting)
- 드라이버 (Drivers)
- 시스템 작업 (System Jobs) ▶

사용자 추가

사용자 인증 및 권한을 지정하는 작업은 중요한 작업입니다. 선택한 항목은 HP NA(Network Automation)를 사용하는 방식에 영향을 줍니다. 적절한 인증 및 권한 설정을 채택할 경우 많은 보안 위험이 완화될 수 있습니다.

일반적으로 정보 보안 및 IT 부서 모두에서 행하는 가장 좋은 방식은 "최저 권한" 개념을 포함합니다. 즉 각 사용자에게 직무를 수행하는 데 필요한 최소한의 권한을 할당해야 함을 의미합니다. 또한 일부 조직은 특성 상 각 사용자가 수행할 수 있는 작업을 사용자의 역할별로 구분하기에 적절한 환경을 만듭니다.



이 섹션에서는 다음과 같은 용어가 사용됩니다.

- **역할** — 사용자를 동일한 보안 권한을 공유하는 그룹으로 분할하는 데 역할을 사용합니다. 역할에 할당된 사용자에게는 역할별로 정의된 권한이 허가됩니다. 예를 들어 사용자에게 장치 추가, 구성 정책 관리 또는 소프트웨어 배포와 같은 특정 운영을 수행할 수 있는 권한이 부여된 경우 NA는 리소스에 액세스할 고정 역할 ID를 사용합니다. 기존 역할을 시작점으로 사용하지 않고 처음부터 새 사용자 역할을 생성하면 모든 작업 유형에 대한 기본 거부 권한을 포함한 템플릿이 생성됩니다. 이를 통해 "최저 권한" 보안 모범 사례와 더불어 역할을 쉽게 생성할 수 있습니다.
- **사용자 그룹** — 사용자 그룹은 사용자 관리 목적을 위한 논리적 컨테이너입니다. 시스템 관리자는 사용자를 사용자 그룹에 할당하고, 사용자 그룹을 특정 역할에 매핑할 수 있습니다. 사용자 그룹에 하나 이상의 역할을 할당할 수 있습니다.

새 사용자를 추가하려면 관리 아래의 메뉴 모음에서 사용자를 클릭합니다. 모든 사용자 페이지가 열립니다. 페이지 상단에 있는 새 사용자 링크를 클릭합니다. 새 사용자 페이지가 열립니다. **323페이지의 "새 사용자 페이지 필드"**를 참조하십시오.

참고: 관리에서 새 사용자 옵션을 클릭하여 새 사용자 페이지로 이동할 수도 있습니다.

모든 사용자 페이지 필드

필드	설명
새 사용자 링크	사용자를 추가할 수 있는 새 사용자 페이지를 엽니다. 자세한 내용은 323페이지의 "새 사용자 페이지 필드" 를 참조하십시오. 시스템 관리자만 사용자를 추가할 수 있습니다.
사용자 검색 링크	사용자 검색 페이지를 엽니다. 이 페이지에서 이름, 성, 전자 메일 주소 및/또는 AAA 사용자 이름으로 사용자를 검색할 수 있습니다. 자세한 내용은 648페이지의 "사용자 검색" 을 참조하십시오.
로그온한 사용자 링크	사용자 이름, 사용자 호스트 및 마지막 액세스 시간을 포함하여 현재 로그인된 사용자를 볼 수 있는 로그온한 사용자 페이지를 엽니다. 이 페이지는 명령줄 인터페이스 (CLI)가 아닌 웹 UI를 사용하여 로그인한 사용자만 표시합니다. (참고: 또한 관리 드롭다운 메뉴에서 로그온한 사용자 옵션을 선택하여 이 페이지를 볼 수 있습니다.) 자세한 내용은 321페이지의 "로그온한 사용자 페이지 필드" 를 참조하십시오.
사용자 그룹 링크	사용자 그룹을 추가 및 편집할 수 있는 사용자 그룹 페이지를 엽니다. 자세한 내용은 330페이지의 "사용자 그룹 페이지 필드" 를 참조하십시오.
사용자 역할 및 권한 링크	사용자 권한을 편집할 수 있는 사용자 역할 및 권한 페이지를 엽니다. 자세한 내용은 335페이지의 "사용자 역할 및 권한 페이지 필드" 를 참조하십시오.
이 그룹에 있는 사용자	다음 아이콘을 표시합니다. <ul style="list-style-type: none">  일반 사용자 계정  비활성화된 사용자 계정
사용자 이름	사용자의 전체 이름을 표시합니다.
이름	사용자의 이름을 표시합니다.
성	사용자의 성을 표시합니다.
전자 메일	사용자의 전자 메일 주소를 표시합니다.

필드	설명
작업	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 편집 — 사용자 편집 페이지를 엽니다. 계정이 사용자 자신의 계정인 경우 내 프로필 페이지가 열립니다. 관리자 그룹 내 사용자만 내 프로필 페이지의 암호 옵션을 볼 수 있습니다. 자세한 내용은 339페이지의 "내 프로필 페이지 필드"를 참조하십시오. 프로필에 대한 변경 내용이 사용자 목록 페이지에 표시됩니다. • 삭제 — 관리 권한으로 사용자를 삭제할 수 있습니다. • 권한 — 사용자 권한 페이지를 엽니다. 페이지 상단에 있는 사용자 프로필 편집 옵션을 클릭하면 사용자 편집 페이지가 열립니다. 사용자 프로필을 변경하고 저장할 수 있습니다. 변경 사항은 사용자 목록 페이지에 표시됩니다. 자세한 내용은 323페이지의 "새 사용자 페이지 필드"를 참조하십시오. • 구성 변경 사항 — 구성 검색 결과 페이지를 엽니다. 이 페이지는 사용자가 작성한 구성 변경 사항을 표시합니다. 자세한 내용은 223페이지의 "장치 구성 변경 보기"를 참조하십시오.

로그온한 사용자 페이지 필드

로그온 사용자 페이지를 사용하면 사용자 이름, 전자 메일 주소, 사용자 호스트 시스템, 그리고 사용자가 호스트 시스템에 액세스한 마지막 날짜 및 시간 등 NA에 현재 로그인되어 있는 사람을 볼 수 있습니다. 이 페이지는 CLI(명령줄 인터페이스)가 아닌 NA UI를 사용하여 로그인한 사용자만 표시합니다.

필드	설명/작업
사용자 이름	사용자 이름을 표시합니다.
전자 메일 주소	사용자의 전자 메일 주소를 표시합니다. 전자 메일 메시지를 로그인한 사용자와 주고 받으려면 322페이지의 "전자 메일 알림" 을 참조하십시오.
사용자 호스트	사용자가 로그인된 시스템의 호스트 IP 주소를 표시합니다.
마지막 액세스 시간	사용자가 시스템에 마지막으로 액세스한 날짜 및 시간을 표시합니다.

전자 메일 알림

NA에 로그인한 동안은 한 명 이상의 로그인된 NA 사용자에게 메시지를 보낼 수 있습니다. 메시지를 삭제할 수 있지만, NA에서 로그아웃하고 나면 모든 메시지가 자동으로 삭제됩니다.

참고: NA UI 프레임워크가 메시지를 전달하므로 API를 사용하여 이 기능을 구현할 수 없습니다. 데이터베이스 액세스 권한이 없습니다.

메시지를 보내려면

1. 관리 메뉴에서 로그인한 사용자를 클릭합니다. 로그인한 사용자 페이지가 열립니다.
2. 메시지를 보낼 사용자의 확인란을 선택합니다. 선택 드롭다운 메뉴에서 모든 사용자를 선택할 수 있습니다.
3. 작업 드롭다운 메뉴에서 메시지 보내기를 선택합니다. 메시지 보내기 페이지가 열립니다.
4. 메시지 필드에 메시지 텍스트를 입력합니다.
5. 메시지 텍스트를 입력했으면 제출 버튼을 클릭합니다. 성공하면 "메시지가 전송되었습니다." 메시지가 로그인한 사용자 페이지 맨 위에 표시됩니다.

메시지를 읽으려면

1. 새 메시지가 있으면 NA UI의 왼쪽 프레임 맨 위에서 "새 메시지가 도착했습니다." 링크를 클릭합니다. 메시지를 보낸 사람과 보낸 시간 등의 메시지가 표시됩니다. 메시지에 회신하거나 메시지를 삭제할 수 있습니다.

참고: 모든 메시지를 읽은 후에는 "새 메시지가 도착했습니다." 링크가 메시지 보기로 바뀝니다. 모든 메시지가 전송된 순서대로 표시됩니다.

2. 회신 버튼을 클릭하면 메시지에 회신할 수 있는 메시지 보내기 페이지가 열립니다. 삭제 버튼을 클릭하면 메시지가 삭제됩니다.

회신을 보내는 경우 NA는 원본 메시지의 보낸 사람 사용자 ID에 지정된 사용자 ID를 사용합니다. 현재의 사용자가 새 메시지의 보낸 사람 ID에 자동으로 지정됩니다.

1. 메시지 아래에서 회신 버튼을 선택합니다. 메시지 보내기 페이지가 열립니다.
2. 메시지 텍스트를 입력하고 제출 버튼을 클릭합니다. "새 메시지가 도착했습니다." 링크가 메시지를 보낸 대상 사용자의 NA UI에서 왼쪽 프레임 맨 위에 표시됩니다.

새 사용자 페이지 필드

사용자를 처음 추가할 때 관리 계정 정보를 제외하고는 이 페이지가 비어 있습니다. 이 페이지를 완료하고 나서 저장한 후 정보를 편집해야 하는 경우 사용자 편집 페이지에서 편집 작업을 수행할 수 있습니다. 사용자 편집 페이지의 필드는 새 사용자 페이지의 필드와 동일합니다.

필드	설명/작업
사용자 정보	
사용자 이름	사용자의 NA 사용자 이름을 입력합니다. Operator 또는 Administrator와 같이 NA에 로그인하는 데 이 이름을 사용합니다. (참고: 사용자 이름에 공백을 포함하지 마십시오. 사용자 이름에는 문자, 숫자, 점, 밑줄, 하이픈 및 백슬래시만 사용할 수 있습니다.)
암호	사용자의 NA 암호를 입력합니다. 이 암호는 NA에 로그인할 때 사용됩니다. 암호 설정에 대한 자세한 내용은 326페이지의 "사용자 암호 구성" 을 참조하십시오.
암호 확인	확인을 위해 사용자 NA 암호를 입력합니다.
암호 옵션	다음 옵션 중 하나 이상을 선택합니다. <ul style="list-style-type: none"> • 사용자: 다음 로그인 시에 암호를 변경해야 함 • 사용자: 암호를 변경할 수 없음 • 암호 만료 안 함 • 계정이 잠김 <p>암호 옵션 설정에 대한 자세한 내용은 326페이지의 "사용자 암호 구성"을 참조하십시오.</p>
이름	사용자의 이름을 입력합니다.

필드	설명/작업
성	사용자의 성을 입력합니다.
전자 메일 주소	사용자의 전자 메일 주소를 입력합니다.
사용자가 속한 그룹	<p>사용자가 속하는 다음 기본 사용자 그룹 중 하나 이상을 선택합니다. 이러한 그룹은 사용자에게 사용자 역할 및 모든 관련 권한을 제공합니다. NA는 기본적으로 그룹을 할당하지 않습니다. 그룹에 속하지 않는 사용자는 장치 및 구성 변경 보기와 같은 제한된 작업만 수행할 수 있습니다. (참고: 새 그룹을 생성했으면 목록에 표시됩니다.)</p> <ul style="list-style-type: none"> • 제한된 액세스 — 일반적으로 제한된 액세스 사용자는 네트워크 장치를 구성하기 위한 암호를 가지지 않는 운영자입니다. 이들은 장치를 볼 수는 있지만 NA 데이터베이스의 대부분의 정보를 수정하거나 네트워크 장치를 다시 구성하는 운영 또는 일괄 운영을 실행할 수는 없습니다. • 전체 액세스 사용자 — 일반적으로 전체 액세스 사용자는 네트워크의 전체가 아닌 일부 장치를 구성하기 위한 암호로 신뢰된 네트워크 엔지니어입니다. 이들은 NA 데이터베이스에 있는 대부분의 정보를 수정할 수 있으며 일괄 모드가 아닌 한 번에 하나씩 장치를 재구성할 수 있습니다. 종종 이들 사용자는 재구성할 수 있는 장치에 관하여 제한됩니다. • 파워 사용자 — 파워 사용자는 일반적으로 대부분의 작업을 수행할 수 있는 전문 엔지니어입니다. 이들은 장치 그룹을 다시 구성하고 다른 작업을 수행할 수 있습니다. • 관리자 — 관리자는 사용자 관리, 정책 설정 및 네트워크 전체 운영 실행을 포함하여 NA 관리를 책임집니다. 이들은 모든 장치에 모든 작업을 수행하는 권한을 가집니다. • 모든 파티션 보기 — 사용자가 모든 파티션을 볼 수 있습니다. 파티션은 일련의 NA 장치입니다. 각 파티션은 한 NA 코어에만 속합니다. 따라서 파티션은 하나의 NA 코어에 의해서만 관리됩니다. 뿐만 아니라 각 장치는 한 파티션에만 속합니다. 파티션 구성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화"를 참조하십시오.

필드	설명/작업
상태	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 사용함 — 계정이 활성화됩니다(기본값). • 사용 안 함 — 계정이 비활성화됩니다. 이 옵션을 사용하여 계정을 비활성화하면서 시스템에서 계정을 보존할 수 있습니다.
외부 인증 장애 조치	외부 인증 서버에 접근할 수 없는 경우 로컬 인증으로 인증 장애 조치를 활성화할 수 있습니다.
주석	계정에 대한 설명을 입력합니다.
파티션	이 사용자가 속하는 파티션을 선택합니다. 해당 사용자는 해당 파티션에 대한 보기 권한이 있는 다른 사용자에게만 표시됩니다. (참고: 사용자가 한 파티션에만 액세스할 수 있는 경우에는 파티션 드롭다운 메뉴가 표시되지 않습니다.)

AAA

AAA 사용자 이름	이 사용자에 대한 AAA(TACACS+ 또는 RADIUS) 사용자 이름을 입력합니다. 그러면 NA가 AAA 사용자 이름을 NA 사용자 이름과 연관시킬 수 있습니다. NA가 로컬 인증으로 장애 조치를 실행하도록 하려면 사용자 계정에 대해 이 성능을 활성화해야 합니다. 기본적으로 NA는 로컬 인증으로 장애 조치하지 않습니다.
AAA 암호	이 사용자의 AAA 암호를 입력합니다.
AAA 암호 확인	확인을 위해 AAA 암호를 다시 입력합니다.
프록시 인터페이스에 AAA 로그인 사용 확인란	이 옵션을 사용하면 텔넷/SSH 프록시에 사용자를 로그인할 때 NA는 사용자의 AAA 자격 증명을 확인합니다.

SecurID

새 사용자가 추가된 후 사용자 정보를 편집할 때 소프트웨어 토큰 관리 페이지 링크가 표시됩니다. 소프트웨어 토큰 관리 페이지를 사용하면 사용자의 로그인과 연관된 소프트웨어 토큰 라이선스를 추가할 수 있습니다. [793페이지의 "SecurID 소프트웨어 토큰 추가"](#)를 참조하십시오.

사용자 암호 구성

다음 옵션은 새 사용자 프로필을 작성하거나 기존 사용자 프로필을 편집할 때 사용자 암호 설정 권한을 가진 NA 사용자의 새 사용자 및 사용자 편집 페이지에 표시됩니다.

- 사용자는 다음 로그인 시에 암호를 변경해야 함
- 사용자는 암호를 변경할 수 없음
- 암호 만료 안 함
- 계정이 잠김

사용자가 관리자 그룹에 포함된 경우 이러한 옵션이 내 프로필 페이지에도 표시됩니다. 자세한 내용은 [339페이지의 "내 프로필 페이지 필드"](#)를 참조하십시오.

참고: CLI를 사용하는 경우 사용자는 암호가 만료되면 로그인할 수 없습니다. 이 경우에는 NA UI를 사용하여 암호를 재설정해야 합니다.

사용자 시나리오 1

사용자 A가 다른 기회를 위해 회사를 그만두려 하며 이 사용자의 계정을 비활성화해야 하지만 계정과 관련된 기록 데이터는 보존해야 합니다. NA 시스템 관리자는 다음을 수행합니다.

1. NA에 로그인합니다.
2. 관리 아래에 있는 기본 메뉴에서 NA 시스템 관리자가 사용자 옵션을 클릭합니다. 모든 사용자 페이지가 열립니다.
3. NA 시스템 관리자가 사용자 A에 대한 작업 열에서 편집 옵션을 클릭합니다. 사용자 A에 대한 사용자 편집 페이지가 열립니다.
4. 사용자 편집 페이지에서 NA 시스템 관리자는 상태 필드에 대해 "사용 안 함" 옵션을 선택하고 저장 버튼을 클릭합니다.

위의 작업의 결과로서, 사용자 A가 NA에 로그인을 시도할 경우 이 사용자에게는 **계정이 비활성화되었습니다.** 라는 메시지가 표시됩니다.

사용자 시나리오 2

NA 시스템 관리자가 NA 시스템에 대한 유지 보수를 수행하려고 합니다. 관리자는 시스템에 로그인된 NA 사용자가 있는지 확인해야 합니다. 모든 사람이 NA에서 로그아웃한 후 NA 시스템 관리자는 다음을 수행합니다.

1. NA에 로그인합니다.
2. 관리 아래에 있는 기본 메뉴에서 NA 시스템 관리자가 사용자 옵션을 클릭합니다. 모든 사용자 페이지가 열립니다.
3. NA 시스템 관리자가 각 사용자에게 대한 작업 열에서 편집 옵션을 클릭합니다. 사용자 편집 페이지가 열립니다.
4. 사용자 편집 페이지에서 NA 시스템 관리자는 암호 옵션 필드에 대해 계정이 잠김 확인란을 선택하고 저장 버튼을 클릭합니다.

위의 작업의 결과로서 시스템 유지 보수 기간 동안 사용자가 NA에 로그인하려고 할 경우 해당 사용자에게 **계정이 잠겼습니다**. 메시지가 표시됩니다.

시스템 유지 보수를 완료한 NA 시스템 관리자가 각 사용자에게 대한 사용자 편집 페이지로 돌아가서 계정이 잠김 확인란의 선택을 취소하고 저장 버튼을 클릭합니다. 따라서 사용자는 이제 NA에 로그인할 수 있습니다.

참고: 현재 사용자 계정을 일괄 편집하는 방법은 없습니다.

사용자 시나리오 3

사용자 B가 몇 주 동안 휴직했습니다. 그녀가 휴직한 동안 NA 시스템 관리자에게 새로운 회사 암호 정책을 준수하라는 지시가 내려왔습니다. 직원은 이제 30일마다 NA 암호를 변경해야 합니다. 이 새로운 정책을 준수하기 위해 NA 시스템 관리자는 다음을 수행합니다.

1. NA에 로그인합니다.
2. 관리 아래에 있는 기본 메뉴에서 NA 시스템 관리자가 사용자 옵션을 클릭합니다. 모든 사용자 페이지가 열립니다.
3. NA 시스템 관리자가 사용자 B에 대한 작업 열에서 편집 옵션을 클릭합니다. 사용자 편집 페이지가 열립니다.
4. 사용자 편집 페이지에서 NA 시스템 관리자는 사용자는 암호 옵션 필드에 대해 "다음 로그인 시에 암호를 변경해야 함" 확인란을 선택하고 저장 버튼을 클릭합니다.

위의 작업의 결과로, 사용자 B가 회사에 다시 출근하여 NA에 로그인하려 할 때 이 사용자에게 암호가 만료되었습니다. 암호를 재설정하십시오. 새 암호는 이전 <8>개 암호와 일치해서는 안 됩니다. 메시지가 표시됩니다.

사용자 B는 사용자 이름, 이전 암호 및 새 암호를 입력하고 나서 확인을 위해 새 암호를 다시 한 번 입력해야 합니다.

참고: NA 시스템 관리자가 새 사용자 또는 사용자 편집 페이지에서 "사용자는 암호를 변경할 수 없음" 옵션을 선택한 경우가 아니면 사용자는 암호 변경 페이지에서 암호를 변경할 수 있습니다. 자세한 내용은 [344페이지의 "암호 변경 페이지 필드"](#)를 참조하십시오.

암호 만료

NA 시스템 관리자는 새 사용자 및 사용자 편집 페이지에서 암호 만료 안 함 옵션을 선택하여 NA 사용자 암호 만료를 활성화하거나 비활성화할 수 있습니다. 보안을 위해 다음 설정이 *appserver.rcx* 파일이 포함됩니다.

- *security/user_password_expiration_enabled* 기본적으로 이 설정은 False입니다.
- *security/user_password_expire_in_days* 기본적으로 이 값은 180일입니다. 이 값은 0보다 크고 1000보다 작아야 합니다. *security/user_password_expiration_enabled* 설정이 False인 경우 이 설정이 무시됩니다.

기본값을 수정해야 하는 경우 다음을 수행합니다.

1. NA를 중지합니다.
2. *\$NA/adjustable_options.rcx* 파일을 열고 <options>과 </options> 태그 사이에 아무데나 다음 항목을 추가합니다.

```
<option name=security/user_password_expiration_enabled>>false</option>
<option name=security/user_password_expire_in_days>180</option>
<option name=security/user_password_reuse_allowed>>false</option>
<option name=security/user_password_history_size>8</option>
```


3. 필요에 따라 값을 수정하고 파일을 저장합니다.
4. 모든 NA 코어에서 1~3단계를 반복합니다.
5. NA를 다시 시작합니다.

암호 재사용

사용자가 이전 암호를 사용할 수 없도록 하기 위해 이전 암호가 데이터베이스에 저장됩니다. 이 용도로 새 RN_PASSWORD_HISTORY 테이블이 생성되었습니다.

두 개의 새로운 설정이 *appserver.rcx* 파일에 포함됩니다.

- *security/user_password_reuse_allowed* 기본값은 False입니다.
- *security/user_password_history_size* 기본값은 8입니다. 유효한 범위는 [1, 999]입니다.

사용자 그룹 추가

새 사용자 그룹을 추가하려면 관리 아래의 메뉴 모음에서 사용자 그룹을 클릭합니다. 사용자 그룹 페이지가 열립니다. 페이지 상단에 있는 새 사용자 그룹 링크를 클릭합니다. 새 사용자 그룹 페이지가 열립니다. **331페이지의 "새 사용자 그룹 페이지 필드"**를 참조하십시오.

참고: 또한 사용자 그룹 링크를 클릭하여 모든 사용자 페이지에서 이 페이지를 탐색할 수 있습니다.

사용자 그룹 페이지 필드

필드	설명/작업
새 사용자 그룹 링크	사용자 그룹을 추가할 수 있는 새 사용자 그룹 페이지를 엽니다. 자세한 내용은 331페이지의 "새 사용자 그룹 페이지 필드" 를 참조하십시오.
사용자 링크	사용자 그룹을 편집할 수 있는 모든 사용자 페이지를 엽니다. 자세한 내용은 320페이지의 "모든 사용자 페이지 필드" 를 참조하십시오.
사용자 역할 및 권한 링크	사용자 권한을 편집할 수 있는 사용자 역할 및 권한 페이지를 엽니다. 자세한 내용은 335페이지의 "사용자 역할 및 권한 페이지 필드" 를 참조하십시오.
그룹 이름	사용자 그룹의 이름을 표시합니다. 그룹 이름 링크를 클릭하면 그룹의 모든 현재 사용자를 볼 수 있는 사용자 세부사항 페이지가 열립니다. 사용자 추가 및 사용자 프로필 편집에 대한 자세한 내용은 320페이지의 "모든 사용자 페이지 필드" 를 참조하십시오.
설명	그룹에 대한 간단한 설명을 표시합니다.
사용자 역할	그룹에 할당된 사용자 역할을 표시합니다. 사용자 역할을 클릭하면 사용자 역할에 대한 세부사항을 볼 수 있는 사용자 역할 정보 페이지가 열립니다. 자세한 내용은 335페이지의 "사용자 역할 추가" 를 참조하십시오.
작업	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 편집 — 사용자 그룹 편집 페이지를 엽니다. 자세한 내용은 330페이지의 "사용자 그룹 페이지 필드"를 참조하십시오. • 삭제 — 관리 권한으로 그룹을 삭제할 수 있습니다. • 권한 — 보기 권한 페이지를 엽니다. 자세한 내용은 331페이지의 "새 사용자 그룹 페이지 필드"를 참조하십시오.

새 사용자 그룹 페이지 필드

기본적으로 사용자 그룹은 사용자 그룹에 적용된 역할 집합별로 정의된 대로 가장 관대한 명령 권한을 사용합니다. 적절한 권한 잠금을 보장하려면 사용자 그룹에 최대한 제한적인 역할을 할당하십시오.

필드	설명/작업
일반 정보	
그룹 이름	사용자 그룹의 이름을 입력합니다.
설명	사용자 그룹에 대한 설명을 입력합니다.
파티션	이 사용자가 속하는 파티션을 선택합니다. 해당 사용자는 해당 파티션에 대한 보기 권한이 있는 다른 사용자에게만 표시됩니다. 파티션에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오. (참고: 사용자가 한 파티션에만 액세스할 수 있는 경우에는 파티션 드롭다운 메뉴가 표시되지 않습니다.)

필드	설명/작업
명령 권한	
기존 명령 권한 역할	<p>사용자 그룹의 사용자에게는 수행하려는 모든 작업에 대한 해당 명령 권한이 명시적으로 부여되어야 합니다. 이 옵션을 선택하면(기본값) 다음 옵션 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none"> •관리자 — 관리자는 사용자 관리, 정책 설정 및 네트워크 전체 운영 실행을 포함하여 NA 관리를 책임집니다. 이들은 모든 장치에 모든 작업을 수행하는 권한을 가집니다. •파워 — 파워 사용자는 일반적으로 대부분의 작업을 수행할 수 있는 전문 엔지니어입니다. 이들은 장치 그룹을 다시 구성하고 다른 작업을 수행할 수 있습니다. •전체 액세스 — 일반적으로 전체 액세스 사용자는 네트워크의 전체가 아닌 일부 장치를 구성하기 위한 암호로 신뢰된 네트워크 엔지니어입니다. 이들은 NA 데이터베이스에 있는 대부분의 정보를 수정할 수 있으며 일괄 모드가 아닌 개별적으로 장치를 재구성할 수 있습니다. 종종 이들 사용자는 재구성할 수 있는 장치에 관하여 제한됩니다. •제한된 액세스 — 일반적으로 제한된 액세스 사용자는 네트워크 장치를 구성하기 위한 암호를 가지지 않는 운영자입니다. 이들은 장치를 볼 수는 있지만 NA 데이터베이스의 대부분의 정보를 수정하거나 네트워크 장치를 다시 구성하는 운영 또는 일괄 운영을 실행할 수는 없습니다. <p>참고: 기본 명령 권한 역할이 아닌 명령 권한 역할을 정의한 경우 목록에 표시됩니다.</p>

필드	설명/작업
사용자 지정된 명령 권한 역할	<p>이 항목을 선택하면 이 사용자 그룹에 특정한 명령 권한을 사용자 지정할 수 있습니다. 각 명령에 대해 이 역할에 권한을 허가 또는 거부하는 버튼을 클릭합니다. 전체 명령 권한 목록을 보려면 917페이지의 "부록 B: 명령 권한"을 참조하십시오. 모두 부여를 클릭하여 모든 명령에 권한을 부여할 수 있습니다. 이것은 관리 사용자에게, 그리고 몇 개의 명령에 대한 권한만 거부하려고 할 때 유용합니다. 모든 명령에 대한 권한을 거부하려면 모두 거부를 클릭합니다. 기본적으로 모든 명령은 거부됩니다. 특정 명령의 오른쪽에 있는 다음 아이콘은 장치 권한 또는 스크립트 권한을 수정해야 할 수 있음을 나타냅니다.</p> <ul style="list-style-type: none"> • 장치 권한 수정 필수 아이콘 — NA가 장치별 기준으로 권한을 제어할 수 있습니다. 권한별 장치 수정은 장치를 수정할 수 있는지 여부를 지정합니다. 이 명령을 실행할 특정 장치에 대한 장치 수정 권한을 가지고 있어야 합니다. 아래에서 "장치 권한 수정"을 참조하십시오. • 스크립트 권한 필수 아이콘 — NA는 명령 스크립트 기준에 따라 권한을 제어할 수 있습니다. 스크립트 권한은 명령 스크립트를 실행할 수 있는지 여부를 지정합니다. 실행할 특정 명령 스크립트에 대한 스크립트 권한을 가지고 있어야 합니다. 아래에서 "스크립트 권한"을 참조하십시오. <p>참고: 사용자 지정 스크립트는 장치 구성을 수정하는 것으로 받아들여지므로, 사용자의 장치 구성 수정 권한에 대해 확인됩니다.</p>
장치 수정 권한	
모든 장치	<p>그룹의 사용자가 모든 장치를 수정할 수 있습니다.</p> <p>참고: 장치 수정 권한이 없는 사용자가 장치 구성을 보는 경우 암호와 SNMP 커뮤니티 문자열 등 장치 구성의 중요 정보가 마스킹됩니다. 따라서 장치 수정 권한이 없는 사용자가 중요 데이터를 볼 수 없습니다.</p>
없음	<p>수정할 수 있는 장치가 없습니다. 이 옵션은 기본 설정입니다.</p>
기존 장치 수정 권한 역할	<p>그룹의 사용자에 대한 기존 장치 수정 권한 역할을 선택할 수 있습니다. 구성된 기존 역할이 없을 경우 '기존 역할을 찾을 수 없습니다' 메시지가 표시됩니다.</p>

필드	설명/작업
사용자 지정된 장치 수정 권한 역할	이 사용자 그룹에 특정한 목록에서 장치 권한 역할을 선택할 수 있습니다.
스크립트 권한	
모든 스크립트	그룹의 사용자가 모든 스크립트를 수정할 수 있습니다.
없음	수정할 수 있는 스크립트가 없습니다. 이 옵션은 기본 설정입니다.
기존 스크립트 권한 역할	그룹의 사용자에 대한 기존 스크립트 권한 역할을 선택할 수 있습니다. 구성된 기존 역할이 없을 경우 '기존 역할을 찾을 수 없습니다' 메시지가 표시됩니다.
사용자 지정된 스크립트 권한 역할	이 사용자 그룹에 특정한 목록에서 스크립트 권한 역할 중 하나를 선택할 수 있습니다.
사용자 지정된 스크립트 권한 역할	목록에서 사용자 지정된 스크립트 권한 역할을 선택할 수 있습니다.
파티션 보기 권한	
모든 객체	사용자 그룹의 사용자는 모든 파티션을 볼 수 있습니다. (자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.) 참고: 보기 권한을 사용하지 않으면 새 사용자가 모든 파티션 보기 그룹에 놓여 모든 장치에 대한 보기 권한이 부여됩니다. 반면 보기 권한을 생성하면 새 사용자에게는 암시적으로 어떠한 보기 권한도 부여되지 않습니다.
없음	볼 수 있는 파티션이 없습니다. 이 옵션은 기본 설정입니다.
기존 보기 권한 역할	사용자 그룹의 사용자에 대한 기존 보기 권한 역할을 선택할 수 있습니다. 구성된 기존 역할이 없을 경우 '기존 역할을 찾을 수 없습니다' 메시지가 표시됩니다.
사용자 지정된 보기 권한 역할	목록에서 보기 권한 역할을 선택할 수 있습니다. 모두 라디오 버튼을 선택하면 모든 파티션이 포함됩니다.
사용자	
그룹에 있는 사용자/모든 사용자	사용자를 추가하려면 오른쪽 상자에서 사용자를 선택하고 << 추가를 클릭합니다. 사용자를 제거하려면 왼쪽 상자에서 사용자를 선택하고 제거를 클릭합니다.

완료되면 저장 버튼을 클릭해야 합니다.

사용자 역할 추가

사용자에게는 웹 페이지 보기 또는 명령 실행과 같은 수행할 각 작업에 해당하는 명령 권한이 명시적으로 부여되어야 합니다. 명령 권한 집합은 명령 권한 역할을 생성합니다. 그런 다음 사용자 그룹에 역할을 적용하여 지정된 사용자 그룹에 대한 명령 권한을 설정할 수 있습니다. 예를 들어, 네트워크 운영 실무자에게는 장치 레코드에 액세스하고 변경 사항을 보는 권한은 있지만 장치에 대한 변경을 스크립팅하거나 장치를 제거하는 권한은 없습니다.

참고: 보기 권한을 사용하지 않으면 새 사용자가 모든 파티션 보기 그룹에 넣어 모든 장치에 대한 보기 권한이 부여됩니다. 반면 보기 권한을 생성하면 새 사용자에게는 암시적으로 어떠한 보기 권한도 부여되지 않습니다.

새 사용자 역할을 추가하려면

1. 관리 아래의 메뉴 모음에서 사용자 역할 및 권한 옵션을 클릭합니다. 사용자 역할 및 권한 페이지가 열립니다.
2. 페이지 맨 위에 있는 새 사용자 역할 링크를 클릭합니다. 새 사용자 역할 페이지가 열립니다. [337페이지의 "새 사용자 역할 페이지 필드"](#)를 참조하십시오.

사용자 역할 및 권한 페이지 필드

필드	설명/작업
새 사용자 역할 링크	사용자 역할을 선택할 수 있는 새 사용자 역할 페이지를 엽니다. 자세한 내용은 337페이지의 "새 사용자 역할 페이지 필드" 를 참조하십시오.
사용자 링크	현재 사용자를 보고 새 사용자를 추가할 수 있는 모든 사용자 페이지를 엽니다. 자세한 내용은 320페이지의 "모든 사용자 페이지 필드" 를 참조하십시오.
사용자 그룹 링크	현재 사용자 그룹을 보고 새 사용자 그룹을 추가할 수 있는 사용자 그룹 페이지를 엽니다. 자세한 내용은 330페이지의 "사용자 그룹 페이지 필드" 를 참조하십시오.
시스템 기본 역할	
역할 이름	역할 이름을 표시합니다. 역할에 대한 명령 권한 목록을 포함하여, 역할을 선택하여 역할에 대한 정보를 볼 수 있습니다.

필드	설명/작업
역할 유형	명령 권한, 장치 수정 권한, 스크립트 권한 및 파티션 보기 권한을 비롯한 역할 유형을 표시합니다.
설명	역할에 대한 설명을 표시합니다.
작업	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 편집 — 사용자 역할 편집 페이지가 열립니다. 자세한 내용은 335페이지의 "사용자 역할 추가"를 참조하십시오. 기본 역할은 편집할 수 없습니다. • 복사본 생성 — 새 사용자 역할을 추가할 수 있는 사용자 역할 편집 페이지를 엽니다. 자세한 내용은 337페이지의 "새 사용자 역할 페이지 필드"를 참조하십시오. • 삭제 — 역할을 삭제할 수 있습니다(관리 권한만). 기본 역할은 삭제할 수 없습니다.
사용자 정의 역할	
역할 이름	역할 이름을 표시합니다. 역할에 대한 명령 권한 목록을 포함하여, 역할을 선택하여 역할에 대한 정보를 볼 수 있습니다.
역할 유형	명령 권한, 장치 수정 권한, 파티션 보기 권한 및 스크립트 권한과 같은 역할 유형을 표시합니다.
설명	역할에 대한 설명을 표시합니다.
작업	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 편집 — 사용자 역할 편집 페이지가 열립니다. 자세한 내용은 337페이지의 "새 사용자 역할 페이지 필드"를 참조하십시오. • 복사본 생성 — 새 사용자 역할을 추가할 수 있는 사용자 역할 편집 페이지를 엽니다. 자세한 내용은 337페이지의 "새 사용자 역할 페이지 필드"를 참조하십시오. 사용자 정의 역할은 복사할 수 없습니다. • 삭제 — 역할을 삭제할 수 있습니다(관리 권한만).

새 사용자 역할 페이지 필드

필드	설명/작업
새 사용자 역할	<p>드롭다운 메뉴에서 사용자 역할을 선택합니다. 사용자의 선택에 따라 화면 표시가 수정됩니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 명령 권한 — 사용자 역할의 이름과 설명을 입력합니다. 각 명령에 대해 이 역할에 권한을 허가 또는 거부하는 버튼을 클릭합니다. 전체 명령 권한 목록을 보려면 917페이지의 "부록 B: 명령 권한"을 참조하십시오. 모두 부어를 클릭하여 모든 명령에 권한을 부여할 수 있습니다. 이것은 관리 사용자에게, 그리고 몇 개의 명령에 대한 권한만 거부하려고 할 때 유용합니다. 모든 명령에 대한 권한을 거부하려면 모두 거부를 클릭합니다. • 장치 수정 권한 — 사용자 역할의 이름과 설명을 입력합니다. 장치 선택기를 사용하여 장치 그룹을 선택합니다. 장치 선택기를 사용하는 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. 이 역할에는 선택한 장치 그룹의 구성원인 모든 장치에 대한 장치 수정 권한이 있습니다. • 스크립트 권한 — 사용자 역할의 이름과 설명을 입력합니다. 목록에서 스크립트를 선택합니다. 이 역할에는 선택한 모든 스크립트에 대한 스크립트 권한이 있습니다. • 파티션 보기 권한 — 사용자 역할의 이름과 설명을 입력합니다. 목록에서 파티션을 선택합니다. 이 역할은 선택한 파티션의 장치 및/또는 사용자 그룹의 구성원인 모든 장치 및/또는 사용자에 대한 파티션 보기 권한을 가집니다. 파티션 보기 권한은 개별 사용자가 아닌 사용자 그룹에 할당됩니다. 여러 사용자 그룹에 속하는 사용자는 여러 개의 파티션 보기 권한을 얻을 수 있습니다. 장치 세분화에 대한 내용은 191페이지의 "장치 및 사용자 세분화"를 참조하십시오.

완료되면 저장 버튼을 클릭해야 합니다.

사용자 그룹은 자동으로 사용자 역할에 할당되지 않습니다. 사용자 그룹을 사용자 역할에 할당하려면

1. 관리 아래의 메뉴 모음에서 사용자 그룹을 클릭합니다. 사용자 그룹 페이지가 열립니다.
2. 새 역할에 추가할 그룹에 대한 작업 열에서 편집 옵션을 클릭합니다. 사용자 그룹 편집 페이지가 열립니다. 자세한 내용은 [331페이지의 "새 사용자 그룹 페이지 필드"](#)를 참조하십시오.

사용자 설정 편집

NA 홈 페이지의 내 작업 공간 영역에는 다음 옵션이 들어 있습니다.

- 현재 장치 — 해당되는 경우 현재 장치를 표시합니다.
- 현재 장치 그룹 — 현재 장치 그룹을 표시합니다. 인벤토리가 기본입니다.
- 내 즐겨찾기 — 즐겨찾는 장치, URL 및/또는 NA 페이지 목록을 표시합니다. 대부분의 NA 페이지 상단에 있는 즐겨찾기에 추가 링크를 클릭하여 이 목록에 항목을 추가할 수 있습니다.
- 빠른 시작 — [345페이지의 "빠른 시작이란?"](#)을 참조하십시오.
- 내 설정 — 자세한 내용은 [338페이지의 "내 설정"](#)을 참조하십시오.

내 설정

내 설정 아래 선택할 수 있는 옵션은 다음과 같습니다.

- 내 프로필 - [339페이지의 "내 프로필 페이지 필드"](#)를 참조하십시오.
- 내 작업 공간 - [341페이지의 "내 작업 공간 페이지 필드"](#)를 참조하십시오.
- 내 기본 설정 - [341페이지의 "내 기본 설정 페이지 필드"](#)를 참조하십시오.
- 내 권한 - [343페이지의 "내 권한 페이지 필드"](#)를 참조하십시오.
- 암호 변경 - [344페이지의 "암호 변경 페이지 필드"](#)를 참조하십시오.
- 빠른 시작 - [345페이지의 "빠른 시작이란?"](#)을 참조하십시오.

내 프로필 페이지 필드

내 프로필 페이지에서 사용자 이름, 암호 및 전자 메일 주소와 같은 사용자 설정을 변경할 수 있습니다. 관리자 그룹의 사용자만 암호 옵션을 볼 수 있습니다. 자세한 내용은 [326페이지의 "사용자 암호 구성"](#)을 참조하십시오.

NA 홈 페이지의 내 설정 아래 내 프로필을 클릭합니다. 내 프로필 페이지가 열립니다. 완료했으면 저장 버튼을 클릭합니다.

필드	설명/작업
사용자 정보	
사용자 이름	새 NA 사용자 이름을 입력합니다.
암호	새 NA 암호를 입력합니다.
암호 확인	확인을 위해 새 NA 암호를 다시 입력합니다.
암호 옵션	다음 옵션 중 하나 이상을 선택합니다. <ul style="list-style-type: none"> •사용자는 다음 로그인 시에 암호를 변경해야 함 •사용자는 암호를 변경할 수 없음 •암호 만료 안 함 •계정이 잠김 암호 옵션 설정에 대한 자세한 내용은 326페이지의 "사용자 암호 구성" 을 참조하십시오.
외부 리소스 자격 증명	외부 리소스 자격 증명 변경 링크를 클릭하면 암호 변경 페이지가 열립니다. 344페이지의 "암호 변경 페이지 필드" 를 참조하십시오.
이름	새 이름을 입력합니다.
성	새 성을 입력합니다.
전자 메일 주소	새 전자 메일 주소를 입력합니다.
사용자가 속한 그룹	사용자가 속한 그룹을 표시합니다. 그룹을 클릭하면 그룹에 속하는 현재 사용자 목록이 열립니다.
외부 인증 장애조치 확인란	외부 인증이 실패할 때 인증이 자동으로 로컬 인증으로 장애 조치할 경우 선택합니다.
주석	사용자 계정에 대한 설명을 입력합니다.

필드	설명/작업
AAA	
AAA 사용자 이름	새 AAA(TACACS+ 또는 RADIUS) 사용자 이름을 입력합니다.
AAA 암호	새 AAA 암호를 입력합니다.
AAA 암호 확인	확인을 위해 새 AAA 암호를 다시 입력합니다.
프록시 인터페이스에 AAA 로그인 사용 확인란	확인란을 선택하면 각 NA 텔넷 및 SSH 세션에서 AAA 로그인 정보가 사용됩니다.
SecurID	
소프트웨어 토큰 라이선스 관리 링크	NA를 SecurID 자격 증명을 사용하여 장치에 로그인하도록 구성할 수 있습니다. 이 링크를 클릭하면 SecurID 토큰 페이지가 열립니다. 자세한 내용은 793페이지의 "SecurID 소프트웨어 토큰 추가" 를 참조하십시오. (참고: 소프트웨어 토큰이 플랫폼에서 지원되지 않거나 SecurID가 적절하게 구성되지 않으면 이 링크는 표시되지 않습니다.)

내 작업 공간 페이지 필드

작업 공간을 편집하려면 NA 홈 페이지의 내 설정 아래 내 작업 공간을 클릭합니다. 내 작업 공간 페이지가 열립니다.

필드	설명/작업
즐거찾기 링크	즐거찾기 링크를 표시합니다. 링크는 장치, NA 페이지 또는 기타 URL일 수 있습니다. 링크를 제거하려면 제거할 링크 옆에 있는 빨간색 삭제 아이콘을 클릭합니다. 또한 새 이름을 입력한 다음 이름 바꾸기 버튼을 클릭하여 링크의 이름을 바꿀 수 있고, 위쪽 및 아래쪽 화살표를 사용하여 목록에서 즐거찾기 링크를 위 또는 아래로 이동할 수 있습니다.
사용자 지정된 즐거찾기 링크 추가	링크 이름 필드에 링크 이름을 입력합니다. 최대 문자 수는 25자입니다. 링크 URL 주소를 입력할 수도 있습니다. 완료했으면 즐거찾기 링크 추가 버튼을 클릭합니다.
작업 공간 설정	드롭다운 메뉴에서 링크를 선택하여 링크를 기본 홈 페이지로 사용할 수 있습니다. 내 즐거찾기 목록에서 허용되는 링크 수를 변경하려면 드롭다운 메뉴에서 숫자를 선택하십시오. 기본값은 10입니다. 참고: 바로 가기를 추가할 때까지 이 옵션은 사용할 수 없습니다.

내 기본 설정 페이지 필드

현재 NA 홈 페이지 환경 설정을 편집하려면 NA 홈 페이지의 내 설정 아래에서 내 기본 설정을 클릭합니다. 내 기본 설정 페이지가 열립니다. 이 페이지에서 홈 페이지를 사용자 지정하고 장치 소프트웨어 이미지 권장 사항 페이지에 표시되는 Cisco 소프트웨어 이미지를 지정할 수 있습니다. 자세한 내용은 [293페이지의 "장치 소프트웨어 이미지 권장 사항 페이지 필드"](#)를 참조하십시오.

필드	설명/작업
홈 페이지에 내 작업 및 승인 요청(워크플로가 활성화되어 있을 때) 표시	예(기본값) 또는 아니요를 선택합니다.
홈 페이지에 최근 변경 사항 표시	예(기본값) 또는 아니요를 선택합니다.
홈 페이지에 최근 이벤트 표시	예(기본값) 또는 아니요를 선택합니다.

필드	설명/작업
홈 페이지에 시스템 보고서 표시	예 또는 아니오(기본값)를 선택합니다.
홈 페이지에 내 즐겨찾기 보고서 표시	예(기본값) 또는 아니요를 선택합니다.
홈 페이지에 내 장치 그룹 표시	예(기본값) 또는 아니요를 선택합니다.
소프트웨어 이미지 권장 사항 설정	
현재 버전보다 상위 버전인 이미지만 포함	예 또는 아니오(기본값)를 선택합니다.
동일한 하위 집합 기능이 있는 이미지만 포함	예 또는 아니오(기본값)를 선택합니다.
일반 배포 이미지만 포함	예 또는 아니오(기본값)를 선택합니다.
최신 유지 보수 릴리스 이미지만 포함	예 또는 아니오(기본값)를 선택합니다.
이미지 권장을 위해 Cisco.com 이미지 포함	예(기본값) 또는 아니요를 선택합니다.

완료했으면 저장 버튼을 클릭합니다.

내 권한 페이지 필드

보기 권한 페이지는 사용자가 속하는 그룹 때문에 가지는 권한을 표시합니다. 할당된 역할도 있습니다. 자세한 내용은 [337페이지의 "새 사용자 역할 페이지 필드"](#)를 참조하십시오.

참고: 보기 권한을 사용하지 않으면 새 사용자가 모든 파티션 보기 그룹에 넣어 모든 장치에 대한 보기 권한이 부여됩니다. 반면 보기 권한을 생성하면 새 사용자에게는 암시적으로 어떠한 보기 권한도 부여되지 않습니다.

현재 권한을 보려면 NA 홈 페이지의 내 설정 아래에서 내 권한을 클릭합니다. 내 권한 페이지가 열립니다.

필드	설명/작업
사용자 그룹 및 역할	사용자가 속하는 모든 그룹과 각 그룹에 할당된 역할을 표시합니다. 자세한 내용은 335페이지의 "사용자 역할 추가" 를 참조하십시오.
명령 권한 부여됨	명령에 따라 가지는 권한을 표시합니다. 자세한 내용은 917페이지의 "명령 권한 허가" 를 참조하십시오.
장치 수정 권한 부여됨	장치를 수정하기 위해 가지는 권한을 표시합니다.
스크립트 권한 부여됨	스크립트를 실행 및 수정하기 위해 가지는 권한을 표시합니다.
파티션 보기 권한 부여됨	사용자 및/또는 장치를 보기 위해 가지는 권한을 표시합니다. 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.

암호 변경 페이지 필드

로컬 인증 암호 및/또는 외부 리소스 자격 증명을 변경하려면 NA 홈 페이지의 내 설정 아래에서 암호 변경을 클릭합니다. 암호 변경 페이지가 열립니다.

필드	설명/작업
로컬 인증 암호	
새 암호	새 암호를 입력합니다.
새 암호 확인	확인을 위해 새 암호를 다시 입력하고 제출 버튼을 클릭합니다.
외부 리소스 자격 증명/새 외부 리소스 자격 증명 추가	
자격 증명 유형	드롭다운 메뉴에서 자격 증명 유형을 선택합니다. 옵션은 다음과 같습니다. <ul style="list-style-type: none"> •Cisco.com 자격 증명 — 이 자격 증명은 소프트웨어 이미지 권장 사항으로 Cisco.com에서 사용하고 소프트웨어 이미지를 Cisco 장치에 다운로드합니다. Cisco.com은 Cisco의 네트워크 간 제품에 대한 시스템 소프트웨어 및 드라이버의 릴리스 버전을 포함합니다. 자세한 내용은 456페이지의 "Cisco.com에서 이미지 다운로드 작업 페이지"를 참조하십시오. •프록시 자격 증명 — 사용자 이름과 암호가 필요한 프록시를 통해 Cisco.com에 액세스할 때 이 자격 증명이 사용됩니다.
사용자 이름	사용자 이름을 입력합니다. 프록시는 일반적이므로, Cisco.com으로 직접 결합되지 않습니다. 소프트웨어 이미지 관리 수집기 HTTP 프록시 서버 구성에 대한 자세한 내용은 68페이지의 "서버 페이지 필드" 를 참조하십시오.
암호	암호를 입력합니다.
암호 확인	확인을 위해 암호를 다시 입력하고 제출 버튼을 클릭합니다.

기존 외부 리소스 자격 증명을 수정하거나 삭제하려면 수정 및 삭제 버튼을 사용하십시오.

빠른 시작이란?

NA의 이전 버전에서는 스냅샷 작성, 정책 준수 확인 또는 보고서 생성 등의 작업을 실행할 때 현재 페이지에서 다른 위치로 이동해야 했습니다.

작업을 사용자 지정하고 현재 페이지에서 다른 위치로 이동할 필요 없이 미리 작성된 데이터로 작업을 빨리 시작할 수 있습니다. 예를 들어 현재 장치에 대한 장치 세부사항 페이지를 보고 있으며 스냅샷 작성 등 빠른 시작 작업을 구성한 경우 내 작업 공간 영역에서 빠른 시작 아래에 표시되는 빠른 시작 작업을 클릭하기만 하면 해당 작업이 자동으로 실행됩니다.

참고: 관리 권한이 있는 사용자만 빠른 시작을 생성, 실행 및 삭제할 수 있습니다.

빠른 시작을 구성하는 방법

빠른 시작에는 작업 템플릿이 사용됩니다. 작업 템플릿을 사용하면 작업 정의를 저장할 수 있으므로 처음부터 다시 시작하지 않더라도 새로운 작업과 기존 작업을 빨리 구성 및 실행할 수 있습니다.

작업을 빠른 시작에 추가하려면

1. 작업 아래의 기본 메뉴 모음에서 작업 템플릿을 클릭합니다. 작업 템플릿 페이지가 열립니다. 작업 템플릿을 검색할 수도 있습니다. 자세한 내용은 [622페이지의 "작업 검색"](#)을 참조하십시오.
2. 작업 열에서 빠른 시작에 추가 링크를 클릭합니다. 빠른 시작 링크가 내 작업 공간 영역 아래에 있는 빠른 시작 섹션에 자동으로 표시됩니다. 빠른 시작 링크는 현재 작업 템플릿의 이름을 가정합니다. 링크의 이름을 변경하려면 표시된 팝업 상자를 사용하십시오. 중복 이름이 있을 때만 팝업 상자가 표시됩니다.

작업 템플릿에 대한 자세한 내용은 [361페이지의 "작업 템플릿"](#)을 참조하십시오.

작업 템플릿을 아직 정의하지 않았으면 다음을 수행합니다.

1. 작업 아래에 있는 기본 메뉴 모음에서 새 작업을 선택하고 스냅샷 작성 등의 작업을 클릭합니다. 스냅샷 작성 페이지가 열립니다.
2. 새로운 작업 페이지 또는 편집 작업 페이지에서 저장 옵션 필드의 작업 템플릿으로 저장 옵션을 클릭합니다. 작업을 저장하면 작업이 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다.

빠른 시작 관리

빠른 시작을 관리하려면 NA 홈 페이지에서 내 작업 공간 영역의 내 설정 아래에 있는 빠른 시작 링크를 클릭합니다. 빠른 시작 페이지가 열립니다. 이 페이지에서 다음 작업을 수행할 수 있습니다.

- 화살표 버튼이나 끌어서 놓기 기능을 사용하여 표시된 빠른 시작 순서를 조정
- 빠른 시작 삭제
- 빠른 시작 이름 바꾸기
- 내 작업 영역 아래에서 NA 홈 페이지의 빠른 시작 영역 크기를 확인

일반 표시는 [347페이지의 "샘플 빠른 시작 표시"](#)를 참조하십시오.

빠른 시작 사용

빠른 시작을 정의한 후에는 빠른 시작 목록이 NA 홈 페이지의 내 작업 공간 영역에 있는 내 설정 섹션 아래에 표시됩니다.

빠른 시작 링크는 작업 중인 특정 페이지 및 콘텐츠에 따라 달라집니다. 예를 들어 인벤토리 페이지에서는 세부사항을 표시할 장치를 선택합니다. 해당 장치에 대한 장치 세부사항 페이지가 열립니다. 스냅샷 작성 빠른 시작을 구성한 경우 NA 홈 페이지의 내 작업 공간 영역에 있는 내 설정 아래에서 빠른 시작 섹션의 스냅샷 작성 링크를 클릭하면 작업이 자동으로 실행됩니다. 작업을 성공적으로 저장했습니다와 같은 정보 메시지가 표시됩니다.

빠른 시작용 작업을 구성할 때 빠른 시작이 항상 현재 장치나 장치 그룹(또는 둘 다 없는 경우 인벤토리)에 대해 실행됨에 유의하십시오. 작업 템플릿을 구성하는 경우 작업에 대한 장치 및/또는 장치 그룹 정보를 제공합니다. 이 정보는 실행 중인 빠른 시작에 대한 현재 장치 또는 장치 그룹 정보로 대체됩니다.

예를 들어 장치 재부팅 작업 빠른 시작을 구성하고 나서 현재 보고 있는 장치에 대해 해당 빠른 시작을 실행한 경우 원본 작업 템플릿에 제공된 장치 및/또는 장치 그룹 정보와 상관 없이 장치가 자동으로 재부팅됩니다. 재부팅하기 전에 메시지가 표시되지 않습니다.

샘플 빠른 시작 표시

다음 표에서는 샘플 빠른 시작 페이지의 필드를 설명합니다. 빠른 시작 구성 방법에 대한 자세한 내용은 [345페이지의 "빠른 시작이란?"](#)을 참조하십시오.

필드	설명/작업
작업 템플릿 목록 페이지 링크	이 링크를 클릭하면 작업 템플릿 페이지가 열립니다. 자세한 내용은 361페이지의 "작업 템플릿" 을 참조하십시오.
빠른 시작 작업 -- 장치	
작업 이름(예: 스냅샷 작성)	위쪽 및 아래쪽 화살표를 사용하면 나열된 빠른 시작 장치 작업을 정렬할 수 있습니다. 빨간색 X 아이콘을 사용하여 빠른 시작 장치 작업을 삭제할 수 있습니다. 빠른 시작 장치 작업 이름을 변경하려면 새 이름을 입력하고 이름 바꾸기 버튼을 클릭합니다. 작업 이름은 25자를 초과할 수 없습니다.
빠른 시작 작업 -- 정책	
작업 이름(예: 정책 확인)	위쪽 및 아래쪽 화살표를 사용하면 나열된 빠른 시작 정책 작업을 정렬할 수 있습니다. 빨간색 X 아이콘을 사용하여 빠른 시작 장치 작업을 삭제할 수 있습니다.

필드	설명/작업
	빠른 시작 정책 작업 이름을 변경하려면 새 이름을 입력하고 이름 바꾸기 버튼을 클릭합니다. 작업 이름은 25자를 초과할 수 없습니다.
빠른 시작 작업 -- 보고서	
작업 이름(예: 요약 보고서 생성)	위쪽 및 아래쪽 화살표를 사용하면 나열된 빠른 시작 보고서 작업을 정렬할 수 있습니다.
	빨간색 X 아이콘을 사용하여 빠른 시작 보고서 작업을 삭제할 수 있습니다.
	빠른 시작 보고서 작업 이름을 변경하려면 새 이름을 입력하고 이름 바꾸기 버튼을 클릭합니다. 작업 이름은 25자를 초과할 수 없습니다.
빠른 시작 설정	
빠른 시작에 허용되는 최대 링크 개수	풀다운 메뉴에서 값을 선택합니다. 기본값은 10입니다. 이 값은 내 작업 영역 아래에서 NA 홈 페이지의 빠른 시작 영역 크기를 결정합니다. NA 홈 페이지에 대한 자세한 내용은 338페이지의 "사용자 설정 편집" 을 참조하십시오.

NA 홈 페이지 사용자 지정

NA에 로그인할 때마다 NA 홈 페이지가 열립니다. 또한 각 페이지의 왼쪽 위 모서리에 있는 홈 링크를 클릭하여 NA 홈 페이지로 돌아갈 수 있습니다.

NA 홈 페이지에는 두 개 프레임이 포함되어 있습니다. 왼쪽 프레임에는 다음 항목이 포함됩니다.

- 검색 — 검색 옵션을 사용하면 호스트 이름이나 IP 주소별로 장치를 찾고 텔넷이나 SSH를 통해 이러한 장치에 연결할 수 있습니다. 자세한 내용은 [354페이지의 "검색/연결 기능"](#)을 참조하십시오.
- 내 작업 공간 — 내 작업 공간 영역에는 다음 섹션이 포함되어 있습니다.
 - 현재 장치/현재 장치 그룹(기본값은 인벤토리)
 - 내 즐겨찾기
 - 빠른 시작(해당되는 경우)
 - 내 설정

내 작업 공간 영역의 옵션 구성에 대한 자세한 내용은 [338페이지의 "사용자 설정 편집"](#)을 참조하십시오.

다음 항목을 포함하도록 오른쪽 프레임을 사용자 지정할 수 있습니다.

- 워크플로 승인
- 작업 목록
- 최근 구성 변경(장치에서 변경된 설정 및 변경 시기)
- 최근 시스템 이벤트(예: 장치 액세스 실패)
- 선택한 장치 그룹
- 선택한 즐겨찾기 보고서
- 선택한 시스템 보고서

자세한 내용은 [350페이지의 "내 홈 페이지 탭 필드"](#) 및 [353페이지의 "통계 대시보드 탭 필드"](#)를 참조하십시오.

내 홈 페이지 탭 필드

필드	설명/작업
워크플로 승인 (해당되는 경우)	
내 승인을 기다리는 작업 링크	<p>다음에 포함하여 사용자의 승인을 기다리는 작업을 표시합니다.</p> <ul style="list-style-type: none"> •작업 이름 — 작업 이름을 표시합니다. 작업 이름을 클릭하면 작업을 승인할 수 있는 작업 정보 페이지가 열립니다. 작업 정보 페이지에 대한 자세한 내용은 866페이지의 "작업 정보 페이지 필드"를 참조하십시오. •승인 기준 — 작업을 승인해야 하는 날짜 및 시간을 표시합니다. 작업 승인에 대한 자세한 내용은 863페이지의 "승인 요청"을 참조하십시오. •승인 — 승인 상태를 표시합니다. •예약 날짜 — 작업이 예약된 시기를 표시합니다. •상태 — 현재 상태를 표시합니다. <p>모두 보기 링크를 클릭하여 승인 요청 목록을 볼 수 있는 승인 요청 페이지를 여십시오. 승인 요청 페이지에 대한 자세한 내용은 863페이지의 "승인 요청"을 참조하십시오.</p>
내 작업	
작업 이름	작업 목록을 표시합니다. 자세한 내용은 358페이지의 "작업이란?" 을 참조하십시오. NA를 처음 구성할 때 스냅샷 작성, 요약 보고서 생성, 진단 실행 및 데이터 정리를 포함하여 기본 작업 목록이 표시됩니다.
예약 날짜	작업이 예약된 날짜와 시간을 표시합니다.
상태	현재 작업 상태를 표시합니다. 장치 상태 목록을 보려면 503페이지의 "작업 정보 페이지 필드" 를 참조하십시오.
모두 보기 링크	모든 작업을 볼 수 있는 내 작업 페이지를 엽니다. 자세한 내용은 358페이지의 "작업이란?" 을 참조하십시오.

필드	설명/작업
최근 변경 사항	
시간 범위	기본 시간 범위는 과거 24시간입니다. 다음 시간 범위를 선택할 수 있습니다. <ul style="list-style-type: none"> •과거 1, 2, 4, 8, 12, 24 및 48시간 •과거 1 및 2주 •과거 1개월 •모든 구성
날짜	구성 변경의 날짜 및 시간을 표시합니다.
장치	변경된 장치의 호스트 이름 또는 IP 주소를 표시합니다. 장치 링크를 클릭하면 장치 세부사항 페이지가 열립니다.
변경한 사람	구성, 장치 또는 작업을 변경한 사람의 로그인 이름이 표시됩니다. N/A는 해당하는 사람이 없음을 의미합니다.
주석	구성에 대한 주석이 표시됩니다.
작업	선택할 수 있는 작업은 다음과 같습니다. <ul style="list-style-type: none"> •이전과 비교 — 선택한 구성과 다음/이전 구성을 나란히 볼 수 있는 장치 구성 비교 페이지를 엽니다. 차이점은 쉽게 확인할 수 있게 서로 다른 색상으로 강조 표시됩니다. •구성 보기 — 전체 구성을 보고, 장치 실행 구성에 이 버전의 구성을 배포하고, 구성을 편집하고, 진단을 검색하고, 구성과 이전 구성을 비교할 수 있는 장치 구성 세부사항 페이지를 엽니다.
모두 보기 링크	모든 구성 변경 사항을 보고 변경 사항을 볼 시간 범위를 조정할 수 있는 구성 변경 페이지를 엽니다. 자세한 내용은 223페이지의 "장치 구성 변경 보기" 를 참조하십시오.

필드	설명/작업
최근 이벤트	
시간 범위	기본 시간 범위는 과거 24시간입니다. 다음 시간 범위를 선택할 수 있습니다. <ul style="list-style-type: none"> •과거 1, 2, 4, 8, 12, 24 및 48시간 •과거 1 및 2주 •과거 1개월 •모든 구성
이벤트 요약	이벤트 유형을 표시합니다. 링크를 클릭하면 이 유형의 전체 이벤트 목록이 나타납니다. 자세한 내용은 680페이지의 "이벤트 통합 보기(단일 보기)" 를 참조하십시오.
개수	이 유형의 이벤트 수를 표시합니다.
이벤트 목록 페이지 링크	더 긴 이벤트 목록을 보고 이벤트를 볼 시간 범위를 조정할 수 있는 시스템 및 네트워크 이벤트 페이지를 엽니다. 자세한 내용은 680페이지의 "이벤트 통합 보기(단일 보기)" 를 참조하십시오.
내 장치 그룹(해당되는 경우)	
장치 그룹 링크	현재 장치 그룹을 볼 수 있는 장치 그룹 페이지를 엽니다.
내 즐겨찾기 보고서(해당되는 경우)	
모든 즐겨찾기 보고서 링크	시스템 보고서뿐만 아니라, 사용자 지정 검색에서 생성한 보고서도 볼 수 있는 사용자 및 시스템 보고서 페이지를 엽니다.

통계 대시보드 탭 필드

통계 대시보드 탭은 다음 사항에 대한 정보를 제공합니다.

- 공급업체 상위 5개
- OS 버전 상위 5개
- 활성 사용자 상위 5명
- 일별 평균 변경 수
- 변경 빈도
- 가장 많이 액세스한 장치 상위 10개
- 소프트웨어 수준
- OS 인벤토리
- 구성 정책 준수

자세한 내용은 [782페이지의 "요약 보고서"](#)를 참조하십시오.

검색/연결 기능

NA 홈 페이지(및 모든 페이지)에 있는 각 페이지의 왼쪽에는 호스트 이름 및 IP 주소로 장치를 찾고 텔넷 또는 SSH를 통해 이들 장치에 연결할 수 있는 검색 탭이 있습니다. 검색 기능은 와일드카드를 승인하므로, 관련 장치 그룹을 빨리 찾거나 대상 장치를 찾을 때까지 검색 범위를 좁힐 수 있습니다. 장치 검색 페이지 필드에 대한 자세한 내용은 [583 페이지의 "장치 검색"](#)을 참조하십시오.

또한 검색 대상 드롭다운 메뉴를 사용하여 특정 대상을 검색할 수 있습니다.

- 장치
- 인터페이스
- 모듈
- 정책
- 준수
- 구성
- 진단
- 작업
- 세션
- 이벤트
- 사용자
- 단일 검색
- ACL
- MAC 주소
- IP 주소
- VLAN
- 장치 템플릿
- 고급 검색


7장: 작업 예약

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
작업이란?	358페이지의 "작업이란?"
작업 예약	359페이지의 "작업 예약"
작업 템플릿	361페이지의 "작업 템플릿"
Syslog 작업 구성	366페이지의 "Syslog 구성 작업 페이지 필드"
암호 배포 작업	370페이지의 "암호 배포 작업 페이지 필드"
드라이버 검색 작업	375페이지의 "드라이버 검색 작업 페이지 필드"
장치 재부팅 작업	379페이지의 "장치 재부팅 작업 페이지 필드"
ICMP 테스트 실행 작업	383페이지의 "ICMP 테스트 실행 작업 페이지 필드"
명령 스크립트 실행 작업	389페이지의 "명령 스크립트 실행 작업 페이지 필드"
진단 실행 작업	397페이지의 "진단 실행 작업 페이지 필드"
스냅샷 작성 작업	403페이지의 "스냅샷 작성 작업 페이지 필드"
시작 및 실행 동기화 작업	408페이지의 "시작 및 실행 동기화 작업 페이지 필드"
장치 소프트웨어 업데이트 작업	413페이지의 "장치 소프트웨어 업데이트 작업 페이지 필드"
가져오기 작업	421페이지의 "가져오기 작업 페이지 필드"
네트워크 장치 감지 작업	426페이지의 "네트워크 장치 감지 작업 페이지 필드"
중복 방지 작업	433페이지의 "중복 방지 작업 페이지 필드"
OS 분석	436페이지의 "OS 분석 작업 페이지 필드"
포트 스캔	440페이지의 "포트 스캔 페이지 필드"
템플릿에서 장치 프로비전	444페이지의 "장치 프로비전 작업 페이지 필드"
장치 컨텍스트 추가	448페이지의 "장치 컨텍스트 추가 작업 페이지 필드"

항목	참조
VLAN	452페이지의 "VLAN 작업 페이지 필드"
Cisco.com에서 이미지 다운로드 작업	456페이지의 "Cisco.com에서 이미지 다운로드 작업 페이지"
장치 소프트웨어 백업 작업	459페이지의 "장치 소프트웨어 백업 작업 페이지 필드"
정책 준수 확인 작업	462페이지의 "정책 준수 확인 작업 페이지 필드"
요약 보고서 생성 작업	466페이지의 "요약 보고서 생성 작업 페이지 필드"
전자 메일 보고서 작업	469페이지의 "전자 메일 보고서 작업 페이지 필드"
원격 에이전트 배포 작업	472페이지의 "원격 에이전트 배포 페이지 필드"
FQDN 확인 작업	475페이지의 "FQDN 확인 작업 페이지 필드"
데이터 정리 작업	478페이지의 "데이터 정리 작업 페이지 필드"
외부 응용 프로그램 실행 작업	481페이지의 "외부 응용 프로그램 실행 작업 페이지 필드"
멀티 태스킹 프로젝트 예약	485페이지의 "멀티 태스킹 프로젝트 예약"
내 작업 보기	491페이지의 "내 작업 페이지 필드"
예정된 작업 보기	495페이지의 "예정된 작업 보기"
실행 중인 작업 보기	498페이지의 "실행 중인 작업 보기"
최근 작업 보기	500페이지의 "최근 작업 보기"
작업 로드 보기	506페이지의 "작업 로드 보기"

작업 페이지로 이동

 HP Network Automation 로그아웃																																						
장치 ▾	작업 ▾	정책 ▾	보고서 ▾	관리 ▾	도움말 ▾																																	
↓																																						
<table border="1" style="width: 100%;"> <tr><td>내 작업</td></tr> <tr><td>승인 요청</td></tr> <tr><td>새 멀티 태스킹 프로젝트</td></tr> <tr><td>작업 로드</td></tr> <tr><td>활동 캘린더</td></tr> <tr><td>작업 템플릿</td></tr> <tr><td>예정된 작업</td></tr> <tr><td>실행 중인 작업</td></tr> <tr><td>최근 작업</td></tr> <tr><td>새 작업 ▶</td></tr> <tr><td>Syslog 구성</td></tr> <tr><td>암호 배포</td></tr> <tr><td>드라이버 검색</td></tr> <tr><td>장치 재부팅</td></tr> <tr><td>ICMP 테스트 실행</td></tr> <tr><td>명령 스크립트 실행</td></tr> <tr><td>진단 실행</td></tr> <tr><td>스냅샷 작성</td></tr> <tr><td>시작 및 실행 동기화</td></tr> <tr><td>장치 소프트웨어 업데이트</td></tr> <tr><td>가져오기</td></tr> <tr><td>네트워크 장치 감지</td></tr> <tr><td>중복 방지</td></tr> <tr><td>OS 분석</td></tr> <tr><td>포트 스캔</td></tr> <tr><td>템플릿에서 장치 프로비전</td></tr> <tr><td>정책 준수 확인</td></tr> <tr><td>요약 보고서 생성</td></tr> <tr><td>전자 메일 보고서</td></tr> <tr><td>원격 에이전트 배포</td></tr> <tr><td>FQDN 확인</td></tr> <tr><td>데이터 정리</td></tr> <tr><td>외부 응용 프로그램 실행</td></tr> </table>						내 작업	승인 요청	새 멀티 태스킹 프로젝트	작업 로드	활동 캘린더	작업 템플릿	예정된 작업	실행 중인 작업	최근 작업	새 작업 ▶	Syslog 구성	암호 배포	드라이버 검색	장치 재부팅	ICMP 테스트 실행	명령 스크립트 실행	진단 실행	스냅샷 작성	시작 및 실행 동기화	장치 소프트웨어 업데이트	가져오기	네트워크 장치 감지	중복 방지	OS 분석	포트 스캔	템플릿에서 장치 프로비전	정책 준수 확인	요약 보고서 생성	전자 메일 보고서	원격 에이전트 배포	FQDN 확인	데이터 정리	외부 응용 프로그램 실행
내 작업																																						
승인 요청																																						
새 멀티 태스킹 프로젝트																																						
작업 로드																																						
활동 캘린더																																						
작업 템플릿																																						
예정된 작업																																						
실행 중인 작업																																						
최근 작업																																						
새 작업 ▶																																						
Syslog 구성																																						
암호 배포																																						
드라이버 검색																																						
장치 재부팅																																						
ICMP 테스트 실행																																						
명령 스크립트 실행																																						
진단 실행																																						
스냅샷 작성																																						
시작 및 실행 동기화																																						
장치 소프트웨어 업데이트																																						
가져오기																																						
네트워크 장치 감지																																						
중복 방지																																						
OS 분석																																						
포트 스캔																																						
템플릿에서 장치 프로비전																																						
정책 준수 확인																																						
요약 보고서 생성																																						
전자 메일 보고서																																						
원격 에이전트 배포																																						
FQDN 확인																																						
데이터 정리																																						
외부 응용 프로그램 실행																																						

작업이란?

작업은 HP NA(Network Automation)가 네트워크와 인터랙션하는 기본 메커니즘입니다. 작업은 예약하거나 즉시 실행할 수 있는 특정 동작입니다. 작업 정보 페이지에서는 수행된 작업에 대한 결과를 제공합니다. 이러한 결과에는 장치와 구성 변경을 식별하기 위한 스냅샷, 장치의 정책 준수 여부를 식별하기 위한 소프트웨어 정책 준수 등이 있습니다.

임시 장치 그룹에 대한 작업 실행

임시 장치 그룹을 만들어 장치의 임시 그룹에 대해 한 작업이나 일련의 작업(멀티 태스킹 프로젝트)을 실행할 수 있습니다. 다음 방법 중 하나를 사용하여 임시 장치 그룹을 만들 수 있습니다.

- 장치 목록 페이지에서 확인란을 선택하여 장치를 선택한 다음 작업 드롭다운 메뉴를 사용하여 장치에 대해 실행할 작업을 선택합니다. 자세한 내용은 [241페이지의 "장치 보기"](#)를 참조하십시오.
- 장치의 임시 목록이 포함된 CSV 파일을 가져옵니다. 예를 들어 네트워크에 200개의 장치가 있고 50개의 장치로 구성된 그룹마다 DNS 서버가 한 대 있습니다. 4개의 장치 그룹(각각 50대의 서버가 있음)을 생성하는 대신 장치를 DNS 서버에 매핑하는 CSV 파일을 생성할 수 있습니다. 그런 다음 CSV 파일을 명령 스크립트에 로드하고 DNS 서버를 모두 업데이트하는 작업을 하나 실행할 수 있습니다. 명령 스크립트 실행에 대한 자세한 내용은 [389페이지의 "명령 스크립트 실행 작업 페이지 필드"](#)를 참조하십시오.

멀티 태스킹 프로젝트에 대한 자세한 내용은 [487페이지의 "멀티 태스킹 프로젝트 페이지 필드"](#)를 참조하십시오.

작업 예약

작업을 생성하거나 업데이트할 때 다른 작업보다 더 높은 우선 순위에서 실행되도록 작업의 우선 순위를 설정할 수 있습니다. 작업 우선 순위 수준에는 1 ~ 5가 있습니다. 1은 최고 작업 우선 순위 수준입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다.

모든 작업은 기본 작업 우선 순위 수준 3으로 생성됩니다. 작업을 우선 순위 1로 설정하려면 관리 권한이 있거나 NA 관리자가 이러한 작업을 수행할 수 있는 권한을 부여해야 합니다. 이 권한이 없는 사용자는 작업의 우선 순위 수준을 2 ~ 5로 설정할 수 있습니다. 명령 권한에 대한 자세한 내용은 [337페이지의 "새 사용자 역할 페이지 필드"](#)를 참조하십시오.

현재 실행 중인 상위 작업의 우선 순위를 변경하는 경우 보류 또는 대기 상태에 있는 기존 하위 작업의 우선 순위가 그에 맞게 상위 작업의 우선 순위로 변경됩니다. 하지만 아직 생성되지 않았거나 다른 상태(예: 실행 중 또는 일시 중지)의 하위 작업은 상위 작업을 원래 우선 순위로 유지합니다. 상위 작업이 실행되고 있지 않으며 우선 순위가 변경된 경우 모든 상위 작업의 하위 작업에 새 우선 순위가 부여됩니다.

참고: 작업 관련 API에는 `-taskpriority` 옵션이 제공됩니다. 자세한 내용은 *Network Automation 9.10 API Reference Guide*를 참조하십시오.

용어

다음 용어는 NA 작업 스케줄러를 설명하는 데 사용됩니다.

- **작업** — NA 작업 스케줄러에서 실행할 최소 단위입니다. 작업에는 하나 이상의 하위 작업이 포함될 수 있습니다. 고유의 NA 코어 ID, 작업 ID, 상위 작업 ID(선택 사항), 우선 순위 및 예약 시간이 지정됩니다. NA 코어 ID에 대한 자세한 내용은 *HP Network Automation 9.10 Multimaster Distributed System on Oracle Users Guide* 또는 *HP Network Automation Multimaster Distributed System on SQL Server Users Guide*를 참조하십시오. Multimaster Distributed System 설명서는 Distributed System DVD 및 HP selfsolve 설명서 사이트에서 구할 수 있습니다.
- **작업 대기열** — 동일한 NA 코어 ID, 상위 작업 ID 및 우선 순위가 지정된 작업 그룹입니다. 작업에 상위 작업이 없으면 작업 ID가 상위 작업 ID로 사용됩니다.
- **작업 대기열 그룹** — 동일한 NA ID 및 우선 순위가 지정된 작업 대기열 그룹입니다. 총 5개 작업 대기열 그룹이 있을 수 있습니다.

- **작업 풀** — 동일한 NA 코어 ID가 지정된 총 5개의 작업 대기열 그룹입니다. 작업 풀이 메모리 안에 캐싱되어 작업 예약용으로 사용됩니다. 작업 풀은 데이터베이스에 정의된 작업과 동기화됩니다. 데이터베이스에서 작업을 만들거나 업데이트하거나 삭제할 경우 NA가 작업 풀을 업데이트합니다. 작업이 로컬 NA 코어용일 경우 로컬 작업 풀이 업데이트됩니다. 작업이 원격 NA 코어용일 경우 원격 NA 코어의 작업 풀이 업데이트됩니다.
- **작업 풀 캐싱** — 작업 풀은 아직 실행하지 않은 모든 작업을 캐싱합니다.

작업 풀 외부에 있는 작업을 풀링하는 경우 NA는 다음을 처리합니다.

1. 우선 순위의 오름차순으로 된 작업 대기열 그룹.
2. 각 작업 대기열의 작업은 예정된 시간에 따라 FIFO(선입선출) 알고리즘을 사용합니다. NA는 특정 시간 동안 일정보다 뒤에 있는 경우 작업의 우선 순위를 높입니다. 이 작업의 모든 하위 작업은 새 우선 순위를 사용합니다. 작업이 반복 작업이면 새 우선 순위는 동시에 발생하는 이 작업과 하위 작업에만 적용됩니다.

NA는 사용할 수 있는 메모리가 충분하지 않으면 최대 동시 작업을 실행하지 않습니다. 따라서 최대 동시 작업이 200으로 설정되면 NA는 200개 동시 작업 모두를 실행할 수 없습니다. 동시 작업의 최대 개수를 설정하는 방법에 대한 자세한 내용은 [68페이지의 "서버 페이지 필드"](#)를 참조하십시오.

참고: 스케줄러를 통해 작업을 다시 예약해야 하는 경우(시간 및 작업 우선 순위 예약) 새 정보는 작업 풀에서만 업데이트됩니다. 이 정보는 데이터베이스에 저장할 수 없거나 사용자가 사용할 수 없습니다.

라운드 로빈 그룹 작업

작업이 완료되면 NA는 그룹 1에서 다음 하위 작업을 받은 다음 그룹 2에서 다음 하위 작업을 받습니다. 예를 들어 라운드-로빈 알고리즘을 사용하여 오전 10시에 10,000대 장치에 대해 그룹 작업을 시작하고 나서 오전 10시 5분에 10대 장치에 대한 그룹 작업을 시작한 경우 두 번째 그룹 작업이 시작되기 전에 첫 번째 그룹 작업이 완료될 때까지 더 이상 기다릴 필요가 없습니다.

작업 템플릿

작업 템플릿을 사용하면 작업 정의를 저장할 수 있으므로 처음부터 다시 시작하지 않더라도 새로운 작업과 기존 작업을 쉽게 구성 및 실행할 수 있습니다. 또한 NA 홈 페이지의 내 작업 공간 영역에 있는 내 즐겨찾기 섹션에서 가장 자주 실행되는 작업에 대한 링크를 만들 수도 있습니다.

작업 템플릿을 만드는 방법에는 세 가지가 있습니다.

- 새로운 작업 페이지 또는 편집 작업 페이지에서 저장 옵션 필드의 작업 템플릿으로 저장 옵션을 클릭합니다. 따라서 작업이 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 구성에 대한 자세한 내용은 [364페이지의 "NA 작업"](#)을 참조하십시오.
- 예정된 작업 페이지의 작업 열에서 템플릿 생성 링크를 클릭합니다. 자세한 내용은 [495페이지의 "예정된 작업 페이지 필드"](#)를 참조하십시오.
- 최근 작업 페이지의 작업 열에서 템플릿 생성 링크를 클릭합니다. 자세한 내용은 [500페이지의 "최근 작업 페이지 필드"](#)를 참조하십시오.

멀티 태스킹 프로젝트를 예약하고 프로젝트를 작업 템플릿으로 저장하는 경우 프로젝트 하위 작업으로 인해 프로젝트가 적용되는 장치 및/또는 모든 장치를 선택해야 합니다. 또한 멀티 태스킹 프로젝트에 대한 올바른 사용 권한이 있어야 합니다. 자세한 내용은 [485페이지의 "멀티 태스킹 프로젝트 예약"](#)을 참조하십시오.

참고: 작업 검색 페이지에서 작업 템플릿을 검색할 수도 있습니다. 자세한 내용은 [622페이지의 "작업 검색"](#)을 참조하십시오.

현재 작업 템플릿을 보려면 작업 아래의 메뉴 모음에서 작업 템플릿을 클릭합니다. 작업 템플릿 페이지가 열립니다.

참고: 또한 예정된 작업, 실행 중인 작업 및 최근 작업 페이지에서 작업 템플릿 페이지로 이동할 수도 있습니다.

필드	설명/작업
내 작업 링크	내 작업 페이지가 열립니다. 자세한 내용은 491페이지의 "내 작업 페이지 필드" 를 참조하십시오.
내 드래프트 링크	내 드래프트 페이지가 열립니다. 자세한 내용은 491페이지의 "내 작업 페이지 필드" 를 참조하십시오.

필드	설명/작업
승인 요청 링크	현재 로그인한 사용자가 승인해야 하는 작업을 볼 수 있는 승인 요청 페이지가 열립니다. 자세한 내용은 863페이지의 "승인 요청" 을 참조하십시오.
예정된 작업 링크	예정된 작업 페이지가 열립니다. 자세한 내용은 495페이지의 "예정된 작업 페이지 필드" 를 참조하십시오.
실행 중인 작업 링크	실행 중인 작업 페이지가 열립니다. 자세한 내용은 498페이지의 "작업 실행 중 페이지 필드" 를 참조하십시오.
최근 작업	최근 작업 페이지가 열립니다. 자세한 내용은 500페이지의 "최근 작업 페이지 필드" 를 참조하십시오.
확인란	왼쪽의 확인란을 통해 템플릿을 삭제할 수 있습니다. 템플릿을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 템플릿을 선택하거나 선택 취소할 수 있습니다.
생성 날짜	NA에서 작업 실행을 시작한 날짜와 시간을 표시합니다.
템플릿 이름	템플릿 이름을 표시합니다.
호스트/그룹	작업과 연관된 네트워크 장치의 호스트 또는 그룹 이름을 표시합니다. 링크를 클릭하여 그룹의 장치에 대한 자세한 정보를 볼 수 있는 장치 정보 페이지를 열 수 있습니다.
우선 순위	작업 우선 순위를 표시합니다. 1~5의 5가지 작업 우선 순위 수준이 있으며, 최고 작업 우선 순위는 1입니다. 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
파티션	보안 또는 업무 상의 이유로 파티션을 만든 경우 파티션이 이 열에 표시됩니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
생성자	작업을 예약한 사람(또는 작업을 수정한 마지막 사용자)의 로그인 이름을 표시합니다.
주석	작업에 대한 주석을 표시합니다.

필드	설명/작업
작업	<p>선택할 수 있는 작업은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 삭제 — 템플릿을 삭제할지 확인하는 대화 상자가 열립니다. 템플릿을 삭제하면 해당 즐겨찾기 링크도 제거됩니다. • 편집 — 선택한 작업의 작업 편집 페이지(예: 작업 편집 - 스냅샷 페이지)를 엽니다. 작업을 편집하고 템플릿으로 저장할 수 있습니다. (참고: 템플릿의 이름을 변경하지 않으면 새 템플릿이 이전 템플릿을 오버라이드합니다.) • 실행 — 작업 재실행 페이지를 엽니다. 이 페이지에서는 작업을 재실행하고 편집한 후 다시 실행할 수 있습니다. (참고: 이 옵션은 작업을 예약 옵션 필드에 구성된 대로 재실행할 수 있는 경우에만 나타납니다.) • 즐겨찾기에 추가 — NA 홈 페이지의 내 작업 공간 영역에 있는 내 즐겨찾기 섹션에 작업이 추가되므로 작업 페이지로 이동하지 않고도 작업을 실행할 수 있습니다. • 빠른 시작에 추가 — NA 홈 페이지의 내 작업 공간 탭 아래에 있는 빠른 시작 섹션에 빠른 시작 링크를 추가합니다. 빠른 시작 링크는 현재 작업 템플릿의 이름을 가정합니다. 링크의 이름을 변경하려면 표시된 팝업 상자를 사용하십시오. 빠른 시작에 대한 자세한 내용은 345페이지의 "빠른 시작이란?"을 참조하십시오.
페이지별 결과 표시 수	드롭다운 메뉴에서 페이지당 표시할 항목 수를 설정할 수 있습니다. 기본값은 25입니다.

NA 작업

새 작업/템플릿 페이지를 열려면 작업 아래의 메뉴 모음에서 작업을 선택하고 예약할 작업을 클릭합니다. 해당 작업에 대한 새 작업/템플릿 페이지가 열립니다. 다음 표에 선택할 수 있는 작업이 나와 있습니다.

작업	참조 페이지
Syslog 구성	366페이지의 "Syslog 구성 작업 페이지 필드"
암호 배포	370페이지의 "암호 배포 작업 페이지 필드"
드라이버 검색	375페이지의 "드라이버 검색 작업 페이지 필드"
장치 재부팅	379페이지의 "장치 재부팅 작업 페이지 필드"
ICMP 테스트 실행	383페이지의 "ICMP 테스트 실행 작업 페이지 필드"
명령 스크립트 실행	389페이지의 "명령 스크립트 실행 작업 페이지 필드"
진단 실행	397페이지의 "진단 실행 작업 페이지 필드"
스냅샷 작성	403페이지의 "스냅샷 작성 작업 페이지 필드"
시작 및 실행 동기화	408페이지의 "시작 및 실행 동기화 작업 페이지 필드"
장치 소프트웨어 업데이트	413페이지의 "장치 소프트웨어 업데이트 작업 페이지 필드"
장치 가져오기	421페이지의 "가져오기 작업 페이지 필드"
네트워크 장치 감지	426페이지의 "네트워크 장치 감지 작업 페이지 필드"
중복 방지	433페이지의 "중복 방지 작업 페이지 필드"
OS 분석	436페이지의 "OS 분석 작업 페이지 필드"
포트 스캔	440페이지의 "포트 스캔 페이지 필드"
템플릿에서 장치 프로비전	444페이지의 "장치 프로비전 작업 페이지 필드"
장치 컨텍스트	448페이지의 "장치 컨텍스트 추가 작업 페이지 필드"
VLAN	452페이지의 "VLAN 작업 페이지 필드"
Cisco.com에서 이미지 다운로드 작업	456페이지의 "Cisco.com에서 이미지 다운로드 작업 페이지"
템플릿에서 장치 프로비전	444페이지의 "장치 프로비전 작업 페이지 필드"

작업	참조 페이지
Cisco.com에서 이미지 다운로드 작업	456페이지의 "Cisco.com에서 이미지 다운로드 작업 페이지"
장치 소프트웨어 백업 작업	459페이지의 "장치 소프트웨어 백업 작업 페이지 필드"
정책 준수 확인	462페이지의 "정책 준수 확인 작업 페이지 필드"
요약 보고서 생성	466페이지의 "요약 보고서 생성 작업 페이지 필드"
전자 메일 보고서	469페이지의 "전자 메일 보고서 작업 페이지 필드"
원격 에이전트 배포	472페이지의 "원격 에이전트 배포 페이지 필드"
FQDN 확인	475페이지의 "FQDN 확인 작업 페이지 필드"
데이터 정리	478페이지의 "데이터 정리 작업 페이지 필드"
외부 응용 프로그램 실행	481페이지의 "외부 응용 프로그램 실행 작업 페이지 필드"

Syslog 구성 작업 페이지 필드

Syslog 구성 작업을 통해 Syslog 메시지를 보낼 하나 이상의 장치에 대한 자동 구성을 예약할 수 있습니다. NA는 Syslog 메시지를 사용하여 실시간 구성 변경을 감지합니다.

검색 후(또는 각 장치에 드라이버를 할당할 때) NA는 다음을 수행합니다.

1. 구성의 스냅샷을 작성합니다.
2. 구성을 업데이트하여 Syslog 메시지를 NA로 보냅니다.
3. 장치가 변경 감지를 활성화하도록 자동 구성되었음을 나타내는 주석을 구성에 작성합니다.
4. 최종 스냅샷을 작성합니다.

필드	설명/작업
작업 이름	Syslog 구성을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>

필드	설명/작업
시작 날짜	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 가능한 한 빨리 시작(기본값) • 시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	<p>작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.</p>
주석	<p>작업에 대한 주석을 입력합니다.</p>
작업 옵션	
세션 로그	<p>전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버깅할 때는 맨 먼저 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.)</p>
Syslog 구성	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • NA Syslog 서버에 기록할 장치 설정(기본값) • 장치가 syslog 릴레이에 로그되므로 올바른 로깅 수준 설정 릴레이 호스트를 입력합니다.
추산 기간	<p>이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.</p>
장치 자격 증명 옵션	
<p>장치 자격 증명 옵션은 장치 액세스 페이지의 관리 설정 아래에서 구성된 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 56페이지의 "장치 액세스 페이지 필드"를 참조하십시오.</p>	

필드	설명/작업
장치 자격 증명	<p>서버 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) • 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력 하라는 메시지가 표시됩니다. • 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명이 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
승인 옵션	
승인 옵션	승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기 열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	<p>작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행 합니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.

필드	설명/작업
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

암호 배포 작업 페이지 필드

암호 배포 작업을 통해 중앙 위치에서 여러 장치에 대한 암호 설정 및 SNMP 커뮤니티 문자열을 변경할 수 있습니다.

참고: 단일 장치에 암호를 배포하려면 프로비전 메뉴에서 암호 배포 옵션을 선택합니다. [314페이지의 "프로비전 메뉴 옵션"](#)을 참조하십시오.

네트워크에서 NA와 함께 AAA를 사용하는 경우 NA를 통해서가 아니라 AAA 서버를 통해 암호를 변경해야 합니다. 이렇게 하지 않으면 NA에서 장치와의 연결이 손실될 수도 있습니다. 또한 NA는 실제로 AAA 암호를 관리하지 않으며 장치에서 유지 관리하는 사용자 계정도 관리하지 않습니다. NA는 단일 장치에 대한 암호 배포를 예약하는 경우에 표시되는 메시지와 그룹 암호 배포를 예약하는 경우 "의미" 링크의 출력만 관리합니다.

NA는 Nortel Baystack 450과 같은 메뉴 방식의 장치를 비롯하여 대부분의 장치에 대한 암호 및 커뮤니티 문자열 변경을 지원합니다. 지원되는 장치에 대한 자세한 내용은 DRS(장치 릴리스 서비스) 설명서를 참조하십시오. DRS는 자동화된 새로운 드라이버 릴리스 및 전달 시스템입니다.

성공적으로 변경되면 NA는 장치 스냅샷을 수행하고 변경된 구성을 다운로드합니다. 신속하게 암호 또는 SNMP 커뮤니티 문자열의 최근 변경을 모두 보려면 구성 변경 페이지로 이동합니다. 자세한 내용은 [223페이지의 "장치 구성 변경 보기"](#)를 참조하십시오.

AAA를 사용하는 경우 암호 배포 기능을 사용하여 장치 암호를 변경하려고 하면 NA는 AAA가 아니라 새 암호를 사용하여 장치에 연결하려고 할 수 있습니다. 그러나 장치는 여전히 AAA 로그인을 기대할 수 있습니다. 필요하다면 AAA를 사용하도록(변경된 경우) 장치를 수동으로 다시 구성하고 올바른 AAA 자격 증명을 사용하여 장치에 로그인하도록 NA를 다시 구성해야 합니다.

참고: 경우에 따라 암호 배포 작업에서 NA가 장치에 액세스하는 데 필요한 자격 증명의 일부로 새 자격 증명의 사용자 이름 부분을 할당하지 않을 수도 있습니다. 암호 배포 작업을 실행하여 장치 로그인에 사용자 이름이 필요한 장치에 대한 암호를 변경하는 경우에 이러한 현상이 발생할 수 있습니다. 작업이 완료되고 스냅샷이 실행되면 오류 메시지에서 사용자 이름이 없다고 보고합니다. 이 경우 암호 배포 작업을 실행한 후 장치를 편집하고 "장치별 암호 정보 사용" 섹션에 사용자 이름을 추가합니다. 자세한 내용은 [171페이지의 "장치 암호 규칙 페이지 필드"](#)를 참조하십시오.

필드	설명/작업
작업 이름	암호 배포를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>
시작 날짜	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.

필드	설명/작업
작업 옵션	
세션 로그	전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버깅할 때는 맨 먼저 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.)
제한된 액세스 사용자 이름	NA에서 장치에 액세스하는 데 필요한 제한된 액세스 사용자 이름을 입력합니다. 사용자 이름은 장치의 공급업체와 운영 체제에 따라 다릅니다. 장치 관련 정보를 보려면 "의미" 링크를 클릭합니다. (참고: 사용자 이름이 없으면 연관된 필드가 장치에서 변경되지 않습니다.)
제한된 액세스 암호	NA에서 장치에 액세스하는 데 필요한 제한된 액세스 암호를 입력합니다. 암호는 장치의 공급업체와 운영 체제에 따라 다릅니다. 장치 관련 정보를 보려면 "의미" 링크를 클릭합니다. (참고: 암호가 없으면 연관된 필드가 장치에서 변경되지 않습니다.)
암호 확인	확인하기 위해 암호를 다시 입력합니다.
전체 액세스 사용자 이름	NA에서 장치에 액세스하는 데 필요한 전체 액세스 사용자 이름을 입력합니다. 사용자 이름은 장치의 공급업체와 운영 체제에 따라 다릅니다. 장치 관련 정보를 보려면 "의미" 링크를 클릭합니다. (참고: 사용자 이름이 없으면 연관된 필드가 장치에서 변경되지 않습니다.)
전체 액세스 암호	NA에서 장치에 액세스하는 데 필요한 전체 액세스 암호를 입력합니다. 암호는 장치의 공급업체와 운영 체제에 따라 다릅니다. 장치 관련 정보를 보려면 "의미" 링크를 클릭합니다. (참고: 암호가 없으면 연관된 필드가 장치에서 변경되지 않습니다.)
암호 확인	확인하기 위해 암호를 다시 입력합니다.
SNMP 읽기 커뮤니티 문자열	SNMP 읽기 커뮤니티 문자열을 추가하려면 오른쪽 상자에 문자열을 입력한 다음 << 읽기 커뮤니티 문자열 추가를 클릭합니다. SNMP 읽기 커뮤니티 문자열을 제거하려면 왼쪽 상자에서 이름을 선택한 다음 읽기 커뮤니티 문자열 삭제를 클릭합니다. "장치의 기존 커뮤니티 문자열에 추가"(기본값) 또는 "장치의 기존 커뮤니티 문자열 대체"를 선택합니다.

필드	설명/작업
SNMP 쓰기 커뮤니티 문자열	SNMP 쓰기 커뮤니티 문자열을 추가하려면 오른쪽 상자에 문자열을 입력한 다음 << 쓰기 커뮤니티 문자열 추가를 클릭합니다. SNMP 쓰기 커뮤니티 문자열을 제거하려면 왼쪽 상자에서 이름을 선택한 다음 쓰기 커뮤니티 문자열 삭제를 클릭합니다. "장치의 기존 커뮤니티 문자열에 추가"(기본값) 또는 "장치의 기존 커뮤니티 문자열 대체"를 선택합니다.
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.
장치 자격 증명 옵션 장치 자격 증명 옵션은 장치 액세스 페이지의 관리 설정 아래에서 구성된 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 56페이지의 "장치 액세스 페이지 필드" 를 참조하십시오.	
장치 자격 증명	서버 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다. <ul style="list-style-type: none"> • 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) • 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력하라는 메시지가 표시됩니다. • 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
승인 옵션 승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.

필드	설명/작업
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	사용할 수 없음
작업 로깅	
작업 로깅	사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

드라이버 검색 작업 페이지 필드

드라이버 검색 작업을 통해 드라이버 검색을 예약할 수 있습니다.

필드	설명/작업
작업 이름	드라이버 검색을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.

필드	설명/작업
작업 옵션	
세션 로그	전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버깅할 때는 맨 먼저 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.)
옵션	설정된 드라이버가 없는 경우 "설정된 드라이버가 없는 경우에만" 확인란(기본값)을 선택합니다.
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.
장치 자격 증명 옵션	
장치 자격 증명 옵션은 장치 액세스 페이지의 관리 설정 아래에서 구성된 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 56페이지의 "장치 액세스 페이지 필드" 를 참조하십시오.	
장치 자격 증명	<p>서버 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) • 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력하라는 메시지가 표시됩니다. • 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명이 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	

필드	설명/작업
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기 열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). •주기적으로 — 반복 간격(분)을 지정합니다. •매일 — 작업이 매일 지정된 시간에 발생합니다. •매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. •매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.

필드	설명/작업
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다.

자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오. 작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

장치 재부팅 작업 페이지 필드

장치 재부팅 작업을 통해 장치를 재부팅할 수 있습니다.

필드	설명/작업
작업 이름	장치 재부팅을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.

필드	설명/작업
작업 옵션	
세션 로그	전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 많은 양의 데이터를 저장할 수 있습니다. 이 옵션은 장치 문제 해결에만 사용하는 것이 좋습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.
장치 자격 증명 옵션	
장치 자격 증명 옵션은 장치 액세스 페이지의 관리 설정 아래에서 구성된 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 56페이지의 "장치 액세스 페이지 필드" 를 참조하십시오.	
장치 자격 증명	<p>서버 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력하라는 메시지가 표시됩니다. 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명이 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	

필드	설명/작업
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기 열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	사용할 수 없음
작업 로깅	
작업 로깅	사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

ICMP 테스트 실행 작업 페이지 필드

ICMP(Internet Control Message Protocol) 테스트 실행 작업을 통해 한 장치에서 하나 이상의 장치로의 Ping 또는 traceroute 테스트를 예약할 수 있습니다.

Traceroute에서는 패킷이 네트워크를 통해 전달되는 경로를 추적하려고 하며 작은 TTL(Time-To-Live) 값을 사용하여 패킷을 전송합니다. TTL은 패킷이 루프에서 실행되는 것을 방지하기 위해 설계된 IP 헤더 필드이며 *출제/한*이라고도 합니다. Traceroute는 ICMP Time Exceeded 메시지를 보낸 사람에게 다시 보내는 장치에 의존합니다. Traceroute는 패킷의 일반 전달 경로에 있는 장치가 경로를 식별하는 이러한 ICMP 메시지를 생성하게 합니다.

Ping(Packet INternet Groper)은 한 패킷을 보내고 한 응답 패킷을 수신합니다. Ping은 필요한 ICMP 에코 기능을 사용하여 구현됩니다.

일반적으로 Traceroute 옵션은 장치가 인식하는 경로에 있는 장치를 차례로 이동하면서 작업을 수행합니다. 또한 Ping은 경로에 있는 각 장치로 개별적으로 이동합니다.

Traceroute 및 Ping 명령은 NA에서 완료하는 기능이 아닙니다. 장치에서 이러한 기능을 수행합니다. NA는 소스 장치에 로그인하고 추적할 장치에 적절한 명령을 대상 장치에 대해 실행할 수 있어야 합니다. 각 장치는 이러한 기능을 서로 다르게 구현하거나 전혀 구현하지 않을 수 있습니다. ICMP 테스트 결과 페이지에 표시되는 것은 장치가 화면에 표시하는 내용의 덤프입니다.

Ping과 traceroute는 훌륭한 네트워킹 문제 해결 도구입니다. 예를 들어, Ping을 사용하여 특정 장치에 액세스할 수 있는지 확인하기 위해 100개의 장치를 테스트할 수 있습니다. 또는 20개의 장치가 특정 장치에 액세스하는 데 문제가 있는 경우 자동화된 원격 Traceroute를 실행하고 각 장치가 해당 대상까지 사용하는 경로를 확인할 수 있습니다.

참고: ICMP 테스트는 변경 후 또는 간헐적으로 연결을 확인하려는 경우에만 사용하십시오. 이러한 테스트는 모니터링 소프트웨어를 대체하지 않습니다. 10분 이상의 간격으로 ICMP 테스트를 예약해야 합니다.

필드	설명/작업
작업 이름	ICMP 테스트 실행을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.

필드	설명/작업
작업 옵션	
세션 로그	전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버깅할 때는 맨 먼저 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.)
테스트 유형	Ping 또는 traceroute를 선택합니다.
대상 호스트 목록	호스트를 추가하려면 오른쪽 상자에 이름을 입력한 다음 << 호스트 추가를 클릭합니다. 호스트를 제거하려면 왼쪽 상자에서 호스트 이름을 선택한 다음 호스트 제거를 클릭합니다.
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.
장치 자격 증명 옵션	
장치 자격 증명 옵션은 장치 액세스 페이지의 관리 설정 아래에서 구성된 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 56페이지의 "장치 액세스 페이지 필드" 를 참조하십시오.	
장치 자격 증명	서버 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다. <ul style="list-style-type: none"> • 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) • 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력하라는 메시지가 표시됩니다. • 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명에 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	

필드	설명/작업
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.

필드	설명/작업
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예약된 경우 ICMP 테스트 결과 페이지가 열립니다.

참고: ICMP 테스트 결과 페이지에 표시되는 것은 장치가 화면에 표시하는 내용의 덤프입니다.

작업이 성공하고 Ping 옵션을 선택한 경우 ICMP 테스트 실행 작업 페이지에서 입력한 정보와 장치에 따라 다음과 같은 정보가 표시됩니다.

- 생성 날짜
- 명령 실행
- 결과
- 명령 출력(예: Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms)

Traceroute 옵션을 선택한 경우 ICMP 테스트 실행 작업 페이지에서 입력한 정보와 장치에 따라 다음과 같은 정보가 표시됩니다.

- 생성 날짜
- 명령 실행
- 결과

- 명령 출력(예:

```
1 1ms 1ms 1ms 10.255.111.2
2 4ms 4ms 4ms 10.255.111.3
3 * * * *
```

첫 번째 열에 흡이 표시됩니다. 다음 세 열에는 장치가 응답하는 데 걸린 시간이 표시됩니다. 장치가 응답하는 데 걸린 시간이 지정된 제한 시간보다 길면 별표가 표시됩니다.). 마지막 열은 응답한 호스트입니다.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

명령 스크립트 실행 작업 페이지 필드

명령 스크립트 실행 작업을 통해 명령 스크립트를 실행할 수 있습니다.

필드	설명/작업
새 명령 스크립트 링크	새 명령 스크립트 페이지가 열립니다. 스크립트 작성에 대한 자세한 내용은 722페이지의 "새 명령 스크립트 페이지 필드" 를 참조하십시오.
명령 스크립트 링크	명령 스크립트 페이지가 열립니다. 자세한 내용은 717페이지의 "명령 스크립트 페이지 필드" 를 참조하십시오.
작업 이름	명령 스크립트 실행 이름을 표시합니다. 해당하는 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다(IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.

필드	설명/작업
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~ 5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.
작업 옵션	
세션 로그	전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.

필드	설명/작업
실행할 명령 스크립트	<p>실행할 명령 스크립트를 선택합니다. 옵션은 선택하는 스크립트 유형에 따라 변경됩니다. 표준 명령 스크립트에는 다음이 포함됩니다.</p> <ul style="list-style-type: none"> • Cisco IOS 초기 설정 • Cisco IOS에서 ACL ID로 ACL에 라인 삽입 • Cisco IOS에서 핸들로 ACL에 라인 삽입 • Cisco IOS에서 ACL ID로 ACL의 라인 제거 • Cisco IOS에서 핸들로 ACL의 라인 제거 • 플래시 압축 • Contivity 1100 SNMP 커뮤니티 문자열 배포 • 확장된 Ping • 전이중 • ios_7k_reboot • ios_generic_reboot • ios_l3switch_reboot • Passport 8xxx - 커뮤니티 문자열 배포 • Passport 8xxx - SNMP-v3 커뮤니티 문자열 배포 • Passport 8xxx - 사용자 암호 배포 • Passport 8xxx - Radius 사용 • Passport 8xxx - 웹 서버 사용 • 샘플 - FastEther 인터페이스 프로비전 • 배너 설정 • 필요한 경우 배너만 설정 • 위치 설정 • NTP 서버 설정 • 전달된 브로드캐스트 끄기 • 인터페이스 업데이트
미리 보기 옵션	<p>전체 스크립트를 작성할 수 있지만 실행할 수는 없습니다. 따라서 실제로 명령을 실행하지 않고 실행되는 명령을 볼 수 있습니다.</p>

필드	설명/작업
스크립트 유형으로 제한	모두 선택하거나(기본값) 다음 중 하나를 선택합니다. <ul style="list-style-type: none"> •ACL 고급 스크립트 •ACL 응용 프로그램 스크립트 •ACL 생성 스크립트 •ACL 편집 스크립트
선택하는 명령 스크립트에 따라 다음과 같은 옵션이 표시될 수 있습니다.	
모드	Cisco Exec 또는 Nortel Manager와 같은 장치 액세스 모드를 표시합니다. 이것은 장치 플랫폼과 유사합니다.
변수	스크립트에 입력할 변수 필드가 있는 경우 값을 입력합니다. 완료하면 스크립트 업데이트를 클릭하여 해당 변수 값으로 실행될 스크립트를 볼 수 있습니다. 사용자 지정 변수 정의에 대한 자세한 내용은 722페이지의 "새 명령 스크립트 페이지 필드" 를 참조하십시오.
장치 제품군	(고급 스크립팅) 이 스크립트가 실행되는 장치 제품군의 이름을 표시합니다. 장치 제품군은 유사한 구성 CLI 명령 구문을 공유하는 장치의 모음입니다.
매개 변수	스크립트의 매개 변수를 입력합니다.
스크립트	실행할 장치별 명령을 표시합니다. 이 스크립트 인스턴스를 편집할 수 있지만 이 인스턴스가 실행된 후 변경 내용이 저장되지 않습니다. 여러 모드가 있는 경우 모드마다 스크립트 인스턴스가 하나씩 나타납니다. <p>참고: 스크립트 상자의 높이와 너비는 관리 설정 페이지에서 사용자 인터페이스 탭을 설정하여 제어됩니다. 스크립팅 기능을 광범위하게 사용하는 경우 스크롤하지 않고 스크립트를 볼 수 있도록 이러한 설정을 조정할 수 있습니다.</p>
배포 옵션	스크립트를 한꺼번에 배포하지 않고 라인별로 실행하려면 "스크립트를 한꺼번에 배포하지 않고 라인별로 실행..." 확인란을 선택합니다. Cisco IOS 구성 스크립트와 같이 대량 배포 방법을 통해 스크립트를 실행할 수 있는 장치는 가능한 경우 항상 이렇게 합니다. 기본적으로 스크립트의 전체 내용이 단일 배치로 배포되고 실행됩니다. 오류가 발생하는 경우 스크립트가 계속 실행됩니다. 이러한 경우에 스크립트를 라인별로 실행하면 스크립트에서 오류를 캡처하고 실행을 중지합니다.

필드	설명/작업
대기 옵션	기본적으로 선택됩니다. 이 옵션의 선택을 취소하면 동일한 장치에 대해 다른 작업이 이미 실행되고 있는 경우에도 작업이 실행될 수 있습니다.
언어	(고급 스크립팅) 스크립트가 작성된 언어를 표시합니다.
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본 값은 60분입니다.

장치 자격 증명 옵션

장치 자격 증명 옵션은 장치 액세스 페이지의 관리 설정 아래에서 구성된 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 [56페이지의 "장치 액세스 페이지 필드"](#)를 참조하십시오.

장치 자격 증명	<p>서버 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력하라는 메시지가 표시됩니다. 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명이 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
----------	---

사전 작업/사후 작업 스냅샷 옵션

스냅샷 옵션은 시스템이 구성 관리 페이지의 관리 설정에서 사용자 오버라이드를 활성화하도록 구성된 경우에만 표시됩니다. (자세한 내용은 [43페이지의 "구성 관리 페이지 필드"](#)를 참조하십시오.)

사전 작업 스냅샷	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 없음(기본값) 작업에 포함됨
-----------	--

필드	설명/작업
사후 작업 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨(기본값) •별도 작업으로 예정됨
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.

필드	설명/작업
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

진단 실행 작업 페이지 필드

진단 실행 작업을 통해 진단 실행을 예약할 수 있습니다. 작업 아래의 메뉴 모음에서 새 작업을 선택하고 진단 실행을 선택합니다. 진단 실행 페이지가 열립니다.

필드	설명/작업
새 진단 링크	새 진단 페이지가 열립니다. 자세한 내용은 686페이지의 "새 진단 페이지 필드" 를 참조하십시오.
진단 링크	진단 페이지가 열립니다. 진단 관리에 대한 자세한 내용은 684페이지의 "진단 페이지 필드" 를 참조하십시오.
작업 이름	진단 실행을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다(IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>

필드	설명/작업
시작 날짜	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 가능한 한 빨리 시작(기본값) • 시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	<p>작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.</p>
주석	<p>작업에 대한 주석을 입력합니다.</p>
작업 옵션	
세션 로그	<p>전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

필드	설명/작업
실행할 진단	<p>실행할 진단을 선택합니다. 추가 진단을 선택/선택 취소하려면 Ctrl 키를 누른 상태에서 진단을 클릭합니다. 진단에는 다음이 포함됩니다.</p> <ul style="list-style-type: none"> • 하드웨어 정보 • 메모리 문제 해결 • NA 감지 장치 부팅 • NA 장치 파일 시스템 • NA 이중 데이터 수집 • NA 플래시 저장 공간 • NA 인터페이스 • NA 모듈 상태 • NA OSPF 인접 환경 • NA 라우팅 테이블 • NA 토폴로지 수집 • NA VLAN 데이터 수집 • NA 포트 스캔 <p>참고: 진단에 대한 자세한 내용은 261페이지의 "메뉴 옵션 보기"를 참조하십시오.</p>
추산 기간	<p>이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본 값은 60분입니다.</p>

장치 자격 증명 옵션

장치 자격 증명 옵션은 장치 액세스 페이지의 관리 설정 아래에서 구성된 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 [56페이지의 "장치 액세스 페이지 필드"](#)를 참조하십시오.

필드	설명/작업
장치 자격 증명	<p>서버 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력하라는 메시지가 표시됩니다. 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명이 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
<p>사전 작업/사후 작업 스냅샷 옵션</p> <p>스냅샷 옵션은 시스템이 구성 관리 페이지의 관리 설정에서 사용자 오버라이드를 활성화하도록 구성된 경우에만 표시됩니다. (자세한 내용은 43페이지의 "구성 관리 페이지 필드"를 참조하십시오.)</p>	
사전 작업 스냅샷	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 없음(기본값) 작업에 포함됨
사후 작업 스냅샷	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> 없음 작업에 포함됨(기본값) 별도 작업으로 예정됨
<p>승인 옵션</p> <p>승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.</p>	
승인 요청	<p>작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.</p>
승인 오버라이드	<p>작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.</p>

필드	설명/작업
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다. <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.

필드	설명/작업
작업 로깅	
작업 로깅	사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

스냅샷 작성 작업 페이지 필드

스냅샷 작성 작업을 통해 스냅샷을 예약할 수 있습니다. 스냅샷 작성 작업에서는 저장된 구성이 장치에서 실행 중인 구성과 일치하는지 확인하고, 일치하지 않으면 장치 구성과 관련 데이터의 새 복사본을 NA 데이터베이스에 저장합니다.

"스냅샷을 검사점으로 만들기" 옵션을 선택하면 NA가 차이를 감지하지 않은 경우에도 NA 데이터베이스가 업데이트됩니다. 따라서 스냅샷이 여전히 홈 페이지, 요약 보고서, 구성 변경 검색 결과 등에 구성 변경으로 표시됩니다.

필드	설명/작업
작업 이름	스냅샷 작성을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>

필드	설명/작업
시작 날짜	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 가능한 한 빨리 시작(기본값) • 시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	<p>작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.</p>
주석	<p>작업에 대한 주석을 입력합니다.</p>
작업 옵션	
세션 로그	<p>디버깅 로그를 저장하려면 "전체 장치 세션 로그 저장" 상자를 선택합니다. 장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버깅할 때는 맨 먼저 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.)</p>
옵션	<p>다음 옵션 중 하나를 선택하거나 둘 다 선택합니다.</p> <ul style="list-style-type: none"> • 스냅샷을 검사점으로 만들기 — 저장된 구성이 실행 중인 구성과 다른지 먼저 확인하지 않고 실행 중인 구성을 NA 데이터베이스에 복사합니다. 이 옵션은 변경 여부와 상관 없이 구성 파일을 저장합니다. 하지만 변경된 사항이 없어도 스냅샷이 여전히 홈 페이지, 요약 보고서, 구성 변경 검색 결과 등에 구성 변경으로 표시됩니다. 따라서 구성 변경 수에 검사된 구성이 포함되므로 이 개수는 정확하지 않을 수도 있습니다. • 바이너리 구성 검색 — 텍스트 정보뿐만 아니라 바이너리 구성(있는 경우)도 NA 데이터베이스에 복사합니다.
추산 기간	<p>이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.</p>

필드	설명/작업
장치 자격 증명 옵션	<p>장치 자격 증명 옵션은 장치 액세스 페이지의 관리 설정 아래에서 구성된 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 56페이지의 "장치 액세스 페이지 필드"를 참조하십시오.</p>
장치 자격 증명	<p>서버 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) • 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력하라는 메시지가 표시됩니다. • 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명이 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
승인 옵션	<p>승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.</p>
승인 요청	<p>작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.</p>
승인 오버라이드	<p>작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.</p>
드래프트로 저장	<p>이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.</p>
예약 옵션	

필드	설명/작업
재시도 수	<p>작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). •주기적으로 — 반복 간격(분)을 지정합니다. •매일 — 작업이 매일 지정된 시간에 발생합니다. •매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. •매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> •종료 날짜 없음(기본값) •< >번 발생 후 종료 — 반복 횟수를 입력합니다. •종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

시작 및 실행 동기화 작업 페이지 필드

시작 및 실행 동기화 작업을 통해 장치에 대한 구성의 시작과 실행을 동기화할 수 있습니다. NA는 시작 구성을 현재 실행 중인 구성으로 덮어씁니다. 이 작업은 장치가 다시 부팅될 때 현재 구성이 계속 실행되도록 합니다.

필드	설명/작업
작업 이름	시작 및 실행 동기화를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.

필드	설명/작업
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.
작업 옵션	
세션 로그	디버깅 로그를 저장하려면 "전체 장치 세션 로그 저장" 상자를 선택합니다. 이렇게 하면 실패한 스냅샷을 디버깅할 때 유용하지만 많은 양의 데이터가 저장될 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.
옵션	구성이 이미 동기화된 경우 NA에서 작업을 건너뛰게 하려면 "동기화 시 무시" 상자를 선택합니다.
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.

장치 자격 증명 옵션

장치 자격 증명 옵션은 장치 액세스 페이지의 관리 설정 아래에서 구성된 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 [56페이지의 "장치 액세스 페이지 필드"](#)를 참조하십시오.

장치 자격 증명	<p>서버 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) • 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력하라는 메시지가 표시됩니다. • 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명이 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
----------	--

필드	설명/작업
사전 작업/사후 작업 스냅샷 옵션	
스냅샷 옵션은 시스템이 구성 관리 페이지의 관리 설정에서 사용자 오버라이드를 활성화하도록 구성된 경우에만 표시됩니다. (자세한 내용은 43페이지의 "구성 관리 페이지 필드"를 참조하십시오.)	
사후 작업 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨(기본값) •별도 작업으로 예정됨
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기 열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.

필드	설명/작업
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

장치 소프트웨어 업데이트 작업 페이지 필드

장치 소프트웨어 업데이트 작업을 통해 하나 이상의 장치에 대한 소프트웨어 배포를 예약할 수 있습니다. 자세한 내용은 [551페이지의 "소프트웨어 이미지"](#)를 참조하십시오. 다음 사항을 기억하십시오.

- 전체 메모리는 장치에 있는 전체 물리적 메모리입니다.
- 여유 메모리는 마지막 메모리 진단 시 업로드에 사용할 수 있는 여유 메모리입니다.
- 순 메모리는 장치 소프트웨어 업데이트 작업이 실행된 후의 예상 여유 메모리입니다. 이때 장치에서 추가되거나 제거되도록 표시한 파일이 고려되지만 압축 전 또는 후 처리 작업은 고려되지 않습니다.

필드	설명/작업
작업 이름	장치 소프트웨어 업데이트를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. • 작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.

필드	설명/작업
적용 대상	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. • 파티션의 장치로 제한 — 파티션을 선택합니다. 지정된 파티션에 있는 장치에서만 소프트웨어 이미지가 업데이트됩니다. 장치 제한 설정에 대한 추가 정보를 보려면 자세히... 링크를 클릭합니다. • CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다(IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>
시작 날짜	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 가능한 한 빨리 시작(기본값) • 시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	<p>작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.</p>
주석	<p>작업에 대한 주석을 입력합니다.</p>
작업 옵션	
세션 로그	<p>디버깅 로그를 저장하려면 "전체 장치 세션 로그 저장" 상자를 선택합니다. 이렇게 하면 실패한 스냅샷을 디버깅할 때 유용하지만 많은 양의 데이터가 저장될 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>
배포 테이블	<p>한 장치에 소프트웨어를 배포하는 경우 배포 테이블이 열립니다. 자세한 내용은 418페이지의 "배포 테이블"을 참조하십시오.</p>

필드	설명/작업
이미지 집합	배포하고 있는 소프트웨어 이미지의 이름을 선택합니다.
슬롯	소프트웨어를 배포할 슬롯을 선택합니다. NA 데이터베이스에 현재 있는 슬롯이 모두 표시됩니다.
메모리 준비	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 없음 — 소프트웨어를 업데이트하기 전에 장치 메모리를 준비하지 않습니다. 새 소프트웨어를 받는 데 충분한 메모리가 장치에 있는지 수동으로 확인해야 합니다. 이렇게 하지 않으면 작업이 실패합니다. • 선택한 슬롯의 장치 메모리 압축 — 소프트웨어를 배포하기 전에 NA는 장치에서 지원하는 경우 Cisco IOS 압축 명령과 같은 명령을 실행하여 메모리를 압축합니다. 장치에서 파일이 제거되지는 않습니다. 하지만 이 경우에도 사용자가 업데이트에 사용할 수 있는 메모리가 충분한지 확인해야 합니다. • 선택한 슬롯에서 파일을 삭제한 다음 메모리 압축 — 소프트웨어를 배포하기 전에 NA는 플래시에서 모든 부팅 이미지(모든 .bin, .tar, .Z 및 .W 파일)를 삭제한 다음 장치에서 압축 명령을 지원하는 경우 메모리를 압축합니다. (참고: 소프트웨어 배포 작업이 실패한 후 장치에 정전이 발생하거나 장치가 재부팅된 경우 장치를 부팅할 수 없는 상태가 될 수도 있습니다.)
확인	이 옵션을 선택하면 장치에서 사용할 수 있는 명령을 사용하여 이미지가 확인됩니다. 장치의 MD5 체크섬이 데이터베이스에 저장된 MD5 체크섬과 비교됩니다. 장치에서 이 옵션을 지원하지 않는 경우에는 드라이버에서 이미지에 대해 확인 명령을 실행합니다.
재부팅	소프트웨어 배포 후 스크립트를 실행하여 장치를 재부팅하려면 "소프트웨어 배포 후 장치 재부팅" 상자를 선택합니다. 재부팅 후 구성의 스냅샷을 작성하기 전에 일시 중지할 시간(초)을 "재부팅 후 일시 중지" 상자에 입력합니다. 기본 값은 60초입니다.
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본 값은 60분입니다.

필드	설명/작업
장치 자격 증명 옵션 장치 자격 증명 옵션은 장치 페이지의 관리 설정 아래에서 구성된 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 56페이지의 "장치 액세스 페이지 필드" 를 참조하십시오.	
장치 자격 증명	서버 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다. <ul style="list-style-type: none"> • 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) • 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력하라는 메시지가 표시됩니다. • 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명에 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
승인 옵션 승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	

필드	설명/작업
재시도 수	<p>작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	<p>다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.</p>
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

배포 테이블

배포 테이블에서는 한 장치에 소프트웨어를 배포하기 위한 고급 옵션을 제공합니다. 데이터는 마지막 파일 시스템 진단을 기반으로 합니다. 배포 테이블에서는 부팅 또는 OS 이미지로 선택할 수 있는 각 파일 시스템의 이미지를 보여 줍니다. 한 이미지가 둘 이상의 파일 시스템에 있으면 NA는 마지막으로 업로드된 이미지가 부팅할 이미지가 됩니다.

장치에 없는 항목에 대한 부팅 및 OS 라디오 버튼은 처음에 비활성화되어 있습니다. 장치에 업로드될 이미지를 선택할 때 이러한 이미지를 부팅 또는 OS 이미지로 선택할 수 있게 됩니다.

라디오 버튼을 사용하여 부팅 또는 OS 이미지로 설정할 이미지를 선택할 수 있습니다. 그러나 장치에 현재 있거나 업로드되도록 선택한 이미지만 부팅 또는 OS 이미지로 선택할 수 있습니다. 또한 이미지를 부팅 이미지나 OS 이미지 중 하나로만 설정할 수 있고 둘 다로 설정할 수는 없습니다. 흐리게 표시된 열의 라디오 버튼을 사용하면 부팅 및 OS 이미지를 모두 선택하거나 선택 취소할 수 있습니다.

참고: 확인 옵션을 선택하면 장치에서 사용할 수 있는 명령을 사용하여 이미지가 확인됩니다. 장치의 MD5 체크섬이 데이터베이스에 저장된 MD5 체크섬과 비교됩니다. 장치에서 이 옵션을 지원하지 않는 경우에는 드라이버에서 이미지에 대해 확인 명령을 실행합니다.

필드	설명/작업
파일 시스템 진단 실행 링크	장치에서 실행될 파일 시스템 진단을 예약할 수 있는 새 작업 - 진단 실행 페이지가 열립니다. (자세한 내용은 397페이지의 "진단 실행 작업 페이지 필드" 를 참조하십시오.)
사전 처리 작업	소프트웨어를 배포하기 전에 NA는 장치에서 지원하는 경우 Cisco IOS 압축 명령과 같은 명령을 실행하여 메모리를 압축합니다. 장치에서 파일이 제거되지는 않습니다. 하지만 이 경우에도 사용자가 업데이트에 사용할 수 있는 메모리가 충분한지 확인해야 합니다.
이름	장치의 이름을 표시합니다.
크기	다운로드할 소프트웨어 이미지의 크기를 표시합니다.
부팅/OS	장치에 없는 항목에 대한 부팅 및 OS 라디오 버튼은 처음에 비활성화되어 있습니다. 장치에 업로드될 이미지를 선택할 때 이러한 이미지를 부팅 이미지 또는 OS 이미지로 선택할 수 있습니다. 참고: 일부 장치에는 OS 이미지와 별도로 부팅 이미지가 있으며, 이 이미지를 흔히 대형 이미지와 상반된 킥스타트 이미지라고 합니다. 또한 일부 장치는 Boot 명령을 사용하여 재부팅 시 사용할 이미지 파일을 설정합니다. 이미지 파일이 복사된 후 추가 명령을 실행하지 않으려면 모든 라디오 버튼을 선택하지 마십시오.
준수	보안 위험, 사전 프로덕션 및 사용되지 않음과 같은 소프트웨어 이미지의 준수 수준을 표시합니다. 이 필드는 기본적으로 표시되지 않습니다. 자세한 내용은 80페이지의 "사용자 인터페이스 페이지 필드" 를 참조하십시오.
파일 시스템 이름(예: 플래시)	파일 시스템에서 사용되지 않는 전체 여유 메모리 양을 표시합니다.
사후 처리 작업	소프트웨어를 배포한 후에 NA는 장치에서 지원하는 경우 Cisco IOS 압축 명령과 같은 명령을 실행하여 메모리를 압축합니다. 장치에서 파일이 제거되지는 않습니다. 하지만 이 경우에도 사용자가 업데이트에 사용할 수 있는 메모리가 충분한지 확인해야 합니다.
확인란	장치에 있는 파일이 강조 표시되어 있습니다. 이 파일을 장치에 배포하지 않으려면 이 확인란을 선택하십시오.
추가	소프트웨어 배포의 파일, 이미지 집합 및 대상을 표시합니다.

필드	설명/작업
삭제	삭제될 파일이 있으면 표시됩니다.
확인	이 옵션을 선택하면 장치에서 사용할 수 있는 명령을 사용하여 이미지가 확인됩니다. 장치의 MD5 체크섬이 데이터베이스에 저장된 MD5 체크섬과 비교됩니다. 장치에서 이 옵션을 지원하지 않는 경우에는 드라이버에서 이미지에 대해 확인 명령을 실행합니다.
재부팅	소프트웨어 배포 후 스크립트를 실행하여 장치를 재부팅하려면 "소프트웨어 배포 후 장치 재부팅" 상자를 선택합니다. 재부팅 후 구성의 스냅샷을 작성하기 전에 일시 중지할 시간(초)을 "재부팅 후 일시 중지" 상자에 입력합니다. 기본값은 60초입니다.

참고: NA는 여러 이미지가 설치된 장치에서 부팅 이미지 및/또는 OS 이미지로 이미지를 지정하는 기능을 제공합니다. 이 기능은 Cisco IOS를 실행하는 장치에서만 사용할 수 있습니다.

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

참고: 배포하도록 선택한 이미지가 장치의 사용 가능한 여유 디스크 공간에 들어가지 않으면 오류 메시지가 표시됩니다. 작업으로 돌아가서 변경하거나 소프트웨어를 배포할 수 있습니다. 디스크 공간 계산에 오류가 있을 수도 있습니다.

가져오기 작업 페이지 필드

가져오기 작업을 통해 CSV(쉼표로 구분된 값) 형식을 사용하여 장치와 장치 암호 데이터를 가져올 수 있습니다. 네트워크 전체 장치 암호 규칙을 먼저 생성한 다음 장치를 가져오는 것이 좋습니다. 한 파일에서 장치별 데이터의 집합을 가져온 다음 두 번째 파일에서 장치 암호 데이터를 가져올 수도 있습니다.

필드	설명/작업
장치 가져오기 관리 설정 링크	NA 작업 제한 설정, 워크플로 활성화, Syslog 구성 등을 수행할 수 있는 관리 설정 페이지(서버 탭)가 열립니다.
작업 이름	가져오기를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
파티션	파티션을 선택할 수 있는 드롭다운 메뉴가 제공됩니다. 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오. <p>참고: 사이트 값은 CSV(쉼표로 구분된 값) 파일의 SiteName 값에 의해 오버라이드됩니다. CSV 장치 및 암호 파일에 대한 내용은 168페이지의 "CSV 장치 및 암호 데이터 파일 생성"을 참조하십시오.</p>
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.

필드	설명/작업
작업 옵션	
파일 가져오기	가져올 CSV(심표로 구분된 값) 파일의 이름을 입력합니다. 파일이 로컬 시스템에 있으면 찾아보기 버튼을 사용하여 파일을 찾을 수 있습니다. NA 서버에 있는 파일의 전체 경로를 포함해야 합니다. 템플릿을 사용하여 데이터 유형 필드(아래 참조)에 새 CSV 파일을 생성하는 경우 로컬 하드 드라이브에 파일을 저장해야 합니다. 자세한 내용은 168페이지의 "CSV 장치 및 암호 데이터 파일 생성" 을 참조하십시오.
데이터 유형	<p>다음 옵션 중 하나를 선택하고 가져올 데이터를 입력합니다.</p> <ul style="list-style-type: none"> • 장치 — 장치 CSV 템플릿에는 IP 주소, 호스트 이름 및 장치 그룹 이름과 같이 네트워크 장치에서 NA에 입력할 수 있는 다양한 필드가 포함되어 있습니다. • 장치 그룹 — 장치 그룹 CSV 템플릿에는 장치 그룹 이름, 파티션 이름 및 상위 장치 그룹 이름 등 네트워크 장치 그룹을 NA에 입력할 수 있도록 하는 다양한 필드가 포함되어 있습니다. • 암호 — 장치 암호 CSV 템플릿은 장치 암호 규칙을 사용하지 않는 경우에만 필요합니다. <p>템플릿을 사용하여 새 CSV 파일을 생성하는 경우 장치 또는 암호 CSV 템플릿 파일의 링크를 클릭합니다. 파일이 열리면 로컬 하드 드라이브에 다른 이름으로 파일을 저장한 다음 장치 데이터나 암호에 맞게 저장된 파일을 수정합니다.</p>

필드	설명/작업
Syslog 구성	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •NA Syslog 서버에 기록할 장치 설정 •장치가 syslog 릴레이에 로그되므로 올바른 로깅 수준 설정 •syslog를 구성 안 함 <p>NA에서 가져올 CSV 파일과 연관된 장치의 장치 드라이버를 검색하게 하려면 "새로 가져온 장치에서 드라이버 검색 실행" 상자를 선택합니다. 이 옵션을 사용하려면 유효한 장치 암호와 커뮤니티 문자열이 필요합니다. 따라서 네트워크에 대한 암호와 장치 암호 규칙을 이미 설정했고 디버깅했거나 장치 암호 정보가 포함된 두 번째 파일을 가져오는 경우에만 네트워크에 이 옵션을 사용해야 합니다.</p> <p>NA에서 지난 45일 동안 성공적으로 액세스하거나 가져오지 않은 장치를 비활성화하려면 비활성 또는 누락 장치 비활성화 확인란을 선택합니다.</p>
사전 처리 명령	<p>NA에서 전체 프로세스를 자동화하고 예약하려면 데이터를 가져오기 전에 실행할 스크립트 파일의 이름과 경로를 입력합니다. 이 필드에는 서버의 명령/셸 콘솔에서 실행되는 실행 가능한 전체 명령이 필요합니다. 예를 들어 필터가 Windows용 PERL 스크립트인 경우 PERL을 지정해야 합니다(예: perl c:/filter.pl).</p>
로그 파일 이름	<p>NA에서 가져오기 작업에 대한 정보를 쓸 파일의 이름을 입력합니다. 로그 파일은 가져오기 문제를 디버깅할 때 유용합니다. NA에서 기존 로그 파일에 이 데이터를 추가하게 하려면 "로그 파일에 추가"를 선택합니다. 이렇게 하지 않으면 NA에서 로그 파일의 기존 데이터를 덮어씁니다.</p>
장치 원본	<p>이 가져오기 파일에 지정할 이름을 입력합니다. 이 필드는 반복적으로 데이터를 가져오고 여러 데이터 소스와 날짜를 구분해야 하는 경우에 유용합니다.</p>
추산 기간	<p>이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본 값은 60분입니다.</p>
승인 옵션	<p>승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.</p>

필드	설명/작업
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.

필드	설명/작업
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < > 번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

네트워크 장치 감지 작업 페이지 필드

네트워크 장치 감지를 통해 NA 관리 아래에 배치할 장치를 네트워크에서 찾을 수 있습니다. IP 주소 범위를 제공하면 NA에서는 네트워크를 검색하여 장치를 찾습니다. 새로 검색된 장치는 적절한 장치 드라이버와 함께 자동으로 추가됩니다. 또한 관리 설정 - 서버 페이지에서 기본 IP 주소 재할당 옵션을 선택하는 경우 장치에 여러 IP 주소와 인터페이스가 있으면 NA에서 올바른 IP 주소를 장치에 자동으로 할당합니다. 이에 따라 장치가 시스템에 한 번만 입력됩니다. 작업 설정에 대한 자세한 내용은 [56페이지의 "장치 액세스 페이지 필드"](#) 및 [68페이지의 "서버 페이지 필드"](#)를 참조하십시오.

작업 페이지에서 드라이버 검색을 선택하는 경우 NA는 시스템에 장치를 추가한 후 장치를 폴링하여 장치 유형을 확인하고 장치를 관리할 적절한 장치 드라이버를 할당합니다. 그런 다음 NA는 장치의 스냅샷을 작성하고 장치에서 데이터베이스로 구성과 자산 정보를 다운로드합니다.

지원되지 않는 호스트의 경우 그룹도 또한 생성되어 시스템에 추가됩니다(인벤토리). 지원되지 않는 장치가 활성으로 추가되어 장치의 라이선스에 집계되지 않도록 하고 이러한 장치가 포함될 수 있는 인벤토리에 대한 운영 수행을 방지하기 위해 지원되지 않는 호스트의 모든 장치는 기본적으로 비활성으로 설정됩니다.

이러한 장치에 대해 작업을 수행하려면 먼저 해당 장치를 활성화해야 합니다. 다음 중 하나에서 장치를 활성화할 수 있습니다.

- 장치 세부사항 페이지, 프로비전 메뉴 사용(장치 활성화 옵션)
- 그룹 장치 페이지, 확인란을 사용하여 장치를 선택한 다음 작업 드롭다운 메뉴에서 활성화 옵션을 선택할 수 있음

네트워크 장치 감지 작업을 실행할 때 작업 정보 페이지에 다음이 표시됩니다.

- **활성 노드** — 활성 노드는 SNMP 스캔이나 Nmap 스캔에 응답한 IP 주소입니다. NA에서 관리할 수 있는 노드는 활성으로 간주됩니다. 지원되는 장치의 목록은 [HP Network Automation Device Driver Reference](#)를 참조하십시오.

- 비활성 노드 — 비활성 노드는 SNMP 스캔이나 Nmap 스캔 또는 두 스캔 모두에 응답하지 않은 IP 주소입니다. NA에서 잘못된 커뮤니티 문자열을 사용하여 장치를 쿼리하는 경우 장치가 SNMP 스캔에 응답하지 않을 수도 있습니다.
- 지원되지 않는 호스트 — 지원되지 않는 호스트는 SNMP 스캔이나 Nmap 스캔에 응답한 IP 주소입니다. 그러나 SNMP의 경우 NA에서 지원하지 않는 SysOID를 반환했고, Nmap의 경우에는 운영 체제 지문이 NA에서 지원하는 일치 항목을 반환하지 않았습니다.
- 기존 장치 — 기존 장치는 장치의 기본 IP 주소나 IP 주소가 BasicIP 진단의 결과로 데이터베이스에 표시되므로 장치의 IP 주소가 NA에 이미 알려져 있으며 시스템 안에 있음을 나타냅니다.

스캔 방식

두 가지 유형의 IP(Internet Protocol) 트래픽이 있습니다.

- UDP(User Datagram Protocol) — UDP는 간단한 메시지 기반의 연결 없는 프로토콜입니다. UDP를 사용하는 경우 패킷이 네트워크를 통해 청크로 전송됩니다. 일반적으로 UDP는 안정성이 떨어지며 도착하는 패킷의 순서가 보장되지 않습니다.
- TCP(Transmission Control Protocol) — TCP는 연결 지향 프로토콜입니다. TCP는 매우 안정적이며 패킷이 연결을 통해 수신되는 순서가 보장됩니다.

SNMP 스캔은 UDP를 사용합니다. SNMP는 네트워크 장치를 식별하기 위해 알려진 SYSOID를 사용하여 시스템에 연결을 시도합니다. SNMP 스캔 방식은 각 시스템과 여러 연결을 설정할 필요가 없기 때문에 네트워크에 미치는 영향이 적습니다. 또한 SNMP는 빠르지만 스캔되는 IP 주소마다 모든 암호 규칙이 시도되므로 암호 규칙이 많은 경우 처리가 어려울 수 있습니다. SNMP가 성공하려면 로그인 자격 증명(커뮤니티 문자열)도 필요합니다.

Nmap 스캔은 TCP를 사용하지만 일부 작업의 경우 UDP를 사용하도록 구성될 수 있습니다. Nmap이 포트 스캐너이기 때문에 네트워크를 스캔하지 않으려는 경우 SNMP 스캔 방식을 선택해야 합니다. 또한 Nmap은 다양한 포트를 테스트하기 위해 장치와 많은 연결을 설정합니다.

Nmap은 장치에 로그인하지 않으므로 로그인 자격 증명이 필요하지 않습니다. Nmap은 네트워크 구성과 스캔할 IP 주소에 따라 빠를 수도 있고 느릴 수도 있습니다. IP 주소(예: 192.168.0.0)의 스캔은 매우 느릴 수 있습니다. 해당 조직에 있는 IP 주소 범위만 스캔하는 것이 좋습니다.

참고: 많은 조직이 진행 중인 네트워크 스캔을 감지하는 경우 알람을 보내는 모니터링 시스템을 사용합니다. Nmap을 사용하여 네트워크 장치를 감지하는 경우 IT 팀이 예정된 활동을 완전히 알고 있어야 합니다.

IP 주소 범위 정의

하나 이상의 IP 주소 포함 범위를 지정해야 합니다. 두 가지 방식으로 범위를 정의할 수 있습니다.

- CIDR(Classless InterDomain Routing) 표기법 — CIDR은 IP 주소의 블록이나 범위를 나타냅니다. 예를 들어, 10.255.1.0/24는 10.255.1.0에서 10.255.1.255(포함)까지의 IP 주소 범위를 나타냅니다. 총 256개의 IP 주소입니다. 10.255.1.0/24 CIDR 표기법의 /24는 CIDR 블록의 접두사를 구성하는 비트 수를 나타냅니다. 이 경우에는 24비트입니다. 블록의 나머지 부분(최종 8비트)은 와일드카드로 간주됩니다. 다른 예는 다음과 같습니다.
 - 192.168.100.1/32는 단일 호스트 192.168.100.1입니다. (모든 32비트가 와일드카드 비트 없이 접두사를 구성합니다.)
 - 172.16.0.0/16은 172.16.0.0에서 172.16.255.255까지의 매우 큰 범위입니다. 이렇게 큰 범위는 검색하지 않는 것이 좋습니다.
 - 10.255.0.0/23은 적당하게 큰 범위입니다. 이 범위는 10.255.0.0에서 10.255.1.255까지이며 512개의 IP 주소를 포함합니다.

- 범위가 지정된 입력 — IP 주소 블록은 최저-최고 표기법으로 표현됩니다(예: 10.255.1.0 - 10.255.1.255). IP 주소를 하나만 입력할 수 있습니다(예: 192.168.100.1). 제외 범위도 지정할 수 있습니다. 이에 따라 특정 주소나 주소 범위를 마스킹하여 네트워크 장치 감지에서 제외할 수 있습니다. 예를 들어 10.255.1.0/24 범위를 스캔할 수 있습니다. 그러나 스캔하지 않을 10.255.1.10에서 10.255.1.20까지의 프린터가 있는 경우 포함 범위는 10.255.1.0/24이고 제외 범위는 10.255.1.10 -10.255.1.20입니다.

필드	설명/작업
작업 이름	네트워크 장치 감지를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.
작업 옵션	
최대 노드 수	검색할 IP 주소의 수를 입력합니다. 최대값은 1024입니다. 허용되는 최대값보다 많은 노드가 있는 작업은 실패합니다.

필드	설명/작업
포함	IP 주소나 CIDR(Classless Inter-Domain Routing) 범위 포함(예: 192.168.1.0-192.168.2.0 또는 192.168.31.0/24)을 오른쪽 상자에 입력하고 << 검색 범위 추가 버튼을 클릭합니다. 범위가 포함됩니다. 검색 범위 삭제 버튼을 사용하여 범위를 삭제할 수 있습니다.
제외	IP 주소나 CIDR(Classless Inter-Domain Routing) 범위 제외(예: 192.168.1.0-192.168.2.0 또는 192.168.31.0/24)를 오른쪽 상자에 입력하고 << 제외 범위 추가 버튼을 클릭합니다. 범위가 포함됩니다. 제외 범위 삭제 버튼을 사용하여 범위를 삭제할 수 있습니다.
스캔 방식	다음 스캔 방식 중 하나를 선택하거나 둘 다 선택합니다. <ul style="list-style-type: none"> •SNMP(기본값) •Nmap (참고: 스캔할 네트워크 범위를 식별할 때 신중하게 고려해야 합니다. 일부 네트워크 토폴로지에서는 스캔 시간이 매우 오래 걸릴 수 있습니다. 또한 인터넷 주소는 스캔하지 않는 것이 좋습니다.) 스캔 방식에 대한 자세한 내용은 427페이지의 "스캔 방식" 을 참조하십시오.
암호 규칙 플백	이 옵션을 선택하면(기본값) SNMP 스캔에 커뮤니티 문자열이 필요합니다. 이러한 커뮤니티 문자열에 암호 규칙 플백이 사용됩니다.
파티션	드롭다운 메뉴에서 파티션을 선택합니다. 파티션에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.)
장치 그룹 이름	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •기본 그룹 이름(DetectedNetworkDevices<nnn>, 여기서 nnn은 작업 ID 임)을 사용하거나 드롭다운 메뉴에서 장치 그룹을 선택합니다. •추가된 장치에 대한 장치 그룹 이름을 입력합니다(기본값). 참고: 네트워크 장치 감지 작업을 사용할 때 네트워크 스캔에 반응했지만 알려진 OS를 반환하지 않은 장치에서 새 그룹이 생성될 수 있습니다.
드라이버 검색	이 옵션을 선택하면(기본값) 장치가 감지된 후 장치 드라이버가 검색됩니다.

필드	설명/작업
장치 자격 증명 옵션	
장치 자격 증명	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 네트워크 전체 암호 규칙 사용 • 작업별 자격 증명 사용 — 사용자 이름, 암호 및 SNMP 커뮤니티 문자열 정보를 입력합니다.
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.

필드	설명/작업
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 검색된 노드에 대한 자세한 정보가 표시됩니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

중복 방지 작업 페이지 필드

CSV(쉼표로 구분된 값) 파일이나 커넥터를 사용하여 장치를 NA로 가져오는 경우 NA 데이터베이스에 중복 장치가 생성될 수 있습니다. 예를 들어, HP OpenView 또는 CiscoWorks와 같은 서로 다른 관리 시스템에서 장치를 가져오는 경우 이러한 관리 시스템이 서로 다른 관리 IP 주소를 사용하여 동일한 장치를 참조할 수 있습니다.

중복 방지 작업을 통해 장치 중복 문제를 해결할 수 있습니다. 네트워크 장치 감지 작업에서는 장치 중복 문제를 자동으로 해결하지 않습니다. 자세한 내용은 [426페이지의 "네트워크 장치 감지 작업 페이지 필드"](#)를 참조하십시오.

필드	설명/작업
작업 이름	중복 방지를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.

필드	설명/작업
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~ 5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기 열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.

필드	설명/작업
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

OS 분석 작업 페이지 필드

OS 분석 작업 페이지에서는 sysoid(장치 모델의 고유 식별자), OS 버전, 플래시 저장 옵션, 모듈 등의 정보와 같은 Cisco 장치에 대한 데이터를 수집합니다. 이 정보는 소프트웨어 권장 사항을 생성하는 데 사용됩니다. OS 분석 작업을 실행한 후에는 작업 정보 페이지에서 "이 장치에 대한 OS 권장 사항을 보십시오." 링크를 클릭합니다. 자세한 내용은 [293페이지의 "장치 소프트웨어 이미지 권장 사항 페이지 필드"](#)를 참조하십시오.

필드	설명/작업
작업 이름	OS 분석을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.

필드	설명/작업
주석	작업에 대한 주석을 입력합니다.
작업 옵션	
세션 로그	전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버깅할 때는 맨 먼저 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.)
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본 값은 60분입니다.
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.

필드	설명/작업
예약 옵션	
재시도 수	<p>작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

포트 스캔 페이지 필드

Nmap은 네트워크 장치 탐색에 사용됩니다. Nmap은 장치의 포트를 검색하고 열린 포트와 해당 포트에서 제공하는 서비스에 대한 세부 사항을 반환하는 데 사용할 수 있습니다. 포트 스캔 작업을 실행하여 다음을 수행할 수 있습니다.

- 장치에서 열려 있거나 닫힌 포트가 어느 것인지 쉽게 확인
- TCP 스택, OS 검색 및 기타 Nmap 제공 서비스에 따라 장치의 취약성 파악

포트 스캔 결과가 장치 세부사항 페이지의 보기 메뉴에 표시됩니다(보기 --> 진단 --> NA 포트 스캔). 장치 세부사항 보기에 대한 자세한 내용은 [250페이지의 "장치 세부사항 페이지 필드"](#)를 참조하십시오.

포트 스캔 작업 설정을 지정하려면 [55페이지의 "장치 액세스"](#)를 참조하십시오.

참고: 포트 스캔 작업이 실패할 경우 Nmap이 올바르게 구성되지 않을 수도 있습니다. Nmap 유틸리티 경로 입력에 대한 자세한 내용은 [56페이지의 "장치 액세스 페이지 필드"](#)를 참조하십시오. Nmap 설치에 대한 자세한 내용은 *Network Automation 9.10 업그레이드 및 설치 설명서*를 참조하십시오.

포트는 사실상 수신용으로 열려 있는 소프트웨어 기반 소켓입니다. 진단 세부사항은 진단 검색 페이지를 사용하여 검색할 수 있습니다. 자세한 내용은 [617페이지의 "진단 검색 페이지 필드"](#)를 참조하십시오.

필드	설명/작업
작업 이름	포트 스캔을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. • 작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.

필드	설명/작업
적용 대상	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>
시작 날짜	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	<p>작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.</p>
주석	<p>작업에 대한 주석을 입력합니다.</p>
작업 옵션	
세션 로그	<p>전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버깅할 때는 맨 먼저 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.)</p>
추산 기간	<p>이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.</p>

필드	설명/작업
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기 열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). •주기적으로 — 반복 간격(분)을 지정합니다. •매일 — 작업이 매일 지정된 시간에 발생합니다. •매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. •매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.

필드	설명/작업
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

장치 프로비전 작업 페이지 필드

장치 프로비전 작업에서는 장치에 장치 템플릿을 적용합니다. 장치 템플릿 생성에 대한 자세한 내용은 [155페이지의 "장치 템플릿"](#)을 참조하십시오.

참고: 장치 템플릿과 해당 템플릿을 적용할 장치가 일치하지 않으면 작업이 실패합니다.

필드	설명/작업
작업 이름	장치 프로비전을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV 파일 — 장치 목록을 포함하는 CSV 파일 이름을 입력하거나 해당 파일을 찾습니다. 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. CSV 파일을 사용할 때만 여러 장치에 대해 장치 프로비전 작업을 실행할 수 있으며, 작업이 완료된 후 새로운 기본 IP 주소를 장치에 할당할 수도 있습니다. 자세한 내용은 159페이지의 "템플릿 구성 편집 페이지"를 참조하십시오.
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~ 5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.

필드	설명/작업
주석	작업에 대한 주석을 입력합니다.
작업 옵션	
세션 로그	전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버깅할 때는 맨 먼저 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.)
장치 템플릿	드롭다운 메뉴에서 장치 템플릿을 선택합니다.
준수 옵션	이 옵션을 선택하면 NA는 장치를 프로비전하기 전에 정책 준수를 테스트합니다.
상태 옵션	이 옵션을 선택하면 프로비전 시 장치 상태가 활성으로 설정됩니다.
데이터 복사 옵션	이 옵션을 선택하면 장치 템플릿의 추가 정보가 장치에 복사됩니다.
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.
사전 작업/사후 작업 스냅샷 옵션	
사전 작업 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨
사후 작업 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨 •별도 작업으로 예정됨
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	

필드	설명/작업
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기 열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). •주기적으로 — 반복 간격(분)을 지정합니다. •매일 — 작업이 매일 지정된 시간에 발생합니다. •매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. •매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.

필드	설명/작업
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

장치 컨텍스트 추가 작업 페이지 필드

컨텍스트란 장치 내부의 장치를 말합니다. 컨텍스트는 하드웨어(모듈 및 슬롯 포함) 또는 가상일 수 있습니다. NA 7.60 이전의 NA에서는 컨텍스트에 IP 주소를 지정해야만 컨텍스트를 관리할 수 있었습니다. 이제는 더 이상 컨텍스트에 IP 주소를 지정할 필요가 없습니다. NA가 NA 모듈 상태 진단을 사용하여 상위 장치에서 컨텍스트를 자동으로 검색합니다. 발견된 컨텍스트가 NA 모듈 상태 진단의 일부로서 장치로 모두 추가되며 연결 경로가 자동으로 구성됩니다. 장치 통과 연결에 대한 자세한 내용은 [313페이지의 "새 IP 주소 페이지\(새 통과 연결\)"](#)를 참조하십시오.

NA 모듈 상태 진단은 내부 장치 관계도 자동으로 추가합니다. 사용자 정의 장치 관계 추가 및 제거에 대한 자세한 내용은 [299페이지의 "장치 관계 페이지 필드"](#)를 참조하십시오.

Cisco FWSM(방화벽 서비스 모듈)의 경우 CiscoFWSM은 Cisco Catalyst 장치 내 모듈입니다. Cisco FWSM에는 컨텍스트가 포함될 수 있습니다. 따라서 각각의 Cisco FWSM과 관련 컨텍스트마다 고유의 구성이 있으므로 Cisco FWSM과 관련 컨텍스트가 NA에 장치로 나타납니다.

참고: 상위 장치에 연결하고 컨텍스트에 액세스하기 위한 명령을 실행하는 대신에, NA 장치 드라이버는 상위 장치에 연결하고 필요한 스크립트를 자동으로 실행하여 컨텍스트와의 연결을 처리합니다. 따라서 컨텍스트가 독립 실행형 장치로 나타납니다.

NA 인터페이스 장치를 실행할 때 NA가 컨텍스트를 자동으로 검색하고 장치를 추가합니다. NA 인터페이스 진단에서 컨텍스트가 제거되었음을 감지하는 경우 해당 장치가 비활성 상태로 표시됩니다. 나중에 NA 인터페이스 진단에서 해당 장치를 발견할 경우 장치가 다시 활성화되므로 장치 이력이 유지됩니다.

참고: 장치 컨텍스트 제거는 장치 컨텍스트를 추가할 때와 동일한 작업 페이지를 사용합니다. 하지만 NA는 드라이버에서 필요한 변수를 동적으로 가져옵니다.

필드	설명/작업
작업 이름	장치 컨텍스트 추가를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	장치 — 작업을 실행할 IP 주소 또는 호스트 이름을 입력합니다. 장치 컨텍스트 작업(추가 및 제거)은 단일 장치에 대해서만 실행할 수 있습니다.
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.
작업 옵션	
세션 로그	전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버깅할 때는 맨 먼저 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.)

필드	설명/작업
변수	<p>변수는 장치 드라이버에서 정의되며 실행 시 NA에 표시됩니다. 따라서 변수는 각 장치마다 다릅니다. CiscoPIX FWSM 장치의 경우 장치 컨텍스트를 생성하는 데 세 가지 변수가 필요합니다.</p> <ul style="list-style-type: none"> • 컨텍스트 이름 — 생성할 장치 컨텍스트의 이름을 입력합니다. • 구성 위치 — 장치 컨텍스트의 구성 위치를 입력합니다. 이 경우 구성 위치는 구성 제공 방법을 지정하는 프로토콜 집합입니다. 예를 들어 구성이 로컬 디스크에 있으면 드롭다운 메뉴에서 디스크를 선택해야 할 것입니다. • 구성 파일 이름 — default.cfg와 같은 구성 파일 이름을 입력합니다.
추산 기간	<p>이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.</p>
승인 옵션	
승인 옵션	<p>승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.</p>
승인 요청	<p>작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.</p>
승인 오버라이드	<p>작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.</p>
드래프트로 저장	<p>이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.</p>

필드	설명/작업
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	사용할 수 없음
반복 범위	한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다. <ul style="list-style-type: none"> •종료 날짜 없음(기본값) •< >번 발생 후 종료 — 반복 횟수를 입력합니다. •종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.

VLAN 작업 페이지 필드

NA에서는 VLAN 엔티티와 트렁크 포트를 프로비전할 수 있습니다. 다음을 수행할 수 있습니다.

- 새 VLAN 생성
- VLAN 이름 편집
- VLAN 포트 할당 편집
- VLAN 주석 편집(장치가 아닌 데이터베이스에서만)
- 트렁크 포트 구성(자세한 내용은 [455페이지의 "트렁크 포트 구성"](#) 참조)

새 장치 VLAN 페이지에서 새 VLAN을 생성하거나 VLAN 이름 및 포트 할당을 편집하면 장치에 대한 변경을 수행하는 새 VLAN 작업이 예약됩니다. 자세한 내용은 [282페이지의 "VLAN 생성 및 편집"](#)을 참조하십시오.

참고: NA에서는 데이터베이스를 요청한 VLAN 변경 내용으로 업데이트하지 않습니다. 대신에 NA에서는 변경 내용을 새 VLAN 작업의 결과로 캡처하기 위해 사후 스냅샷 작업과 VLAN 데이터 수집 진단 작업을 예약합니다.

필드	설명/작업
작업 이름	VLAN 추가를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. • 작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기" 를 참조하십시오.

필드	설명/작업
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 가능한 한 빨리 시작(기본값) • 시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.
작업 옵션	
세션 로그	전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버깅할 때는 맨 먼저 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.)
VLAN 편집	편집된 VLAN의 이름을 표시합니다.
다른 이름으로 바꾸기	VLAN의 새 이름을 표시합니다.
포트 추가	추가할 포트를 표시합니다.
포트 제거	삭제할 포트를 표시합니다.
승인 옵션	
승인 옵션	승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.

필드	설명/작업
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	사용할 수 없음
반복 범위	한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다. <ul style="list-style-type: none"> •종료 날짜 없음(기본값) •< >번 발생 후 종료 — 반복 횟수를 입력합니다. •종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.

트렁크 포트 구성

인터페이스 세부사항 편집 페이지의 VLAN 트렁크 옵션을 사용하면 트렁크 포트를 구성할 수 있습니다. 특정 포트만 물리적 포트 및 포트 채널(집계된 링크) 등 트렁크 포트 구성할 수 있습니다. VLAN 인터페이스로 사용되는 포트와 루프백 포트는 트렁크 포트 구성할 수 있습니다.

VLAN 트렁크 옵션은 인터페이스 세부사항 편집 페이지의 VLAN 트렁크 옵션을 선택할 때 표시되는 축소 가능한 행 집합입니다. 다음은 표시되는 필드입니다.

- 기본 VLAN ID
- 멤버 VLAN

트렁크 포트에서 기본 VLAN 트래픽에는 태그가 지정되지 않습니다. 또한 트렁크 포트에서 수신되는 태그가 지정되지 않은 모든 패킷을 기본 VLAN의 패킷으로 간주됩니다.

참고: 기본 VLAN은 Cisco 용어입니다. ProCurve에는 기본 VLAN 용어가 사용되지 않습니다. 대신에 ProCurve에는 멤버 VLAN 용어가 사용됩니다. 따라서, 트렁크 포트 하나에서 사용할 수 있는 태그가 지정되지 않은 VLAN 멤버십은 하나뿐입니다. 기본 VLAN ID 용어와 멤버 VLAN 용어의 의미는 본질적으로 동일합니다.

트렁크 포트는 멤버 VLAN 필드에서 선택된 VLAN의 트래픽을 전달합니다. 선택되지 않은 모든 VLAN이 정리됩니다(트렁크 포트가 이전에 VLAN의 멤버였던 경우 VLAN 멤버십이 제거됨). VLAN 트렁크 옵션의 선택을 취소하면 포트가 기본 트렁크 포트 구성되고 이 포트가 기본 VLAN ID 필드에 지정된 VLAN에 할당됩니다.

참고: 트렁크 포트 옵션의 선택을 취소하면 포트가 현재 트렁크 포트일 경우 기본 VLAN ID를 입력하라는 메시지가 표시됩니다. 기본 VLAN ID는 트렁크 포트가 비 트렁크 포트일 때 포트에 할당될 ID입니다. VLAN ID를 입력하라는 메시지가 표시됩니다. VLAN ID를 입력하지 않으면 기본 VLAN ID가 사용됩니다. 기본 VLAN ID가 없으면 NA에서는 기본 VLAN ID를 장치로 보내지 않습니다. 따라서 장치가 해당 포트를 기본 VLAN(VLAN 1)에 할당합니다.

자세한 내용은 [271페이지의 "인터페이스 편집 세부사항 페이지 필드"](#)를 참조하십시오. VLAN 트렁크 포트 설정을 수정하면 장치에 변경 내용을 적용하기 위한 VLAN 작업이 생성됩니다. 자세한 내용은 [452페이지의 "VLAN 작업 페이지 필드"](#)를 참조하십시오.

Cisco.com에서 이미지 다운로드 작업 페이지

Cisco.com에서 이미지 다운로드 페이지를 통해 Cisco.com 소프트웨어 센터를 검색하여 다운로드할 수 있는 이미지를 확인할 수 있습니다. Cisco.com 소프트웨어 센터에는 Cisco의 상호 네트워킹 제품에 대한 시스템 소프트웨어 및 드라이버의 릴리스 버전이 포함되어 있습니다.

Cisco.com에서 이미지 다운로드 페이지를 열려면 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 소프트웨어 이미지를 클릭합니다. 소프트웨어 이미지 페이지가 열립니다. 페이지 위에서 Cisco.com의 이미지 집합 추가 링크를 클릭합니다.

필드	설명/작업
작업 이름	Cisco.com에서 이미지 다운로드가 표시됩니다. 해당하는 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
주석	작업에 대한 주석을 입력합니다.

필드	설명/작업
작업 옵션	
장치/그룹 목록 수정	<p>장치 목록 새로 고침 버튼을 클릭하면 Cisco가 장치 공급업체인 경우 위에서 선택된 모든 장치가 장치 목록 필드에 표시됩니다. 다른 공급업체의 장치가 선택된 경우 장치 목록 필드에 표시되지 않습니다. 일반 플랫폼 정보도 표시됩니다. 따라서 이후에 사용할 계획이거나 아직 NA에 추가하지 않은 장치의 소프트웨어 이미지를 찾을 수 있습니다.</p> <p>장치 목록 필드에서 항목을 선택할 때 다음 필드 간의 흐름이 발생합니다. 다음 필드에 대한 자세한 내용은 293페이지의 "장치 소프트웨어 이미지 권장 사항 페이지 필드"를 참조하십시오.</p> <ul style="list-style-type: none"> • 장치 목록 — 사용 가능한 일반 Cisco 장치가 모두 표시됩니다. • 버전 목록 — 선택된 장치에 대한 장치 버전 정보를 표시합니다. • 기능 목록 — 선택된 장치에 대한 기능 정보를 표시합니다.
선택 다운로드	<p>다운로드할 소프트웨어 이미지를 선택하고 작업 저장 버튼을 클릭합니다. 자세한 내용은 553페이지의 "소프트웨어 이미지 집합 추가 페이지 필드"를 참조하십시오.</p>
파티션에 적용	<p>드롭다운 메뉴에서 파티션을 선택합니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다.) 보안 또는 비즈니스상의 이유로 파티션을 생성한 경우, 파티션에 따라 소프트웨어 이미지를 분할할 수 있습니다. 소프트웨어 이미지가 모든 파티션에 사용 가능한 경우, 구성에 따라 소프트웨어 이미지가 "공유"(또는 "전역")로 표시됩니다.</p>
예약 옵션	
재시도 수	사용할 수 없음
반복 옵션	사용할 수 없음
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

완료되면 저장 버튼을 클릭해야 합니다. 작업 정보 페이지가 열립니다. 이 페이지에는 작업 상태, 영향을 받는 장치, 기간, 결과 정보 등의 자세한 작업 정보가 포함되어 있습니다.

장치 소프트웨어 백업 작업 페이지 필드

장치 소프트웨어 백업 작업을 통해 장치에서 NA 소프트웨어 이미지 리포지토리로 소프트웨어 이미지를 복사할 수 있습니다. 각 소프트웨어 이미지가 고유한 소프트웨어 이미지 집합에 포함되도록 지정하지 않는 한 복사된 모든 소프트웨어 이미지가 기존 소프트웨어 이미지 집합에 추가됩니다. 소프트웨어 이미지 집합의 이름은 지정된 소프트웨어 이미지 집합의 이름과 장치에 복사된 소프트웨어 이미지 집합의 이름을 결합하여 지정됩니다. 다음 사항에 유의해야 합니다.

- 고유 이름을 지정하는 경우 새 소프트웨어 이미지 집합의 이름이 생성됩니다.
- 소프트웨어 이미지 집합의 이름이 고유하지 않은 경우 소프트웨어 이미지 집합이 기존 소프트웨어 이미지 집합에 추가됩니다.
- 중복되는 소프트웨어 이미지는 기존 소프트웨어 이미지 집합에 추가되지 않습니다. 이에 따라 장치 소프트웨어 백업 작업이 실행될 때 경고 메시지가 나타납니다.

새 소프트웨어 이미지 집합이 생성되면 소프트웨어 이미지 집합의 속성이 소프트웨어 이미지 집합이 다운로드된 장치에 대해 알려진 정보와 일치합니다. 이 때문에 다운로드된 소프트웨어 이미지가 소프트웨어 이미지를 실행할 수 없는 장치에 적용되지 않습니다. 자세한 내용은 [776페이지의 "이미지 동기화 보고서 필드"](#)를 참조하십시오.

장치 소프트웨어 백업 작업 결과 페이지에는 모든 소프트웨어 이미지 집합 이름과 요구 사항을 확인할 수 있는 소프트웨어 이미지 집합의 목록에 대한 링크가 제공됩니다.

장치 소프트웨어 백업 작업 페이지를 열려면 보고서 아래의 메뉴 모음에서 이미지 동기화 보고서를 선택합니다. 이미지 동기화 보고서에서 하나 이상의 확인란을 선택한 다음 작업 드롭다운 메뉴에서 동기화 이미지 옵션을 선택합니다.

필드	설명/작업
작업 이름	장치 소프트웨어 백업을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.

필드	설명/작업
시작 날짜	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 가능한 한 빨리 시작(기본값) • 시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	<p>작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.</p>
주석	<p>작업에 대한 주석을 입력합니다.</p>
사용자 지정 1	<p>사용자 지정 데이터를 입력합니다.</p>
작업 옵션	
세션 로그	<p>전체 장치 세션 로그를 저장하려면 "전체 장치 세션 로그 저장" 확인란을 클릭합니다. 장치와 인터랙션하는 모든 작업이 세션 로그를 활성화하여 실행될 수 있습니다. 이 경우 작업 중에 장치와의 인터랙션에 대한 자세한 로그가 제공됩니다. 장치별 문제를 디버깅할 때는 맨 먼저 세션 로그를 확인해야 합니다. 세션 로그는 작업 중에 수행된 CLI, SNMP 및 모든 전송 프로토콜 작업에 대한 세부 사항을 제공합니다. (참고: 많은 양의 데이터를 저장할 수 있습니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.)</p>
기본 이미지 집합 이름	<p>다음 옵션 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 이름 사용 — 기본 이미지 집합 이름을 입력합니다. • 기존 사용 — 드롭다운 메뉴에서 기존 소프트웨어 이미지 집합을 선택합니다.
이미지 저장소	<p>NA 소프트웨어 리포지토리에 복사하고 있는 장치 및 소프트웨어 이미지가 표시됩니다. 다음 옵션 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 이미지 집합 그룹화 — 복사된 모든 소프트웨어 이미지가 새 소프트웨어 이미지 집합이나 기존 소프트웨어 이미지 집합에 추가됩니다. • 이미지를 고유 이미지 집합으로 구분 — 위에서 지정된(수동 또는 선택됨) 이미지 집합 이름이 새 이미지 집합의 기본 이름으로 사용됩니다. 전체 이름에는 원래 이름과 장치에서 복사된 소프트웨어 이미지의 이름이 포함됩니다.

필드	설명/작업
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	이 옵션은 이 작업에 사용할 수 없습니다.
작업 로깅	
작업 로깅	사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.

완료하면 작업 저장 버튼을 클릭해야 합니다. 작업 정보 페이지가 열립니다. 이 페이지에는 작업 상태, 영향을 받는 장치, 기간, 결과 정보 등의 자세한 작업 정보가 포함되어 있습니다.

정책 준수 확인 작업 페이지 필드

정책 준수 확인 작업을 통해 장치가 구성 정책이나 소프트웨어 수준 정책을 준수하는지 확인할 수 있습니다. 정책을 생성하거나 업데이트할 때만 정책 준수 확인 작업을 실행해야 합니다. 이렇게 하면 장치가 새로 생성된 정책을 준수하지 않는지 신속하게 확인할 수 있습니다.

참고: 기본적으로 NA는 구성 변경이 감지될 때마다 장치의 구성에 대한 준수 확인을 실행합니다. 구성된 경우 구성 변경이 적용된 정책을 위반하면 알림을 받습니다. 또한 전자 메일 주의, SNMP 트랩, 장치를 준수 상태로 되돌리는 명령 스크립트 실행 등의 다양한 자동화된 응답을 구성할 수 있습니다.

필드	설명/작업
작업 이름	정책 준수 확인을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>

필드	설명/작업
시작 날짜	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 가능한 한 빨리 시작(기본값) • 시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	<p>작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.</p>
주석	<p>작업에 대한 주석을 입력합니다.</p>
작업 옵션	
작업	<p>다음 옵션 중 하나를 선택하거나 모두 선택합니다.</p> <ul style="list-style-type: none"> • 구성 정책 준수 확인(기본값) — 선택된 장치가 구성 정책을 준수하는지 확인합니다. • 진단 준수 확인 — 선택된 장치가 진단 정책을 준수하는지 확인합니다. • 소프트웨어 준수 확인 — 선택된 장치가 소프트웨어 정책을 준수하는지 확인합니다. • 소프트웨어 수준 확인 — 이 옵션을 선택하면 소프트웨어 수준이 확인되어 소프트웨어 수준과 식별된 보안 취약점을 보여 주는 텍스트 출력이 생성됩니다.
승인 옵션	
<p>승인 옵션은 작업이 워크플로 승인 규칙의 일부인 경우에만 표시됩니다.</p>	
승인 요청	<p>작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.</p>
승인 오버라이드	<p>작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.</p>

필드	설명/작업
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다. <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.

필드	설명/작업
작업 로깅	
작업 로깅	사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅" 을 참조하십시오.

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다.

자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오. 작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

요약 보고서 생성 작업 페이지 필드

요약 보고서 생성 작업을 통해 요약 보고서를 업데이트할 수 있습니다. 요약 보고서는 기본적으로 일요일마다 반복 작업으로 업데이트됩니다. 요약 보고서를 업데이트하는 일정을 영구적으로 변경하려면 기존 반복 작업을 편집하면 됩니다.

필드	설명/작업
작업 이름	요약 보고서 생성을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.
승인 옵션	
승인 옵션	승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.

필드	설명/작업
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). •주기적으로 — 반복 간격(분)을 지정합니다. •매일 — 작업이 매일 지정된 시간에 발생합니다. •매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. •매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다. <ul style="list-style-type: none"> •종료 날짜 없음(기본값) •< >번 발생 후 종료 — 반복 횟수를 입력합니다. •종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 **503페이지의 "작업 정보 페이지 필드"**를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

전자 메일 보고서 작업 페이지 필드

전자 메일 보고서 작업을 통해 NA 보고서를 전자 메일로 전송할 수 있습니다.

필드	설명/작업
작업 이름	전자 메일 보고서를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.
작업 옵션	
실행할 보고서	전자 메일로 보낼 보고서를 선택합니다. 이 작업이 실행될 때마다 마지막으로 저장된 보고서가 새 정보로 덮어쓰입니다. (참고: 요약 보고서는 이 작업을 사용하여 전자 메일로 보낼 수 없습니다.) 보고서의 목록을 보려면 742페이지의 "보고서 탐색" 을 참조하십시오.
적용 대상	이 필드는 네트워크 상태 보고서의 경우에만 표시됩니다. 보고서를 실행할 장치 그룹을 선택합니다.
전자 메일 수신자	하나 이상의 전자 메일 주소를 입력합니다. 쉼표로 주소를 구분해야 합니다.
전자 메일 제목	전자 메일 메시지의 제목 라인을 입력합니다.

필드	설명/작업
전자 메일 형식	드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 기본 형식 • HTML 메일 • CSV 파일 첨부 • 일반 텍스트 • HTML 전자 메일(링크 포함 안 함)
파일 내보내기	보고서의 복사본을 파일에 저장하려면 이 확인란을 클릭합니다.
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기 열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.

필드	설명/작업
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오. 작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

원격 에이전트 배포 페이지 필드

원격 에이전트 배포 작업을 통해 각 위성 게이트웨이 호스트에서 NA 원격 에이전트를 배포할 수 있습니다. 관리되는 장치와 동일한 LAN에 NA 원격 에이전트를 설치하면 WAN 트래픽을 최소화할 수 있으며 Syslog 및 TFTP를 사용하여 장치를 로컬로 관리할 수 있습니다.

원격 에이전트 배포 작업을 열려면 작업 아래의 메뉴 모음에서 새 작업을 선택하고 원격 에이전트 배포를 클릭합니다. 또한 게이트웨이 목록 페이지에서 원격 에이전트 배포 링크를 클릭하여 이 페이지로 이동할 수도 있습니다. 자세한 내용은 [198페이지의 "게이트웨이 목록 페이지 필드"](#)를 참조하십시오.

필드	설명/작업
작업 이름	원격 에이전트 배포를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.
작업 옵션	
작업	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •설치(또는 재설치) — NA 원격 에이전트를 설치합니다. NA 원격 에이전트가 이미 설치되어 있으면 기존 NA 원격 에이전트가 제거되고 새 NA 원격 에이전트가 설치됩니다. •설치 제거 — NA 원격 에이전트를 설치 제거합니다.

필드	설명/작업
게이트웨이에 에이전트 배포	NA 원격 에이전트가 배포될 게이트웨이 이름을 드롭다운 메뉴에서 선택합니다.
로그인	원격 에이전트를 배포하려면 위성 게이트웨이 호스트에서 root 권한이 필요합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •루트로 — SSH가 사용자 이름 root로 사용됩니다. root 암호를 입력해야 합니다. •비루트로 — SSH가 root가 아닌 사용자로 사용됩니다. 이 옵션을 선택하는 경우 su 암호(root 암호)나 sudo 암호(sudo 암호, 대개 사용자 이름 암호와 동일하지만 sudo가 구성된 방식에 따라 다를 수 있음)를 선택합니다.
관리 코어	코어 게이트웨이가 NA 코어와 동일한 호스트에 설치되어 있으면 관리 코어가 "로컬 호스트"(기본값)여야 합니다. 코어 게이트웨이가 NA 코어와 다른 호스트에 있으면 관리 코어가 NA 코어의 호스트 이름이나 IP 주소여야 합니다. (참고: NA 코어 호스트의 IP 주소가 다르면 코어 게이트웨이 호스트에서 NA 코어에 연결할 때 적절한 IP 주소를 사용하십시오.)
영역	코어 게이트웨이의 영역 이름을 드롭다운 메뉴에서 선택합니다.
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.

필드	설명/작업
예약 옵션	
재시도 수	<p>작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	사용할 수 없음
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

FQDN 확인 작업 페이지 필드

FQDN 확인 작업을 통해 장치의 기본 IP 주소에서 역방향 DNS 조회를 실행하여 시스템의 각 장치에 대한 FQDN(정규화된 도메인 이름)을 설정할 수 있습니다.

필드	설명/작업
작업 이름	FQDN 확인을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나 이상을 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. •CSV — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다 (IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다. <p>참고: 장치 목록 페이지에서 확인란을 사용하여 그룹의 장치를 선택하는 방법으로 임시 장치 그룹에 대해 실행할 작업을 예약할 때 이 섹션에 임시 장치 그룹에 포함된 장치가 표시됩니다.</p>
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~ 5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.

필드	설명/작업
주석	작업에 대한 주석을 입력합니다.
작업 옵션 (사용할 수 없음)	
승인 옵션	
승인 옵션	승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기 열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.

필드	설명/작업
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오. 작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

데이터 정리 작업 페이지 필드

데이터 정리는 시스템 관리자나 유사한 권한을 가진 사용자가 시스템을 구성해야 하는 시스템 작업입니다. 데이터를 정리하면 사용되지 않는 파일, 진단, 이벤트 및 작업이 제거됩니다. 다음 파일은 데이터 정리로 제거되지 않습니다.

- 현재 구성
- 배포하도록 예약된 구성

NA 서버가 정리를 수행하도록 구성된 경우 파일을 유지할 기간을 지정할 수 있습니다. 이러한 파일의 기본 설정은 다음과 같습니다.

- 구성 — 365일
- 작업 — 365일
- 진단 — 45일
- 이벤트 — 45일
- 세션 — 45일
- 로그 파일 — 30일

필드	설명/작업
작업 이름	데이터 정리를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.

필드	설명/작업
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.

필드	설명/작업
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다.

자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오. 작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

외부 응용 프로그램 실행 작업 페이지 필드

외부 응용 프로그램 실행 작업을 통해 "Ping" 명령이나 외부 언어 해석기와 같은 NA에서 실행할 외부 응용 프로그램을 예약할 수 있습니다. 이 작업을 사용하여 외부 헬프 데스크 및 NMS 솔루션과 통합할 수 있습니다.

참고: Windows 플랫폼에서는 경로에 Windows 파일 구분자인 백슬래시(\)를 사용해야 합니다. 짧은 이름(~<n>이 포함된 이름)은 파일 이름에 공백이 포함된 경우에만 필요합니다. 예를 들어 C:\Rendition은 적합하지만 C:\Program Files는 적합하지 않습니다. 짧은 이름은 매개 변수를 전달하는 경우에만 필요합니다. 예를 들어 C:\Program Files\Internet Explorer\iexplore.exe는 적합하지만 C:\Program Files\Internet Explorer\iexplore.exe someFilename.html은 작동하지 않습니다. C:\Progra~1\Intern~1\iexplore.exe someFilename.html을 사용해야 합니다.

필드	설명/작업
작업 이름	외부 응용 프로그램 실행을 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	작업에 대한 주석을 입력합니다.

필드	설명/작업
작업 옵션	
실행	실행할 명령줄 유틸리티나 스크립트를 입력합니다. 실행 파일의 정규화된 경로와 파일 이름을 제공해야 합니다. 실행할 응용 프로그램의 이름과 그 뒤에 매개 변수를 제공하여 외부 응용 프로그램에 매개 변수를 제공할 수 있습니다. 예를 들어 외부 명령 "foo"를 매개 변수 "bar" 및 "bat"와 함께 실행하려면 큰따옴표 없이 "foo bar bat"를 입력해야 합니다.
시작 위치	외부 응용 프로그램의 경로와 시작 디렉터리를 입력합니다.
작업 결과	0이 아닌 결과 코드를 실패한 작업으로 처리하려면 "0(영)이 아닌 결과 코드를 실패한 작업으로 처리" 상자를 선택합니다.
텍스트 출력	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • stdout에서 결과(기본값) — 응용 프로그램이 실행된 후 콘솔에 대한 표준 텍스트 출력이 작업 세부사항에 저장됩니다. 이 옵션은 명령줄 유틸리티와 같은 대부분의 응용 프로그램에 사용됩니다. • 파일에서 결과 — 출력이 없는 경우 이 옵션을 선택하고 파일 이름을 비워 둡니다. 응용 프로그램이 실행된 후 NA는 이 파일을 읽고 작업 세부사항에 해당 내용을 포함합니다. 이 옵션은 stdout 대신 파일에 출력을 쓰는 명령에 유용합니다. 해당하는 경우 결과 파일의 정규화된 경로를 입력해야 합니다.
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.

필드	설명/작업
예약 옵션	
재시도 수	<p>작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	<p>작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	<p>한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.
작업 로깅	
작업 로깅	<p>사용 가능한 경우 예정된 특정 작업에 대한 로그가 한 번 실행되도록 설정할 수 있습니다. "이 작업으로 생성된 로그 출력 저장" 확인란을 선택하고 Shift 키를 사용하여 하나 이상의 로그를 선택합니다. 선택한 로그는 강조 표시됩니다. 로깅과 함께 실행되도록 작업이 설정된 경우 로그를 시작할 수 없으면 작업이 더 이상 처리되지 않고 즉시 실패합니다. 로깅에 대한 자세한 내용은 125페이지의 "로깅"을 참조하십시오.</p>

입력이 완료되면 저장을 클릭해야 합니다. 작업이 즉시 실행되도록 예정된 경우 작업 정보 페이지가 열립니다. 작업 정보 페이지에서는 작업의 시작 날짜, 기간 및 상태와 같은 작업 정보를 제공합니다. 자세한 내용은 [503페이지의 "작업 정보 페이지 필드"](#)를 참조하십시오.

작업이 이후에 시작되도록 예정된 경우 내 작업 페이지가 열리고 새 작업이 강조 표시됩니다. 자세한 내용은 [491페이지의 "내 작업 페이지 필드"](#)를 참조하십시오.

멀티 태스킹 프로젝트 예약

단일 프로젝트 아래에 순차적으로 함께 결합된 몇 가지 작업을 실행하도록 멀티 태스킹 프로젝트를 구성할 수 있습니다. 예를 들어, 소프트웨어 업데이트를 수행하고 업데이트된 구성을 장치에 적용할 수 있습니다. 한 프로젝트 아래에 여러 작업을 함께 통합하면 작업 수준이 아니라 프로젝트 수준에서 작업을 인증하므로 관리 승인이 간단해집니다. 또한 서로 다른 작업의 집합을 통합하고 한 단위로 관리할 수도 있습니다.

참고: 멀티 태스킹 프로젝트에 대한 올바른 사용 권한이 있어야 합니다. 자세한 내용은 [335페이지의 "사용자 역할 및 권한 페이지 필드"](#)를 참조하십시오.

멀티 태스킹 프로젝트에 포함된 각 작업은 지정한 순서대로 실행됩니다. 예를 들어, 장치 그룹에 대해 드라이버 검색 및 스냅샷 예약, 사용자 지정 스크립트 실행 등을 수행할 수 있습니다. NA 스케줄러에 관한 한 멀티 태스킹 프로젝트는 한 작업으로 간주됩니다. 멀티 태스킹 프로젝트가 실행되도록 예약되면 NA 스케줄러가 모든 작업을 지정된 순서대로 실행합니다. 특정 이유로 멀티 태스킹 프로젝트의 작업 중 하나가 실행되지 않으면 멀티 태스킹 프로젝트가 실패합니다. 멀티 태스킹 프로젝트에 승인이 필요한 경우 멀티 태스킹 프로젝트가 승인되면 멀티 태스킹 프로젝트에 포함된 모든 작업이 자동으로 승인됩니다.

참고: 멀티 태스킹 프로젝트 페이지를 사용하여 장치 및/또는 장치 그룹을 예약할 수 있습니다.

하위 작업 경고 상태

멀티 태스킹 프로젝트의 경우 하위 작업이 경고 상태로 완료되면 후속 하위 작업을 계속 실행하거나 나머지 하위 작업을 모두 취소할 수 있습니다. 이 기능을 사용하면 문제가 발생할 수 있는 장치에서 실행 중인 작업을 취소할 수 있습니다.

이 기능을 활성화하려면

1. 관리 메뉴에서 사용자 지정 데이터 설정 페이지로 이동합니다.
2. 작업 섹션 아래에 있는 6번째 API 이름 필드까지 아래로 스크롤합니다.
3. 6번째 API 이름 필드에 **subtask_control**을 입력합니다.
4. 표시 이름 필드에 경고 메시지가 표시된 나머지 작업을 취소 입력합니다.
5. 값 필드에 제한 범위: 확인란을 선택하고 예, 아니요를 입력합니다.
6. 저장 버튼을 클릭합니다.

이 기능을 활성화된 경우 멀티 태스킹 프로젝트의 하위 작업을 만들면 경고 메시지가 표시된 나머지 작업 취소 필드가 모든 멀티 태스킹의 하위 작업 페이지에 있는 주식 필드 아래에 표시됩니다.

이 필드에는 다음 옵션이 포함되어 있습니다.

- 공백 — 나머지 하위 작업이 계속 실행됩니다.
- 예 — 나머지 하위 작업이 취소됩니다.
- 아니요 — 나머지 하위 작업이 계속 실행됩니다.

참고: 이 기능을 사용하지 않으려면 사용자 지정 데이터 설정 페이지에서 6번째 API 이름 확인란의 선택을 취소하고 저장 버튼을 클릭합니다.

멀티 태스킹 프로젝트를 생성하려면 작업 아래의 메뉴 모음에서 새 멀티 태스킹 프로젝트를 클릭합니다. 새 작업/템플릿 작업 - 멀티 태스킹 프로젝트 페이지가 열립니다.

멀티 태스킹 프로젝트 페이지 필드

필드	설명/작업
작업 이름	멀티 태스킹 프로젝트를 표시합니다. 해당하는 경우 다른 작업 이름을 입력할 수 있습니다.
저장 옵션	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •작업으로 저장 — 이 옵션은 기본적으로 선택됩니다. •작업 템플릿으로 저장 — 이 옵션을 선택할 경우 작업이 작업 템플릿으로 저장되고 작업 템플릿 페이지에 표시됩니다. 작업 템플릿에 대한 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
시작 날짜	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •가능한 한 빨리 시작(기본값) •시작 날짜/시간 — 작업을 시작할 날짜와 시간을 입력합니다. 날짜 상자 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다.
작업 우선 순위	작업의 우선 순위를 설정할 수 있습니다. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	멀티 태스킹 작업에 대한 설명을 추가합니다.
작업 옵션	
하위 작업	드롭다운 메뉴에서 하위 작업을 선택합니다. 선택하는 하위 작업에 따라 해당 작업의 새 작업 페이지가 열립니다. 이 페이지에서 작업을 구성할 수 있습니다. 예를 들어, Syslog 구성 작업을 선택하는 경우 새 작업 - Syslog 구성 페이지가 열립니다. 작업을 추가하면 작업이 작업 편집 - 멀티 태스킹 프로젝트 페이지에 표시됩니다. 필요한 경우 작업을 편집하거나 삭제할 수 있습니다. 작업 저장을 클릭하면 보류 중 작업 페이지가 열립니다. 495페이지의 "예정된 작업 페이지 필드" 를 참조하십시오.
예약된 장치	장치를 예약하려면 장치 선택기를 사용합니다. 장치 선택기 사용 방법에 대한 자세한 내용을 보려면 183페이지의 "장치 선택기" 를 참조하거나 장치 선택기 오른쪽 위 구석에 있는 물음표(?)를 클릭하십시오.

필드	설명/작업
추산 기간	작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본값은 60분입니다.
승인 옵션	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 재시도 없음(기본값) • 한 번 • 두 번 • 세 번
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	사용할 수 없음

완료하면 저장을 클릭해야 합니다.

멀티 태스킹 프로젝트를 구성하는 방법

이 섹션에서는 프로젝트의 장치 및/또는 장치 그룹을 예약하고 활동 캘린더를 사용하여 프로젝트의 예약된 장치 및/또는 장치 그룹을 보는 등의 멀티 태스킹 프로젝트를 설정하는 프로세스를 단계별로 설명합니다.

1. 작업 아래의 메뉴 모음에서 새 멀티 태스킹 프로젝트를 클릭합니다. 새 작업/템플릿 - 멀티 태스킹 프로젝트 페이지가 열립니다.
2. 작업 이름 필드에 프로젝트의 이름(예: Pine Valley Office)을 입력합니다. 특정 장치 및/또는 장치 그룹을 *Pine Valley Office*라는 상위 그룹에 이미 추가했다고 가정합니다. 이렇게 하지 않은 경우 자세한 내용은 [175페이지의 "장치 그룹 추가"](#)를 참조하십시오.
3. 시작 날짜 필드에서 가능한 한 빨리 시작(기본값)을 선택하거나 프로젝트를 시작할 날짜와 시간을 선택할 수 있는 캘린더를 클릭합니다.
4. 아래쪽 화살표를 클릭하여 1~5의 작업 우선 순위를 선택합니다. 이 때 1은 최고 우선 순위입니다. 기본값은 3입니다. 높은 우선 순위 작업이 낮은 우선 순위 작업보다 먼저 실행됩니다.
5. 주석 필드에서 프로젝트에 대한 설명을 입력합니다.
6. 작업 옵션 아래의 하위 작업 필드에서 프로젝트에 포함할 하위 작업을 드롭다운 메뉴에서 선택합니다. 예를 들어, 암호 배포 작업을 선택하는 경우 새 작업/템플릿 - 암호 배포 페이지가 열립니다.
7. 암호 배포 페이지를 사용하여 적용 대상 필드에서 Pine Valley Office를 드롭다운 메뉴에서 선택합니다. 이름을 입력하거나 Pine Valley Office에 있는 장치 및/또는 장치 그룹의 목록이 포함된 CSV 파일을 찾을 수도 있습니다.
8. 작업 옵션 섹션을 완료합니다. 이 섹션에 표시되는 옵션은 작업에 따라 다릅니다. 암호 배포 작업에 대한 자세한 내용은 [370페이지의 "암호 배포 작업 페이지 필드"](#)를 참조하십시오.
9. 작업 저장을 클릭합니다. 멀티 태스킹 프로젝트 페이지로 돌아옵니다. 이 페이지에서 추가 하위 작업을 프로젝트에 추가할 수 있습니다.
10. Pine Valley Office에 있는 모든 장치를 예약하려면 예약된 장치 필드에서 수정을 클릭합니다. 장치 선택기가 열립니다.
11. Pine Valley Office를 두 번 클릭합니다. Pine Valley Office에 있는 모든 장치가 표시됩니다.

12. Pine Valley Office에 있는 모든 장치를 예약하려면 모두 선택을 클릭한 다음 오른쪽 화살표(>>>)를 클릭합니다. 장치가 선택된 장치 상자에 표시됩니다. 특정 장치만 추가하려면 장치의 호스트 이름이나 IP 주소 중 일부를 입력하여 검색 범위를 좁히거나 추가할 장치만 선택한 다음 오른쪽 화살표를 클릭할 수 있습니다.
13. 장치를 예약할 추산 기간을 입력합니다. 기본값은 1시간입니다.
14. 작업 저장을 클릭합니다. 예약된 장치의 목록이 예약된 장치 필드에 포함됩니다.
15. 작업 저장을 클릭합니다. 프로젝트를 즉시 실행, 편집, 삭제 또는 일시 중지할 수 있는 내 작업 페이지가 열립니다.
16. 작업 아래의 메뉴 모음에서 활동 캘린더를 클릭합니다. 활동 캘린더가 열립니다.
17. 캘린더를 사용하여 프로젝트가 Pine Valley Office 장치를 예약한 일을 선택합니다. Pine Valley Office 프로젝트가 선택한 시간 슬롯에 표시됩니다.
18. Pine Valley Office를 클릭합니다. 프로젝트에 대한 자세한 정보를 볼 수 있는 작업 정보 페이지가 열립니다.

내 작업 보기

내 작업 페이지에는 현재 로그인한 사용자가 주관한 작업이 표시됩니다. 여기에는 작업 승인 상태(해당하는 경우), 작업이 아직 실행되지 않았는지 여부 등이 포함됩니다.

내 작업 페이지를 보려면 작업 아래의 메뉴 모음에서 내 작업을 클릭합니다. 내 작업 페이지가 열립니다.

내 작업 페이지 필드

필드	설명/작업
내 드래프트 링크	해당하는 경우 내 드래프트 페이지가 열립니다.
승인 요청 링크	작업에 승인이 필요한 경우 현재 로그인한 사용자의 승인이 필요한 작업을 볼 수 있는 승인 요청 페이지가 열립니다. 기본적으로 이 페이지에는 다음 작업을 비롯하여 완료되지 않은 작업이 표시됩니다. <ul style="list-style-type: none"> • 승인 안 됨 • 승인 대기 중 • 실행 대기 중 자세한 내용은 863페이지의 "승인 요청" 을 참조하십시오.
예정된 작업 링크	대기열에 있는 예정된 작업을 볼 수 있는 예정된 작업 페이지가 열립니다. 자세한 내용은 495페이지의 "예정된 작업 페이지 필드" 를 참조하십시오.
작업 실행 중 링크	실행 중인 작업을 모두 볼 수 있는 작업 실행 중 페이지가 열립니다. 자세한 내용은 498페이지의 "작업 실행 중 페이지 필드" 를 참조하십시오.
최근 작업 링크	최근 작업을 모두 볼 수 있는 최근 작업 페이지가 열립니다. 자세한 내용은 500페이지의 "최근 작업 페이지 필드" 를 참조하십시오.

필드	설명/작업
작업 표시 확인란	작업에 승인이 필요한 경우 다음 표시 옵션을 선택할 수 있습니다. <ul style="list-style-type: none"> • 승인됨 • 승인 안 됨 • 승인 대기 중 • 오버라이드됨 • 드래프트 • 승인이 필요하지 않음
확인란	왼쪽의 확인란을 사용하여 작업을 삭제할 수 있습니다. 작업을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 작업을 선택하거나 선택 취소할 수 있습니다.
예약 날짜	작업이 생성된 날짜와 시간을 표시합니다.
날짜별 승인	해당하는 경우 작업이 승인되어야 하는 날짜와 시간을 표시합니다. 작업이 승인 날짜까지 승인되지 않으면 상태가 "승인 안 됨"으로 설정됩니다. (참고: 승인 옵션은 작업이 워크플로 승인 규칙의 일부인 경우에만 표시됩니다.)
작업 이름	작업 이름을 표시합니다. 작업을 클릭하면 작업 세부사항 페이지가 열립니다. 자세한 내용은 358페이지의 "작업이란?" 을 참조하십시오.
승인 상태	해당하는 경우 작업의 승인 상태를 표시합니다. 승인 상태는 작업이 워크플로 승인 규칙의 일부인 경우에만 표시됩니다. 승인 상태는 다음과 같습니다. <ul style="list-style-type: none"> • 승인 대기 중 • 승인됨 • 승인 안 됨 • 오버라이드됨 • 승인이 필요하지 않음

필드	설명/작업
작업 상태	<p>작업의 상태를 표시합니다. 상태는 다음과 같습니다.</p> <ul style="list-style-type: none"> • 경고 — 그룹 작업에 일부 실패한 하위 작업이 포함되어 있지만, 모든 작업이 실패한 것은 아닙니다. • 드래프트 — 드래프트 상태에서는 NA에서 작업을 실행하지 않거나 작업이 승인을 위해 전송되지 않습니다. • 중복 — 동일한 작업이 이미 실행 중이기 때문에 작업이 시작되지 않았습니다. • 실패함 — 작업이 실패했습니다. • 일시 중지 — 누군가가 작업을 일시 중지했습니다. 예정된 시간이 되면 실행되지 않습니다. • 보류 중 — 작업이 대기열에 저장되고 예정된 시간을 기다리고 있습니다. • 실행 중 — 작업이 시작되었지만 아직 완료되지 않았습니다. • 건너뛴 — 잘못된 권한, 관리되지 않는 장치 등의 오류 때문에 작업을 건너뛰었습니다. • 성공함 — 작업이 성공했습니다. • 대기 중 — 예정된 시간이 되었지만 "최대 동시 작업 수" 제한에 도달했기 때문에 작업이 대기 중입니다.
우선 순위	<p>작업 우선 순위를 표시합니다. 1~5의 5가지 작업 우선 순위 수준이 있으며, 최고 작업 우선 순위는 1입니다. 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.</p>
작업 유형	<p>작업 유형이 표시됩니다. 예를 들면 다음과 같습니다.</p> <ul style="list-style-type: none"> • 암호 배포 • 구성 배포 • 드라이버 검색 • 장치 재부팅 • 스냅샷 작성 • 시작 및 실행 구성 동기화 <p>작업의 전체 목록을 보려면 358페이지의 "작업이란?"을 참조하십시오. (참고: 멀티 태스킹 프로젝트 작업은 내 작업 결과 페이지에 표시될 수도 있고 표시되지 않을 수도 있습니다. 표시 여부는 멀티 태스킹 프로젝트 작업에 하위 작업으로 위에 나열된 작업 유형이 하나 이상 포함되는지에 따라 결정됩니다.)</p>

필드	설명/작업
작업	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none">• 삭제 — 작업을 삭제할 수 있습니다.• 일시 중지 — 예정된 시간에 실행되지 않도록 작업이 일시 중지됩니다. (참고: 작업을 다시 시작하려면 재개를 선택하면 됩니다.)• 지금 실행 — 작업이 가능한 한 빨리 실행됩니다. 최대 동시 작업 수에 도달하지 않은 경우 작업이 즉시 실행됩니다.• 편집 — 작업 편집 페이지가 열립니다.
페이지별 결과 표시 수	드롭다운 메뉴에서 페이지당 표시할 항목 수를 설정할 수 있습니다. 기본값은 25입니다.

예정된 작업 보기

대기열에 있지만 아직 실행되지 않은 예정된 작업을 보려면 작업 아래의 메뉴 모음에서 예정된 작업을 클릭합니다. 예정된 작업 페이지가 열립니다.

참고: 작업 페이지 새로 고침 간격을 변경하려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 사용자 인터페이스를 클릭합니다. 사용자 인터페이스 페이지에서 기타 섹션까지 아래로 스크롤하고 작업 페이지 새로 고침 간격을 입력합니다.

예정된 작업 페이지 필드

필드	설명/작업
내 작업 링크	내 작업 페이지가 열립니다. 자세한 내용은 491페이지의 "내 작업 페이지 필드" 를 참조하십시오.
작업 템플릿 링크	작업 템플릿 페이지가 열립니다. 자세한 내용은 361페이지의 "작업 템플릿" 을 참조하십시오.
내 드래프트 링크	내 드래프트 페이지가 열립니다. 자세한 내용은 491페이지의 "내 작업 페이지 필드" 를 참조하십시오.
승인 요청 링크	작업에 승인이 필요한 경우 현재 로그인한 사용자의 승인이 필요한 작업을 볼 수 있는 승인 요청 페이지가 열립니다. 자세한 내용은 863페이지의 "승인 요청" 을 참조하십시오.
작업 실행 중 링크	작업 실행 중 페이지가 열립니다. 자세한 내용은 498페이지의 "작업 실행 중 페이지 필드" 를 참조하십시오.
최근 작업 링크	최근 작업 페이지가 열립니다. 자세한 내용은 500페이지의 "최근 작업 페이지 필드" 를 참조하십시오.
현재 작업 그룹	현재 작업 그룹의 이름을 표시합니다. 드롭다운 메뉴에서 다른 그룹을 선택하고 새로 고침 버튼을 클릭할 수 있습니다.
그룹/상위 작업만 표시	이 옵션을 선택하면 그룹과 상위 작업만 표시됩니다.
확인란	왼쪽의 확인란을 사용하여 예정된 작업을 삭제할 수 있습니다. 작업을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 작업을 선택하거나 선택 취소할 수 있습니다.

필드	설명/작업
예약 날짜	NA에서 작업을 실행하도록 예정된 날짜와 시간을 표시합니다.
작업 이름	작업 이름을 표시합니다.
호스트/그룹	작업과 연관된 네트워크 장치의 호스트 또는 그룹 이름을 표시합니다. 링크를 클릭하여 그룹의 장치에 대한 기본 정보를 볼 수 있는 장치 정보 페이지를 열 수 있습니다.
작업 상태	<p>작업의 상태를 표시합니다. 예를 들면 다음과 같습니다.</p> <ul style="list-style-type: none"> •보류 중 — 작업이 대기열에 저장되지만 아직 실행되지 않았습니다. •일시 중지 — 폴링이 일시 중지되었습니다. 폴링을 다시 시작하려면 "resume polling" CLI 명령을 입력합니다. •드래프트 — 작업이 드래프트 모드에 있고 실행되지 않습니다. <p>작업 상태의 전체 목록을 보려면 503페이지의 "작업 정보 페이지 필드"를 참조하십시오.</p>
우선 순위	작업 우선 순위를 표시합니다. 1~5의 5가지 작업 우선 순위 수준이 있으며, 최고 작업 우선 순위는 1입니다. 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.
예약자	작업을 예약한 사람(또는 작업을 수정한 마지막 사용자)의 로그인 이름을 표시합니다.
주석	보류 중인 작업에 대한 설명을 표시합니다.
작업	<p>보류 중 작업 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> •삭제 — 작업을 삭제합니다. •일시 중지 — 예정된 시간에 실행되지 않도록 작업이 일시 중지됩니다. (참고: 작업을 다시 시작하려면 재개를 선택하면 됩니다.) •지금 실행 — 작업이 가능한 한 빨리 실행됩니다. 최대 동시 작업 수에 도달하지 않은 경우 작업이 즉시 실행됩니다. •편집 — 작업을 편집하고 반복되거나 아직 발생하지 않은 작업을 다시 실행할 수 있는 작업 편집 페이지가 열립니다. •템플릿 생성 — 작업 템플릿 페이지가 열립니다. 이 페이지에서는 처음부터 새로 시작하지 않고 새 작업 및 기존 작업을 쉽게 구성 및 실행할 수 있도록 작업 정의를 저장할 수 있습니다. 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.

필드	설명/작업
페이지별 결과 표시 수	드롭다운 메뉴에서 페이지당 표시할 항목 수를 설정할 수 있습니다. 기본값은 25입니다.

실행 중인 작업 보기

실행 중인 작업을 보려면 작업 아래의 메뉴 모음에서 작업 실행 중을 클릭합니다. 작업 실행 중 페이지가 열립니다.

참고: 작업 페이지 새로 고침 간격을 변경하려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 사용자 인터페이스를 클릭합니다. 사용자 인터페이스 페이지에서 기타 섹션까지 아래로 스크롤하고 작업 페이지 새로 고침 간격을 입력합니다.

작업 실행 중 페이지 필드

필드	설명/작업
내 작업 링크	내 작업 페이지가 열립니다. 자세한 내용은 491페이지의 "내 작업 페이지 필드" 를 참조하십시오.
내 드래프트 링크	내 드래프트 페이지가 열립니다. 자세한 내용은 491페이지의 "내 작업 페이지 필드" 를 참조하십시오.
승인 요청 링크	현재 로그인한 사용자가 승인해야 하는 작업을 볼 수 있는 승인 요청 페이지가 열립니다. 자세한 내용은 863페이지의 "승인 요청" 을 참조하십시오.
예정된 작업 링크	예정된 작업 페이지가 열립니다. 자세한 내용은 495페이지의 "예정된 작업 페이지 필드" 를 참조하십시오.
최근 작업 링크	최근 작업 페이지가 열립니다. 자세한 내용은 500페이지의 "최근 작업 페이지 필드" 를 참조하십시오.
현재 작업 그룹	현재 작업 그룹을 표시합니다. 둘 이상의 그룹을 선택/선택 취소하려면 Ctrl 키를 누른 상태에서 그룹을 클릭합니다.
하위/상위 작업만 표시	이 옵션을 선택하면 하위/상위 작업만 표시됩니다.
이 페이지를 60초마다 새로 고칩니다.	60초마다 표시를 새로 고치지 않으려면 이 상자의 선택을 취소합니다. 이 값 설정에 대한 자세한 내용은 80페이지의 "사용자 인터페이스 페이지 필드" 를 참조하십시오.
확인란	왼쪽의 확인란을 사용하여 작업을 삭제할 수 있습니다. 작업을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 작업을 선택하거나 선택 취소할 수 있습니다.
시작 날짜	NA에서 작업 실행을 시작한 날짜와 시간을 표시합니다.

필드	설명/작업
작업 이름	작업 유형을 표시합니다.
호스트/그룹	작업과 연관된 네트워크 장치의 호스트 또는 그룹 이름을 표시합니다. 링크를 클릭하여 그룹의 장치에 대한 기본 정보를 볼 수 있는 장치 정보 페이지를 열 수 있습니다.
작업 상태	작업의 상태를 표시합니다(실행 중). 최대 동시 작업 수에 도달한 경우 해당 작업은 다른 작업이 완료될 때까지 대기합니다. 따라서 작업 실행 중 페이지에 "작업을 찾을 수 없음"이 표시됩니다. (참고: 그룹 상위 작업이 설정에 포함되지 않았기 때문에 작업 수가 최대 동시 작업 수 값을 초과할 수 있습니다.)
우선 순위	작업 우선 순위 수준을 표시합니다. 작업 우선 순위 설정에 대한 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
예약자	작업을 예약한 사람(또는 작업을 수정한 마지막 사용자)의 로그인 이름을 표시합니다.
주석	보류 중인 작업에 대한 설명을 표시합니다.
작업	<p>작업 실행 중 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 편집 — 작업을 편집할 수 있는 작업 편집 페이지가 열립니다. • 세부사항 — 작업에 대한 정보를 볼 수 있는 작업 정보 페이지가 열립니다. • 취소 — 작업을 삭제할 수 있습니다. • 우선 순위 증가 — 작업 우선 순위를 높일 수 있습니다. 작업 우선 순위 수준이 설정할 수 있는 권한이 부여된 최고 우선 순위로 이미 도달한 상태에서는 우선 순위 증가 옵션을 클릭해도 작업 우선 순위 수준이 변경되지 않습니다. 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오. • 우선 순위 감소 — 작업 우선 순위를 낮출 수 있습니다.

최근 작업 보기

최근 작업을 보려면 작업 아래의 메뉴 모음에서 최근 작업을 클릭합니다. 최근 작업 페이지가 열립니다. 최근 작업 페이지에는 상태에 관계없이 최근 작업이 모두 표시됩니다.

참고: 작업 페이지 새로 고침 간격을 변경하려면 관리 아래의 메뉴 모음에서 관리 설정을 선택하고 사용자 인터페이스를 클릭합니다. 사용자 인터페이스 페이지에서 기타 섹션까지 아래로 스크롤하고 작업 페이지 새로 고침 간격을 입력합니다.

최근 작업 페이지 필드

필드	설명/작업
내 작업 링크	내 작업 페이지가 열립니다. 자세한 내용은 491페이지의 "내 작업 페이지 필드" 를 참조하십시오.
작업 템플릿 링크	작업 템플릿 페이지가 열립니다. 자세한 내용은 361페이지의 "작업 템플릿" 을 참조하십시오.
내 드래프트 링크	내 드래프트 페이지가 열립니다. 자세한 내용은 491페이지의 "내 작업 페이지 필드" 를 참조하십시오.
승인 요청 링크	현재 로그인한 사용자가 승인해야 하는 작업을 볼 수 있는 승인 요청 페이지가 열립니다. 자세한 내용은 863페이지의 "승인 요청" 을 참조하십시오.
예정된 작업 링크	예정된 작업 페이지가 열립니다. 자세한 내용은 495페이지의 "예정된 작업 페이지 필드" 를 참조하십시오.
실행 중인 작업 링크	실행 중인 작업 페이지가 열립니다. 자세한 내용은 498페이지의 "작업 실행 중 페이지 필드" 를 참조하십시오.
현재 작업 그룹	작업과 연관된 네트워크 장치의 그룹 이름을 표시합니다. 둘 이상의 그룹을 선택/선택 취소하려면 Ctrl 키를 누른 상태에서 그룹을 클릭합니다.

필드	설명/작업
필터 표시	<p>다음 필터를 표시하려면 필터 표시 옵션을 클릭합니다.</p> <ul style="list-style-type: none"> • 내부 작업 표시 — 최근 작업을 볼 시간 프레임을 선택합니다. • 세부사항 표시 — 세부사항 표시 상자를 클릭한 다음 새로 고침을 클릭하여 최근 작업 페이지에서 각 작업에 대한 작업 세부사항을 봅니다. • 그룹/상위 작업만 표시 — 그룹/상위 작업만 표시하려면 클릭합니다. • 작업 상태 — 표시할 하나 이상의 작업 상태를 선택합니다. <p>상태를 변경하는 경우 새로 고침을 클릭해야 합니다.</p>
확인란	<p>왼쪽의 확인란을 사용하여 작업을 삭제할 수 있습니다. 작업을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 작업을 선택하거나 선택 취소할 수 있습니다.</p>
완료 날짜	<p>NA에서 작업 실행을 시작한 날짜와 시간을 표시합니다.</p>
작업 이름	<p>작업 유형을 표시합니다.</p>
호스트/그룹	<p>작업과 연관된 네트워크 장치의 호스트 또는 그룹 이름을 표시합니다. 링크를 클릭하여 그룹의 장치에 대한 자세한 정보를 볼 수 있는 장치 정보 페이지를 열 수 있습니다.</p>
작업 상태	<p>작업의 상태를 표시합니다. 예를 들면 다음과 같습니다.</p> <ul style="list-style-type: none"> • 성공함 — 작업이 성공했습니다. • 실패함 — 작업이 실패했습니다. • 중복 — 작업이 다른 작업과 중복됩니다. • 건너뛴 — 이 작업의 실행 시간에 도달했을 때 이미 동일한 작업이 실행 중이어서 작업을 건너뛰었습니다. <p>작업 상태의 전체 목록을 보려면 503페이지의 "작업 정보 페이지 필드"를 참조하십시오.</p>
우선 순위	<p>작업 우선 순위를 표시합니다. 1~5의 5가지 작업 우선 순위 수준이 있으며, 최고 작업 우선 순위는 1입니다. 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.</p>
예약자	<p>작업을 예약한 사람(또는 작업을 수정한 마지막 사용자)의 로그인 이름을 표시합니다.</p>

필드	설명/작업
주석	작업에 대한 주석을 표시합니다.
작업	<p>최근 작업 표의 각 작업에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 세부사항 — 작업에 대한 정보를 볼 수 있는 작업 정보 페이지가 열립니다. • 다시 실행 — 작업을 편집하고 다시 실행할 수 있는 작업 재실행 페이지가 열립니다. (참고: 이 옵션은 작업을 다시 실행할 수 있는 경우에만 나타납니다.) • 템플릿 생성 — 작업 템플릿 페이지가 열립니다. 이 페이지에서는 처음부터 새로 시작하지 않고 새 작업 및 기존 작업을 쉽게 구성 및 실행할 수 있도록 작업 정의를 저장할 수 있습니다. 자세한 내용은 361페이지의 "작업 템플릿"을 참조하십시오.
페이지별 결과 표시 수	드롭다운 메뉴에서 페이지당 표시할 항목 수를 설정할 수 있습니다. 기본값은 25입니다.

작업 정보 페이지 필드

작업 정보 페이지에는 다음을 비롯한 작업에 대한 자세한 정보가 포함되어 있습니다.

- 작업 상태
- 작업 우선 순위
- 주관자
- 영향 받은 장치
- 기간
- 승인 정보
- 결과 세부사항
- 작업 이력

작업 정보 페이지에서는 경고 또는 실패 시 더욱 자세한 정보에 대한 링크도 제공합니다. 작업을 성공적으로 완료할 수 있지만 여전히 오류를 포함할 수 있습니다. 예를 들어, 실행 중인 구성에 성공적으로 배포할 수 있지만 구성 안에 잘못된 명령이 있을 수 있습니다.

작업 정보 페이지를 열려면 다음 단계를 수행하십시오.

1. 인벤토리 페이지에서 장치를 선택합니다. 장치 세부사항 페이지가 열립니다.
2. 보기 드롭다운 메뉴에서 장치 작업을 클릭합니다. 장치 작업 페이지가 열립니다.
3. 작업 열에서 자세한 정보를 원하는 작업에 대한 세부사항 옵션을 클릭합니다. 작업 정보 페이지가 열립니다.

필드	설명/작업
작업 편집 링크	작업을 편집할 수 있도록 작업 페이지가 열립니다. 이 링크는 보류 중인 작업에만 표시됩니다. 358페이지의 "작업이란?" 을 참조하십시오.
다시 실행 링크	작업을 다시 실행할 수 있도록 작업 페이지가 열립니다. 이 링크는 완료된 작업에만 표시됩니다. 358페이지의 "작업이란?" 을 참조하십시오.
목록으로 돌아가기 링크	내 작업 페이지가 열립니다. 491페이지의 "내 작업 보기" 를 참조하십시오.

필드	설명/작업
일반 정보	
작업 이름	작업 이름을 표시합니다.
작업 상태	<p>다음은 비롯한 작업 상태를 표시합니다.</p> <ul style="list-style-type: none"> •드래프트 •중복 •실패함 •일시 중지 •보류 중 •요청됨(참고: 요청됨은 작업이 승인을 기다리고 있다는 의미입니다. (866페이지의 "작업 승인"을 참조하십시오.) •실행 •건너뛴 •성공함 •동기(참고: 일반적으로 NA는 스레드를 만들고 작업이 백그라운드에서 비동기적으로 실행되게 하여 작업을 실행합니다. CLI 및 API를 통해 현재 스레드에서 실행되는 동기 작업을 활성화할 수 있으며 명령이 완료될 때까지 명령이 차단됩니다.) •대기 중 •경고 <p>참고: 경고가 발생하는 경우 멀티 태스킹 프로젝트의 처리가 계속됩니다. 경고 상태는 상위 작업에 표시됩니다.</p>
주석	작업에 대한 설명을 표시합니다.
주관자	작업을 예약한 사용자 이름이나 프로세스를 표시합니다.
우선 순위	작업 우선 순위를 표시합니다. 1~5의 5가지 작업 우선 순위 수준이 있으며, 최고 작업 우선 순위는 1입니다. 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.
생성 날짜	작업이 생성된 날짜와 시간을 표시합니다.
영향 받은 장치	영향 받은 장치의 호스트 이름 및/또는 IP 주소를 표시합니다.

필드	설명/작업
예약 날짜	작업이 실행되도록 예약된 날짜와 시간을 표시합니다.
시작 날짜	작업의 시작 날짜를 표시합니다.
완료 날짜	작업의 완료 날짜를 표시합니다.
기간	작업 기간을 표시합니다.
반복 유형	반복 유형(예: 반복되지 않음)을 표시합니다.
상위 작업	상위 작업을 표시합니다.
승인 정보	
승인자	작업 승인자의 목록을 표시합니다.
승인 상태	작업 승인 상태를 표시합니다.
우선 순위	작업 우선 순위를 표시합니다.
승인 날짜	작업이 승인되어야 하는 날짜와 시간을 표시합니다.
새 주석	작업에 대한 추가 설명을 입력합니다.
승인 버튼	작업을 승인하려면 승인 버튼을 클릭합니다.
작업 세부사항 보기 링크	작업 보기 링크를 클릭하면 진단 이력 페이지가 열립니다.
추가 정보	
결과 세부사항	장치 유형에 따라 자동으로 실행된 진단을 표시합니다. 예를 들면 다음과 같습니다. <ul style="list-style-type: none"> • "NA 모듈 상태" 진단이 완료되었습니다. • "NA 라우팅 테이블" 진단이 완료되었습니다. • "NA 인터페이스" 진단이 완료되었습니다. • "NA OSPF 인접 환경" 진단이 완료되었습니다.
작업 이력	
작업 이력 정보	작업 실행 시기, 반복 유형 및 상태와 같은 작업 이력 정보를 표시합니다.

작업 로드 보기

작업 로드 페이지에는 시스템에 현재 있는 작업 수를 표시합니다. 작업은 세 가지 범주로 분류됩니다.

- 다음 15분 안에 시작되도록 예정된 작업
- 실행 대기 중인 작업
- 현재 실행 중인 작업

작업 로드 페이지에는 시스템의 모든 작업이 포함되어 있습니다. 이러한 작업에는 현재 사용자가 볼 수 있는 권한이 없는 작업도 포함됩니다. 이에 따라 작업 수가 작업 검색 페이지의 작업 수와 일치하지 않을 수도 있습니다.

작업 로드 페이지를 보려면 작업 아래의 메뉴 모음에서 작업 로드를 클릭합니다. 작업 로드 페이지가 열립니다. (관리 아래에서 이 페이지에 액세스할 수도 있습니다.)

작업 로드 페이지

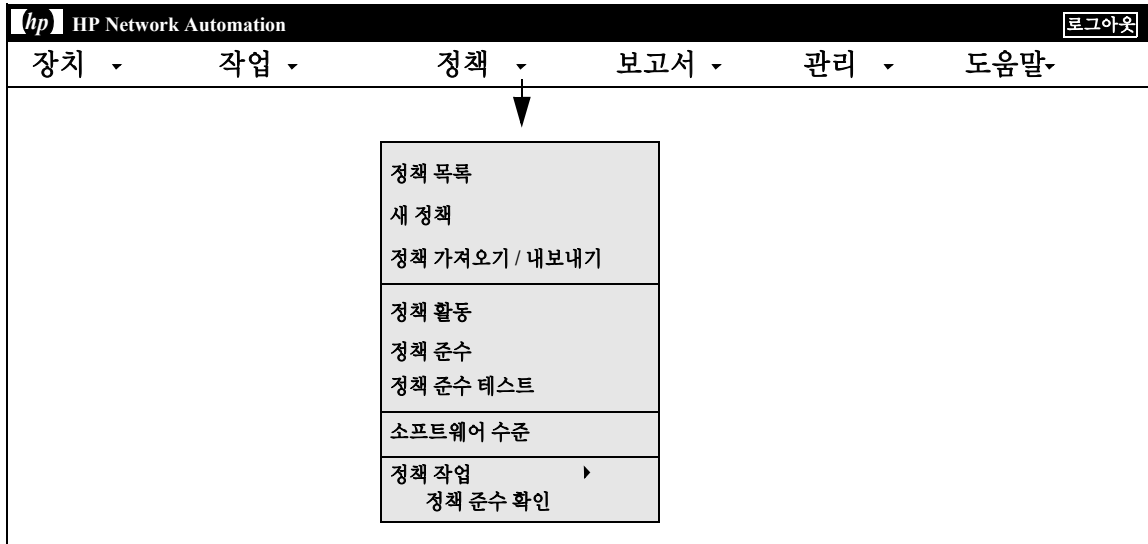
필드	설명
시작 예정 작업 수(15분 이내)	다음 15분 안에 시작되도록 예정된 작업 수를 표시합니다.
대기 중인 작업 수	대기 중인 작업 수를 표시합니다. 최대 동시 작업 수에 도달한 경우 해당 작업은 다른 작업이 완료될 때까지 대기합니다.
실행 중인 작업 수	실행 중인 작업 수를 표시합니다.

8장: 정책 보증 관리

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	509페이지의 "시작하기"
정책 생성	511페이지의 "정책 생성"
정책 규칙 생성	518페이지의 "새 규칙 페이지 필드"
정책 가져오기/내보내기	524페이지의 "정책 가져오기/내보내기"
정책 편집	525페이지의 "정책 편집"
적용된 정책 보기	531페이지의 "적용된 정책 보기"
정책 활동 보기	532페이지의 "정책 활동 보기"
정책 준수 보기	534페이지의 "정책 준수 보기"
새 준수 추가	537페이지의 "새 소프트웨어 수준 추가"
정책 준수 테스트	545페이지의 "정책 준수 테스트"

정책 보증으로 이동



시작하기

HP NA(Network Automation) 정책 관리자를 사용하면 네트워크가 보안과 신뢰성, 품질 목표를 달성할 수 있도록 표준 또는 모범 사례를 확립할 수 있습니다. NA에서는 정책 적용 기능과 통합 수정을 제공하여 정의된 모범 사례와 일치하는 장치와 구성을 확인하며 장치를 모범 사례에 맞게 되돌리기 위해 필요한 수정 단계를 확인하는 번거로운 작업을 자동화합니다.

NA 정책 관리자 역시 PCI나 Sarbanes-Oxley(SOX) 등의 규정 준수 요구 사항을 경제적이고 효율적인 방식으로 충족시키는 데에 있어 중요한 역할을 담당합니다.

이 섹션에서 사용되는 용어는 다음과 같습니다.

- 정책 — 정책은 장치의 구성과 런타임 상태를 테스트하는 규칙을 말합니다.
- 규칙 — 규칙은 다음 중 하나 이상을 확인하는 자동화된 테스트입니다.
 - 특정 구성 설정
 - 특정 데이터 모델 요소
 - 장치의 런타임 상태(일명 진단)
 - 장치에서 실행되는 소프트웨어 버전
- 진단 — 진단은 장치에서 구성 파일을 통해 캡처되지 않은 장치 관련 정보를 수집하기 위해 실행하는 명령입니다. 예를 들어, Cisco 라우터에서 진단은 NTP 상태 표시 명령의 출력을 나타냅니다. 진단 목록은 [261페이지의 "메뉴 옵션 보기"](#) 섹션의 진단 필드를 참조하십시오.
- 규칙 예외 — 규칙 예외는 규칙의 일부입니다. 하지만 규칙 예외는 장치 구성에서 일치하는 텍스트를 텍스트가 속한 규칙의 고려 대상에서 제외하는 것을 목적으로 합니다.
- 자동 수정 — 장치가 정책 규칙을 준수하지 않을 때 자동으로 실행되도록 미리 정의된 스크립트입니다.

NA 정책 관리자의 작업 방식

NA 정책 관리자를 시작하려면 먼저 NA 내에 정책을 생성하여 장치가 따라야 할 모범 사례를 정의합니다. 다음으로는 정책을 테스트하여 위반이 올바르게 파악되는지 확인합니다. 마지막으로는 각 정책을 특정 장치 그룹(또는 장치 그룹 집합)에 할당합니다. 그러면 NA에서 장치가 정의된 정책과 일치하는지 자동으로 확인합니다.

장치를 다시 로드하거나 구성을 변경하는 등의 방법으로 장치가 변경될 때마다 NA에서는 장치 그룹에 할당된 정책에 따라 장치를 확인합니다. 장치의 정책 확인에 실패하면 장치는 정책을 준수하지 않는 것으로 표시됩니다. 장치 또는 장치 그룹의 변경 사항이 표준을 준수하지 않는 경우에는 NA 정책 관리자에서 알림 규칙을 트리거하는 이벤트를 생성합니다. 따라서 사용자는 비준수 변경 사항을 수정하고 준수 및 네트워크 가용성을 유지할 수 있습니다.

관리되는 모든 장치의 정책 준수 상태를 요약할 수 있습니다. 그러면 정책 준수 상태에서 위험과 관련된 스냅샷을 제공할 수 있으며 위험이 큰 구성 및 소프트웨어 수준 위반을 빠르게 식별하고 해결할 수 있습니다.

NA에서 장치의 정책 확인을 실행하면 각 규칙이 처리되며 규칙이 장치에 적용되는지 여부가 확인됩니다. 규칙이 적용되는 경우에는 규칙에 따라 장치를 테스트합니다. 규칙이 적용되지 않는 경우에는 그 장치에 대해 규칙을 건너뜁니다.

규칙은 두 가지 방법으로 적용할 수 있습니다.

- 규칙이 장치 제품군별로 적용됩니다. 규칙은 장치에서 Cisco IOS 또는 Juniper JunOS와 같은 특정 드라이버를 사용하는 경우에만 장치에 대해 확인됩니다. 예를 들어 Cisco IOS 드라이버가 있는 장치에 적용되는 규칙을 생성한 경우 이 규칙은 Extreme 스위치에 대해 확인되지 않습니다.
- 규칙이 장치 제품군에 관계 없이 적용됩니다. 규칙은 정규화된 데이터 모델의 확인 기준이므로 장치 제품군과 관계가 없습니다. 기본적으로 NA에서는 장치 정보를 데이터 모델에 대해 정규화된 요소로 구문 분석합니다. 여기에는 모델 번호, 호스트 이름, 위치 등의 장치 속성이 포함됩니다. 이 데이터는 모든 장치 제품군에서 정규화되기 때문에 장치 제품군과 관계 없이 적용됩니다. 따라서 모든 장치 제품군에 규칙을 적용하여 네트워크의 각 장치 제품군에 대해 특정한 규칙을 생성해야 할 필요가 없어집니다.

참고: 모든 장치 제품군에 대해 규칙을 설정한 경우에는 그 규칙에서 구성 또는 구성 블록 기준을 사용할 수 없습니다. 구성 및 구성 블록 형식은 장치 제품군별로 적용됩니다. 구성 또는 구성 블록 기준을 사용하며 규칙이 모든 장치 제품군을 지원하도록 설정하면 NA에서 각 장치 구성에서 구성 텍스트를 찾으려 하기 때문에 잘못 표시되는 결과가 많아집니다.

구성 텍스트를 확인하는 정책을 실행할 경우 NA가 기본적으로 선행 여백을 제거합니다. 따라서 선행 여백이 있는 구성 텍스트를 정의할 경우 여백 문자를 찾는 정규식을 수식화해야 합니다.

예를 들어 검색할 구성 텍스트가 다음과 같은 경우(라인 시작 부분에 선행 여백 2개가 있음):

```
description this yields unexpected results
```

일반적으로 다음 정규식을 사용하여 정책에서 찾을 구성 텍스트 블록을 정의하게 됩니다.

```
\s+description.*
```

참고: \s는 여백 문자와 일치하는 정규식입니다. 하지만 구성에 대해 정책을 실행할 경우 구성이 정책을 통과하지 못합니다. \s를 정책 규칙의 구성 텍스트 정의에서 제거할 경우 NA가 기본적으로 구성 텍스트에서 선행 여백을 제거하므로 구성이 정책을 통과합니다.

정책 생성

정책 규칙을 생성하려면 먼저 정책을 생성해야 합니다. 정책을 생성하려면 정책 아래의 메뉴 모음에서 정책 목록을 클릭합니다. 정책 페이지가 열립니다.

NA에서는 NSA 라우터 모범 사례 정책을 비롯한 여러 기본 정책을 함께 제공합니다. 구성할 만한 정책의 예에는 다음이 포함됩니다.

- 장치 그룹에 있는 모든 구성에는 액세스 목록 110이 정의되어 있어야 합니다.
- 모든 고속 이더넷 인터페이스에서는 이중을 자동 협상으로 설정해야 합니다.
- 모든 경계 라우터에는 특정 DNS 서버가 있어야 합니다.

참고: 새 정책 옵션을 클릭하여 새 정책 페이지로 바로 이동할 수도 있고 정책 페이지에서 기존 정책을 보다가 페이지 맨 위의 새 정책 링크를 클릭할 수도 있습니다.

정책 페이지 필드

필드	설명
새 정책 링크	새 구성 정책을 생성할 수 있는 새 정책 페이지를 엽니다. 자세한 내용은 514페이지의 "새 정책 페이지 필드" 를 참조하십시오.
정책 준수 확인 링크	정책 준수 확인 작업 페이지를 엽니다. 이 페이지에서 정책 준수 여부를 확인할 수 있습니다. 자세한 내용은 462페이지의 "정책 준수 확인 작업 페이지 필드" 를 참조하십시오. (참고: 메뉴 모음의 정책 --> 정책 작업에서 정책 준수 확인을 클릭하여 정책 준수 확인 작업 페이지로 이동할 수도 있습니다.)
가져오기/내보내기 링크	미리 구성된 구성 정책을 가져오거나 구성 정책을 파일로 내보낼 수 있는 정책 가져오기/내보내기 페이지를 엽니다. 자세한 내용은 524페이지의 "정책 가져오기/내보내기" 를 참조하십시오. (참고: 정책 가져오기/내보내기 옵션을 클릭하여 정책 가져오기/내보내기 페이지로 이동할 수도 있습니다.)
정책 태그 드롭다운 메뉴	정책 태그를 선택할 수 있습니다. 따라서 정책을 쉽게 그룹화할 수 있습니다.
확인란	<p>왼쪽의 확인란을 사용하여 구성 정책을 관리할 수 있습니다. 정책을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음을 클릭합니다.</p> <ul style="list-style-type: none"> • 활성화 — NA에서 선택한 정책을 기준으로 준수 구성을 확인하도록 설정합니다. • 비활성화 — NA에서 선택한 정책을 기준으로 준수 구성을 확인하지 않도록 설정합니다. • 일괄 편집 — 정책을 일괄 편집할 수 있습니다. 그 결과로 정책이 적용되는 정책 상태(활성 또는 비활성) 및 장치 그룹(범위)을 쉽게 변경할 수 있습니다. • 삭제 — 선택한 정책을 삭제합니다. <p>인접한 선택 드롭다운 메뉴를 통해 모든 정책을 선택하거나 선택 취소할 수 있습니다.</p>
정책 이름	정책 이름을 표시합니다.
상태	정책의 상태를 활성 또는 비활성으로 표시합니다.

필드	설명
파티션	보안 또는 비즈니스상의 이유로 파티션을 생성한 경우 특정 파티션에 대해 정책을 파티셔닝할 수 있습니다. 특정 파티션의 특정 사용자뿐만 아니라 파티션의 모든 사용자가 공유하도록 정책을 구성할 수 있습니다. 모든 파티션에서 정책을 사용할 수 있으면 [공유]라는 레이블이 붙습니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
CVE	CVE(Common Vulnerabilities and Exposures) 이름을 표시합니다. CVE는 취약점의 표준화된 이름과 보안 노출에 관한 기타 정보의 목록입니다.
생성 날짜	정책이 생성된 날짜를 표시합니다.
작업	다음 작업을 선택할 수 있습니다. <ul style="list-style-type: none"> •보기 및 편집 — 구성 정책을 편집할 수 있는 정책 편집 페이지를 엽니다. 자세한 내용은 525페이지의 "정책 편집"을 참조하십시오. •테스트 — 장치 또는 장치 그룹의 정책을 테스트할 수 있는 정책 테스트 페이지를 엽니다. (참고: 정책에 규칙이 포함되어 있는지 확인하는 과정에서 성능 문제가 발생할 수 있으므로 각 정책 옆에는 테스트 가능 여부에 관계없이 테스트 옵션이 표시됩니다. 자세한 내용은 546페이지의 "정책 테스트 페이지 필드"을 참조하십시오.)

새 정책 페이지 필드

새 정책 페이지를 열려면 정책 아래의 메뉴 모음에서 새 정책을 클릭합니다. 새 정책 페이지가 열립니다.

필드	설명/작업
새 정책	
정책 이름	정책 이름을 입력합니다. 정책은 장치 또는 장치 그룹에 적용되는 규칙 집합입니다.
정책 설명	정책의 설명을 입력합니다.
파티션	드롭다운 메뉴에서 파티션을 선택합니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다.) 일반적으로 파티션이란 고유한 IP 주소를 갖는 장치의 그룹입니다. 단일 NA 코어로 여러 파티션을 관리할 수 있습니다. 설치된 NA 서버의 NA 코어는 단일 관리 엔진, 연관된 서비스 및 단일 데이터베이스로 구성되어 있습니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
정책 태그	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 일반 목적 — 정책에 태그를 지정하지 않는 경우 일반 목적 정책으로 사용 됩니다. • 기존 — 드롭다운 메뉴에서 태그를 선택합니다. • 새로 만들기 — 태그 이름을 입력하여 새 정책 태그를 생성합니다.
범위	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 이 정책이 적용되는 장치 그룹 선택 — 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. • 동적 필터 범위 정의를 위해 필터 사용 — 정책 범위에는 정책으로 영향을 받을 수 있는 장치가 포함됩니다. 장치가 포함된 장치 제품군에 영향을 주는 정책 규칙이 정책에 들어 있는 경우에만 정책 범위로 장치에 영향을 줄 수 있습니다. 정책을 정의할 때에는 동적 그룹을 정의하는 것과 같은 방법으로 정책 범위를 정의할 수 있습니다. 따라서 정책과 함께 개인 동적 그룹을 생성할 수 있습니다. 동적 그룹 생성에 대한 자세한 내용은 180페이지의 "동적 장치 그룹"을 참조하십시오.

필드	설명/작업
검색 기준 (필터를 사용하여 동적 정책 범위를 정의하는 경우)	기준 추가 드롭다운 메뉴에서 검색 기준을 선택할 때마다 선택된 항목이 검색 기준 섹션에 표시됩니다. 이 위치에서는 다음을 포함, 일치, 다음과 같음 등의 연산자를 선택할 수도 있고 검색할 정보를 입력할 수도 있습니다. 정의된 기준을 삭제하려면 검색 기준 인덱스 문자 옆의 X를 클릭합니다.
기준 추가	<p>드롭다운 메뉴에서 다음과 같은 검색 기준을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> •구성 텍스트 •장치 IP •장치 상태 •호스트 이름 •암호 규칙
부울 표현식	
표현식	<p>기본적으로 정의된 기준 인덱스 문자는 부울 'and' 표현식과 함께 표시됩니다. 예를 들어 3개의 검색 기준을 정의하면 표현식은 <i>A and B and C</i>와 같이 됩니다. 부울 표현식은 필요에 따라 편집할 수 있습니다. 표현식을 기본값으로 재설정하려면 표현식 재설정 버튼을 클릭합니다. (참고: 부울 연산자는 소문자로 입력해야 합니다. 또한 최대 기준 수는 10개입니다.)</p>
장치 그룹으로 검색 제한	
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> •선택한 그룹 중 하나(기본값) •선택한 그룹 모두 •선택한 그룹 모두 없음 <p>참고: 여러 장치 그룹을 선택/선택 취소하려면 Shift를 누른 상태에서 클릭하십시오. 장치 그룹을 선택하지 않으면 NA는 검색 시 장치 그룹 필터를 무시합니다.</p>
보기 및 파티션으로 검색 제한 (보기 및 파티션을 구성한 경우에 이 정보가 표시됩니다. 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.)	

필드	설명/작업
예외 장치	오른쪽 상자에 장치의 IP 주소 또는 호스트 이름을 입력한 다음 예외 추가 <<를 클릭합니다. 장치를 제거하려면 왼쪽 상자에서 장치의 IP 주소 또는 호스트 이름을 선택하고 예외 제거를 클릭합니다.
정책 규칙	정책 규칙 테이블에는 정책에 의해 적용되는 모든 규칙이 표시됩니다. 정책에서는 이 정책에 대해 선택한 저장된 장치 각각에 모든 규칙을 적용합니다. 규칙은 특정한 순서 없이 적용됩니다.
새 규칙 버튼	이 정책에 대해 새 규칙을 생성하려면 새 규칙 버튼을 클릭합니다. 새 규칙 페이지가 열립니다. 자세한 내용은 518페이지의 "새 규칙 페이지 필드" 를 참조하십시오.
자세한 설명	정책이 자세한 설명을 입력합니다. 정책이 나타나는 모든 목록에는 정책에 대한 짧은 설명이 표시됩니다. 이 필드를 사용하면 정책에 대한 자세한 설명을 추가할 수 있습니다.
정책 상태	다음 옵션 중 하나를 클릭합니다. <ul style="list-style-type: none"> •활성 — 정책을 활성화로 표시합니다(기본값). •비활성 — 정책을 비활성화합니다.
추가 정책 필드(정책이 HP Security and Compliance Service에서 제공된 경우에는 이 필드가 자동으로 입력됩니다.)	
CVE	CVE(Common Vulnerabilities and Exposures) 이름을 입력합니다. CVE는 취약점의 표준화된 이름과 보안 노출에 관한 기타 정보의 목록입니다. 자세한 내용은 www.cve.mitre.org 를 참조하십시오.
공급업체 자문 URL	취약점에 관한 자문 정보를 얻을 수 있는 외부 참조 URL을 입력합니다. 정책을 만들고 공급업체 자문 URL 및/또는 공급업체 솔루션 URL을 포함하는 경우 URL은 http:// 접두사로 시작되어야 합니다. 그렇지 않으면 브라우저에서 링크를 올바르게 해석하지 못할 수 있습니다. URL 링크가 비어 있는 경우 URL 링크를 선택하면 링크가 NA 홈 페이지를 엽니다.
솔루션 링크	취약점을 해결할 수 있는 솔루션에 대한 자세한 정보를 볼 수 있는 외부 참조 URL을 입력합니다.
공개 날짜	소프트웨어 취약점에 yyyy-MM-dd 형식의 플래그가 지정된 날짜를 입력합니다.

필드	설명/작업
솔루션	자세한 솔루션 정보를 입력합니다.

완료되면 저장 버튼을 클릭해야 합니다.

새 규칙 페이지 필드

새 정책 페이지에서 새 규칙 버튼을 클릭하면 새 규칙 페이지가 열립니다. 규칙은 두 가지로 적용될 수 있습니다.

- 규칙이 장치 제품군별로 적용됩니다. 규칙은 장치에서 Cisco IOS 또는 Juniper JunOS와 같은 특정 드라이버를 사용하는 경우에만 장치에 대해 확인됩니다. 예를 들어 Cisco IOS 드라이버가 있는 장치에 적용되는 규칙을 생성한 경우 이 규칙은 Extreme 스위치에 대해 확인되지 않습니다.
- 규칙이 장치 제품군에 관계 없이 적용됩니다. 규칙은 정규화된 데이터 모델의 확인 기준이므로 장치 제품군과 관계가 없습니다. 기본적으로 NA에서는 장치 정보를 데이터 모델에 대해 정규화된 요소로 구문 분석합니다. 여기에는 모델 번호, 호스트 이름, 위치 등의 장치 속성이 포함됩니다. 이 데이터는 모든 장치 제품군에서 정규화되기 때문에 장치 제품군과 관계 없이 적용됩니다. 따라서 모든 장치 제품군에 규칙을 적용하여 네트워크의 각 장치 제품군에 대해 특정한 규칙을 생성해야 할 필요가 없어집니다.

필드	설명/작업
새 규칙	
규칙 이름	규칙 이름을 입력합니다.
규칙 유형	<p>규칙 유형을 선택합니다. 예를 들어 선택한 장치의 구성 텍스트로부터 풀링한 구성 텍스트 또는 데이터 모델 요소를 기반으로 규칙을 정의할 수 있습니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 구성 — 이 옵션을 선택하면 구성 규칙에서는 선택한 장치 구성 텍스트가 현재 구성 규칙에 맞는지 확인합니다. • 진단 — 이 옵션을 선택하면 규칙에서는 선택한 장치 진단 텍스트가 현재 진단 규칙에 맞는지 확인합니다. 진단 텍스트는 진단을 실행하여 생성됩니다. 자세한 내용은 397페이지의 "진단 실행 작업 페이지 필드"를 참조하십시오. (참고: 정책 규칙에 기반이 되는 진단의 이름을 바꿀 때 각별히 주의하십시오. 정책 규칙의 기반이 되는 진단의 이름을 바꿀 경우 정책 규칙 조건이 손실됩니다. • 소프트웨어 — 이 옵션을 선택하면 규칙에서는 선택한 장치가 현재 소프트웨어 규칙에 맞는지 확인합니다. 자세한 내용은 772페이지의 "소프트웨어 수준 보고서 필드"를 참조하십시오.

필드	설명/작업
규칙 설명	규칙의 설명을 입력합니다.
이 드라이버가 있는 장치에 적용됩니다.	
모든 장치 제품군	<p>모든 장치 제품군에 규칙을 적용하려면 이 라디오 버튼을 클릭합니다. 기본적으로 NA에서는 장치 정보를 데이터 모델에 대해 정규화된 요소로 구문 분석합니다. 여기에는 모델 번호, 호스트 이름, 위치 등의 장치 속성이 포함됩니다. 이 데이터는 모든 장치 제품군에서 정규화되기 때문에 장치 제품군과 관계 없이 적용됩니다.</p> <p>참고: 모든 장치 제품군에 대해 규칙을 설정한 경우에는 그 규칙에서 구성 또는 구성 블록 기준을 사용할 수 없습니다. 구성 및 구성 블록 형식은 장치 제품군별로 적용됩니다. 구성 또는 구성 블록 기준을 사용하며 규칙이 모든 장치 제품군을 지원하도록 설정하면 NA에서 각 장치 구성에서 구성 텍스트를 찾으려 하기 때문에 잘못 표시되는 결과가 많아집니다.</p>
장치 제품군	<p>드롭다운 메뉴에서 규칙을 적용할 장치 제품군을 선택합니다. 예를 들면 BayStack, Cisco IOS 또는 Nortel ASF가 있습니다. 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 모든 해당 드라이버 — 이 옵션을 선택하면(기본값) NA에서 해당 드라이버가 모두 선택됩니다. 규칙은 특정 드라이버가 할당된 장치에만 적용됩니다. • 특정 드라이버 선택 — 이 옵션을 선택한 경우에는 목록에서 드라이버를 하나 이상 선택합니다. 구성 규칙은 특정 드라이버가 할당된 장치의 구성에만 적용됩니다.
텍스트 블록 정의	<p>구성 블록 조건에서 사용할 텍스트 블록을 선택할 수 있도록 설정합니다. 텍스트 블록 설정 옵션을 선택하면 블록 시작 패턴 및 블록 끝 패턴 필드가 표시됩니다. 이러한 필드는 "구성 블록" 유형의 조건이 추가되는 경우에만 사용됩니다. 조건은 구성 파일에 있는 특정 텍스트 블록(Cisco IOS 장치에 있는 단일 인터페이스 등)에 적용됩니다. 구성 파일에 있는 특정 블록의 인스턴스마다 규칙을 적용하려면 블록 시작 패턴(<i>interface.*</i> 등)과 블록 끝 패턴(! 등)을 입력합니다.</p>

필드	설명/작업
텍스트 블록 정의(계속)	<p>블록 시작 및 끝 패턴에 의해 추출된 구성 텍스트에 시작 및 끝 패턴과 일치하는 라인이 포함됩니다. 따라서 구성 블록 조건이 시작 패턴과 끝 패턴 사이에 있는 라인뿐만 아니라, 시작 및 끝 패턴과 일치하는 라인에 대해서도 일치됩니다. 예를 들어, 다음과 같은 블록 시작 및 끝 패턴이 있는 경우:</p> <pre>block start: interface .* block end : !</pre> <p>그리고 구성 텍스트에 다음 라인이 포함됩니다.</p> <pre>... no service pad service timestamps log uptime service timestamps log uptime interface FastEthernet0/7 description testfor bug 145762 speed 100 duplex full ! ip default-gateway 10.255.1.1 ip http server ...</pre> <p>구성 블록 조건 일치에 사용될 구성의 추출된 부분은 다음과 같습니다.</p> <pre>interface FastEthernet0/7 description testfor bug 145762 speed 100 duplex full !</pre> <p>시작 및 끝 패턴이 각각 interface FastEthernet0/7 및 !와 일치하는 라인이 포함됩니다.</p>

필드	설명/작업
규칙 조건	<p>드롭다운 메뉴에서 구성 텍스트, 플래시 메모리 및 호스트 이름과 같은 조건을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> • 정규 표현식 — 이 옵션을 선택하면 패턴이 정규 표현식이 됩니다. 이 옵션을 선택하지 않으면 패턴은 구성(진단) 텍스트 또는 데이터 모델 요소 값과 일치시킬 문자열이 됩니다. • 포함해야 함 — 구성(진단) 텍스트 또는 데이터 모델 요소 값에 패턴이 포함되어야 합니다. • 포함하지 않아야 함 — 구성(진단) 텍스트 또는 데이터 모델 요소 값에 패턴이 포함되지 않아야 합니다. • 다음만 포함해야 함 — 구성(진단) 텍스트 또는 데이터 모델 요소 값에 패턴은 포함되어야 하지만 "그러나 다음을 포함하는 추가 라인이 없어야 함" 필드에 지정된 패턴과 일치하는 다른 모든 항목은 포함되지 않아야 합니다. • 정확한 순서의 라인 — 이 옵션을 선택하면 패턴 라인이 지정된 순서로 일치되어야 합니다. 조건 패턴의 각 라인은 독립 패턴으로 해석되어 별도로 확인됩니다. 이 옵션을 선택하면 독립된 일치 항목은 일치하지 않는 문자(공백 제외) 없이 지정된 순서가 되어야 합니다. <p>"and" 및 "or"를 사용하여 부울 표현식을 구성하는 것 외에도 "if-then-else" 논리를 사용하여 조건 규칙을 구성할 수 있습니다. 이 때 선택적으로 "else"를 사용할 수도 있습니다. 예를 들어 "A"부터 "E"까지의 다섯 가지 조건을 정의한 경우 <i>"if (A and B) then (C or D) else E"</i>와 같은 부울 표현식을 구성할 수 있습니다. (참고: 부울 연산자는 소문자로 입력해야 합니다. 또한 최대 기준 수는 10개입니다.)</p> <p>도움말 보기 링크에서는 정규 표현식 사용에 대한 정보를 제공합니다. 장치 변수 링크를 클릭하면 장치 변수 페이지가 열립니다. 이 페이지에는 정책 규칙 정의에 사용할 수 있는 기본 제공 변수 목록이 포함되어 있습니다. 따라서 정책 규칙을 확인하면 해당 값이 대체됩니다.</p> <p>표현식을 기본값으로 재설정하려면 표현식 재설정 버튼을 클릭합니다.</p>

필드	설명/작업
중요도	<p>중요도 수준을 선택합니다. 이 값은 정책 규칙의 비준수 위험 등급을 나타냅니다. NA에서는 심각도에 따라 위반을 정렬할 수 있습니다. 예를 들어, 심각한 위반이 발생한 경우에는 변경 관리 시스템에 문제 티켓이 열릴 수 있지만 정보 위반이 발생한 경우에는 매일의 보고서에만 표시됩니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> •정보용 — 일반적으로 응답이 필요하지 않은 이벤트 •낮음 — 시간이 허용될 경우 응답이 필요할 수 있는 이벤트 •중간 — 일반적으로 72시간(기본값) 이내에 시기 적절한 응답이 필요한 이벤트 •높음 — 일반적으로 24시간 이내에 신속한 응답이 필요한 이벤트 •심각 — 즉각적인 응답이 필요한 이벤트
자세한 설명	<p>규칙의 설명을 입력합니다.</p>
규칙 예외	<p>규칙 예외가 있는 경우 규칙 예외 목록을 표시합니다. 규칙 예외도 규칙의 일부입니다. 예를 들어, 규칙 예외를 통해 장치 구성이 일치하는 텍스트를 구성 규칙의 고려 대상에서 제외할 수 있습니다.</p> <p>예외 규칙을 추가하려면 새 예외 링크를 클릭합니다. 새 규칙 예외 페이지가 열립니다. (자세한 내용은 529페이지의 "규칙 예외 추가"를 참조하십시오.)</p>

필드	설명/작업
자동 수정 스크립트	<p>자동 수정 팝업 창에서는 정책 규칙 페이지의 데이터에 액세스하여 변수 매핑을 표시하고, 샘플 코드를 생성하며, 스크립트를 저장하기 전에 검증할 수 있습니다.</p> <p>자동 수정 스크립트를 사용하면 위반된 정책 규칙의 정규 표현식 패턴 그룹에서 데이터를 참조하는 변수를 스크립트에 정의할 수 있습니다. 자세한 내용은 726페이지의 "자동 수정 스크립트 생성"을 참조하십시오.</p> <p>새 자동 수정 스크립트를 추가하려면 새 자동 수정 스크립트 링크를 클릭합니다. 자동 수정 스크립트 팝업 창에는 명령 스크립트 페이지가 있습니다. 자동 수정 스크립트를 입력하는 데 도움을 주려면 다음 링크를 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 변수 표시 — 변수 매핑을 정규 표현식 패턴으로 표시합니다. 따라서 패턴의 어떤 부분이 어떤 정규 표현식 그룹에 적용되는지 확인할 수 있습니다. 정규 표현식 패턴에서 강조 표시된 부분은 왼쪽의 변수에서 참조됩니다. 변수에서 (.*) 앞에 있는 섹션은 @foreach 루프 변수로 대체되어야 합니다. 변수 이름에는 정규 표현식 그룹이 표시됩니다. 또한 정규 표현식 그룹 영(0)은 전체 패턴을 나타냅니다. • 샘플 코드 생성 — 사용할 수 있는 변수로 샘플 템플릿 코드를 생성합니다. 장치 명령을 @foreach 루프에 추가해야 합니다. 장치 명령은 위의 생성된 각 루프에 나열된 변수를 참조할 수 있습니다.

완료되면 저장 버튼을 클릭하여 규칙을 저장하거나, 저장 및 다른 항목 추가 버튼을 클릭하여 현재 규칙을 저장한 후 새 규칙을 추가하거나, 새 예외 링크를 클릭하여 새 규칙 예외를 추가할 수 있습니다.

정책 가져오기/내보내기

미리 정의된 정책을 가져오거나 정책을 파일로 내보낼 수 있습니다. 이 방법으로 정책을 쉽게 공유할 수 있습니다.

정책을 가져오거나 내보내려면 정책 아래의 메뉴 모음에서 정책 가져오기/내보내기를 클릭합니다. 정책 가져오기/내보내기 페이지가 열립니다.

참고: NA에서는 NA 6.2부터 이전 버전의 정책을 가져올 수 있습니다.

정책 가져오기/내보내기 페이지 필드

필드	설명/작업
정책 가져오기	가져올 정책 파일을 입력하거나 찾아보기 버튼을 클릭하여 정책 파일을 찾습니다. 정책 파일이 표시되면 가져오기 버튼을 클릭합니다. 정책이 이미 있는 경우에는 이름을 바꾸라는 내용의 프롬프트가 표시됩니다.
정책 내보내기	현재 구성 정책의 목록을 표시합니다. 내보낼 구성 정책을 클릭한 다음 내보내기 버튼을 클릭합니다. 구성 정책과 연결되어 있는 장치 그룹은 내보낼 수 없습니다. 구성 정책 예외 규칙도 내보내지 않습니다.

정책 편집

정책을 편집하려면

1. 정책 아래의 메뉴 모음에서 정책 목록을 클릭합니다. 정책 페이지가 열립니다.
2. 편집할 정책의 보기 및 편집 작업을 클릭합니다. 정책 편집 페이지가 열립니다. 설정이 완료되면 저장을 클릭해야 합니다.

정책 편집 페이지 필드

필드	설명/작업
정책 이름	정책 이름을 표시합니다.
정책 설명	정책의 설명을 표시합니다.
파티션	드롭다운 메뉴에서 파티션을 선택합니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다.) 일반적으로 파티션이란 고유한 IP 주소를 갖는 장치의 그룹입니다. 단일 NA 코어로 여러 파티션을 관리할 수 있습니다. 설치된 NA 서버의 NA 코어는 단일 관리 엔진, 연관된 서비스 및 단일 데이터베이스로 구성되어 있습니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
정책 태그	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 일반 목적 — 정책에 태그를 지정하지 않는 경우 일반 목적 정책으로 사용됩니다. • 기존 — 드롭다운 메뉴에서 새 정책을 선택합니다. • 새로 만들기 — 정책의 위치를 입력합니다.

필드	설명/작업
범위	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 정책이 적용되는 장치 그룹 선택 — 목록에서 장치 그룹을 하나 이상 선택합니다. Shift 키 또는 Ctrl 키를 누른 채로 클릭하여 여러 장치 그룹을 선택할 수 있습니다. • 동적 필터 범위 정의를 위해 필터 사용 — 정책 범위에는 정책으로 영향을 받을 수 있는 장치가 포함됩니다. 장치가 포함된 장치 제품군에 영향을 주는 정책 규칙이 정책에 들어 있는 경우에만 정책 범위로 장치에 영향을 줄 수 있습니다. 정책을 정의할 때에는 동적 그룹을 정의하는 것과 같은 방법으로 정책 범위를 정의할 수 있습니다. 따라서 정책과 함께 개인 동적 그룹을 생성할 수 있습니다. 동적 그룹 생성에 대한 자세한 내용은 180페이지의 "동적 장치 그룹"을 참조하십시오. <p>검색 기준(필터를 사용하여 동적 정책 범위를 정의하는 경우) 기준 추가 드롭다운 메뉴에서 검색 기준을 선택할 때마다 선택된 항목이 검색 기준 섹션에 표시됩니다. 이 위치에서는 다음을 포함, 일치, 다음과 같음 등의 연산자를 선택할 수도 있고 검색할 정보를 입력할 수도 있습니다. 정의된 기준을 삭제하려면 검색 기준 인덱스 문자 옆의 X를 클릭합니다.</p>
기준 추가	<p>드롭다운 메뉴에서 다음과 같은 검색 기준을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> • 구성 텍스트 • 장치 IP • 장치 상태 • 암호 규칙 • 호스트 이름
부울 표현식	
표현식	<p>기본적으로 정의된 기준 인덱스 문자는 부울 'and' 표현식과 함께 표시됩니다. 예를 들어 3개의 검색 기준을 정의하면 표현식은 <i>A and B and C</i>와 같이 됩니다. 부울 표현식은 필요에 따라 편집할 수 있습니다. 표현식을 기본값으로 재설정하려면 표현식 재설정 버튼을 클릭합니다. (참고: 부울 연산자는 소문자로 입력해야 합니다. 또한 최대 기준 수는 10개입니다.)</p>
장치 그룹으로 검색 제한	

필드	설명/작업
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> • 선택한 그룹 중 하나(기본값) • 선택한 그룹 모두 • 선택한 그룹 모두 없음 <p>참고: 여러 장치 그룹을 선택/선택 취소하려면 Shift를 누른 상태에서 클릭하십시오. 장치 그룹을 선택하지 않으면 NA는 검색 시 장치 그룹 필터를 무시합니다.</p>
<p>보기 및 파티션으로 검색 제한(보기 및 파티션을 구성한 경우에 이 정보가 표시됩니다. 자세한 내용은 191페이지의 "장치 및 사용자 세분화"를 참조하십시오.)</p>	
예외 장치	<p>장치의 IP 주소 또는 호스트 이름을 추가하려면 오른쪽 상자에 호스트 이름 또는 IP 주소를 입력한 다음 예외 추가 <<를 클릭합니다. 장치를 제거하려면 왼쪽 상자에서 장치의 IP 주소 또는 호스트 이름을 선택하고 예외 제거를 클릭합니다.</p>
정책 규칙	<p>정책으로 적용할 모든 규칙을 표시합니다. 정책에서는 이 정책에 대해 선택한 저장된 장치 각각에 모든 구성 규칙을 적용합니다. 규칙은 특정한 순서 없이 적용됩니다. 중요도 열에는 정보용, 낮음, 중간, 높음 또는 심각이 표시됩니다. 이 값은 정책 규칙의 비준수 위험 등급을 나타냅니다. 규칙을 편집하려면 작업 열에서 보기 및 편집 링크를 클릭합니다.</p>
새 규칙 버튼	<p>이 정책에 대해 새 규칙을 생성하려면 새 규칙 버튼을 클릭합니다. 새 규칙 페이지가 열립니다. 자세한 내용은 518페이지의 "새 규칙 페이지 필드"를 참조하십시오.</p>
자세한 설명	<p>정책의 자세한 설명을 표시합니다.</p>
정책 상태	<p>다음 옵션 중 하나를 클릭합니다.</p> <ul style="list-style-type: none"> • 활성화 — 정책을 활성화로 표시합니다(기본값). • 비활성 — 정책을 비활성화합니다.
<p>소프트웨어 정책 필드(정책이 HP Security and Compliance Service에서 제공된 경우에는 이 필드가 자동으로 입력됩니다.)</p>	

필드	설명/작업
CVE	CVE(Common Vulnerabilities and Exposures) 이름을 표시합니다. CVE는 취약점의 표준화된 이름과 보안 노출에 관한 기타 정보의 목록입니다. 자세한 내용은 www.cve.mitre.org 를 참조하십시오.
공급업체 자문 URL	취약점에 대한 자문 정보를 볼 수 있는 외부 참조의 URL을 표시합니다.
솔루션 링크	취약점을 해결할 수 있는 솔루션에 대한 자세한 정보를 볼 수 있는 외부 참조 URL을 표시합니다.
공개 날짜	소프트웨어에 플래그가 지정된 날짜를 <i>yyyy-MM-dd</i> 형식으로 표시합니다.
솔루션	자세한 솔루션 정보를 표시합니다.

규칙 예외 추가

규칙 예외도 규칙의 일부입니다. 규칙과 마찬가지로 규칙 예외 역시 정규 표현식입니다. 하지만 규칙 예외의 목적은 장치 구성에서 일치하는 텍스트를 속한 구성 규칙의 고려에서 제외하는 것입니다.

예외 규칙으로는 보통 구성 규칙의 텍스트 패턴 또는 특정 장치 구성을 제외합니다. 예외는 보통 규칙에 맞지 않는 장치 구성이 하나 이상 있지만 그러한 구성을 위해 규칙을 수정할 수 없는 경우에 생성합니다.

기존 구성 규칙에 규칙 예외를 추가하려면

1. 정책 아래의 메뉴 모음에서 정책 목록을 클릭합니다. 정책 페이지가 열립니다.
2. 예외를 추가할 정책을 선택하고 보기 및 편집을 클릭합니다. 정책 편집 페이지가 열립니다.
3. 정책 내에서 예외가 필요한 규칙을 찾고 보기 및 편집을 클릭합니다. 새 규칙 페이지가 열립니다.
4. 페이지의 아래쪽에 있는 새 예외 링크를 클릭합니다. 새 규칙 예외 페이지가 열립니다.

새 규칙 예외 페이지 필드

필드	설명/작업
장치	이 예외 규칙이 적용되는 장치의 IP 주소 또는 호스트 이름을 입력합니다.
다음에 만료	이 옵션을 선택한 경우에는 규칙에 의해 예외를 무시할 경과 시간을 월, 일, 년, 시간, 분 단위로 선택합니다. 예외 규칙의 만료 날짜는 규칙에서 예외가 더 이상 영향을 주지 못하게 되는 경과 날짜를 나타냅니다. 만료 날짜가 지나도 예외 규칙은 계속 존재하지만 구성 정책은 예외 규칙이 존재하지 않는 것처럼 적용됩니다.
구성 규칙을 확인할 때 이 패턴과 일치하는 텍스트 무시	이 옵션을 선택한 경우에는 텍스트를 입력합니다. 장치 구성에서 입력한 텍스트와 일치하는 모든 텍스트에는 이 구성 규칙이 적용되지 않습니다. (참고: 도움말 보기 링크를 클릭하면 이에 대한 예를 볼 수 있습니다.)
구성 규칙을 확인할 때 이 장치 완전히 무시	이 옵션을 선택하면 NA에서 구성 규칙을 확인할 때 이 장치를 건너뛸 것입니다.

완료되면 저장 버튼을 클릭해야 합니다.

적용된 정책 보기

장치에 적용되는 정책을 볼 수 있습니다. 따라서 다음을 수행할 수 있습니다.

- 현재 정책이 장치에 적용되었는지 확인
- 정책 통과/실패 여부 보기
- 장치가 NA에 추가될 때 장치에 적용되는 정책 보기
- 장치에 적용된 정책에 대한 예외 보기

적용된 정책을 보려면

1. 장치의 새 정책을 만듭니다. 자세한 내용은 [511페이지의 "정책 생성"](#)을 참조하십시오.
2. 장치에 대해 정책을 실행합니다. 자세한 내용은 [534페이지의 "정책 준수 테스트 페이지 필드"](#)를 참조하십시오.
3. 해당 장치에 대한 장치 세부사항 페이지를 엽니다.
4. 보기 메뉴를 클릭합니다.
5. 장치 세부사항을 선택하고 정책을 클릭합니다. 장치 정책 페이지가 엽니다. 자세한 내용은 [290페이지의 "장치 정책 페이지 필드"](#)를 참조하십시오.

정책 활동 보기

하나 이상의 정책에 포함된 규칙을 준수하지 않는 장치 구성을 이벤트로 표시하여 볼 수 있습니다. 이벤트에는 NA에서 장치의 비준수 사실을 감지하여 기록한 시기가 표시됩니다.

정책 활동 페이지를 보려면 정책 아래의 메뉴 모음에서 정책 활동을 클릭합니다. 정책 활동 페이지가 열립니다.

정책 활동 페이지 필드

필드	설명/작업
다음 대상(시간 프레임)	비준수 이벤트를 볼 시간 프레임을 선택합니다. 기본값은 최근 1시간입니다.
현재 작업 그룹	비준수 이벤트를 볼 대상 그룹을 선택합니다. 기본값인 인벤토리에는 다른 모든 그룹이 포함됩니다.
이벤트 날짜	정책의 비준수 사실이 발견된 날짜를 표시합니다.
정책 이름	정책의 이름을 표시합니다. 이 링크를 클릭하면 정책 편집 페이지가 열립니다. 정책과 포함된 규칙을 편집할 수 있습니다. 자세한 내용은 525페이지 의 "정책 편집"을 참조하십시오.
호스트 이름	장치의 호스트 이름을 표시합니다. 장치에 대한 기본 정보를 보려면 이 링크를 클릭합니다.
장치 IP	장치의 IP 주소를 표시합니다. 장치에 대한 기본 정보와 구성 이력을 보려면 이 링크를 클릭합니다.
요약	이벤트 유형을 표시합니다(구성 정책 비준수). 이 링크를 클릭하면 시스템 이벤트 세부사항 페이지가 열리며 비준수 이벤트의 세부사항을 볼 수 있게 됩니다.

필드	설명/작업
중요도	<p>위반된 규칙의 중요도를 나타내며, 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none">• 정보용 — 일반적으로 응답이 필요하지 않은 이벤트• 낮음 — 시간이 허용될 경우 응답이 필요할 수 있는 이벤트• 중간 — 일반적으로 72시간 이내에 시기 적절한 응답이 필요한 이벤트• 높음 — 일반적으로 24시간 이내에 신속한 응답이 필요한 이벤트• 심각 — 즉각적인 응답이 필요한 이벤트

정책 준수 보기

정책 준수 페이지에서는 구성이 구성 정책에 맞는 장치와 맞지 않는 장치를 볼 수 있습니다.

정책 준수 페이지를 보려면 정책 아래의 메뉴 모음에서 정책 준수를 클릭합니다. 정책 준수 페이지가 열립니다.

정책 준수 테스트 페이지 필드

필드	설명/작업
정책 준수 확인 링크	정책 준수 확인 작업 페이지를 엽니다. 이 페이지에서 구성의 준수 여부를 확인할 수 있습니다. 자세한 내용은 462페이지의 "정책 준수 확인 작업 페이지 필드" 를 참조하십시오.
현재 작업 그룹	장치 준수 상태를 볼 그룹을 선택합니다.
준수하지 않는 장치만 표시합니다.	이 옵션을 선택하면 준수하는 장치가 표시되지 않습니다.
호스트 이름	장치의 호스트 이름을 표시합니다. 장치에 대한 기본 정보를 보려면 이 링크를 클릭합니다.
장치 IP	장치의 IP 주소를 표시합니다. 장치에 대한 기본 정보와 구성 이력을 보려면 이 링크를 클릭합니다.
정책 준수	<ul style="list-style-type: none"> 예 — 장치 구성이 모든 정책을 준수하는 것을 나타냅니다. 예 — 장치 구성이 일부 구성 정책을 준수하지 않음을 나타냅니다. 아니요를 클릭하면 구성 정책 활동 페이지가 열립니다. 자세한 내용은 532페이지의 "정책 활동 페이지 필드"를 참조하십시오. 알 수 없음 — 정책 준수가 확인되지 않은 장치를 나타냅니다.
파티션	장치가 속한 파티션이 있는 경우 파티션을 표시합니다.
마지막으로 변경된 시간	장치 구성이 마지막으로 변경된 날짜와 시간을 표시합니다.

필드	설명/작업
작업	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none">• 정책 이벤트 — 구성 정책 활동 페이지를 엽니다. 이 페이지에서 비준수 이벤트의 세부사항을 볼 수 있습니다. 자세한 내용은 532페이지의 "정책 활동 페이지 필드"를 참조하십시오.• 적용된 정책 — 장치에 적용되는 구성 정책 페이지를 엽니다. 이 페이지에서 특정 장치에 해당되는 구성 정책과 규칙을 볼 수 있습니다. 자세한 내용은 536페이지의 "장치에 적용되는 구성 정책 페이지 필드"를 참조하십시오.

장치에 적용되는 구성 정책 페이지 필드

장치에 적용되는 구성 정책 페이지를 보려면

1. 정책 아래의 메뉴 모음에서 정책 준수를 클릭합니다.
2. 정보가 필요한 장치의 작업 열에서 적용된 정책 링크를 클릭합니다. 장치에 적용되는 구성 정책 페이지가 열립니다.

필드	설명/작업
정책 이름	장치에 적용되는 구성 정책의 이름을 표시합니다.
규칙 이름	장치에 적용되는 구성 규칙의 이름을 표시합니다.
준수되지 않음 키	장치가 현재 준수되지 않는 경우 상태를 표시하며 다음이 포함됩니다. <ul style="list-style-type: none"> • 중요도 높음(빨간) • 중요도 중간(주황) • 중요도 낮음(녹색)
작업	선택할 수 있는 옵션은 다음과 같습니다. <ul style="list-style-type: none"> • 호스트 이름 또는 IP 주소 — 장치 정보 페이지를 엽니다. 이 페이지에서 장치에 대한 기본 정보와 구성 이력을 볼 수 있습니다. • 정책 이름 — 구성 정책 편집 페이지를 엽니다. 이 페이지에서 정책을 편집하고 구성 규칙을 추가/편집할 수 있습니다. 525페이지의 "정책 편집"을 참조하십시오. • 규칙 이름 — 구성 규칙 편집 페이지를 엽니다. 이 페이지에서 구성 규칙을 편집할 수 있습니다. 529페이지의 "규칙 예외 추가"를 참조하십시오.

새 소프트웨어 수준 추가

보안 취약점에 관한 네트워크 장치 보안 주의와 알림 수가 늘어남에 따라 여러 조직에서 각 장치에 있는 OS 버전과 그 OS 버전이 보안 문제에 취약한지 여부를 추적해야 할 필요성도 늘고 있습니다. NA에서는 보안 문제에 취약한 OS 버전을 지정한 다음 그 버전이 발견된 경우에 주의나 자동 응답을 생성할 수 있습니다. 이미지를 "사전 프로덕션"이나 "사용되지 않음"과 같은 범주로 그룹화할 수 있습니다. 또한 최근에 발견된 취약점 기준 "보안 위험"과 같이 이미지를 분류할 수도 있습니다.

새 소프트웨어 수준을 추가하거나 기존 준수 정의를 검토하려면

1. 정책 아래의 메뉴 모음에서 소프트웨어 수준을 클릭합니다. 소프트웨어 수준 페이지가 열립니다. 소프트웨어 수준 페이지에 대한 자세한 내용은 [540페이지의 "소프트웨어 수준 페이지 필드"](#)를 참조하십시오.
2. 수준 추가 링크를 클릭합니다. 수준 추가 페이지가 열립니다. 입력이 완료되면 저장 버튼을 클릭해야 합니다.

소프트웨어 수준 추가 페이지 필드

필드	설명/작업
소프트웨어 수준 추가	
수준 이름	수준 이름을 입력합니다.
상태	다음 옵션 중 하나를 표시합니다. <ul style="list-style-type: none"> •활성 — 구성 정책을 활성화로 표시합니다(기본값). •비활성 — 구성 정책을 비활성화합니다. 비활성 정책은 비준수 이벤트를 생성하지 않습니다.

필드	설명/작업
수준	<p>준수 등급 이름을 선택합니다. 요구 사항 및 검증 절차에 따라 주어진 준수 정의 중 어느 것이라도 사용할 수 있습니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 보안 위험 • 사전 프로덕션 • 사용되지 않음 • 브론즈 • 실버 • 골드 • 플래티늄
설명	<p>준수에 대한 설명을 입력합니다. 보안 문제에 대한 인식을 높이려면 보안 문제 설명에 취약점을 짧게 기록한 제목, 적용되는 CVE/CAN 또는 CERT 지정 사항 및 공급업체 알림 링크를 포함해야 합니다.</p>
파티션	<p>드롭다운 메뉴에서 파티션을 선택합니다. 보안 또는 비즈니스상의 이유로 파티션을 생성한 경우 특정 파티션에 대해 소프트웨어 수준을 파티셔닝할 수 있습니다. 특정 파티션의 특정 사용자뿐만 아니라 파티션의 모든 사용자가 공유하도록 정책을 구성할 수 있습니다. 모든 파티션에서 소프트웨어 수준을 사용할 수 있으면 [공유]라는 레이블이 붙습니다.</p>
일치 기준(일치 기준에 와일드카드 연산자(* 및 ?) 사용 가능)	
소프트웨어 버전	이 준수 정책이 적용되는 소프트웨어 버전을 입력합니다.
장치 드라이버	장치에 액세스하는 데 사용되는 장치 드라이버를 드롭다운 메뉴에서 선택합니다. (모두가 기본값입니다.)
장치 모델	장치 모델을 입력합니다.
파일 이름	해당되는 경우 파일 이름을 입력합니다.
구성에 포함	해당 장치에 준수가 적용되는지 확인하기 위해 현재 장치 구성과 일치하는 패턴을 입력합니다.
소프트웨어 취약점 정보(보안 위험 수준별)	
공개 날짜	소프트웨어 취약점에 yyyy-MM-dd 형식의 플래그가 지정된 날짜를 입력합니다.

필드	설명/작업
중요도	다음과 같은 보안 취약점의 심각도를 드롭다운 메뉴에서 선택합니다. <ul style="list-style-type: none"> • 정보용 • 낮음 • 중간 • 높음 • 심각
CVE 이름	CVE(Common Vulnerabilities and Exposures) 이름을 입력합니다. CVE는 취약점의 표준화된 이름과 보안 노출에 관한 기타 정보의 목록입니다. 자세한 내용은 www.cve.mitre.org 를 참조하십시오.
솔루션	솔루션 정보를 입력합니다.
자문 링크	취약점에 관한 자문 정보를 얻을 수 있는 외부 참조 URL을 입력합니다.
솔루션 링크	취약점을 해결할 수 있는 솔루션에 대한 자세한 정보를 볼 수 있는 외부 참조 URL을 입력합니다.

소프트웨어 수준 페이지 필드

NA에는 소프트웨어 수준, 기본적으로 소프트웨어 버전과 일치하는 정규 표현식을 정의하는 기능이 있습니다. 해당 정규 표현식에 소프트웨어 수준을 할당할 수 있습니다. 소프트웨어 버전이 정규 표현식과 일치하는 모든 장치는 해당 수준으로 고려됩니다.

참고: 소프트웨어 수준을 파티셔닝하여 적절한 권한이 있는 사용자만 해당 수준을 보고 편집하도록 할 수 있습니다. 자세한 내용은 [201페이지의 "파티션"](#)을 참조하십시오.

소프트웨어 수준 페이지를 사용하면 기존 소프트웨어 수준 정의를 검토할 수 있습니다.

필드	설명/작업
수준 추가 링크	소프트웨어 수준 추가 페이지를 엽니다. 이 페이지에서 소프트웨어 수준을 추가할 수 있습니다. 537페이지의 "소프트웨어 수준 추가 페이지 필드" 를 참조하십시오.
장치 소프트웨어 보고서 링크	현재 각 장치에 할당된 소프트웨어 버전 및 준수 등급을 볼 수 있는 장치 소프트웨어 보고서를 엽니다. 770페이지의 "장치 소프트웨어 보고서 필드" 를 참조하십시오.
소프트웨어 수준 보고서 링크	소프트웨어 수준 보고서를 엽니다. 이 보고서에서 현재 각 장치에 할당된 소프트웨어 수준을 볼 수 있습니다. 772페이지의 "소프트웨어 수준 보고서 필드" 를 참조하십시오.
보기	드롭다운 메뉴에서 "사용자 정의 정책" 또는 "보안 주의 서비스 주의"를 선택합니다. 보안 주의 서비스 주의를 보안 주의 서비스에서 오는 이벤트입니다. (참고: 보안 주의 서비스는 가입 기반 서비스입니다.)
확인란	왼쪽의 확인란을 사용하여 소프트웨어 수준 정의를 관리할 수 있습니다. 준수 정의를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음을 클릭합니다. <ul style="list-style-type: none"> •활성화 — NA에서 소프트웨어 수준 정의를 활성화하도록 지정합니다. •비활성화 — NA에서 소프트웨어 수준 정의를 비활성화하도록 지정합니다. •삭제 — 소프트웨어 수준 정의를 삭제합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 정책을 선택하거나 선택 취소할 수 있습니다.
이름	준수 이름을 표시합니다.

필드	설명/작업
버전	소프트웨어 버전을 표시합니다.
드라이버	드라이버 이름을 표시합니다.
모델	지정된 장치 모델이 표시됩니다.
파일 이름	시스템에서 준수 여부 확인에 사용되는 파일 이름을 입력할 수 있습니다. 와일드카드도 허용됩니다. 예를 들어 <code>router5*.bin</code> 으로 시작하는 모든 이미지에 사용되지 않음 태그를 지정할 수 있습니다.
소프트웨어 수준	<p>준수 등급 이름을 표시합니다. 다음과 같은 등급이 있습니다.</p> <ul style="list-style-type: none"> • 보안 위험 • 사전 프로덕션 • 사용되지 않음 • 브론즈 • 실버 • 골드 • 플래티늄
중요도	<p>정보용, 낮음, 중간, 높음 또는 심각이 표시됩니다. 이 값은 위반된 준수 규칙의 중요도를 나타냅니다.</p> <ul style="list-style-type: none"> • 정보용 — 일반적으로 응답이 필요하지 않은 이벤트 • 낮음 — 시간이 허용될 경우 응답이 필요할 수 있는 이벤트 • 중간 — 일반적으로 72시간 이내에 시기 적절한 응답이 필요한 이벤트 • 높음 — 일반적으로 24시간 이내에 신속한 응답이 필요한 이벤트 • 심각 — 즉각적인 응답이 필요한 이벤트
마지막 수정일	소프트웨어 수준이 마지막으로 수정된 시간을 표시합니다.
파티션	보안 또는 비즈니스상의 이유로 파티션을 생성한 경우 특정 파티션에 대해 소프트웨어 수준을 파티셔닝할 수 있습니다. 특정 파티션의 특정 사용자뿐 아니라 파티션의 모든 사용자가 공유하도록 소프트웨어 수준을 구성할 수 있습니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.

필드	설명/작업
CVE	CVE(Common Vulnerabilities and Exposures) 이름을 표시합니다. CVE는 취약점의 표준화된 이름과 보안 노출에 관한 기타 정보의 목록입니다.
주석	준수 설명을 표시합니다.
작업	선택할 수 있는 옵션은 다음과 같습니다. <ul style="list-style-type: none">• 편집 — 준수 값을 편집할 수 있는 준수 편집 페이지를 엽니다.• 삭제 — 준수를 삭제할 수 있습니다.

소프트웨어 수준 편집

소프트웨어 수준을 편집하려면

1. 정책 아래의 메뉴 모음에서 소프트웨어 수준을 클릭합니다. 소프트웨어 수준 페이지가 열립니다.
2. 편집할 소프트웨어 수준의 편집 작업을 클릭합니다. 소프트웨어 수준 편집 페이지가 열립니다. 설정이 완료되면 저장을 클릭해야 합니다.

소프트웨어 수준 편집 페이지 필드

필드	설명/작업
준수 편집	
수준 이름	정책 이름을 표시합니다.
상태	다음 옵션 중 하나를 표시합니다. <ul style="list-style-type: none"> •활성 — 구성 정책을 활성화로 표시합니다(기본값). •비활성 — 구성 정책을 비활성화합니다. 비활성 정책은 비준수 이벤트를 생성하지 않습니다.
수준	소프트웨어 수준 등급 이름을 표시합니다. 요구 사항 및 확인 절차에 따라 지정된 정의를 사용할 수 있습니다. 다음과 같은 옵션이 있습니다. <ul style="list-style-type: none"> •보안 위험 •사전 프로덕션 •사용되지 않음 •브론즈 •실버 •골드 •플래티늄
설명	준수 설명을 표시합니다.
일치하는 기준	
소프트웨어 버전	이 준수 정책이 적용되는 소프트웨어 버전을 표시합니다.

필드	설명/작업
장치 드라이버	장치 액세스에 사용된 장치 드라이버를 표시합니다.
장치 모델	장치 모델을 표시합니다.
구성에 포함	현재 장치 구성과의 일치성을 통해 장치 준수가 적용되는지 여부를 결정하는 일에 사용되는 패턴을 표시합니다.
소프트웨어 취약점 정보(보안 위험 준수 수준별)	
공개 날짜	소프트웨어 취약점 플래그가 지정된 날짜를 표시합니다.
중요도	보안 취약점의 심각도를 다음과 같이 표시합니다. <ul style="list-style-type: none"> • 정보용 • 낮음 • 중간 • 높음 • 심각
CVE 이름	CVE(Common Vulnerabilities and Exposures) 이름을 표시합니다. CVE는 취약점의 표준화된 이름과 보안 노출에 관한 기타 정보의 목록입니다. 자세한 내용은 www.cve.mitre.org 를 참조하십시오.
솔루션	솔루션 정보를 표시합니다.
자문 링크	취약점에 대한 자문 정보를 볼 수 있는 외부 참조의 URL을 표시합니다.
공급업체 솔루션 링크	취약점을 해결할 수 있는 솔루션에 대한 자세한 정보를 볼 수 있는 외부 참조 URL을 표시합니다.

정책 준수 테스트

하나 이상의 구성 정책에 대해 장치 구성의 준수 여부를 테스트하거나 하나 이상의 구성에 대해 구성 정책을 테스트할 수 있습니다. 이 방법으로 장치의 구성 준수를 테스트하거나 배포 전의 구성 정책을 테스트할 수 있습니다.

정책 아래의 메뉴 모음에서 정책 준수 테스트를 클릭합니다. 정책 준수 테스트 페이지가 열립니다.

정책 준수 테스트 페이지 필드

필드	설명/작업
정책 목록 링크	정책 페이지를 엽니다. 이 페이지에서 정책 목록을 볼 수 있습니다. 자세한 내용은 512페이지의 "정책 페이지 필드" 를 참조하십시오.
테스트할 정책 선택	다음 옵션 중 하나를 선택할 수 있습니다. <ul style="list-style-type: none"> • 모든 정책 — 이 옵션을 선택하면(기본값) 모든 구성 정책이 테스트됩니다. • 선택한 장치 그룹에 적용할 수 있는 정책 — 테스트를 실행할 장치 그룹을 선택합니다. 여러 장치 그룹을 선택하려면 Shift 키를 누른 채로 장치 그룹을 선택합니다. • 선택한 정책 — 특정 정책을 선택합니다. 여러 정책을 선택하려면 Shift 키를 누른 채로 정책을 선택합니다.
기존 장치에 대해 정책 테스트	정책을 테스트할 장치를 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기" 를 참조하십시오.
구성에 대해 정책 테스트	이 옵션을 선택한 경우에는 상자에 구성 텍스트를 입력하거나 붙여넣고 드롭다운 메뉴에서 입력한 구성 텍스트에 맞는 장치 제품군을 선택합니다.

설정이 완료되면 테스트 수행을 클릭합니다. 구성 정책 확인을 통과하면 "[장치 이름] 장치가 선택된 정책 중 적용 가능한 정책을 준수합니다." 메시지가 새 창에 표시됩니다. 구성 정책 확인에 실패하면 각 위반 목록이 새 창에 표시되며 자세한 정보를 볼 수 있는 링크가 표시됩니다.

정책 테스트 페이지 필드

먼저 정책을 생성하고 나면 정책 테스트를 통해 장치의 문제를 정확하게 발견할 수 있는지 확인하는 것이 좋습니다. 하지만 NA에서 비준수 이벤트가 생성되어 장애 관리 시스템에서 주의를 트리거되거나 네트워크 준수 측정 항목이 영향을 받는 일은 피하는 것이 좋습니다. 이런 경우에 정책 테스트 기능이 이상적입니다. 정책 테스트 조건을 사용하면 이벤트가 생성되지 않습니다. 따라서 비준수 이벤트를 생성하지 않고도 정책을 테스트할 수 있습니다.

장치를 선택한 후에 테스트 수행 버튼을 클릭합니다.

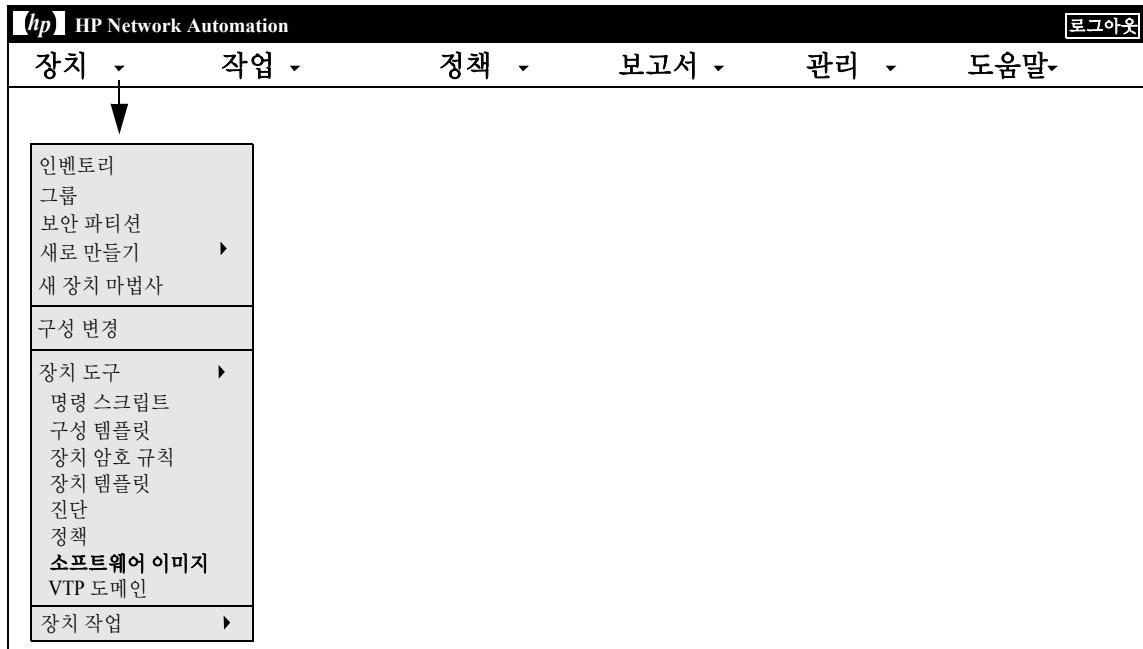
필드	설명/작업
테스트할 정책 선택	드롭다운 메뉴에서 정책을 선택합니다.
다음에 대하여 테스트할 장치 선택	정책을 테스트할 기준 장치를 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기" 를 참조하십시오.

9장: 소프트웨어 배포

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	548페이지의 "시작하기"
소프트웨어 이미지	551페이지의 "소프트웨어 이미지"
이미지 집합 추가	553페이지의 "이미지 집합 추가"
소프트웨어 배포	556페이지의 "소프트웨어 배포"
새 준수 추가	557페이지의 "새 소프트웨어 수준 추가"
장치 소프트웨어 버전 보기	560페이지의 "장치 소프트웨어 버전 보기"

소프트웨어 이미지 탐색



시작하기

HP Network Automation(NA)에서는 운영 체제(OS) 이미지를 포함한 장치 소프트웨어의 중앙 리포지토리를 제공합니다. 동일한 소프트웨어를 공유하는 하나 이상의 장치에 이를 배포할 수 있습니다. 중앙 저장 위치가 있으면 확인된 마지막 정상 소프트웨어를 사내에서 이용할 수 있습니다.

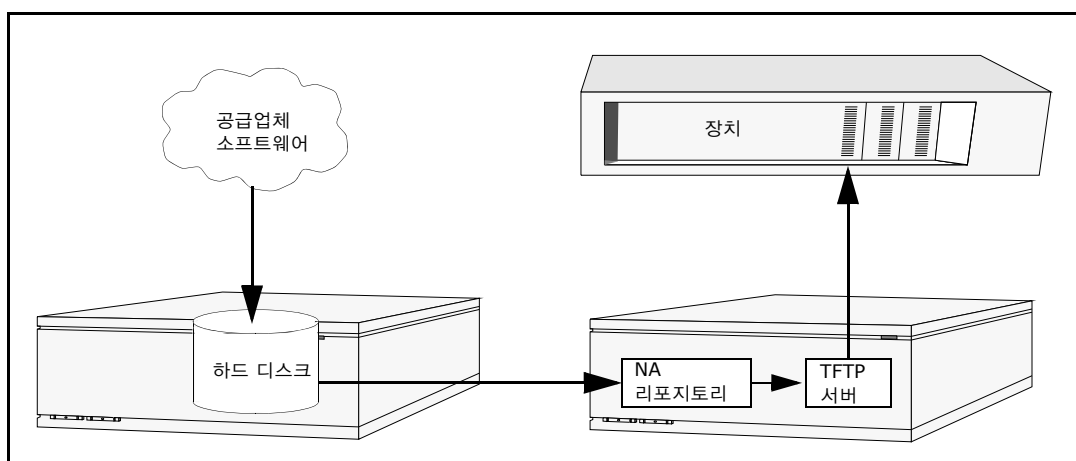
다음 작업을 수행할 수 있습니다.

- 소프트웨어 이미지 집합을 시스템에 업로드합니다. 이미지 집합은 장치에 즉시 배포할 수 있는 이미지의 그룹입니다. 이미지 집합에는 하나 이상의 이미지가 포함될 수 있습니다. 소프트웨어 업로드를 시작할 때 업로드할 이미지 집합을 선택합니다. 이미지 집합의 각 이미지가 차례로 업로드됩니다. 장치에 메모리 부족과 같은 문제가 있는 경우 업로드의 나머지 부분이 중단됩니다.
- 장치에 파일을 추가하거나 업로드합니다.
- 이미지 집합의 최소 요구 사항, 즉 성공적인 이미지 실행에 필요한 장치 제품군, 장치 모델, 최소 RAM, 프로세서 또는 부팅 ROM 버전 등을 정의합니다.
- 이미지를 배포하기 전에 파일을 삭제하여 플래시 메모리 공간을 확보하거나 플래시 메모리를 압축하는 방법으로 장치를 준비합니다.
- 이미지를 배포한 후 장치를 다시 부팅합니다.
- NA를 통한 업데이트를 예약합니다. 예를 들어, 주간 교대 시간 중에 하나의 장치에 새 이미지를 성공적으로 배포한 후 교대 시간이 아닌 한산한 시간에 더 많은 장치에 대해 업데이트하도록 예약할 수 있습니다.
- 리소스가 허용하는 범위에서 소프트웨어 버전 및 업그레이드 장치를 식별하도록 여러 준수 등급을 정의합니다.
- 여러 개의 부팅 이미지가 있는 장치에서 어떤 이미지가 부팅 이미지가 될 것인지 지정합니다. 현재 장치에 있는 부팅 이미지(및 필요하다면 OS 이미지)를 선택하거나 새 부팅 및/또는 OS 이미지를 전송할 수 있습니다. 단일 부팅 및/또는 OS 이미지를 선택한 경우, 해당 이미지를 부팅 및/또는 OS에 사용할 이미지로 설정하기 위해 장치에서 명령이 실행됩니다. 장치에 따라, 다음에 장치가 다시 부팅될 때까지 이 사항이 적용되지 않습니다. 이는 장치 소프트웨어 업데이트 작업의 일부로 선택 가능합니다. 자세한 내용은 [413페이지의 "장치 소프트웨어 업데이트 작업 페이지 필드"](#)를 참조하십시오.

또 다른 기능인 이미지 동기화 보고서를 사용하면 NA 소프트웨어 이미지 리포지토리에 상주하지 않는 장치 또는 장치 그룹에서 현재 실행 중인 소프트웨어 이미지 또는 백업 소프트웨어 이미지를 볼 수 있습니다. 자세한 내용은 [776페이지의 "이미지 동기화 보고서 필드"](#)를 참조하십시오.

참고: 부팅 이미지는 시스템 저장 미디어의 모든 내용과 구조를 포함합니다. 부팅 이미지를 사용하면 연관된 하드웨어를 부팅할 수 있습니다. OS 이미지는 장치가 켜진 후 그 인터페이스에 관한 정보를 수집한 후 장치를 실행하는 명령을 포함합니다. OS 이미지는 라우팅 프로토콜과 같은 항목을 포함합니다.

아래의 그림은 다운로드 프로세스를 보여 줍니다.



소프트웨어 업데이트 기능을 사용할 경우에는 몇 가지 모범 사례를 따라야 합니다. HP에서는 소프트웨어 이미지를 배포할 때 다음 사항에 따를 것을 권장합니다.

- 표준 변경 제어 및 승인 프로세스를 준수합니다. 장치의 상태를 수정할 때마다 몇 가지 위험이 따릅니다. 네트워크에 미칠 영향을 최소화하기 위해 조직에서 정의된 모든 변경 프로세스(예: 승인, 알림, 변경 윈도우 등)를 준수하십시오.
- 특정 장치와 OS 버전을 업데이트하는 데 적합한 단계를 조사하고 파악합니다. 여러 개의 이미지를 업그레이드해야 하는 장치도 있습니다. 뿐만 아니라 펌웨어 또는 하드웨어 의존성이 존재할 수도 있습니다.

- 어떤 OS 버전을 프로덕션 네트워크에 배포하기 전에 그 기능을 테스트합니다. OS 버전을 업그레이드하거나 특히 다운그레이드할 때 변경 전후에 장치 구성이 바뀌거나 업데이트가 필요할 수 있습니다. 프로덕션 환경에서 지정된 버전을 배포하기 전에 테스트-연구소 환경에서 철저한 테스트를 실시하여 구성이 성공적으로 업그레이드되는지 그리고 장치가 예상대로 작동하는지 확인하십시오.
- 현재 장치 이미지를 백업합니다. 업그레이드에 앞서 NA 리포지토리를 사용하여 해당 장치의 기존 이미지를 저장합니다. 그러면 새 이미지에서 예상치 못한 결과가 나타날 경우 신속하게 복구할 수 있습니다. 이미지 동기화 보고서를 이용하면 NA 소프트웨어 이미지 리포지토리에 상주하지는 않지만 어떤 장치나 장치 그룹에서 현재 실행 중인 소프트웨어 이미지 또는 백업 소프트웨어 이미지를 볼 수 있습니다. 자세한 내용은 [776페이지의 "이미지 동기화 보고서 필드"](#)를 참조하십시오.
- 장치를 업그레이드할 때 콘솔 서버를 통해 장치에 대한 대역 외(out-of-band) 관리 액세스 권한을 갖는 것이 좋습니다.
- 이미지 요구 사항을 제공하고 이를 신중하게 검증합니다. NA는 각 소프트웨어 이미지의 요구 사항을 지정할 수 있게 합니다.
- 업무상 중요한 장치에 이미지를 배포할 경우 자동 재부팅 기능을 사용하면 안 됩니다. 그 대신 소프트웨어 업데이트 기능을 사용하여 장치를 준비하고 이미지를 로드한 다음 각 장치를 수동으로 검사하면서 문제 없는 상태인지 확인한 다음 재부팅하십시오.
- 단일 장치를 먼저 업데이트한 다음 장치 그룹을 업데이트합니다.

소프트웨어 이미지

장치의 소프트웨어를 업그레이드하기 전에 다음을 비롯하여 장치별로 현재 설치된 소프트웨어를 파악해야 합니다.

- 이미지 집합
- 파일 이름
- 필요한 드라이버

장치 아래의 메뉴 모음에서 장치 도구를 선택하고 소프트웨어 이미지를 클릭합니다. 소프트웨어 이미지 페이지가 열립니다.

소프트웨어 이미지 페이지 필드

필드	설명/작업
Cisco.com 링크의 이미지 집합 추가	Cisco.com 작업에서 이미지 다운로드 페이지를 엽니다. 자세한 내용은 456페이지의 "Cisco.com에서 이미지 다운로드 작업 페이지" 를 참조하십시오.
이미지 집합 추가 링크	소프트웨어 이미지 집합 추가 페이지를 엽니다. 여기서 이미지 집합을 추가할 수 있습니다. 자세한 내용은 553페이지의 "이미지 집합 추가" 를 참조하십시오.
소프트웨어 수준 링크	소프트웨어 수준 페이지를 엽니다. 여기서 새 소프트웨어 수준을 추가하거나 장치 소프트웨어 보고서를 볼 수 있습니다. 새 수준 추가에 대한 자세한 내용은 537페이지의 "새 소프트웨어 수준 추가" 를 참조하십시오. 장치 소프트웨어 보고서에 대한 자세한 내용은 770페이지의 "장치 소프트웨어 보고서" 를 참조하십시오.
이미지 집합	이미지 집합의 이름을 표시합니다.
드라이버 필요	이 플랫폼에 필요한 NA 드라이버의 이름을 표시합니다.
모델 필요	필요한 모델의 이름을 표시합니다. 이 필드는 사용 가능한 모든 모델을 지원하기 위해 255자에서 4,000자로 확장되었습니다.
하드웨어 필요	하드웨어 요구 사항이 있으면 표시합니다.

필드	설명/작업
파티션	보안 또는 비즈니스상의 이유로 파티션을 생성한 경우, 파티션에 따라 소프트웨어 이미지를 분할할 수 있습니다. 소프트웨어 이미지가 모든 파티션에 사용 가능한 경우, 구성에 따라 소프트웨어 이미지가 "공유"(또는 "전역")로 표시됩니다. 적절한 권한이 없으면 소프트웨어 이미지를 편집하거나 삭제할 수 없습니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
작업	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 편집 — 소프트웨어 이미지 편집 페이지를 엽니다. 여기서 기존 소프트웨어 정보를 편집할 수 있습니다. 자세한 내용은 555페이지의 "소프트웨어 이미지 편집 페이지 필드"를 참조하십시오. • 소프트웨어 이미지 — 집합에 있는 이미지 관리 페이지를 엽니다. 여기서 이미지 집합을 편집하고 이미지를 추가하며 소프트웨어를 배포할 수 있습니다. 553페이지의 "소프트웨어 이미지 집합 추가 페이지 필드", 555페이지의 "소프트웨어 이미지 편집 페이지 필드" 또는 556페이지의 "소프트웨어 배포"를 참조하십시오. • 삭제 — 이미지를 삭제할 수 있습니다. • 장치 업데이트 — 장치 소프트웨어 업데이트 작업 페이지를 엽니다. 자세한 내용은 556페이지의 "소프트웨어 배포"를 참조하십시오.

이미지 집합 추가

이미지 집합을 추가하려면

1. 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 소프트웨어 이미지를 클릭합니다. 소프트웨어 이미지 페이지가 열립니다.
2. 이미지 집합 추가 링크를 클릭합니다. 소프트웨어 이미지 집합 추가 페이지가 열립니다. 완료되면 소프트웨어 저장 버튼을 클릭해야 합니다.

참고: 파일 크기는 256MB를 초과할 수 없습니다.

소프트웨어 이미지 집합 추가 페이지 필드

필드	설명/작업
이미지 집합 이름	이미지 집합 이름을 입력합니다. 특정 이미지 집합에 있는 모든 이미지가 장치의 동일한 파일 시스템 위치에 적용됩니다.
파티션	드롭다운 메뉴에서 파티션을 선택합니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다.) 일반적으로 파티션이란 고유한 IP 주소를 갖는 장치의 그룹입니다. 단일 NA 코어로 여러 파티션을 관리할 수 있습니다. 설치된 NA 서버의 NA 코어는 단일 관리 엔진, 연관된 서비스 및 단일 데이터베이스로 구성되어 있습니다.
이미지 1... 5	최대 5개의 새 이미지 또는 구성 파일을 이미지 집합에 입력할 수 있습니다.
공급업체 MD5 체크섬	공급업체의 MD5 체크섬을 입력합니다. 체크섬은 MD5 알고리즘을 사용하여 계산된 128비트 체크섬입니다. MD5는 암호 작성 보안 알고리즘입니다. 누군가가 고의적으로 파일을 변경한 다음 그 파일에 대해 동일한 체크섬을 계속 갖는 것은 쉽지 않습니다. 공급업체가 해당 장치에 대해 이 체크섬을 소프트웨어 이미지와 함께 제공하는 경우가 종종 있습니다. 이미지에 대해 체크섬을 계산하는 경우(또는 NA에서 대신 계산해 주는 경우) 공급업체가 제공한 것과 일치해야 합니다. 일치하지 않는다면 배포해서는 안 되는 손상된 이미지 파일을 갖고 있거나 공급업체가 다른 알고리즘을 사용하여 체크섬을 계산했을 가능성이 있습니다.
여러 이미지가 있는 ZIP	압축 해제할 ZIP 압축 파일을 지정합니다. ZIP의 모든 파일을 이미지 집합에 추가합니다.

필드	설명/작업
<p>이미지 집합 요구 사항</p>	<p>이미지 집합 요구 사항은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 드라이버 — 소프트웨어와 함께 저장할 드라이버 정보. 알려진 모든 드라이버가 목록에 포함됩니다. 예를 들어, Cisco Aironet 1100 Access Point에 소프트웨어를 업로드하려는 경우 "Cisco Aironet access points, 350, 1100, and 1200 series, IOS version 12.2" 드라이버를 선택합니다. • 모델 — 소프트웨어와 함께 저장할 모델 정보. 알려진 모든 모델이 목록에 포함됩니다. 예를 들어, Cisco Aironet 1200 series Access Point가 있다면 "AIR-AP1220-IOS-UPGRD (C1200 Series)"를 선택합니다. • 시스템 메모리(바이트) >= — 이미지 집합이 성공적으로 작동하는 데 필요한 최소 RAM입니다. 대부분의 장치에서 이미지는 시스템 메모리 또는 DRAM이라고도 하는 프로세서 메모리에 상주합니다. 물리적으로 존재하는 프로세서 메모리의 양은 장치별로 파일 시스템 진단을 사용하여 계산됩니다. 예를 들어, 16,384바이트는 16k에 해당합니다. 일부 장치는 파일 시스템 진단을 지원하지 않습니다. 그러한 장치에서는 RAM 요구 사항이 무시됩니다. • 프로세서 — 장치의 CPU. 예를 들어, Cisco Aironet 1200 series Access Point가 있다면 "AIR-AP1220-IOS-UPGRD (PowerPC405GP)"를 선택합니다. • 부팅 ROM — 장치의 ROM
<p>설명</p>	<p>이 소프트웨어 다운로드를 다른 것과 구별하기 위한 간단한 설명을 입력합니다.</p>

소프트웨어 이미지 편집 페이지 필드

소프트웨어 이미지를 편집하려면

1. 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 소프트웨어 이미지를 클릭합니다. 소프트웨어 이미지 페이지가 열립니다.
2. 편집하려는 이미지 집합에 대해 작업 열에서 편집 옵션을 클릭합니다. 소프트웨어 이미지 집합 편집 페이지가 열립니다.

필드	설명/작업
이미지 집합 이름	이 이미지 집합의 이름을 표시합니다. 기존의 이미지 집합을 지정할 수도 있습니다. 이 경우 NA는 새 이미지를 기존의 이미지 집합에 추가합니다. 특정 이미지 집합에 있는 모든 이미지가 장치의 동일한 파일 시스템 위치에 적용됩니다.
파티션	드롭다운 메뉴에서 파티션을 선택합니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다.)
이미지 집합 요구 사항	<ul style="list-style-type: none"> • 드라이버 — 소프트웨어와 함께 저장할 드라이버 정보. 알려진 모든 드라이버가 목록에 포함됩니다. 예를 들어, Cisco Aironet 1100 Access Point에 소프트웨어를 업로드하려는 경우 "Cisco Aironet access points, 350, 1100, and 1200 series, IOS version 12.2" 드라이버를 선택합니다. • 모델 — 소프트웨어와 함께 저장할 모델 정보. 알려진 모든 모델이 목록에 포함됩니다. 예를 들어, Cisco Aironet 1200 series Access Point가 있다면 "AIR-AP1220-IOS-UPGRD (C1200 Series)"를 선택합니다. • 장치 RAM 필요 >= — 장치의 최소 RAM • 프로세서 — 장치의 CPU. 예를 들어, Cisco Aironet 1200 series Access Point가 있다면 "AIR-AP1220-IOS-UPGRD (PowerPC405GP)"를 선택합니다. • 부팅 ROM — 장치의 ROM • 설명 — 이 소프트웨어 다운로드를 다른 것과 구별하기 위한 간단한 설명

완료되면 소프트웨어 저장을 클릭해야 합니다.

소프트웨어 배포

소프트웨어 업데이트 옵션을 사용하면 장치에 설치된 현재 소프트웨어 이미지를 자동으로 업그레이드할 수 있습니다. 그러면 네트워크 전체 소프트웨어 업그레이드를 수동으로 돌아오는 데 걸리는 시간이 크게 줄어들며, 모든 정책과 절차를 따르고 있는지 확인하기 위한 소프트웨어 업그레이드 감사 추적이 제공됩니다.

장치의 현재 소프트웨어 이미지를 자동으로 업그레이드하려면

1. 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 소프트웨어 이미지를 클릭합니다. 소프트웨어 이미지 페이지가 열립니다.
2. 배포하려는 이미지 집합에 대해 작업 열에서 소프트웨어 업데이트 옵션을 클릭합니다. 장치 소프트웨어 업데이트 작업이 열립니다. 자세한 내용은 [413페이지의 "장치 소프트웨어 업데이트 작업 페이지 필드"](#)를 참조하십시오.

다음 사항을 기억하십시오.

- 전체 메모리는 장치에 있는 전체 물리적 메모리입니다.
- 여유 메모리는 마지막 메모리 진단 시 업로드에 사용할 수 있는 여유 메모리입니다.
- 순 메모리는 장치 소프트웨어 업데이트 작업이 실행된 후의 예상 여유 메모리입니다. 이때 장치에서 추가되거나 제거되도록 표시한 파일이 고려되지만 압축 전 또는 후 처리 작업은 고려되지 않습니다.

새 소프트웨어 수준 추가

해당 장치에서 최신 승인 소프트웨어를 실행하고 있어야 합니다. 네트워크 관리자는 이미지를 사전 프로덕션이나 사용되지 않음과 같은 범주로 그룹화할 수 있습니다. 또한 최근에 발견된 취약점 기준 보안 위험과 같이 이미지를 분류할 수도 있습니다.

새 소프트웨어 수준을 추가하거나 기존 정의를 검토하려면

1. 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 소프트웨어 이미지를 클릭합니다. 소프트웨어 이미지 페이지가 열립니다.
2. 페이지 맨 위의 소프트웨어 수준 옵션을 클릭합니다. 소프트웨어 수준 페이지가 열립니다.
3. 수준 추가 옵션을 클릭합니다. 소프트웨어 수준 추가 페이지가 열립니다. 완료되면 저장을 클릭해야 합니다.

소프트웨어 수준 추가 페이지 필드

필드	설명/작업
소프트웨어 수준 추가	
수준 이름	수준 이름을 입력합니다.
상태	다음 옵션 중 하나를 표시합니다. <ul style="list-style-type: none"> •활성 — 구성 정책을 활성화로 표시합니다(기본값). •비활성 — 구성 정책을 비활성화합니다. 비활성 정책은 비준수 이벤트를 생성하지 않습니다.

필드	설명/작업
수준	<p>준수 등급 이름을 선택합니다. 요구 사항 및 검증 절차에 따라 주어진 준수 정의 중 어느 것이라도 사용할 수 있습니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 보안 위험 • 사전 프로덕션 • 사용되지 않음 • 브론즈 • 실버 • 골드 • 플래티늄
설명	준수에 대한 설명을 입력합니다.
파티션	드롭다운 메뉴에서 파티션을 선택합니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다.)
일치 기준 (일치 기준에 와일드카드 연산자(* 및 ?) 사용 가능)	
소프트웨어 버전	현재 장치에서 실행 중인 소프트웨어 버전을 입력합니다.
장치 드라이버	장치에 액세스하는 데 사용되는 장치 드라이버를 드롭다운 메뉴에서 선택합니다. (모두가 기본값입니다.)
장치 모델	장치 모델을 입력합니다.
파일 이름	OS 파일 이름과 일치하는 문자열을 입력합니다.
구성에 포함	해당 장치에 준수가 적용되는지 확인하기 위해 현재 장치 구성과 일치하는 패턴을 입력합니다.
소프트웨어 취약점 정보(보안 위험 준수 수준별)	
공개 날짜	소프트웨어 취약점에 yyyy-MM-dd 형식의 플래그가 지정된 날짜를 입력합니다.

필드	설명/작업
중요도	다음과 같은 보안 취약점의 심각도를 드롭다운 메뉴에서 선택합니다. <ul style="list-style-type: none">•심각•높음•중간•낮음•정보용
CVE 이름	CVE(Common Vulnerabilities and Exposures) 이름을 입력합니다. CVE는 취약점의 표준화된 이름과 보안 노출에 관한 기타 정보의 목록입니다. 자세한 내용은 www.cve.mitre.org 를 참조하십시오.
솔루션	자세한 솔루션 정보를 입력합니다.
자문 링크	취약점에 관한 자문 정보를 얻을 수 있는 외부 참조 URL을 입력합니다.
솔루션 링크	취약점의 가능한 솔루션에 대한 자세한 정보를 얻을 수 있는 외부 참조 URL을 입력합니다.

장치 소프트웨어 버전 보기

장치 소프트웨어 보고서에서는 현재 각 장치에 지정된 소프트웨어 버전 및 준수 등급을 볼 수 있습니다.

1. 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 소프트웨어 이미지를 클릭합니다. 소프트웨어 이미지 페이지가 열립니다.
2. 페이지 맨 위의 소프트웨어 수준 옵션을 클릭합니다. 소프트웨어 수준 페이지가 열립니다.
3. 페이지 맨 위의 장치 소프트웨어 보고서 옵션을 클릭합니다. 장치 소프트웨어 보고서가 열립니다. 자세한 내용은 [770페이지의 "장치 소프트웨어 보고서 필드"](#)를 참조하십시오.

참고: 보고서 드롭다운 메뉴에서 장치 소프트웨어 보고서로 이동할 수도 있습니다.

10장: 이벤트 알림 규칙

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	563페이지의 "시작하기"
이벤트 규칙 추가	569페이지의 "이벤트 규칙 추가"
이벤트 규칙 검색 결과	570페이지의 "이벤트 알림 및 응답 규칙 페이지 필드"
새 이벤트 알림 규칙	571페이지의 "새 이벤트 알림 및 응답 규칙 페이지 필드"
이벤트 규칙 변수	577페이지의 "이벤트 규칙 변수"

이벤트 알림 규칙 탐색

hp HP Network Automation 로그아웃

장치 ▾ 작업 ▾ 정책 ▾ 보고서 ▾ **관리 ▾** 도움말 ▾

사용자
 사용자 그룹
 새 사용자
 새 사용자 그룹
 로그인한 사용자

사용자 역할 및 권한

보안 파티션
 게이트웨이
 장치 암호 규칙
이벤트 알림 및 응답 규칙

사용자 지정 데이터 설정
 Active Directory 설정
 워크플로 설정

관리 설정 ▶

작업 로드
 시스템 상태
 서비스 시작 / 중지
 문제 해결

시스템 작업 ▶

시작하기

HP NA(Network Automation)를 사용하면 시스템에서 다음과 같은 이벤트가 발생할 때 서로 다른 많은 작업을 트리거할 수 있습니다.

- 스냅샷 또는 진단과 같은 작업 실행
- 전자 메일 알림 보내기
- 전자 메일 다이제스트
- SNMP 트랩 보내기
- Syslog 메시지 보내기

이벤트 규칙은 특정 장치 그룹 및/또는 일일 횟수로 제한될 수 있습니다. 다음 표는 선택할 수 있는 사용 가능한 이벤트에 대해 설명합니다.

이벤트	설명
승인 거부됨	사용자가 승인 요청을 거부했습니다.
승인 허가됨	사용자가 작업을 승인했습니다.
더 이상 승인이 필요하지 않음	작업 승인이 더 이상 필요하지 않습니다.
승인 오버라이드	승인 없이 작업을 실행할 수 있도록 사용자가 작업의 승인을 오버라이드했습니다.
승인 요청	사용자가 실행 전에 승인이 필요한 작업을 작성했습니다.
승인 작업 변경됨	사용자가 실행 전에 승인이 필요한 작업을 변경했습니다.
승인 작업 삭제됨	사용자가 승인을 위해 표시된 작업을 삭제했습니다.
승인 작업 시간 초과	할당된 시간에 작업이 승인되지 않았습니다.
명령 인증 오류	사용이 인증되지 않은 사용자가 명령을 실행하려고 시도했습니다.
동시 텔넷/SSH 세션 오버라이드	사용자가 동시 로그인에 대한 제한을 무시했습니다. 이 사용자는 다른 사용자가 이미 로그인했음에도 불구하고 프록시를 통해 장치에 로그인했습니다.
정책 추가됨	사용자가 새 구성 정책을 추가했습니다.

이벤트	설명
정책 변경됨	사용자가 구성 정책을 변경했습니다.
정책 비준수	구성 변경이 정책 규칙을 위반했습니다.
정책 패턴 시간 초과	정책 패턴 일치에 30초 이상이 걸렸습니다.
정책 규칙 추가됨	사용자가 새 구성 규칙을 추가했습니다.
정책 규칙 변경됨	사용자가 구성 규칙을 변경했습니다.
장치 액세스 실패	NA가 장치에 액세스할 수 없습니다. 암호가 잘못되었거나 호스트에 대한 경로가 없기 때문일 수 있습니다.
장치 추가됨	사용자가 장치를 추가했습니다.
장치 부팅됨	장치가 재부팅되었습니다.
장치 명령 스크립트 완료됨	장치 명령 스크립트 실행에 성공했습니다.
장치 명령 스크립트 실패	장치 명령 스크립트 실행에 실패했습니다.
장치 구성 변경	스냅샷 작업이 실행되는 동안 NA가 구성 변경을 감지했습니다.
장치 구성 변경 - 사용자 없음	NA가 알 수 없는 사용자에게 의한 구성 변경을 감지했습니다.
장치 구성 배포	NA가 장치에 구성을 성공적으로 배포했습니다.
장치 구성 배포 실패	NA가 장치에 구성을 배포하는 데 실패했습니다.
장치 데이터 실패	NA가 구성 또는 진단 출력을 데이터베이스에 저장하는 데 실패했습니다.
장치 삭제됨	사용자가 장치를 영구적으로 제거했습니다.
장치 진단 변경됨	진단 결과가 이전 결과와 다릅니다.
장치 진단 완료됨	장치 진단에 성공했습니다.
장치 진단 실패	장치 진단에 실패했습니다.

이벤트	설명
장치 편집됨	사용자가 장치의 정보를 수정했습니다.
실행 중인 장치 플래시 저장 공간이 적음	장치의 플래시 저장 공간이 얼마 남지 않았습니다.
장치 액세스 불가능	장치에 액세스할 수 없습니다.
장치 관리됨	사용자가 장치를 "활성"으로 표시했습니다.
가져오기에서 누락된 장치	가져오기 작업이 주기적으로 실행되고 가져오기 작업에 가져올 장치 파일이 제공되었을 때, 마지막으로 가져오기가 발생한 시기에는 파일에 장치가 포함되었지만 현재 가져오기 중에는 포함되지 않은 경우 이 이벤트가 발생합니다.
장치 암호 변경	사용자가 암호 변경을 배포했습니다.
장치 암호 변경 실패	NA가 장치 암호 변경에 실패했습니다.
장치 권한 - 수정됨	장치가 그룹에 추가되거나 그룹에서 제거되어, 사용자의 장치 수정 권한 등의 권한이 변경되었습니다.
장치 권한 - 새 장치	장치 그룹에 새 장치가 추가되어, 해당 장치 그룹과 연관된 사용자 권한이 변경되었습니다.
장치 다시 로드 실패	장치 다시 로드 실패했습니다.
장치 예약 충돌	장치 예약 충돌이 있었습니다.
장치 스냅샷	NA가 구성 변경을 위해 장치를 확인했습니다.
장치 소프트웨어 변경	NA가 장치에서 새 OS 버전을 감지했습니다(예: IOS 11에서 IOS 12로).
장치 시작/실행 구성 차이	NA가 시작 구성과 실행 구성 간의 차이점을 감지했습니다.
장치 관리되지 않음	사용자가 장치를 "비활성"으로 표시했습니다. 특정 기간 동안 접근할 수 없는 경우 가져온 장치도 "비활성"이 될 수 있습니다.
전자 메일 보고서 저장됨	사용자가 전자 메일 보고서를 저장했습니다.
분산 시스템 - 손상된 복제 작업	NA가 손상된 복제 작업을 감지했습니다.

이벤트	설명
분산 시스템 - 데이터 동기화 지연 경고	NA가 데이터 동기화 지연 경고를 감지했습니다.
분산 시스템 - 지연된 LOB 임계값 초과	NA가 지연된 LOB의 초과를 감지했습니다.
분산 시스템 - 장치 소프트웨어 전송 오류	NA가 장치 소프트웨어 전송 오류를 감지했습니다.
분산 시스템 - 수정된 복제 작업	NA가 수정된 복제 작업을 감지했습니다.
분산 시스템 - RMI 오류	NA가 RMI 오류를 감지했습니다.
분산 시스템 - 복제 오류	NA가 복제 오류를 감지했습니다.
분산 시스템 - 중지된 병합 에이전트 작업	NA가 중지된 병합 에이전트 작업을 감지했습니다.
분산 시스템 - 시간 동기화 경고	NA가 시간 동기화 경고를 감지했습니다.
분산 시스템 - 삭제할 수 없는 예외 생성	NA가 삭제할 수 없는 예외 생성을 감지했습니다.
분산 시스템 - 고유성 충돌	NA가 고유성 충돌을 감지했습니다.
외부 디렉터리 서버 인증 오류	NA가 외부 LDAP 인증 서버에 연결할 수 없습니다.
그룹 추가됨	사용자가 그룹을 추가했습니다.
그룹 삭제됨	사용자가 그룹을 삭제했습니다.
그룹 수정됨	사용자가 장치 그룹을 수정했습니다.
마지막으로 사용한 장치 암호 변경됨	장치 액세스를 위해 마지막으로 사용된 암호가 변경되었습니다.
라이센스가 거의 초과됨	장치가 총 라이선스 노드 수의 90%를 초과합니다.
라이센스가 거의 만료됨	NA 라이선스가 곧 만료됩니다(날짜 기반 라이선스 전용).

이벤트	설명
라이센스가 초과됨	장치가 총 라이선스 노드 수를 초과합니다. NA는 20%의 초과를 허용합니다.
라이센스가 만료됨	라이센스가 만료되었습니다. NA가 더 이상 로그인을 허용하지 않지만 예정된 스냅샷 및 레코드 변경은 계속 진행됩니다.
모듈 추가됨	장치에 모듈/블레이드/카드가 추가되었습니다.
모듈 변경됨	장치에 설치된 모듈/블레이드/카드의 속성이 변경되었습니다.
모듈 제거됨	장치에서 모듈/블레이드/카드가 제거되었습니다.
모니터 오류	서버 모니터가 실행에 실패했습니다.
모니터 정상	서버 모니터가 성공적으로 실행되었습니다.
보류 중 작업 삭제됨	사용자가 예정된 작업을 실행 전에 삭제했습니다.
예약된 장치 구성이 변경됨	사용자가 예약된 장치에서 장치 구성을 변경했습니다.
구성 배포를 위한 예정 편집됨	배포하기로 예정된 구성을 사용자가 수정했습니다.
구성 배포를 위한 예정 수정됨	새 암호가 배포되었는데, 또 다른 암호 배포 작업이 예정되었습니다. 이는 방금 배포된 새 암호가 다시 변경될 것임을 나타냅니다(보류 중인 암호 배포 작업이 실행될 때).
보안 주의	NA가 보안 주의를 감지했습니다.
서버 시작	NA 관리 엔진이 시작되었습니다.
세션 데이터 캡처됨	프록시가 데이터베이스에 연결 세션을 저장했습니다.
소프트웨어 업데이트 실패함	NA가 장치에서 OS 소프트웨어 업데이트에 실패했습니다.
소프트웨어 업데이트 성공함	NA가 장치에서 OS 소프트웨어를 성공적으로 업데이트했습니다.

이벤트	설명
소프트웨어 취약점이 감지됨	소프트웨어 수준을 "보안 위험"으로 설정한 경우 NA가 장치를 스냅샷하고 "보안 위험"으로 태그가 지정된 OS 버전을 감지하면 이 이벤트가 생성됩니다.
요약 보고서 생성됨	사용자가 요약 보고서를 생성했습니다.
작업 완료됨	작업이 완료되었습니다.
작업 시작됨	작업이 시작되었습니다.
티켓 생성됨	HP Remedy AR System Connector(또는 타사 티켓팅 시스템과 인터랙션하는 HP Connector 중 하나)를 사용할 경우 이 이벤트는 NA가 타사 티켓팅 시스템에서 티켓을 생성했음을 나타냅니다.
사용자 추가됨	사용자가 추가되었습니다.
사용자 인증 오류	사용자가 NA에 로그인할 때 잘못된 암호를 입력했습니다.
사용자 인증 오류 잠금	연속적으로 실패한 로그인 시도가 너무 많아서 사용자가 잠겼습니다.
사용자 삭제됨	사용자가 삭제되었습니다.
사용자 사용 안 함	사용자 레코드가 편집되어 사용자의 상태가 활성화됨에서 비활성화됨으로 변경됩니다.
사용자 사용	사용자 레코드가 편집되어 사용자의 상태가 사용 안 함에서 사용함으로 변경됩니다.
사용자 로그인	사용자가 NA에 로그인했습니다.
사용자 로그아웃	사용자가 NA에서 로그아웃했습니다.
사용자 메시지	사용자가 새 메시지 링크를 클릭하여 메시지를 생성했습니다.
사용자 권한 변경됨	사용자의 권한이 변경되었습니다.

이벤트 규칙 추가

이벤트 알림 규칙을 추가하려면 관리 아래의 메뉴 모음에서 "이벤트 알림 및 응답 규칙"을 클릭합니다. 이벤트 알림 및 응답 규칙 페이지가 열립니다. 이 페이지에는 NA 이벤트에 의해 트리거되는, 현재 정의된 규칙이 나열됩니다. 파운드 기호(#)가 표시된 이벤트 규칙은 비활성 상태입니다.

참고: 관리 사용자는 모든 이벤트 규칙을 볼 수 있고, 다른 사용자는 자신의 이벤트 규칙만 볼 수 있습니다.

이벤트 알림 및 응답 규칙 페이지 필드

필드	설명/작업
새 이벤트 알림 및 응답 규칙 링크	새 이벤트 알림 및 응답 규칙 페이지를 엽니다. 자세한 내용은 571페이지 의 "새 이벤트 알림 및 응답 규칙 페이지 필드"를 참조하십시오.
규칙 이름	이벤트 규칙의 이름을 표시합니다.
파티션	보안 또는 비즈니스상의 이유로 파티션을 생성한 경우 파티션에 따라 이벤트 규칙을 파티셔닝할 수 있습니다. 모든 파티션에서 이벤트 규칙을 사용할 수 있으면 구성에 따라 이벤트 규칙에 "공유"(또는 "전역")라는 레이블이 붙습니다. 적절한 권한이 없으면 이벤트 규칙을 편집하거나 삭제할 수 없습니다. 파티션 생성에 대한 자세한 내용은 191페이지 의 "장치 및 사용자 세분화"를 참조하십시오.
작업	이벤트 규칙에 의해 수행되는 작업을 표시합니다. 작업에는 다음이 포함됩니다. <ul style="list-style-type: none"> •작업 실행 •전자 메일 보내기 •SNMP 트랩 전송 •전자 메일 다이제스트에 추가 •Syslog 메시지 전송
생성자	이벤트 규칙의 소유자를 표시합니다.
작업	다음 옵션 중에서 선택할 수 있습니다. <ul style="list-style-type: none"> •편집 — 이벤트 규칙을 편집할 수 있는 이벤트 알림 및 응답 규칙 편집 페이지를 엽니다. 자세한 내용은 571페이지의 "새 이벤트 알림 및 응답 규칙 페이지 필드"를 참조하십시오. •삭제 — 삭제 확인을 요청하는 확인 창을 엽니다. 이벤트 규칙을 삭제할 권한이 있는 경우에만 이 옵션이 나타납니다.

새 이벤트 알림 및 응답 규칙 페이지 필드

새 이벤트 알림 및 응답 규칙 페이지에서는 새 알림 및 응답 규칙을 추가/편집할 수 있습니다.

1. 관리 아래의 메뉴 모음에서 "이벤트 알림 및 응답 규칙"을 클릭합니다. 이벤트 알림 및 응답 규칙 페이지가 열립니다.
2. 페이지 맨 위에서 "새 이벤트 알림 및 응답 규칙" 링크를 클릭합니다. 새 이벤트 알림 및 응답 규칙 페이지가 열립니다.

필드	설명/작업
다음 이름의 전자 메일 및 이벤트 규칙 추가	이벤트 규칙 이름을 입력합니다.
이 작업 수행	<p>다음 옵션 중 하나를 선택합니다. (참고: 선택하는 옵션에 따라 페이지가 새로고쳐지고 작업에 대한 특정 필드가 제공됩니다.)</p> <ul style="list-style-type: none"> •작업 실행 — 573페이지의 "작업 실행 작업"을 참조하십시오. •전자 메일 다이제스트 보내기 — 573페이지의 "전자 메일 다이제스트 보내기 작업"을 참조하십시오. •전자 메일 메시지 보내기 — 574페이지의 "전자 메일 메시지 보내기 작업"을 참조하십시오. •SNMP 트랩 전송 — 575페이지의 "SNMP 트랩 전송 작업"을 참조하십시오. •전자 메일 메시지 보내기 — 576페이지의 "Syslog 메시지 전송 작업"을 참조하십시오. •티켓에 생성/추가 — 576페이지의 "티켓에 생성/추가"를 참조하십시오.

필드	설명/작업
다음 이벤트가 발생할 경우	<p>이벤트 목록에서 하나 이상의 이벤트를 선택합니다. Ctrl+클릭 또는 Shift+클릭을 사용하면 여러 이벤트를 선택할 수 있습니다. 이벤트 규칙에 대한 설명은 563페이지의 "시작하기"를 참조하십시오. 구성 정책 비준수 이벤트를 선택할 경우 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 임의의 중요도 — 이 옵션을 선택하면(기본값) 위반된 구성 정책 규칙의 중요도에 관계없이 이벤트 규칙이 트리거됩니다. 구성 정책 규칙 중요도 설정 방법에 대한 자세한 내용은 518페이지의 "새 규칙 페이지 필드"를 참조하십시오. • 최소 < > 중요도 — 심각, 높음, 중간(기본값), 낮음, 정보용 중 하나를 선택할 수 있습니다. 선택한 중요도보다 높거나 같은 중요도의 구성 정책 규칙 실패로 인해 이벤트가 생성된 경우 이벤트 규칙이 트리거됩니다. 구성 규칙 중요도 설정 방법에 대한 자세한 내용은 518페이지의 "새 규칙 페이지 필드"를 참조하십시오. • 모든 정책 대상 — 이 옵션을 선택하면(기본값) 모든 구성 정책이 확인됩니다. • 선택한 정책 대상 — 목록에서 하나 이상의 구성 정책을 선택합니다. 여러 구성 정책을 선택하려면 Shift+클릭 또는 Ctrl+클릭을 사용할 수 있습니다. <p>"장치 명령 스크립트 완료됨" 또는 "장치 명령 스크립트 실패" 이벤트를 선택하는 경우 드롭다운 메뉴에서 명령 스크립트를 선택할 수 있습니다. "장치 진단 변경됨" 또는 "장치 진단 완료됨" 이벤트를 선택하는 경우 드롭다운 메뉴에서 진단을 선택할 수 있습니다.</p>
규칙 상태	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 활성 — 이 옵션을 선택하면(기본값) 이벤트 발생 시 이벤트 규칙이 실행됩니다. • 비활성 — 이 옵션을 선택하면 이벤트 규칙이 실행되지 않습니다. 이 옵션은 이벤트 규칙을 일시적으로 비활성화하기 위해 사용할 수 있습니다.
사이	<p>이 옵션을 선택할 경우, 시간 범위를 지정하고 이벤트 규칙을 시작하고 종료할 시간을 선택합니다.</p>
이 파티션에 있는 장치에서	<p>파티션을 사용할 수 있으면 드롭다운 메뉴에서 파티션을 선택합니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화"를 참조하십시오.</p>

필드	설명/작업
----	-------

다음 그룹에 있는 장치에서	이 옵션을 선택할 경우, 목록에서 하나 이상의 그룹을 선택합니다.
----------------	--------------------------------------

선택하는 작업에 따라 새 이벤트 알림 및 응답 규칙 페이지 하단의 내용이 달라질 수 있습니다.	
--	--

작업 실행 작업

이벤트 발생 시 NA 작업이 트리거되도록 할 수 있습니다. NA가 스냅샷을 작성하거나 진단을 저장하거나 명령 스크립트를 실행하도록 할 수 있으며 심지어 외부 응용 프로그램을 실행하도록 할 수도 있습니다. 외부 응용 프로그램에 대해 명령줄에 이벤트 변수를 공급할 수도 있습니다. 이를 통해 NA를 사용자 지정하고 필요에 따라 작동을 맞춤화할 수 있습니다.

대기	작업을 실행하기 전에 대기해야 할 초, 분, 시 또는 날짜 수를 입력합니다.
----	--

작업	실행할 작업을 드롭다운 메뉴에서 선택합니다.
----	--------------------------

전자 메일 다이제스트 보내기 작업

전자 메일 다이제스트는 여러 NA 이벤트를 주기적으로 전송되는 단일 전자 메일 보고서로 결합합니다. 구성 변경, 장치 추가나 삭제, 활동 변경 등의 일반적인 시스템 이벤트를 사용자에게 알리는 데에도 전자 메일 다이제스트를 사용할 수 있습니다.

전자 메일 볼륨을 최소화하는 한편 관심 있는 이벤트에 대해 다이제스트를 신속하게 검색할 수 있습니다. 각 사용자는 하나의 전자 메일 다이제스트를 가질 수 있습니다. 사용자는 여러 이벤트 규칙을 설정할 수 있습니다. 각 규칙은 해당 다이제스트에 서로 다른 이벤트 집합을 제공합니다.

참고: 서로 다른 일정 또는 수신자 목록을 가진 여러 전자 메일 다이제스트를 원하는 경우 적절한 다이제스트 규칙 정의가 유일한 목적인 사용자들을 작성할 수 있습니다.

XX의 다이제스트 보내기(시)	NA가 전자 메일 다이제스트를 전송하도록 할 하루 중 시간을 입력합니다.
------------------	--

그리고 XX시간마다 반복	NA가 전자 메일 다이제스트를 전송하도록 할 시간 간격을 입력합니다. 예를 들어 6을 입력하면 다이제스트가 6시간마다 전송됩니다.
---------------	--

보내는 사람	수신자의 전자 메일 주소를 입력합니다. 기본값은 NA입니다.
--------	-----------------------------------

받는 사람	수신자의 전자 메일 주소를 입력합니다. 주소가 여러 개인 경우 쉼표로 구분하십시오. 참고: 변수가 \$EventUserEmail\$로 설정되어 있으면, 전자 메일 주소는 전자 메일 다이제스트를 생성한 사용자로부터 나옵니다. 따라서 사용자의 전자 메일 주소가 변경되면 새 전자 메일 주소가 사용됩니다.
-------	---

제목	메시지의 간단한 제목 라인을 입력합니다.
----	------------------------

필드	설명/작업
메시지 머리글	메시지 머리글을 입력합니다. 이것은 메시지의 머리글 또는 요약 섹션을 시작하는 텍스트입니다. HTML 메시지의 경우 이것은 종종 순서 있는 목록 태그인 <i>입니다.
종료 요약	메시지의 머리글 또는 요약 섹션을 끝내는 텍스트를 입력합니다. HTML 메시지의 경우 흔히 순서가 지정된 목록 종료 태그인 </i>입니다.
메시지 바닥글	메시지 바닥글을 입력합니다. 필요에 따라 바닥글을 맞춤화할 수 있습니다. 예를 들어 연락처 정보를 제공하거나 이 메시지가 NA 서버에서 전송되는 것임을 나타낼 수 있습니다.
텍스트 메시지 또는 HTML 메시지	텍스트 메시지 또는 HTML 메시지(기본값)를 선택합니다. HTML 메시지를 선택하면 NA는 메일을 읽는 사람이 메시지에서 HTML을 해석할 수 있도록 적절한 메일 헤더를 전송합니다. 텍스트 메시지를 선택하면 NA는 일반 텍스트 메시지를 전송하며 HTML 태그는 있는 그대로 표시됩니다.
이벤트 요약	이 필드는 이벤트를 간단하게 설명하는 요약 텍스트를 제공합니다. 특정 메시지 내용은 규칙에 대해 고유합니다. HTML 메시지에서는 이 줄이 종종 목록 항목 태그인 로 시작되며 추가 HTML 태그 및 NA 변수가 이 줄에 포함될 수 있습니다. 변수 이름 표시 링크를 클릭하면 이벤트 규칙 변수 창이 열리면서 사용할 수 있는 모든 변수가 나열됩니다.
이벤트 세부사항	이 필드는 이벤트를 자세히 설명하는 텍스트, 변수 및 선택적인 HTML 태그를 포함합니다.

전자 메일 메시지 보내기 작업

NA 이벤트가 발생할 때 사용자나 배포 목록을 대상으로 전자 메일 메시지를 보낼 수 있습니다. 각 이벤트에 대해 하나의 전자 메일 메시지가 전송됩니다. 예를 들면, 이 작업을 사용하여 핵심 장치의 구성이 변경될 때 모든 사용자에게 알리거나, 장치에 액세스할 수 없을 때 시스템 관리자에게 알리거나, 공용 폴더에 시스템 이벤트 아카이브를 보관할 수 있습니다. 호출기로 전자 메일을 보낼 간단한 메시지와 함께 텍스트 전용 이벤트 규칙을 정의할 수도 있습니다.

보내는 사람	사람이나 프로세스 및 전자 메일 메시지를 보내는 전자 메일 주소를 입력합니다. 변수 이름 표시 링크를 클릭하면 이벤트 규칙 변수 창이 열리면서 사용할 수 있는 모든 변수가 나열됩니다. 자세한 내용은 577페이지의 "이벤트 규칙 변수" 를 참조하십시오.
받는 사람	메시지를 전송할 전자 메일 주소를 입력합니다. 주소가 여러 개인 경우 쉼표로 구분하십시오. 이벤트와 관련된 사용자에게 전자 메일을 보내려면 \$EventUserEmail\$ 변수를 사용합니다.

필드	설명/작업
제목	전자 메일 메시지의 제목 라인을 입력합니다. 변수를 사용하여 제목 라인에 시스템 정보를 입력할 수 있습니다.
텍스트 메시지	이 옵션을 선택하면 NA는 일반 텍스트 메시지를 보냅니다. HTML 태그는 있는 그대로 표시됩니다.
HTML 메시지	이 옵션을 선택하면 NA는 메일을 읽는 사람이 메시지에서 HTML을 해석할 수 있도록 적절한 메일 헤더를 전송합니다.
텍스트와 HTML 모두	이 옵션(기본값)을 선택하면 텍스트 메시지와 HTML 메시지가 모두 전송됩니다. NA는 여러 부분 전자 메일 메시지를 보냅니다. 전자 메일 클라이언트는 적절한 형식의 부분을 표시합니다. 예를 들어 Outlook은 기본적으로 HTML을 표시합니다. 호출기, PDA 또는 유사 장치에서 메시지를 수신할 경우 짧은 텍스트 전용 메시지를 사용하는 것이 좋습니다.

SNMP 트랩 전송 작업

SNMP 트랩은 네트워크 상태 메시지입니다(RFCs 1155 및 1215에서 정의). 이 작업은 NA 이벤트가 발생할 때 SNMP 트랩을 보내기 위해 사용됩니다. 예를 들어, 스냅샷이 작성될 때마다 NMS(Network Management System)로 SNMP 트랩을 보낼 수 있습니다. 트랩을 정확하게 표시하려면 우선 메시지 형식을 정의하는 NA MIB(Management Information Base)를 로드해야 할 수 있습니다. (**참고:** SNMP 트래픽이 라우터, 방화벽 및 기타 네트워크 장치를 통과할 수 있도록 네트워크를 구성해야 합니다.)

SNMP 트랩 수신기 호스트 이름	호스트의 DNS 이름 또는 IP 주소를 입력합니다.
SNMP 트랩 수신기 포트	SNMP 트랩을 수신하는 호스트 포트를 입력합니다. 기본 포트 사용 링크를 클릭하면 기본 포트 번호가 입력됩니다. 162가 표준 SNMP 포트입니다.
SNMP 커뮤니티 문자열	SNMP 트랩을 보낼 때 사용할 커뮤니티 문자열을 입력합니다. 이 문자열을 허용하도록 수신자를 구성해야 합니다. 기본 커뮤니티 문자열 사용 링크를 클릭하면 기본 커뮤니티 문자열인 Public이 입력됩니다.
SNMP 버전	사용할 SNMP 버전, 즉 v1(기본값) 또는 v2를 선택합니다.
이벤트 설명	이벤트 설명을 입력합니다. NA 변수를 포함할 수 있습니다. 변수 이름 표시 링크를 클릭하면 이벤트 규칙 변수 창이 열리면서 사용할 수 있는 모든 변수가 나열됩니다. 자세한 내용은 577페이지의 "이벤트 규칙 변수" 를 참조하십시오.

필드	설명/작업
심각도	<p>이벤트 심각도를 나타내는 다음 옵션 중 하나를 선택합니다. 각 이벤트와 연관된 고유 보안 수준은 없습니다. 따라서 합당한 값을 선택하여 할당할 수 있습니다.</p> <ul style="list-style-type: none"> • 주의 • 심각 • 디버그 • 응급 • 오류 • 정보 • 알림 • 경고
Syslog 메시지 전송 작업	
<p>NA 이벤트를 외부 관리 시스템으로 전달하기 위해 syslog 메시지를 사용할 수 있습니다. 예를 들면 NA가 장치 구성 변경을 감지할 때 CA UniCenter 시스템에 알려 운영 콘솔에 경고가 나타나도록 할 수 있습니다.</p>	
Syslog 호스트 이름	Syslog 서버의 호스트 이름을 입력합니다.
Syslog 포트	Syslog에서 사용하는 포트를 입력합니다. 기본 포트 사용 링크를 클릭하면 기본 Syslog 포트 514가 입력됩니다.
Syslog 메시지	Syslog 메시지를 변수와 함께 입력합니다. 변수 이름 표시 링크를 클릭하면 이벤트 규칙 변수 창이 열리면서 사용할 수 있는 모든 변수가 나열됩니다. 자세한 내용은 577페이지의 "이벤트 규칙 변수" 를 참조하십시오.
티켓에 생성/추가	
시스템 호스트 이름 티케팅	티케팅 시스템 호스트 이름을 입력합니다.
이벤트 설명	이벤트 설명을 입력합니다.

완료되면 규칙 저장을 클릭해야 합니다.

이벤트 규칙 변수

다음에 대해 여러 이벤트 규칙 변수를 사용할 수 있습니다.

- 장치 이벤트
- 장치 구성 이벤트
- 장치 진단 이벤트
- 모든 이벤트

장치 이벤트 변수

참고: 변수는 대소문자를 구분합니다. 따라서 보이는 그대로 입력해야 합니다.

다음 변수는 장치 이벤트 규칙에만 사용할 수 있습니다.

변수	설명
\$DeviceID\$	장치에 대한 NA의 식별 번호
\$HostName\$	장치 호스트 이름
\$IPAddress\$	장치의 기본 IP 주소
\$FQDN\$	장치의 정규화된 도메인 이름
\$Vendor\$	장치 제조업체
\$Model\$	장치 모델 번호

장치 구성 이벤트에 대한 변수

참고: 변수는 대소문자를 구분합니다. 따라서 보이는 그대로 입력해야 합니다.

다음 변수는 장치 구성 이벤트 규칙에만 사용할 수 있습니다.

변수	설명
\$DataID\$	최신 구성에 대한 NA의 식별 번호
\$Comments\$	구성 주석
\$Diff\$	구성 변경의 텍스트 차이

장치 진단 이벤트에 대한 변수

참고: 변수는 대소문자를 구분합니다. 따라서 보이는 그대로 입력해야 합니다.

다음 변수는 장치 진단 이벤트 규칙에만 사용할 수 있습니다.

변수	설명
\$CurrentDiag\$	현재 진단 텍스트
\$PreviousDiag\$	이전 진단 텍스트
\$Diff\$	현재 진단과 이전 진단 간 변경의 텍스트 차이
\$DataID\$	진단 이벤트에도 사용됨

모든 이벤트에 대한 변수

다음 변수는 모든 이벤트 규칙에 사용할 수 있습니다. 변수는 대소문자를 구분합니다. 따라서 보이는 그대로 입력해야 합니다. (참고: 변수의 전체 목록을 보려면 새 이벤트 알림 및 응답 규칙 페이지에서 변수 이름 표시 링크를 클릭하십시오.)

변수	설명
\$ApprovalPriority\$	작업 승인 우선 순위
\$ApprovalDate\$	작업 승인 날짜
\$ApproverEmails\$	작업 승인자의 전자 메일 주소를 쉼표로 구분한 목록
\$AppURL\$	NA에 대한 링크를 직접 전자 메일 메시지에 포함하기 위해 사용되는 NA의 응용 프로그램 URL(예: https://host/)
\$EventID\$	이 이벤트에 대한 NA의 식별 번호
\$EventType\$	이벤트 유형
\$EventDate\$	이벤트가 발생한 날짜
\$EventText\$	이벤트 세부사항
\$EventUserFirstName\$	이 이벤트와 연관된 NA 사용자의 이름. (참고: 이벤트와 연관된 사용자가 없거나 해당 사용자에게 설정된 이름이 없을 경우 이것은 빈 문자열이 됩니다.)
\$EventUserLastName\$	이 이벤트와 연관된 NA 사용자의 성. (참고: 이벤트와 연관된 사용자가 없거나 해당 사용자에게 설정된 성이 없을 경우 이것은 빈 문자열이 됩니다.)
\$EventUserName\$	이 이벤트와 연관된 NA 사용자 이름(해당되는 경우 "사용자 없음"을 나타냄)
\$EventUserEmail\$	이 이벤트와 연관된 사용자의 전자 메일 주소
\$FyiEmails\$	작업 참고 수신자의 전자 메일 주소를 쉼표로 구분한 목록
\$LocalHostName\$	NA 서버의 호스트 이름
\$LocalHostAddress\$	NA 서버의 IP 주소
\$OriginatorFirstName\$	작업 주관자의 이름


변수	설명
\$OriginatorLastName\$	작업 주관자의 성
\$OriginatorName\$	작업 주관자의 이름
\$TaskName\$	작업 이름
\$TaskComments\$	작업 주석
\$TaskDevices\$	작업의 영향을 받는 장치 목록
\$TaskFrequency\$	작업의 빈도
\$TaskID\$	이벤트가 작업과 연관되지 않은 경우 null 문자열

11장: 검색 수행

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

검색	참조
장치 검색	583페이지의 "장치 검색"
인터페이스 검색	593페이지의 "인터페이스 검색"
모듈 검색	597페이지의 "모듈 검색"
정책 검색	601페이지의 "정책 검색"
준수 검색	605페이지의 "정책, 규칙 및 준수 검색"
구성 검색	610페이지의 "구성 검색 페이지 필드"
진단 검색	616페이지의 "진단 검색"
작업 검색	622페이지의 "작업 검색"
세션 검색	630페이지의 "세션 검색"
이벤트 검색	636페이지의 "이벤트 검색"
이벤트 설명	640페이지의 "이벤트 설명"
사용자 검색	648페이지의 "사용자 검색"
ACL 검색	651페이지의 "ACL 검색"
MAC 주소 검색	657페이지의 "MAC 주소 검색"
IP 주소 검색	661페이지의 "IP 주소 검색"
VLAN 검색	665페이지의 "VLAN 검색"
장치 템플릿 검색	668페이지의 "장치 템플릿 검색"
단일 검색	671페이지의 "단일 검색"
고급 검색	674페이지의 "고급 검색"

검색 페이지로 이동

 HP Network Automation 로그아웃							
장치 ▾	작업 ▾	정책 ▾	보고서 ▾	관리 ▾	도움말 ▾		
↓							
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"></td> <td style="width: 50%;"> <ul style="list-style-type: none"> 단일 보기 단일 검색 사용자 및 시스템 보고서 검색 대상 ▶ <ul style="list-style-type: none"> 장치 인터페이스 모듈 정책 준수 구성 진단 작업 텔넷 /SSH 세션 이벤트 사용자 ACL MAC 주소 IP 주소 VLAN 장치 템플릿 고급 검색 준수 센터 네트워크 상태 모범 사례 장치 상태 통계 대시보드 다이어그램 작성 장치 소프트웨어 소프트웨어 취약점 이미지 동기화 보고서 시스템 및 네트워크 이벤트 요약 보고서 보고서 작업 ▶ </td> </tr> </table>							<ul style="list-style-type: none"> 단일 보기 단일 검색 사용자 및 시스템 보고서 검색 대상 ▶ <ul style="list-style-type: none"> 장치 인터페이스 모듈 정책 준수 구성 진단 작업 텔넷 /SSH 세션 이벤트 사용자 ACL MAC 주소 IP 주소 VLAN 장치 템플릿 고급 검색 준수 센터 네트워크 상태 모범 사례 장치 상태 통계 대시보드 다이어그램 작성 장치 소프트웨어 소프트웨어 취약점 이미지 동기화 보고서 시스템 및 네트워크 이벤트 요약 보고서 보고서 작업 ▶
	<ul style="list-style-type: none"> 단일 보기 단일 검색 사용자 및 시스템 보고서 검색 대상 ▶ <ul style="list-style-type: none"> 장치 인터페이스 모듈 정책 준수 구성 진단 작업 텔넷 /SSH 세션 이벤트 사용자 ACL MAC 주소 IP 주소 VLAN 장치 템플릿 고급 검색 준수 센터 네트워크 상태 모범 사례 장치 상태 통계 대시보드 다이어그램 작성 장치 소프트웨어 소프트웨어 취약점 이미지 동기화 보고서 시스템 및 네트워크 이벤트 요약 보고서 보고서 작업 ▶ 						

장치 검색

장치 검색을 사용하면 여러 기준과 연산자를 조합하여 장치를 검색할 수 있습니다. 지정된 정책이나 규칙을 준수하지 않는 장치를 검색할 수도 있습니다. 정책에 대한 자세한 내용은 [511페이지의 "정책 생성"](#)을 참조하십시오.

장치를 검색하려면 보고서 아래의 메뉴 모음에서 검색 대상을 선택하고 장치를 클릭합니다. 장치 검색 페이지가 열립니다. 검색 기준 입력을 완료한 후에는 검색 버튼을 클릭합니다. NA는 장치 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 장치 목록을 반환합니다. 자세한 내용은 [590페이지의 "장치 검색 결과 페이지 필드"](#)를 참조하십시오.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

장치 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 장치 검색 결과 페이지에 포함할 정보를 선택합니다.
호스트 이름	연산자를 선택하고 호스트 이름을 입력합니다. 연산자는 다음과 같습니다. <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 IP	연산자를 선택하고 장치의 IP 주소를 입력합니다.
보조 IP 주소	연산자를 선택하고 장치의 보조 IP 주소를 입력합니다.
장치 공급업체	연산자를 선택하고 장치를 제조한 공급업체의 이름을 입력합니다.
장치 모델	연산자를 선택하고 장치의 모델 명칭을 입력합니다.
장치 유형	스크롤 다운 메뉴에서 라우터, 스위치, 방화벽, VPN, 가상 스위치, 전화 접속, DSL_ISDN, WAN, 무선 AP 또는 로드 밸런서 등의 네트워크 장치 유형을 선택합니다.
장치 상태	장치에 대해 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 활성화 • 비활성 • 사전 프로덕션(사전 프로덕션 장치는 프로덕션 네트워크에서 아직 활성화되지 않은 장치입니다. 자세한 내용은 153페이지의 "Bare Metal 프로비전"을 참조하십시오.)

필드	설명/작업
드라이버 이름	스크롤 다운 메뉴에서 장치와 연관된 하나 이상의 드라이버를 선택합니다. 여러 드라이버를 선택하려면 첫 번째 드라이버를 클릭한 다음 Ctrl을 누른 상태에서 클릭하여 추가 드라이버를 선택합니다.
FQDN	연산자를 선택하고 FQDN(정규화된 도메인 이름)을 선택합니다.
정책 준수	장치에 대해 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •모두(기본값) •준수하는 장치 •준수하지 않는 장치 •장치에 적용 가능한 정책 없음 •규칙 우선 순위에 따른 비준수 — 드롭다운 메뉴에서 규칙 우선 순위를 선택합니다. 심각, 높음, 중간, 낮음 또는 정보용을 선택할 수 있습니다. 이를 통해 지정된 중요도 이상의 구성 규칙을 위반하는 장치만을 포함하도록 검색을 필터링할 수 있습니다. (구성 정책 규칙의 중요도 등급에 대한 자세한 내용은 518페이지의 "새 규칙 페이지 필드"를 참조하십시오.) •선택한 정책 비준수 — 목록에서 하나 이상의 정책을 선택합니다. •선택한 규칙 비준수 — 목록에서 하나 이상의 규칙을 선택합니다. 정책 규칙에 대한 자세한 내용은 518페이지의 "새 규칙 페이지 필드"를 참조하십시오.
액세스 방법	스크롤 다운 메뉴에서 액세스 방법을 선택합니다. <ul style="list-style-type: none"> •FTP •RLogin •SCP •SNMP •SSH •TFTP •텔넷
장치 위치	연산자를 선택하고 장치의 위치를 입력합니다.
일련 번호	연산자를 선택하고 장치의 일련 번호를 입력합니다.

필드	설명/작업
자산 태그	연산자를 선택하고 장치 자산 태그에서 정보를 입력합니다.
장치 소프트웨어 버전	연산자를 선택하고 장치에서 실행 중인 운영 체제의 버전 번호를 입력합니다.
장치 펌웨어 버전	연산자를 선택하고 장치에서 실행 중인 펌웨어의 버전 번호를 입력합니다.
장치 설명	연산자를 선택하고 설명을 입력합니다.
주석	연산자를 선택하고 장치 주석의 고유한 부분을 입력합니다.
사용 가능 포트	연산자(다음과 같음, 이(가) 다음보다 작음 또는 이(가) 다음보다 큼)를 선택하고 사용 가능한 포트 수를 입력합니다.
사용 가능한 포트의 백분율	연산자(다음과 같음, 이(가) 다음보다 작음 또는 이(가) 다음보다 큼)를 선택하고 사용 가능한 포트의 백분율을 입력합니다.
총 포트 수	연산자(다음과 같음, 이(가) 다음보다 작음 또는 이(가) 다음보다 큼)를 선택하고 장치의 총 포트 수를 입력합니다.
사용 중인 포트	연산자(다음과 같음, 이(가) 다음보다 작음 또는 이(가) 다음보다 큼)를 선택하고 사용 중인 포트 수를 입력합니다.
사용 중인 포트 백분율	연산자(다음과 같음, 이(가) 다음보다 작음 또는 이(가) 다음보다 큼)를 선택하고 사용 중인 포트의 백분율을 입력합니다.
시스템 메모리	연산자(다음과 같음, 이(가) 다음보다 작음 또는 이(가) 다음보다 큼)를 선택하고 장치의 총 RAM(MB) 크기를 입력합니다.
작동 시간	연산자(다음과 같음, 이(가) 다음보다 작음 또는 이(가) 다음보다 큼)를 선택하고 총 일수를 입력합니다. 장치 검색 결과 페이지에 장치가 마지막으로 재부팅된 이후의 총 일수, 시간 수, 분수 및 초수가 표시됩니다.

참고: 작동 시간 데이터는 NA 감지 장치 부팅 진단 중에 수집됩니다. 작동 시간 데이터를 신뢰할 수 있으려면 이 데이터를 정기적으로 수집하는 반복 진단 작업이 마련되어야 합니다. 일부 장치의 경우 NA 감지 장치 부팅 진단을 지원하지 않을 수도 있습니다. 진단을 지원하지 않은 장치와 진단이 한 번도 실행되지 않은 장치는 작동 시간 및 작동 시간 저장 날짜 필드가 비어 있습니다. 진단 실행 작업에 대한 자세한 내용은 [397페이지의 "진단 실행 작업 페이지 필드"](#)를 참조하십시오.

필드	설명/작업
작동 시간 저장 날짜	<p>연산자(이후 또는 까지)를 선택한 다음 풀다운 메뉴에서 타임프레임을 선택합니다. 기본값은 항상입니다. 캘린더 옵션을 사용하여 특정 일을 선택할 수 있습니다. NA 감지 장치 부팅 진단이 마지막으로 실행된 시간이 장치 검색 결과 페이지에 표시됩니다. NA 감지 장치 부팅 진단에 대한 자세한 내용은 261페이지의 "메뉴 옵션 보기"를 참조하십시오.</p> <p>참고: 작동 시간 데이터는 NA 감지 장치 부팅 진단 중에 수집됩니다. 작동 시간 데이터를 신뢰할 수 있으려면 이 데이터를 정기적으로 수집하는 반복 진단 작업이 마련되어야 합니다. 일부 장치의 경우 NA 감지 장치 부팅 진단을 지원하지 않을 수도 있습니다. 진단을 지원하지 않은 장치와 진단이 한 번도 실행되지 않은 장치는 작동 시간 및 작동 시간 저장 날짜 필드가 비어 있습니다.</p>
구성 텍스트	<p>연산자(다음 포함 또는 다음 포함하지 않음)를 선택하고 검색할 장치 구성의 고유 부분을 입력합니다. 검색 연산자가 "다음 포함"인 경우에는 페이지 아래쪽에 있는 "현재 구성을 표시할 때 일치하는 라인 주변에 <#>개의 컨텍스트 라인 표시" 확인란에 값을 입력할 수 있습니다. 결과 페이지에 검색 텍스트의 위아래로 최대 5개 라인까지 포함할 수 있습니다. 기본값은 세 개입니다. (참고: 로드할 결과 수가 많은 경우에는 성능이 상당히 느려질 수 있습니다.)</p>
다른 시작/실행	<p>선택된 경우, 시작 및 실행 구성이 다른 장치를 검색합니다.</p>
마지막으로 변경된 시간	<p>다음 연산자를 선택합니다.</p> <ul style="list-style-type: none"> •이래 또는 다음까지 •항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>
생성 날짜	<p>다음 연산자를 선택합니다.</p> <ul style="list-style-type: none"> •이래 또는 다음까지 •항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>

필드	설명/작업
암호 규칙	연산자를 선택하고 암호 규칙 이름을 입력합니다.
ACL ID	연산자를 선택하고 ACL ID를 입력합니다.
ACL 핸들	연산자를 선택하고 ACL 핸들을 입력합니다.
ACL 유형	연산자를 선택하고 ACL 유형을 입력합니다.
ACL 구성	연산자를 선택하고 ACL 유형을 입력합니다.
ACL 응용 프로그램	연산자를 선택하고 ACL 응용 프로그램을 입력합니다.
모듈 슬롯	연산자를 선택하고 모듈 슬롯을 입력합니다.
모듈 설명	연산자를 선택하고 모듈 설명을 입력합니다.
모듈 모델	연산자를 선택하고 모듈 모델을 입력합니다.
모듈 일련 번호	연산자를 선택하고 모듈 일련 번호를 입력합니다.
모듈 메모리	연산자를 선택하고 모듈 메모리를 입력합니다.
모듈 펌웨어 버전	연산자를 선택하고 모듈의 펌웨어 버전을 입력합니다.
모듈 하드웨어 개정판	연산자를 선택하고 모듈 하드웨어 개정판을 입력합니다.
ROM 버전	연산자를 선택하고 모듈 ROM 버전을 입력합니다. ROM 버전은 ROM에서 운영 체제를 부팅하고 로드하는 방법을 장치에 지시하는 데 사용되는 부트스트랩 코드 버전입니다.
서비스 유형	연산자를 선택하고 서비스 유형을 입력합니다.
사용자 지정 서비스 유형	연산자를 선택하고 사용자 지정 서비스 유형을 입력합니다.
VTP 도메인 이름	연산자를 선택하고 VTP(VLAN Trunking Protocol) 도메인 이름을 입력합니다.
VTP 운영 모드	연산자를 선택하고 VTP(VLAN Trunking Protocol) 운영 모드를 입력합니다.
장치 사용자 지정 데이터	연산자를 선택하고 나열된 사용자 지정 필드에 나타날 수 있는 고유한 텍스트를 입력합니다. (참고: 이 섹션은 사용자 지정 필드가 없는 경우에는 표시되지 않습니다.)

필드	설명/작업
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> • 선택한 그룹 중 하나(기본값) • 선택한 그룹 모두 • 선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

검색 버튼을 클릭하면 **NA**는 장치 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 장치 목록을 반환합니다. 자세한 내용은 [590페이지의 "장치 검색 결과 페이지 필드"](#)를 참조하십시오.

장치 검색 결과 페이지 필드

장치 검색 결과 페이지는 장치 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 검색 기준에 대한 자세한 내용은 [584페이지의 "장치 검색 페이지 필드"](#)를 참조하십시오. 다음 표는 장치 검색 결과 페이지에서 사용 가능한 옵션을 설명합니다.

옵션	설명/작업
이 검색 수정 링크	장치 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.

옵션	설명/작업
확인란	<p>왼쪽의 확인란을 사용하여 장치를 관리할 수 있습니다. 장치를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음을 클릭합니다.</p> <ul style="list-style-type: none"> • 활성화 — 선택한 장치를 관리하도록 NA에 지시합니다. • 비활성화 — 선택한 장치를 관리하지 않도록 NA에 지시합니다. • 일괄 편집 — 일괄 편집 페이지를 엽니다. 209페이지의 "장치 일괄 편집 페이지 필드"를 참조하십시오. • 다이어그램 — 758페이지의 "다이어그램 작성"을 참조하십시오. • 삭제 — 선택한 장치를 삭제합니다. • 정책 준수 확인 — 462페이지의 "정책 준수 확인 작업 페이지 필드"를 참조하십시오. • Syslog 구성 — 366페이지의 "Syslog 구성 작업 페이지 필드"를 참조하십시오. • 암호 배포 — 370페이지의 "암호 배포 작업 페이지 필드"를 참조하십시오. • 드라이버 검색 — 375페이지의 "드라이버 검색 작업 페이지 필드"를 참조하십시오. • 장치 재부팅 — 379페이지의 "장치 재부팅 작업 페이지 필드"를 참조하십시오. • 명령 스크립트 실행 — 389페이지의 "명령 스크립트 실행 작업 페이지 필드"를 참조하십시오. • 진단 실행 — 397페이지의 "진단 실행 작업 페이지 필드"를 참조하십시오. • ICMP 테스트 실행 — 383페이지의 "ICMP 테스트 실행 작업 페이지 필드"를 참조하십시오. • 스냅샷 작성 — 403페이지의 "스냅샷 작성 작업 페이지 필드"를 참조하십시오. • 시작 및 실행 동기화 — 408페이지의 "시작 및 실행 동기화 작업 페이지 필드"를 참조하십시오. • 장치 소프트웨어 업데이트 — 413페이지의 "장치 소프트웨어 업데이트 작업 페이지 필드"를 참조하십시오. • ALC 삭제 — 888페이지의 "ACL 삭제 작업 페이지"를 참조하십시오. • OS 분석 — 436페이지의 "OS 분석 작업 페이지 필드"를 참조하십시오. • 장치 프로비전 — 146페이지의 "장치 편집 페이지 필드"를 참조하십시오.

옵션	설명/작업
	<p>인접한 선택 드롭다운 메뉴를 통해 모든 장치를 선택하거나 선택 취소할 수 있습니다.</p>
작업	<p>장치 검색 결과 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 편집 — 이 장치에 대한 정보를 편집할 수 있는 장치 편집 페이지를 엽니다. • 텔넷 — NA CLI의 텔넷 창을 엽니다. NA에서 장치에 로그인하려고 합니다. • SSH — NA CLI에 대한 SSH 창을 엽니다. NA에서 장치에 로그인하려고 합니다. • 구성 보기 — 선택한 구성을 편집하고 주석을 추가할 수 있는 현재 구성 페이지를 엽니다.
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> • 새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다. • 기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다. • 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. • 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. • 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

인터페이스 검색

인터페이스 검색을 사용하여 NA 데이터베이스에서 장치에 설치된 인터페이스에 대한 정보를 검색할 수 있습니다. 포트는 레이어 2 용어이고 인터페이스는 레이어 3 용어지만 NA는 이 둘을 구분하지 않습니다.

인터페이스를 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 인터페이스를 클릭합니다. 인터페이스 검색 페이지가 열립니다. 검색 기준 입력을 완료한 후에는 검색 버튼을 클릭합니다. NA는 인터페이스 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 인터페이스 목록을 반환합니다. 자세한 내용은 [596페이지의 "인터페이스 검색 결과 페이지 필드"](#)를 참조하십시오.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

인터페이스 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 인터페이스 검색 결과 페이지에 포함할 정보를 선택합니다.
포트 이름	연산자를 선택하고 Ethernet0 또는 Serial1 등의 포트 이름을 입력합니다. 포트는 바인딩과 네트워크 주소의 결합으로 정의되는 단일 종결 지점으로 정의되어 있습니다. 연산자는 다음과 같습니다. <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음
포트 IP	연산자를 선택하고 포트 IP를 입력합니다.
CIDR 범위	연산자를 선택하고 포트의 CIDR(Classless Inter-Domain Routing) 범위를 입력합니다(예: 192.168.1.0-192.168.2.0 또는 192.168.31.0/24). CIDR 범위가 포함됨을 잊지 마십시오.

필드	설명/작업
포트 유형	연산자를 선택하고 Ethernet, FastEthernet 또는 PortChannel 등 포트 유형을 입력합니다.
포트 상태	연산자를 선택하고 포트가 구성 또는 관리를 위해 작동이 중지 등 포트 상태를 입력합니다.
실행 중인 포트 상태	포트가 구성(Configured Up) 또는 관리를 위해 작동이 중지(Administratively Down)인 경우 표시됩니다. (참고: 이는 포트의 프로토콜 상태는 반영하지 않고 구성된 상태만 반영합니다.)
설명	연산자를 선택하고 포트 설명을 입력합니다.
구성된 이중	연산자를 선택하고 포트의 구성된 이중 설정을 입력합니다.
구성된 속도	연산자를 선택하고 포트의 구성된 속도 설정을 입력합니다.
협상 이중	연산자를 선택하고 포트의 감지된 이중 설정을 입력합니다.
협상 속도	연산자를 선택하고 포트의 감지된 속도 설정을 입력합니다.
VLAN	연산자를 선택하고 포트 VLAN 이름을 입력합니다. VLAN 이름은 검색을 제한할 VLAN의 이름(예: VLAN2 또는 VLAN3)입니다.
호스트 이름	연산자를 선택하고 장치 호스트 이름을 입력합니다. 와일드 카드 문자를 사용할 수 있음을 잊지 마십시오. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)
장치 IP	연산자를 선택하고 장치의 IP 주소를 입력합니다.
모듈 슬롯	연산자를 선택하고 모듈 슬롯 번호를 입력합니다.
모듈 설명	연산자를 선택하고 모듈 설명을 입력합니다.
모듈 모델	연산자를 선택하고 모듈의 모델 번호를 입력합니다.
모듈 일련 번호	연산자를 선택하고 모듈의 일련 번호를 입력합니다.
모듈 펌웨어 버전	연산자를 선택하고 모듈의 펌웨어 버전을 입력합니다.

필드	설명/작업
인터페이스 사용자 지정 데이터	연산자를 선택하고 나열된 사용자 지정 필드에 나타날 수 있는 고유한 텍스트를 입력합니다. (참고: 이 섹션은 사용자 지정 필드가 없는 경우에는 표시되지 않습니다.)
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> • 선택한 그룹 중 하나(기본값) • 선택한 그룹 모두 • 선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 여러 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

인터페이스 검색 결과 페이지 필드

인터페이스 검색 결과 페이지는 인터페이스 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 검색 기준에 대한 자세한 내용은 [593페이지의 "인터페이스 검색 페이지 필드"](#)를 참조하십시오. 다음 표는 인터페이스 검색 결과 페이지에서 사용 가능한 옵션을 설명합니다.

옵션	설명/작업
이 검색 수정 링크	인터페이스 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
확인란	<p>왼쪽의 확인란을 통해 인터페이스를 선택할 수 있습니다. 인터페이스를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 인터페이스 스크립트 실행을 클릭합니다. 새 작업 - 명령 스크립트 실행 페이지가 열립니다. 자세한 내용은 738페이지의 "명령 스크립트 실행"을 참조하십시오.</p> <p>인접한 선택 드롭다운 메뉴를 사용하면 모든 인터페이스를 선택하거나 선택 취소할 수 있습니다.</p>
작업	<p>인터페이스 검색 결과 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 인터페이스 편집 — 이 인터페이스에 대한 정보를 편집할 수 있는 인터페이스 세부사항 편집 페이지를 엽니다. 자세한 내용은 271페이지의 "인터페이스 편집 세부사항 페이지 필드"를 참조하십시오. • 인터페이스 보기 — 인터페이스 세부 정보를 볼 수 있는 인터페이스 세부사항 페이지를 엽니다. 자세한 내용은 269페이지의 "인터페이스 세부사항 페이지 필드"를 참조하십시오.
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> • 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. • 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. • 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

모듈 검색

모듈 검색을 사용하여 NA 데이터베이스에서 장치에 설치된 카드, 블레이드 또는 모듈에 대한 정보를 검색할 수 있습니다.

모듈을 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 모듈을 클릭합니다. 모듈 검색 페이지가 열립니다. 검색 기준 입력을 완료한 후 검색 버튼을 클릭하면 NA는 모듈 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 모듈 목록을 반환합니다. 자세한 내용은 [601페이지의 "정책 검색"](#)을 참조하십시오.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

모듈 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 모듈 검색 결과 페이지를 사용자 지정합니다.
호스트 이름	연산자를 선택하고 호스트 이름을 입력합니다. 연산자는 다음과 같습니다. <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 IP	연산자를 선택하고 장치의 IP 주소를 입력합니다.
모듈 슬롯	연산자를 선택하고 모듈이 설치된 장치의 슬롯을 입력합니다.

필드	설명/작업
모듈 설명	연산자를 선택하고 모듈 설명의 고유한 부분을 입력합니다.
모듈 모델	연산자를 선택한 다음 모듈의 모델을 입력합니다. 연산자는 다음과 같습니다. <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
모듈 일련 번호	연산자를 선택하고 모듈의 일련 번호를 입력합니다.
모듈 메모리	연산자를 선택하고 모듈의 총 RAM(MB) 크기를 입력합니다.
모듈 펌웨어 버전	연산자를 선택하고 모듈에 로드된 펌웨어의 버전 번호를 입력합니다.
모듈 하드웨어 개정판	연산자를 선택하고 모듈의 하드웨어 수정 버전 명칭의 일부를 입력합니다.
주석	연산자를 선택하고 모듈 설명 부분을 입력합니다.
모듈 사용자 지정 데이터	연산자를 선택하고 나열된 사용자 지정 필드에 나타날 수 있는 고유한 텍스트를 입력합니다. (참고: 이 섹션은 사용자 지정 필드가 없는 경우에는 표시되지 않습니다.)

필드	설명/작업
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none">• 선택한 그룹 중 하나(기본값)• 선택한 그룹 모두• 선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

모듈 검색 결과 페이지 필드

모듈 검색 결과 페이지는 모듈 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [597페이지의 "모듈 검색 페이지 필드"](#)를 참조하십시오. 다음 표는 모듈 검색 결과 페이지에서 사용 가능한 옵션을 설명합니다.

옵션	설명/작업
이 검색 수정 링크	모듈 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
작업	<p>모듈 검색 결과 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 모듈 편집 — 이 모듈에 대한 정보를 편집할 수 있는 블레이드/모듈 세부 사항 편집 페이지를 엽니다. • 모듈 보기 — 모듈 세부사항을 볼 수 있는 블레이드/모듈 세부사항 페이지를 엽니다.
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> • 새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다. • 기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다. • 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. • 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. • 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

정책 검색

NA 정책 관리자는 NA가 감지하는 각 장치 구성 변경 사항에 규칙 또는 필터 집합을 적용합니다. 장치 또는 장치 그룹의 변경 사항이 표준을 준수하지 않는 경우에는 NA 정책 관리자에서 알림 규칙을 트리거할 수 있는 이벤트를 생성합니다. 따라서 사용자는 비준수 변경 사항을 수정하고 준수 및 네트워크 가용성을 유지할 수 있습니다. 정책 관리에 대한 자세한 내용은 [511페이지의 "정책 생성"](#)을 참조하십시오. 자동 수정 기능에 대한 내용은 [510페이지의 "NA 정책 관리자의 작업 방식"](#)을 참조하십시오.

정책 검색 페이지를 사용하면 보려는 정책 목록의 범위를 좁힐 수 있습니다. 다음을 수행할 수 있습니다.

- 정책 속성을 검색 기준으로 사용하여 NA에서 정책 목록을 쉽게 생성합니다.
- NA에서 정책을 쉽게 관리합니다.

현재 정책을 모두 보려면 정책 아래의 기본 메뉴 모음에서 정책 목록을 클릭합니다. 자세한 내용은 [512페이지의 "정책 페이지 필드"](#)를 참조하십시오.

정책을 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 정책을 클릭합니다. 정책 검색 페이지가 열립니다. 검색 기준 입력을 완료한 후에는 검색 버튼을 클릭합니다. NA는 정책 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 정책 목록을 반환합니다.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

정책 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 정책 검색 결과 페이지를 사용자 지정합니다.

필드	설명/작업
정책 이름	연산자를 선택하고 정책 이름을 입력합니다. 연산자는 다음과 같습니다. <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음
장치 그룹	검색될 정책 범위와 일치하는 장치 그룹을 선택합니다. 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기" 를 참조하십시오.
생성 날짜	다음 연산자를 선택합니다. <ul style="list-style-type: none"> • 이래 또는 다음까지 • 항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>
상태	다음 연산자 중 하나를 선택합니다. <ul style="list-style-type: none"> • 모두(기본값) • 활성 • 비활성
CVE	CVE(Common Vulnerabilities and Exposures) 이름을 연산자와 함께 입력합니다. CVE는 취약점의 표준화된 이름과 보안 노출에 관한 기타 정보의 목록입니다.
공개 날짜	다음 연산자를 선택합니다. <ul style="list-style-type: none"> • 이래 또는 다음까지 • 항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>
솔루션	솔루션 텍스트를 연산자와 함께 입력합니다.

필드	설명/작업
공급업체 URL	취약점에 대한 자세한 내용은 외부 참조에 대한 URL을 연산자와 함께 입력합니다.
솔루션 URL	취약점에 대한 가능한 솔루션에 대한 자세한 내용은 외부 참조에 대한 URL을 연산자와 함께 입력합니다.
정책 태그	검색할 정책 태그를 선택합니다. 정책 태그를 사용하면 선택한 태그가 있는 정책과 관련된 준수 항목을 검색할 수 있습니다.
파티션	검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션" 을 참조하십시오.)

정책 검색 결과 페이지 필드

정책 검색 결과 페이지는 정책 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [601페이지의 "정책 검색 페이지 필드"](#)를 참조하십시오.

옵션	설명/작업
확인란/드롭다운 메뉴	<p>왼쪽의 확인란을 사용하여 장치를 관리할 수 있습니다. 장치를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음을 클릭합니다.</p> <ul style="list-style-type: none"> •활성화 — 선택한 장치를 관리하도록 NA에 지시합니다. •비활성화 — 선택한 장치를 관리하지 않도록 NA에 지시합니다. •일괄 편집 — 선택한 정책의 범위를 수정하고, 장치 예외를 추가하며 해당 정책의 상태를 설정할 수 있는 정책 일괄 편집 페이지를 엽니다. •삭제 — 선택한 장치를 삭제합니다.
이 검색 수정 링크	정책 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
작업	<p>각 정책에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> •보기 및 편집 — 정책을 수정할 수 있는 정책 편집 페이지를 엽니다. •테스트 — 테스트 정책 페이지를 엽니다. 자세한 내용은 545페이지의 "정책 준수 테스트 페이지 필드"를 참조하십시오.
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> •검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. •검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. •검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

정책, 규칙 및 준수 검색

정책, 규칙 및 준수 검색 페이지에서는 장치 및 장치와 연관된 준수 및 해당되는 정책/규칙을 검색할 수 있습니다. 다음을 수행할 수 있습니다.

- 준수를 지키거나 지키지 않는 장치 목록을 쉽게 생성합니다.
- 특정 정책 규칙을 아직 확인하지 않은 장치 목록을 쉽게 생성합니다.
- 정책 규칙이 적용된 장치를 식별합니다.
- 특정 장치에 적용되는 정책 규칙을 식별합니다.
- 적용 가능한 정책이 없는 장치를 식별합니다.

참고: 장치와 관련되지 않은 정책이나 규칙을 검색할 수 없음을 유의하십시오.

정책, 정책 규칙 및 준수 위반을 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 준수를 클릭합니다. 정책, 규칙 및 준수 검색 페이지가 열립니다. 검색 기준 입력을 완료한 후에는 검색 버튼을 클릭합니다. NA는 정책, 규칙 및 준수 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 장치 목록을 반환합니다.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

정책, 규칙 및 준수 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 정책 검색 결과 페이지를 사용자 지정합니다.
호스트 이름	연산자를 선택하고 호스트 이름을 입력합니다. 연산자는 다음과 같습니다. <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 IP	연산자를 선택하고 장치의 IP 주소를 입력합니다.
장치 그룹	장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기" 를 참조하십시오.
준수	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 모든 준수 상태 • 준수하는 장치 • 준수하지 않는 장치 • 장치가 아직 확인되지 않음 • 장치에 적용 가능한 정책 없음
정책	정책 이름을 입력하거나 드롭다운 메뉴에서 정책을 선택합니다.
규칙	정책 구성 규칙을 입력하거나 드롭다운 메뉴에서 하나를 선택합니다.

필드	설명/작업
규칙 유형	<p>다음 옵션 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none"> •구성 •진단 •소프트웨어
규칙 중요성	<p>하나 이상의 중요도 수준을 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> •정보용 — 일반적으로 응답이 필요하지 않은 이벤트 •낮음 — 시간이 허용될 경우 응답이 필요할 수 있는 이벤트 •중간 — 일반적으로 72시간 이내에 시기 적절한 응답이 필요한 이벤트 •높음 — 일반적으로 24시간 이내에 신속한 응답이 필요한 이벤트 •심각 — 즉각적인 응답이 필요한 이벤트
규칙 설명	<p>검색 결과에 규칙 설명을 포함합니다.</p>
CVE	<p>CVE(Common Vulnerabilities and Exposures) 이름을 연산자와 함께 입력합니다. CVE는 취약점의 표준화된 이름과 보안 노출에 관한 기타 정보의 목록입니다.</p>
마지막으로 확인된 날짜	<p>다음 연산자를 선택합니다.</p> <ul style="list-style-type: none"> •이래 또는 다음까지 •항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>
정책 태그	<p>정책 태그를 선택합니다. 정책 태그를 사용하면 선택한 태그가 있는 정책과 관련된 준수 항목을 검색할 수 있습니다.</p>
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

정책, 규칙 및 준수 검색 결과 페이지 필드

정책, 규칙 및 준수 검색 결과 페이지에는 정책, 규칙 및 준수 검색 페이지에서 선택한 검색 기준이 표시됩니다. 자세한 내용은 [606페이지의 "정책, 규칙 및 준수 검색 페이지 필드"](#)를 참조하십시오.

옵션	설명/작업
확인란/드롭다운 메뉴	<p>왼쪽의 확인란을 사용하여 장치를 관리할 수 있습니다. 장치를 선택한 후 작업 드롭다운 메뉴를 클릭하고 다음과 같은 작업을 선택합니다.</p> <ul style="list-style-type: none"> •활성화 — 선택한 장치를 관리하도록 NA에 지시합니다. •비활성화 — 선택한 장치를 관리하지 않도록 NA에 지시합니다. •일괄 편집 — 드라이버를 할당하고 선택한 모든 장치의 연결 방법을 설정할 수 있는 장치 일괄 편집 페이지를 엽니다. •다이어그램 — 758페이지의 "다이어그램 작성"을 참조하십시오. •삭제 — 선택한 장치를 삭제합니다. •정책 준수 확인 — 462페이지의 "정책 준수 확인 작업 페이지 필드"를 참조하십시오. •Syslog 구성 — 366페이지의 "Syslog 구성 작업 페이지 필드"를 참조하십시오. •암호 배포 — 370페이지의 "암호 배포 작업 페이지 필드"를 참조하십시오. •드라이버 검색 — 375페이지의 "드라이버 검색 작업 페이지 필드"를 참조하십시오. •장치 재부팅 — 379페이지의 "장치 재부팅 작업 페이지 필드"를 참조하십시오. •명령 스크립트 실행 — 389페이지의 "명령 스크립트 실행 작업 페이지 필드"를 참조하십시오. •진단 실행 — 397페이지의 "진단 실행 작업 페이지 필드"를 참조하십시오. •ICMP 테스트 실행 — 383페이지의 "ICMP 테스트 실행 작업 페이지 필드"를 참조하십시오. •스냅샷 작성 — 403페이지의 "스냅샷 작성 작업 페이지 필드"를 참조하십시오.

옵션	설명/작업
확인란/드롭다운 메뉴(계속)	<ul style="list-style-type: none"> • 시작 및 실행 동기화 — 408페이지의 "시작 및 실행 동기화 작업 페이지 필드"를 참조하십시오. • 장치 소프트웨어 업데이트 — 413페이지의 "장치 소프트웨어 업데이트 작업 페이지 필드"를 참조하십시오. • ALC 삭제 — 888페이지의 "ACL 삭제 작업 페이지"를 참조하십시오. • OS 분석 — 436페이지의 "OS 분석 작업 페이지 필드"를 참조하십시오. • 장치 프로비전 — 146페이지의 "장치 편집 페이지 필드"를 참조하십시오.
자세한 CVS 보고서 보기	<p>준수에 실패한 이유를 설명하는 이벤트 세부사항을 포함하여 모든 레코드로 CSV 파일을 작성할 수 있습니다.</p>
이 검색 수정 링크	<p>정책, 규칙 및 준수 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.</p>
검색 기준 보기 링크	<p>검색 기준 정보로 아래로 스크롤합니다.</p>
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> • 새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다. • 기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다. • 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. • 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. • 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

구성 검색

구성 검색을 사용하면 여러 기준과 연산자를 조합하여 구성 파일을 검색할 수 있습니다. 모든 검색 기준은 부울 연산자인 AND/OR로 결합되어 있으며 결과는 모든 기준과 일치합니다.

구성 파일을 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 구성을 클릭합니다. 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

참고: 구성을 포함하는 기준을 사용하여 검색할 때 저장된 구성이 많은 경우 쿼리가 느릴 수 있습니다. 구성을 검색할 때 포함 옵션을 선택하는 것이 좋습니다. 따라서 Oracle이나 SQL Server 데이터베이스의 전체 텍스트 검색 기능이 사용됩니다.

검색 기준 입력을 완료한 후 검색 버튼을 클릭하면 NA는 구성 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 구성 목록을 반환합니다. 자세한 내용은 [614페이지의 "구성 검색 결과 페이지 필드"](#)를 참조하십시오.

구성 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 구성 검색 결과 페이지를 사용자 지정합니다.

필드	설명/작업
호스트 이름	<p>연산자를 선택하고 장치의 호스트 이름을 입력합니다. 연산자는 다음과 같습니다.</p> <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다 (예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 IP	연산자를 선택하고 장치의 IP 주소를 입력합니다.
날짜	<p>다음 연산자를 선택합니다.</p> <ul style="list-style-type: none"> • 이래 또는 다음까지 • 항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>
변경한 사람	연산자를 선택한 다음 장치 구성을 변경한 사용자의 로그인 이름을 입력합니다.
장치 상태	<p>장치에 대해 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 활성화 • 비활성 • 사전 프로덕션(사전 프로덕션 장치는 프로덕션 네트워크에서 아직 활성화되지 않은 장치입니다. 자세한 내용은 153페이지의 "Bare Metal 프로비전"을 참조하십시오.)
장치 유형	스크롤 다운 메뉴에서 라우터, 스위치, 방화벽, VPN, DialUp, DSL_ISDN 또는 로드 밸런서 등의 네트워크 장치 유형을 선택합니다.

필드	설명/작업
주석	연산자(다음을 포함 또는 다음을 포함하지 않음)를 선택한 다음 찾으려는 주석 텍스트를 입력합니다. 이는 장치 구성 세부사항 페이지의 구성 주석 상자에 나타나는 텍스트만을 검색합니다.
구성 텍스트	연산자(다음을 포함, 다음을 포함하지 않음, 포함 또는 포함하지 않음)를 선택하고 현재 장치 구성 파일의 고유한 부분을 입력합니다. 저장된 구성이 많으면 구성을 검색할 때 포함 옵션을 선택하는 것이 좋습니다. 검색 연산자가 "다음 포함"인 경우에는 페이지 아래쪽에 있는 "현재 구성을 표시할 때 일치하는 라인 주변에 <#>개의 컨텍스트 라인 표시" 확인란에 값을 입력할 수 있습니다. 결과 페이지에 검색 텍스트의 위아래로 최대 5개 라인까지 포함할 수 있습니다. 기본 값은 세 개입니다. (참고: 로드할 결과 수가 많은 경우에는 성능이 상당히 느려질 수 있습니다.)
검색 범위	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 현재 구성만 검색 — 이 옵션을 선택하면 현재 구성만 검색됩니다. • 모든 구성 검색 — 이 옵션을 선택하면 현재 및 이전의 모든 구성이 검색됩니다.
다른 시작/실행	선택된 경우, 시작 및 실행 구성이 다른 장치를 검색합니다.
구성 사용자 지정 데이터	연산자를 선택하고 나열된 사용자 지정 필드에 나타날 수 있는 고유한 텍스트를 입력합니다. (참고: 이 섹션은 사용자 지정 필드가 없는 경우에는 표시되지 않습니다.)
장치가 속한 위치	드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다. <ul style="list-style-type: none"> • 선택한 그룹 중 하나(기본값) • 선택한 그룹 모두 • 선택한 그룹 모두 없음 참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기" 를 참조하십시오.

필드	설명/작업
파티션	검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션" 을 참조하십시오.)

구성 검색 결과 페이지 필드

구성 검색 결과 페이지는 구성 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [610페이지의 "구성 검색 페이지 필드"](#)를 참조하십시오. 다음 표는 구성 검색 결과 페이지에서 사용 가능한 옵션을 설명합니다.

필드	설명/작업
이 검색 수정 링크	구성 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
확인란	<p>왼쪽의 확인란을 통해 NA 데이터베이스에서 구성을 비교하고 삭제할 수 있습니다. 구성을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음 중 하나를 클릭합니다.</p> <ul style="list-style-type: none"> •비교 — 두 개의 구성을 비교할 수 있는 장치 구성 비교 페이지를 엽니다. 차이점은 쉽게 비교할 수 있게 서로 다른 색상으로 강조 표시됩니다. 이 페이지에서 구성을 배포할 수도 있습니다. •삭제 — NA 데이터베이스에서 선택한 구성을 삭제합니다. <p>인접한 선택 드롭다운 메뉴를 통해 모든 장치를 선택하거나 선택 취소할 수 있습니다.</p>
작업	<p>구성 검색 결과 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> •이전과 비교 — 장치 구성을 보고 이전 구성과 나란히 비교해볼 수 있는 장치 구성 비교 페이지를 엽니다. 차이점은 쉽게 읽을 수 있게 서로 다른 색상으로 강조 표시됩니다. •구성 보기 — 선택한 구성을 편집하고 주석을 추가할 수 있는 장치 구성 세부사항 페이지를 엽니다. 이 페이지에서 선택한 구성을 배포할 수도 있습니다. •진단 — 이 구성에 대한 진단 정보를 볼 수 있는 진단 페이지를 엽니다.

필드	설명/작업
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> • 결과 장치를 새 장치 그룹으로 저장 — 새 그룹의 이름을 입력하고 그룹 생성을 클릭합니다. • 기존 장치 그룹에 결과 장치 추가 — 드롭다운 메뉴에서 그룹을 선택하고 추가를 클릭합니다. 참고: 동적 그룹 생성에 대한 자세한 내용은 180 페이지의 "동적 장치 그룹"을 참조하십시오. • 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. • 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. • 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다. (참고: 구성 텍스트 옵션을 선택했으며 구성 검색 페이지에서 검색 기준을 정의할 때 찾으려는 구성 텍스트를 입력한 경우 결과 세부 사항 포함 옵션을 선택합니다. 결과 세부사항 포함 옵션을 선택하지 않을 경우 구성 텍스트가 CSV 파일 안에 포함되지 않습니다.)

진단 검색

진단 검색은 사용자가 정의한 검색 기준을 기반으로 장치 진단 정보에 대한 액세스를 제공합니다. 결과는 모든 검색 기준과 일치합니다. 각 진단이 제공하는 정보 유형은 장치별로 제공됩니다.

진단을 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 진단을 클릭합니다. 진단 검색 페이지가 열립니다.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

검색 기준 입력을 완료한 후 검색 버튼을 클릭하면 NA는 진단 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 진단 목록을 반환합니다. 자세한 내용은 [620페이지의 "진단 검색 결과 페이지 필드"](#)를 참조하십시오.

참고: NA VLAN 데이터 수집과 NA 토폴로지 수집 진단은 검색할 수 있습니다. 자세한 내용은 [261페이지의 "메뉴 옵션 보기"](#)를 참조하십시오.

진단 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 진단 검색 결과 페이지를 사용자 지정합니다.
호스트 이름	<p>연산자를 선택하고 장치의 호스트 이름을 입력합니다. 연산자는 다음과 같습니다.</p> <ul style="list-style-type: none">• 다음을 포함• 다음을 포함하지 않음• 다음과 일치함• 다음과 같음• 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 IP	연산자를 선택하고 장치의 IP 주소를 입력합니다.
날짜	<p>다음 연산자를 선택합니다.</p> <ul style="list-style-type: none">• 이래 또는 다음까지• 항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>

필드	설명/작업
진단 유형	<p>스크롤 다운 메뉴에서 검색할 진단 데이터 유형을 선택합니다. 여러 유형을 선택하거나 선택 취소하려면 Ctrl을 누른 상태로 클릭합니다. 진단 유형은 다음과 같습니다.</p> <ul style="list-style-type: none"> •NA 장치 파일 시스템 •하드웨어 정보 •ICMP 테스트 •메모리 문제 해결 •NA 감지 장치 부팅 •NA 플래시 저장 공간 •NA 인터페이스 •NA 모듈 상태 •NA OSPF 인접 환경 •NA 포트 스캔 •NA 라우팅 테이블 •NA 토폴로지 데이터 수집 <p>참고: 진단에 대한 자세한 내용은 261페이지의 "메뉴 옵션 보기"의 진단 필드를 참조하십시오.</p>
장치 상태	<p>장치에 대해 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •활성 •비활성 •사전 프로덕션(사전 프로덕션 장치는 프로덕션 네트워크에서 아직 활성화되지 않은 장치입니다. 자세한 내용은 153페이지의 "Bare Metal 프로비전"을 참조하십시오.)
진단 텍스트	<p>연산자(다음은 포함 또는 다음을 포함하지 않음)를 선택하고 검색하거나 검색 결과에서 제외하고 싶은 진단의 고유한 일부분을 입력합니다.</p>
진단 사용자 지정 데이터	<p>연산자를 선택하고 나열된 사용자 지정 필드에 나타날 수 있는 고유한 텍스트를 입력합니다. (참고: 이 섹션은 사용자 지정 필드가 없는 경우에는 표시되지 않습니다.)</p>

필드	설명/작업
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none">• 선택한 그룹 중 하나(기본값)• 선택한 그룹 모두• 선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

진단 검색 결과 페이지 필드

진단 검색 결과 페이지는 진단 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [617페이지의 "진단 검색 페이지 필드"](#)를 참조하십시오. 다음 표는 진단 검색 결과 페이지에서 사용 가능한 옵션을 설명합니다.

옵션	설명/작업
이 검색 수정 링크	진단 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
확인란	<p>왼쪽의 확인란을 통해 NA 데이터베이스에서 진단을 선택할 수 있습니다. 진단을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음 중 하나를 클릭합니다.</p> <ul style="list-style-type: none"> •비교 — 같은 유형의 진단 두 개를 비교할 수 있는 진단 유형 비교 페이지를 엽니다. •삭제 — NA 데이터베이스에서 선택한 구성을 삭제합니다. <p>인접한 선택 드롭다운 메뉴를 통해 모든 진단을 선택하거나 선택 취소할 수 있습니다.</p>
작업	<p>진단 검색 결과 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> •세부사항 보기 — 진단 세부사항을 볼 수 있습니다. •이전과 비교 — 이 진단을 이전 진단과 비교합니다.

옵션	설명/작업
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none">• 새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다.• 기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다.• 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오.• 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오.• 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

작업 검색

작업 검색을 사용하면 NA 데이터베이스에서 네트워크에 예약된 작업을 검색할 수 있습니다.

작업을 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 작업을 클릭합니다. 작업 검색 페이지가 열립니다. 검색 버튼을 클릭하면 NA는 작업 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 작업 목록을 반환합니다. 자세한 내용은 [628페이지](#)의 "작업 검색 결과 페이지 필드"를 참조하십시오.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

작업 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 작업 검색 결과 페이지를 사용자 지정합니다.
작업 이름	연산자를 선택하고 작업 이름을 입력합니다. 연산자는 다음과 같습니다. <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음
호스트 이름	연산자를 선택하고 장치의 호스트 이름을 입력합니다. 와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)
장치 IP	연산자를 선택하고 작업과 관련된 장치의 IP 주소를 입력합니다.
예약자	연산자를 선택하고 작업을 예약한 사용자의 이름을 입력합니다.

필드	설명/작업
예약 날짜	<p>다음 연산자를 선택합니다.</p> <ul style="list-style-type: none"> •이래 또는 다음까지 •항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>
작업 상태	<p>스크롤 다운 목록에서 하나 이상의 상태를 선택합니다. 항목을 둘 이상 선택하려면 Ctrl을 누른 상태에서 클릭합니다. 사용 가능한 상태는 다음과 같습니다.</p> <ul style="list-style-type: none"> •보류 중 •성공함 •실패함 •실행 •일시 중지 •드래프트 •대기 중 •중복 •건너뛴 •경고 •요청됨 •템플릿
작업 우선 순위	<p>작업 우선 순위를 입력합니다. 작업 예약에 대한 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.</p>

필드	설명/작업
작업 유형	<p>검색할 작업 유형을 선택합니다. 여러 작업 유형을 선택하거나 선택 취소하려면 Ctrl을 누른 상태로 클릭합니다. 작업 유형은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 장치 소프트웨어 백업 • 정책 준수 확인 • Syslog 구성 • 데이터 정리 • 중복 방지 • ACL 삭제 • 구성 배포 • 암호 배포 • 원격 에이전트 배포 • 장치 컨텍스트 • 장치 컨텍스트 제거 • 네트워크 장치 감지 • 드라이버 검색 • Cisco.com에서 이미지 다운로드 • 전자 메일 보고서 • 요약 보고서 생성 • 가져오기 • IOS XR 소프트웨어 • 멀티 태스킹 프로젝트 • OS 분석 • 장치 프로비전 • 장치 재부팅 • FQDN 확인 • 명령 스크립트 실행

필드	설명/작업
작업 유형(계속)	<ul style="list-style-type: none"> • 진단 실행 • 외부 응용 프로그램 실행 • ICMP 테스트 실행 • 시작 및 실행 동기화 • 스냅샷 작성 • 장치 소프트웨어 업데이트 • VLAN 작업
실패 유형	<p>스크롤 다운 목록에서 하나 이상의 실패 유형을 선택합니다. 항목을 둘 이상 선택하려면 Ctrl을 누른 상태에서 클릭합니다. 사용 가능한 실패 유형은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 접근할 수 없는 장치 • 잘못된 암호 • 권한 없음 • 암호 없음 • 인식되지 않는 장치 • 지원되지 않는 장치
주석	<p>연산자(다음은 포함 또는 다음을 포함하지 않음)를 선택하고 작업에 대해 고유한 주석 부분을 입력합니다.</p>
결과	<p>연산자(다음은 포함 또는 다음을 포함하지 않음)를 선택하고 검색 중인 작업 결과의 고유한 텍스트를 입력합니다.</p> <p>작업 검색 결과 페이지에 작업 정보를 표시하려면 검색 결과에 이 열 포함 상자를 선택합니다. 검색 연산자가 "다음은 포함"이면 페이지 아래쪽에 있는 <#>개의 컨텍스트 라인 상자에 값을 제공할 수 있습니다. 검색 텍스트의 위아래로 최대 5개 라인까지 포함할 수 있습니다. (참고: 이 기능을 사용할 경우 로드할 결과 수가 많으면 성능이 상당히 느려질 수 있습니다.)</p>

필드	설명/작업
날짜별 승인	<p>다음 연산자를 선택합니다.</p> <ul style="list-style-type: none"> • 아래/다음까지 • 항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>
승인 상태	<p>스크롤 다운 목록에서 하나 이상의 승인 상태를 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 승인됨 • 드래프트 • 해당 안 됨 • 승인 안 됨 • 오버라이드됨 • 승인 대기 중
장치 유형	<p>스크롤 다운 메뉴에서 라우터, 스위치, 방화벽, VPN, DialUp, DSL_ISDN 또는 로드 밸런서 등의 네트워크 장치 유형을 선택합니다.</p>
하위 작업 제외	<p>선택하면 하위 작업이 검색에서 제외됩니다.</p>
사용자 지정 데이터	<p>연산자를 선택하고 나열된 사용자 지정 필드에 나타날 수 있는 고유한 텍스트를 입력합니다. (참고: 이 섹션은 사용자 지정 필드가 없는 경우에는 표시되지 않습니다.)</p>
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> • 선택한 그룹 중 하나(기본값) • 선택한 그룹 모두 • 선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>

필드	설명/작업
파티션	검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션" 을 참조하십시오.)

작업 검색 결과 페이지 필드

작업 검색 결과 페이지는 작업 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [622페이지의 "작업 검색 페이지 필드"](#)를 참조하십시오. 다음 표는 작업 검색 결과 페이지에서 사용 가능한 옵션을 설명합니다.

옵션	설명/작업
이 검색 수정 링크	작업 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
확인란	<p>왼쪽의 확인란을 통해 작업 검색 결과 표에서 작업을 삭제할 수 있습니다. 작업을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음 중 하나를 클릭합니다.</p> <ul style="list-style-type: none"> •삭제 — 선택한 작업을 삭제합니다. <p>인접한 선택 드롭다운 메뉴를 통해 모든 작업을 선택하거나 선택 취소할 수 있습니다.</p>
작업	<p>작업 검색 결과 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> •편집 — 반복되거나 아직 발생하지 않은 작업을 편집하거나 다시 실행할 수 있는 작업 편집 페이지를 엽니다. 이 링크는 작업을 편집할 수 있을 때에만 나타납니다. •삭제 — 작업을 삭제합니다. 이 링크는 작업이 아직 실행되지 않은 경우에만 나타납니다. •일시 중지 — 작업을 일시 중지합니다. 이 링크는 작업이 아직 실행되지 않은 경우에만 나타납니다. •지금 실행 — 작업을 실행합니다. 이 링크는 작업이 아직 실행되지 않은 경우에만 나타납니다. •다시 실행 — 작업을 재실행할 수 있는 작업 재실행 페이지가 열립니다. •세부사항 — 작업 세부사항을 볼 수 있는 작업 정보 페이지가 열립니다. •취소 — 작업을 취소합니다.

옵션	설명/작업
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> • 새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다. • 기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다. • 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. • 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. • 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다. (참고: 결과 옵션을 선택했으며 작업 검색 페이지에서 검색 기준을 정의할 때 찾으려는 작업 결과를 입력한 경우 결과 세부사항 포함 옵션을 선택합니다. 결과 세부사항 포함 옵션을 선택하지 않을 경우 작업 결과가 CSV 파일 안에 포함되지 않습니다.)

세션 검색

NA의 스크립트 실행 및 관리 기능은 여러 장치를 동시에 변경할 때 특히 많은 장점을 제공합니다. 그러나 작은 스크립트 실행이나 명령 스크립트 작성 등은 어려울 수도 있습니다. 따라서 NA의 ScriptMaster를 사용하면 NA가 텔넷/SSH 프록시를 통해 기록된 텔넷이나 SSH 세션을 기반으로 하는 스크립트를 자동으로 생성할 수 있습니다.

세션 검색을 사용하여 텔넷/SSH 프록시 세션을 찾을 수 있습니다. 또한 결과를 해석하기 위한 컨텍스트를 제공하기 위해 일치하는 세션 데이터 전후에 나타나는 세션 데이터를 포함하도록 세션 검색 결과 페이지를 구성할 수 있습니다.

NA가 명령만 저장할지 또는 전체 텔넷/SSH 명령을 저장할지 여부를 결정하는 관리 설정이 있음을 유의하십시오. [86페이지의 "텔넷/SSH 페이지 필드"](#)를 참조하십시오.

세션을 검색하려면 보고서 아래의 메뉴 모음에서 검색 대상을 선택하고 텔넷/SSH 세션을 클릭합니다. 세션 검색 페이지가 열립니다. 검색 기준 입력을 완료한 후 검색 버튼을 클릭하면 NA는 세션 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 텔넷/SSH 세션 목록을 반환합니다. 자세한 내용은 [634페이지의 "세션 검색 결과 페이지 필드"](#)를 참조하십시오.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

세션 검색 페이지 필드

필드	설명/작업
호스트 이름	<p>연산자를 선택하고 세션과 연관된 장치의 호스트 이름을 입력합니다. 연산자는 다음과 같습니다.</p> <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 IP	연산자를 선택하고 세션과 연관된 장치의 IP 주소를 입력합니다.
장치 상태	<p>장치에 대해 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 활성화 • 비활성 • 사전 프로덕션(사전 프로덕션 장치는 프로덕션 네트워크에서 아직 활성화되지 않은 장치입니다. 자세한 내용은 153페이지의 "Bare Metal 프로비전"을 참조하십시오.)
생성자	연산자를 선택하고 세션을 생성한 사용자의 로그인 이름을 입력합니다.
시작 날짜	<p>다음 연산자를 선택합니다.</p> <ul style="list-style-type: none"> • 이래/다음까지 • 항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>

필드	설명/작업
종료 날짜	<p>다음 연산자를 선택합니다.</p> <ul style="list-style-type: none"> •이래/다음까지 •항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>
상태	<p>다음 상태 옵션 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none"> •실패함 •열기 •종료됨
세션 유형	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •모두 •텔넷 •SSH
세션 데이터	<p>연산자(다음을 포함 또는 다음을 포함하지 않음)를 선택하고 찾고 싶은 세션의 고유한 일부를 입력합니다.</p> <p>검색 연산자가 "다음을 포함"이면 페이지 아래쪽에 있는 <#>개의 컨텍스트 라인 상자에 값을 제공할 수 있습니다. 결과에 검색 텍스트의 위아래로 최대 5개 라인까지 포함할 수 있습니다. (참고: 이 기능을 사용할 경우 로드할 결과 수가 많으면 성능이 상당히 느려질 수 있습니다.)</p>
세션 사용자 지정 데이터	<p>연산자를 선택하고 나열된 사용자 지정 필드에 나타날 수 있는 고유한 텍스트를 입력합니다. (참고: 이 섹션은 사용자 지정 필드가 없는 경우에는 표시되지 않습니다.)</p>

필드	설명/작업
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> • 선택한 그룹 중 하나(기본값) • 선택한 그룹 모두 • 선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

세션 검색 결과 페이지 필드

세션 검색 결과 페이지는 세션 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [631페이지의 "세션 검색 페이지 필드"](#)를 참조하십시오. 다음 표는 세션 검색 결과 페이지에서 사용 가능한 옵션을 설명합니다.

옵션	설명/작업
이 검색 수정 링크	세션 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
작업	<p>세션 검색 결과 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> •호스트 이름 — 장치와 해당 구성 이력에 대한 기본 정보를 볼 수 있는 장치 정보 페이지를 엽니다. •장치 IP — 장치와 해당 구성 이력에 대한 기본 정보를 볼 수 있는 장치 정보 페이지를 엽니다. •전체 텔넷/SSH 세션 보기 — 해당 세션의 명령 및 시스템 응답을 볼 수 있는 텔넷/SSH 세션 페이지를 엽니다. 이 페이지에는 현재 세션 중에 명령 실행에서 스크립트를 간단하게 작성할 수 있는 스크립트로 변환 링크가 포함됩니다. 자세한 내용은 720페이지의 "명령 스크립트 추가"를 참조하십시오. 이 세션에 의해 생성된 구성(있는 경우)에 대한 링크도 있습니다. •명령만 보기 — 해당 세션의 명령만 볼 수 있는 텔넷/SSH 세션 페이지를 엽니다. 이 페이지에는 현재 세션 중에 명령 실행에서 스크립트를 간단하게 작성할 수 있는 스크립트로 변환 링크가 포함됩니다. 이 세션에 의해 생성된 구성(있는 경우)에 대한 링크도 있습니다.

옵션	설명/작업
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> • 새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다. • 기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다. • 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. • 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. • 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다. (참고: 세션 데이터 옵션을 선택했으며 세션 검색 페이지에서 검색 기준을 정의할 때 찾으려는 세션 데이터를 입력한 경우 결과 세부 사항 포함 옵션을 선택합니다. 결과 세부사항 포함 옵션을 선택하지 않을 경우 세션 데이터가 CSV 파일 안에 포함되지 않습니다.)

이벤트 검색

장치 액세스 실패와 같은 시스템 및 사용자 이벤트를 검색할 수 있습니다. NA 이벤트에 대한 설명은 [640페이지의 "이벤트 설명"](#)을 참조하십시오.

이벤트를 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 이벤트를 클릭합니다. 이벤트 검색 페이지가 열립니다. 검색 기준 입력을 완료한 후 검색 버튼을 클릭하면 NA는 이벤트 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 이벤트 목록을 반환합니다. 자세한 내용은 [639페이지의 "이벤트 검색 결과 페이지 필드"](#)를 참조하십시오.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

이벤트 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 이벤트 검색 결과 페이지를 사용자 지정합니다.
날짜	다음 연산자를 선택합니다. <ul style="list-style-type: none"> •이래/다음까지 •항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.
요약	하나 이상의 이벤트 이름을 선택합니다. 추가로 이벤트를 선택/선택 취소하려면 Ctrl을 누릅니다. 각 이벤트에 대한 자세한 내용은 640페이지의 "이벤트 설명" 을 참조하십시오.
추가한 사람	연산자를 선택하고 이벤트를 만든 사용자의 로그인 이름을 제공합니다.

필드	설명/작업
중요도	<p>다음 옵션 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none"> • 정보용 — 일반적으로 응답이 필요하지 않은 이벤트 • 낮음 — 시간이 허용될 경우 응답이 필요할 수 있는 이벤트 • 중간 — 일반적으로 72시간 이내에 시기 적절한 응답이 필요한 이벤트 • 높음 — 일반적으로 24시간 이내에 신속한 응답이 필요한 이벤트 • 심각 — 즉각적인 응답이 필요한 이벤트
호스트 이름	<p>연산자를 선택하고 이러한 이벤트와 연관된 장치의 호스트 이름을 입력합니다. 연산자는 다음과 같습니다.</p> <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 IP	<p>연산자를 선택하고 이러한 이벤트와 연관된 장치의 IP 주소를 입력합니다.</p>
설명	<p>연산자(다음을 포함 또는 다음을 포함하지 않음)를 선택하고 검색 중인 이벤트의 고유한 텍스트를 입력합니다. 결과 페이지에 텍스트를 표시하려면 결과에 검색 텍스트의 위아래로 최대 5개 라인까지 포함할 수 있습니다. (참고: 이 기능을 사용할 경우 로드할 결과 수가 많으면 성능이 상당히 느려질 수 있습니다.)</p>

필드	설명/작업
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none">• 선택한 그룹 중 하나(기본값)• 선택한 그룹 모두• 선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

이벤트 검색 결과 페이지 필드

이벤트 검색 결과 페이지는 이벤트 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [636페이지의 "이벤트 검색 페이지 필드"](#)를 참조하십시오. 다음 표는 이벤트 검색 결과 페이지에서 사용 가능한 옵션을 설명합니다.

필드	설명/작업
이 검색 수정 링크	이벤트 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
확인란	<p>각 이벤트의 확인란을 사용하면 이벤트를 삭제할 수 있습니다. 이벤트를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음 중 하나를 클릭합니다.</p> <ul style="list-style-type: none"> •삭제 — 선택한 이벤트를 삭제합니다. <p>인접한 선택 드롭다운 메뉴를 통해 모든 작업을 선택하거나 선택 취소할 수 있습니다.</p>
작업	<p>이벤트 검색 결과 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> •요약 — 이 이벤트의 자세한 결과를 볼 수 있는 이벤트 세부사항 페이지를 엽니다. •호스트 이름 — 장치와 해당 구성 이력에 대한 기본 정보를 볼 수 있는 장치 세부사항 페이지를 엽니다.

필드	설명/작업
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> • 새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다. • 기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다. • 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. • 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. • 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다. (참고: 설명 옵션을 선택했으며 이벤트 검색 페이지에서 검색 기준을 정의할 때 찾으려는 이벤트 설명 텍스트를 입력한 경우 결과 세부사항 포함 옵션을 선택합니다. 결과 세부사항 포함 옵션을 선택하지 않을 경우 이벤트 설명 텍스트가 CSV 파일 안에 포함되지 않습니다.

이벤트 설명

다음 표에서는 NA 이벤트에 대해 설명합니다. 이벤트는 알파벳 순서로 나열되어 있습니다.

이벤트	설명
승인 거부됨	사용자가 승인 요청을 거부했습니다.
승인 허가됨	사용자가 작업을 승인했습니다.
더 이상 승인이 필요하지 않음	작업 승인이 더 이상 필요하지 않습니다.
승인 오버라이드	승인 없이 작업을 실행할 수 있도록 사용자가 작업의 승인을 오버라이드했습니다.

이벤트	설명
승인 요청	사용자가 실행 전에 승인이 필요한 작업을 작성했습니다.
승인 작업 변경됨	사용자가 실행 전에 승인이 필요한 작업을 변경했습니다.
승인 작업 삭제됨	사용자가 승인을 위해 표시된 작업을 삭제했습니다.
승인 작업 시간 초과	할당된 시간에 작업이 승인되지 않았습니다.
명령 인증 오류	사용이 인증되지 않은 사용자가 명령을 실행하려고 시도했습니다.
명령 스크립트 실행	명령 스크립트가 수정되었습니다.
동시 텔넷/SSH 세션 오버라이드	사용자가 동시 로그인에 대한 제한을 무시했습니다. 이 사용자는 다른 사용자가 이미 로그인했음에도 불구하고 프록시를 통해 장치에 로그인했습니다.
장치 액세스 실패	NA가 장치에 액세스할 수 없습니다. 암호가 잘못되었거나 호스트에 대한 경로가 없기 때문일 수 있습니다.
장치 추가됨	사용자가 장치를 추가했습니다.
장치 부팅됨	장치가 재부팅되었습니다.
장치 명령 스크립트 완료됨	장치 명령 스크립트 실행에 성공했습니다.
장치 명령 스크립트 실패	장치 명령 스크립트 실행에 실패했습니다.
장치 컨텍스트 추가	장치 컨텍스트가 추가되었습니다.
장치 컨텍스트 추가 실패	장치 컨텍스트가 추가되지 않았습니다.
장치 컨텍스트 제거됨	장치 컨텍스트가 제거되었습니다.
장치 컨텍스트 제거 실패	장치 컨텍스트를 제거하지 못했습니다.
장치 구성 변경	스냅샷 작업이 실행되는 동안 NA가 구성 변경을 감지했습니다.
장치 구성 변경 - 사용자 없음	NA가 알 수 없는 사용자에 의한 구성 변경을 감지했습니다.
장치 구성 배포	NA가 장치에 구성을 성공적으로 배포했습니다.

이벤트	설명
장치 구성 배포 실패	NA가 장치에 구성을 배포하는 데 실패했습니다.
장치 데이터 실패	NA가 구성 또는 진단 출력을 데이터베이스에 저장하는 데 실패했습니다.
장치 삭제됨	사용자가 장치를 영구적으로 제거했습니다.
장치 진단 변경됨	진단 결과가 이전 결과와 다릅니다.
장치 진단 완료됨	장치 진단에 성공했습니다.
장치 진단 실패	장치 진단에 실패했습니다.
장치 편집됨	사용자가 장치의 정보를 수정했습니다.
실행 중인 장치 플래시 저장 공간이 적음	장치의 플래시 저장 공간이 얼마 남지 않았습니다.
장치 그룹 추가됨	사용자가 그룹을 추가했습니다.
장치 그룹 삭제됨	사용자가 그룹을 삭제했습니다.
장치 그룹 수정됨	사용자가 장치 그룹을 수정했습니다.
장치 액세스 불가능	장치에 액세스할 수 없습니다.
장치 관리됨	사용자가 장치를 "활성"으로 표시했습니다.
가져오기에서 누락된 장치	가져오기 작업이 주기적으로 실행되고 가져오기 작업에 가져올 장치 파일이 제공되었을 때, 마지막으로 가져오기가 발생한 시기에는 파일에 장치가 포함되었지만 현재 가져오기 중에는 포함되지 않은 경우 이 이벤트가 발생합니다.
장치 암호 변경	사용자가 암호 변경을 배포했습니다.
장치 암호 변경 실패	NA가 장치 암호 변경에 실패했습니다.
장치 권한 - 수정됨	장치가 그룹에 추가되거나 그룹에서 제거되어, 사용자의 장치 수정 권한 등의 권한이 변경되었습니다.
장치 권한 - 새 장치	장치 그룹에 새 장치가 추가되어, 해당 장치 그룹과 연관된 사용자 권한이 변경되었습니다.

이벤트	설명
장치 포트 이중 불일치 감지됨	장치 포트 이중 불일치가 감지되었습니다.
장치 프로비전 실패	장치가 프로비전되지 않았습니다.
장치 프로비전 성공	장치가 프로비전되었습니다.
장치 관계 추가됨	장치 관계가 추가되었습니다.
장치 관계 삭제됨	장치 관계가 삭제되었습니다.
장치 관계 수정됨	장치 관계가 수정되었습니다.
다시 로드된 장치	장치가 다시 로드되었습니다.
장치 다시 로드 실패	장치 다시 로드 실패했습니다.
장치 예약 충돌	장치 예약 충돌이 있었습니다.
장치 스냅샷	NA가 구성 변경을 위해 장치를 확인했습니다.
장치 소프트웨어 변경	NA가 장치에서 새 OS 버전을 감지했습니다(예: IOS 11에서 IOS 12로).
장치 시작/실행 구성 차이	NA가 시작 구성과 실행 구성 간의 차이점을 감지했습니다.
장치 템플릿 추가됨	장치 템플릿이 추가되었습니다.
장치 템플릿 삭제됨	장치 템플릿이 삭제되었습니다.
장치 템플릿 편집됨	장치 템플릿이 편집되었습니다.
장치 관리되지 않음	사용자가 장치를 "비활성"으로 표시했습니다. 특정 기간 동안 접근할 수 없는 경우 가져온 장치도 "비활성"이 될 수 있습니다.
진단 수정됨	사용자가 진단을 수정했습니다.
분산 시스템 - 손상된 복제 작업	NA가 손상된 복제 작업을 감지했습니다.
분산 시스템 - 데이터 동기화 지연 경고	NA가 데이터 동기화 지연 경고를 감지했습니다.
분산 시스템 - 지연된 LOB 임계값 초과	NA에서 임계값이 초과된 지연된 LOB를 감지했습니다.

이벤트	설명
분산 시스템 - 지연된 트랜잭션 임계값 초과	NA에서 임계값이 초과된 지연된 트랜잭션을 감지했습니다.
분산 시스템 - 장치 소프트웨어 전송 오류	NA가 장치 소프트웨어 전송 오류를 감지했습니다.
분산 시스템 - 수정된 복제 작업	NA가 수정된 복제 작업을 감지했습니다.
분산 시스템 - 복제 오류	NA가 복제 오류를 감지했습니다.
분산 시스템 - RMI 오류	NA가 RMI 오류를 감지했습니다.
분산 시스템 - 중지된 병합 에이전트 작업	NA가 중지된 병합 에이전트 작업을 감지했습니다.
분산 시스템 - 시간 동기화 경고	NA가 시간 동기화 경고를 감지했습니다.
분산 시스템 - 삭제할 수 없는 예외 생성	NA가 삭제할 수 없는 예외 생성을 감지했습니다.
분산 시스템 - 고유성 충돌	NA가 고유성 충돌을 감지했습니다.
드라이버 검색 실패	NA가 실패한 드라이버 검색을 감지했습니다.
드라이버 검색 성공	NA가 성공한 드라이버 검색을 감지했습니다.
드라이버 로드 오류	NA가 드라이버 로드 오류를 감지했습니다.
중복 장치 감지됨	NA가 중복 장치를 감지했습니다.
동적 그룹 업데이트 오류	NA가 장치 그룹 업데이트 오류를 감지했습니다.
전자 메일 보고서 저장됨	사용자가 전자 메일 보고서를 저장했습니다.
외부 디렉터리 서버 인증 오류	NA가 외부 LDAP 인증 서버에 연결할 수 없습니다.
마지막으로 사용한 장치 암호 변경됨	장치 액세스를 위해 마지막으로 사용된 암호가 변경되었습니다.
라이센스가 거의 초과됨	장치가 총 라이센스 노드 수의 90%를 초과합니다.

이벤트	설명
라이센스가 거의 만료됨	NA 라이센스가 곧 만료됩니다(날짜 기반 라이센스 전용).
라이센스가 초과됨	장치가 총 라이센스 노드 수를 초과합니다. NA는 20%의 초과를 허용합니다.
라이센스가 만료됨	라이센스가 만료되었습니다. NA가 더 이상 로그인을 허용하지 않지만 예정된 스냅샷 및 레코드 변경은 계속 진행됩니다.
모듈 추가됨	장치에 모듈/블레이드/카드가 추가되었습니다.
모듈 변경됨	장치에 설치된 모듈/블레이드/카드의 속성이 변경되었습니다.
모듈 제거됨	장치에서 모듈/블레이드/카드가 제거되었습니다.
모니터 오류	서버 모니터가 실행에 실패했습니다.
모니터 정상	서버 모니터가 성공적으로 실행되었습니다.
보류 중 작업 삭제됨	사용자가 예정된 작업을 실행 전에 삭제했습니다.
정책 추가됨	사용자가 새 구성 정책을 추가했습니다.
정책 변경됨	사용자가 구성 정책을 변경했습니다.
정책 비준수	구성 변경이 정책 규칙을 위반했습니다.
정책 패턴 시간 초과	정책 패턴 일치에 30초 이상이 걸렸습니다.
정책 규칙 추가됨	사용자가 새 구성 규칙을 추가했습니다.
정책 규칙 변경됨	사용자가 구성 규칙을 변경했습니다.
예약된 장치 구성이 변경됨	사용자가 예약된 장치에서 장치 구성을 변경했습니다.
구성 배포를 위한 예정 편집됨	배포하기로 예정된 구성을 사용자가 수정했습니다.

이벤트	설명
구성 배포를 위한 예정 수정됨	새 암호가 배포되었는데, 또 다른 암호 배포 작업이 예정되었습니다. 이는 방금 배포된 새 암호가 다시 변경될 것임을 나타냅니다(보류 중인 암호 배포 작업이 실행될 때).
보안 주의	NA가 보안 주의를 감지했습니다.
서버 시작	NA 관리 엔진이 시작되었습니다.
세션 데이터 캡처됨	프록시가 데이터베이스에 연결 세션을 저장했습니다.
소프트웨어 업데이트 실패함	NA가 장치에서 OS 소프트웨어 업데이트에 실패했습니다.
소프트웨어 업데이트 성공함	NA가 장치에서 OS 소프트웨어를 성공적으로 업데이트했습니다.
소프트웨어 취약점이 감지됨	소프트웨어 수준을 "보안 위험"으로 설정한 경우 NA가 장치를 스냅샷하고 "보안 위험"으로 태그가 지정된 OS 버전을 감지하면 이 이벤트가 생성됩니다.
요약 보고서 생성됨	사용자가 요약 보고서를 생성했습니다.
작업 완료됨	작업이 완료되었습니다.
작업 시작됨	작업이 시작되었습니다.
티켓 생성됨	HP Remedy AR System Connector(또는 타사 티켓팅 시스템과 인터랙션하는 HP Connector 중 하나)를 사용할 경우 이 이벤트는 NA가 타사 티켓팅 시스템에서 티켓을 생성했음을 나타냅니다.
사용자 추가됨	사용자가 추가되었습니다.
사용자 인증 오류	사용자가 NA에 로그인할 때 잘못된 암호를 입력했습니다.
사용자 인증 오류 잠금	연속적으로 실패한 로그인 시도가 너무 많아서 사용자가 잠겼습니다.
사용자 삭제됨	사용자가 삭제되었습니다.
사용자 사용 안 함	사용자 레코드가 편집되어 사용자의 상태가 활성화됨에서 비활성화됨으로 변경됩니다.

이벤트	설명
사용자 사용	사용자 레코드가 편집되어 사용자의 상태가 사용 안 함에서 사용함으로 변경됩니다.
사용자 로그인	사용자가 NA에 로그인했습니다.
사용자 로그아웃	사용자가 NA에서 로그아웃했습니다.
사용자 메시지	사용자가 새 메시지 링크를 클릭하여 메시지를 생성했습니다.
사용자 권한 변경됨	사용자의 권한이 변경되었습니다.

사용자 검색

사용자 검색 페이지를 사용하여 이름, 성, 전자 메일 주소 및/또는 AAA 사용자 이름으로 사용자를 검색할 수 있습니다. 사용자를 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 사용자를 클릭합니다. 사용자 검색 페이지가 열립니다.

검색 버튼을 클릭하면 NA는 사용자 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 이벤트 목록을 반환합니다. 자세한 내용은 [650페이지의 "사용자 검색 결과 페이지"](#)를 참조하십시오.

사용자 검색 페이지

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 사용자 검색 결과 페이지를 사용자 지정합니다.
이름	연산자를 선택하고 사용자의 이름을 입력합니다. 연산자는 다음과 같습니다. <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음
성	연산자를 선택하고 사용자의 성을 입력합니다.
사용자 이름	연산자를 선택하고 사용자의 사용자 이름을 입력합니다. 와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)
전자 메일 주소	연산자를 선택하고 사용자의 전자 메일 주소를 입력합니다.
AAA 사용자 이름	연산자를 선택하고 사용자의 AAA 사용자 이름을 입력합니다.
주석	연산자(다음을 포함 또는 다음을 포함하지 않음)를 선택한 다음 찾으려는 주석 텍스트를 입력합니다.

필드	설명/작업
사용자 그룹 구성원	사용자가 구성원인 사용자 그룹을 선택합니다.
사용자 사용자 지정 데이터	연산자를 선택하고 사용자 지정 서비스 데이터를 입력합니다.
파티션	검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션" 을 참조하십시오.)

사용자 검색 결과 페이지

사용자 검색 결과 페이지는 사용자 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [648페이지의 "사용자 검색 페이지"](#)를 참조하십시오.

필드	설명/작업
이 검색 수정 링크	이벤트 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
작업	<p>작업 검색 결과 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 편집 — 사용자의 프로필을 편집할 수 있는 내 프로필 페이지를 엽니다. 자세한 내용은 339페이지의 "내 프로필 페이지 필드"를 참조하십시오. • 삭제 — 적절한 권한이 있는 경우 사용자를 삭제할 수 있습니다. 그렇지 않은 경우에는 옵션이 회색으로 처리됩니다. • 권한 — 사용자의 권한을 편집할 수 있는 내 권한 페이지를 엽니다. 자세한 내용은 343페이지의 "내 권한 페이지 필드"를 참조하십시오. • 구성 변경 사항 — 사용자가 수행한 구성 변경 사항을 볼 수 있는 구성 검색 결과를 엽니다.
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> • 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. • 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. • 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

ACL 검색

ACL(액세스 제어 목록)은 대부분의 장치에서 구성의 일부입니다. 라우팅된 패킷이 라우터의 인터페이스에서 승인되었거나 차단되었는지 여부를 제어하여 네트워크 트래픽을 필터링합니다. 일반적으로 ACL은 명령문 모음입니다. 각 명령문은 IP 패킷에서 볼 수 있는 패턴을 정의합니다. ACL은 종종 라우팅 업데이트 내용을 제어하고 네트워크 보안을 제공하는 데 사용됩니다.

NA는 장치에서 구성 정보를 검색하고 구성에서 ACL 명령문을 추출합니다. 그런 후 NA는 구성과는 별도로 ACL을 저장합니다. 따라서 다음을 수행할 수 있습니다.

- 장치에서 현재 ACL을 보고 이를 이전 ACL과 비교합니다.
- ACL에 주석을 추가합니다.
- ACL을 수정/작성하고 이를 다시 장치에 배포합니다.

ACL 수정 및/또는 작성에 대한 자세한 내용은 [879페이지의 "ACL 생성"](#)을 참조하십시오.

ACL을 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 ACL을 클릭합니다. ACL 검색 페이지가 열립니다.

ACL 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 ACL 검색 결과 페이지를 사용자 지정합니다.
호스트 이름	<p>연산자를 선택하고 세션과 연관된 장치의 호스트 이름을 입력합니다. 연산자는 다음과 같습니다.</p> <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 IP	연산자를 선택하고 장치의 IP 주소를 입력합니다.
ACL ID	연산자를 선택하고 ACL의 ID를 입력합니다. ACL ID는 장치 ACL 목록을 기반으로 한 번호 또는 이름이며 ACL 핸들은 사용자가 지정한 설명 이름 또는 값입니다. 기본적으로 ACL ID 및 ACL 핸들은 사용자가 ACL 핸들을 정의하기 전까지는 동일합니다.
ACL 핸들	연산자를 선택하고 ACL 핸들을 입력합니다. ACL 핸들은 사용자가 지정한 설명 이름 또는 값입니다. 기본적으로 ACL ID 및 ACL 핸들은 사용자가 ACL 핸들을 정의하기 전까지는 동일합니다.
ACL 유형	연산자를 선택하고 ACL 유형(예: "extended")을 입력합니다. ACL 유형은 드라이버에 따라 달라집니다.

필드	설명/작업
ACL 구성	<p>연산자(다음을 포함 또는 다음을 포함하지 않음)를 선택하고 ACL을 정의하는 구성 명령을 입력합니다.</p> <p>검색 연산자가 "다음 포함"이면 페이지 아래쪽에 있는 <#>개의 컨텍스트 라인 상자에 값을 제공할 수 있습니다. 결과에 검색 텍스트의 위아래로 최대 5개 라인까지 포함할 수 있습니다. (참고: 이 기능을 사용할 경우 로드할 결과 수가 많으면 성능이 상당히 느려질 수 있습니다.)</p>
ACL 응용 프로그램	연산자(다음 포함 또는 다음 포함하지 않음)를 선택하고 ACL을 사용하는 엔티티를 입력합니다. 예를 들어, ACL이 인터페이스에 적용된 경우에는 인터페이스는 ACL의 응용 프로그램입니다.
검색 범위	선택된 경우 검색 결과는 현재 모든 장치에 구성된 ACL로 제한됩니다. 선택되지 않은 경우에는 검색 결과에는 현재 및 기록 ACL 모두가 포함됩니다.
주석	연산자(다음 포함 또는 다음 포함하지 않음)를 선택하고 ACL 주석을 입력합니다.
변경한 사람	연산자를 선택하고 ACL을 마지막으로 변경한 사용자의 이름을 입력합니다.
마지막 수정일	<p>다음 연산자를 선택합니다.</p> <ul style="list-style-type: none"> •이래 또는 다음까지 •항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> •선택한 그룹 중 하나(기본값) •선택한 그룹 모두 •선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>

필드	설명/작업
파티션	검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션" 을 참조하십시오.)

검색 버튼을 클릭하면 NA는 ACL 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 ACL 목록을 반환합니다. 자세한 내용은 [655페이지의 "ACL 검색 결과 페이지 필드"](#)를 참조하십시오.

ACL 검색 결과 페이지 필드

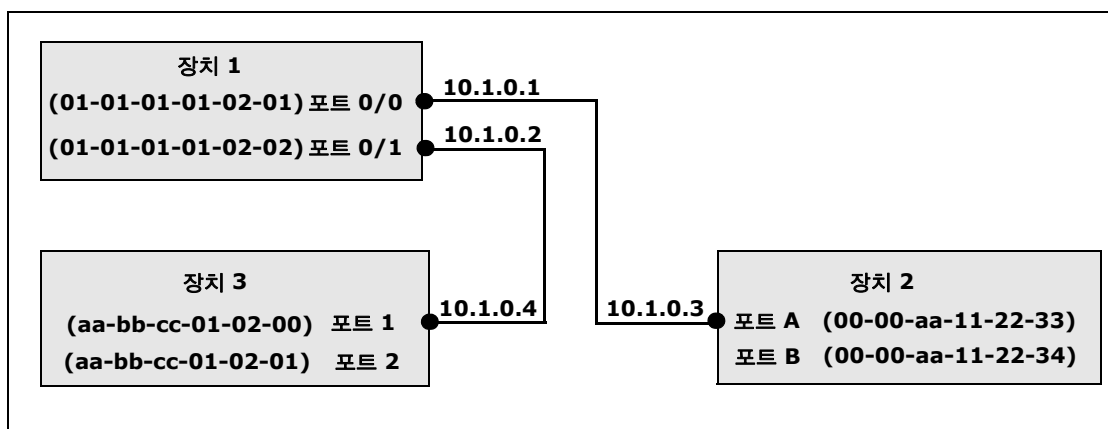
ACL 검색 결과 페이지는 ACL 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [652페이지의 "ACL 검색 페이지 필드"](#)를 참조하십시오. 다음 표는 ACL 검색 결과 페이지에서 사용 가능한 옵션을 설명합니다.

옵션	설명/작업
이 검색 수정 링크	ACL 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
확인란	<p>각 ACL의 확인란을 사용하면 2개의 ACL을 비교할 수 있습니다. ACL을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 비교 — 두 개의 ACL을 비교할 수 있는 ACL 비교 페이지를 엽니다. 차이 점은 쉽게 비교할 수 있게 서로 다른 색상으로 강조 표시됩니다. 컨텍스트와의 차이점을 표시하여 전체 텍스트를 표시하거나 UNIX 스타일 차이 점을 표시하는 옵션이 있습니다. <p>인접한 선택 드롭다운 메뉴를 통해 모든 ACL을 선택하거나 선택 취소할 수 있습니다.</p>
작업	<p>ACL 검색 결과 표의 각 항목에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • ACL 편집 — ACL을 편집할 수 있는 ACL 편집 페이지를 엽니다. 자세한 내용은 887페이지의 "ACL 삭제"를 참조하십시오. • ACL 보기 — ACL을 볼 수 있는 ACL 보기 페이지를 엽니다. 자세한 내용은 874페이지의 "ACL 보기"를 참조하십시오. • ACL 이력 — ACL을 편집하고 볼 수 있는 ACL 이력 페이지를 엽니다.

옵션	설명/작업
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none">• 선택한 ACL용 핸들 설정 — ACL 핸들을 입력합니다. ACL 핸들은 사용자가 지정한 설명 이름 또는 값입니다.• 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오.• 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오.• 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다. <hr/>

MAC 주소 검색

MAC 주소는 장치에서 포트를 식별하는 고유한 주소입니다. MAC 주소는 BIA(Burned-in Addresses), 하드웨어 주소 및 실제 주소로도 알려져 있습니다. NA는 장치에 지정된 MAC 주소와 이러한 포트에서 표시되는 MAC 주소에 대한 정보를 수집합니다. 다음 그림은 MAC 주소, IP 주소 및 포트 간의 관계를 설명합니다.



MAC 주소를 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 MAC 주소를 클릭합니다. MAC 주소 검색 페이지가 열립니다. 검색 기준 입력을 완료한 후 검색 버튼을 클릭하면 NA는 MAC 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 MAC 주소 목록을 반환합니다. 자세한 내용은 [660페이지의 "MAC 주소 검색 결과 페이지 필드"](#)를 참조하십시오.

MAC 주소 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 MAC 주소 검색 결과 페이지를 사용자 지정합니다.
호스트 이름	<p>연산자를 선택하고 장치의 호스트 이름을 입력합니다. 연산자는 다음과 같습니다.</p> <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 IP	연산자를 선택하고 장치의 IP 주소를 입력합니다.
포트 이름	연산자를 선택하고 장치 포트 이름을 입력합니다. 포트 이름은 장치에 있는 실제 포트의 이름입니다. 예를 들면 Ethernet0/1입니다.
포트 설명	연산자를 선택하고 포트에 대한 설명을 입력합니다.
주소	연산자를 선택하고 검색할 MAC 주소 패턴을 입력합니다.

필드	설명/작업
주소 유형	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 모든 주소(기본값) • 포트에서 표시됨 — 장치/포트에 연결되어 있는 MAC 주소(즉, 장치/포트 외부의 MAC 주소 유형이지만 장치/포트에 표시된 MAC 주소)만을 표시합니다. • 포트 주소 — 장치 내부의 MAC 주소(즉, 장치에 있는 포트에만 지정된 MAC 주소)만을 표시합니다. <p>참고: "검색을 더 이상 표시되지 않는 MAC 주소로 제한" 확인란을 사용하면 검색 결과는 최신 데이터 캡처에서 더 이상 표시되지 않는 MAC 주소로 제한할 수 있습니다.</p>
검색 범위	<p>선택하면 검색이 더 이상 표시되지 않는 MAC 주소로 제한됩니다.</p>
VLAN	<p>연산자를 선택하고 포트 VLAN 이름을 입력합니다. VLAN 이름은 검색을 제한할 VLAN2 또는 VLAN3 등 VLAN의 이름입니다.</p>
연관된 IP	<p>연산자를 선택하고 검색하려는 MAC과 연관된 IP 주소를 입력합니다.</p>
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> • 선택한 그룹 중 하나(기본값) • 선택한 그룹 모두 • 선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

MAC 주소 검색 결과 페이지 필드

MAC 주소 검색 결과 페이지는 MAC 주소 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [658페이지의 "MAC 주소 검색 페이지 필드"](#)를 참조하십시오.

옵션	설명/작업
이 검색 수정 링크	MAC 주소 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
작업	<p>각 MAC 주소에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> 세부사항 보기 — 장치, 장치 포트, MAC 주소, 유형, 첫 번째로 표시됨, 마지막으로 업데이트됨 등의 정보에 대한 세부사항을 볼 수 있는 MAC 주소 세부사항 페이지를 엽니다. IP 보기 — 이 MAC 주소와 상호 참조된 IP 주소 세부사항 페이지를 엽니다. 이 옵션은 "포트에서 표시됨" 레코드에서만 사용할 수 있습니다. 상호 참조란 NA가 데이터를 수집할 때 IP 주소와 MAC 주소가 동일한 소스에서 오는 것으로 표시되었음을 의미합니다.
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> 새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다. 기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다. 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

IP 주소 검색

IP 주소(인터넷 프로토콜 주소)는 네트워크 장치의 고유한 숫자 주소입니다. 라우터, 스위치, 방화벽 등의 참여하는 모든 네트워크 장치에는 각자 고유한 IP 주소가 있습니다. 현재 NA는 다음을 지원합니다.

- IPv4 — IPv4는 옥텟 표기 형식의 32비트 및 64비트 주소를 지원합니다.
- IPv6 — IPv6은 옥텟 표기 형식의 128비트 주소를 지원합니다. IPv6 지원에 대한 자세한 내용은 *Network Automation 9.10 업그레이드 및 설치 설명서*를 참조하십시오.

IP 주소를 검색하려면 보고서 아래의 메뉴 모음에서 검색을 선택하고 IP 주소를 클릭합니다. IP 주소 검색 페이지가 열립니다. 검색 기준 입력을 완료한 후에는 검색 버튼을 클릭합니다. NA는 IP 주소 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 IP 주소 목록을 반환합니다.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

IP 주소 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 IP 주소 검색 결과 페이지를 사용자 지정합니다.
호스트 이름	연산자를 선택하고 세션과 연관된 장치의 호스트 이름을 입력합니다. 연산자는 다음과 같습니다. <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)

필드	설명/작업
장치 IP	연산자를 선택하고 장치의 IP 주소를 입력합니다. 예: IPv4: 10.255.?.255, 192.*, 172.16.30.1 IPv6: aff:38:?:10, fc00:c0a8:*, ::1
포트 이름	연산자를 선택하고 장치 포트 이름을 입력합니다. 포트 이름은 장치에 있는 실제 포트의 이름입니다. 예를 들면 Ethernet0/1입니다.
포트 설명	연산자를 선택하고 포트에 대한 설명을 입력합니다.
주소	연산자를 선택하고 검색할 IP 주소 패턴을 입력합니다. 예: IPv4: 10.255.?.255, 192.*, 172.16.30.1 IPv6: aff:38:?:10, fc00:c0a8:*, ::1
주소 유형	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 모든 주소(기본값) • 포트에서 표시됨 — 장치/포트에 연결되어 있는 IP 주소(즉, 장치/포트 외부의 IP 주소 유형이지만 장치/포트에 표시된 MAC 주소)만을 표시합니다. • 포트 주소 — 장치 내부의 IP 주소(즉, 장치에 있는 포트에만 지정된 IP 주소)만을 표시합니다. <p>참고: "검색을 더 이상 표시되지 않는 IP 주소로 제한" 확인란을 사용하면 검색 결과는 최신 데이터 캡처에서 더 이상 표시되지 않는 IP 주소로 제한할 수 있습니다.</p>
검색 범위	선택하면 검색이 더 이상 표시되지 않는 IP 주소로 제한됩니다.
VLAN	연산자를 선택하고 포트 VLAN 이름을 입력합니다. VLAN 이름은 검색을 제한할 VLAN2 또는 VLAN3 등 VLAN의 이름입니다.
연관된 MAC	연산자를 선택하고 연관된 MAC 주소를 입력합니다.

필드	설명/작업
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> • 선택한 그룹 중 하나(기본값) • 선택한 그룹 모두 • 선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 파티션)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

IP 주소 검색 결과 페이지 필드

IP 주소 검색 결과 페이지는 IP 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [661페이지의 "IP 주소 검색 페이지 필드"](#)를 참조하십시오.

옵션	설명/작업
이 검색 수정 링크	IP 주소 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
작업	<p>각 MAC 주소에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> 세부사항 보기 — 장치, 장치 포트, IP 주소, 유형, 첫 번째로 표시됨, 마지막으로 업데이트됨 등의 정보에 대한 세부사항을 볼 수 있는 IP 주소 세부사항 페이지를 엽니다. IP 보기 — 이 IP 주소와 상호 참조된 IP 주소 세부사항 페이지를 엽니다. 이 옵션은 "포트에서 표시됨" 레코드에서만 사용할 수 있습니다. 상호 참조란 NA가 데이터를 수집할 때 IP 주소와 MAC 주소가 동일한 소스에서 오는 것으로 표시되었음을 의미합니다.
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> 새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다. 기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다. 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

VLAN 검색

VLAN(가상 로컬 영역 네트워크)은 패킷의 단일 브로드캐스트 도메인 역할을 하는 포트를 모아놓은 집합입니다. VLAN은 계층 2(데이터 링크 계층)에서 작동합니다. NA는 장치에 정의된 VLAN과 각 포트가 지정된 VLAN에 대한 정보를 수집합니다. VLAN에 대한 자세한 내용은 [278페이지의 "VLAN\(가상 로컬 영역 네트워크\)"](#)을 참조하십시오.

VLAN을 검색하려면 보고서 아래의 메뉴 모음에서 검색 대상을 선택하고 VLAN을 클릭합니다. VLAN 검색 페이지가 열립니다. 검색 기준 입력을 완료한 후에는 검색 버튼을 클릭합니다. NA는 VLAN 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 VLAN 목록을 반환합니다.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

VLAN 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 VLAN 검색 결과 페이지를 사용자 지정합니다.
호스트 이름	연산자를 선택하고 세션과 연관된 장치의 호스트 이름을 입력합니다. 연산자는 다음과 같습니다. <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 IP	연산자를 선택하고 장치의 IP 주소를 입력합니다.

필드	설명/작업
VLAN ID	연산자를 선택하고 VLAN ID를 입력합니다. VLAN ID는 VLAN 태그의 12비트 필드를 사용하여 VLAN을 식별합니다. VLAN에 대한 자세한 내용은 278페이지의 "VLAN(가상 로컬 영역 네트워크)"을 참조하십시오.
VLAN 이름	연산자를 선택하고 VLAN 이름을 입력합니다.
VLAN 유형	연산자를 선택하고 VLAN 유형을 입력합니다.
VLAN 설명	연산자를 선택하고 VLAN 설명을 입력합니다.
사설 VLAN	연산자를 선택하고 사설 VLAN 설명을 입력합니다.
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> •선택한 그룹 중 하나(기본값) •선택한 그룹 모두 •선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

VLAN 검색 결과 페이지 필드

VLAN 검색 결과 페이지는 VLAN 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [665페이지의 "VLAN 검색 페이지 필드"](#)를 참조하십시오.

옵션	설명/작업
이 검색 수정 링크	VLAN 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
작업	<p>각 VLAN에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> 세부사항 보기 — 장치 및 인터페이스 세부사항 페이지에 대한 링크를 사용하여 검색에 대한 세부사항을 볼 수 있는 VLAN 세부사항 페이지를 엽니다. 자세한 내용은 283페이지의 "VLAN 세부사항 페이지 필드"를 참조하십시오. 편집 — VLAN 세부사항 편집 페이지가 열립니다. 자세한 내용은 282페이지의 "VLAN 생성 및 편집"을 참조하십시오. 삭제 — VLAN 삭제 확인 대화 상자를 엽니다.
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> 새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다. 기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다. 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

장치 템플릿 검색

장치 템플릿을 사용하면 구성, OS/파일 사양 및 기타 장치별 정보를 정의한 다음 기존 장치에 적용할 수 있습니다. 장치 템플릿에는 정책 확인처럼 테스트할 실제 장치가 없어도 특정 장치 운영을 지원하는 기능도 있습니다. 자세한 내용은 [155페이지의 "장치 템플릿"](#)을 참조하십시오.

장치 템플릿을 검색하려면 보고서 아래의 메뉴 모음에서 검색 대상을 선택하고 장치 템플릿을 클릭합니다. 장치 템플릿 검색 페이지가 열립니다. 검색 기준 입력을 완료한 후에는 검색 버튼을 클릭합니다. NA는 장치 템플릿 검색 결과 페이지에 지정된 모든 검색 기준을 포함하는 장치 템플릿 목록을 반환합니다.

참고: 검색 기준을 입력할 때 검색을 실행하기 전에 다른 페이지로 변경하면 설정이 없어집니다.

장치 템플릿 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 장치 템플릿 검색 결과 페이지를 사용자 지정합니다.
템플릿 이름	<p>연산자를 선택하고 장치 템플릿의 이름을 입력합니다. 연산자는 다음과 같습니다.</p> <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 공급업체	연산자를 선택하고 장치 공급업체를 입력합니다.

필드	설명/작업
장치 모델	연산자를 선택하고 장치 모델을 입력합니다.
드라이버 이름	목록에서 드라이버를 선택합니다.
장치 설명	연산자를 선택하고 설명을 입력합니다.
주석	연산자를 선택하고 주석을 입력합니다.
구성 텍스트	연산자를 선택하고 구성 텍스트를 입력합니다.
생성 날짜	<p>검색 연산자가 "다음에 포함"이면 페이지 아래쪽에 있는 <#>개의 컨텍스트 라인 상자에 값을 제공할 수 있습니다. 결과에 검색 텍스트의 위아래로 최대 5개 라인까지 포함할 수 있습니다. (참고: 이 기능을 사용할 경우 로드할 결과 수가 많으면 성능이 상당히 느려질 수 있습니다.)</p> <p>다음 연산자를 선택합니다.</p> <ul style="list-style-type: none"> •이래 또는 다음까지 •항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>
장치 사용자 지정 데이터	연산자를 선택하고 장치 사용자 지정 데이터를 입력합니다.
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

장치 템플릿 검색 결과 페이지 필드

장치 검색 결과 페이지는 장치 템플릿 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [668페이지의 "장치 템플릿 검색"](#)을 참조하십시오.

옵션	설명/작업
이 검색 수정 링크	장치 템플릿 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
작업	<p>각 장치 템플릿에 대해 다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 편집 — 이 장치 템플릿에 대한 정보를 편집할 수 있는 장치 템플릿 편집 페이지를 엽니다. 155페이지의 "장치 템플릿 페이지 필드"를 참조하십시오. • 구성 보기 — 선택한 구성을 편집하고 주석을 추가할 수 있는 현재 구성 페이지를 엽니다.
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> • 새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다. • 기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다. • 검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. • 검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. • 검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

단일 검색

장치 변경 이벤트를 검색하려면 보고서 아래의 메뉴 모음에서 단일 검색을 클릭합니다. 단일 검색 페이지가 열립니다. 검색 버튼을 클릭하면 NA는 이 페이지에서 사용자가 지정한 모든 검색 기준을 포함하는 이벤트 목록을 단일 검색 결과 페이지에 반환합니다. [673페이지의 "단일 검색 결과 페이지 필드"](#)를 참조하십시오.

단일 검색 페이지 필드

필드	설명/작업
확인란	왼쪽의 확인란을 사용하여 선택한 정보만 표시하도록 이벤트 검색 결과 페이지를 사용자 지정합니다.
날짜	다음 연산자를 선택합니다. <ul style="list-style-type: none"> •이래 또는 다음까지 •항상, 사용자 지정(캘린더 열기), 지금 또는 1시간 전부터 1년 전 <p>참고: 캘린더 아이콘을 클릭하면 캘린더가 열립니다. 여기에서 날짜와 시간을 선택할 수 있습니다.</p>
요약	하나 이상의 이벤트 이름을 선택합니다. 추가로 이벤트를 선택/선택 취소하려면 Ctrl을 누릅니다. 각 이벤트에 대한 자세한 내용은 640페이지의 "이벤트 설명" 을 참조하십시오.
추가한 사람	연산자를 선택하고 이벤트를 만든 사용자의 로그인 이름을 제공합니다. 연산자는 다음과 같습니다. <ul style="list-style-type: none"> • 다음을 포함 • 다음을 포함하지 않음 • 다음과 일치함 • 다음과 같음 • 다음과 같지 않음

필드	설명/작업
중요도	<p>하나 이상의 중요도 수준을 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> •정보용 — 일반적으로 응답이 필요하지 않은 이벤트 •낮음 — 시간이 허용될 경우 응답이 필요할 수 있는 이벤트 •중간 — 일반적으로 72시간 이내에 시기 적절한 응답이 필요한 이벤트 •높음 — 일반적으로 24시간 이내에 신속한 응답이 필요한 이벤트 •심각 — 즉각적인 응답이 필요한 이벤트
호스트 이름	<p>연산자를 선택하고 이러한 이벤트와 연관된 장치의 호스트 이름을 입력합니다. 연산자는 다음과 같습니다.</p> <ul style="list-style-type: none"> •다음을 포함 •다음을 포함하지 않음 •다음과 일치함 •다음과 같음 •다음과 같지 않음 <p>와일드카드 문자를 사용할 수 있습니다. ?는 해당 위치에서 하나의 문자를 상징하고, *는 해당 위치에서 여러 개의 문자를 상징합니다(예: usa-ny-ny-*, 10.0.*.2 및 ?jones). (참고: 와일드 카드는 "다음과 같음" 및 "다음과 같지 않음" 연산자와는 작동하지 않습니다.)</p>
장치 IP	<p>연산자(위 참조)를 선택하고 이러한 이벤트와 연관된 장치의 IP 주소를 입력합니다.</p>
설명	<p>연산자(다음을 포함 또는 다음을 포함하지 않음)를 선택하고 검색 중인 이벤트의 고유한 텍스트를 입력합니다. 이벤트 설명을 표시할 때 일치하는 라인 주변의 컨텍스트 라인을 표시하려면 표시를 선택하고 라인 수를 입력합니다. 3개가 기본값입니다.</p>
장치가 속한 위치	<p>연산자(선택한 그룹 중 하나, 선택한 그룹 모두 또는 선택한 그룹 모두 없음)를 선택하고 스크롤 다운 목록에서 하나 이상의 그룹을 선택합니다.</p>
파티션	<p>검색 결과를 해당 파티션의 장치로 제한하려면 파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>

단일 검색 결과 페이지 필드

단일 검색 결과 페이지는 단일 검색 페이지에서 선택한 검색 기준에 따라 표시됩니다. 자세한 내용은 [671페이지의 "단일 검색 페이지 필드"](#)를 참조하십시오. 다음 표에서는 단일 검색 결과 페이지에서 사용 가능한 옵션을 설명합니다.

필드	설명/작업
이 검색 수정 링크	단일 검색 페이지로 돌아갑니다. 여기서 검색 기준을 편집하고 검색을 다시 실행할 수 있습니다.
검색 기준 보기 링크	검색 기준 정보로 아래로 스크롤합니다.
확인란	<p>각 이벤트의 확인란을 사용하면 이벤트를 삭제할 수 있습니다. 이벤트를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음 중 하나를 클릭합니다.</p> <ul style="list-style-type: none"> •삭제 — 선택한 이벤트를 삭제합니다. <p>인접한 선택 드롭다운 메뉴를 통해 모든 작업을 선택하거나 선택 취소할 수 있습니다.</p>
검색 기준	<p>검색에 사용된 검색 기준을 표시합니다. 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> •새 장치 그룹으로 저장 — 모든 결과 장치 또는 선택한 장치만을 선택하고 새 장치 그룹의 이름을 입력한 다음 그룹 생성을 클릭합니다. •기존 정적 장치 그룹에 추가 — 모든 결과 장치 또는 선택한 장치만을 선택하고 드롭다운 메뉴에서 장치 그룹을 선택한 다음 추가를 클릭합니다. •검색을 사용자 보고서로 저장 — 사용자 보고서의 이름을 입력하고 저장을 클릭합니다. 사용자 및 시스템 보고서 페이지에서 사용자 보고서를 볼 수 있습니다. 자세한 내용은 744페이지의 "사용자 및 시스템 보고서"를 참조하십시오. •검색 결과 메일 전송 — 검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 주소가 여러 개이면 쉼표로 분리하십시오. •검색 결과를 CSV 파일로 보기 — 검색 결과를 CSV 형식으로 다운로드합니다.

고급 검색

고급 검색 페이지를 사용하면 다음을 수행할 수 있습니다.

- 부울 표현식(and/or)을 사용하여 검색을 필터링합니다. 검색을 세분화하기 위해 부울 표현식에 괄호를 사용할 수 있음을 유의하십시오.
- 하나 이상의 검색 기준(예: IP 주소, 도메인 이름 및 정책 준수)을 사용하여 검색을 구성합니다.
- 장치 그룹으로 검색을 제한합니다.
- 고급 검색 결과 페이지의 출력을 사용자 지정합니다.

고급 검색 페이지를 열려면 보고서 아래의 메뉴 모음에서 고급 검색을 클릭합니다. 검색 버튼을 클릭하면 NA는 지정한 검색 기준을 반환합니다.

고급 검색 페이지 필드

필드	설명/작업
검색 대상	드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •ACL •준수 •구성 •장치 •진단 •이벤트 •인터페이스 •모듈 •세션 •작업

검색 기준

검색 기준을 선택할 때마다 검색 기준 섹션에 표시되고, 여기에서 다음을 포함, 일치 또는 다음과 같음 등의 연산자를 선택하고 검색할 정보를 입력할 수 있습니다. 정의된 기준을 삭제하려면 검색 기준 인덱스 문자 옆의 X를 클릭합니다.

필드	설명/작업
기준 추가	<p>드롭다운 메뉴에서 다음과 같은 검색 기준을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> • 호스트 이름 • 장치 IP • 도메인 이름 • 장치 상태 • 정책 준수
부울 표현식	
표현식	<p>기본적으로 정의된 기준 인덱스 문자는 부울 'and' 표현식과 함께 표시됩니다. 예를 들어 3개의 검색 기준을 정의하면 표현식은 <i>A and B and C</i>와 같이 됩니다. 부울 표현식은 필요에 따라 편집할 수 있습니다. 표현식을 기본값으로 재설정하려면 표현식 재설정 버튼을 클릭합니다. (참고: 최대 기준 수는 10개입니다.)</p>
장치 그룹으로 검색 제한	
장치가 속한 위치	<p>드롭다운 메뉴에서 다음 연산자 중 하나를 선택한 다음 장치 그룹을 하나 이상 선택합니다.</p> <ul style="list-style-type: none"> • 선택한 그룹 중 하나(기본값) • 선택한 그룹 모두 • 선택한 그룹 모두 없음 <p>참고: 장치 선택기를 사용하여 그룹을 선택합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오.</p>
파티션	<p>파티션을 선택합니다. 처음에는 기본 파티션(이름이 지정된 기본 사이트)에 모든 인벤토리가 포함됩니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 파티션에 대한 자세한 내용은 201페이지의 "파티션"을 참조하십시오.)</p>
출력 사용자 지정	
검색 결과에 포함할 필드 선택	<p>고급 검색 결과 페이지에 포함할 필드를 선택합니다. 여러 필드를 선택하려면 첫 번째 필드를 클릭한 다음 Ctrl을 누른 상태에서 클릭하여 추가 필드를 선택/선택 취소합니다.</p>

필드	설명/작업
결과 정렬 기준	드롭다운 메뉴에서 검색 결과를 정렬할 검색 기준을 선택합니다. 오름차순(기본값) 또는 내림차순을 지정할 수 있습니다.
페이지별 결과 표시 수	고급 검색 결과 페이지에 표시할 항목 수를 입력합니다. 기본값은 25입니다.
텍스트 필드를 표시할 때 일치하는 라인 주변에서 <#>개의 컨텍스트 라인 표시	고급 검색 결과 페이지에 텍스트 필드를 표시할 때 함께 표시할 일치하는 라인 주위의 라인 수를 입력합니다. 기본값은 3입니다.

샘플 고급 검색

다음 고급 검색에서는 사용자가 두 개의 데이터 센터를 관리 중인 것으로 가정합니다. 한 개의 데이터 센터는 뉴욕에 있고 다른 하나는 캘리포니아에 있습니다. 검색은 데이터 센터에 설치된 모든 Cisco 장치의 시간대가 올바르게 설정되지 않았음을 알려줍니다.

1. NA에 로그인합니다.
2. 보고서 아래의 기본 메뉴에서 고급 검색을 클릭합니다. 고급 검색 페이지가 열립니다.
3. 검색 필드에서 드롭다운 메뉴에서 장치를 선택합니다.
4. 검색 기준 필드에서 드롭다운 메뉴에서 드라이버 이름을 선택합니다.
5. NA가 사용 중인 모든 Cisco 드라이버를 선택합니다.
6. 기준 추가 드롭다운 메뉴에서 호스트 이름을 선택합니다.
7. 드롭다운 메뉴에서 "다음을 포함"을 선택하고 redmond를 입력합니다.
8. 기준 추가 드롭다운 메뉴에서 구성 텍스트를 선택합니다.
9. 드롭다운 메뉴에서 "다음을 포함하지 않음"을 선택하고 `set timezone PST`를 입력합니다.
10. 부울 표현식 필드에서 기본 문자열을 "A and (B or C)"로 수정합니다.
11. 검색 버튼을 클릭합니다.

12장: 진단 및 이벤트 관리

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
이벤트 통합 보기(단일 보기)	680페이지의 "이벤트 통합 보기(단일 보기)"
진단	684페이지의 "진단"
진단 추가 및 사용자 지정	687페이지의 "사용자 지정 진단 추가 및 편집"

진단 및 단일 보기 탐색

HP Network Automation
로그아웃

장치 ▾
작업 ▾
정책 ▾
보고서 ▾
관리 ▾
도움말 ▾

인벤토리 그룹
보안 파티션 새로 만들기 ▶
새 장치 마법사

구성 변경

장치 도구 ▶
명령 스크립트
구성 템플릿
장치 암호 규칙
장치 템플릿

진단
정책
소프트웨어 이미지

장치 작업 ▶

단일 보기

단일 검색

사용자 및 시스템 보고서

검색 대상 ▶
고급 검색

준수 센터

네트워크 상태
모범 사례
장치 상태
통계 대시보드
다이어그램 작성

장치 소프트웨어
소프트웨어 취약점
이미지 동기화 보고서

시스템 및 네트워크 이벤트

요약 보고서
보고서 작업 ▶

이벤트 통합 보기(단일 보기)

단일 보기를 통해 하나의 페이지에서 모든 해당 장치 또는 단일 장치의 변경 사항을 표시하는 이벤트를 추적할 수 있습니다. 이벤트 유형 목록에서 선택할 수 있는 옵션은 다음과 같습니다.

- 장치 부팅됨
- 장치 구성 변경
- 장치 진단 변경됨
- 장치 암호 변경
- 다시 로드된 장치
- 장치 소프트웨어 변경
- 모듈 추가됨
- 모듈 변경됨
- 모듈 제거됨
- 예약된 장치 구성이 변경됨
- 사용자 메시지

NA 이벤트의 전체 목록은 [640페이지의 "이벤트 설명"](#)을 참조하십시오.

단일 보기 페이지를 보려면 보고서 아래의 메뉴 모음에서 단일 보기를 클릭합니다. 단일 보기 페이지가 열립니다.

단일 보기 페이지 필드

필드	설명/작업
검색 결과를 CSV 파일로 보기 링크	CSV 파일로 표시된 결과를 저장할 위치를 입력하라는 메시지가 표시됩니다.
표시된 변경 이벤트 유형 링크	표시된 변경 이벤트 유형 메뉴로 스크롤합니다. 이 메뉴에서 표시할 이벤트를 선택할 수 있습니다.
다음 대상:	이벤트를 볼 시간 프레임을 표시합니다. 옵션은 다음과 같습니다. <ul style="list-style-type: none"> •과거 1, 2, 4, 8, 12, 24 및 48시간 •과거 1 및 2주 •과거 1개월 •모든 이벤트
현재 작업 그룹	드롭다운 메뉴에서 장치 그룹을 선택합니다.
확인란	왼쪽의 확인란을 통해 NA 데이터베이스의 이벤트를 삭제할 수 있습니다. 이벤트를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 이렇게 하면 NA 데이터베이스에서 선택한 이벤트가 삭제됩니다. 인접한 선택 드롭다운 메뉴를 통해 모든 이벤트를 선택하거나 선택 취소할 수 있습니다.
이벤트 날짜	이벤트 날짜/시간을 MMM-dd-yy HH:mm:ss 형식으로 표시합니다. 형식은 시스템 관리자가 구성합니다.
호스트 이름	장치의 호스트 이름 또는 IP 주소를 표시합니다. 호스트 이름 또는 IP 주소를 클릭하면 장치 및 구성 이력에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.

필드	설명/작업
요약	<p>이벤트 유형을 표시합니다. NA 이벤트의 목록은 640페이지의 "이벤트 설명"을 참조하십시오. 이벤트 유형 링크를 클릭하면 이벤트 세부사항 페이지가 열립니다. 이 페이지에 포함된 내용은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 이벤트 발생 날짜 및 시간 • 이벤트를 추가한 사람 또는 프로세스의 로그인 이름 • 이벤트 유형 • 이벤트에 대한 간단한 설명 • 장치에 대한 자세한 내용 링크
추가한 사람	<p>이벤트 생성을 초래한 작업을 수행한 사용자의 로그인 이름을 표시합니다.</p>
작업	<p>이전과 비교 링크가 다음 이벤트에 표시됩니다.</p> <ul style="list-style-type: none"> • 장치 구성 변경 — 장치 구성 비교 페이지가 열립니다. 자세한 내용은 231페이지의 "장치 구성 비교"를 참조하십시오. • 장치 진단 변경됨 — 예를 들어 NA 장치 파일 시스템 비교 페이지 또는 NA 모듈 상태 비교 페이지와 같이 변경된 진단 유형에 따라 해당 비교 페이지가 열립니다. • 장치 암호 변경 — 장치 구성 비교 페이지가 열립니다. 자세한 내용은 231페이지의 "장치 구성 비교"를 참조하십시오.

필드	설명/작업
표시된 변경 이벤트 유형	<p>이벤트 유형의 목록을 표시합니다. 여기에서 다음을 비롯하여 선택할 수 있습니다.</p> <ul style="list-style-type: none">• 장치 부팅됨• 장치 구성 변경• 장치 진단 변경됨• 장치 암호 변경• 다시 로드된 장치• 장치 소프트웨어 변경• 모듈 추가됨• 모듈 변경됨• 모듈 제거됨• 예약된 장치 구성이 변경됨• 사용자 메시지

진단

구성 파일 이외에 추가로 NA는 라우팅 테이블, 포트 통계 및 IP 설정 등의 기타 장치 정보를 수집합니다. 이를 통틀어 *진단*이라고 합니다. 진단은 구성 변경 사항의 효과를 확인하고 라우팅 문제점 및 성능 저하 등의 복잡한 문제를 해결하는 데 사용할 수 있습니다.

기본적으로 NA는 해당 장치의 구성 변경 사항을 감지할 때마다 장치에서 기본 진단 집합을 캡처합니다. 추가 진단 작업 또는 이벤트 규칙을 정의하여 여러 시간대에서 진단을 캡처할 수 있으며, 추가 사용자 지정 진단을 정의하여 해당 환경에 유용한 특정 장치 정보를 캡처할 수 있습니다.

NA를 통해 진단을 특정 이벤트의 결과로 자동 실행할 수 있습니다. 또한 특정 임계값 도달 시 자동화된 반응 및 응답이 발생할 수 있도록 CPU 사용률 등의 환경 진단을 만들고 모니터링할 수 있습니다. 구성 변경 또는 기타 이벤트의 결과로 진단 자동 실행에 대한 정보는 [569페이지의 "이벤트 규칙 추가"](#)를 참조하십시오.

장치 아래의 메뉴 모음에서 장치 도구를 선택하고 진단을 클릭합니다. 진단 페이지가 열립니다. 사용 가능한 진단이 나열됩니다.

진단 페이지 필드

필드	설명/작업
새 진단 링크	새 진단을 작성할 수 있는 새 진단 페이지가 열립니다. 자세한 내용은 686페이지의 "새 진단 페이지 필드" 를 참조하십시오.
진단 실행 링크	진단을 실행할 수 있는 진단 작업 실행 페이지가 열립니다. 자세한 내용은 397페이지의 "진단 실행 작업 페이지 필드" 를 참조하십시오.
진단 가져오기/내보내기 링크	미리 구성된 명령 스크립트 또는 진단 스크립트를 가져오거나 명령 스크립트 또는 진단 스크립트를 파일로 내보낼 수 있는 명령 스크립트/진단 가져오기/내보내기 페이지가 열립니다. 자세한 내용은 719페이지의 "스크립트/진단 가져오기/내보내기 페이지 필드" 를 참조하십시오.

필드	설명/작업
확인란	왼쪽의 확인란을 통해 진단을 삭제할 수 있습니다. 진단을 선택한 후에 작업 드롭다운 메뉴를 클릭한 후 삭제를 클릭합니다. 그러면 선택된 진단이 삭제됩니다. 인접한 선택 드롭다운 메뉴를 통해 모든 진단을 선택하거나 선택 취소할 수 있습니다.
스크립트 이름	진단의 이름을 표시합니다.
모드/장치 제품군	Cisco IOS 사용 등 진단이 실행되는 데 사용하는 장치 액세스 모드를 표시합니다.
마지막 수정일	진단이 마지막으로 수정된 날짜 및 시간을 표시합니다.
파티션	진단은 특정 파티션에 적용할 수 있습니다. 진단은 모든 파티션에 적용할 수 있으므로 모든 사용자가 [공유]로 표시된 진단을 볼 수 있습니다. 참고: NA 관리자가 장치를 분할한 경우, 볼 수 있는 권한이 있는 특정 파티션(및 해당 파티션에 속한 장치)에 속한 진단만 보고 편집하고 실행할 수 있습니다. 장치 및 사용자 세분화에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
마지막으로 수정한 사람	최종 사용자의 이름을 표시하여 진단을 수정합니다(사용 가능한 경우).
작업	다음 옵션 중에서 선택할 수 있습니다. <ul style="list-style-type: none"> • 편집 — 진단을 편집할 수 있는 진단 편집 페이지가 열립니다. 자세한 내용은 686페이지의 "새 진단 페이지 필드"를 참조하십시오. • 실행 — 진단을 실행할 수 있는 새 작업 - 진단 실행 페이지가 열립니다. 자세한 내용은 397페이지의 "진단 실행 작업 페이지 필드"를 참조하십시오.

새 진단 페이지 필드

새 진단을 생성하려면

1. 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 진단을 클릭합니다. 진단 페이지가 열립니다.
2. 페이지의 맨 위에 새 진단 링크를 클릭합니다. 새 진단 페이지가 열립니다. 완료되면 스크립트 저장 버튼을 클릭해야 합니다.

필드	설명/작업
진단 링크	사전 정의된 진단을 작성하거나 실행할 수 있는 진단 페이지가 열립니다. 자세한 내용은 684페이지의 "진단 페이지 필드" 를 참조하십시오.
이름	진단의 이름을 입력합니다.
설명	진단에 대한 설명을 입력합니다.
파티션	<p>진단은 특정 파티션에 적용할 수 있습니다. 진단은 모든 파티션에 적용할 수 있으므로 모든 사용자가 [공유]로 표시된 진단을 볼 수 있습니다.</p> <p>참고: NA 관리자가 장치를 분할한 경우, 볼 수 있는 권한이 있는 특정 파티션(및 해당 파티션에 속한 장치)에 속한 진단만 보고 편집하고 실행할 수 있습니다. 장치 및 사용자 세분화에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화"를 참조하십시오.</p>
고급 스크립팅 확인란	<p>이 옵션이 선택되면 사용자 정의된 변수를 사용하지 않고 고급 스크립트로 진단을 정의할 수 있습니다. 다음 필드는 모드 및 드라이버 필드를 대체합니다.</p> <ul style="list-style-type: none"> • 장치 제품군 — 이 스크립트가 실행되는 장치 제품군의 이름을 선택합니다. 장치 제품군은 유사한 구성 CLI 명령 구문을 공유하는 장치의 모음입니다. • 언어 — 스크립트 작성 시 사용된 언어를 선택합니다. • 매개 변수 — 스크립트의 매개 변수를 입력합니다. <p>고급 스크립트 작성에 대한 자세한 정보는 720페이지의 "명령 스크립트 추가"를 참조하십시오.</p>

필드	설명/작업
모드	Cisco Exec 또는 Nortel Manager와 같은 장치 액세스 모드를 선택합니다.
드라이버	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •모든 해당 드라이버(기본값) •특정 드라이버 선택 <p>목록에서 하나 이상의 드라이버를 선택하는 경우 하나의 드라이버를 클릭하거나 Shift를 누르고 클릭 또는 Shift를 누르고 클릭을 사용하여 드라이버를 여러 개 선택할 수 있습니다. (참고: Baystack 470과 같은 메뉴 기반 장치는 사용자 지정 진단으로 액세스할 수 없음)</p>
스크립트	실행할 명령을 장치별로 입력합니다. 스크립트 상자의 높이 및 너비는 관리 설정 옵션의 설정을 통해 제어됩니다. 스크립팅 기능을 광범위하게 사용하는 경우 스크롤하지 않고 스크립트를 볼 수 있도록 이러한 설정을 조정할 수 있습니다. <p>참고: 스크립트의 이름은 동일하지만 모드가 서로 다를 수 있습니다. 이 방법을 통해 NA는 여러 공급업체의 스크립트를 관리합니다. 스크립트를 실행하려면 스크립트 이름을 선택하기만 하면 각 버전의 스크립트가 로드됩니다. 장치 그룹에 대해 스크립트를 실행하면 NA가 장치 유형을 인식하여 해당 스크립트를 적용합니다.</p>

특정 장치에 대한 진단을 보려면

1. 장치 아래의 메뉴 탭에서 인벤토리를 클릭합니다.
2. 진단 정보를 원하는 대상 장치의 호스트 이름 또는 IP 주소를 클릭합니다.
3. 보기 드롭다운 메뉴에서 진단을 선택하고 보려는 진단을 클릭합니다. 각 옵션은 장치에 대한 진단의 기록 목록을 보여줍니다.

사용자 지정 진단 추가 및 편집

NA를 통해 해당 환경에 유용한 특정 정보를 캡처하기 위해 사용자 지정 진단을 정의할 수 있습니다. 각 사용자가 사용자 지정 진단을 실행할 수 있으므로 모든 사용자는 장치 구성을 수정할 수 있는 권한이 없더라도 네트워크 문제점을 분석할 수 있습니다.

사용자 지정 진단을 정의하려면 장치에서 실행할 명령을 하나 이상 입력합니다. NA는 해당 명령의 결과를 진단 결과로 저장합니다. 모든 사용자에게 진단을 실행할 수 있는 권한이 있으므로 해당 명령으로는 장치 구성이 변경되지 않습니다. 사용자 지정 진단은 읽기 전용 작업을 수행해야 합니다.

이벤트 규칙을 사용하여 진단을 트리거할 수 있습니다. 예를 들어 구성 배포가 실패할 때마다 규칙을 설정하여 진단을 실행할 수 있습니다.

공급업체가 여러 개인 네트워크의 경우 여러 진단을 같은 이름으로 생성할 수 있지만 이러한 진단은 서로 다른 장치 유형에서 실행됩니다. 이름이 같은 진단은 링크로 연결되어 있습니다. 그룹 작업 실행 시 NA는 각 장치별로 올바른 진단 버전을 자동으로 실행합니다. 예를 들어 공급업체가 여러 개인 라우터가 있는 경우에도 San Francisco에서 모든 해당 라우터의 데이터를 수집하기 위해 그룹 진단을 실행할 수 있습니다.

참고: NA 데이터베이스에서는 오래된 데이터를 정기적으로 제거해야 합니다. 성능을 유지 보수하고 디스크 공간을 복원하려면 정기적으로 오래된 데이터를 모두 제거해야 하며 특히 진단 및 스크립트 데이터를 제거해야 합니다. 이전 인스턴스와 다른 경우에만 저장되는 구성과 달리 진단 및 스크립트 데이터는 모두 저장됩니다. 기본적으로 NA는 45일 후에 진단 데이터를 제거합니다. 자세한 내용은 [478페이지의 "데이터 정리 작업 페이지 필드"](#)를 참조하십시오.

690

HP Network Automation 사용 설명서

13장: 사용자 지정 데이터 설정

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	693페이지의 "시작하기"
사용자 지정 데이터 설정 페이지 필드	694페이지의 "사용자 지정 데이터 설정 페이지 필드"
향상된 사용자 지정 필드 설정	699페이지의 "향상된 사용자 지정 필드 설정"

사용자 지정 데이터 설정 탐색

HP Network Automation		로그아웃
장치 ▾	작업 ▾	정책 ▾
		보고서 ▾
		관리 ▾
		도움말 ▾
↓		
<ul style="list-style-type: none"> 사용자 사용자 그룹 새 사용자 새 사용자 그룹 로그온한 사용자 		
<ul style="list-style-type: none"> 사용자 역할 및 권한 		
<ul style="list-style-type: none"> 보안 파티션 게이트웨이 장치 암호 규칙 이벤트 알림 및 응답 규칙 		
<ul style="list-style-type: none"> 사용자 지정 데이터 설정 향상된 사용자 지정 필드 설정 LDAP 설정 워크플로 설정 		
<ul style="list-style-type: none"> 관리 설정 ▶ 		
<ul style="list-style-type: none"> 작업 로드 시스템 상태 서비스 시작 / 중지 문제 해결 드라이버 		
<ul style="list-style-type: none"> 시스템 작업 ▶ 		

시작하기

사용자 지정 데이터 필드는 사용자가 특정 장치, 구성, 사용자 등에 유용한 데이터를 할당할 수 있게 하는 데 사용됩니다. 이를 통해 좀 더 유연해지고, NA를 다른 응용 프로그램과 통합할 수 있습니다.

기본적으로 HP Network Automation(NA)은 사용자 지정 데이터 필드를 최대 6개까지 지원합니다. 이 사용자 지정 데이터 필드 수를 무제한으로 확장할 수 있습니다. 확장된 사용자 지정 데이터 필드를 활성화한 경우 [699페이지의 "향상된 사용자 지정 필드 설정"](#)을 참조하십시오.

이전에 몇몇 CLI 명령에는 명령에서 customname 및 customvalue 옵션을 사용하여 사용자 지정 필드를 수정할 수 있는 기능이 있었습니다. 하지만 한 번에 한 필드만 조작할 수 있었습니다. 이러한 제한이 여러 필드를 수정해야 하는 경우에는 다소 불편하기도 했습니다. 따라서 새로운 customnames 및 customvalues 값을 사용하면 여러 필드를 동시에 수정할 수 있습니다.

이름과 값은 쉼표로 구분된 목록 안에 나열됩니다. 쉼표를 포함하는 값이 있으면 따옴표 안에 지정해야 합니다. 예를 들면 다음과 같습니다.

```
mod device -customnames Location, Floor, Rack -customvalues  
'Seattle, WA',3rd,'126-18,10'
```

참고: 이전 옵션도 여전히 사용할 수 있으므로 기존 스크립트의 이전 버전과의 호환성이 유지됩니다.

사용자 지정 데이터를 추가하려면 관리 아래의 메뉴 모음에서 사용자 지정 데이터 설정을 클릭합니다. 사용자 지정 데이터 설정 페이지가 열립니다.

사용자 지정 데이터 설정 페이지 필드

필드	설명/작업
사용자 지정 데이터 설정	<p>드롭다운 메뉴에서 사용자 지정 데이터 설정을 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> •장치 구성 및 진단 •장치 •장치 블레이드/모듈 •장치 인터페이스 •장치 그룹 •사용자 •작업 •텔넷/SSH 세션
확인란	<p>왼쪽의 확인란을 통해 필드를 활성화할 수 있습니다. 따라서 필드는 사용자 인터페이스에 나타나며 통합 API에 사용할 수 있습니다.</p>
장치 구성 및 진단	
	<p>이러한 필드는 장치 구성 세부사항 페이지에 나타납니다. 장치 구성 세부사항 편집 페이지를 여는 주석 편집 링크를 클릭하여 값을 입력하거나 편집할 수 있습니다.</p>
API 이름	<p>통합 API 및 알림 규칙에 대해 필드를 식별합니다. API 이름에 A-Z, a-z, 0-9, _, -, &(첨표 포함되지 않음)를 사용할 수 있습니다.</p>
이름 표시	<p>사용자가 사용자 인터페이스에서 보는 이름을 표시합니다.</p>
값	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •HTML 포함 가능 — 이 옵션을 선택하면 (기본) 사용자(또는 통합 API)가 이 필드에 HTML 코드를 입력해야 합니다. NA에서는 사용자 인터페이스에 텍스트가 아닌 HTML로 필드를 표시합니다. 이를 통해 외부 문제 티켓 응용 프로그램에 링크를 포함할 수 있습니다. •제한 범위 — 이 옵션을 선택하면 드롭다운 목록 상자에 나타나는, 첨표로 구분된 값을 입력합니다.
장치	

필드	설명/작업
----	-------

이러한 필드는 장치 정보 페이지에 나타납니다. 장치 편집 페이지를 여는 편집 링크를 클릭하거나 새 장치 페이지를 여는 장치 드롭다운 메뉴에서 추가를 클릭하여 값을 입력하거나 편집할 수 있습니다.

API 이름	통합 API 및 알림 규칙에 대해 필드를 식별합니다. API 이름에 A-Z, a-z, 0-9, _, -, &(쉼표 포함되지 않음)를 사용할 수 있습니다.
이름 표시	사용자가 사용자 인터페이스에서 보는 이름을 표시합니다.
값	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •HTML 포함 가능 — 이 옵션을 선택하면 (기본) 사용자(또는 통합 API)가 이 필드에 HTML 코드를 입력해야 합니다. NA에서는 사용자 인터페이스에 텍스트가 아닌 HTML로 필드를 표시합니다. 이를 통해 외부 문제 티켓 응용 프로그램에 링크를 포함할 수 있습니다. •제한 범위 — 이 옵션을 선택하면 드롭다운 목록 상자에 나타나는, 쉼표로 구분된 값을 입력합니다.

장치 블레이드/모듈

이러한 필드는 보기/편집 모듈 페이지에 나타납니다.

API 이름	통합 API 및 알림 규칙에 대해 필드를 식별합니다. API 이름에 A-Z, a-z, 0-9, _, -, &(쉼표 포함되지 않음)를 사용할 수 있습니다.
이름 표시	사용자가 사용자 인터페이스에서 보는 이름을 표시합니다.
값	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •HTML 포함 가능 — 이 옵션을 선택하면 (기본) 사용자(또는 통합 API)가 이 필드에 HTML 코드를 입력해야 합니다. NA에서는 사용자 인터페이스에 텍스트가 아닌 HTML로 필드를 표시합니다. 이를 통해 외부 문제 티켓 응용 프로그램에 링크를 포함할 수 있습니다. •제한 범위 — 이 옵션을 선택하면 드롭다운 목록 상자에 나타나는, 쉼표로 구분된 값을 입력합니다.

장치 인터페이스

이러한 필드는 보기/편집 모듈 페이지에 나타납니다.

필드	설명/작업
API 이름	통합 API 및 알림 규칙에 대해 필드를 식별합니다. API 이름에 A-Z, a-z, 0-9, _, -, &(쉼표 포함되지 않음)를 사용할 수 있습니다.
이름 표시	사용자가 사용자 인터페이스에서 보는 이름을 표시합니다.
값	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •HTML 포함 가능 — 이 옵션을 선택하면 (기본) 사용자(또는 통합 API)가 이 필드에 HTML 코드를 입력해야 합니다. NA에서는 사용자 인터페이스에 텍스트가 아닌 HTML로 필드를 표시합니다. 이를 통해 외부 문제 티켓 응용 프로그램에 링크를 포함할 수 있습니다. •제한 범위 — 이 옵션을 선택하면 드롭다운 목록 상자에 나타나는, 쉼표로 구분된 값을 입력합니다.

장치 그룹

이러한 필드는 그룹에 대한 장치 목록 페이지에 나타납니다. 그룹 편집 페이지를 여는 그룹 편집 링크를 클릭하거나 새 그룹 페이지를 여는 장치 드롭다운 메뉴에서 그룹을 클릭하여 값을 입력하거나 편집할 수 있습니다.

API 이름	통합 API 및 알림 규칙에 대해 필드를 식별합니다. API 이름에 A-Z, a-z, 0-9, _, -, &(쉼표 포함되지 않음)를 사용할 수 있습니다.
이름 표시	사용자가 사용자 인터페이스에서 보는 이름을 표시합니다.
값	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •HTML 포함 가능 — 이 옵션을 선택하면 (기본) 사용자(또는 통합 API)가 이 필드에 HTML 코드를 입력해야 합니다. NA에서는 사용자 인터페이스에 텍스트가 아닌 HTML로 필드를 표시합니다. 이를 통해 외부 문제 티켓 응용 프로그램에 링크를 포함할 수 있습니다. •제한 범위 — 이 옵션을 선택하면 드롭다운 목록 상자에 나타나는, 쉼표로 구분된 값을 입력합니다.

사용자

이러한 필드는 내 프로필 페이지에 나타납니다. 사용자 편집 페이지를 여는 사용자 목록 페이지에서 편집 링크를 클릭하거나 새 사용자 페이지를 여는 사용자 목록 페이지에서 새 사용자를 클릭하여 값을 입력하거나 편집할 수 있습니다.

필드	설명/작업
API 이름	통합 API 및 알림 규칙에 대해 필드를 식별합니다. API 이름에 A-Z, a-z, 0-9, _, -, &(쉼표 포함되지 않음)를 사용할 수 있습니다.
이름 표시	사용자가 사용자 인터페이스에서 보는 이름을 표시합니다.
값	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •HTML 포함 가능 — 이 옵션을 선택하면 (기본) 사용자(또는 통합 API)가 이 필드에 HTML 코드를 입력해야 합니다. NA에서는 사용자 인터페이스에 텍스트가 아닌 HTML로 필드를 표시합니다. 이를 통해 외부 문제 티켓 응용 프로그램에 링크를 포함할 수 있습니다. •제한 범위 — 이 옵션을 선택하면 드롭다운 목록 상자에 나타나는, 쉼표로 구분된 값을 입력합니다.

작업

이러한 필드는 작업 페이지에 나타납니다. 사용자 인터페이스를 통해 값을 입력하거나 편집할 수 없으며 통합 API를 통해서만 가능합니다.

API 이름	통합 API 및 알림 규칙에 대해 필드를 식별합니다. API 이름에 A-Z, a-z, 0-9, _, -, &(쉼표 포함되지 않음)를 사용할 수 있습니다.
이름 표시	사용자가 사용자 인터페이스에서 보는 이름을 표시합니다.
값	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •HTML 포함 가능 — 이 옵션을 선택하면 (기본) 사용자(또는 통합 API)가 이 필드에 HTML 코드를 입력해야 합니다. NA에서는 사용자 인터페이스에 텍스트가 아닌 HTML로 필드를 표시합니다. 이를 통해 외부 문제 티켓 응용 프로그램에 링크를 포함할 수 있습니다. •제한 범위 — 이 옵션을 선택하면 드롭다운 목록 상자에 나타나는, 쉼표로 구분된 값을 입력합니다.

텔넷/SSH 세션

이러한 필드는 텔넷/SSH 세션 목록 페이지에 나타납니다. 사용자 인터페이스를 통해 값을 입력하거나 편집할 수 없으며 통합 API를 통해서만 가능합니다.

API 이름	통합 API 및 알림 규칙에 대해 필드를 식별합니다. API 이름에 A-Z, a-z, 0-9, _, -, &(쉼표 포함되지 않음)를 사용할 수 있습니다.
--------	---

필드	설명/작업
이름 표시	사용자가 사용자 인터페이스에서 보는 이름을 표시합니다.
값	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none">•HTML 포함 가능 — 이 옵션을 선택하면 (기본) 사용자(또는 통합 API)가 이 필드에 HTML 코드를 입력해야 합니다. NA에서는 사용자 인터페이스에 텍스트가 아닌 HTML로 필드를 표시합니다. 이를 통해 외부 문제 티켓 응용 프로그램에 링크를 포함할 수 있습니다.•제한 범위 — 이 옵션을 선택하면 드롭다운 목록 상자에 나타나는, 쉼표로 구분된 값을 입력합니다.

향상된 사용자 지정 필드 설정

사용자 지정 필드를 사용하면 특정 장치에 유용한 데이터를 할당할 수 있습니다. 이를 통해 좀 더 유연해지고, NA를 다른 응용 프로그램과 통합할 수 있습니다.

참고: 향상된 사용자 지정 필드를 추가하려면 먼저 향상된 사용자 지정 필드 응용 프로그램을 활성화해야 합니다. 자세한 지침은 [80페이지의 "사용자 인터페이스 페이지 필드"](#)를 참조하십시오.

현재 사용자 지정 필드를 보고 장치 세부사항 및 장치 인터페이스 페이지에 데이터를 추가하려면, 관리의 메뉴 모음에서 향상된 사용자 지정 필드 데이터 설정을 클릭합니다. 향상된 사용자 지정 필드 데이터 설정 페이지가 열립니다.

필드	설명/작업
드롭다운 메뉴	드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •장치(기본값) •장치 인터페이스
사용자 지정 장치 필드 추가 링크	사용자 지정 장치 필드 추가 링크를 클릭하면 사용자 지정 데이터 필드를 추가할 수 있는 새 사용자 지정 데이터 필드 페이지가 열립니다. 이러한 데이터 필드는 장치 세부사항 및 장치 인터페이스 페이지에 표시됩니다. 자세한 내용은 700페이지의 "새 사용자 지정 데이터 필드 페이지" 를 참조하십시오. 장치 세부사항 및 장치 인터페이스 페이지에 대한 자세한 내용은 261페이지의 "메뉴 옵션 보기" 및 267페이지의 "장치 인터페이스 페이지 필드" 를 참조하십시오.
장치/장치 인터페이스	
사용함	사용자 지정 데이터 필드의 활성화 여부를 나타냅니다.
필드 이름	사용자 지정 데이터 필드의 이름을 표시합니다.
값을 다음으로 제한	심표로 구분된 값의 목록을 표시합니다. 이 목록은 실제 데이터를 편집할 때 드롭다운 메뉴로 표시됩니다.
HTML 허용	사용자가 이 데이터 필드에 HTML 코드를 입력할 수 있는지 여부를 나타냅니다. NA에서는 텍스트가 아닌 HTML로 데이터 필드를 표시합니다.

필드	설명/작업
작업	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 편집 — 현재 정보를 편집할 수 있는 사용자 지정 데이터 필드 편집 페이지를 엽니다. 700페이지의 "새 사용자 지정 데이터 필드 페이지"를 참조하십시오. • 삭제 — 사용자 지정 데이터 필드를 삭제할 수 있습니다. 데이터 필드를 삭제하면 해당 필드와 연관된 데이터도 삭제됩니다.

새 사용자 지정 데이터 필드 페이지

장치 세부사항 및 장치 인터페이스 페이지에 사용자 지정 데이터를 추가하려면 관리의 메뉴 모음에서 향상된 사용자 지정 필드 설정을 클릭합니다. 향상된 사용자 지정 필드 설정 페이지가 열립니다. 페이지 맨 위에 있는 사용자 지정 장치 필드 추가 링크를 클릭합니다.

필드	설명/작업
사용함	이 옵션을 선택하면 사용자 지정 데이터 필드가 활성화됩니다.
필드 이름	데이터 필드 이름을 입력합니다.
값을 다음으로 제한	선택으로 구분된 값의 목록을 입력합니다. 이 목록은 실제 데이터를 편집할 때 드롭다운 메뉴로 표시됩니다.
HTML 허용	이 옵션을 선택하면 사용자가 이 필드에 HTML 코드를 입력할 수 있습니다. NA에서는 텍스트가 아닌 HTML로 필드를 표시합니다.

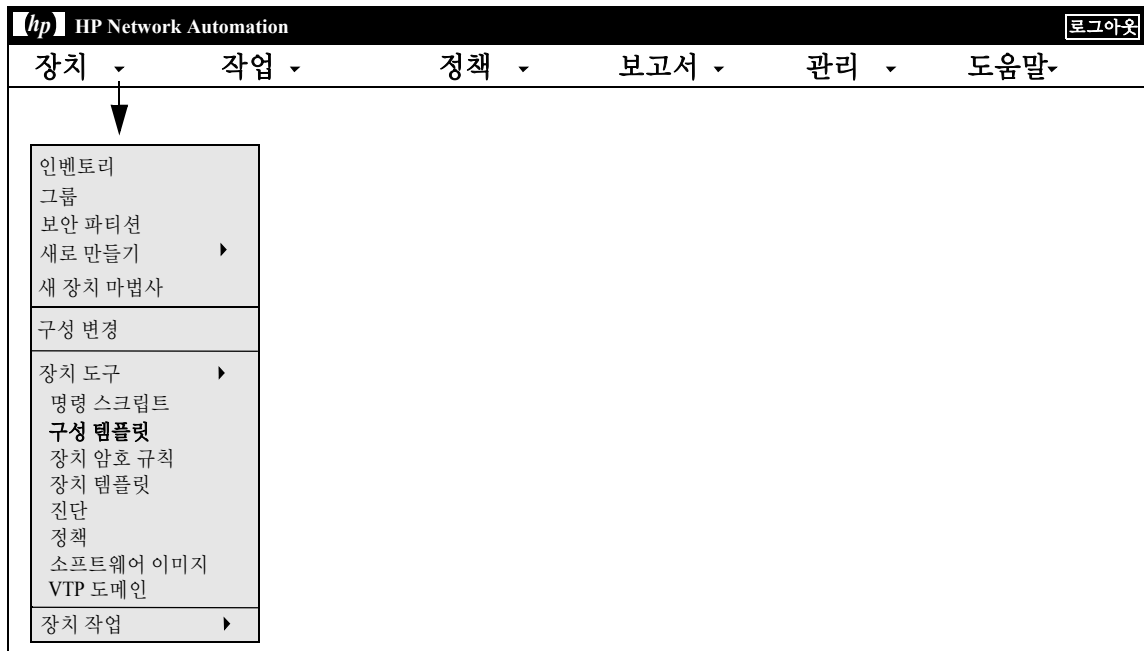
완료되면 저장 버튼을 클릭합니다. 향상된 사용자 지정 필드 설정 페이지에 새 필드가 표시됩니다.

14장: 구성 템플릿 생성

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	702페이지의 "시작하기"
구성 템플릿 보기	703페이지의 "구성 템플릿 보기"
새 구성 템플릿 생성	706페이지의 "새 구성 템플릿 생성"

구성 템플릿 탐색



시작하기

구성 템플릿을 통해 새 장치 구성을 신속하고 간단하게 배포할 수 있습니다. 구성 템플릿을 사용하여 다음을 수행할 수 있습니다.

- 엔지니어는 부서별 구성 표준을 준수하면서 장치나 서비스를 신속하게 프로비전할 수 있습니다.
- 네트워크 설계자는 검증 매개 변수를 포함하는 편리한 GUI 프롬프트를 생성할 수 있습니다. 그러면 템플릿 사용자가 빈 칸을 채우면서 새 구성을 신속하게 입력하고 배포할 수 있습니다.

일반적으로 구성 템플릿은 다양한 방식으로 조합하여 스크립트를 작성할 수 있는 구성 데이터의 단편입니다. 따라서 이 스크립트는 장치에 이미 있는 데이터에 추가하거나 구성의 일부를 대체할 수 있습니다.

장치 템플릿 생성에 대한 자세한 내용은 [155페이지의 "장치 템플릿"](#)을 참조하십시오.

구성 템플릿을 생성하고 명령을 채운 후 템플릿에서 스크립트를 생성할 수 있습니다. 스크립트를 실행하면 하나 이상의 장치에 단편(fragment) 또는 전체 구성의 형태로 구성 명령이 배포됩니다.

구성 템플릿 보기

현재 구성 템플릿을 보려면 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 구성 템플릿을 클릭합니다. 구성 템플릿 페이지가 열립니다. 이 페이지에서는 공급업체별로 정렬된 구성 템플릿 목록을 볼 수 있습니다.

구성 템플릿 페이지 필드

필드	설명/작업
새 구성 템플릿 링크	새 구성 템플릿 페이지를 엽니다. 여기서 새 구성 템플릿을 생성합니다. 자세한 내용은 706페이지의 "새 구성 템플릿 생성" 을 참조하십시오.
공급업체	이 구성 템플릿이 적용될 장치의 공급업체를 표시합니다. 공급업체 링크를 클릭하면 구성 템플릿 페이지가 열리며, 여기서 해당 공급업체에 대한 템플릿을 볼 수 있습니다. 이 페이지에서 다음 작업을 수행할 수 있습니다. <ul style="list-style-type: none"> •스크립트에 구성 템플릿을 포함시키고 이 템플릿에서 전체 스크립트를 작성합니다. •새 구성 템플릿을 생성합니다.
확인란	왼쪽의 확인란을 통해 구성 템플릿을 삭제할 수 있습니다. 템플릿을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 그러면 선택된 구성 템플릿이 삭제됩니다. 인접한 선택 드롭다운 메뉴를 통해 모든 구성 템플릿을 선택하거나 선택 취소할 수 있습니다.
이름	구성 템플릿의 이름을 표시합니다.

필드	설명/작업
파티션	<p>보안 또는 비즈니스상의 이유로 파티션을 생성한 경우 특정 파티션의 각 장치에 대해 구성 템플릿을 파티셔닝할 수 있습니다. 특정 파티션의 특정 장치뿐만 아니라 모든 파티션의 모든 장치에서 공유할 템플릿을 구성할 수 있습니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화"를 참조하십시오.</p> <p>참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다. 일반적으로 파티션이란 고유한 IP 주소를 갖는 장치의 그룹입니다. 단일 NA 코어로 여러 파티션을 관리할 수 있습니다. 설치된 NA 서버의 NA 코어는 단일 관리 엔진, 연관된 서비스 및 단일 데이터베이스로 구성되어 있습니다.</p>
역할	<p>구성 템플릿의 역할을 표시합니다. 기본 역할은 다음과 같습니다.</p> <ul style="list-style-type: none"> •모두 •코어 •테두리 •테스트
모델	이 구성 템플릿이 적용될 장치의 모델을 표시합니다.
프로세서/구성 요소	이 구성 템플릿이 적용될 장치의 프로세서를 표시합니다.
드라이버	이 구성 템플릿이 적용될 장치에 지정된 드라이버를 표시합니다.

필드	설명/작업
작업	<p>다음 옵션 중 하나를 선택할 수 있습니다.</p> <ul style="list-style-type: none">• 세부사항 보기 — 구성 템플릿 보기 페이지를 엽니다. 여기서 별도의 브라우저 창에서 HTML 형식으로 구성 템플릿을 볼 수 있습니다. 자세한 내용은 708페이지의 "구성 템플릿 보기 페이지 필드"를 참조하십시오.• 텍스트 보기 — 텍스트 창을 엽니다. 여기서 별도의 브라우저 창에서 텍스트 형식으로 구성 템플릿을 볼 수 있습니다. 자세한 내용은 708페이지의 "구성 템플릿 보기 페이지 필드"를 참조하십시오.• 편집 — 구성 템플릿 편집 페이지를 엽니다. 여기서 구성 템플릿을 추가하거나 편집할 수 있습니다. 자세한 내용은 706페이지의 "새 구성 템플릿 페이지 필드"를 참조하십시오.

새 구성 템플릿 생성

새 구성 템플릿을 생성하려면

1. 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 구성 템플릿을 클릭합니다. 구성 템플릿 페이지가 열립니다.
2. 페이지 맨 위의 새 템플릿 링크를 클릭합니다. 새 구성 템플릿 페이지가 열립니다. 완료되면 템플릿 저장 버튼을 클릭해야 합니다.

새 구성 템플릿 페이지 필드

필드	설명/작업
템플릿 링크	구성 템플릿 페이지를 엽니다. 여기서는 현재 구성 템플릿을 모두 볼 수 있습니다. 자세한 내용은 703페이지의 "구성 템플릿 보기" 를 참조하십시오.
이름	구성 템플릿의 이름을 입력합니다.
파티션	드롭다운 메뉴에서 파티션을 선택합니다. (참고: 이 필드는 하나 이상의 파티션을 구성한 경우에만 표시됩니다.) 보안 또는 비즈니스상의 이유로 파티션을 생성한 경우 특정 파티션의 각 장치에 대해 구성 템플릿을 파티셔닝할 수 있습니다. 특정 파티션의 특정 장치뿐만 아니라 모든 파티션의 모든 장치에서 공유할 템플릿을 구성할 수 있습니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
주석	구성 템플릿에 대한 설명을 입력합니다. 주석은 모든 표에 포함되므로, 중요한 정보만 입력하십시오.
역할	구성 템플릿을 위한 역할을 선택합니다. 기본 역할은 다음과 같습니다. <ul style="list-style-type: none"> •모두 •코어 •테두리 •테스트

필드	설명/작업
모델	이 구성 템플릿이 적용될 장치의 모델을 입력합니다.
프로세서/구성 요소	이 구성 템플릿이 적용될 장치의 프로세서를 입력합니다.
모드	구성 템플릿이 실행될 장치 CLI(명령줄 인터페이스) 모드를 선택합니다. (참고: 명령에서 CLI 프롬프트나 모드를 변경해서는 안 됩니다. 해당 명령에서 스크립트 실행이 중지되고 오류가 반환됩니다.)
드라이버	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 모든 해당 드라이버(기본값) • 특정 드라이버 선택 — 이 구성 템플릿이 적용될 장치에 지정된 드라이버를 선택합니다. 이 목록에는 선택된 모드와 호환되는 드라이버만 있습니다.
템플릿	구성 템플릿을 채울 구성 명령과 주석을 입력합니다. 입력한 각 행은 장치에 대한 하나의 완전한 명령이어야 합니다. 명령 입력 후에 장치 프롬프트를 다시 볼 수 있어야 합니다. 구성 템플릿이 장치에 적용될 때 이 구성이 배포됩니다. <p>변수 이름은 tc_로 시작할 수 없지만 영어 대소문자, 0 ~ 9 및 밑줄 문자의 어떤 조합도 포함할 수 있습니다.</p>

구성 템플릿 보기 페이지 필드

특정 구성 템플릿을 보려면

1. 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 구성 템플릿을 클릭합니다. 구성 템플릿 페이지가 열립니다.
2. 보려는 구성 템플릿에 대한 작업 열에서 세부사항 보기 옵션을 클릭합니다. 해당 템플릿에 대한 구성 템플릿 보기 페이지가 열립니다.

필드	설명/작업
템플릿 편집 링크	구성 템플릿 편집 페이지를 엽니다. 여기서 새 구성 템플릿을 생성할 수 있습니다. 자세한 내용은 706페이지의 "새 구성 템플릿 페이지 필드" 를 참조하십시오.
텍스트 버전 링크	텍스트 창을 엽니다. 여기서는 별도의 브라우저 창에서 텍스트 형식으로 구성 템플릿을 볼 수 있습니다. 텍스트는 다음과 같은 모양으로 표시됩니다. <pre>sflow destination \$dest_ip_1\$ \$dest_udp_port1\$ sflow destination \$dest_ip_2\$ \$dest_udp_port2\$</pre>
템플릿 링크	구성 템플릿 페이지를 엽니다. 여기서는 공급업체별로 정렬된 구성 템플릿 목록을 볼 수 있습니다. 자세한 내용은 703페이지의 "구성 템플릿 페이지 필드" 를 참조하십시오.
주석	구성 템플릿 작성자가 입력했거나 나중에 편집한 주석을 표시합니다. (참고: 채워지지 않은 주석 상자는 숨겨집니다.)
라인	각 라인의 번호가 구성 템플릿에 표시됩니다.
템플릿 텍스트	구성 템플릿을 채울 구성 명령과 주석을 표시합니다.
이름	구성 템플릿의 이름을 표시합니다.

필드	설명/작업
파티션	보안 또는 비즈니스상의 이유로 파티션을 생성한 경우 특정 파티션의 각 장치에 대해 구성을 파티셔닝할 수 있습니다. 특정 파티션의 특정 장치뿐만 아니라 모든 파티션의 모든 장치에서 공유할 템플릿을 구성할 수 있습니다. 파티션 생성에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
모델	이 구성 템플릿이 적용될 장치의 모델을 표시합니다.
마지막으로 수정한 사람	마지막으로 구성 템플릿을 수정한 사용자 또는 프로세스를 표시합니다.
역할	구성 템플릿의 역할을 표시합니다. 기본 역할은 다음과 같습니다. <ul style="list-style-type: none"> •모두 •코어 •테두리 •테스트
마지막 수정일	구성 템플릿이 마지막으로 수정된 날짜를 표시합니다.
프로세서/구성 요소	이 구성 템플릿이 적용될 장치의 프로세서를 표시합니다.
모드	구성 템플릿이 실행될 장치 CLI(명령줄 인터페이스) 모드를 표시합니다.
드라이버	이 구성 템플릿이 적용될 장치에 지정된 드라이버를 표시합니다.

710

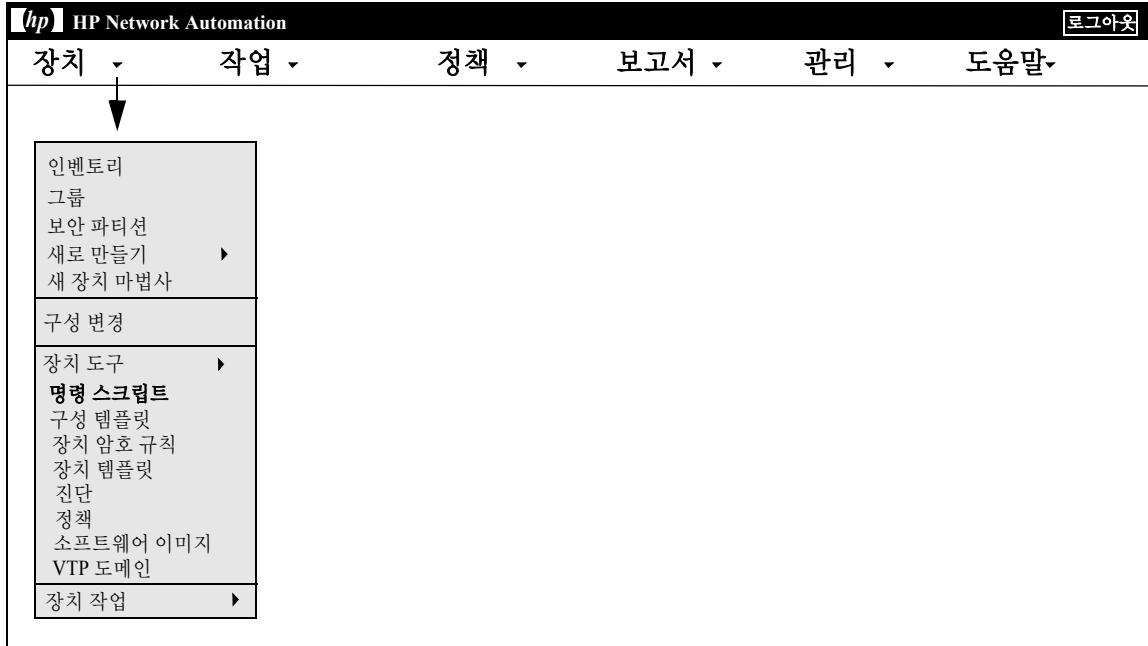
HP Network Automation 사용 설명서

15장: 명령 스크립트 관리

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	713페이지의 "시작하기"
명령 스크립트 추가 및 편집	720페이지의 "명령 스크립트 추가"
명령 스크립트 실행	738페이지의 "명령 스크립트 실행"
자동 수정 스크립트 생성	726페이지의 "자동 수정 스크립트 생성"
명령 스크립트 및 진단 가져오기/내보내기	719페이지의 "스크립트/진단 가져오기/내보내기 페이지 필드"

명령 스크립트로 이동



시작하기

하나 이상의 활성 장치에서 명령 집합을 실행하기 위해 명령 스크립트를 정의할 수 있습니다. 명령 스크립트는 특히 장치 그룹에 대한 일괄 작업에 유용합니다. 예를 들어, 인벤토리 그룹에 대해 스크립트를 실행하여 표준 정책과 일치하도록 모든 장치를 업데이트할 수 있습니다(예: SNMP 트랩 로깅 호스트, NTP 서버 또는 회사 로그인 배너 설정).

고급 스크립팅 기능을 사용하면 Expect 및 PERL 등 다양한 명령줄 언어로 작성된 사용자 지정 스크립트를 실행할 수 있습니다. 고급 스크립팅은 조건부 논리의 확장 기능을 지원합니다. 고급 스크립트는 전 기능 Expect 엔진을 지원해야 하므로 외부 텔넷/SSH 클라이언트가 별도의 프로세스로 호출되어 실행됩니다. 고급 스크립팅 기능에 대한 자세한 내용은 [722페이지의 "새 명령 스크립트 페이지 필드"](#)를 참조하십시오.

참고: 고급 스크립팅 기능을 사용하려면 언어 지원이 설치되어야 합니다. 또한 이를 사용 가능하도록 관리 설정을 구성해야 합니다. Expect 언어 지원은 NA와 함께 설치됩니다. PERL 스크립팅 기능이 있는 Windows 환경에서 PERL(CPAN)을 설치해야 합니다.

HP OO(HP Operations Orchestration) 흐름

고급 명령 스크립트를 통해 HP OO(HP Operations Orchestration) 흐름을 실행하려면

1. HP Operations Orchestration 인증 설정이 올바르게 구성되어 있는지 확인합니다. 자세한 내용은 [97페이지의 "사용자 인증"](#)을 참조하십시오.
2. 고급 스크립팅 상자를 선택하고 흐름을 언어로 선택합니다. 고급 스크립팅은 NA에 흐름 언어 유형을 사용하도록 지시합니다. 그렇지 않으면 NA는 IOS와 같은 구문을 장치 구문으로 해석합니다.
3. 스크립트 필드에 `/PAS/services/http/execute/Library/<path to flow>?flowvariable=value,flowvariable2=value2`를 입력합니다.

참고: 여전히 필요에 따라 명령 스크립트 변수와 임의 개수의 HP OO 흐름 입력 변수를 사용할 수 있습니다. HP OO 사용에 대한 자세한 내용은 *HP Operations Orchestration Software Development Kit Guide*를 참조하십시오.

Bare Metal 프로비전 스크립트

Bare metal 프로비전 스크립트를 사용하면 bare metal 장치를 NA 장치 드라이버에서 액세스할 수 있는 상태로 지정할 수 있습니다. bare metal 스크립트 생성은 표준 명령 스크립트 생성과 동일합니다. 모든 사용자 지정 스크립트 변수를 bare metal 스크립트에서 사용할 수 있습니다. 그러나 bare metal 스크립트를 생성할 때는 다음을 수행해야 합니다.

- Bare Metal 스크립트를 스크립트 유형으로 선택
- Bare Metal 모드 중 하나 선택
- 스크립트가 실행되도록 지정된 장치 제품군을 비롯한 명령 스크립트에 적합한 이름 지정

참고: Bare Metal 스크립트 유형을 선택할 때 고급 스크립팅을 사용할 수 있지만 "고급 스크립트" 확인란을 선택하지 않는 것이 좋습니다.

bare metal 프로비전에 대한 자세한 내용은 [146페이지의 "장치 편집 페이지 필드"](#)를 참조하십시오.

일반적인 bare metal 스크립트 시나리오는 다음과 같습니다.

1. 장치를 랙에 마운트합니다.
2. 장치(또는 관리 IP 주소)에 대한 콘솔 액세스를 설정합니다.
3. NA에 로그인합니다.
4. 장치 아래의 메뉴 모음에서 새로 만들기를 선택하고 장치를 클릭합니다. 새 장치 페이지가 열립니다. NA에 장치를 추가하는 방법에 대한 자세한 내용은 [137페이지의 "장치 추가"](#)를 참조하십시오.
5. 다음 정보와 함께 장치를 NA에 추가합니다.
 - IP 주소
 - 호스트 이름
 - 암호
 - 콘솔 주소/포트(장치가 액세스 가능한 관리 IP 주소로 구성되지 않은 경우)
 - 기타 적합한 장치 필드
6. 사전 프로덕션의 관리 상태를 선택합니다.
7. 이 장치에 대해 bare metal 드라이버를 지정합니다.

8. 장치를 저장합니다. 장치 세부사항 페이지가 열립니다.
9. 프로비전 메뉴에서 명령 스크립트 실행을 클릭합니다. 명령 스크립트 실행 페이지가 열립니다. 이 페이지는 bare metal 스크립트 목록으로 자동으로 채워집니다. **738페이지의 "명령 스크립트 실행"**을 참조하십시오.
10. 장치에 적합한 bare metal 스크립트를 선택하고 필요한 경우 스크립트 변수에 대한 값을 제공합니다.
11. 스크립트를 실행합니다. 명령 스크립트 실행 페이지에서 "드라이버 검색 작업 실행" 옵션을 활성화한 경우 스크립트 실행에 성공하면 검색 작업이 자동으로 예약됩니다. 필요한 경우 이 옵션을 비활성화할 수 있습니다.
12. 검색 작업에 성공하면 장치가 bare metal 스크립트에서 사전 프로덕션 장치로 이동합니다.

다음은 Cisco 2800 장치에 대한 샘플 bare metal 스크립트입니다.

```
#scriptvar.carriage_return="\r"
#scriptvar.command_delay="3"
#scriptvar.baremetal_timeout="5"
#scriptvar.success_pattern=/Building configuration/
yes
yes
$tc_device_hostname$
$tc_device_password$
$legacy_enable_password$
$tc_device_enable_password$
no
FastEthernet0/0
yes
no
yes
$tc_device_ip$
$network_mask$
2
```

bare metal 스크립트를 생성할 때는 다음 사항에 주의해야 합니다.

- bare metal 스크립트 맨 위에서 일부 스크립트 설정(모두 선택 사항)을 정의하도록 선택할 수 있습니다. 이러한 라인은 항상 `#scriptvar`로 시작됩니다.
- `Carriage_return`은 각 명령에 대해 장치로 전송되는 줄 바꿈의 형식을 정의합니다. 여기에는 `\r`, `\n`, `\r\n` 또는 `none`(각 명령 후 줄 바꿈이 전송되지 않음)이 사용될 수 있습니다.
- `Command_delay`는 NA가 스크립트에 있는 장치로 다음 명령을 전송할 때까지의 대기 시간(초)을 정의합니다.
- `Baremetal_timeout`은 명령에 대한 Expect 제한 시간을 정의합니다.
- `Success_pattern`은 정규 표현식 패턴을 정의합니다. 유효한 성공 패턴을 지정하면 해당 패턴이 장치 출력과 일치하는 경우에만 작업이 성공한 것으로 간주됩니다.

명령 스크립트 보기

사전 정의된 명령 스크립트와 사용자 지정 명령 스크립트의 목록을 보려면 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 명령 스크립트를 클릭합니다. 명령 스크립트 페이지가 열립니다. 사용자에게 권한이 있는 명령 스크립트의 목록이 페이지에 표시됩니다. 명령 스크립트에 대한 전체 액세스 권한이 있는 사용자에게는 NA와 함께 제공되는, 사전 정의 스크립트가 표시되어 선택할 수 있습니다.

명령 스크립트 페이지 필드

필드	설명/작업
새 명령 스크립트 링크	새 명령 스크립트 페이지를 엽니다. 여기서 프롬프트 정의를 위한 새 스크립트와 스크립트의 pull 변수를 작성할 수 있습니다. 자세한 내용은 722페이지의 "새 명령 스크립트 페이지 필드" 를 참조하십시오.
명령 스크립트 실행 링크	명령 스크립트 실행 작업 페이지를 엽니다. 여기서 명령 스크립트를 실행하기 위한 작업을 설정할 수 있습니다. 작업을 저장하기 전에 스크립트의 변수를 편집하여 해당 스크립트의 고유한 인스턴스를 생성할 수 있습니다. 자세한 내용은 389페이지의 "명령 스크립트 실행 작업 페이지 필드" 를 참조하십시오.
명령 스크립트 가져오기/내보내기 링크	미리 구성된 명령 스크립트를 가져오거나 명령 스크립트를 파일로 내보낼 수 있는 명령 스크립트/진단 가져오기/내보내기 페이지를 엽니다. 자세한 내용은 719페이지의 "스크립트/진단 가져오기/내보내기 페이지 필드" 를 참조하십시오.
스크립트 유형	스크립트 유형 드롭다운 메뉴에서는 특정 유형의 스크립트만 표시하도록 스크립트 목록을 필터링할 수 있습니다.
확인란	왼쪽의 확인란을 통해 스크립트를 삭제할 수 있습니다. 스크립트를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 그러면 선택된 스크립트가 삭제됩니다. 인접한 선택 드롭다운 메뉴를 통해 모든 스크립트를 선택하거나 선택 취소할 수 있습니다.
스크립트 이름	스크립트의 이름을 표시합니다.

필드	설명/작업
모드/장치 제품군	스크립트가 실행되는 장치 액세스 모드(예: Cisco Exec, Nortel Manager)를 표시합니다. 장치 제품군이 고급 스크립팅에 사용되며, 비슷한 구성 CLI 명령 구문을 공유하는 장치의 모음을 표시합니다.
마지막 수정일	스크립트가 마지막으로 수정된 날짜와 시간을 표시합니다.
파티션	명령 스크립트 및/또는 진단을 특정 파티션에 적용할 수 있습니다. "전역"이라는 레이블이 붙은 명령 스크립트 및/또는 진단은 모든 파티션에 적용되므로 모든 사용자가 볼 수 있습니다. 참고: NA 관리자가 장치를 파티셔닝한 경우에는 보기 권한이 있는 특정 파티션에 속하는 명령 스크립트 및/또는 진단만 보고 편집하며 실행할 수 있습니다. 장치 및 사용자 세분화에 대한 자세한 내용은 191 페이지의 "장치 및 사용자 세분화" 를 참조하십시오.
마지막으로 수정한 사람	스크립트를 마지막으로 수정한 사용자의 이름을 표시합니다. 예를 들어, 스크립트가 스크립트 템플릿인 경우 이 필드는 특정 인스턴스에 대해 스크립트를 수정한 사람을 표시합니다.
작업	다음 옵션 중 하나를 선택할 수 있습니다. <ul style="list-style-type: none"> • 편집 — 명령 스크립트 편집 페이지를 엽니다. 여기서 기존의 스크립트를 수정할 수 있습니다. 자세한 내용은 722페이지의 "새 명령 스크립트 페이지 필드"를 참조하십시오. • 실행 — 명령 스크립트 실행 작업 페이지를 엽니다. 여기서 명령 스크립트를 실행할 수 있습니다. 자세한 내용은 389페이지의 "명령 스크립트 실행 작업 페이지 필드"를 참조하십시오.

스크립트/진단 가져오기/내보내기 페이지 필드

명령 스크립트 페이지에서 명령 스크립트 가져오기/내보내기 링크를 클릭하면 스크립트/진단 가져오기/내보내기 페이지가 열립니다.

필드	설명/작업
가져오기	가져올 명령 스크립트나 진단 스크립트를 선택하거나 찾아보기 버튼을 클릭하여 명령 스크립트나 진단 스크립트를 찾습니다. 명령 스크립트나 진단 스크립트가 표시되면 가져오기 버튼을 클릭합니다. 명령 스크립트나 진단 스크립트가 이미 있으면 이름을 바꾸라는 메시지가 표시됩니다.
스크립트/진단 내보내기	현재 명령 스크립트 및 진단 스크립트 목록을 표시합니다. 내보낼 스크립트를 클릭한 다음 내보내기 버튼을 클릭합니다.

명령 스크립트 추가

명령 스크립트를 사용하여 다음을 수행할 수 있습니다.

- 하나 이상의 장치에서 사용자 지정 명령 집합을 실행합니다.
- 예약된 작업으로 스크립트를 실행하고 이벤트 규칙을 사용하여 스크립트 실행을 트리거합니다. 예를 들어, 특정 유형의 장치가 추가될 때마다 그 장치 유형에 표준 설정을 구성하도록 규칙을 설정할 수 있습니다.

NA는 스크립트 추가를 위한 몇 가지 옵션을 제공합니다. 다음을 수행할 수 있습니다.

- 새 명령 스크립트 페이지에 스크립트를 작성하거나 복사하면서 필요에 따라 변수를 추가하거나 프롬프트를 정의합니다.
- 스크립트를 실행하기 전에 사용자가 변수 값을 편집할 수 있는 템플릿 스크립트를 작성합니다. 자세한 내용은 [739페이지의 "구성 템플릿에서 스크립트 생성"](#)을 참조하십시오.
- 세션 로그를 Expect 또는 Perl 스크립트로 변환합니다. NA에서 Expect를 설치하기 때문에 Expect 스크립트로 변환 링크는 자동으로 사용 가능해집니다. Perl 스크립트로 변환 링크는 관리 설정에서 Perl이 스크립팅 언어로 구성된 경우에만 표시됩니다. 자세한 내용은 [68페이지의 "서버 페이지 필드"](#)를 참조하십시오. Perl 스크립트로 변환 링크를 사용하려면 NA가 설치될 때 설치되는 `Opware::NA::Connect Perl` 모듈이 필요합니다.

NA는 단순 및 고급 스크립팅을 모두 지원합니다.

단순 스크립팅은 모드 기반입니다(CLI 명령 언어). 단순 명령 스크립트에서는 장치 CLI 오류를 인식하지 않습니다. 따라서 NA에서는 실행된 장치 CLI 명령이 성공적이었다고 가정합니다. 단순 명령 스크립트는 장치에 연결할 수 없거나 스크립트 실행 중에 장치와의 연결이 끊긴 경우에만 실패합니다.

고급 스크립팅은 조건부 논리(*if*, *while* 및 *for* 조건)를 포함하는 스크립트를 비롯하여 Expect, PERL과 같은 명령줄 스크립팅 언어를 기반으로 합니다. 변수를 포함시켜 스크립트의 인스턴스를 사용자 지정할 수 있습니다. 스크립트를 실행할 때 각 변수의 값을 묻는 프롬프트가 나타납니다. 자세한 내용은 다음 표를 참조하십시오.

참고: '\$' 문자는 변수 이름용으로 예약되었습니다. 스크립트에 상수 '\$'를 입력해야 할 경우 이스케이프 시퀀스 `\x24`를 사용하십시오.

단순 스크립트	고급 스크립트
<ul style="list-style-type: none"> • if 또는 루프 없음 • 장치 명령 사용(<i>show conf</i>와 같은 Cisco 명령) • 오류 처리 없음 • 로그인 필요 없음 • NA 장치 변수 없음 	<ul style="list-style-type: none"> • If 및 루프 허용 • 언어 명령(<i>send "show conf\n"</i> 또는 <i>print SOCKET "show conf\n"</i>과 같은 PERL 또는 Expect 명령) 사용 • 오류 처리 가능 • 로그인 코드 필요 • NA 장치 변수에 액세스 가능

스크립트를 사용하여 여러 장치 유형에 동일한 작업을 수행할 수 있습니다. 동일한 이름으로 여러 개의 스크립트를 생성하여 해당 이름의 모든 스크립트가 단일 작업처럼 실행되게 합니다. 장치는 장치 그룹으로 구성되어야 합니다. 스크립트를 실행할 때 해당 그룹의 장치에 적용되는 스크립트의 모든 인스턴스가 표시됩니다. 예를 들어, 모든 라우터에서 NTP 서버를 변경하기 위해(다른 공급업체의 라우터인 경우도 포함) 스크립트를 실행할 수 있습니다. 동일한 이름의 여러 스크립트를 실행할 때 스크립트의 각 인스턴스를 편집할 수 있습니다.

새 명령 스크립트를 추가하려면

1. 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 명령 스크립트를 클릭합니다. 명령 스크립트 페이지가 열립니다.
2. 페이지 맨 위의 새 명령 스크립트 링크를 클릭합니다. 새 명령 스크립트 페이지가 열립니다. 완료되면 스크립트 저장을 클릭해야 합니다. 스크립트가 성공적으로 저장되면 명령 스크립트 페이지가 열립니다. 추가한 스크립트가 목록에 나타나고 강조 표시됩니다. 스크립트는 작업으로 예약될 때까지 실행되지 않습니다.

참고: "tc_"로 시작하는 변수는 특수한 용도로 예약된 것입니다. 사용자 지정 또는 고급 스크립트에서 이 문자 시퀀스로 시작하는 변수를 정의할 수 없습니다.

새 명령 스크립트 페이지 필드

명령 스크립트를 사용하여 다음을 수행할 수 있습니다.

- 하나 이상의 장치에서 사용자 지정 명령 집합을 실행합니다.
- 예약된 작업으로 스크립트를 실행하고 이벤트 규칙을 사용하여 스크립트 실행을 트리거합니다. 예를 들어, 특정 유형의 장치가 추가될 때마다 그 장치 유형에 표준 설정을 구성하도록 규칙을 설정할 수 있습니다.

명령 스크립트를 생성할 때 `$MyVar$`와 같은 사용자 지정 변수를 직접 정의할 수 있습니다. 사용자 지정 변수는 명령 스크립트 실행 작업 페이지에서 사용자가 제공한 변수로 표시됩니다.

사용자 지정 변수를 CSV 파일로 제공하려는 경우 기존의 `scriptField1`, `scriptField2`와 같은 헤더를 스크립트의 사용자 지정 변수로 대체할 수 있습니다. 그러면 명령 스크립트를 실행할 때, 스크립트의 사용자 지정 변수(CSV 파일에서도 참조됨)가 명령 스크립트 실행 작업 페이지의 작업 옵션/변수 필드에서 CSV 데이터 파일로 제공됨으로 표시됩니다.

스크립트에 정의되었으나 CSV 파일에서 참조되지 않는 모든 사용자 지정 변수는 사용자 입력용으로 표시됩니다. 자세한 내용은 [389페이지의 "명령 스크립트 실행 작업 페이지 필드"](#)를 참조하십시오.

필드	설명/작업
명령 스크립트 링크	명령 스크립트 페이지를 엽니다. 여기서 명령 스크립트의 목록을 볼 수 있습니다. 자세한 내용은 717페이지의 "명령 스크립트 페이지 필드" 를 참조하십시오.
이름	새 스크립트의 이름을 입력합니다.
설명	스크립트에 대한 설명(템플릿에서 생성되었는지 여부, 생성한 사람 등)을 입력합니다.
파티션	스크립트 및/또는 진단을 특정 파티션에 적용하거나 전역으로 적용할 수 있습니다. "전역"이라는 레이블이 붙은 스크립트 및/또는 진단은 모든 파티션에 적용되므로 모든 사용자가 볼 수 있습니다. 드롭다운 메뉴에서 특정 파티션을 선택할 수 있습니다.
	참고: NA 관리자가 장치를 파티셔닝한 경우에는 보기 권한이 있는 특정 파티션에 속하는 스크립트 및/또는 진단만 보고 편집하며 실행할 수 있습니다. 장치 및 사용자 세분화에 대한 자세한 내용은 191페이지의 "장치 및 사용자 세분화" 를 참조하십시오.

필드	설명/작업
스크립트 유형	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none">• 일반 목적(기본값)• 기존 — 드롭다운 메뉴에서 스크립트를 선택합니다.• 새로 만들기 — 새 스크립트 유형을 입력합니다.

필드	설명/작업
고급 스크립팅	<p>이 옵션을 선택하면 페이지가 새로 고쳐져 Expert, PERL과 같은 명령줄 언어로 작성된 사용자 지정 스크립트 특정 설정을 제공합니다. 고급 스크립팅 특정 필드는 다음과 같습니다.</p> <ul style="list-style-type: none"> • 장치 제품군 — 장치 제품군은 유사한 구성 CLI 명령 구문을 공유하는 장치의 모음입니다. 장치 제품군을 하나 선택합니다. 그러면 스크립트는 선택된 장치 제품군에 속한 드라이버의 장치에 대해서만 실행되도록 제한됩니다. 이 기능을 사용하면 서로 다른 장치를 위해 생성된 스크립트의 여러 구현에 하나의 이름을 지정하여 이들이 단일 작업으로 실행되게 할 수 있습니다. • 언어 — 추가하려는 스크립트가 작성된 스크립팅 언어를 선택합니다. 이 기능을 사용하려면 언어 지원을 설치하고 관리 설정/서버/고급 스크립팅에서 언어를 구성해야 합니다. Expect, Perl 및 흐름과 같은 옵션이 있습니다. (참고: Expect 지원은 NA와 함께 설치되지만 역시 경로를 구성해야 합니다.) 흐름에 대한 자세한 내용은 101페이지의 "HP OO(HP Operations Orchestration)" 을 참조하십시오. • 매개 변수 — 스크립트의 인증 매개 변수를 입력합니다. NA 또는 사용자 지정 변수를 포함시킬 수 있습니다. (참고: 인증용 매개 변수를 사용하는 것이 좋습니다. 이 전략은 파일에 암호를 기록하는 데 따르는 보안 위험을 줄여 줍니다.) • 스크립트 — 고급 스크립팅 언어는 조건부 논리를 포함하고 사전 정의된 변수를 포함할 수 있습니다. 변수 이름에는 문자, 숫자 및 밑줄(_)만 사용할 수 있습니다. 필요한 형식은 \$report\$, \$my_address\$, \$port_3_ip\$와 같이 두 개의 달러 기호(\$) 사이에 변수 이름이 들어간 것입니다. 고급 스크립트에는 장치에 연결하여 로그인하는 데 필요한 모든 코드가 포함되어야 합니다. 예를 들어, \$tc_device_ip\$에 연결하고 \$tc_device_password\$를 사용하여 로그인할 수 있습니다. • 장치 변수 링크 — 고급 사용자 지정 스크립트에서 사용할 수 있는 장치 변수의 목록을 표시합니다. 이 변수는 항상 \$tc_로 시작하며, 이름에서 대소문자를 구별합니다. (사용자가 직접 변수를 생성할 수도 있음) • Pull 변수 버튼 — 스크립트에 사용된 변수별로 입력 필드를 페이지 맨 아래에 추가하면서 페이지를 새로 고칩니다. 변수를 위한 사용자 지정 프롬프트를 정의하고 각 프롬프트에서 허용하는 값을 제한할 때 이 필드를 사용합니다. 변수별로 다음 옵션을 선택할 수 있습니다. <ul style="list-style-type: none"> - 값에 라인을 여러 개 허용합니다. - 값을 다음으로 제한: (첫 번째, 마지막, 끝에서 두 번째) - 암호(이 옵션을 선택하면 NA는 명령 스크립트 실행 작업 페이지에서 값 프롬프트가 표시될 때 암호를 에코하지 않음)

필드	설명/작업
모드	Cisco Exec 또는 Nortel Manager와 같은 장치 액세스 모드를 선택합니다.
드라이버	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 모든 해당 드라이버(기본값) • 특정 드라이버 선택 — 목록에서 하나 이상의 드라이버를 선택할 경우 드라이버 하나를 클릭하거나 Shift 또는 Ctrl 키와 함께 클릭하여 여러 개의 드라이버를 선택할 수 있습니다. (참고: Baystack 470과 같은 메뉴 기반 장치는 사용자 지정 스크립트로 액세스할 수 없습니다.)
스크립트	장치에 보낼 장치별 명령을 입력하거나 기존 스크립트를 붙여넣고 편집합니다. 명령을 입력하는 방법에 대해서는 명령 스크립트 페이지 도움말 정보를 참조하십시오. <p>참고: 변수 이름은 tc_(NA용으로 예약됨)로 시작할 수 없지만 영어 대소문자, 0 ~ 9 및 밑줄 문자의 어떤 조합도 포함할 수 있습니다.</p>
Pull 변수 버튼	스크립트에 사용되는 변수별로 입력 필드를 페이지 맨 아래에 추가하면서 페이지를 새로 고칩니다. 변수를 위한 사용자 지정 프롬프트를 정의하고 각 프롬프트에서 허용하는 값을 제한할 때 이 필드를 사용합니다. 다음은 샘플 필드입니다. <ul style="list-style-type: none"> • HOSTNAME • ETH_SLOT1 <p>이 스크립트가 실행될 때 사용자가 응답할 사용자 지정 프롬프트 그리고 이 프롬프트에서 허용할 응답 값을 입력합니다. 값은 심표로 구분해야 하므로, 심표가 포함된 값은 사용할 수 없습니다. 여러 개의 값을 지정하는 경우, 사용자에게 프롬프트가 표시될 때 허용되는 값의 목록이 프롬프트 대화 상자에 제공됩니다.</p>

자동 수정 스크립트 생성

자동 수정 스크립트를 사용하면 위반된 정책 규칙의 정규 표현식 패턴 그룹에서 데이터를 참조하는 변수를 스크립트에 정의할 수 있습니다. 자동 수정 변수는 비정규 표현식 패턴에서도 사용할 수 있습니다.

자동 수정 스크립트는 표준 명령 스크립트와 다릅니다. 복잡한 정책을 정의할 수 있도록 하려는 경우 사전 처리 단계에서 장치에서 실행될 실제 명령 스크립트를 생성할 수 있도록 하려면 자동 수정 스크립트에 for-loop 및 if-statements와 같은 기본 언어 구성이 있어야 합니다.

자동 수정 스크립트에는 일치하는 항목을 반복할 수 있는 구문이 있습니다. 자동 수정 스크립트는 정규 표현식 변수 대체를 통해 명령 스크립트로 변환됩니다. 템플릿 프로세서(명령 스크립트 생성기)에서는 실행 파일 명령 스크립트를 구문 분석하고 생성한 다음 자동 수정 작업을 통해 실행합니다.

새로운 자동 수정 스크립트를 추가하려면 [518페이지의 "새 규칙 페이지 필드"](#)를 참조하십시오.

자동 수정 스크립트 구문

NA에는 위반 데이터에 액세스할 수 있는 새로운 자동 수정 스크립트 구문이 포함되어 있습니다. 다음 표에서는 자동 수정 스크립트에 사용된 스크립팅 언어 요소에 대해 설명합니다.

언어 요소	설명
@foreach	일치하는 라인을 반복하는 루프 구문입니다.
@ifexists	변수에 일치하는 항목이 있는지 여부를 테스트하는 구문을 제어합니다.
@end	@foreach 또는 @ifexists의 끝을 나타냅니다.
\$loop_variable\$	정규 표현식 패턴 라인의 일치하는 항목을 조건에서 반복하는 데 사용할 변수 이름입니다.
\$line_match_variable\$	조건의 정규 표현식 패턴 라인에 일치하는 구성 라인의 배열을 나타냅니다. 예를 들어 조건 A의 첫 번째 라인에 일치하는 구성 라인은 \$condition_A_line_1\$입니다.

언어 요소	설명
<code>\$regex_group_match_variable\$</code>	정규 표현식 그룹에 일치하는 텍스트를 나타냅니다.
<code>@</code>	장치 명령에서 자동 수정 언어 요소를 구분하기 위한 자동 수정 언어 요소의 접두사입니다.
<code>//</code>	자동 수정 스크립트에서 라인을 주석 처리하는 접두사입니다.

자동 수정 스크립트 변수 명명 규칙

다음 표에서는 자동 수정 스크립트 명명 규칙에 대해 설명합니다.

변수	명명 규칙	예
루프	<code>\$any_string\$</code>	<code>\$interface\$</code> — 정규 표현식 패턴과 일치하는 각 구성 라인입니다.
정규 표현식 패턴의 라인에 일치하는 항목을 나타내는 패턴 라인 일치	<code>\$condition_<label>_line_<number>\$</code>	<code>\$condition_A_line_2</code> — 조건 A의 두 번째 라인에 일치하는 구성 라인입니다.
정규 표현식 그룹 일치	<code>\$<loop_variable>.regex_group_<number>\$</code>	<code>\$interface.regex_group_1\$</code> — 정규 표현식 패턴에 일치하는 구성 라인의 첫 번째 정규 표현식 그룹에 일치하는 항목입니다. <ul style="list-style-type: none"> 숫자 = 0: 전체 일치 숫자 > 0: 정규 표현식 캡처 그룹
블록 시작 패턴	<code>\$block_start\$</code>	블록 시작 패턴에 대한 기본 제공 변수 이름입니다.

변수	명명 규칙	예
블록 끝 패턴	<code>\$block_end\$</code>	블록 끝 패턴에 대한 기본 제공 변수 이름입니다.

참고:

- `@foreach $loop_variable$ in $line_match_variable$`, 여기서 `$loop_variable$`은 `$line_match_variable$`(조건에 있는 정규 표현식 패턴의 라인에 일치하는 항목의 배열)에서 일치하는 각 라인을 나타내는 데 사용됩니다. 예를 들어 `$condition_A_line_1$`은 조건 A의 첫 번째 라인에 일치하는 모든 구성 라인을 나타내는 일치 변수입니다.
- `@ifexists $regex_group_match_variable$`, 여기서 `$regex_group_match_variable$`은 정규 표현식 그룹에 일치하는 항목을 나타내는 데 사용됩니다.
- 중첩된 `@foreach` 루프가 허용됩니다.
- 블록 시작 및 끝 패턴은 `$block_start$` 및 `$block_end$` 배열 변수로 액세스할 수 있습니다. 639 페이지의 예 3을 참조하십시오.
- 정규 표현식 그룹은 괄호로 둘러싸인 정규 표현식 패턴의 일부입니다. 예를 들어 `interface (.*)` 패턴에서 `(.*)`는 정규 표현식 그룹(캡처 그룹이라고도 함)입니다.
- 위반 데이터는 "포함하지 않아야 함" 및 "다음만 포함해야 함" 연산자에 사용할 수 있습니다. 위반은 "포함해야 함" 연산자를 사용하는 패턴에 일치하는 항목이 없을 때 발생하므로 "포함해야 함" 연산자에 대한 위반 데이터는 없습니다. 자동 수정 스크립트는 변수 참조 없이도 작성할 수 있습니다. 따라서 자동 수정 스크립트 구문 요소가 사용되지 않습니다.
- 자동 수정 변수는 비정규 표현식 패턴에서 사용할 수 있습니다. 따라서 정규 표현식 그룹 변수가 없습니다. 전체 일치 항목은 그룹 0(영) 변수(예: `$matching_line.regex_group_0$`, 여기서 `$matching_line$`은 `@foreach` 루프 변수임)로 액세스할 수 있습니다.

- 자동 수정 작업은 명령 스크립트 실행 작업으로 실행됩니다. 그러나 실제로 장치에서는 명령 스크립트 실행 작업을 예약하기 전에 자동 수정 스크립트 사전 처리 엔진에서 생성한 명령 스크립트가 실행됩니다. 명령 스크립트 실행에 대한 자세한 내용은 [389페이지의 "명령 스크립트 실행 작업 페이지 필드"](#)를 참조하십시오.
- 자동 수정 스크립트는 구성 관리 페이지의 "구성 정책 확인" 섹션에서 활성화되어야 합니다. 자세한 내용은 [42페이지의 "구성 관리"](#)를 참조하십시오.

자동 수정 스크립트 예

예 1: 위반 데이터 없음(가장 간단한 케이스)

가장 간단한 자동 수정 스크립트는 결과에서 위반 데이터를 생성하지 않기 때문에 "포함해야 함" 연산자와 함께 사용됩니다. 따라서 스크립트에는 자동 수정 스크립트 구문이 필요하지 않습니다.

다음과 같이 패턴이 정규 표현식이 아니라는 조건을 가정합니다.

```
Condition A: Config Text
must contain
ntp server 169.243.103.34
ntp server 170.242.62.16
ntp server 170.242.62.17
ntp server 169.243.226.94
```

구성 텍스트에서 패턴에 라인을 포함하지 않으면 조건 A가 위반됩니다. 위반을 해결하기 위해 다음 자동 수정 스크립트에서는 구성에 라인을 삽입합니다.

```
Script:
ntp server 169.243.103.34
ntp server 170.242.62.16
ntp server 170.242.62.17
ntp server 169.243.226.94
```

위에서 설명한 대로 스크립트에서 자동 수정 스크립트 구문을 사용할 필요가 없습니다.

예 2: 위반 데이터

다음 예에서는 위반 데이터 참조에서 자동 수정을 사용하는 방법을 보여 줍니다. 이것은 예일 뿐이며 실제로는 사용되지 않습니다.

두 개의 정규 표현식 패턴 라인이 포함된 아래의 조건에 대해 구성의 다음 줄을 확인한다고 가정합니다.

Configuration text:

```
...
access-list 139 deny ip host 192.168.139.1 any
access-list 139 deny ip host 192.168.139.2 any
access-list 139 permit ip any any
...
```

Condition A: Config Text

must not contain

```
access-list (.*) deny ip host (.*) any
access-list (.*) permit (192\.0\.0\..*)
```

위의 구성 텍스트에서 다음 줄은 조건을 위반합니다.

```
access-list 139 deny ip host 192.168.139.1 any
access-list 139 deny ip host 192.168.139.2 any
```

두 라인은 조건 A의 첫 번째 패턴 라인과 일치되므로 `$condition_A_line_1$` 배열 변수에 배치됩니다. 일치되는 라인의 굵게 표시된 텍스트는 정규 표현식 그룹에 일치되므로 정규 표현식 그룹 일치 변수로 참조될 수 있습니다.

자동 수정 변수는 @foreach 루프 내에서만 액세스할 수 있습니다. 각 패턴 라인은 여러 구성 라인과 일치될 수 있으므로 일치되는 라인은 루프 내에서 반복됩니다. 조건 A의 첫 번째 패턴 라인과 일치되는 위의 두 라인에 액세스하려면 @foreach 루프 구문을 사용하십시오.

```
@foreach $matching_line$ in $condition_A_line_1$
    ...
@end
```

위 라인은 \$matching_line\$ 루프 변수를 사용하여 \$condition_A_line_1\$의 배열 변수(패턴 라인 일치 변수)에 배치된 일치되는 각 구성 라인에 액세스할 수 있다는 의미입니다.

\$matching_line\$ 루프 변수를 사용하여 자동 수정 스크립트는 루프가 반복될 때마다 일치되는 하나의 라인에 액세스할 수 있습니다. 일치되는 라인 및 정규 표현식 그룹의 해당 부분은 위의 @foreach 루프에서 다음과 같이 루프 변수를 통해 액세스합니다.

```
$matching_line.regex_group_0$
$matching_line.regex_group_1$
$matching_line.regex_group_2$
```

그룹 0(\$matching_line.regex_group_0\$)에 대한 변수는 일치하는 전체 구성 라인을 포함하지만 다른 그룹(그룹 1과 2)은 괄호 내에 정의된 정규 표현식 그룹을 포함합니다. 따라서 첫 번째 루프 반복의 변수에 대한 값은 다음과 같습니다.

```
$matching_line.regex_group_0$: access-list 139 deny ip host 192.168.139.1 any
$matching_line.regex_group_1$: 139
$matching_line.regex_group_2$: 192.168.139.1
```

예를 들어 다음 자동 수정 스크립트에서 위반을 수정한다고 가정합니다.

```
@foreach $matching_line$ in $condition_A_line_1$
  no $matching_line.regex_group_0$
  access-list 100 permit $matching_line.regex_group_2$ any
@end
```

@foreach 루프 내의 각 라인은 장치에서 실행될 명령입니다. 이 예에서 첫 번째 라인 (no <line>)은 장치의 구성 텍스트에서 라인을 제거하지만 두 번째 라인은 장치의 구성 텍스트에 라인을 삽입합니다.

샘플 자동 수정 스크립트에서 두 개의 변수 참조 \$matching_line.regex_group_0\$ 및 \$matching_line.regex_group_2\$가 사용됩니다. 준수 확인 후 정책 관리자에서 이 자동 수정 스크립트를 실행하면 다음과 같은 명령 스크립트가 생성되고 장치에서 실행되도록 예약됩니다.

```
no access-list 139 deny ip host 192.168.139.1 any
access-list 100 permit 192.168.139.1
no access-list 139 deny ip host 192.168.139.2 any
access-list 100 permit 192.168.139.2
```

예 3: 블록

조건 패턴의 블록 및 일치 항목을 반복하려면 블록 기반 조건에 중첩된 루프가 있어야 합니다. 다음 정책 규칙 정의에 블록 시작/끝 패턴과 하나의 블록 텍스트 조건이 포함되어 있다고 가정합니다.

```
Configuration text:
...
interface Ethernet0/0
  description New York LAN Back Bone
  ip address 10.16.241.1 255.255.255.224
  no ip mroute-cache
  half-duplex
!
interface Ethernet0/1
  description Chicago LAN Back Bone
  ip address 10.1.1.1 255.255.255.252
  half-duplex
!
...

Block Start: interface (.*)
Block End:   !

Condition A: Config Block
must not contain
  ip address (10\..*)\s(.*)
```

위 조건의 위반 데이터에 액세스하는 데 사용된 @foreach 루프는 다음과 같습니다.

```
@foreach $matching_line$ in $condition_A_line_1$
  no $matching_line.regex_group_0$
@end
```

그러나 조건 A와 일치하는 항목은 블록으로 구성됩니다. 위의 @foreach 루프는 \$condition_A_line_1\$ 배열에서 일치 항목이 있는 블록을 인식하지 못합니다. 따라서 조건 패턴을 블록에 대한 @foreach 루프로 다음과 같이 둘러싸야 합니다.

```
@foreach $matching_block$ in $block_start$
  @foreach $matching_line$ in $condition_A_line_1$
    interface $matching_block.regex_group_1$
      no $matching_line.regex_group_0$
  @end
@end
```

생성된 명령 스크립트는 다음과 같습니다.

```
interface Ethernet0/0
no ip address 10.16.241.1 255.255.255.224
interface Ethernet0/1
no ip address 10.1.1.1 255.255.255.252
```

예 4: 다음만 포함해야 함 연산자

"다음만 포함해야 함" 연산자에는 다음과 같은 두 가지 패턴이 있습니다.

- 첫 번째 패턴에서는 포함되어야 하는 구성 텍스트를 정의합니다.
- 두 번째 패턴에서는 첫 번째 패턴과 일치하는 항목을 제외하고 포함되어서는 안 되는 구성 텍스트를 정의합니다.

위반 데이터는 두 번째 패턴에 대해 생성됩니다. 예를 들면 다음과 같습니다.

```
Condition A: ConfigText
must contain only:
  Must contain these lines:
    ntp server 169\.243\.103\.34
    ntp server 170\.242\.62\.16
    ntp server 170\.242\.62\.17
    ntp server 169\.243\.226\.94
  But must not have any additional lines containing:
    ntp server(.*)
```

다음과 같은 두 가지 위반이 발생할 수 있습니다.

1. "이 라인을 포함해야 함" 패턴의 모든 라인이 구성 텍스트와 일치하지 않습니다. 이런 경우에는 원하는 라인이 없어서 위반이 발생하므로 위반 데이터가 생성되지 않습니다.
2. `ntp server(.*)` 패턴과 일치하는 구성 텍스트 라인이 "이 라인을 포함해야 함" 패턴의 라인과 일치하지 않습니다. 이런 경우에는 위반 데이터가 있습니다. 위반 데이터는 `$condition_A_line_1$` array 변수를 통해 액세스할 수 있습니다.

가능한 위반을 해결하는 자동 수정 스크립트는 다음과 같이 표시됩니다.

```
ntp server 169.243.103.34
ntp server 170.242.62.16
ntp server 170.242.62.17
ntp server 169.243.226.94

@foreach $matching_line$ in $condition_A_line_1$
  no ntp server $matching_line.regex_group_1$
@end
```

처음 네 라인을 통해 구성 텍스트는 "이 라인을 포함해야 함" 패턴에 라인을 정의할 수 있습니다. `@foreach` 루프는 위반의 원인이 된 `ntp server(.*)`와 일치하는 모든 라인을 제거합니다.

예 5: `@ifexists` 명령문

일치하는 텍스트가 없는 그룹이 정규 표현식에 포함될 수 있습니다. 따라서 이러한 그룹을 참조하는 변수에는 저장된 값이 없을 수 있습니다. 예를 들면 다음과 같습니다.

```
logging ((10\.1\..*)|(172\.1\..*))
```

정규 표현식 그룹:

```
Group 0: logging ((10\.1\.*)|(172\.1\.*))
Group 1: ((10\.1\.*)|(172\.1\.*))
Group 2: (10\.1\.*)
Group 3: (172\.1\.*)
```

그룹 2 또는 3의 IP 주소에 대한 정규 표현식 캡처 그룹 중 하나에 값이 없습니다.
위의 정규 표현식 패턴에 다음 조건을 사용한다고 가정합니다.

```
Condition A: Config Text
must not contain
  logging ((10\.1\.*)|(172\.1\.*))
```

위의 위반 데이터에 액세스하는 자동 수정 스크립트는 `@ifexists` 명령문을 사용하여 그룹 2 및 3에 대한 캡처 그룹 변수에 사용할 수 있는 위반 데이터가 있는지 여부를 테스트합니다. 그렇지 않으면 자동 수정 스크립트에서 값이 없는 캡처 그룹 변수에 액세스하려고 할 때 명령 스크립트가 생성되지 않습니다.

자동 수정 스크립트는 다음과 같이 표시됩니다.

```
@foreach $matching_line$ in $condition_A_line_1$
  @ifexists $matching_line.regex_group_2$
    no logging $matching_line.regex_group_2$
  @end
  @ifexists $matching_line.regex_group_3$
    no logging $matching_line.regex_group_3$
  @end
@end
```


예 6: 여러 조건

다음 예에서는 여러 조건을 보여 줍니다.

```
Block Start: interface (.*)
Block End:   !

Condition A: Config Block
must not contain
  ip address (10\..*)\s(.*)

Condition B: Config Text
must contain only:
  Must contain these lines:
    ntp server 169\.243\.103\.34
    ntp server 170\.242\.62\.16
    ntp server 170\.242\.62\.17
    ntp server 169\.243\.226\.94

But must not have any additional lines containing:
  ntp server(.*)

Logic: A AND B
```

자동 수정 스크립트는 다음과 같이 표시됩니다.

```
@foreach $matching_block$ in $block_start$
  @foreach $matching_line$ in $condition_A_line_1$
    interface $matching_block.regex_group_1$
    no $matching_line.regex_group_0$
  @end
@end

ntp server 169.243.103.34
ntp server 170.242.62.16
ntp server 170.242.62.17
ntp server 169.243.226.94

@foreach $matching_line$ in $condition_B_line_1$
  no ntp server $matching_line.regex_group_1$
@end
```

명령 스크립트 실행

명령 스크립트의 인스턴스를 실행하고 편집하는 작업은 사용자의 권한에 의해 제한됩니다. 제한된 권한의 사용자인 경우 그리고 전체 권한 사용자 또는 파워 사용자이지만 장치 수정 권한이 없는 경우에는 스크립트를 실행할 수 없습니다.

스크립트가 한 번, 사용자 정의 간격에 따라 정기적으로 또는 반복적인 작업으로 실행되게 설정할 수 있습니다. 또한 특정 시간에 또는 가능한 빨리 작업이 시작되도록 예약할 수 있습니다. 스크립트 실행에 앞서 스크립트를 편집하고 변수 값을 제공할 수 있습니다.

명령 스크립트 페이지에서 스크립트를 실행하려면

1. 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 명령 스크립트를 클릭합니다. 명령 스크립트 페이지가 열립니다.
2. 실행하려는 스크립트의 이름을 선택합니다.
3. 작업 열에서 실행을 클릭합니다. 명령 스크립트 실행 작업 페이지가 열립니다. 자세한 내용은 [389페이지의 "명령 스크립트 실행 작업 페이지 필드"](#)를 참조하십시오.

참고: 또한 작업 메뉴에서 명령 스크립트를 실행할 수도 있습니다.

구성 템플릿에서 스크립트 생성

구성 템플릿에서 스크립트를 생성하려면

1. 장치 아래의 메뉴 모음에서 장치 도구를 선택하고 구성 템플릿을 클릭합니다. 구성 템플릿 페이지가 열립니다. **703페이지의 "구성 템플릿 페이지 필드"**를 참조하십시오.
2. 공급업체 링크를 클릭합니다. 해당 공급업체의 구성 템플릿 페이지가 열립니다.
3. 스크립트에 포함할 구성 템플릿을 선택하고 스크립트 업데이트를 클릭합니다.
4. 필요한 경우 스크립트를 편집하고, 스크립트 생성 버튼을 클릭하여 장치에 배포 가능한 스크립트를 생성합니다. 템플릿에서 스크립트 저장 페이지가 열립니다.
5. 이름, 설명 및 그 밖의 필드를 편집합니다. 변수 이름은 "tc_"로 시작할 수 없습니다. 그러나 영어 대소문자, 0 ~ 9 및 밑줄 문자의 어떤 조합도 포함할 수 있습니다.
6. 스크립트 저장을 클릭합니다. 명령 스크립트 페이지가 열립니다. 새 스크립트가 강조 표시됩니다.

740

HP Network Automation 사용 설명서

16장: 보고서

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

보고서	참조
시작하기	743페이지의 "시작하기"
사용자 및 시스템 보고서	744페이지의 "사용자 및 시스템 보고서"
네트워크 상태 보고서	748페이지의 "네트워크 상태 보고서"
모범 사례 보고서	752페이지의 "모범 사례 보고서"
장치 상태 보고서	755페이지의 "장치 상태 보고서"
통계 대시보드	757페이지의 "통계 대시보드"
다이어그램 작성	758페이지의 "다이어그램 작성"
장치 소프트웨어 보고서	770페이지의 "장치 소프트웨어 보고서"
소프트웨어 수준 보고서	772페이지의 "소프트웨어 수준 보고서 필드"
소프트웨어 취약점 보고서	774페이지의 "소프트웨어 취약점 보고서"
이미지 동기화 보고서	776페이지의 "이미지 동기화 보고서 필드"
시스템 및 네트워크 이벤트 보고서	778페이지의 "시스템 및 네트워크 이벤트 보고서"
소프트웨어 취약점 이벤트 세부사항 보고서	780페이지의 "소프트웨어 취약점 이벤트 세부사항 보고서"
요약 보고서	782페이지의 "요약 보고서"
전자 메일 보고서	786페이지의 "전자 메일 보고서"

보고서 탐색

HP Network Automation 로그아웃

장치 ▾ 작업 ▾ 정책 ▾ **보고서 ▾** 관리 ▾ 도움말 ▾

↓

<ul style="list-style-type: none"> 단일 보기 단일 검색
사용자 및 시스템 보고서
<ul style="list-style-type: none"> 검색 대상 ▶ 고급 검색
준수 센터
<ul style="list-style-type: none"> 네트워크 상태 모범 사례 장치 상태 통계 대시보드 다이어그램 작성
<ul style="list-style-type: none"> 장치 소프트웨어 소프트웨어 취약점 이미지 동기화 보고서
시스템 및 네트워크 이벤트
<ul style="list-style-type: none"> 요약 보고서 보고서 작업 ▶ <ul style="list-style-type: none"> 요약 보고서 생성 전자 메일 보고서

시작하기

HP Network Automation(NA)에서는 입력이 필요하지 않은 기본 보고서와 임시 보고서가 모두 제공됩니다. 기본 보고서에는 다음이 포함됩니다.

- 사용자 및 시스템 보고서
- 대시보드 보고서
- 요약 보고서
- 모범 사례 보고서
- 네트워크 상태 보고서
- 구성 보고서
- 장치 상태 보고서
- 소프트웨어 취약점 보고서
- 작업 보고서
- 텔넷/SSH 사용자 세션 로그 보고서
- 준수 센터 보고서

임시 보고서에서는 NA 내의 데이터에 대해 보고하기 위한 유연성 및 제어를 제공합니다. 임시 보고서는 하나 이상의 필드에 대해 정규 표현식 기준을 기반으로 하여 수동 또는 자동으로 생성될 수 있습니다. 공통 임시 보고서에는 다음이 포함될 수 있습니다.

- IOS 12.* 버전을 실행하는 모든 Cisco 장치
- 구성 관리에 대해 안전하지 않은 프로토콜을 사용하는 모든 장치
- 모듈에 결함이 있는 모든 장치
- 장치 집합에 대해 일정 기간 동안 작성된 모든 구성 변경 사항
- 특정 사용자에게 의해 시작된 모든 텔넷/SSH 세션 로그
- 승인 오버라이드로 인한 모든 장치 변경 사항
- 특정 포트에서 트래픽을 거부하는 모든 ACL

사용자 및 시스템 보고서

사용자 및 시스템 보고서는 검색 기능을 사용하여 정의하고 저장한 검색 결과입니다. 정의한 검색만 사용자 보고서의 목록에 나타납니다. 검색할 수 있는 항목은 다음과 같습니다.

- 장치
- 인터페이스
- 모듈
- 구성
- 진단
- 정책
- 준수
- 작업
- 세션
- 이벤트
- 사용자
- ACL
- IP 주소
- MAC 주소
- VLAN

검색 수행에 대한 자세한 내용은 [583페이지의 "장치 검색"](#)을 참조하십시오.

각 보고서에는 검색에 사용되는 기준에 대한 요약이 포함되어 있습니다. 저장된 검색은 사용자 및 NA 관리자만 사용할 수 있습니다.

참고: 검색을 실행 및 저장할 수 없는 경우 사용자 보고서를 사용할 수 없습니다.

시스템에서는 미리 정의된 쿼리에 대해 보고합니다. 쿼리는 보고서를 선택하면 생성됩니다. 각 보고서에는 검색에 사용되는 기준에 대한 요약이 포함되어 있습니다. 시스템 보고서에는 다음이 포함됩니다.

- | | |
|--------|--|
| 구성 | <ul style="list-style-type: none">• 최근 12시간 동안 작성된 모든 변경 사항• 최근 24시간 동안 작성된 모든 변경 사항• 최근 48시간 동안 작성된 모든 변경 사항• 지난 주에 작성된 모든 변경 사항• 지난 달에 작성된 모든 변경 사항• 최근 48시간 동안 직접 작성한 모든 변경 사항 |
| 정책 이벤트 | 지난 24시간 동안 정책 규칙 위반 |
| 장치 | <ul style="list-style-type: none">• 최근 24시간 동안 변경된 모든 장치• 지난 주에 변경된 모든 장치• 액세스가 실패한 모든 장치• 모든 비활성 장치(참고: 비활성 장치를 삭제하지 않고 구성 이력을 유지하도록 비활성으로 지정할 수 있음)• 모든 중복 IP 주소• 드라이버가 할당되지 않은 모든 장치• 드라이버가 할당되어 있지만 구성이 저장되지 않은 모든 장치• 여러 개의 시작 및 실행 구성이 있는 모든 장치 |

중복 IP	<p>모든 중복 IP 주소 — 이 보고서는 동일한 IP 주소로 구성되는 인터페이스가 있는 장치를 표시합니다. 하지만, 중복 감지를 초래하는 IP 주소를 제거하지 않습니다.</p> <p>IP 유형은 IP 주소가 추가되었거나 사용된 방식입니다. 이 열에 대한 값은 다음과 같습니다.</p> <ol style="list-style-type: none"> 1 — 수동(수동으로 추가된 IP 주소) 2 — NAT(네트워크 주소 변환, 사용자 정의 네트워크 주소 변환된 IP 주소) 3 — 포트에서 기본(포트의 기본 IP 주소) 4 — 포트에서 보조(포트의 보조 IP 주소) 5 — 장치에 TFTP(TFTP를 통해 장치에 액세스하기 위한 IP 주소) 6 — 장치에서 기본(장치에 액세스하기 위해 사용되는 기본 IP 주소) 7 — 콘솔(장치에 콘솔 액세스를 위한 IP 주소)
세션	<ul style="list-style-type: none"> • 최근 24시간 동안 생성된 모든 세션 • 최근 48시간 동안 생성된 모든 세션 • 지난 주에 생성된 모든 세션 • 최근 48시간 동안 직접 생성한 모든 세션
소프트웨어 수준	<ul style="list-style-type: none"> • 장치 소프트웨어 수준
작업	<ul style="list-style-type: none"> • 최근 24시간 동안 발생한 모든 실패한 작업, 건너뛴 작업 및 중복된 작업 • 지난 주에 발생한 모든 실패한 작업, 건너뛴 작업 및 중복된 작업

- 기타
- 모범 사례 보고서
 - 네트워크 상태 보고서
 - 장치 상태 보고서
 - COSO 준수 상태
 - COBIT 준수 상태
 - GLBA 준수 상태

사용자 및 시스템 보고서를 보려면 보고서 아래의 메뉴 모음에서 사용자 및 시스템 보고서를 클릭하십시오. 사용자 및 시스템 보고서 페이지가 열립니다.

사용자 및 시스템 보고서 필드

필드	설명/작업
유형	이벤트 또는 보고서 유형을 표시합니다.
보고서	장치 상태, HIPAA 준수 상태, 모든 비활성 장치 등과 같은 보고서 이름을 표시합니다. 보고서를 클릭하면 보고서가 열립니다.
작업	<p>선택할 수 있는 작업은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 전자 메일 보고서 — 전자 메일을 통해 보고서 출력을 보내는 작업을 생성할 수 있는 전자 메일 보고서 양식을 표시합니다. 수신자를 지정할 수 있습니다. 사용자 로그인은 기본입니다. 전자 메일 메시지를 생성할 작업을 저장해야 합니다. • 수정 — 사용자 보고서에 대해 이벤트 옵션 수정을 클릭할 수 있습니다. 이벤트 검색 페이지가 열립니다. • 시스템 보고서로 표시 — 사용자 보고서에 대해 시스템 보고서로 표시를 클릭할 수 있습니다. 보고서가 시스템 보고서 섹션으로 이동됩니다. • 삭제(빨강 X 아이콘) — 보고서를 영구적으로 삭제합니다. • 목록에서 보고서를 위 또는 아래로 이동하려면 위쪽 또는 아래쪽 화살표를 클릭합니다.

네트워크 상태 보고서

네트워크 상태 보고서에서는 다음과 같은 두 개의 네트워크의 독립 보기와 함께 네트워크 구성, 상태 및 준수에 대한 개요를 제공합니다.

- 모범 사례
- 장치 상태

네트워크 상태 보고서에는 사전 준비 보고 기능이 제공됩니다. 반복되는 전자 메일 보고서 작업으로 실행되도록 보고서를 예약함으로써, 네트워크 관리자 및 엔지니어는 네트워크에 영향을 미치기 전에 문제를 제거할 수 있도록 해주는 최신 정보를 자동으로 받습니다. 또한 네트워크 상태 보고서에는 정책 및 소프트웨어 수준 문제를 해결하고 구성 변경 사항을 처리하는 데 있어 네트워크 운영의 효율성 대한 개요와 함께 관리를 제공할 수 있습니다.

참고: 이 보고서에 대한 기본 구성은 인벤토리 장치 그룹에 대해 실행하는 작업입니다.

이벤트는 네트워크에 도입된 세 가지 티어로 구분된 위험 표시를 기준으로 보고됩니다. 시스템 관리자는 네트워크에 미치는 영향을 반영하기 위해 각 범주에 대한 임계값을 설정하고 위험 수준 표시기 색상을 할당합니다.

- 빨강 — 위험도 높음(기타 노랑 수준의 이벤트와 결합된 정책 위반, 소프트웨어 수준 위반 및 장치 액세스 실패 등)
- 노랑 — 위험도 중간(시작과 실행 구성 불일치 및 장치 액세스 실패 등)
- 녹색 — 임계값 이내 또는 위험도 낮음. 이는 모범 사례입니다.

장치 그룹 상태는 그룹에 있는 장치의 최고 위험 조건을 기준으로 하며, 네트워크 상태는 네트워크에 있는 그룹의 최고 위험 조건을 기반으로 합니다.

네트워크 상태 보고서를 보려면 보고서 아래의 메뉴 모음에서 네트워크 상태를 클릭합니다. 보고서 페이지의 다시 실행 버튼을 사용하여 요청 시 이 보고서를 실행하거나, 전자 메일 보고서 옵션을 사용하여 주요 네트워크 및 관리 직원에게 이 보고서를 메일로 전송하고 작업으로 실행할 수 있도록 보고서를 예약할 수 있습니다. 전자 메일 보고서에 대한 자세한 내용은 [786페이지의 "전자 메일 보고서"](#)를 참조하십시오.

네트워크 상태 보고서 필드

필드	설명/작업
모범 사례 보고서 링크	모범 사례 보고서를 엽니다. 752페이지의 "모범 사례 보고서" 를 참조하십시오.
장치 상태 보고서 링크	장치 상태 보고서를 엽니다. 755페이지의 "장치 상태 보고서" 를 참조하십시오.
보고서 날짜	보고서를 마지막으로 실행한 날짜 및 시간을 표시합니다.
보고된 장치 그룹 수	보고된 장치 그룹의 수를 표시합니다.
장치 그룹 변경	현재 정의된 장치 그룹의 목록을 표시합니다. 단일 장치 그룹 또는 여러 장치 그룹에 대해 네트워크 상태 보고서를 실행할 수 있습니다. 다른 매개 변수가 모두 미리 정의됩니다. 요약 및 세부사항 정보가 지정한 각 장치 그룹에 대해 범주별로 제공됩니다. 완료되면 다시 실행 버튼을 클릭합니다.
상태	장치 그룹의 이름 및 그룹에 있는 장치의 수를 표시합니다.
장치 상태	
장치 상태	<p>발견된 문제점(백분율)이 상태 수준 표시기로 표시됩니다. 상태 수준은 다음과 같습니다.</p> <ul style="list-style-type: none"> •빨강 — 위험도 높음 •노랑 — 위험도 중간 •녹색 — 위험도 낮음 <p>장치 상태를 클릭하면 장치 상태 보고서가 열립니다. 755페이지의 "장치 상태 보고서"를 참조하십시오.</p>

필드	설명/작업
모범 사례 상태	
문제	<p>다음에 포함하여 NA에서 추적하는 5가지 주요 네트워크 문제를 표시합니다.</p> <ul style="list-style-type: none"> • 정책 규칙 위반 — 정의된 구성 정책을 하나 이상 준수하지 않는 장치. 자세한 내용을 보려면 커서를 정보 아이콘 위로 이동하십시오. • 24시간 내 소프트웨어 수준 위반 — 미승인 소프트웨어 버전이 실행 중인 장치. 자세한 내용을 보려면 커서를 정보 아이콘 위로 이동하십시오. • 시작 구성과 실행 구성 간 불일치 — 시작 및 실행 구성이 일치하지 않는 장치. 자세한 내용을 보려면 커서를 정보 아이콘 위로 이동하십시오. • 장치 액세스 실패 — NA에서 연결할 수 없는 장치. 자세한 내용을 보려면 커서를 정보 아이콘 위로 이동하십시오. • 24시간 내 구성 변경 — 지난 24시간 동안 감지된 장치 구성 변경. 자세한 내용을 보려면 커서를 정보 아이콘 위로 이동하십시오. <p>각 문제에 대해 사용할 수 있는 작업 링크가 다릅니다. 예를 들어, 모든 보고된 장치 액세스 실패에 대해 링크를 클릭하면 실패한 작업을 식별할 수 있는 장치 세부사항 작업 옵션 보기를 볼 수 있습니다. 시작 구성과 실행 구성 간 불일치에 대해 링크를 클릭하면 차이가 있는 구성을 강조 표시하는 시작과 실행 비교 옵션을 볼 수 있습니다.</p> <p>모범 사례 상태를 클릭하면 모범 사례 보고서가 열립니다. 752페이지의 "모범 사례 보고서"를 참조하십시오.</p>

필드	설명/작업
네트워크 상태 보고서 세부사항	
위험도 높음(빨강) 문제	<p>빨강 상태가 반환된 5가지 문제에 대해 요약 정보를 표시합니다. 각 문제에 대해 사용할 수 있는 작업 링크가 다릅니다. 예를 들면 다음과 같습니다.</p> <ul style="list-style-type: none">• 모든 보고된 장치 액세스 실패 — 실패한 작업을 식별할 수 있는 장치 세부사항 작업 옵션 보기를 보려면 클릭합니다.• 정책 규칙 위반 — 하나 이상의 구성 정책에 포함된 구성 규칙을 장치 구성이 준수하지 않는지 표시하는 이벤트를 볼 수 있는 구성 정책 활동 페이지를 보려면 클릭합니다. 정책 중요도 열에 표시된 값은 장치가 현재 위반한 모든 구성 규칙 중 최고 중요도입니다.• 시작 구성과 실행 구성 간 불일치 — 구성을 모두 표시하는 시작과 실행 비교 옵션을 보려면 클릭합니다. 모든 차이는 강조 표시됩니다.

모범 사례 보고서

네트워크 관리에 대한 모범 사례에서는 다음 문제가 있는 미준수 항목에 대해 주의해서 모니터링해야 함을 보여 줍니다.

- 24시간 내 정책 규칙 위반
- 소프트웨어 수준 위반
- 시작 구성과 실행 구성 간 불일치
- 장치 액세스 실패
- 24시간 내 구성 변경

NA를 사용하면 이러한 각 문제에 대해 허용 가능한 미준수 수준을 정의할 수 있습니다. 임계값을 초과한 경우 미준수 수준에 따라 노랑 또는 빨강 경고가 표시됩니다. 또한 NA는 준수하지 못한 장치를 표시하여 수정 작업을 할 수 있도록 합니다.

모든 5가지 표시기가 녹색인 경우에는 NA가 네트워크를 평가하고 상태가 양호하다고 확인했음을 나타냅니다. 일부 표시기가 노랑으로 표시되면 이 부분은 수정 작업의 대상이 됩니다. 일부 표시기가 빨강으로 표시되면 플래그가 지정된 문제에서 네트워크 안정성에 대해 심각한 위험으로 표시될 수 있으며 이에 대해 즉각적인 주의가 필요합니다.

모범 사례 보고서를 보려면 보고서 아래의 메뉴 모음에서 모범 사례를 클릭합니다. 모범 사례 보고서가 열립니다.

참고: 네트워크 상태 보고서뿐만 아니라 모범 사례 보고서도 탐색할 수 있습니다.

모범 사례 보고서 필드

필드	설명/작업
네트워크 상태 보고서 링크	네트워크 상태 보고서를 엽니다. 748페이지의 "네트워크 상태 보고서" 를 참조하십시오.
장치 상태 보고서 링크	장치 상태 보고서를 엽니다. 755페이지의 "장치 상태 보고서" 를 참조하십시오.
보고서 날짜	보고서를 마지막으로 실행한 날짜 및 시간을 표시합니다.
보고된 장치 그룹 수	보고된 장치 그룹의 수를 표시합니다.
장치 그룹 변경	현재 정의된 그룹의 목록을 표시합니다. 단일 그룹 또는 여러 그룹에 대해 모범 사례 보고서를 실행할 수 있습니다. 다른 매개 변수가 모두 미리 정의됩니다. 요약 및 세부사항 정보가 지정한 각 그룹에 대해 범주별로 제공됩니다. 완료되면 다시 실행 버튼을 클릭합니다.
상태	<p>그룹의 이름 및 그룹에 있는 장치의 수를 표시합니다. 상태 수준은 다음과 같습니다.</p> <ul style="list-style-type: none"> •빨강 — 위험도 높음 •노랑 — 위험도 중간 •녹색 — 임계값 이내
문제	<p>다음에 포함하여 NA에서 추적하는 5가지 주요 네트워크 문제를 표시합니다.</p> <ul style="list-style-type: none"> •24시간 내 정책 규칙 위반 — 정의된 구성 정책을 하나 이상 준수하지 않는 장치. 자세한 내용을 보려면 커서를 정보 아이콘 위로 이동하십시오. •소프트웨어 수준 위반 — 미승인 소프트웨어 버전이 실행 중인 장치. 자세한 내용을 보려면 커서를 정보 아이콘 위로 이동하십시오. •시작 구성과 실행 구성 간 불일치 — 시작 및 실행 구성이 일치하지 않는 장치. 자세한 내용을 보려면 커서를 정보 아이콘 위로 이동하십시오. •장치 액세스 실패 — NA에서 연결할 수 없는 장치. 자세한 내용을 보려면 커서를 정보 아이콘 위로 이동하십시오. •24시간 내 구성 변경 — 지난 24시간 동안 감지된 장치 구성 변경. 자세한 내용을 보려면 커서를 정보 아이콘 위로 이동하십시오.

필드	설명/작업
모범 사례 보고서 세부사항	
위험도 높음(빨강) 문제	빨강 상태가 반환된 5가지 문제에 대해 요약 정보를 표시합니다. 각 문제에 대해 사용할 수 있는 작업 링크가 다릅니다. 예를 들어, 모든 보고된 장치 액세스 실패에 대해 링크를 클릭하면 실패한 작업을 식별할 수 있는 장치 세부사항 작업 옵션 보기를 볼 수 있습니다. 시작 구성과 실행 구성 간 불일치에 대해 링크를 클릭하면 구성을 모두 표시하는 시작과 실행 비교 옵션을 볼 수 있습니다. 모든 차이는 강조 표시됩니다.

장치 상태 보고서

장치 상태 보고서에서는 네트워크에 있는 모든 장치를 나열하고 각 모범 사례 문제에 대해 개별적으로 분석합니다. 각 모범 사례 문제에 대한 자세한 내용은 [749페이지의 "네트워크 상태 보고서 필드"](#)를 참조하십시오.

하나 이상의 문제를 준수하지 않은 각 장치는 노랑 또는 빨강 경고로 플래그가 지정됩니다. 또한 보고서에는 노랑 또는 빨강 경고를 생성한 장치 수를 표시하는 전체 네트워크가 요약되어 있습니다.

장치 상태 보고서를 보려면 보고서 아래의 메뉴 모음에서 장치 상태를 클릭합니다. 장치 상태 보고서가 열립니다.

참고: 네트워크 상태 보고서 또는 모범 사례 보고서뿐만 아니라 장치 상태 보고서도 탐색할 수 있습니다.

장치 상태 보고서 필드

필드	설명/작업
네트워크 상태 보고서 링크	네트워크 상태 보고서를 엽니다. 748페이지의 "네트워크 상태 보고서" 를 참조하십시오.
모범 사례 보고서 링크	모범 사례 보고서를 엽니다. 752페이지의 "모범 사례 보고서" 를 참조하십시오.
보고서 날짜	보고서를 마지막으로 실행한 날짜 및 시간을 표시합니다.
보고된 장치 그룹 수	보고된 장치 그룹의 수를 표시합니다.
장치 그룹 변경	현재 정의된 그룹의 목록을 표시합니다. 단일 그룹 또는 여러 그룹에 대해 모범 사례 보고서를 실행할 수 있습니다. 다른 매개 변수가 모두 미리 정의됩니다. 요약 및 세부사항 정보가 지정한 각 그룹에 대해 범주별로 제공됩니다. 완료되면 다시 실행 버튼을 클릭합니다.
상태	그룹의 이름 및 그룹에 있는 장치의 수를 표시합니다. 상태 수준은 다음과 같습니다. <ul style="list-style-type: none">•빨강 — 위험도 높음•노랑 — 위험도 중간•녹색 — 임계값 이내

필드	설명/작업
장치 상태 보고서 세부사항	
위험도 중간(노랑) 및 위험도 높음(빨강) 문제	노랑 또는 빨강 상태가 반환된 5가지 문제에 대해 요약 정보를 표시합니다. 각 문제에 대해 사용할 수 있는 작업 링크가 다릅니다. 예를 들어, 24시간 내 모든 보고된 구성 변경에 대해 구성 보기 링크를 클릭하면 해당 장치에 대한 구성 정보를 볼 수 있습니다. 장치 액세스 실패에 대해 실패한 작업을 식별할 수 있는 장치 작업 보기 링크를 클릭할 수 있습니다.

통계 대시보드

통계 대시보드를 보려면 보고서 아래의 메뉴 모음에서 통계 대시보드를 클릭합니다. 통계 대시보드가 열립니다. 통계 대시보드에서는 다음 보고서에 대한 정보를 제공합니다.

- 공급업체 상위 5개 — 자세한 내용은 [782페이지의 "요약 보고서"](#)를 참조하십시오.
- OS 공급업체 상위 5개 — 자세한 내용은 [782페이지의 "요약 보고서"](#)를 참조하십시오.
- 구성 변경 수 - 최근 7일간 — 자세한 내용은 [744페이지의 "사용자 및 시스템 보고서"](#)를 참조하십시오.
- 시간대별 변경 이력 — 자세한 내용은 [782페이지의 "요약 보고서"](#)를 참조하십시오.
- 가장 많이 액세스한 장치 상위 10개 — 자세한 내용은 [782페이지의 "요약 보고서"](#)를 참조하십시오.
- 시스템 상태 — 자세한 내용은 [748페이지의 "네트워크 상태 보고서"](#)를 참조하십시오.
- 소프트웨어 수준 — 자세한 내용은 [782페이지의 "요약 보고서"](#)를 참조하십시오.
- 구성 정책 준수 — 자세한 내용은 [782페이지의 "요약 보고서"](#)를 참조하십시오.

다이어그램 작성

다이어그램 작성을 수행하면 네트워크 장치에서 토폴로지 데이터를 수집할 수 있습니다. 네트워크 다이어그램은 Visio, 정적 JPEG 또는 대화식 JPEG 형식 및 인쇄물로 볼 수 있습니다. 레이어 3 IP 주소와 서브넷, MAC 주소와 VLAN에 걸쳐 있는 레이어 2 세부 사항을 포함하여 토폴로지 데이터에서는 현재 네트워크 상태의 스냅샷을 제공합니다.

VLAN 부분에서, 지정된 VLAN과 연관된 포트는 VLAN 상자에서 가져옵니다. 해당되는 경우 Cisco VTP(VLAN Trunking Protocol) 도메인 정보도 표시됩니다. 모든 집계된 포트와 함께, 집계된 포트 이름을 나열하는 연관된 포트 채널에 대한 주석이 표시되지 않습니다. VLAN에 대한 자세한 내용은 [278페이지의 "VLAN\(가상 로컬 영역 네트워크\)"](#)을 참조하십시오.

레이어 3 데이터에는 장치 구성 파일에서 가져온 IP 주소가 포함되어 있습니다. 레이어 2 데이터는 각 장치 인터페이스의 MAC 주소와, 장치에 표시되는 MAC 주소를 표시하는 MAC 테이블의 데이터와 관련됩니다. NA는 동일한 네트워크에 있다는 이유로 서로 통신할 수 있는 장치를 매핑합니다.

사용자는 레이어 1(물리적 케이블) 연결을 감지할 수 있습니다. 레이어 1 연결은 레이어 2 데이터(스위치에 의해 표시되는 MAC 주소)에서 추론되고 캡처된 다음 NA 데이터베이스에 추가됩니다. NA의 레이어 1 다이어그램 유형은 HP SA에서와 동일한 연결을 표시합니다. 자세한 내용은 *HP Server Automation User's Guide*를 참조하십시오.

추론되는 레이어 1 데이터는 발견을 기반으로 합니다. NA는 네트워크 다이어그램을 더 쉽게 읽을 수 있도록 장치 및/또는 서버 사이의 데이터 링크 연결 수를 줄입니다. 종속적인 연결을 통해 추론할 수 있는 연결만 감소됩니다.

OSI 모델에 있는 각 레이어는 그 아래에 있는 레이어를 숨기도록 추상적으로 설계되어 있습니다. 따라서, 장치에서 수집된 레이어 2 데이터는 100% 정확한 레이어 1 데이터를 생성할 수 없습니다. 특히 레이어 1 데이터는 다음 상황에 해당하는 경우 잘못될 수 있습니다.

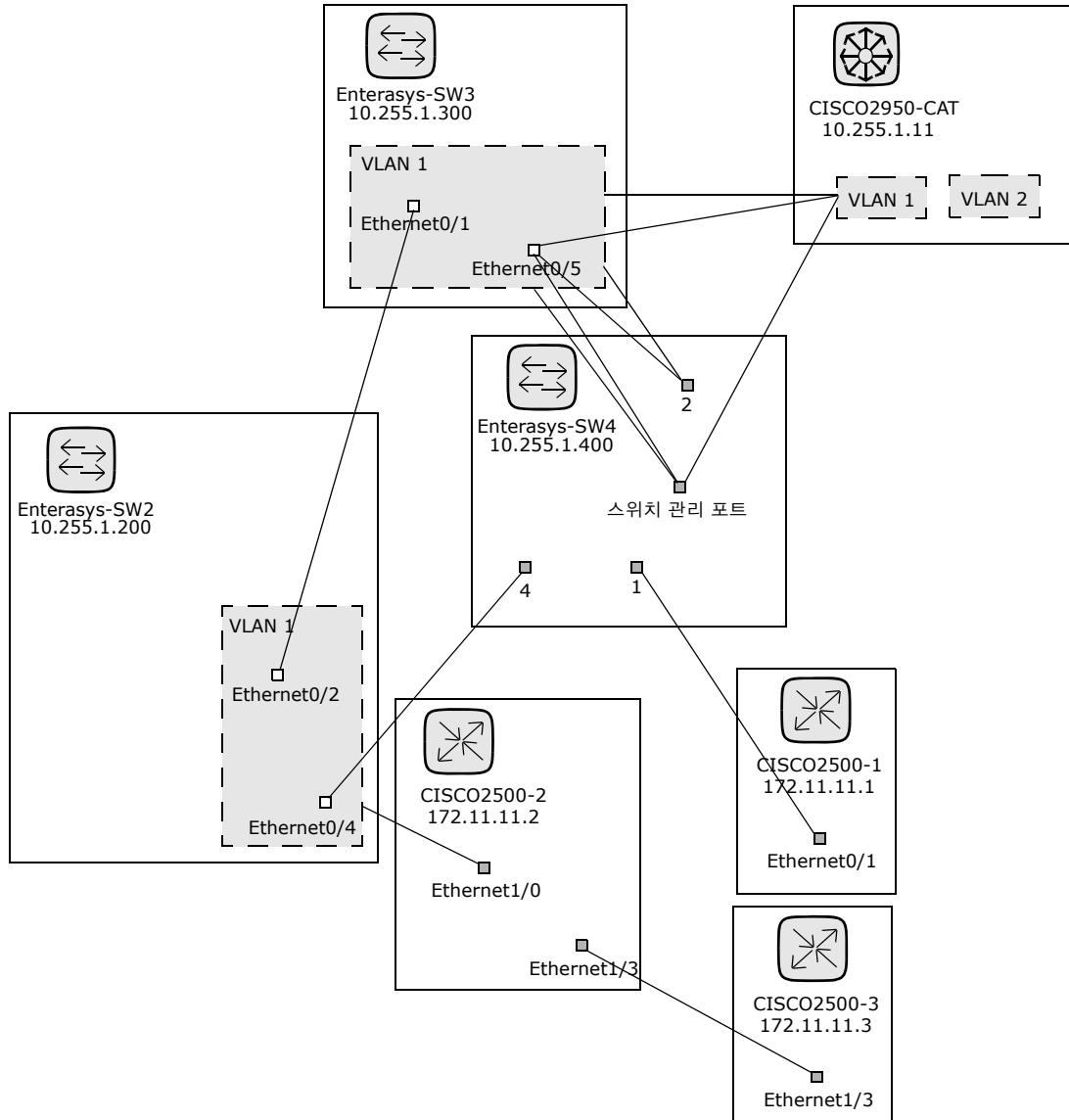
- MAC 주소가 표시되어 있는 인터페이스 수가 장치에서 반환되지 않습니다.
- NA에서 토폴로지 데이터(MAC 주소가 표시되어 있음)를 수집하는 몇 분 동안 장치 간 트래픽이 없었습니다.
- 2개의 관리되는 장치 간에 허브와 같이 주소가 지정되지 않은 장치가 있습니다.

다음과 같은 색상, 테두리, 라인 및 아이콘이 다이어그램에서 사용됩니다.

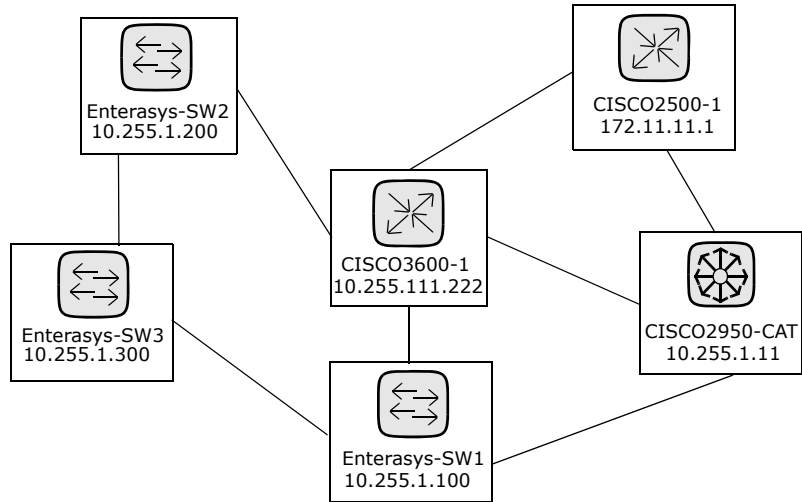
- 빨강 — 스냅샷 작업 또는 다른 작업의 결과로 장치의 마지막 액세스가 실패했습니다. (참고: VLAN 및 포트에 대해 빨강은 관리 목적으로 VLAN이 중지됨을 나타내고 회색은 VLAN이 작동 및 실행 중임을 나타냅니다.)
- 회색 — 장치에 스냅샷 데이터가 없습니다.
- 흰색 — 장치가 작동 및 실행 중입니다.
- 장치 테두리 — 실선 테두리는 장치를 나타냅니다. 파선 테두리는 장치의 각 VLAN이 고유 장치로 표시되는 가상 그룹을 나타냅니다.
- 파선 — 레이어 3 연결을 나타냅니다.
- 실선 — 레이어 2 연결을 나타냅니다.

 레이어 3 스위치	 DSL 모뎀	 라우터
 레이어 4-7 스위치	 방화벽	 서버
 ATM 스위치	 ISDN	 스위치
 네트워크 클라우드	 로드 밸런서	 알 수 없는 장치
 데스크톱	 프록시	 VPN
 비활성 장치	 정책 준수 위반	 시작 / 실행 불일치

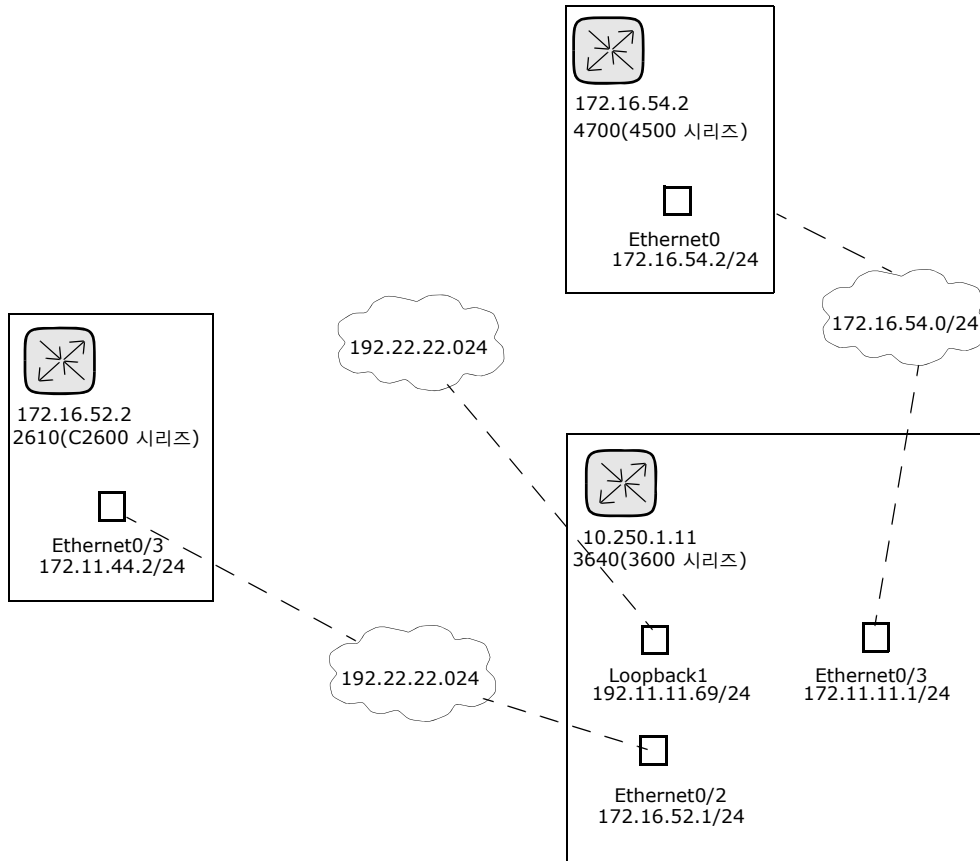
다음 그림은 VLAN 및 포트 간 연결을 포함하여 간단한 네트워크 다이어그램을 표시합니다.



다음 샘플 그림은 축소된 장치가 있는 간단한 네트워크 다이어그램을 표시합니다.



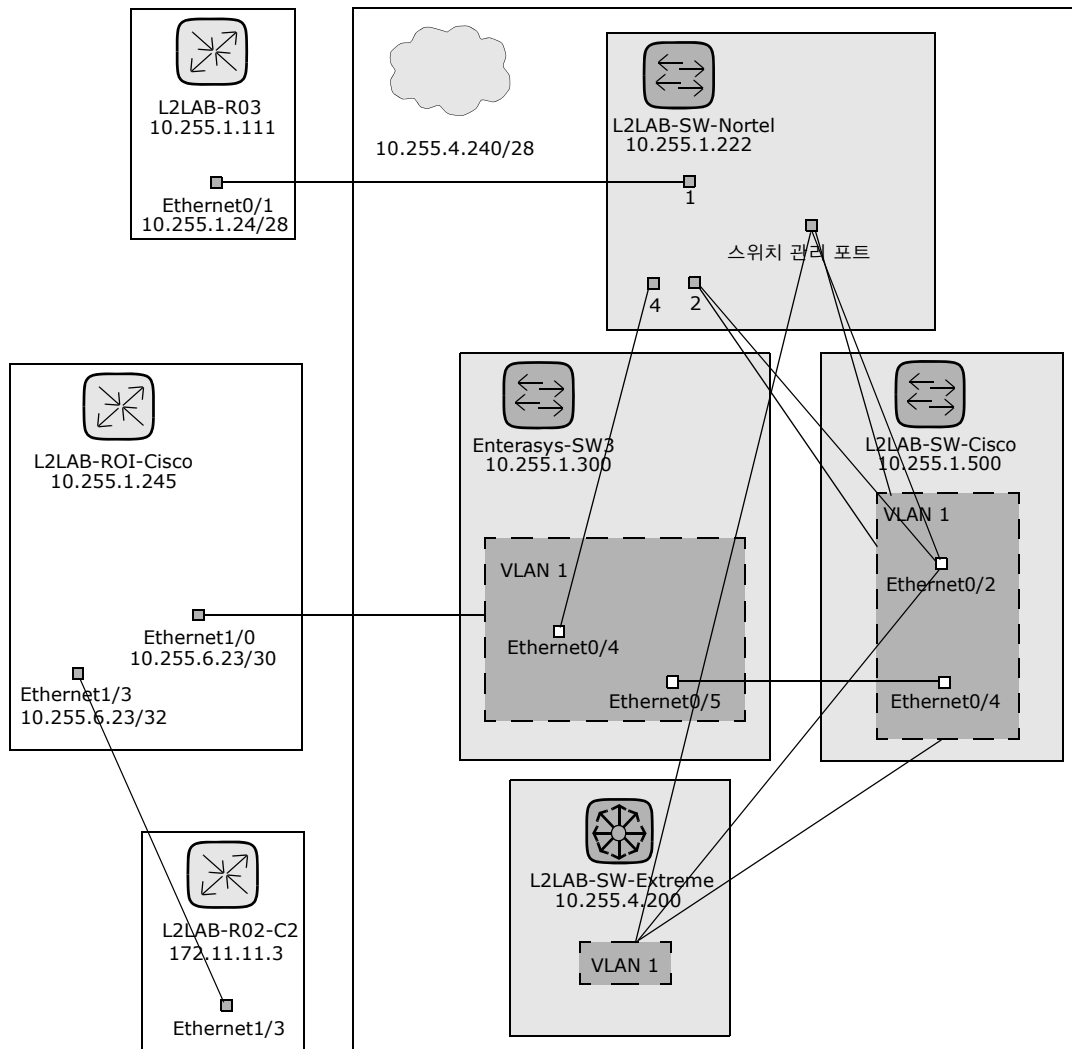
다음 샘플 그림은 동일한 서브넷을 공유하는 장치를 연결하기 위한 바로 가기 방법으로 클라우드를 사용하는 간단한 네트워크 다이어그램을 표시합니다. 클라우드는 라우터 및 스위치와 같은 게이트웨이 객체를 논리적으로 나타낼 수 있습니다.



레이어 3 다이어그램은 IP 주소 및 서브넷 마스크를 사용하여 모든 선택한 장치를 수집하고 동일한 서브넷에 있는 장치를 연결합니다. 서브넷에 있는 여러 장치는 클라우드로 연결됩니다. 결과적으로 클라우드는 서브넷을 나타냅니다.

확장된 레이어 3 다이어그램은 기본 레이어 3 다이어그램으로 시작합니다. 둘 이상의 장치가 서브넷에 연결된 경우 서브넷 내에 놓일 모든 장치를 찾기 위해 서브넷이 확장됩니다. 확장된 레이어 3 다이어그램에는 클라우드로 연결된 모든 인터페이스가 포함되며 알려진 레이어 2 연결(토폴로지 수집 진단에서 검색됨)을 통해 다른 장치로 변환됩니다. 그러면 확장된 클라우드는 서브넷에 참여하는 모든 장치의 컨테이너가 됩니다. 레이어 2 연결이 변환되면서 원래 선택하지 않았던 다이어그램에 장치가 추가될 수 있습니다.

다음 샘플 그림은 확장된 레이어 3 네트워크 다이어그램을 표시합니다. 기본 레이어 3 다이어그램이 생성되면 여기에 연결된 둘 이상의 장치가 있는 클라우드가 각각 확장됩니다. NA는 모든 레이어 2 연결로 이동합니다. 결과적으로 클라우드에 있는 장치는 클라우드 노드 내에 그룹화됩니다.



다이어그램 작성 페이지를 보려면 보고서 아래의 메뉴 모음에 있는 다이어그램 작성을 클릭합니다. 다이어그램 작성 페이지가 열립니다. 다이어그램 구성이 완료되면 생성 버튼을 클릭합니다.

다이어그램 작성 페이지 필드

필드	설명/작업
다이어그램 유형	<p>드롭다운 메뉴에서 다음 다이어그램 유형 중 하나를 선택합니다. 다이어그램 유형을 나타내는 샘플 다이어그램이 드롭다운 메뉴의 오른쪽에 표시됩니다.</p> <ul style="list-style-type: none"> •레이어 1: 포트(추론됨) •레이어 2: 포트 •레이어 3: 포트 •레이어 3: 포트(확장됨) •레이어 1: 장치(추론됨) •레이어 2: 장치 •레이어 3: 장치 •레이어 3: 장치(확장됨) <p>참고: 추론되는 레이어 1 데이터는 발견적 방법(heuristics)을 기반으로 합니다. NA는 네트워크 다이어그램을 더 쉽게 읽을 수 있도록 장치 및/또는 서버 사이의 데이터 링크 연결 수를 줄입니다. 종속적인 연결을 통해 추론할 수 있는 연결만 감소됩니다. 자세한 내용은 254페이지의 "NA/SA 통합"을 참조하십시오.</p>
출력 형식	<p>네트워크 다이어그램에 대해 다음 형식 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> •JPEG(대화식) — JPEG(Joint Photographic Experts Group) 출력에 있는 네트워크 다이어그램을 표시하고 네트워크 다이어그램에 있는 장치를 선택할 수 있습니다. 장치를 선택하면 장치에 대한 장치 세부사항 페이지가 열립니다. (261페이지의 "메뉴 옵션 보기"를 참조하십시오.) •JPEG(정적) — JPEG(Joint Photographic Experts Group) 형식으로 네트워크 다이어그램을 표시합니다. •Visio — Visio에서 네트워크 다이어그램을 보려면 Service Pack 2 이상 또는 Visio 뷰어를 포함하여 Visio 2003 이상이 시스템에 설치되어 있어야 합니다. 이러한 파일은 .rdx 파일입니다.

필드	설명/작업
장치 선택	<p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> • 장치 및 그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. • 라우팅 — 라우팅 시작 장치 및 라우팅 종료 장치를 입력합니다. NA에서는 두 장치 간 ICMP 테스트 작업을 실행합니다. ICMP 테스트 작업에 대한 자세한 내용은 383페이지의 "ICMP 테스트 실행 작업 페이지 필드"를 참조하십시오. 이 작업은 소스 장치 및 대상 장치 간에 사용된 모든 IP 주소를 표시하는 Traceroute로 수행됩니다. • 단일 장치 — 장치의 IP 주소 또는 호스트 이름을 입력합니다. 최대 3개 hops를 표시할 연결 수를 지정할 수 있습니다.
계층 레이어 필터	<p>계층 레이어는 장치 속성입니다. 장치를 추가하거나 편집할 때 장치의 계층 레이어를 설정할 수 있습니다. (자세한 내용은 137페이지의 "장치 추가"를 참조하십시오.) 결과적으로 다이어그램을 구성하면 필터링할 계층 레이어를 선택할 수 있습니다. 예를 들어, 전체 네트워크(인벤토리)의 다이어그램을 작성한 다음 코어 장치(코어로 설정된 계층 레이어가 있는 장치)만 다이어그램하도록 "코어"에 대해 필터링할 수 있습니다.</p> <p>참고: 아래 제공된 옵션은 기본 필터입니다. 여기에 필터를 지정할 수 있도록 하려면 장치에 필터링 값을 할당해야 합니다. 사용자 정의 필터 생성에 대한 정보는 768페이지의 "appserver.rcx 파일 편집"을 참조하십시오.</p> <p>드롭다운 메뉴에서 다음 옵션 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none"> • 코어 • 배포 • 액세스 • 가장자리

필드	설명/작업
고급 옵션	
고급 필터	<p>다음 옵션 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none"> • 비활성 장치 숨기기 — 네트워크 다이어그램에서 모든 비활성 장치를 제거합니다. • 선택한 다른 장치에 연결되지 않은 장치 숨기기 — 네트워크 다이어그램에서 다른 장치에 대한 연결이 없는 모든 장치를 제거합니다. • 연결이 없는 VLAN 숨기기 — 네트워크 다이어그램에서 포트 또는 다른 VLAN에 연결되지 않은 VLAN을 제거합니다. • 연결되지 않은 인터페이스/포트 숨기기 — 네트워크 다이어그램에서 다른 장치에 대한 연결이 없는 모든 인터페이스 및 포트를 제거합니다. • 장치와 연결되지 않은 포트 숨기기 — 네트워크 다이어그램에서 장치와 연결되지 않은 모든 레이어 2 포트를 제거합니다. (참고: NA에서는 각 관리되는 장치에서 라우팅 정보를 수집합니다. 종종 장치는 관리되지 않는 장치에 연결되는 포트 및 장치에 라우팅합니다. 장치에서는 NA 관리 장치에 있는 포트가 표시될 수 있지만 NA 토폴로지 데이터 수집 진단이 지원되지 않을 수 있습니다. 이 경우 NA에서는 포트와 장치 간 그룹화 연결을 할 수 없습니다.) • 서브넷 클라우드를 생성하려면 최소 서브넷 연결 수를 입력하십시오. 기본값은 2입니다.
그룹화	<p>다음 옵션 중 하나 또는 둘 다를 선택합니다.</p> <ul style="list-style-type: none"> • 포함된 서브넷을 슈퍼넷에 연결 — 서브넷을 그룹화할 수 있습니다. 예를 들어, IP 주소 범위 10.255.0.0/23와 범위 10.255.1.0/24의 경우 /24 네트워크는 /23 네트워크 내에 포함됩니다. 두 네트워크 간에 트래픽이 흐를 수 있습니다. 결과적으로 /23 네트워크 및 /24 네트워크는 다이어그램에 연결된 대로 표시됩니다. • VLAN을 별도의 장치로 표시 — 동일한 장치의 여러 표현으로 장치를 구분합니다(각 VLAN에 대해 하나). VLAN 장치는 다른 그래프 유형에 대해 장치 내 VLAN 그룹화와 동일한 파선 윤곽선으로 표시됩니다. (참고: 이 옵션은 확장된 L3 다이어그램에 대해 자동으로 선택되며 비활성화할 수 없습니다.)

필드	설명/작업
주석	
장치 주석	<p>각 그래프로 작성된 장치와 함께 표시하려는 필드를 선택합니다. 그래프에는 텍스트로 가득 찰 수 있을 정도의 필드가 많지 않습니다. 일부 사용 가능한 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none">•호스트 이름•기본 IP•FQDN•장치 설명•파티션•모델•공급업체•일련 번호•자산 태그•마지막으로 변경된 날짜•사용자 지정 필드•마지막 액세스 상태•비활성 장치 표시•정책 준수 상태 표시•시작/실행 불일치 표시•VTP 정보
종결 지점 주석	<p>다음 옵션 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none">•인터페이스 설명•포트 이름•IP 주소•포트 유형•포트 상태•실행 중인 포트 상태•MAC 주소•영역

필드	설명/작업
상호 연결 주석	다음 옵션 중 하나 이상을 선택합니다. <ul style="list-style-type: none"> • 서브넷 — 서브넷 정보가 있는 상호 연결 라인의 레이블을 지정합니다. • VLAN — VLAN 정보가 있는 상호 연결 라인의 레이블을 지정합니다.
클라우드 주석	다음 옵션을 선택합니다. <ul style="list-style-type: none"> • 서브넷 — 텍스트가 레이어 3 클라우드에 포함됩니다(동일한 서브넷을 공유하는 장치를 연결하기 위한 바로가기). • 영역 — 텍스트가 레이어 3 클라우드에 포함됩니다. 영역은 오버랩되는 IP 주소가 없는 네트워크 세그먼트입니다.
그래프 주석	다음 옵션을 선택합니다. <ul style="list-style-type: none"> • 주석 제목 — 각 선택한 주석에 대해 제목을 제공합니다. 예: 호스트 이름: L2LAB-SW01-C0000xl
다이어그램을 다음 이름의 사용자 보고서로 저장	다이어그램의 이름으로 입력하고 저장 버튼을 클릭합니다.
다이어그램을 전자 메일로 보낼 대상	전자 메일 주소를 입력하고 전자 메일 버튼을 클릭합니다.

JPEG — 대화식 옵션을 선택한 경우, 다이어그램을 생성한 후 장치를 클릭하면 장치에 대한 장치 세부사항 페이지가 열립니다. 자세한 내용은 [249페이지의 "장치 세부사항 보기"](#)를 참조하십시오.

appserver.rcx 파일 편집

계층 필터링 레이어는 표시 순으로 값이 주어집니다. 예를 들어, 코어는 1, 배포는 2입니다. 이 정보는 *Product/config* 디렉터리에 있는 *appserver.rcx* 파일에 저장됩니다. 파일은 다음과 같이 표시됩니다.

```
<array name="diagramming/hierarchy_layers">
  <value>core</value>
  <value>distribution</value>
  <value>access</value>
  <value>edge</value>
</array>
```


숫자 값은 데이터베이스에 저장됩니다. appserver.rcx 파일을 편집하는 경우 변경 사항은 데이터베이스에 반영되지 않습니다. 따라서 장치와 연관된 데이터도 변경해야 합니다. (자세한 내용은 [138페이지의 "새 장치 페이지 필드"](#)를 참조하십시오.)

장치 소프트웨어 보고서

장치 소프트웨어 보고서에서는 현재 각 장치에 지정된 소프트웨어 버전 및 준수 등급을 볼 수 있습니다.

장치 소프트웨어 보고서를 보려면 보고서 아래의 메뉴 모음에서 장치 소프트웨어를 클릭합니다. 장치 소프트웨어 보고서가 열립니다.

장치 소프트웨어 보고서 필드

필드	설명
소프트웨어 수준 보고서 링크	현재 각 장치에 할당된 소프트웨어 버전 및 수준을 볼 수 있는 소프트웨어 수준 보고서를 엽니다. 772페이지의 "소프트웨어 수준 보고서 필드" 를 참조하십시오.
소프트웨어 수준 링크	소프트웨어 수준을 편집하거나 삭제할 수 있는 소프트웨어 수준 페이지를 엽니다. 557페이지의 "새 소프트웨어 수준 추가" 를 참조하십시오.
현재 작업 그룹	드롭다운 메뉴에서 장치 그룹을 선택합니다. 인벤토리가 기본입니다.
수준 위치	다음과 같은 소프트웨어 수준을 선택합니다. <ul style="list-style-type: none"> • 모든 수준 • 보안 위험 • 사전 프로덕션 • 브론즈 • 실버
호스트 이름	장치의 호스트 이름을 표시합니다. 호스트 이름을 클릭하면 장치에 대한 자세한 내용을 볼 수 있는 장치 세부사항 페이지가 열립니다.
장치 IP	장치의 IP 주소를 표시합니다. 빨간색으로 표시된 장치는 마지막 스냅샷 시도에서 실패한 장치입니다. 비활성 장치는 IP 주소 옆에 아이콘이 표시됩니다.
변경 날짜	소프트웨어가 장치에 마지막으로 배포된 때를 표시합니다.
장치 소프트웨어 버전	장치에서 실행 중인 감지된 소프트웨어 버전을 표시합니다.

필드	설명
소프트웨어 수준	해당되는 경우 소프트웨어 수준을 표시합니다.
중요도	보안 취약점의 심각도를 다음과 같이 표시합니다. <ul style="list-style-type: none">•정보용 — 일반적으로 응답이 필요하지 않은 이벤트•낮음 — 시간이 허용될 경우 응답이 필요할 수 있는 이벤트•중간 — 일반적으로 72시간 이내에 시기 적절한 응답이 필요한 이벤트•높음 — 일반적으로 24시간 이내에 신속한 응답이 필요한 이벤트•심각 — 즉각적인 응답이 필요한 이벤트
주석	취약점에 대한 설명을 제공합니다.
작업	다음 작업을 선택할 수 있습니다. <ul style="list-style-type: none">•소프트웨어 감사 추적 보기 — 장치에서 로드된 소프트웨어를 볼 수 있는 장치 소프트웨어 감사 추적 페이지를 엽니다. 자세한 내용은 301페이지의 "장치 소프트웨어 이력 페이지 필드"를 참조하십시오.

소프트웨어 수준 보고서

소프트웨어 수준 보고서를 사용하면 현재 각 장치에 할당된 소프트웨어 버전 및 수준을 볼 수 있습니다.

소프트웨어 수준 보고서를 보려면

1. 정책 아래의 메뉴 모음에서 소프트웨어 수준을 클릭합니다. 소프트웨어 수준 페이지가 열립니다. 자세한 내용은 [540페이지의 "소프트웨어 수준 페이지 필드"](#)를 참조하십시오.
2. 페이지의 맨 위에 있는 소프트웨어 수준 보고서 링크를 클릭합니다. 소프트웨어 수준 보고서가 열립니다.

소프트웨어 수준 보고서 필드

필드	설명
장치 소프트웨어 보고서 링크	현재 각 장치에 할당된 소프트웨어 버전 및 준수 등급을 볼 수 있는 장치 소프트웨어 보고서를 엽니다. 770페이지의 "장치 소프트웨어 보고서 필드" 를 참조하십시오.
소프트웨어 수준 링크	소프트웨어 수준을 편집하거나 삭제할 수 있는 소프트웨어 수준 페이지를 엽니다. 557페이지의 "새 소프트웨어 수준 추가" 를 참조하십시오.
현재 작업 그룹	드롭다운 메뉴에서 장치 그룹을 선택합니다. 인벤토리가 기본입니다.
중요도 위치	다음에 포함하여 보안 취약점의 심각도에 대한 중요 수준을 선택합니다. <ul style="list-style-type: none"> • 정보용 — 일반적으로 응답이 필요하지 않은 이벤트 • 낮음 — 시간이 허용될 경우 응답이 필요할 수 있는 이벤트 • 중간 — 일반적으로 72시간 이내에 시기 적절한 응답이 필요한 이벤트 • 높음 — 일반적으로 24시간 이내에 신속한 응답이 필요한 이벤트 • 심각 — 즉각적인 응답이 필요한 이벤트

필드	설명
호스트 이름	장치의 호스트 이름을 표시합니다. 호스트 이름을 클릭하면 장치에 대한 자세한 내용을 볼 수 있는 장치 세부사항 페이지가 열립니다.
장치 IP	장치의 IP 주소를 표시합니다. IP 주소를 클릭하면 장치에 대한 자세한 내용을 볼 수 있는 장치 세부사항 페이지가 열립니다.
변경 날짜	소프트웨어가 장치에 마지막으로 배포된 날짜 및 시간을 표시합니다.
장치 소프트웨어 버전	장치에서 실행 중인 감지된 소프트웨어 버전을 표시합니다.
소프트웨어 수준	소프트웨어의 소프트웨어 수준 등급을 표시합니다.
중요도	<p>보안 취약점의 심각도를 다음과 같이 표시합니다.</p> <ul style="list-style-type: none"> •정보용 — 일반적으로 응답이 필요하지 않은 이벤트 •낮음 — 시간이 허용될 경우 응답이 필요할 수 있는 이벤트 •중간 — 일반적으로 72시간 이내에 시기 적절한 응답이 필요한 이벤트 •높음 — 일반적으로 24시간 이내에 신속한 응답이 필요한 이벤트 •심각 — 즉각적인 응답이 필요한 이벤트
주석	취약점에 대한 자세한 설명을 제공합니다.
작업	<p>다음 작업을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> •소프트웨어 감사 추적 보기 — 장치에서 로드된 소프트웨어를 볼 수 있는 장치 소프트웨어 감사 추적 페이지를 엽니다. 자세한 내용은 301페이지의 "장치 소프트웨어 이력 페이지 필드"를 참조하십시오.

소프트웨어 취약점 보고서

HP Live Network 정책을 로드하지 않았다면 소프트웨어 취약점 보고서는 빈 검색 결과 페이지를 표시합니다.

참고: TON을 사용하면 보안 주의 서비스 데이터 및 다른 NA 콘텐츠 서비스 자료를 다운로드할 수 있습니다. HP Live Network에 대한 자세한 내용은 [29페이지의 "도움말 메뉴 옵션"](#)을 참조하십시오.

TON 정책을 가져오고 준수 확인을 실행했으면 CVE(Common Vulnerabilities and Exposures) 값이 있는 해당 정책별로 결과가 표시됩니다.

소프트웨어 취약점 보고서는 준수 및 정책 확인 결과를 포함하는 표에서 데이터를 수집합니다. 결과적으로 생성된 특정 소프트웨어 취약점 이벤트가 없습니다. 생성된 이벤트는 정책 비준수 이벤트입니다.

소프트웨어 취약점 보고서를 보려면 보고서의 메뉴 모음에 있는 소프트웨어 취약점을 클릭합니다. 소프트웨어 취약점 보고서가 열립니다.

소프트웨어 취약점 보고서 필드

필드	설명/작업
확인란/드롭다운 메뉴	왼쪽의 확인란을 통해 특정 장치를 선택할 수 있습니다. 장치를 선택한 후에 작업 드롭다운 메뉴를 선택하여 다음과 같은 작업을 선택할 수 있습니다. <ul style="list-style-type: none"> •일괄 편집 •정책 준수 확인 •암호 배포 •장치 재부팅
호스트 이름	장치 호스트 이름을 표시합니다.
장치 IP	장치 IP 주소를 표시합니다.
장치 준수 상태	장치 준수 상태를 표시합니다.
정책	정책의 이름을 표시합니다.

필드	설명/작업
규칙	정책 구성 규칙을 표시합니다.
규칙 중요성	다음과 같이 중요 수준을 표시합니다. <ul style="list-style-type: none">•정보용 — 일반적으로 응답이 필요하지 않은 이벤트•낮음 — 시간이 허용될 경우 응답이 필요할 수 있는 이벤트•중간 — 일반적으로 72시간 이내에 시기 적절한 응답이 필요한 이벤트•높음 — 일반적으로 24시간 이내에 신속한 응답이 필요한 이벤트•심각 — 즉각적인 응답이 필요한 이벤트
규칙 설명	규칙 설명을 표시합니다.
CVE	연산자와 함께 CVE(Common Vulnerabilities and Exposures) 이름을 표시합니다. CVE는 취약점의 표준화된 이름과 보안 노출에 관한 기타 정보의 목록입니다.
마지막으로 확인된 날짜	마지막으로 확인된 날짜를 표시합니다.

이미지 동기화 보고서

이미지 동기화 보고서를 사용하면 NA 소프트웨어 이미지 리포지토리에 상주하지 않는 장치 또는 장치 그룹에서 현재 실행 중인 소프트웨어 이미지 또는 백업 소프트웨어 이미지를 볼 수 있습니다. 그런 다음 장치에서 NA 소프트웨어 이미지 리포지토리로 소프트웨어 이미지를 복사할 작업을 예약할 수 있습니다. 결과적으로 응급 상황이 발생하면 NA 소프트웨어 리포지토리에서 모든 소프트웨어 이미지를 다운로드할 수 있습니다.

참고: 모든 장치 드라이버에서 이 기능을 지원하지는 않습니다. 지원되는 장치에 대한 자세한 내용은 DRS(장치 릴리스 서비스) 설명서를 참조하십시오. DRS는 자동화된 새로운 드라이버 릴리스 및 전달 시스템입니다.

이미지 동기화 보고서를 보려면 보고서의 메뉴 모음에 있는 이미지 동기화 보고서를 선택합니다. 이미지 동기화 보고서가 열립니다.

이미지 동기화 보고서 필드

필드	설명/작업
현재 작업 그룹	기본 그룹을 표시합니다. 드롭다운 메뉴에서 다른 그룹을 선택할 수 있습니다(해당되는 경우).
확인란/드롭다운 메뉴	왼쪽의 확인란을 통해 특정 장치를 선택할 수 있습니다. 장치를 선택한 후에 드롭다운 메뉴 선택을 선택하여 모두 또는 없음을 클릭하거나 인접한 작업 드롭다운 메뉴를 선택하고 동기화 이미지 또는 파일 이름 제외 옵션을 클릭할 수 있습니다. 파일 이름 제외 옵션을 사용하면 NA가 무시한 목록에 파일 이름을 추가할 수 있습니다. 결과적으로 해당 파일 이름이 이미지 동기화 보고서에 표시되지 않습니다. (참고: 동기화 이미지 옵션을 사용하려면 장치 수정 권한이 있어야 합니다.)
동기화 이미지 옵션	NA 소프트웨어 이미지 리포지토리에 소프트웨어 이미지를 복사할 수 있는 백업 장치 소프트웨어 작업 페이지를 엽니다. 자세한 내용은 459 페이지의 "장치 소프트웨어 백업 작업 페이지 필드" 를 참조하십시오.
호스트 이름	장치의 호스트 이름을 표시합니다. 호스트 이름을 클릭하면 장치 및 구성 이력에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.

필드	설명/작업
장치 IP	장치의 IP 주소를 표시합니다. IP 주소를 클릭하면 장치 및 구성 이력에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.
슬롯	장치에서 소프트웨어 이미지가 상주하는 슬롯을 표시합니다.
파일 이름	소프트웨어 이미지의 이름을 표시합니다.
파일 크기	소프트웨어 이미지의 크기를 표시합니다.
검색 결과 메일 전송	검색 결과를 보낼 전자 메일 주소를 입력하고 보내기를 클릭합니다. 쉼표로 여러 전자 메일 주소를 구분해야 합니다.
검색 결과를 CSV 파일로 보기 링크	Excel(Windows 플랫폼) 또는 Star Office 또는 Gnumeric(Unix 플랫폼)을 사용하여 CSV 형식으로 검색 결과를 엽니다.

시스템 및 네트워크 이벤트 보고서

시스템 및 네트워크 이벤트 보고서를 사용하면 단일 장치 또는 모든 장치에 대한 변경 사항을 나타내는 이벤트를 추적할 수 있습니다. 전체 이벤트 목록을 보려면 **640페이지의 "이벤트 설명"**을 참조하십시오.

시스템 및 네트워크 이벤트 보고서를 보려면 보고서 아래의 메뉴 모음에서 시스템 및 네트워크 이벤트를 클릭합니다. 시스템 및 네트워크 이벤트 보고서가 열립니다.

시스템 및 네트워크 이벤트 보고서 필드

필드	설명/작업
새 메시지 링크	이 장치를 참조하는 모든 사용자에게 메시지를 게시할 수 있는 새 메시지 페이지를 엽니다. 단일 보기로 이벤트를 추적할 수도 있습니다.
다음 대상:	이벤트를 볼 시간 프레임을 표시합니다. 옵션은 다음과 같습니다. <ul style="list-style-type: none"> •과거 1, 2, 4, 8, 12, 24 및 48시간 •과거 1 및 2주 •과거 1개월 •모든 이벤트
현재 작업 그룹	드롭다운 메뉴에서 장치 그룹을 선택합니다.
확인란	왼쪽의 확인란을 통해 NA 데이터베이스의 이벤트를 삭제할 수 있습니다. 이벤트를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 이렇게 하면 NA 데이터베이스에서 선택한 이벤트가 삭제됩니다. 인접한 선택 드롭다운 메뉴를 통해 모든 이벤트를 선택하거나 선택 취소할 수 있습니다.
이벤트 날짜	이벤트 날짜/시간을 MMM-dd-yy HH:mm:ss 형식으로 표시합니다. 형식은 시스템 관리자가 구성합니다.
호스트 이름	장치의 호스트 이름 또는 IP 주소를 표시합니다. 호스트 이름 또는 IP 주소를 클릭하면 장치 및 구성 이력에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.

필드	설명/작업
요약	<p>이벤트 유형을 표시합니다. 이벤트 목록을 보려면 640페이지의 "이벤트 설명"을 참조하십시오. 이벤트 유형 링크를 클릭하면 이벤트 세부사항 페이지가 열립니다. 이 페이지에 포함된 내용은 다음과 같습니다.</p> <ul style="list-style-type: none">• 이벤트 발생 날짜 및 시간• 이벤트를 추가한 사람 또는 프로세스의 로그인 이름. 진단 변경 사항에 대한 세부사항 링크를 클릭하면 작업 세부사항을 볼 수 있는 작업 결과 페이지가 열립니다. 503페이지의 "작업 정보 페이지 필드"를 참조하십시오.• 이벤트 유형• 이벤트에 대한 간단한 설명• 장치에 대한 자세한 내용 링크
추가한 사람	<p>이벤트 생성을 초래한 작업을 수행한 사용자의 로그인 이름을 표시합니다.</p>

소프트웨어 취약점 이벤트 세부사항 보고서

소프트웨어 취약점 이벤트 세부사항 보고서를 사용하면 자문 정보 및 가능한 솔루션을 포함하여 소프트웨어 취약점에 대한 세부사항을 볼 수 있습니다.

소프트웨어 취약점 이벤트 세부사항을 보려면

1. 메뉴 모음에서 검색을 선택하고 이벤트를 클릭합니다. 이벤트 검색 페이지가 열립니다.
2. 소프트웨어 취약점이 감지됨 이벤트 요약을 선택하고 검색 버튼을 클릭합니다. 이벤트 검색 결과 페이지가 열립니다.

필드	설명/작업
확인란	왼쪽의 확인란을 통해 NA 데이터베이스의 이벤트를 삭제할 수 있습니다. 이벤트를 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 이렇게 하면 NA 데이터베이스에서 선택한 이벤트가 삭제됩니다. 인접한 선택 드롭다운 메뉴를 통해 모든 이벤트를 선택하거나 선택 취소할 수 있습니다.
날짜	이벤트 날짜/시간을 MMM-dd-yy HH:mm:ss 형식으로 표시합니다. 형식은 시스템 관리자가 구성합니다.
요약	소프트웨어 취약점이 감지됨을 표시합니다. 링크를 클릭하면 다음을 포함하여 보안 취약점에 대한 정보를 볼 수 있는 이벤트 세부사항 페이지가 열립니다. <ul style="list-style-type: none"> • 날짜 • 추가한 사람 • 요약 • 이름, 중요도 및 CVE(Common Vulnerabilities and Exposures)를 포함한 설명 • 작업 — NA 보고서에 대한 링크 및 자문 및 솔루션 정보에 대한 외부 링크를 제공합니다. • 장치
호스트 이름	장치의 호스트 이름 또는 IP 주소를 표시합니다. 호스트 이름 또는 IP 주소를 클릭하면 장치 및 구성 이력에 대한 정보를 볼 수 있는 장치 세부사항 페이지가 열립니다.

필드	설명/작업
추가한 사람	이벤트 추가자의 사용자 이름을 표시합니다.

요약 보고서

요약 보고서는 네트워크의 구성 작업에 대한 개요를 제공합니다. 추세를 분석하고 각별한 주의가 요구되는 문제 영역을 표시할 수 있도록 합니다. 이러한 보고서를 통해 팀에서 수행하는 업무 및 조직에 기여하는 가치에 대해 경영진에게 손쉽게 전달할 수 있습니다. 데이터는 표준 Microsoft Excel 스프레드시트로 제공되기 때문에, 정보를 쉽게 분류하고 필터링할 수 있으며 다른 응용 프로그램으로 잘라내기 및 붙여넣기를 수행할 수 있습니다.

기본적으로 NA는 주 단위로 요약 보고서를 업데이트하도록 구성되어 있습니다. 업데이트될 때마다 사전 요약 보고서 파일이 백업되므로, 기록 분석을 위해 또는 감사 추적을 제공하기 위해 이러한 보고서에 대한 아카이브를 유지할 수 있습니다. 보고서는 기본적으로 `.\<설치 디렉터리>\addins`에 저장됩니다.

요약 보고서를 수동으로 업데이트하려면

1. 작업 아래의 메뉴 모음에서 새 작업을 클릭하고 요약 보고서 생성을 선택합니다. 새 작업 - 요약 보고서 생성 페이지가 열립니다.
2. 가능한 한 빨리 시작이 선택되어 있는지 확인합니다.
3. 작업 저장을 클릭합니다.

작업은 작업 정보 페이지에서 작업 상태를 표시하며 요약 보고서를 업데이트합니다. 성공한 상태가 되면 최신 요약 보고서를 열 수 있습니다.

참고: 요약 보고서는 Microsoft Excel에서 사용할 수 있습니다. Excel 매크로는 보고서 데이터를 계산하기 위해 사용됩니다. 브라우저 및 Excel 보안 설정에 따라, 요약 보고서를 열면 매크로를 사용하도록 하는 메시지가 표시될 수 있습니다.

요약 보고서를 열려면 보고서 아래의 메뉴 모음에서 요약 보고서를 클릭합니다. 요약 보고서가 드롭다운 메뉴에 표시되지 않는 경우 시스템 관리자는 관리 설정을 확인해야 합니다.

최상위 요약 보고서에 있는 콘텐츠 링크를 클릭하고 최상위 요약 보고서로 돌아가기 위해 홈 링크를 사용하거나, 각 보고서의 맨 아래에 있는 탭을 사용하여 특정 요약 보고서로 이동할 수 있습니다. 맨 아래에 있는 탭이 모두 보이지 않는 경우, 창을 최대화하거나 열 조정 장치를 클릭하여 오른쪽으로 드래그하십시오.

요약 보고서 설명

보고서	보고되는 내용
요약	<p>최근 변경 작업 비율, 가장 활동적인 사용자 및 네트워크 프로필에 대한 개요를 표시합니다. 보고서에는 다음이 포함됩니다.</p> <ul style="list-style-type: none">•공급업체 상위 5개 — 상위 5개 공급업체별 장치 수를 표시합니다.•OS 버전 상위 5개 — 사용 중인 상위 5개 OS 버전을 표시합니다.•구성 변경 수 - 최근 7일간 — 최근 7일 동안 일별 평균 구성 변경 수를 표시합니다.•시간대별 변경 이력 — 구성 변경 사항이 작성된 시간을 표시합니다.•가장 많이 액세스한 장치 상위 10개 — 보고 기간 동안 가장 많이 액세스한 장치 상위 10개를 표시합니다.
변경 빈도	<p>네트워크에서 작성된 모든 변경 사항에 대한 개요를 표시합니다. 보고서는 사용자 및 장치 그룹별로 자세히 표시되어 지난 30일 동안의 주당 평균 변경 수를 제공합니다. 이렇게 하면 변경 비율을 부적절하게 표시하는 네트워크 영역뿐만 아니라 상위 수행자를 식별할 수 있습니다.</p>
일별 변경	<p>지난 2주 동안 일별 구성 변경 수를 표시합니다. 보고서에는 동일한 데이터가 있는 막대 차트 및 표 모두 포함됩니다. 세로 축은 변경 수를 표시합니다. 가로 축은 2주 동안의 각 요일을 표시합니다.</p>

보고서	보고되는 내용
통계 차트	<p>지난 주 동안의 구성 변경을 표시합니다. 변경 감지 방법 원형 차트에는 다음을 포함하여 변경 감지 방법이 표시됩니다.</p> <ul style="list-style-type: none"> • Syslog • 텔넷/SSH • 프록시 • 정기 또는 수동 폴링 • AAA • 구성 또는 스크립트 배포 <p>시간대별 변경 이력 막대 차트에는 NA 감지 변경 시간이 표시됩니다. 이러한 차트를 사용하면 변경 사항을 모니터링할 수 있습니다. 텔넷/SSH 프록시, 명령 스크립트 또는 구성 편집 및 배포를 사용하여 네트워크 엔지니어가 변경할 수 있도록 정책을 설정할 수도 있습니다.</p>
구성 변경	<p>지난 주 동안 변경된 내용을 표시합니다.</p> <ul style="list-style-type: none"> • 변경 수 및 트리거를 포함한 변경 감지 • 시간대별 변경 이력 • 호스트 이름, IP 주소, 최근 변경 날짜 및 시간, 프록시, AAA, Syslog 등에서 사용자 이름을 포함한 장치 구성 변경
장치 상태	<p>NA에서 추적한 비활성 장치를 표시합니다.</p> <ul style="list-style-type: none"> • 가장 많이 액세스한 장치 상위 10개 — 지난 주에 구성 스냅샷을 가장 많이 가져온 장치를 표시합니다. 일반적으로 이러한 장치는 엔지니어가 기록하거나 가장 자주 변경하는 장치입니다. • 장치 암호 변경 — 지난 주에 암호가 변경된 모든 장치에 대한 레코드를 표시합니다. • 액세스에 실패한 장치 — 장치를 사용할 수 없거나 암호 정보가 잘못되었기 때문에 NA가 액세스할 수 없는 장치를 표시합니다. 이 목록은 NA에서 장치를 성공적으로 관리할 수 있도록 확인 목록으로 제공합니다.

보고서	보고되는 내용
장치 인벤토리	<p>다음에 포함하여 NA에서 추적한 모든 장치를 표시합니다.</p> <ul style="list-style-type: none">• 호스트 이름(장치 정보 페이지에서)• IP 주소(장치 정보 페이지에서)• 자산 태그(장치 정보 페이지에서)• 위치(구성 파일에서)• 공급업체(구성 파일에서)• 모델(구성 파일에서)• 운영 체제 버전(구성 파일에서)• 일련 번호(구성 파일에서)• 장치 설명(장치 정보 페이지에서)• 마지막 스냅샷 결과(작업에서)• 마지막 수정한 구성(작업에서)
운영 체제(OS) 인벤토리	<p>네트워크에서 실행 중인 모든 장치 OS 버전을 표시하며 각 버전을 실행 중인 장치 수를 나열합니다. 이 보고서를 사용하여 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none">• 적용된 OS 버전에 대해 기업 표준 준수• 아키텍처 또는 서비스에 대해 제안된 변경 사항 테스트 또는 평가• 특정 OS 버전에 공급업체의 보안 주의 또는 패치를 적용하는 시간 저장

보고서	보고되는 내용
시스템 상태	<p>NA 시스템의 활동 및 상태를 표시합니다. 보고서에는 할당된 장치 드라이버가 없어 관리할 수 없는 장치가 나열됩니다. 또한 최근 시스템 활동 및 NA 데이터베이스의 레코드 수에 대한 요약 정보도 제공됩니다.</p> <ul style="list-style-type: none"> • 시스템 상태 — 장치 및 그룹에 대해 보고서는 구성, 장치, 장치 그룹, 관리되지 않는 장치 및 인증 규칙의 전체 수를 표시합니다. 사용자에게 대해 보고서는 NA 계정이 없는 사용자 및 AAA 사용자의 전체 수를 표시합니다. 또한 보고서는 사용자 지정 보고서 수를 표시합니다. • 시스템 활동 — 작업 및 메시지에 대해 보고서는 성공한 작업, 실패한 작업 및 시스템 이벤트의 전체 수를 표시합니다. 통합된 텔넷/SSH 클라이언트에 대해 보고서는 기록된 텔넷 및 SSH 세션의 전체 수를 표시합니다. • 드라이버가 없는 장치 — 드라이버가 없는 장치의 호스트 이름 및 IP 주소를 표시합니다.
정책 준수	<p>준수 및 준수하지 않는 정책의 수를 표시합니다. 호스트 이름, IP 주소 및 마지막 구성 변경 정보가 표시됩니다. 보고서에는 숫자 총계가 있는 간단한 원형 차트 및 다음과 같은 상세 데이터가 있는 세 개의 표가 모두 포함됩니다.</p> <ul style="list-style-type: none"> • 준수하는 구성 정책 • 준수하지 않는 구성 정책 • 구성 정책(구성 정책의 이름 및 연관된 규칙의 수 포함)

전자 메일 보고서

보고서를 전자 메일로 보낼 수 있습니다. 보고서 아래의 메뉴 모음에서 보고서 작업을 선택하고 전자 메일 보고서를 클릭합니다. 전자 메일 보고서 작업 페이지가 열립니다. 자세한 내용은 [469페이지의 "전자 메일 보고서 작업 페이지 필드"](#)를 참조하십시오.

17장: SecurID 사용

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	788페이지의 "시작하기"
설치 필요 조건	789페이지의 "설치 필요 조건"
RSA 서버 인증 관리자	789페이지의 "RSA 서버 인증 관리자"
사용자 인증	789페이지의 "사용자 인증"
네트워크 장치 액세스	790페이지의 "네트워크 장치 액세스"
SecurID 토큰 추가	793페이지의 "SecurID 소프트웨어 토큰 추가"
SecurID를 통한 NA 로그인	794페이지의 "SecurID를 통한 로그인"
SecurID 문제점 해결	798페이지의 "SecurID 문제점 해결"

시작하기

RSA SecurID 솔루션은 인증된 사용자에게만 네트워크 리소스에 대한 액세스를 부여하여 조직을 보호할 수 있도록 설계되었습니다. 일반적으로 SecurID는 두 부분으로 이루어진 인증 스키마로, 실제 하드웨어 구성요소와 함께 암호/PIN이 필요합니다. 하드웨어 구성 요소는 60초마다 암호 코드를 변경합니다. 일부 장치 작성자는 해당 네트워크 장치로 이 인증 시스템을 통합합니다. SecurID 작동 방식에 대한 자세한 정보는 SecurID 문서를 참조하십시오.

참고: NA가 외부 인증용으로 SecurID를 사용하도록 구성되면 NA 프록시에 연결 시 단일 사인온 기능이 비활성화됩니다. SecurID 암호 코드를 재사용할 수 없으므로 해당 SecurID 자격 증명을 사용하여 다시 인증해야 합니다.

HP Network Automation(NA)은 보안 수준이 높은 2가지 유형의 인증에 필요한 SecurID를 지원하여 다음을 수행합니다.

- NA에 로그인한 사용자 인증
- NA를 통한 네트워크 장치 액세스

다음 표에서는 NA SecurID 지원에 대해 설명합니다.

NA 액세스	연결 방법	SecurID 지원
웹 사용자 인터페이스	HTTP	예
SSH/텔넷 프록시	SSH	예
	텔넷	예
API	RMI	아니요

참고: 장치 SecurID 인증에 SSH를 사용하려면, 먼저 장치가 키보드 대화식을 사용하여 SSH에서 SecurID를 지원하고 Next-token-code 모드를 특별히 지원하는지 확인해야 합니다.

설치 필요 조건

SecurID를 사용하여 NA에 로그인하는 경우 NA에서는 다음 토큰 알고리즘 및 토큰 버전을 지원합니다.

- AES SDTID 3.0
- SID SDTID 2.0

참고: RSA SecurID 6.1은 NA가 Windows 2k3(64비트) 플랫폼에 설치된 경우 작동하지 않습니다.

RSA 서버 인증 관리자

설치 시 NA 설치 프로그램은 NA_DIRECTORY/jre 디렉터리에 *rsa_api.properties* 파일을 설치합니다. 다음을 포함하도록 이 파일을 편집해야 합니다.

- RSA_AGENT_HOST - NA가 상주하는 서버의 IP 주소입니다.
- SDCONF_LOC - RSA 서버 인증 관리자가 생성하는 RSA conf 파일의 위치입니다.

다음 예는 IP 주소가 10.255.140.124인 서버에 NA가 설치되어 있음을 나타냅니다. RSA conf 파일은 c:\NA\jre\sdconf.rec에 있습니다.

```
RSA_AGENT_HOST=10.255.140.124
SDCONF_LOC=C:/NA/jre/sdconf.rec(Unix platform)
SDCONF_LOC=C:\\NA\\jre\\sdconf.rec(Windows platform)
```

사용자 인증

NA에 대한 사용자 인증을 위해 다음 사항을 확인합니다.

- RSA에서 하드웨어 또는 소프트웨어 토큰을 구입했습니다.
- ACEServer가 실행 중이고 NA 서버에서 액세스 가능합니다.
- ACEServer에서, 에이전트 호스트로 NA가 실행 중인 호스트가 추가되어 있습니다.
- 에이전트 호스트 설정에서 에이전트 유형이 "UNIX 에이전트"입니다.
- ACEServer에서 사용자를 생성했습니다.
- ACEServer 사용자에게 소프트웨어 토큰을 할당했습니다.

- 사용자가 에이전트 호스트에서 연결할 수 있도록 설정했습니다.

NA가 장치에 액세스할 수 있도록 다음을 확인합니다.

- NA가 실행 중입니다.
- NA 서버에 RSA 소프트웨어 토큰 소프트웨어가 설치되어 있습니다.
- ACEServer가 실행 중이고 장치에서 액세스 가능합니다.
- RSA에서 소프트웨어 토큰을 가져왔습니다.
- RSA 소프트웨어 토큰 응용 프로그램을 통해 SecurID 토큰을 NA 서버로 가져왔습니다.
- ACEServer에 라이선스를 추가했습니다.
- ACEServer에서 사용자를 생성했습니다.
- 사용자에게 소프트웨어 토큰을 할당했습니다.
- 토큰의 PIN을 설정했습니다.
- 사용자가 장치에 연결할 수 있도록 설정했습니다.
- NA에서 SecurID 사용자에게 해당되는 사용자를 추가했습니다.
- 토큰 풀 또는 사용자별 고유 토큰을 사용할지 선택했습니다.
- 토큰 풀 사용 시 토큰 풀 사용자 이름을 할당했습니다.
- 사용자에게 토큰을 할당했습니다.

네트워크 장치 액세스

NA에서 장치에 액세스하려면 RSA에서 소프트웨어 토큰 소프트웨어 및 라이선스를 다운로드해야 합니다. FOBS 및 핀패드 등의 하드웨어 토큰 라이선스는 사용할 수 없습니다.

RSA의 웹 사이트에서 소프트웨어 토큰 소프트웨어를 다운로드할 수 있습니다. NA가 설치된 동일한 시스템에 소프트웨어를 설치해야 합니다. 일반 SecurID 메커니즘을 통해 이 시스템에 소프트웨어 토큰 라이선스도 가져와야 합니다.

참고: NA를 실행 중인 서버 및 ACEServer의 시간이 동기화되어야 합니다. 소프트웨어 토큰은 시간 차이의 영향을 받습니다. 두 서버가 2분 이상의 차이로 동기화되지 않으면 생성된 암호 코드가 실패할 수 있습니다. 두 서버에서 NTP를 사용하여 시간을 정확하게 유지할 수 있습니다.

NA 모니터는 제공된 토큰 코드가 두 번 사용되지 않는지 확인하기 위해 SecurID 사용 시 장치에 액세스합니다. 그러면 SecurID 장치 액세스 사용 시 NA의 활동이 느려질 수 있습니다. 이를 해결하기 위해 NA는 시스템에 여러 소프트웨어 토큰 시드를 로드할 수 있는 기능을 제공합니다. 다음 토큰 관리 모드 중 하나를 사용할 수 있습니다.

- 사용자별 — 각 NA 사용자에게는 하나 이상의 해당되는 소프트웨어 토큰 시드가 있습니다. 이 모드에서 각 장치 액세스에는 NA 프록시 연결 또는 태스크를 시작한 사용자에게 해당되는 시드만 사용됩니다. 시스템의 모든 사용자에게 올바른 소프트웨어 토큰이 지정되는 것이 좋습니다.
 - 내 설정의 홈 페이지에서 내 프로필을 클릭합니다. 내 프로필 페이지가 열립니다. 내 프로필 페이지 필드에 대한 정보는 [339페이지의 "내 프로필 페이지 필드"](#)를 참조하십시오.

참고: SecurID 토큰 추가 및/또는 업데이트에 대한 정보는 [793페이지의 "SecurID 소프트웨어 토큰 추가"](#)를 참조하십시오.

- 풀 — 일반적으로 사용하는 풀 소프트웨어 토큰 시드는 NA에 제공되어 최대 성능을 위해 가능한 한 효과적으로 사용됩니다. 관리 아래의 메뉴 모음에서 관리 설정을 선택한 후 장치 액세스 옵션을 클릭합니다. 장치 액세스 페이지가 열리고 여기서 SecurID 장치 액세스를 구성할 수 있습니다. 자세한 내용은 [56페이지의 "장치 액세스 페이지 필드"](#)를 참조하십시오.

소프트웨어 시드가 NA에 로드되었으면 RSA SecureID 인증을 통해 관리용으로 장치 세트 또는 특정 장치를 지정할 수 있습니다. 특정 장치에 SecurID 액세스를 사용하려면

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다. 모든 관리 장치의 목록이 열립니다.
2. SecurID 액세스를 사용하려는 장치를 클릭합니다. 장치 세부사항 페이지가 열립니다.
3. 작업 열에서 편집을 클릭합니다. 장치 편집 페이지가 열립니다. 자세한 내용은 [138페이지의 "새 장치 페이지 필드"](#)를 참조하십시오.
4. 암호 정보 섹션으로 스크롤하여 장치별 암호 정보 사용 옵션을 선택합니다.
5. 아래로 스크롤하여 장치 액세스 설정(장치별 설정) 표시 필드를 클릭합니다.
6. 설정 드롭다운 메뉴에서 "SecurID 사용"을 선택하고 값에 *exec* 또는 *enable* 중 하나를 입력합니다. Exec 모드로 SecurID를 사용하려면 *exec*를 입력합니다. *exec*를 사용하면 일반적으로 장치에 로그인할 때 첫 번째로 사용하는 모드인 Exec 모드가 활성화됩니다. Exec 모드 및 Enable 모드 둘 다에서 SecureID를 사용하려면 *enable*을 입력합니다.
7. 이 장치가 SecurID 토큰의 특정 사용자 풀을 사용하도록 하려면 사용자 정의 설정 필드에서 *securid_pool_override*를 입력합니다. 값 필드에서 사용자 이름을 입력합니다.
8. 장치 저장 단추를 클릭합니다.

장치(또는 장치 그룹)가 SecurID 액세스용으로 구성되고 소프트웨어 시드가 입력되었으면, NA는 장치에 액세스해야 할 때마다 올바른 시간 제한 토큰 코드를 자동으로 생성합니다.

RSA SecurID 인증을 통해 관리용으로 장치의 네트워크 암호 규칙도 설정할 수 있습니다. 자세한 내용은 [172페이지의 "장치 암호 규칙 페이지 필드"](#)를 참조하십시오. 그런 다음 위의 4, 5 및 6단계를 따르십시오.

SecurID 소프트웨어 토큰 추가

SecurID 소프트웨어 토큰을 추가하려면

1. RSA 소프트웨어 토큰 응용 프로그램을 사용하여 NA가 실행 중인 서버에 토큰을 가져오십시오.
2. 내 설정의 홈 페이지에서 내 프로필을 클릭합니다. 내 프로필 페이지가 열립니다. 내 프로필 페이지 필드에 대한 정보는 [339페이지의 "내 프로필 페이지 필드"](#)를 참조하십시오.
3. 페이지 맨 아래의 SecurID 섹션에서 소프트웨어 토큰 라이선스 관리 링크를 클릭합니다. SecurID 토큰 보기 페이지가 열립니다. 여기서 해당 사용자 로그인과 연관된 소프트웨어 토큰 라이선스를 보고 추가하거나 업데이트할 수 있습니다. 이 라이선스는 장치가 SecurID 자격 증명을 요구하도록 구성되어 있는 경우 장치에 로그인하는 데 사용됩니다.
4. 토큰 추가 링크를 클릭합니다. 새 SecurID 토큰 페이지가 열립니다. 사용자별로 일반 사용의 풀 소프트웨어 토큰 또는 단일 소프트웨어 토큰을 추가할 수 있습니다.

참고: 관리의 사용자 옵션을 클릭한 다음 해당 사용자의 편집 옵션을 클릭하여 소프트웨어 토큰 라이선스 관리 링크를 탐색할 수도 있습니다.

새 SecurID 토큰 페이지

필드	설명/작업
SecurID 사용자	ACEServer의 토큰에 지정된 사용자 이름을 입력합니다.
소프트웨어 토큰 일련 번호	토큰의 일련 번호(제로 패드됨)를 입력합니다.
PIN	PIN이 ACE/Server에서 발행 시 토큰용으로 구성된 경우 여기에 입력합니다. (참고: PIN이 업데이트되면 여기에서도 업데이트되어야 합니다.)
PIN 확인	확인용 PIN을 재입력합니다.
암호	암호가 ACE/Server에서 발행 시 토큰용으로 구성된 경우 여기에 입력합니다.

완료되면 저장을 클릭해야 합니다.

SecurID를 통한 로그인

외부 인증 메커니즘으로 RSA SecurID를 지정할 수 있습니다. 자세한 내용은 [102페이지의 "사용자 인증 페이지 필드"](#)를 참조하십시오.

NA 서버로 RSA SecurID ACE 서버의 *sdconf.rec* 파일을 설치해야 합니다(예: *C:\WINDOWS\SYSTEM32\sdconf.rec*). 이 파일은 NA가 SecurID에 액세스하도록 필수 연결 정보를 제공합니다.

참고: Linux 또는 Solaris 플랫폼에서 기본적으로 NA는 */var/ace* 디렉터리의 *sdconf.rec* 파일을 검색합니다. 이 파일은 NA가 SecurID에 액세스하도록 필수 연결 정보를 제공합니다.

설치 완료 시 NA 관리 엔진을 다시 시작해야 합니다. NA 관리 엔진 다시 시작에 대한 정보는 [123페이지의 "서비스 시작 및 중지"](#)를 참조하십시오.

토큰의 모드가 새 PIN 모드인 경우 SecurID를 통해 NA에 로그인하는 데 2가지 방법이 있습니다.

- SecurID 시스템 PIN 사용
- 새 SecurID PIN 사용

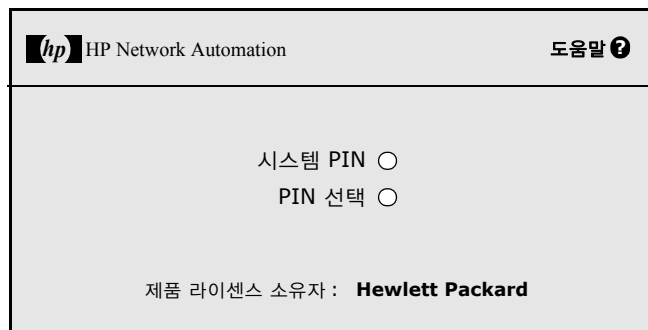
항상 RSA의 로그인 프로시저에서는 사용자가 새 PIN으로 다시 인증해야 합니다.

아래에 표시된 대로 NA 로그인 프롬프트에서 다음과 같이 수행합니다.

1. NA 사용자 이름을 입력합니다.
2. 암호 필드에 해당 암호 코드를 입력합니다.
3. 로그인을 클릭합니다.

The screenshot shows a login window for HP Network Automation. At the top left is the HP logo and the text 'HP Network Automation'. At the top right is a '도움말' (Help) icon. The main content area has two input fields: '사용자 이름 : ' followed by a text box, and '암호 : ' followed by another text box. To the right of the password field is a button labeled '로그인'. At the bottom of the window, it displays '제품 라이선스 소유자 : Hewlett Packard'.

해당 SecurID 시스템이 시스템 PIN 또는 새 PIN 중 하나를 사용하라는 메시지를 표시하도록 구성된 경우 다음 페이지가 열립니다.




시스템 PIN을 클릭한 경우 [796페이지의 "로그인 방법 1: 시스템 PIN 사용"](#)을 참조하십시오. PIN 선택을 클릭한 경우 [797페이지의 "로그인 방법 2: 새 PIN 사용"](#)을 참조하십시오.

참고: 해당 SecurID 시스템이 시스템 PIN 또는 새 PIN 중 하나를 사용하라는 메시지를 표시하도록 구성되지 않은 경우 해당 SecurID 시스템 구성에 따라 로그인 방법 1 또는 로그인 방법 2를 참조하십시오.

로그인 방법 1: 시스템 PIN 사용

로그인 페이지에서

1. 460페이지에 표시된 대로 시스템 PIN을 클릭합니다. SecurID에서 시스템 PIN을 가져왔으면 아래에 표시된 대로 예를 클릭합니다.
2. 로그인을 클릭합니다.
3. 대기하고 그 다음 토큰 코드를 사용하여 로그인하라는 메시지가 표시됩니다.

 HP Network Automation 도움말 ?

시스템에서 선택한 PIN 은 1574 입니다. 적용하시겠습니까 ?


예 : **로그인**
아니요 :

제품 라이선스 소유자 : **Hewlett Packard**

로그인 방법 2: 새 PIN 사용

로그인 페이지에서

1. 402페이지에 표시된 대로 PIN 선택을 클릭합니다.
2. 아래에 표시된 대로 새 PIN을 두 번 입력합니다.
3. 로그인을 클릭합니다. PIN 매개변수를 준수하도록 PIN을 확인합니다.

 HP Network Automation 도움말 ?

4~8 개의 숫자로 새 PIN 을 입력합니다.

새 PIN 입력

새 PIN 다시 입력

제품 라이선스 소유자 : **Hewlett Packard**

SecurID 문제점 해결

I. SecurID를 통해 NA에 로그인할 수 없는 경우 해당 RSA 관리자에 문의하십시오.

II. 장치 액세스용으로 SecurID를 사용할 경우 변경 감지용 Syslog 사용자 식별 옵션을 끄는 것이 좋습니다. 그렇지 않으면 스냅샷 작업 실패 메시지가 수신될 수 있습니다.

1. 관리 아래의 메뉴 모음에서 관리 설정 클릭을 선택한 후 구성 관리를 클릭합니다. 구성 관리 페이지가 열립니다.
2. 사용자 ID 변경 섹션에서 — Syslog 사용자 식별, "가능한 경우 syslog 메시지 텍스트에서 구성을 변경한 사용자를 식별합니다" 확인란을 선택 해제합니다.
3. 사용자 ID 변경 섹션에서 — Syslog에서 사용자 자동 작성, "syslog에서 식별된 변경 작성자가 아직 없을 때 NA의 사용자를 새로 작성합니다(사용자 자동 작성이 사용 가능해야 함)" 확인란을 선택 해제합니다.
4. 저장 버튼을 클릭합니다.

III. 외부 인증에 실패하면 NA가 다음과 같은 경우 로컬 사용자 자격 증명에 폴백하려고 합니다.

- 외부 인증 서비스가 중단되거나 액세스될 수 없는 경우
- 외부 인증 방법을 통해 성공적으로 로그인하지 않은 정적 사용자 계정인 경우
- 기본 제공된 관리 사용자 계정인 경우

IV. 노드 암호 파일은 RSA ACE/Agent client 및 RSA ACE/Server 간의 통신을 인증하는 데 사용됩니다. ACE/Server 로그 파일에서 다음 유형의 메시지를 보면 NA 서버용 노드 암호 파일을 업데이트해야 합니다.

```
07/12/2006 22:00:19U ----/core15.hp.com      ---->/
07/12/2006 18:00:19L Node verification failed  NArsa.rduNA.HP.com
```

노드 암호를 작성하려면

1. 에이전트 호스트 클릭 --> 에이전트 호스트 추가(또는 편집)
2. 노드 암호 작성을 클릭합니다.
3. 암호 상자에 암호를 입력한 다음 암호 확인 상자에 다시 입력합니다.
4. 기본 이름 및 디렉터리에서 노드 암호 파일을 저장하려면 확인을 클릭합니다. 노드 암호 파일은 기본 이름 *nodesecret.rec*로 기본 디렉터리에 작성됩니다. 다른 디렉터를 지정할 때까지 기본 디렉터리는 *ACEPROG*입니다. 그러한 경우, 데이터 베이스 관리 응용 프로그램을 다시 시작할 때까지 지정한 디렉터리가 기본 디렉터리가 됩니다. 다른 이름으로 파일을 저장하려면 찾아보기를 클릭합니다. 노드 암호 파일 이름 사양 대화 상자에서 이름 및 디렉터를 변경한 다음 저장을 클릭합니다.

참고: 지정된 디렉터리에 동일한 이름의 노드 암호 파일이 있는 경우, 덮어쓰려면 예를 클릭하거나 노드 암호 파일 이름 사양 대화 상자로 돌아가려면 아니요를 클릭합니다. 예를 클릭하면 지정한 이름 및 디렉터를 통해 노드 암호 파일이 작성됩니다.

에이전트 호스트 추가(또는 편집) 대화 상자에서 노드 암호 파일 작성 단추를 사용할 수 없습니다. 작성된 노드 암호를 선택합니다.

5. 확인을 클릭합니다.
6. 에이전트 호스트에 노드 암호 로드 유틸리티 및 새 노드 암호 파일을 복사합니다. 노드 암호 로드 유틸리티는 에이전트 호스트에 새 노드 암호 파일을 로드합니다. RSA 보안에서는 RSA 인증 관리자 CD의 4개 플랫폼별 버전(Windows, Solaris, HP-UX 및 IBM AIX) 유틸리티(*agent_nsload*)를 제공합니다.
7. 에이전트 호스트에서 노드 암호 로드 유틸리티를 실행합니다. 명령행 프롬프트에서 *agent_nsload -f path -p password*를 입력합니다. 여기서 *path*는 노드 암호 파일의 디렉터리 위치 및 이름이고 *password*는 노드 암호 파일을 보호하는데 사용하는 암호입니다.

참고: ACE/Server가 NA 서버와는 다른 플랫폼에 있는 경우 *agent_nsload* 실행 파일이 호환되지 않을 수 있습니다. 이러한 경우 RSA에 접속하여 올바른 바이너리를 가져오십시오. 또한 RSA dll이 새 노드 암호 파일을 찾을 수 있도록 NA 서버를 재부팅해야 할 수도 있습니다.

800

HP Network Automation 사용 설명서

18장: 준수 센터

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	803페이지의 "시작하기"
COBIT 준수 상태 보고서	805페이지의 "COBIT 준수 상태 보고서"
COSO 준수 상태 보고서	816페이지의 "COSO 준수 상태 보고서"
ITIL 준수 상태 보고서	820페이지의 "ITIL 준수 상태 보고서"
GLBA 준수 상태 보고서	825페이지의 "GLBA 준수 상태 보고서"
HIPAA 준수 상태 보고서	829페이지의 "HIPAA 준수 상태 보고서"
Visa CISP 준수 상태 보고서	838페이지의 "Visa CISP(PCI 데이터 보안 표준) 준수 상태 보고서"

참고: HP 준수 센터는 제공된 규정 및 표준에 대한 HP의 이해에 바탕을 두고 있습니다. HP는 감사자나 법률 기관이 아니므로, 자세한 내용은 회사의 감사자나 법률 담당자에게 문의해야 합니다.

준수 센터 탐색

hp HP Network Automation		로그아웃																																					
장치 ▾	작업 ▾	정책 ▾	보고서 ▾	관리 ▾	도움말 ▾																																		
↓																																							
<table border="1"> <tr> <td>단일 보기</td> <td></td> </tr> <tr> <td>단일 검색</td> <td></td> </tr> <tr> <td>사용자 및 시스템 보고서</td> <td></td> </tr> <tr> <td>검색 대상</td> <td>▶</td> </tr> <tr> <td>고급 검색</td> <td></td> </tr> <tr> <td>준수 센터</td> <td></td> </tr> <tr> <td>네트워크 상태</td> <td></td> </tr> <tr> <td>모범 사례</td> <td></td> </tr> <tr> <td>장치 상태</td> <td></td> </tr> <tr> <td>통계 대시보드</td> <td></td> </tr> <tr> <td>다이어그램 작성</td> <td></td> </tr> <tr> <td>장치 소프트웨어</td> <td></td> </tr> <tr> <td>소프트웨어 취약점</td> <td></td> </tr> <tr> <td>이미지 동기화 보고서</td> <td></td> </tr> <tr> <td>시스템 및 네트워크 이벤트</td> <td></td> </tr> <tr> <td>요약 보고서</td> <td></td> </tr> <tr> <td>보고서 작업</td> <td>▶</td> </tr> </table>						단일 보기		단일 검색		사용자 및 시스템 보고서		검색 대상	▶	고급 검색		준수 센터		네트워크 상태		모범 사례		장치 상태		통계 대시보드		다이어그램 작성		장치 소프트웨어		소프트웨어 취약점		이미지 동기화 보고서		시스템 및 네트워크 이벤트		요약 보고서		보고서 작업	▶
단일 보기																																							
단일 검색																																							
사용자 및 시스템 보고서																																							
검색 대상	▶																																						
고급 검색																																							
준수 센터																																							
네트워크 상태																																							
모범 사례																																							
장치 상태																																							
통계 대시보드																																							
다이어그램 작성																																							
장치 소프트웨어																																							
소프트웨어 취약점																																							
이미지 동기화 보고서																																							
시스템 및 네트워크 이벤트																																							
요약 보고서																																							
보고서 작업	▶																																						

시작하기

준수 센터는 Sarbanes-Oxley(섹션 404)와 관련하여 네트워크 인프라의 현재 준수 상태를 확인하는 데 도움이 되는 정보와 보고서에 액세스할 수 있으며 내부 제어 프레임워크를 지원하는 NA의 포털입니다.

Sarbanes-Oxley라고 하는 The Public Company Accounting Reform and Investor Protection Act of 2002는 투자자에게 제공하는 정확하고 신뢰할 수 있는 기업 공개를 개선하기 위해 제정되었습니다. Sarbanes-Oxley는 일반적으로 SEC(Securities and Exchange Commission)에 등록되었거나 SEC에 보고서를 제출해야 하는 모든 미국 회사에 적용됩니다. 이 규정은 보고하는 회사의 CEO 및 CFO가 그들 회사의 SEC 보고서를 증명하도록 규정하고 있습니다.

Sarbanes-Oxley의 주요 규정은 섹션 404로, 이 규정은 특별히 재무 보고에 대한 내부 제어를 다룹니다. 섹션 404에서는 보고 회사가 재무 보고의 일부로서 내부 제어 보고서 및 평가를 포함하도록 규정하고 있습니다. Sarbanes-Oxley(섹션 404)에서는 IT 관련 준수 활동을 위한 특정 제어 요구 사항을 제공하지 않으므로 조직에서는 COSO, COBIT, ITIL 또는 Visa CISP 등의 내부 제어 프레임워크를 선택하여 해당 프레임워크에 대해 적용 및 보고해야 합니다. NA를 사용한 Sarbanes-Oxley(섹션 404) 준수에 대한 자세한 내용은 준수 센터 홈 페이지에 제공된 온라인 정보를 참조하십시오.

준수 센터 홈 페이지에 액세스하려면 보고서 아래의 메뉴 모음에서 준수 센터를 클릭합니다. 준수 센터 홈 페이지가 열립니다.

준수 센터 홈 페이지

옵션	설명/작업
Sarbanes-Oxley(섹션 404)	Sarbanes-Oxley(섹션 404) 준수 상태 개요 정보를 엽니다.
COBIT 준수 상태 링크	COBIT 준수 상태 보고서를 엽니다. 자세한 내용은 805페이지 의 "COBIT 준수 상태 보고서"를 참조하십시오.
COSO 준수 상태 링크	COSO 준수 상태 보고서를 엽니다. 자세한 내용은 816페이지 의 "COSO 준수 상태 보고서"를 참조하십시오.
ITIL 준수 상태 링크	ITIL 준수 상태 보고서를 엽니다. 자세한 내용은 820페이지 의 "ITIL 준수 상태 보고서"를 참조하십시오.
GLBA 준수 상태 링크	GLBA 준수 상태 보고서를 엽니다. 자세한 내용은 825페이지 의 "GLBA 준수 상태 보고서"를 참조하십시오.
HIPAA 준수 상태 링크	HIPAA 준수 상태 보고서를 엽니다. 자세한 내용은 829페이지 의 "HIPAA 준수 상태 보고서"를 참조하십시오.
Visa CISP(PCI 데이터 보안 표준) 준수 상태 링크	PCI 데이터 보안 표준(Visa CISP) 보고서를 엽니다. 자세한 내용은 838페이지 의 "Visa CISP(PCI 데이터 보안 표준) 준수 상태 보고서"를 참조하십시오.

COBIT 준수 상태 보고서

COBIT(Control Objectives for Information and related Technology)은 비즈니스 위험, 제어 요구 및 기술적인 문제들 간에 존재하는 괴리를 없애면서 IT 및 관련 프로세스에서 위험 대비 수익의 균형을 유지함으로써 관리 요구를 충족시킬 수 있도록 도와주는 내부 제어 프레임워크입니다.

NA에서는 COBIT에서 정의한 효과적인 내부 제어 시스템의 4가지 도메인 구현을 향상시킵니다.

- 모니터링 — NA에서는 프로세스를 모니터링하고 내부 제어 적합성을 평가하며 독립 보증을 보호하고 독립 감사를 제공합니다.
- 전달 및 지원 — NA에서는 서비스 수준, 타사 서비스, 성능 및 용량 관리, 지속적인 서비스 시스템 보안 보장, 비용 식별 및 할당, 사용자 교육 및 훈련, 고객 지원 및 조언, 구성, 데이터, 설비 및 운영 관리를 지원합니다.
- 계획 및 조직 — NA에서는 전략적 IT 계획 정의, 기술적 방향 결정, IT 투자 및 인사 관리, 관리 목표 및 지시 사항 전달, 외부 요구 사항 준수 보장을 지원합니다.
- 취득 및 구현 — NA에서는 자동화된 솔루션 식별, 기술 인프라 취득 및 유지 보수, 절차 개발 및 유지 보수, 시스템 설치 및 승인, 변경 관리를 지원합니다.

COBIT 및 NA에서 COBIT 구현을 향상시키는 방법에 대한 자세한 내용은 COBIT 상태 준수 페이지에서 "COBIT에 대한 자세한 정보와 HP Network Automation을 사용한 준수 실현" 링크를 클릭하십시오.

COBIT 준수 상태 보고서를 보려면

1. 보고서 아래의 메뉴 모음에서 준수 센터를 클릭합니다. 준수 센터 홈 페이지가 열립니다.
2. COBIT 준수 상태 링크를 클릭합니다. COBIT 준수 상태 페이지가 열립니다.

COBIT 준수 상태 페이지 필드

필드	설명/작업
모니터링	
M1 프로세스 모니터링	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 여러 개의 시작 및 실행 구성이 있는 장치. 장치 목록 링크를 클릭하면 장치 검색 결과 보고서가 열립니다. • 비활성 장치. 비활성 장치 링크를 클릭하면 장치 검색 결과 페이지가 열립니다. • ACL. 모든 ACL 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다. • ACL 사용 중. 사용 중인 ACL 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다. • ACL 변경 사항(최근 7일). ACL 변경 사항 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다. • 승인된 변경(최근 7일). 승인된 변경 링크를 클릭하면 승인된 변경 검색 결과 페이지가 열립니다.
M2 내부 제어 적합성 평가	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 적소에 있는 워크플로 규칙. 워크플로 설정 링크를 클릭하면 워크플로 마법사가 열립니다. • 적소에 있는 구성 정책. 구성 정책 링크를 클릭하면 정책 페이지가 열립니다. • 승인되지 않은 변경(최근 7일). 승인되지 않은 변경 링크를 클릭하면 승인되지 않은 변경 검색 결과 페이지가 열립니다.

필드	설명/작업
M3 독립 보증 획득	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • "정상" 상태를 표시하는 모니터. 시스템 상태 링크를 클릭하면 시스템 상태 보고서가 열립니다. • 소프트웨어 수준의 장치. 장치 소프트웨어 보고서 링크를 클릭하면 소프트웨어 수준 검색 결과 페이지가 열립니다. • 구성 정책 비준수 이벤트(최근 24시간). 구성 정책 이벤트(24시간) 링크를 클릭하면 구성 정책 활동 페이지가 열립니다. • 구성 정책 비준수 이벤트(최근 7일). 구성 정책 이벤트(7일) 링크를 클릭하면 구성 정책 활동 페이지가 열립니다. • 녹색 상태(임계값 내)의 구성 관리 "모범 사례". 네트워크 상태 보고서 링크를 클릭하면 네트워크 상태 보고서가 열립니다.
M4 독립 감사 제공	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 액세스 가능한 사용자 보고서. 사용자 및 시스템 보고서 링크를 클릭하면 사용자 및 시스템 보고서 페이지가 열립니다. • 액세스 가능한 시스템 보고서. 사용자 및 시스템 보고서 링크를 클릭하면 사용자 및 시스템 보고서가 열립니다.
전달 및 지원	
DS1 서비스 수준 정의 및 관리	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 녹색 상태(임계값 내)의 구성 관리 "모범 사례". 네트워크 상태 보고서 링크를 클릭하면 네트워크 상태 보고서가 열립니다. • 일별 평균 변경 사항(최근 7일간). 요약 보고서 링크를 클릭하면 요약 보고서가 열립니다. • 일별 평균 변경 사항(최근 30일간). 요약 보고서 링크를 클릭하면 요약 보고서가 열립니다.

필드	설명/작업
DS2 타사 서비스 관리	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 액세스 실패가 발생한 장치. 액세스 불가능 장치 링크를 클릭하면 장치 검색 결과 페이지가 열립니다. • 시작 및 실행 구성이 다른 장치. 장치 목록 링크를 클릭하면 장치 검색 결과 페이지가 열립니다. • 비활성 장치. 비활성 장치 링크를 클릭하면 장치 검색 결과 페이지가 열립니다.
DS3 성능 및 용량 관리	<p>포트 가용성이 10% 미만인 장치의 수를 표시합니다. 포트 가용성 링크를 클릭하면 장치 검색 결과 페이지가 열립니다.</p>
DS4 지속적인 서비스 보장	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 실행된 진단(최근 24시간). 진단(24시간) 링크를 클릭하면 진단 검색 결과 페이지가 열립니다. • 실행된 진단(최근 7일). 진단(7일) 링크를 클릭하면 진단 검색 결과 페이지가 열립니다.
DS5 시스템 보안 보장	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자가 특정 장치 집합으로 제한됨. 사용자 목록 링크를 클릭하면 사용자 검색 결과 페이지가 열립니다. • 관리자 액세스 권한이 할당된 사용자. 사용자 목록 링크를 클릭하면 모든 사용자 페이지가 열립니다. • 적소에 있는 장치 암호 규칙. 장치 암호 규칙 링크를 클릭하면 장치 암호 규칙 목록 페이지가 열립니다. • ACL. 모든 ACL 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다. • ACL 사용 중. 사용 중인 ACL 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다. • ACL 변경 사항(최근 7일). ACL 변경 사항 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다.
DS6 비용 식별 및 할당	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 인벤토리에 있는 장치. 장치 목록 링크를 클릭하면 인벤토리 페이지가 열립니다. • 인벤토리에 있는 모듈. 모듈 링크를 클릭하면 모듈 검색 결과 페이지가 열립니다.

필드	설명/작업
DS7 사용자 교육 및 훈련	<p>다음 문서에 대한 링크를 제공합니다.</p> <ul style="list-style-type: none"> • <i>HP 7.60 Network Automation 사용 설명서</i> • <i>HP 7.60 Network Automation 릴리스 노트</i>
DS8 고객 지원 및 조언	<p>다음에 대한 링크를 제공합니다.</p> <ul style="list-style-type: none"> • 드라이버 업데이트 패키지 다운로드 • 최신 릴리스 노트 보기 • 라이선스 정보 보기 • 기술 지원 티켓 생성 • 고객 지원 센터에 문의
DS9 구성 관리	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 감지된 구성 변경(최근 7일). 구성 변경 링크를 클릭하면 구성 검색 결과 페이지가 열립니다. • 저장된 장치 구성. 활성 구성 링크를 클릭하면 구성 검색 결과 페이지가 열립니다. • 승인이 보류 중인 변경. 승인이 보류 중인 변경 링크를 클릭하면 보류 중인 변경 검색 결과 페이지가 열립니다. • 승인된 변경(최근 7일). 승인된 변경 링크를 클릭하면 승인된 변경 검색 결과 페이지가 열립니다. • 승인되지 않은 변경(최근 7일). 승인되지 않은 변경 링크를 클릭하면 승인되지 않은 변경 검색 결과 페이지가 열립니다.
DS10 문제 및 인시던트 관리	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 감지된 구성 변경(최근 24시간). 대시보드 링크를 클릭하면 홈 페이지가 열립니다. • 발생한 NA 이벤트(최근 24시간). 대시보드 링크를 클릭하면 홈 페이지가 열립니다.
DS11 데이터 관리	<p>저장된 장치 구성의 수를 표시합니다.</p>

필드	설명/작업
DS12 설비 관리	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •인벤토리에 있는 장치. 장치 목록 링크를 클릭하면 인벤토리 페이지가 열립니다. •인벤토리에 있는 모듈. 모듈 링크를 클릭하면 모듈 검색 결과 페이지가 열립니다.
DS13 운영 관리	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •예약된 장치 변경 작업(다음 24시간). 보류 중인 작업(24시간) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. •예약된 장치 변경 작업(다음 7일). 보류 중인 작업(7일) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. •예약된 소프트웨어 배포(다음 24시간). 보류 중인 배포(24시간) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. •예약된 소프트웨어 배포(다음 7일). 보류 중인 배포(7일) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. •승인이 보류 중인 변경. 승인이 보류 중인 변경 링크를 클릭하면 보류 중인 변경 검색 결과 페이지가 열립니다.
계획 및 조직	
PO1 전략적 IP 계획 정의	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •인벤토리에 있는 장치. 장치 목록 링크를 클릭하면 장치 세부사항 페이지가 열립니다. •인벤토리에 있는 모듈. 모듈 링크를 클릭하면 모듈 검색 결과 페이지가 열립니다. •포트 가용성이 10% 미만인 장치의 수를 표시합니다. 포트 가용성 링크를 클릭하면 장치 검색 결과 페이지가 열립니다.

필드	설명/작업
PO2 정보 아키텍처 정의	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •인벤토리에 있는 장치. 장치 목록 링크를 클릭하면 인벤토리 페이지가 열립니다. •인벤토리에 있는 모듈. 모듈 링크를 클릭하면 모듈 검색 결과 페이지가 열립니다. •저장된 장치 구성. 활성 구성 링크를 클릭하면 구성 검색 결과 페이지가 열립니다.
PO3 기술적 방향 결정	<p>총 공급업체 수에서 인벤토리에 있는 장치의 수를 표시합니다. 공급업체별 장치 목록 링크를 클릭하면 인벤토리 페이지가 열립니다.</p>
PO4 IT 조직 및 관계 정의	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •사용자가 특정 장치 집합으로 제한됨. 사용자 목록 링크를 클릭하면 모든 사용자 페이지가 열립니다. •관리자 액세스 권한이 할당된 사용자. 사용자 목록 링크를 클릭하면 모든 사용자 페이지가 열립니다. •적소에 있는 장치 암호 규칙. 장치 암호 규칙 링크를 클릭하면 장치 암호 규칙 목록 페이지가 열립니다.
PO5 IT 투자 관리	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •인벤토리에 있는 장치. 장치 목록 링크를 클릭하면 인벤토리 페이지가 열립니다. •인벤토리에 있는 모듈. 모듈 링크를 클릭하면 모듈 검색 결과 페이지가 열립니다. •활성 상태가 아닌 장치. 장치 목록 링크를 클릭하면 인벤토리 페이지가 열립니다.
PO6 관리 목표 및 지시 사항 전달	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •녹색 상태(임계값 내)의 구성 관리 "모범 사례". 네트워크 상태 보고서 링크를 클릭하면 네트워크 상태 보고서가 열립니다. •활성 구성 정책. 구성 정책 링크를 클릭하면 구성 검색 결과 페이지가 열립니다.

필드	설명/작업
PO7 인사 관리	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자가 특정 장치 집합으로 제한됨. 사용자 목록 링크를 클릭하면 사용자 검색 결과 페이지가 열립니다. • 관리자 액세스 권한이 할당된 사용자. 사용자 목록 링크를 클릭하면 사용자 검색 결과 페이지가 열립니다. • 적소에 있는 장치 암호 규칙. 장치 암호 규칙 링크를 클릭하면 장치 암호 규칙 목록 페이지가 열립니다.
PO8 외부 요구 사항 준수 관리	<p>활성 구성 정책의 수를 표시합니다. 구성 정책 링크를 클릭하면 구성 검색 결과 페이지가 열립니다. 준수 센터 링크를 클릭하면 준수 센터 홈 페이지가 열립니다.</p>
PO9 위험 평가	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 녹색 상태(임계값 내)의 구성 관리 "모범 사례". 네트워크 상태 보고서 링크를 클릭하면 네트워크 상태 보고서가 열립니다. • 액세스 실패가 발생한 장치. 액세스 불가능 장치 링크를 클릭하면 장치 검색 결과 페이지가 열립니다. • 포트 가용성이 10% 미만인 장치의 수를 표시합니다. 포트 가용성 링크를 클릭하면 장치 검색 결과 페이지가 열립니다.
PO10 프로젝트 관리	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 예약된 장치 변경 작업(다음 24시간). 보류 중인 작업(24시간) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 예약된 장치 변경 작업(다음 7일). 보류 중인 작업(7일) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 예약된 소프트웨어 배포(다음 24시간). 보류 중인 배포(24시간) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 예약된 소프트웨어 배포(다음 7일). 보류 중인 배포(7일) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다.

필드	설명/작업
PO11 품질 관리	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • "정상" 상태를 표시하는 모니터. 시스템 상태 링크를 클릭하면 시스템 상태 보고서가 열립니다. • 소프트웨어 준수 상태의 장치. 장치 소프트웨어 보고서 링크를 클릭하면 소프트웨어 준수 검색 결과 페이지가 열립니다. • 구성 정책 비준수 이벤트(최근 24시간). 정책 이벤트(24시간) 링크를 클릭하면 구성 정책 활동 페이지가 열립니다. • 구성 정책 비준수 이벤트(최근 7일). 정책 이벤트(7일) 링크를 클릭하면 구성 정책 활동 페이지가 열립니다. • 녹색 상태(임계값 내)의 구성 관리 "모범 사례". 네트워크 상태 보고서 링크를 클릭하면 네트워크 상태 보고서가 열립니다.
취득 및 구현	
AI1 자동화된 솔루션 식별	<p>다음 기본 링크를 제공합니다.</p> <ul style="list-style-type: none"> • 데이터베이스를 정리하는 시스템 작업이 매주 실행됩니다. 보류 중인 작업 링크를 클릭하여 보류 중인 작업 페이지를 엽니다. • 모듈 인벤토리 데이터를 수집하는 시스템 작업이 매주 실행됩니다. 보류 중인 작업 링크를 클릭하여 예약된 작업 페이지를 엽니다. • 요약 보고서를 업데이트하는 시스템 작업이 매일 실행됩니다. 보류 중인 작업 링크를 클릭하여 예약된 작업 페이지를 엽니다. • 장치 구성 변경 사항에 대해 폴링할 시스템 작업이 매일 실행됩니다. 보류 중인 작업 링크를 클릭하여 예약된 작업 페이지를 엽니다.
AI2 응용 프로그램 소프트웨어 취득 및 유지 보수	<p>이는 해당되지 않습니다.</p>

필드	설명/작업
AI3 기술 인프라 취득 및 유지 보수	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 인벤토리에 있는 장치. 장치 목록 링크를 클릭하면 인벤토리 페이지가 열립니다. • 인벤토리에 있는 모듈. 모듈 링크를 클릭하면 모듈 검색 결과 페이지가 열립니다. • 저장된 장치 구성. 활성 구성 링크를 클릭하면 구성 검색 결과 페이지가 열립니다.
AI4 절차 개발 및 유지 보수	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 녹색 상태(임계값 내)의 구성 관리 "모범 사례". 네트워크 상태 보고서 링크를 클릭하면 네트워크 상태 보고서가 열립니다. • 활성 구성 정책. 구성 정책 링크를 클릭하면 구성 검색 결과 페이지가 열립니다.
AI5 시스템 설치 및 승인	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • "정상" 상태를 표시하는 모니터. 시스템 상태 링크를 클릭하면 시스템 상태 보고서가 열립니다. • 장치 소프트웨어 준수. 장치 소프트웨어 보고서 링크를 클릭하면 소프트웨어 수준 검색 결과 페이지가 열립니다. • 녹색 상태(임계값 내)의 구성 관리 "모범 사례". 네트워크 상태 보고서 링크를 클릭하면 네트워크 상태 보고서가 열립니다.

필드	설명/작업
AI6 변경 관리	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none">• 텔넷/SSH 프록시 세션(최근 7일). 세션 링크를 클릭하면 세션 검색 결과 페이지가 열립니다.• 예약된 장치 변경 작업(최근 7일). 지난 작업(7일) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다.• 예약된 장치 변경 작업(다음 7일). 보류 중인 작업(7일) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다.• 승인이 보류 중인 변경. 승인이 보류 중인 변경 링크를 클릭하면 보류 중인 변경 검색 결과 페이지가 열립니다.• 승인된 변경(최근 7일). 승인된 변경 링크를 클릭하면 승인된 변경 검색 결과 페이지가 열립니다.• 승인되지 않은 변경(최근 7일). 승인되지 않은 변경 링크를 클릭하면 승인되지 않은 변경 검색 결과 페이지가 열립니다.

COSO 준수 상태 보고서

1992년 COSO(Committee of Sponsoring Organizations of the Treadway Commission)에서는 내부 제어에 대한 획기적인 보고서를 발행했습니다. "COSO"라고 하는 *내부 제어-통합 프레임워크*는 내부 제어 시스템을 설정하고 그 효율성을 확인하기 위한 기초를 제공합니다.

NA에서는 효과적인 내부 제어 시스템의 5가지 필수 구성 요소를 제공합니다.

- 제어 환경 — 기본적인 규율 및 구조를 제공하여 내부 제어 시스템에 대한 기초를 수립합니다.
- 위험 평가 — 목표 실현과 관련된 위험을 관리 부서에서 식별 및 분석합니다.
- 제어 활동 — 관리 목표가 실현되고 위험 완화 전략이 수행되도록 합니다.
- 정보 및 통신 — 직원에게 제어 책임을 전달하고 사람들이 자신의 직무를 수행할 수 있도록 양식과 타임프레임 형태로 정보를 제공하여 다른 모든 제어 구성 요소를 지원합니다.
- 모니터링 — 프로세스 외부의 타사나 관리 부서에 의한 내부 제어의 외부 누락 사항이 포함됩니다.

COSO에 대한 자세한 내용은 "COSO에 대한 자세한 정보와 HP Network Automation을 사용한 준수 실현" 링크를 클릭하십시오.

COSO 준수 상태 보고서를 보려면

1. 보고서 아래의 메뉴 모음에서 준수 센터를 클릭합니다. 준수 센터 홈 페이지가 열립니다.
2. COSO 준수 상태 링크를 클릭합니다. COSO 준수 상태 페이지가 열립니다.

COSO 준수 상태 페이지 필드

필드	설명/작업
제어 환경	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none">• 사용자가 특정 장치 집합으로 제한됨. 사용자 목록 링크를 클릭하면 사용자 검색 결과 페이지가 열립니다.• 관리자 액세스 권한이 할당된 사용자. 사용자 목록 링크를 클릭하면 사용자 검색 결과 페이지가 열립니다.• 적소에 있는 장치 암호 규칙. 장치 암호 규칙 링크를 클릭하면 장치 암호 규칙 목록 페이지가 열립니다.• 적소에 있는 구성 정책. 구성 정책 링크를 클릭하면 정책 페이지가 열립니다.• 적소에 있는 워크플로 규칙. 워크플로 설정 링크를 클릭하면 워크플로 마법사가 열립니다.• ACL. 모든 ACL 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다.• ACL 사용 중. 사용 중인 ACL 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다.
위험 평가	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none">• 녹색 상태(임계값 내)의 구성 관리 "모범 사례". 네트워크 상태 보고서 링크를 클릭하면 네트워크 상태 보고서가 열립니다.• 액세스 실패가 발생한 장치. 액세스 불가능 장치 링크를 클릭하면 장치 검색 결과 페이지가 열립니다.• 포트 가용성이 10% 미만인 장치의 수를 표시합니다. 포트 가용성 링크를 클릭하면 장치 검색 결과 페이지가 열립니다.

필드	설명/작업
제어 활동	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 텔넷/SSH 프록시 세션(최근 7일). 세션 링크를 클릭하면 세션 검색 결과 페이지가 열립니다. • 예약된 장치 변경 작업(다음 24시간). 보류 중인 작업(24시간) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 예약된 장치 변경 작업(다음 7일). 보류 중인 작업(7일) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 예약된 소프트웨어 배포(다음 24시간). 보류 중인 배포(24시간) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 예약된 소프트웨어 배포(다음 7일). 보류 중인 배포(7일) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 승인이 보류 중인 변경. 승인이 보류 중인 변경 링크를 클릭하면 보류 중인 변경 검색 결과 페이지가 열립니다.
정보 및 통신	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 감지된 구성 변경(최근 24시간). 대시보드 링크를 클릭하면 홈 페이지가 열립니다. • 발생한 NA 이벤트(최근 24시간). 대시보드 링크를 클릭하면 홈 페이지가 열립니다. • 일별 평균 변경 사항 개수(최근 7일간). 요약 보고서 링크를 클릭하면 요약 보고서가 열립니다. • 일별 평균 변경 사항 개수(최근 30일간). 요약 보고서 링크를 클릭하면 요약 보고서가 열립니다.

필드	설명/작업
모니터링	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • "정상" 상태를 표시하는 모니터. 시스템 상태 링크를 클릭하면 시스템 상태 보고서가 열립니다. • 장치 소프트웨어 준수. 장치 소프트웨어 보고서 링크를 클릭하면 소프트웨어 준수 검색 결과 페이지가 열립니다. • 구성 정책 비준수 이벤트(최근 24시간). 구성 정책 이벤트(24시간) 링크를 클릭하면 구성 정책 활동 페이지가 열립니다. • 구성 정책 비준수 이벤트(최근 7일). 구성 정책 이벤트(7일) 링크를 클릭하면 구성 정책 활동 페이지가 열립니다. • 시작 및 실행 구성이 다른 장치. 장치 목록 링크를 클릭하면 장치 검색 결과 페이지가 열립니다. • 비활성 장치. 비활성 장치 링크를 클릭하면 장치 검색 결과 페이지가 열립니다. • 승인된 변경(최근 7일). 승인된 변경 링크를 클릭하면 승인된 변경 검색 결과 페이지가 열립니다. • 승인되지 않은 변경(최근 7일). 승인되지 않은 변경 링크를 클릭하면 승인되지 않은 변경 검색 결과 페이지가 열립니다. • ACL 변경 사항(최근 7일). ACL 변경 사항 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다.

ITIL 준수 상태 보고서

ITIL(IT Infrastructure Library)은 CCTA(현재는 OGC(Office of Government Commerce))에서 영국 정부용으로 개발한 표준으로, 전 세계에 걸쳐 IT 서비스 규정 관련 모범 사례 표준으로 빠르게 채택되고 있습니다. ITIL의 세 가지 주요 영역에는 다음이 포함됩니다.

- 서비스 지원 — IT 서비스가 효과적으로 제공될 수 있도록 합니다.
- 서비스 전달 — IT 서비스를 관리할 수 있도록 합니다.
- 보안 관리 — 데이터 및 인프라를 보호할 수 있도록 합니다.

ITIL에 대한 자세한 내용은 "ITIL에 대한 자세한 정보와 HP Network Automation을 사용한 준수 실현" 링크를 클릭하십시오.

ITIL 준수 상태 보고서를 보려면

1. 보고서 아래의 메뉴 모음에서 준수 센터를 클릭합니다. 준수 센터 홈 페이지가 열립니다.
2. ITIL 준수 상태 링크를 클릭합니다. ITIL 준수 상태 페이지가 열립니다.

ITIL 준수 상태 페이지 필드

필드	설명/작업
구성 관리	
서비스 지원 프로세스	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 감지된 구성 변경(최근 7일). 구성 변경 링크를 클릭하면 구성 검색 결과 페이지가 열립니다. • 저장된 장치 구성. 활성 구성 링크를 클릭하면 구성 검색 결과 페이지가 열립니다.

필드	설명/작업
인시던트 관리	
서비스 지원 프로세스	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 감지된 구성 변경(최근 24시간). 대시보드 링크를 클릭하면 홈 페이지가 열립니다. • 발생한 NA 이벤트(최근 24시간). 대시보드 링크를 클릭하면 홈 페이지가 열립니다.
문제 관리	
서비스 지원 프로세스	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 녹색 상태(임계값 내)의 구성 관리 "모범 사례". 네트워크 상태 보고서 링크를 클릭하면 네트워크 상태 보고서가 열립니다. • 액세스 실패가 발생한 장치. 액세스 불가능 장치 링크를 클릭하면 장치 검색 결과 페이지가 열립니다.
변경 관리	
서비스 지원 프로세스	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 텔넷/SSH 프록시 세션(최근 7일). 세션 링크를 클릭하면 세션 검색 결과 페이지가 열립니다. • 예약된 장치 변경 작업(다음 24시간). 보류 중인 작업(24시간) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 예약된 장치 변경 작업(다음 7일). 보류 중인 작업(7일) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 승인이 보류 중인 변경. 승인이 보류 중인 변경 링크를 클릭하면 보류 중인 변경 검색 결과 페이지가 열립니다. • 승인된 변경(최근 7일). 승인된 변경 링크를 클릭하면 승인된 변경 검색 결과 페이지가 열립니다. • 승인되지 않은 변경(최근 7일). 승인되지 않은 변경 링크를 클릭하면 승인되지 않은 변경 검색 결과 페이지가 열립니다. • 적소에 있는 구성 정책. 구성 정책 링크를 클릭하면 정책 페이지가 열립니다. • 적소에 있는 워크플로 규칙. 워크플로 설정 페이지를 클릭하면 워크플로 마법사가 열립니다.

필드	설명/작업
서비스 데스크	
서비스 지원 기능	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 예약된 장치 변경 작업(다음 24시간). 보류 중인 작업(24시간) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 예약된 장치 변경 작업(다음 7일). 보류 중인 작업(7일) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다.
릴리스 관리	
서비스 지원 프로세스	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 예약된 소프트웨어 배포(다음 24시간). 보류 중인 배포(24시간) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 예약된 소프트웨어 배포(다음 7일). 보류 중인 배포(7일) 링크를 클릭하면 작업 검색 결과 페이지가 열립니다. • 소프트웨어 준수 상태의 장치. 장치 소프트웨어 보고서 링크를 클릭하면 소프트웨어 준수 검색 결과 페이지가 열립니다.
서비스 수준 관리	
서비스 전달 프로세스	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 녹색 상태(임계값 내)의 구성 관리 "모범 사례". 네트워크 상태 보고서 링크를 클릭하면 네트워크 상태 보고서가 열립니다. • 일별 평균 변경 사항(최근 7일간). 요약 보고서 링크를 클릭하면 요약 보고서가 열립니다. • 일별 평균 변경 사항(최근 30일간). 요약 보고서 링크를 클릭하면 요약 보고서가 열립니다.
용량 관리	
서비스 전달 프로세스	<p>포트 가용성이 10% 미만인 장치의 수를 표시합니다. 포트 가용성 링크를 클릭하면 장치 검색 결과 페이지가 열립니다.</p>

필드	설명/작업
연속성 관리	
서비스 전달 프로세스	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 실행된 진단(최근 24시간). 진단(24시간) 링크를 클릭하면 진단 검색 결과 페이지가 열립니다. • 실행된 진단(최근 7일). 진단(7일) 링크를 클릭하면 진단 검색 결과 페이지가 열립니다.
가용성 관리	
서비스 전달 프로세스	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 구성 정책 비준수 이벤트(최근 24시간). 구성 정책 이벤트(24시간) 링크를 클릭하면 구성 정책 활동 페이지가 열립니다. • 구성 정책 비준수 이벤트(최근 7일). 구성 정책 이벤트(7일) 링크를 클릭하면 구성 정책 활동 페이지가 열립니다.
IT 재무 관리	
서비스 전달 프로세스	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • "정상" 상태를 표시하는 모니터. 시스템 상태 링크를 클릭하면 시스템 상태 보고서가 열립니다. • 인벤토리에 있는 장치. 장치 목록 링크를 클릭하면 인벤토리 페이지가 열립니다. • 인벤토리에 있는 모듈. 모듈 링크를 클릭하면 모듈 검색 결과 페이지가 열립니다.

필드	설명/작업
보안 관리	
서비스 전달 프로세스	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none">• 사용자가 특정 장치 집합으로 제한됨. 사용자 목록 링크를 클릭하면 모든 사용자 페이지가 열립니다.• 관리자 액세스 권한이 할당된 사용자. 사용자 목록 링크를 클릭하면 사용자 검색 결과 페이지가 열립니다.• 적소에 있는 장치 암호 규칙. 장치 암호 규칙 링크를 클릭하면 장치 암호 규칙 목록 페이지가 열립니다.• ACL. 모든 ACL 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다.• ACL 사용 중. 사용 중인 ACL 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다.• ACL 변경 사항(최근 7일). ACL 변경 사항 링크를 클릭하면 ACL 검색 결과 페이지가 열립니다.

GLBA 준수 상태 보고서

Gramm-Leach-Bliley Act(GLBA)라고도 하는 Financial Modernization Act of 1999에는 금융 기관에서 보유하는 소비자의 개인 금융 정보를 보호하기 위한 규정이 포함되어 있습니다. 개인 정보 보호 요구 사항에는 세 가지 기본 사항이 있습니다.

- 위장 규정
- 금융 개인 정보 보호 규칙
- 보호 조치 규칙

보호 조치 규칙에서는 모든 금융 조직이 고객 정보를 보호하기 위한 보호 조치를 설계, 구현 및 유지하도록 규정하고 있습니다. 보호 조치 규칙은 자사 고객으로부터 정보를 수집하는 금융 기관뿐만 아니라 다른 금융 기관의 고객 정보를 받는 신용 보고 기관과 같은 금융 기관에도 적용됩니다.

GLBA에 대한 자세한 내용은 "GLBA에 대한 자세한 정보와 HP Network Automation을 사용한 준수 실현" 링크를 클릭하십시오.

GLBA 준수 상태 보고서를 보려면

1. 보고서 아래의 메뉴 모음에서 준수 센터를 클릭합니다. 준수 센터 홈 페이지가 열립니다.
2. GLBA 준수 상태 링크를 클릭합니다. GLBA 준수 상태 페이지가 열립니다.

GLBA 준수 상태 페이지 필드

필드	설명/작업
공동 지침 섹션	
II.A. 정보 보안 프로그램	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •인벤토리에 있는 장치 •인벤토리에 있는 모듈 •저장된 장치 구성
II.B. 목표	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •사용자가 특정 장치 그룹으로 제한됨 •관리자 권한이 할당된 사용자 •실패한 사용자 로그인 시도(지난 7일) •승인이 보류 중인 변경 •승인된 변경(최근 7일) •승인되지 않은 변경(지난 7일) •ACL 식별됨 •ACL 사용 중 •ACL 변경 사항(지난 7일)
III.A. 이사회 참여	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •사용 가능한 사용자 보고서 •사용 가능한 시스템 보고서
III.B. 위험 평가	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •녹색 상태의 구성 관리 "모범 사례" •장치 소프트웨어 수준 •"정상" 상태의 모니터 •액세스 실패가 발생한 장치 •포트 가용성이 10% 미만인 장치 •여러 개의 시작 및 실행 구성이 있는 장치

필드	설명/작업
III.C.1. 위험 관리 및 제어(정책 및 절차)	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 적소에 있는 워크플로 규칙 • 적소에 있는 구성 정책 • 적소에 있는 장치 암호 규칙
III.C.2. 위험 관리 및 제어(교육)	<p>다음 HP 문서에 액세스할 수 있습니다.</p> <ul style="list-style-type: none"> • <i>HP 7.60 Network Automation 사용 설명서</i> • <i>HP 7.60 Network Automation 릴리스 노트</i>
III.C.3. 위험 관리 및 제어(테스트)	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 구성 정책 비준수 이벤트(지난 24시간) • 구성 정책 비준수 이벤트(지난 7일) • 소프트웨어 수준이 아닌 장치 • 실행된 진단(지난 24시간) • 실행된 진단(지난 7일)
III.D. 서비스 공급자 협의 감독	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 저장된 구성 • 여러 개의 시작 및 실행 구성이 있는 장치 • 비활성 장치 • 액세스 실패가 발생한 장치.
III.E. 프로그램 조정	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자가 지난 달에 추가됨 • 추가된 장치(지난 달) • 추가된 장치 그룹(지난 달) • 저장된 구성(지난 달)

필드	설명/작업
III.F. 이사회에 보고	다음을 표시합니다. <ul style="list-style-type: none">• 녹색 상태의 구성 관리 "모범 사례" 수• 시스템 상태 보고서• 요약 보고서• HP Network Automation 준수 센터
III.G. 표준 구현	이 요구 사항은 NA의 범위를 벗어났습니다.

HIPAA 준수 상태 보고서

HIPAA는 Health Insurance Portability & Accountability Act of 1996입니다. 최종 HIPAA 보안 규칙은 2003년 2월 20일에 발표되었습니다. 최종 규칙에 따르면 대상 엔티티에는 PHI(보호된 건강 정보)를 전자 형태로 처리, 전송 및/또는 저장하는 HHS(Department of Health and Human Services: 보건 복지부) 의료 프로그램, 연방 기관에서 운영하는 건강 보험사 또는 연방 기관에서 제공하는 건강 관리 서비스, 주에서 주관하는 메디케이드(저소득층 의료 보험) 기관, 사설 건강 보험사, 보건 공급자 및 보건 정보 센터가 포함됩니다.

HIPAA에 대한 자세한 내용은 "HIPAA에 대한 자세한 정보와 HP Network Automation을 사용한 준수 실현" 링크를 클릭하십시오.

HIPAA 준수 상태 보고서를 보려면

1. 보고서 아래의 메뉴 모음에서 준수 센터를 클릭합니다. 준수 센터 홈 페이지가 열립니다.
2. HIPAA 준수 상태 링크를 클릭합니다. HIPAA 준수 상태 페이지가 열립니다.

HIPAA 준수 상태 페이지 필드

필드	설명/작업
보안 표준: 일반 규칙	
(1) 대상 엔티티가 생성, 수신, 유지 또는 전송하는 전자적으로 보호된 모든 건강 정보의 기밀성, 무결성 및 가용성을 보장합니다.	다음의 수를 표시합니다. <ul style="list-style-type: none">• 저장된 장치 구성• 액세스 실패가 발생한 장치• 포트 가용성이 10% 미만인 장치
(2) 이러한 정보의 보안이나 무결성에 대해 적절하게 예측된 위협이나 위험으로부터 보호합니다.	다음의 수를 표시합니다. <ul style="list-style-type: none">• 실패한 사용자 로그인 시도(지난 7일)• ACL 식별됨• ACL 사용 중• ACL 변경 사항(지난 7일)

필드	설명/작업
(3) 이 파트의 하위 파트 E에서 허용하지 않거나 필요로 하지 않는 예측된 사용이나 공개로부터 보호합니다.	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자가 특정 장치 집합으로 제한됨 • 관리자 액세스 권한이 할당된 사용자
(4) 이 하위 파트에 대한 준수를 직원별로 관리합니다.	HP Network Automation 준수 센터 HIPAA 준수 상태 보고서를 열 수 있습니다.
관리 보호 조치	
(A) 위험 분석(필수). 대상 엔티티가 보유하는 전자적으로 보호된 건강 정보의 기밀성, 무결성 및 가용성에 대한 잠재적 위험 및 취약점을 정확하고 철저하게 평가합니다.	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 녹색 상태의 구성 관리 "모범 사례" • 소프트웨어 수준의 장치 • "정상" 상태의 모니터 • 액세스 실패가 발생한 장치 • 포트 가용성이 10% 미만인 장치 • 소프트웨어 취약점이 감지됨 • 여러 개의 시작 및 실행 구성이 있는 장치
(B) 위험 관리(필수). 위험과 취약점을 합리적이고 적절한 수준으로 충분히 줄일 수 있는 164.306(a)를 준수하는 보안 방법을 구현합니다.	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 적소에 있는 워크플로 규칙 • 활성 구성 정책 • 적소에 있는 장치 암호 규칙
(C) 제재 정책(필수). 대상 엔티티의 보안 정책 및 절차를 준수하지 못하는 직원 구성원에 대해 적절한 제재를 적용합니다.	이 요구 사항은 NA의 범위를 벗어났습니다.

필드	설명/작업
<p>(D) 정보 시스템 활동 검토(필수). 감사 로그, 액세스 보고서 및 보안 인시던트 추적 보고서 등 정보 시스템 활동에 대한 레코드를 정기적으로 검토하기 위한 절차를 구현합니다.</p> <p>엔티티에 대한 이 하위 파트에 필요한 정책과 절차의 개발 및 구현을 담당하는 보안 관계자를 식별합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자 로그인 시도(지난 7일) • 사용자 추가됨(지난 7일) • 사용자 삭제됨(지난 7일) • 변경된 사용자 권한(지난 7일) • 변경된 구성 정책(지난 7일) • 추가된 구성 정책(지난 7일) <p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>직원 보안</p> <p>(A) 인증 및/또는 감독(선택). 전자적으로 보호된 건강 정보를 사용하거나 그러한 정보를 액세스할 수 있는 위치에서 작업 중인 직원에 대한 인증 및/또는 감독 절차를 구현합니다.</p> <p>(B) 직원 정보 취급 허가 절차(선택). 전자적으로 보호되는 건강 정보에 대한 직원의 액세스가 적절한지 확인하기 위한 절차를 구현합니다.</p> <p>(C) 종료 절차(선택). 이 섹션의 (a)(3)(ii)(B) 단락에 지정된 확인 사항에 필요할 경우 또는 직원 고용이 종료될 때 전자적으로 보호된 건강 정보에 대한 액세스를 종료하기 위한 절차를 구현합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자가 특정 장치 그룹으로 제한됨 • 승인된 변경(최근 7일) • 승인되지 않은 변경(최근 7일) <p>관리자 액세스 권한이 할당된 사용자 수를 표시합니다.</p> <p>삭제된 사용자의 수를 표시합니다(지난 7일).</p>

필드	설명/작업
<p>정보 액세스 관리</p> <p>(A) 보건 정보 센터 기능 분리(필수). 보건 정보 센터가 대규모 조직의 일부인 경우 이 정보 센터는 정보 센터에서 보유하는 전자적으로 보호된 건강 정보를 대규모 조직의 무단 액세스로부터 보호하는 정책 및 절차를 구현해야 합니다.</p> <p>(B) 액세스 인증(선택). 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스 등 전자적으로 보호된 건강 정보에 대한 액세스 권한을 허가하기 위한 정책 및 절차를 구현합니다.</p> <p>(C) 액세스 설정 및 수정(선택). 엔티티의 액세스 인증 정책에 기반을 두고 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 설정, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자가 특정 장치 그룹으로 제한됨 • 제한된(비관리자) 액세스 권한이 할당된 사용자 <p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자가 특정 장치 그룹으로 제한됨 • 제한된(비관리자) 액세스 권한이 할당된 사용자 <p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • HP Network Automation에서 활성화된 사용자 계정 • HP Network Automation에서 비활성화된 사용자 계정
<p>보안 인식 및 교육</p> <p>(A) 보안 미리 알림(선택). 정기적인 보안 업데이트입니다.</p> <p>(B) 악성 소프트웨어로부터 보호(선택). 악성 소프트웨어로부터 보호하고 이를 감지 및 보고하기 위한 절차입니다.</p> <p>(C) 로그인 모니터링(선택). 로그인 시도와 보고 불일치를 모니터링하기 위한 절차입니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • HP Network Automation에서 활성화된 사용자 계정 • HP Network Automation에서 비활성화된 사용자 계정 <p>이 요구 사항은 NA의 범위를 벗어났습니다.</p> <p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자 로그인 시도(지난 7일) • 실패한 사용자 로그인 시도(지난 7일)

필드	설명/작업
(D) 암호 관리(선택). 암호 생성, 변경 및 보호 조치 절차입니다.	NA 암호 변경의 수를 표시합니다(지난 7일).
보안 인시던트 절차	
대응과 보고(필수). 의심되거나 알려진 보안 인시던트를 식별하고 그에 대응하며, 대상 엔티티에게 알려져 있는 보안 인시던트의 유해 효과를 가능한 정도까지 완화하고, 보안 인시던트 및 그 결과를 문서화합니다.	다음의 수를 표시합니다. <ul style="list-style-type: none"> • 사용자 로그인 시도(지난 7일) • 실패한 사용자 로그인 시도(지난 7일) • 감지된 구성 변경(지난 7일)
비상 계획	
(A) 데이터 백업 계획(필수). 전자적으로 보호된 건강 정보의 검색 가능한 정확한 복사본을 생성 및 유지 관리하기 위한 절차를 설정하고 구현합니다.	NA에서는 전자적으로 보호된 건강 정보를 생성하거나 유지하지 않습니다.
(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 설정하고 필요에 따라 구현합니다.	NA는 데이터 손실이 없는 자동(또는 수동) 장애 조치 및 자동 장애 감지를 지원하기 위해 구현할 수 있는 HA(고가용성) 시스템입니다.
(C) 응급 모드 운영 계획(필수). 응급 모드로 운영되는 동안 전자적으로 보호된 건강 정보의 보안 유지를 위해 중요 비즈니스 프로세스의 연속성을 활성화할 절차를 설정하고 필요에 따라 구현합니다.	NA는 데이터 손실이 없는 자동(또는 수동) 장애 조치 및 자동 장애 감지를 지원하기 위해 구현할 수 있는 HA(고가용성) 시스템입니다.
(D) 테스트 및 개정 절차(선택). 비상 계획의 정기적인 테스트 및 수정을 위한 절차를 구현합니다.	NA에서는 자동 장애 감지 및 자동(또는 수동) 장애 조치에 대한 정기적인 테스트를 지원합니다.
(E) 응용 프로그램 및 데이터 위험성 분석(선택). 다양한 비상 계획 구성 요소를 지원하면서 특정 응용 프로그램 및 데이터의 상대적 위험성을 평가합니다.	NA의 견고한 보고 기능은 다양한 비상 계획 구성 요소와 관련되어 NA의 상대적 위험성을 평가할 수 있는 기초를 제공합니다.

필드	설명/작업
<p>평가</p> <p>기술적 및 비기술적인 평가를 정기적으로 수행합니다.</p> <p>서면 계약 또는 기타 협의(필수). 164.314(a)의 해당 요구 사항을 충족하는 비즈니스 관계자와의 서면 계약이나 다른 협의를 통해 이 섹션의 (b)(1) 단락에서 요구하는 충분한 보증을 문서화합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자가 특정 장치 그룹으로 제한됨 • 관리자 액세스 권한이 할당된 사용자 • 적소에 있는 워크플로 규칙 워크플로 설정 페이지를 클릭하면 워크플로 마법사가 열립니다. • 적소에 있는 구성 정책 • 적소에 있는 장치 암호 규칙 <p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>물리 보호 조치</p> <p>(i) 비상 운영(선택). 응급 상황 시 응급 모드 운영 계획과 재해 복구 계획에서 손실된 데이터 복원 지원에 대한 설비 액세스를 허용하는 절차를 설정하고 필요에 따라 구현합니다.</p> <p>(ii) 설비 보안 계획(선택). 설비 및 장비의 무단 물리적 액세스, 변조 또는 도난으로부터 보호할 정책 및 절차를 구현합니다.</p> <p>(iii) 액세스 제어 및 유효성 검사 절차(선택). 테스트 및 변경을 위한 소프트웨어 프로그램 액세스 제어와 방문자 제어 등 역할이나 기능에 따라 사용자의 설비 액세스를 제어하고 확인하기 위한 절차를 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p> <p>이 요구 사항은 NA의 범위를 벗어났습니다.</p> <p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자 로그인 시도(지난 7일) • 실패한 사용자 로그인 시도(지난 7일) • 사용자가 특정 장치 그룹으로 제한됨 • 제한된(비관리자) 액세스 권한이 할당된 사용자

필드	설명/작업
<p>(iv) 유지 보수 레코드(선택). 보안과 관련된 설비의 물리적 구성 요소(예: 하드웨어, 벽, 문 및 잠금 장치)에 대한 수리 및 수정 사항을 문서화하기 위한 정책 및 절차를 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>워크스테이션 사용</p>	
<p>수행할 올바른 기능을 지정하는 정책 및 절차를 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>액세스를 인증 사용자로 제한하기 위해 전자적으로 보호된 건강 정보에 액세스하는 모든 워크스테이션에 대한 물리 보호 조치를 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>장치 및 미디어 제어</p>	
<p>(i) 폐기(필수). 전자적으로 보호된 건강 정보 및/또는 보관된 하드웨어 또는 전자 미디어의 최종 폐기를 다룰 정책 및 절차를 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>(ii) 미디어 재사용(필수). 미디어를 재사용 가능한 상태로 만들기 전에 전자 미디어에서 전자적으로 보호된 건강 정보를 제거하는 절차를 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>(iii) 책임(선택). 하드웨어 및 전자 미디어의 이동과 이를 담당하는 담당자에 대한 레코드를 유지합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>(iv) 데이터 백업 및 저장(선택). 장비 이동 전에 필요할 경우 전자적으로 보호된 건강 정보의 검색 가능한 정확한 복사본을 생성합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>

필드	설명/작업
<p>기술 보호 조치</p> <p>(i) 고유 사용자 ID(필수). 사용자 ID를 식별 및 추적하기 위한 고유 이름 및/또는 번호를 할당합니다.</p> <p>(ii) 응급 액세스 절차(필수). 응급 상황 시 전자적으로 보호된 필요한 건강 정보를 얻기 위한 절차를 설정하고 필요에 따라 구현합니다.</p> <p>(iii) 자동 로그오프(선택). 미리 지정된 비활성 시간이 경과된 후 전자 세션을 종료하는 전자 절차를 구현합니다.</p> <p>(iv) 암호화 및 암호 해독(선택). 전자적으로 보호된 건강 정보를 암호화 및 암호 해독하는 메커니즘을 구현합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •HP Network Automation에서 활성화된 사용자 계정 •HP Network Automation에서 비활성화된 사용자 계정 <p>HP Network Automation은 데이터 손실이 없는 자동(또는 수동) 장애 조치 및 자동 장애 감지를 지원하기 위해 구현할 수 있는 HA(고가용성) 시스템입니다.</p> <p>비활성 시간(1800초)이 경과된 후 종료되는 웹 사용자 세션. 기본값은 1800입니다. 이 값은 구성할 수 있습니다.</p> <p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>감사 제어</p> <p>전자적으로 보호된 건강 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록 및 검사하는 하드웨어, 소프트웨어 및/또는 절차 메커니즘을 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>표준 무결성</p> <p>전자적으로 보호된 건강 정보를 인증하기 위한 메커니즘(선택). 전자적으로 보호된 건강 정보가 무단으로 변경 또는 삭제되지 않았음을 입증하기 위한 전자 메커니즘을 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>

필드	설명/작업
<p>사람 또는 엔티티 인증</p>	
<p>전자적으로 보호된 건강 정보에 대한 액세스를 필요로 하는 사용자나 엔티티가 요구된 대상인지 검증하는 절차를 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>전송 보안</p>	
<p>(i) 무결성 제어(선택). 전자적으로 전송 및 보호된 건강 정보가 폐기될 때까지 발견되지 않고 잘못 수정되지 않도록 하기 위한 보안 방법을 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>(ii) 암호화(선택). 적절하다고 생각될 때마다 전자적으로 보호된 건강 정보를 암호화하는 메커니즘을 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>정책 및 절차</p>	
<p>표준, 구현 사양 또는 기타 요구 사항을 준수하기 위한 합리적이고 적절한 정책 및 절차를 구현합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>문서</p>	
<p>(i) 시간 제한(필수). 생성 날짜 이후로 6년 동안 또는 마지막 시행 날짜까지(둘 중 더 늦은 날짜 적용) 이 섹션의 (b)(1) 단락에 필요한 문서를 보존합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>(ii) 가용성(필수). 문서를 문서와 관련된 절차를 구현할 책임이 있는 담당자가 사용할 수 있도록 합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>(iii) 업데이트(필수). 전자적으로 보호된 건강 정보의 보안에 적용되는 환경 또는 운영 변경과 관련하여 정기적으로 문서를 검토하고 필요에 따라 업데이트합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>

Visa CISP(PCI 데이터 보안 표준) 준수 상태 보고서

데이터 도난으로부터 대처하고 소비자의 신뢰를 유지하기 위한 노력으로 모든 주요 신용 카드 발급 업체에서는 다음을 포함하는 상세 보안 프로그램을 공식적으로 발표했습니다.

- Visa USA CISP(카드 소유자 정보 보안 프로그램)
- MasterCard SDP(Site Data Protection) 프로그램
- DISC(Discover Information Security and Compliance) 프로그램
- American Express DSOP(Data Security Operating Policy)

2004년 후반 Visa 및 MasterCard사는 PCI(신용 카드 산업) 데이터 보안 표준이라는 단일 표준에 맞춰 자신들의 프로그램을 조정했습니다. 카드 소유자 데이터 보호에 중점을 둔 기본 보안 모범 사례는 12개 PCI 요구 사항으로 구성됩니다. 요구 사항을 준수하지 않거나 보안 문제를 수정하지 못했을 경우 그 대가는 매우 심각합니다. 이를 테면, Visa 프로그램에 대한 판매자 참여가 영구적으로 금지되거나 판매자에 대한 제한이 있을 수 있으며, 벌금은 인시던트당 최대 \$500,000까지 부과됩니다.

Visa CISP에 대한 자세한 내용은 "Visa CISP(PCI 데이터 보안 표준)에 대한 자세한 정보와 HP Network Automation을 사용한 준수 실현" 링크를 클릭하십시오.

Visa CISP 준수 상태 보고서를 보려면

1. 보고서 아래의 메뉴 모음에서 준수 센터를 클릭합니다. 준수 센터 홈 페이지가 열립니다.
2. Visa CISP 준수 상태 링크를 클릭합니다. Visa CISP 준수 상태 페이지가 열립니다.

Visa CISP(PCI 데이터 보안 표준) 준수 상태 페이지 필드

필드	설명/작업
<p>보안 네트워크 구축 및 유지 보수</p> <p>1.1: 다음을 포함하는 방화벽 구성 표준을 설정합니다.</p> <ul style="list-style-type: none"> • 모든 연결과 방화벽 구성에 대한 변경 사항을 승인 및 테스트하기 위한 공식 프로세스 • 카드 소유자 데이터에 대한 모든 연결이 있는 현재 네트워크 다이어그램 • DMZ와 인트라넷 사이, 그리고 각 인터넷 연결에서의 방화벽 요구 사항 • 네트워크 구성 요소에 대한 논리적 관리와 관련된 그룹, 역할 및 책임에 대한 설명 • 비즈니스에 필요한 서비스/포트의 문서화된 목록 • HTTP, SSL, SSH 및 VPN 이외의 사용 가능한 프로토콜에 대한 정당화 및 문서화 • 위험성이 있는 프로토콜에 대한 정당화 및 문서화 • 방화벽/라우터 규칙 집합에 대한 정기적 검토 • 라우터 구성 표준 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 배포된 장치(라우터/방화벽) • 저장된 장치 구성 • 방화벽 구성 변경(최근 7일) • 적소에 있는 구성 정책 • NSA 라우터 보안 모범 사례 정책 위반(최근 7일) • 승인된 방화벽 변경(최근 7일) • 승인되지 않은 방화벽 변경(최근 7일)

필드	설명/작업
<p>1.2 "신뢰할 수 없는" 네트워크/호스트로부터의 모든 트래픽을 거부하는 방화벽 구성을 구축합니다. 단, 다음의 경우는 제외됩니다.</p> <ul style="list-style-type: none">• 웹 프로토콜 - HTTP(포트 80) 및 SSL(Secure Sockets Layer)(일반적으로 포트 443)• 시스템 관리 프로토콜• 비즈니스에 필요한 기타 프로토콜	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none">• 구성 정책 비준수 상태의 방화벽• 방화벽 구성 미준수 이벤트(최근 7일)

필드	설명/작업
<p>1.3: 다음을 포함하여 카드 소유자 데이터를 저장하는 시스템 구성 요소와 공개적으로 액세스 가능한 서버 간 연결을 제한하는 방화벽 구성을 구축합니다.</p> <ul style="list-style-type: none"> • 인바운드 인터넷 트래픽을 DMZ 내 IP 주소로 제한(수신 필터) • 인바운드 및 아웃바운드 인터넷 트래픽을 포트 80 및 443으로 제한 • 인터넷에서 DMZ로 내부 주소 전달 금지(송신 필터) • 내부 네트워크 구역에 데이터베이스 배치 • 아웃바운드 트래픽을 신용 카드 환경에 필요한 트래픽으로 제한 • 라우터 구성 파일 보안 및 동기화 • 특별히 허용되지 않는 다른 모든 인바운드 및 아웃바운드 트래픽 거부 • 무선 네트워크와 신용 카드 환경 간 경계 방화벽 설치 • 인터넷 직접 연결을 통해 모바일 및/또는 직원 소유의 컴퓨터에 개인 방화벽 소프트웨어 설치 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 구성 정책 비준수 상태의 방화벽 • 방화벽 구성 미준수 이벤트(최근 7일) • 배포된 방화벽

필드	설명/작업
<p>1.4: 다음을 포함하여 카드 소유자 정보를 저장하는 시스템 구성 요소와 외부 네트워크 간 직접 공개 액세스를 금지합니다.</p> <ul style="list-style-type: none"> • 인바운드 및 아웃바운드 인터넷 트래픽에 대한 직접 라우트를 금지하기 위해 모든 트래픽을 필터링 및 보호할 DMZ 구현 • 신용 카드 응용 프로그램의 아웃바운드 트래픽을 DMZ 내 IP 주소로 제한 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 구성 정책 비준수 상태의 방화벽 • 방화벽 구성 미준수 이벤트(최근 7일) • 배포된 방화벽
<p>1.5: 내부 주소가 인터넷에서 변환되거나 노출되는 것을 방지하기 위한 IP(Internet Protocol) 매스커레이딩(masquerading)을 구현합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 구성 정책 비준수 상태의 방화벽 • 방화벽 구성 미준수 이벤트(최근 7일) • 배포된 방화벽
<p>2.1: 네트워크에 시스템을 설치하기 전에 항상 공급업체에서 제공한 기본값을 먼저 변경합니다. 무선 환경의 경우 항상 무선 공급업체 기본값을 변경합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 적소에 있는 장치 암호 규칙 • 암호 변경(최근 7일) • 장치 암호 변경 실패(최근 7일)
<p>2.2: 다음을 포함하여 모든 시스템 구성 요소에 대한 구성 표준을 개발합니다.</p> <ul style="list-style-type: none"> • 서버당 기본 기능을 하나만 구현합니다. • 불필요하고 안전하지 않은 모든 서비스와 프로토콜을 비활성화합니다. • 오용 방지를 위한 시스템 보안 매개 변수를 구성합니다. • 스크립트, 드라이버, 기능, 하위 시스템 및 파일 시스템 등 불필요한 모든 기능을 제거합니다. 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 구성 정책 비준수 상태의 장치 • 구성 정책 비준수 이벤트(최근 7일) • 적소에 있는 구성 정책 • 추가된 구성 정책 규칙(최근 7일) • 변경된 구성 정책 규칙(최근 7일)
<p>2.3: 모든 비 콘솔 관리 액세스를 암호화합니다.</p>	<p>SSH 또는 SCP를 사용하도록 구성된 장치의 수를 표시합니다.</p>

필드	설명/작업
<p>카드 소유자 데이터 보호</p> <p>4.1: 강력한 암호 작성법(cryptography) 및 암호화(encryption) 기술을 사용합니다. 카드 소유자 데이터를 전송하는 무선 네트워크의 경우 128비트에서 WPA를 사용할 수 있는 경우 WPA(Wi-Fi 보호 액세스) 기술을 사용하거나, VPN 또는 SSL을 사용하여 전송을 암호화합니다.</p> <p>4.2: 암호화되지 않은 전자 메일을 통해 카드 소유자 정보를 전송하지 마십시오.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •구성 정책 비준수 상태의 장치 •구성 정책 비준수 이벤트(최근 7일) •NSA 라우터 보안 모범 사례 정책 위반(최근 7일) •적소에 있는 구성 정책 <p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>
<p>취약점 관리 프로그램 유지 관리</p> <p>6.1: 모든 시스템 구성 요소 및 소프트웨어에 공급업체에서 제공한 최신 보안 패치가 있어야 하며 릴리스한 후 한 달 내에 관련 보안 패치를 설치해야 합니다.</p> <p>6.2: 새로 발견된 보안 취약점을 식별하기 위한 프로세스를 설정합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •성공한 소프트웨어 업데이트(최근 7일) •실패한 소프트웨어 업데이트(최근 7일) <p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •소프트웨어 준수 상태가 아닌 장치 수 •감지된 소프트웨어 취약점(최근 7일)

필드	설명/작업
<p>6.3: 다음을 포함하여 업계 모범 사례에 기반을 둔 소프트웨어 응용 프로그램을 개발하고 소프트웨어 개발 수명 주기 전체에 대한 정보 보안을 포함시킵니다.</p> <ul style="list-style-type: none"> • 개발 전 모든 보안 패치와 시스템 및 소프트웨어 구성 변경 사항 테스트 • 개발/테스트 환경과 프로덕션 환경 분리 • 프로덕션 데이터(실제 신용 카드 번호)는 테스트 및 개발에 사용되지 않음 • 프로덕션 시스템이 활성화되기 전에 테스트 데이터 및 계정 제거 • 잠재적인 코딩 취약점을 식별할 수 있도록 프로덕션 또는 고객에게 릴리스하기 전에 사용자 지정 코드 검토 	<p>NA에서는 정책 비준수를 식별하기 위해 배포 전에 시스템에 입력된 구성 데이터에 대해 정책을 테스트할 수 있는 기능을 제공합니다.</p>
<p>6.4: 다음을 포함하여 모든 시스템 및 소프트웨어 구성 변경에 대한 변경 제어 절차를 수행합니다.</p> <ul style="list-style-type: none"> • 영향도 관련 문서 • 해당 관계자의 관리 사인오프 • 운영 기능을 검증하는 테스트 • 백아웃(Backout) 절차 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자가 특정 장치 집합으로 제한됨. 관리자 액세스 권한이 할당된 사용자 • 적소에 있는 워크플로 규칙 • 승인된 변경(최근 7일) • 승인되지 않은 변경(최근 7일) • 저장된 장치 구성 • 저장된 장치 구성(최근 7일)

필드	설명/작업
<p>6.5: 다음을 포함하여 보안 코딩 지침에 따라 소프트웨어 및 응용 프로그램을 개발합니다.</p> <ul style="list-style-type: none"> • 무효화된 입력 • 손상된 액세스 제어 • 손상된 인증/세션 관리 • XSS(사이트 간 스크립팅) 공격 • 버퍼 오버플로우 • 삽입 결함 • 잘못된 오류 처리 • 안전하지 않은 저장소 • 서비스 거부 • 안전하지 않은 구성 관리 <p>강력한 액세스 제어 방법 구현</p> <p>7.1: 컴퓨팅 리소스와 카드 소유자 정보에 대한 액세스를 그와 같은 액세스가 필요한 업무를 수행하는 개인으로만 제한합니다.</p> <p>7.2: 사용자가 여러 명인 시스템에 대해 사용자가 꼭 알 필요가 있는 사항에 따라 액세스를 제한하고 별도로 허용하지 않을 경우 "모두 거부"로 설정되는 메커니즘을 설정합니다.</p> <p>8.1: 시스템 구성 요소나 카드 소유자 데이터에 대한 액세스를 허용하기 전에 고유한 사용자 이름으로 모든 사용자를 식별합니다.</p>	<p>HP는 업계에서 허용되는 소프트웨어 디자인 원칙과 코딩 관행을 사용하며 내부 엔지니어링 정책에서 우수한 품질의 안전한 코드 작성에 중점을 둡니다.</p> <p>HP는 다양한 보안 게시판과 주의를 모니터링하고, 메일링 목록에 가입하며, 취약점이 식별되고 처리될 수 있도록 코드의 정기적인 보안 검토를 실시하고 있습니다.</p> <p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자 로그인 시도(최근 7일) • 사용자 추가됨(최근 7일) • 사용자 삭제됨(최근 7일) • 변경된 사용자 권한(최근 7일) <p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자가 특정 장치 집합으로 제한됨 • 관리자 액세스 권한이 할당된 사용자 <p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • NA에서 활성화된 사용자 계정 • NA에서 비활성화된 사용자 계정

필드	설명/작업
<p>8.2 고유한 식별 방법 외에도 추가로 아래 방법 중 하나 이상을 사용하여 모든 사용자를 인증합니다.</p> <ul style="list-style-type: none"> • 암호 • 토큰 장치 • 생체 인식 정보 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 암호 변경(최근 7일) • 외부 인증이 Active Directory를 통해 활성화되어 있습니다.
<p>8.3: 직원, 관리자 및 타사의 네트워크 원격 액세스에 대해 2가지 유형의 인증을 구현합니다.</p>	<p>Active Directory를 통해 활성화되어 있는 외부 인증의 수를 표시합니다.</p>
<p>8.4: 모든 시스템 구성 요소에서 전송 및 저장 시 모든 암호를 암호화합니다.</p>	<p>NA 암호는 로그인 시 키를 입력할 때 마스킹되며, 전송 시 디스크에서 암호화됩니다.</p>

필드	설명/작업
<p>8.5: 다음을 포함하여 소비자가 아닌 사용자 및 관리자에 대해 올바른 사용자 인증 및 암호 관리를 보장합니다.</p> <ul style="list-style-type: none"> • 사용자 ID, 자격 증명 및 기타 식별자 객체의 추가, 삭제 및 수정을 제어합니다. • 암호를 재설정하기 전에 사용자 ID를 검증합니다. • 첫 번째 암호를 사용자별로 고유한 값으로 설정하고, 첫 번째 사용 직후 변경합니다. • 최소 90일마다 비활성 사용자 계정을 제거합니다. • 필요한 시간 동안에만 원격 유지 보수를 수행할 수 있도록 공급업체에서 사용되는 계정을 활성화합니다. • 카드 소유자 정보에 액세스할 수 있는 모든 사용자에게 암호 절차 및 정책을 배포합니다. • 그룹, 공유 또는 일반 계정/암호를 사용하지 마십시오. • 최소 90일마다 사용자 암호를 변경합니다. • 암호 길이는 최소 7자 이상이어야 합니다. • 숫자 및 영문자 모두를 포함하는 암호를 사용합니다. • 6번 이상 시도 시 사용자 ID 잠금을 통해 반복적인 액세스 시도를 제한합니다. • 잠금 지속 시간을 30분 또는 관리자가 사용자 ID를 활성화할 때까지로 설정합니다. • 카드 소유자 정보를 포함하는 데이터베이스에 대한 모든 액세스를 인증합니다. 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자 로그인 시도(최근 7일) • 실패한 사용자 로그인 시도(최근 7일) • 암호 변경(최근 7일) • NA에서 활성화된 사용자 계정 • NA에서 비활성화된 사용자 계정

필드	설명/작업
네트워크에 대한 정기적인 모니터링 및 테스트	
<p>10.1: 시스템 구성 요소에 대한 모든 액세스를 연결하는 데 필요한 프로세스를 설정합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •NA에서 활성화된 사용자 계정 •NA에서 비활성화된 사용자 계정
<p>10.2: 자동화된 감사 추적을 구현하여 다음 이벤트를 다시 구성합니다.</p> <ul style="list-style-type: none"> •카드 소유자 데이터에 대한 모든 개인 사용자 액세스 •root 또는 관리 권한을 가진 개인이 수행하는 모든 작업 •모든 감사 추적에 대한 액세스 •잘못된 논리 액세스 시도 •식별 및 인증 메커니즘 사용 •감사 로그 초기화 •시스템 수준 객체의 생성 및 삭제 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •사용자 작업 감사 로깅이 비활성화됩니다. •실패한 사용자 로그인 시도(최근 7일) •외부 인증이 활성화되어 있지 않습니다. •사용자 추가됨(최근 7일) •사용자 삭제됨(최근 7일) •추가된 장치(최근 7일) •삭제된 장치(최근 7일) •장치 구성 변경(최근 7일)
<p>10.3: 각 이벤트마다 최소한 다음과 같은 감사 추적 항목을 기록합니다.</p> <ul style="list-style-type: none"> •사용자 ID •이벤트 유형 •날짜 및 시간 •성공 또는 실패 표시 •이벤트 주관 •영향 받은 데이터, 시스템 구성 요소 또는 리소스의 ID 또는 이름 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> •사용자 로그인 시도(최근 7일) •실패한 사용자 로그인 시도(최근 7일)
<p>10.4: 모든 중요 시스템 시계와 시간을 동기화합니다.</p>	<p>NTP로 구성된 장치의 수를 표시합니다.</p>

필드	설명/작업
<p>10.5: 다음을 포함하여 감사 추적을 변경할 수 없도록 보안을 유지합니다.</p> <ul style="list-style-type: none"> • 감사 추적 보기를 작업 관련 요구에 대한 감사 추적으로 제한합니다. • 감사 추적 파일을 무단 수정으로부터 보호합니다. • 변경하기 어려운 중앙 로그 서버 또는 미디어에서 감사 추적 파일을 즉시 백업합니다. • 무선 네트워크용 로그를 내부 LAN에 있는 로그 서버로 복사합니다. • 경고를 생성하지 않고는 기존 로그 데이터를 변경할 수 없도록 로그에 대해 파일 무결성 모니터링/변경 감지 소프트웨어를 사용합니다. 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 세션을 삭제할 수 있는 사용자 수 • 시스템 이벤트를 삭제할 수 있는 사용자 수
<p>10.6: 하루에 한 번 이상 모든 시스템 구성 요소에 대한 로그를 검토합니다.</p>	<p>로그 파일이 저장된 일수를 표시합니다.</p>
<p>10.7: 실제 사용 기간 및 법률 규정 기간과 일치하는 기간 동안 감사 추적 이력을 보관합니다.</p>	<p>저장된 다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 구성 • 진단 • 이벤트 • 작업 • 세션 • 로그 파일
<p>11.1: 보안 제어, 제한 사항, 네트워크 연결 및 제한을 테스트합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 모든 ACL • ACL 사용 중 • ACL 변경 사항(최근 7일)
<p>11.2: 최소 매 분기별로 네트워크에서 중요한 변경이 있는 후에는 내부 및 외부 네트워크 취약점 검사를 실행합니다.</p>	<p>이 요구 사항은 NA의 범위를 벗어났습니다.</p>

필드	설명/작업
<p>11.3: 1년에 한 번 이상, 그리고 중요한 인프라 또는 응용 프로그램 업그레이드나 수정이 있을 후 네트워크 인프라와 응용 프로그램에 대한 침투 테스트를 수행합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 구성 정책 비준수 상태의 장치 • 구성 정책 비준수 이벤트(최근 7일) • 장치 소프트웨어 수준 • 감지된 소프트웨어 취약점(최근 7일) • 적소에 있는 이벤트 알림 및 응답 규칙
<p>11.4: 네트워크 침입 탐지 시스템, 호스트 기반 침입 탐지 시스템 및/또는 침입 방지 시스템을 사용하여 모든 네트워크 트래픽을 모니터링하고 사용자에게 의심되는 손상에 대해 경고합니다.</p>	<p>NA에서는 IDS(침입 탐지 시스템)와 IPS(침입 방지 시스템) 모듈을 사용하여 장치를 중앙 집중식으로 안전하게 관리할 수 있습니다.</p>
<p>11.5: 파일 무결성 모니터링 기능을 배포하여 중요 시스템 또는 콘텐츠 파일에 대한 무단 변경 사실을 사용자에게 경고하고, 하루에 한 번 이상 중요 파일 비교를 수행합니다. 프로세스를 자동화할 수 있는 경우에는 이 작업을 더 자주 수행합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 장치 구성 변경(최근 7일) • 구성 정책 비준수 이벤트(최근 7일) • 구성 정책 비준수 상태의 장치 • 성공한 소프트웨어 업데이트(최근 7일) • 실패한 소프트웨어 업데이트(최근 7일) • 감지된 소프트웨어 취약점(최근 7일) • 장치 소프트웨어 수준

필드	설명/작업
정보 보안 정책 유지	
<p>12.2: 일일 운영 보안 절차를 개발합니다.</p>	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 사용자가 특정 장치 집합으로 제한됨 • 관리자 액세스 권한이 할당된 사용자 • 사용자 추가됨(최근 7일) • 사용자 삭제됨(최근 7일) • 변경된 사용자 권한(최근 7일) • 저장된 구성, 저장된 진단, 저장된 이벤트, 저장된 작업, 저장된 세션 및 저장된 로그 파일
<p>12.5: 다음 정보 보안 관리 책임을 개인 또는 팀에게 할당합니다.</p> <ul style="list-style-type: none"> • 보안 정책 및 절차를 설정, 문서화 및 배포합니다. • 보안 주의 및 정보를 모니터링 및 분석하고 해당 담당자에게 배포합니다. • 모든 상황을 적시에 효과적으로 처리할 수 있도록 보안 인시던트 대응 및 단계적 확대 절차를 설정, 문서화 및 배포합니다. • 추가, 삭제 및 변경 등 사용자 계정을 관리합니다. • 데이터에 대한 모든 액세스를 모니터링 및 제어합니다. 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 적소에 있는 구성 정책 • 적소에 있는 이벤트 알림 및 응답 규칙 • "정상" 상태의 모니터 • 녹색 상태의 구성 관리 모범 사례 • NA에서 활성화된 사용자 계정 • NA에서 비활성화된 사용자 계정 • 사용자가 특정 장치 집합으로 제한됨 • 관리자 액세스 권한이 할당된 사용자 • 사용자 추가됨(최근 7일) • 사용자 삭제됨(최근 7일) • 변경된 사용자 권한(최근 7일) • 사용자 로그인 시도(최근 7일) • 실패한 사용자 로그인 시도(최근 7일)

필드	설명/작업
<p>12.9: 다음을 포함하여 인시던트 대응 계획을 구현합니다.</p> <ul style="list-style-type: none"> • 시스템 손상 시 사용할 인시던트 대응 계획을 작성합니다. • 일년에 한 번 이상 계획을 테스트합니다. • 연중무휴로 주위에 응답할 수 있는 특정 담당자를 배정합니다. • 보안 위반 대응 책임이 있는 직원에게 적절한 교육을 제공합니다. • 침입 탐지, 침입 방지 및 파일 무결성 모니터링 시스템의 주의를 포함합니다. • 인시던트 대응 계획을 수정 및 개선하는 프로세스를 마련합니다. 	<p>다음의 수를 표시합니다.</p> <ul style="list-style-type: none"> • 장치 구성 변경(최근 7일) • 구성 정책 비준수 이벤트(최근 7일) • 성공한 소프트웨어 업데이트(최근 7일) • 실패한 소프트웨어 업데이트(최근 7일)

19장: 워크플로 생성

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	855페이지의 "시작하기"
워크플로 마법사	856페이지의 "워크플로 마법사"
내 작업	859페이지의 "내 작업"
승인 요청	863페이지의 "승인 요청"
작업 승인	866페이지의 "작업 승인"
전자 메일 알림	869페이지의 "전자 메일 알림"

워크플로 탐색

HP Network Automation 로그아웃

장치 ▾ 작업 ▾ 정책 ▾ 보고서 ▾ 관리 ▾ 도움말 ▾

내 작업

- 승인 요청
- 새 멀티 태스킹 프로젝트
- 작업 로드
- 활동 캘린더
- 예정된 작업
- 실행 중인 작업
- 최근 작업
- 새 작업 ▶

관리

- 사용자
- 사용자 그룹
- 새 사용자
- 새 사용자 그룹
- 로그온한 사용자
- 사용자 역할 및 권한
- 보안 파티션
- 게이트웨이
- 장치 암호 규칙
- 이벤트 알림 및 응답 규칙
- 사용자 지정 데이터 설정
- LDAP 설정
- 워크플로 설정**
- 관리 설정 ▶
- 작업 로드
- 시스템 상태
- 서비스 시작 / 중지
- 문제 해결
- 시스템 작업 ▶

시작하기

HP Network Automation(NA) 워크플로 통합 및 라우팅 엔진(WIRE)은 네트워크 구성 프로세스를 관리하여, 네트워크 변경 내용이 미리 정의된 정책에 따라 올바른 순서로 완료되고 담당자에 의해 승인되도록 합니다.

네트워크에서 누가 무엇을 왜 수행하는지를 제어하여, 장치 구성을 해당 조직의 목표에 따라 정확하게 수행할 수 있습니다. 워크플로는 작업 순서, 승인 얻기 및 결과 감사를 관리하므로, 정책에 어긋나는 변경 작업이나 구성 오류가 발생할 가능성이 훨씬 적습니다.

이 장에서는 다음 용어가 사용됩니다.

- **작업** — 작업은 NA가 네트워크와 인터랙션하는 기본 메커니즘입니다. 작업은 예약하거나 즉시 실행할 수 있는 특정 동작입니다. 완료된 작업은 NA 활동 결과를 제공합니다. 워크플로 작업에는 다음과 같은 모든 작업이 포함됩니다.
 - 암호 배포
 - 장치 재부팅
 - 작업 스냅샷
 - 명령 스크립트 실행
 - 시작 및 실행 구성 동기화
 - 장치 소프트웨어 업데이트
 - 진단 실행

작업의 전체 목록을 보려면 [358페이지의 "작업이란?"](#)을 참조하십시오.

- **프로젝트** — 프로젝트는 작업 주문 순서입니다. NA의 관점에서 프로젝트는 단지 순서대로 실행되는(병렬 대신) 하위 작업이 있는 작업의 다른 유형입니다.
- **주관자** — 승인을 위해 작업을 제출하는 개인
- **승인자** — 작업을 승인할 수 있으며 작업이 모든 내부 정책을 준수하는지 확인하는 개인 또는 개인 집단
- **참고 수신자** — 주관자 또는 승인자가 수행한 작업을 기반으로 알림 메시지를 수신하는 개인 또는 개인 집단

- 승인됨 — 실행이 승인된 작업의 승인 상태.
- 승인 안 됨 — 거부된 작업의 승인 상태. 충분한 데이터가 없거나 또는 네트워크에 부정적인 결과를 가져올 수 있는 잘못된 데이터가 있는 거부된 작업. 거부된 작업은 재활용될 수 없습니다.
- 보류됨 — 임시로(또는 영구적으로) 보류 중인 작업의 승인 상태.
- 오버라이드 — 승인 프로세스가 오버라이드될 필요가 있는 경우 응급 시 사용하기 위한 작업에 대해 주관자가 수행하는 작업. 이 기능은 관리 설정에서 사용할 수 있는 경우에만 사용할 수 있습니다.

참고: 승인이 필요하지 않는 작업을 생성하기 위해 모든 파워 사용자를 사용할 수 있습니다. 규칙 생성에 대한 정보는 [856페이지의 "워크플로 마법사"](#)를 참조하십시오. 예를 들어, 파워 사용자가 승인을 무시할 수 있도록 하려면 "모든 사용자는 관리에 의한 승인이 필요합니다" 규칙 전에 "모든 파워 사용자가 승인을 필요로 하지는 않습니다"라는 규칙을 생성할 수 있습니다.

워크플로 마법사

워크플로 마법사를 사용하면 작업에 대한 워크플로를 쉽게 설정할 수 있습니다. 워크플로 마법사를 열려면 관리 아래의 메뉴 모음에서 워크플로 설정을 클릭합니다. 워크플로 마법사가 열립니다.

단계	설명/작업
시작 페이지	시작 페이지에서는 워크플로 마법사에 대한 간단한 소개를 제공합니다. 계속하려면 다음을 클릭합니다.
1단계: 워크플로 사용	워크플로를 사용할지 여부 및 일부 또는 모든 작업에 대해 승인이 필요한지 여부를 묻는 메시지가 표시됩니다. 계속하려면 예를 클릭하고 다음을 클릭합니다. 아니요를 클릭하고 다음을 클릭하면, 워크플로 마법사 홈 페이지로 돌아갈 수 있는 설정 완료 페이지가 열립니다.
2단계: 워크플로 사용 - 계속됨	워크플로 사용 - 계속됨 페이지에서는 워크플로를 생성할 때 제공해야 하는 정보에 대한 개요를 제공합니다. 계속하려면 다음을 클릭합니다.

단계	설명/작업
3단계: 승인 규칙 관리	<p>계속하려면 새 워크플로 승인 규칙 이름을 입력하고 다음을 클릭합니다. 또한 기존 워크플로 승인 규칙을 수정하거나 삭제하는 옵션이 제공됩니다. 모든 기존 워크플로 승인 규칙은 페이지의 맨 아래에 표시됩니다. (참고: NA는 다음과 같은 하나의 기본 워크플로 승인 규칙과 함께 제공됩니다. <i>관리자가 승인한 모든 사용자</i>)</p> <p>참고: 워크플로 승인 규칙은 파티션에 따라 분할할 수 있습니다. 모든 파티션에 사용할 수 있는 워크플로 승인 규칙이 있습니다. 이러한 워크플로 승인 규칙은 구성에 따라 "공유"(또는 "전역")로 표시됩니다. 단, 적절한 권한이 없으면 편집 또는 삭제할 수 없습니다. 파티션 생성에 대한 내용은 191페이지의 "장치 및 사용자 세분화"를 참조하십시오.</p>
4단계: 주관자 설정	<p>주관자 설정 페이지에서는 작업을 생성할 때 이 규칙을 트리거할 사용자를 지정할 수 있습니다. 계속하려면 사용자 추가를 마쳤을 때 다음을 클릭합니다.</p>
5단계: 작업 설정	<p>작업 설정 페이지에서는 승인이 필요한 작업을 지정할 수 있습니다. 계속하려면 작업 추가를 마쳤을 때 다음을 클릭합니다. 승인이 필요한 작업을 지정하지 않는 경우 작업에 대한 승인 설정은 "해당되지 않습니다"로 표시됩니다.</p>
6단계: 장치 그룹 설정	<p>장치 그룹 설정 페이지에서는 장치 그룹을 기반으로 하여 워크플로 승인 규칙을 정의할 수 있습니다. 이를 통해 장치 사용, 장치 유형 등에 대한 워크플로 승인 규칙을 구성할 수 있습니다. 장치 파티셔닝을 활성화한 경우, 파티션 선택 드롭다운 메뉴가 표시됩니다. 우선 순위 수준은 파티션 내에서만 조정 가능합니다. 전역 규칙은 파티션 규칙보다 항상 높은 우선 순위를 가집니다. 장치 그룹 추가를 마치면 다음을 클릭합니다. 작업 생성 시간에 워크플로 승인 규칙은 다음과 같은 경우에만 나타납니다.</p> <ul style="list-style-type: none"> •작업이 단일 장치에 대해서이며 워크플로 승인 규칙 장치 그룹에 장치가 포함됩니다. •작업이 장치 그룹에 대해서이며 워크플로 승인 규칙 장치 그룹에 작업 장치 그룹과의 비어 있지 않은 교집합이 있습니다.

단계	설명/작업
7단계: 승인자 설정	<p>승인자 설정 페이지에서는 작업을 승인하고 모든 내부 정책을 준수하는 작업을 확인할 수 있는 사람을 지정할 수 있으며, 또는 승인이 필요하지 않은지 지정할 수 있습니다. 작업 주권자는 자신의 작업을 검토할 수 없습니다. 계속하려면 사용자 추가를 마쳤을 때 다음을 클릭합니다.</p>
8단계: 참고 수신자 설정	<p>참고 수신자 설정 페이지에서는 워크플로 승인 규칙 주권자 또는 승인자가 수행한 작업을 기반으로 알림 메시지 수신자를 지정할 수 있습니다. 사용자 추가를 마치면 저장을 클릭합니다. 주권자 및 승인자는 수신자로 추가하지 않아도 됩니다. 전자 메일 알림에 대한 자세한 내용은 869페이지의 "전자 메일 알림"을 참조하십시오.</p>
설정 완료	<p>워크플로 승인 규칙을 성공적으로 추가한 후, "새 규칙 <규칙 이름>이 (가) 성공적으로 생성되었습니다" 메시지가 페이지 맨 위에 표시됩니다. 이제 승인 규칙 관리 링크를 클릭하여 다른 사용자(주권자)에 대한 새 워크플로 승인 규칙을 생성하거나 또는 기존 승인 규칙을 수정/삭제할 수 있습니다. 주권자 및 승인자 작업의 요약을 보려면 작업 드롭다운 메뉴에서 내 작업 옵션을 클릭할 수 있습니다. 자세한 내용은 859페이지의 "내 작업"을 참조하십시오.</p>

내 작업

내 작업 페이지에서는 해당하는 경우 작업이 아직 실행되지 않았다면 작업 승인 상태를 포함하여 현재 로그인되어 있는 사용자가 시작한 작업이 표시됩니다.

내 작업 페이지를 보려면 작업의 메뉴 모음에서 내 작업을 클릭합니다. 내 작업 페이지가 열립니다.

내 작업 페이지 필드

필드	설명/작업
내 드래프트 링크	해당하는 경우 내 드래프트 페이지가 열립니다.
승인 요청 링크	<p>작업에 승인이 필요한 경우 현재 로그인한 사용자의 승인이 필요한 작업을 볼 수 있는 승인 요청 페이지가 열립니다. 기본적으로 이 페이지에는 다음 작업을 비롯하여 완료되지 않은 작업이 표시됩니다.</p> <ul style="list-style-type: none"> • 승인 안 됨 • 승인 대기 중 • 실행 대기 중 <p>자세한 내용은 863페이지의 "승인 요청"을 참조하십시오.</p>
예정된 작업 링크	대기열에 있는 예정된 작업을 볼 수 있는 예정된 작업 페이지가 열립니다. 자세한 내용은 495페이지의 "예정된 작업 페이지 필드" 를 참조하십시오.
실행 중인 작업 링크	모든 실행 중인 작업을 볼 수 있는 작업 실행 중 페이지가 열립니다. 자세한 내용은 498페이지의 "작업 실행 중 페이지 필드" 를 참조하십시오.
최근 작업 링크	최근 작업을 모두 볼 수 있는 최근 작업 페이지가 열립니다. 자세한 내용은 500페이지의 "최근 작업 페이지 필드" 를 참조하십시오.

필드	설명/작업
작업 표시 확인란	작업에 승인이 필요한 경우 다음 표시 옵션을 선택할 수 있습니다. <ul style="list-style-type: none"> • 승인됨 • 승인 안 됨 • 승인 대기 중 • 오버라이드됨 • 드래프트 • 승인이 필요하지 않음
확인란	왼쪽의 확인란을 사용하여 작업을 삭제할 수 있습니다. 작업을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 삭제를 클릭합니다. 인접한 선택 드롭다운 메뉴를 통해 모든 작업을 선택하거나 선택 취소할 수 있습니다.
예약 날짜	작업이 생성된 날짜와 시간을 표시합니다.
작업 이름	작업 이름을 표시합니다. 작업을 클릭하면 작업 정보 페이지가 열립니다. 작업에 대한 자세한 내용은 358페이지의 "작업이란?" 을 참조하십시오.
날짜별 승인	해당하는 경우 작업이 승인되어야 하는 날짜와 시간을 표시합니다. 작업이 승인 날짜까지 승인되지 않으면 상태가 "승인 안 됨"으로 설정됩니다. (참고: 승인 옵션은 작업이 워크플로 승인 규칙의 일부인 경우에만 표시됩니다.)
승인 상태	해당하는 경우 작업의 승인 상태를 표시합니다. 승인 상태는 작업이 워크플로 승인 규칙의 일부인 경우에만 표시됩니다. 승인 상태는 다음과 같습니다. <ul style="list-style-type: none"> • 승인 대기 중 • 승인됨 • 승인 안 됨 • 오버라이드됨 • 승인이 필요하지 않음

필드	설명/작업
작업 상태	<p>작업의 상태를 표시합니다. 상태는 다음과 같습니다.</p> <ul style="list-style-type: none"> • 경고 — 그룹 작업에 일부 실패한 하위 작업이 포함되어 있지만, 모든 작업이 실패한 것은 아닙니다. • 드래프트 — 드래프트 상태에서는 NA에서 작업을 실행하지 않거나 작업이 승인을 위해 전송되지 않습니다. • 중복 — 동일한 작업이 이미 실행 중이기 때문에 작업이 시작되지 않았습니다. • 실패함 — 작업이 실패했습니다. • 일시 중지 — 누군가가 작업을 일시 중지했습니다. 예정된 시간이 되면 실행되지 않습니다. • 보류 중 — 작업이 대기열에 저장되고 예정된 시간을 기다리고 있습니다. • 실행 중 — 작업이 시작되었지만 아직 완료되지 않았습니다. • 건너뛴 — 잘못된 권한, 관리되지 않는 장치 등의 오류 때문에 작업을 건너뛰었습니다. • 성공함 — 작업이 성공했습니다. • 대기 중 — 예정된 시간이 되었지만 "최대 동시 작업 수" 제한에 도달했기 때문에 작업이 대기 중입니다.
우선 순위	<p>작업 우선 순위를 표시합니다. 작업 우선 순위에 대한 자세한 내용은 359페이지의 "작업 예약"을 참조하십시오.</p>
작업 유형	<p>작업 유형이 표시됩니다. 예를 들면 다음과 같습니다.</p> <ul style="list-style-type: none"> • 암호 배포 • 구성 배포 • 드라이버 검색 • 장치 재부팅 • 스냅샷 작성 • 시작 및 실행 구성 동기화 <p>작업의 전체 목록을 보려면 358페이지의 "작업이란?"을 참조하십시오. (참고: 멀티 태스킹 프로젝트 작업은 내 작업 결과 페이지에 표시될 수도 있고 표시되지 않을 수도 있습니다. 표시 여부는 멀티 태스킹 프로젝트 작업에 하위 작업으로 위에 나열된 작업 유형이 하나 이상 포함되는지에 따라 결정됩니다.)</p>

필드	설명/작업
작업	<p>다음 옵션 중 하나를 선택할 수 있습니다.</p> <ul style="list-style-type: none">• 삭제 — 작업을 삭제할 수 있습니다.• 일시 중지 — 예정된 시간에 실행되지 않도록 작업이 일시 중지됩니다. (참고: 작업을 다시 시작하려면 재개를 선택하면 됩니다.)• 지금 실행 — 작업이 가능한 한 빨리 실행됩니다. 최대 동시 작업 수에 도달하지 않은 경우 작업이 즉시 실행됩니다.• 편집 — 해당 작업에 대한 작업 편집 페이지를 엽니다.
페이지별 결과 표시 수	<p>드롭다운 메뉴에서 페이지당 표시할 항목 수를 설정할 수 있습니다. 기본값은 25입니다.</p>

승인 요청

승인 요청 페이지에서 현재 로그인된 사용자의 승인을 필요로 하는 작업을 볼 수 있습니다. 기본적으로 페이지에서 승인 상태가 승인됨, 승인 대기 중 또는 승인 안 됨이라고 표시되면 아직 완료되지 않은 작업을 표시합니다.

참고: 완료된 작업을 보려면 보고서 아래의 메뉴 모음에서 검색 대상을 선택하고 작업을 클릭합니다. 자세한 내용은 [622페이지의 "작업 검색 페이지 필드"](#)를 참조하십시오.

승인 요청 페이지를 보려면 작업의 메뉴 모음에서 승인 요청을 클릭합니다. 승인 요청 페이지가 열립니다.

승인 요청 페이지 필드

필드	설명/작업
내 작업	각 작업 상태를 볼 수 있는 내 작업 페이지가 열립니다. 자세한 내용은 859페이지의 "내 작업 페이지 필드" 를 참조하십시오.
예정된 작업 링크	대기열에 있는 예정된 작업을 볼 수 있는 예정된 작업 페이지가 열립니다. 자세한 내용은 495페이지의 "예정된 작업 페이지 필드" 를 참조하십시오.
실행 중인 작업 링크	모든 실행 중인 작업을 볼 수 있는 작업 실행 중 페이지가 열립니다. 자세한 내용은 498페이지의 "작업 실행 중 페이지 필드" 를 참조하십시오.
최근 작업 링크	최근 작업을 모두 볼 수 있는 최근 작업 페이지가 열립니다. 자세한 내용은 500페이지의 "최근 작업 페이지 필드" 를 참조하십시오.
작업 표시	이 옵션을 선택하면 승인 상태가 다음과 같은 작업이 표시됩니다. <ul style="list-style-type: none"> • 승인됨 • 승인 안 됨 • 승인 대기 중

필드	설명/작업
작업 이름	작업 이름을 표시합니다. 작업을 승인하려면 작업 이름을 클릭합니다. 작업 정보 페이지가 열립니다. 자세한 내용은 866페이지의 "작업 정보 페이지 필드" 를 참조하십시오.
승인 기준	작업이 승인되어야 하는 날짜와 시간을 표시합니다. 작업이 승인 날짜까지 승인되지 않으면 상태가 "승인 안 됨"으로 설정됩니다. (참고: 실행한 작업은 승인 요청 페이지에서 제거됩니다. 승인 날짜가 지난 작업은 승인 안 됨으로 표시되며 데이터 정리가 이들 작업을 삭제할 때까지 승인 요청 페이지에 남습니다. 데이터 정리에 대한 자세한 내용은 478페이지의 "데이터 정리 작업 페이지 필드" 를 참조하십시오.)
승인 상태	작업 승인 상태를 표시합니다. 승인 상태는 다음과 같습니다. <ul style="list-style-type: none"> • 승인 대기 중 • 승인 안 됨
우선 순위	작업 우선 순위를 표시합니다.
날짜	작업이 생성된 날짜와 시간을 표시합니다.

필드	설명/작업
상태	<p>작업의 상태를 표시합니다. 상태는 다음과 같습니다.</p> <ul style="list-style-type: none"> • 경고 — 모든 작업 실패가 아닌, 일부 실패한 작업을 포함하는 그룹 작업. • 드래프트 — 드래프트 상태에서는 NA에서 작업을 실행하지 않거나 작업이 승인을 위해 전송되지 않습니다. • 중복 — 동일한 작업이 이미 실행 중이기 때문에 작업이 시작되지 않았습니다. • 실패함 — 작업이 실패했습니다. • 일시 중지 — 누군가가 작업을 일시 중지했습니다. 예정된 시간이 되면 실행되지 않습니다. • 보류 중 — 작업이 대기열에 저장되고 예정된 시간을 기다리고 있습니다. • 실행 중 — 작업이 시작되었지만 아직 완료되지 않았습니다. • 건너뛴 — 잘못된 권한, 관리되지 않는 장치 등의 오류 때문에 작업을 건너뛰었습니다. • 성공함 — 작업이 성공했습니다. • 대기 중 — 예정된 시간이 되었지만 "최대 동시 작업 수" 제한에 도달했기 때문에 작업이 대기 중입니다.
예약자	작업 예약자의 이름을 표시합니다.

작업 승인

다음 작업을 승인하도록 지정한 경우

1. 작업 아래의 메뉴 모음에서 승인 요청을 클릭합니다. 승인 요청 페이지가 열립니다. **863페이지의 "승인 요청 페이지 필드"**를 참조하십시오.
2. 승인 옵션을 보려면 작업 이름을 클릭합니다. 작업 정보 페이지가 열립니다.
3. 승인 버튼을 클릭합니다.

작업 정보 페이지 필드

작업 정보 페이지에는 다음을 비롯한 작업에 대한 자세한 정보가 포함되어 있습니다.

- 작업 상태
- 주관자
- 영향 받은 장치
- 기간
- 승인 정보
- 결과 세부사항

작업 정보 페이지에서는 경고 또는 실패 시 더욱 자세한 정보에 대한 링크도 제공합니다. 작업을 성공적으로 완료할 수 있지만 여전히 오류를 포함할 수 있습니다. 예를 들어, 실행 중인 구성에 성공적으로 배포할 수 있지만 구성 안에 잘못된 명령이 있을 수 있습니다.

작업 정보 페이지를 열려면 다음 단계를 수행하십시오.

1. 인벤토리 페이지에서 장치를 선택합니다. 장치 세부사항 페이지가 열립니다.
2. 보기 드롭다운 메뉴에서 장치 작업을 클릭합니다. 장치 작업 페이지가 열립니다.
3. 작업 열에서 자세한 정보를 원하는 작업에 대한 세부사항 옵션을 클릭합니다. 작업 정보 페이지가 열립니다.

필드	설명/작업
작업 편집 링크	작업을 편집할 수 있도록 작업 페이지가 열립니다. 이 링크는 보류 중인 작업에만 표시됩니다.
다시 실행 링크	작업을 다시 실행할 수 있도록 작업 페이지가 열립니다. 이 링크는 완료된 작업에만 표시됩니다.
목록으로 돌아가기 링크	내 작업 페이지가 열립니다. 491페이지의 "내 작업 페이지 필드" 를 참조하십시오.
일반 정보	
작업 이름	작업 이름을 표시합니다.
작업 상태	<p>다음과 비롯한 작업 상태를 표시합니다.</p> <ul style="list-style-type: none"> •드래프트 •중복 •실패함 •일시 중지 •보류 중 •요청됨(참고: 요청됨은 작업이 승인을 기다리고 있다는 의미입니다. (866페이지의 "작업 승인"을 참조하십시오.) •실행 •건너뛸 •성공함 •동기(참고: 일반적으로 NA는 스레드를 생성하고 백그라운드에서 작업을 비동기적으로 실행시킴으로써 작업을 실행합니다. CLI 및 API를 통해 현재 스레드에서 실행되는 동기 작업을 활성화할 수 있으며 명령이 완료될 때까지 명령이 차단됩니다.) •대기 중 •경고 <p>참고: 경고가 발생하는 경우 멀티 태스킹 프로젝트의 처리가 계속됩니다. 경고 상태는 상위 작업에 표시됩니다.</p>
주석	작업에 대한 설명을 표시합니다.

필드	설명/작업
주관자	작업을 예약한 사용자 이름이나 프로세스를 표시합니다.
생성 날짜	작업이 생성된 날짜와 시간을 표시합니다.
영향 받은 장치	영향 받은 장치의 호스트 이름 및/또는 IP 주소를 표시합니다.
예약 날짜	작업이 실행되도록 예약된 날짜와 시간을 표시합니다.
시작 날짜	작업의 시작 날짜를 표시합니다.
완료 날짜	작업의 완료 날짜를 표시합니다.
기간	작업 기간을 표시합니다.
반복 유형	반복 유형(예: 반복되지 않음)을 표시합니다.
승인 정보	
승인자	작업 승인자의 목록을 표시합니다.
승인 상태	작업 승인 상태를 표시합니다.
우선 순위	작업 우선 순위를 표시합니다.
승인 날짜	작업이 승인되어야 하는 날짜와 시간을 표시합니다.
새 주석	작업에 대한 추가 설명을 입력합니다.
승인 버튼	작업을 승인하려면 승인 버튼을 클릭합니다.
작업 세부사항 보기 링크	작업 보기 링크를 클릭하면 진단 이력 페이지가 열립니다.
추가 정보	
결과 세부사항	장치 유형에 따라 자동으로 실행된 진단을 표시합니다. 예를 들면 다음과 같습니다. <ul style="list-style-type: none"> • "NA 모듈 상태" 진단이 완료되었습니다. • "NA 라우팅 테이블" 진단이 완료되었습니다. • "NA OSPF 인접 환경" 진단이 완료되었습니다.
작업 이력	
작업 이력 정보	작업 실행 시기, 반복 유형 및 상태와 같은 작업 이력 정보를 표시합니다.

전자 메일 알림

작업 승인자는 워크플로 규칙 주관자가 수행한 작업을 기반으로 전자 메일 알림을 수신합니다. 워크플로 마법사의 참조 수신자 설정 페이지는 작업 승인자가 아닌 사용자에게 알리도록 사용될 수 있습니다. **856페이지의 "워크플로 마법사"**를 참조하십시오.

샘플 전자 메일 알림은 아래와 같이 표시됩니다.

```
From: HP on jbbrennan1
Sent: Thursday, January 10, 2007 2:00 PM
To: Tad Martin
Subject: Request for Approval
```

```
Liza has requested the Snapshot task for your approval
on or before 2004-11-06 00:00:00:0
```

```
Task Name: Snapshot
Description: Taking a snapshot of Lab2
Priority: High
Approval required on or before: 2004-11-06 00:00:00:0
Originator: Liza
Devices Affected: 172.22.123.26
Task Frequency: Repeat once
Task Start Date: 2004-11-06 15:00:00.0
```

```
You may approve, reject, or request clarification by
accessing HP Network Automation at
http://liza/task.view.htm/taskID=10023
```

전자 메일의 맨 아래에 있는 링크를 클릭하면 작업을 승인하거나 승인할 수 없는 승인 요청 페이지가 열립니다. **863페이지의 "승인 요청 페이지 필드"**를 참조하십시오.

870

HP Network Automation 사용 설명서

20장: ACL 작업

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
시작하기	873페이지의 "시작하기"
ACL 보기	874페이지의 "ACL 보기"
명령 스크립트 실행	878페이지의 "명령 스크립트 실행"
ACL 생성	879페이지의 "ACL 생성"
ACL 응용 프로그램 변경	880페이지의 "ACL 응용 프로그램 변경"
ACL 라인 일괄 삽입	881페이지의 "ACL 라인 일괄 삽입"
ACL 라인 일괄 삭제	882페이지의 "ACL 라인 일괄 삭제"
ACL 주석 처리 및 ACL 핸들 생성	884페이지의 "ACL 주석 처리 및 ACL 핸들 생성"
ACL 템플릿 생성	885페이지의 "ACL 템플릿 생성"
ACL 편집	886페이지의 "ACL 편집"
ACL 삭제	887페이지의 "ACL 삭제"

ACL 탐색

The screenshot shows the HP Network Automation web interface. At the top, there is a navigation bar with the HP logo and the text "HP Network Automation" on the left, and a "로그아웃" (Logout) button on the right. Below the navigation bar, there are several menu items: "장치" (Devices), "작업" (Jobs), "정책" (Policies), "보고서" (Reports), "관리" (Management), and "도움말" (Help). The "장치" menu is expanded, showing a dropdown list of options: "인벤토리 그룹" (Inventory Group), "새로 만들기" (New) with a right-pointing arrow, "새 장치 마법사" (New Device Wizard), "구성 변경" (Change Configuration), "장치 도구" (Device Tools) with a right-pointing arrow, "장치 작업" (Device Jobs) with a right-pointing arrow, and "ACL 삭제" (Delete ACL) with sub-options: "ACL 라인 일괄 삽입" (Bulk Insert ACL Lines) and "ACL 라인 일괄 삭제" (Bulk Delete ACL Lines).

시작하기

ACL(액세스 제어 목록)은 많은 조직에서 IP 트래픽 흐름을 제어하기 위해 사용됩니다. 이는 주로 보안을 강화하기 위해 수행되지만 공개 웹 사이트에서 오디오 또는 비디오 스트리밍과 같은 대역폭 집중 시스템 운영을 미리 방지하여 성능을 향상시키는 데 사용될 수도 있습니다.

일반적으로 ACL의 정의는 구성 명령문을 모아 놓은 것입니다. 이러한 명령문에서는 허용 또는 거부할 주소 및/또는 패턴을 정의합니다. NA는 장치에서 구성 정보를 검색하고 구성에서 ACL 명령문을 추출합니다. 그런 후 NA는 구성과는 별도로 ACL을 저장합니다.

NA ACL 관리자에서는 다음 작업을 수행할 수 있는 빠른 방법을 제공합니다.

- 장치에서 ACL 보기
- ACL 이력 유지 관리
- ACL에 대한 주석 처리 및 구성 주석 유지 관리

ACL 관리자에서는 ACL 템플릿을 생성하기 위해 기존 ACL 구성을 사용하는 빠른 방법도 제공합니다.

이 장에는 장치 또는 장치 그룹에 대해 ACL 구문 분석을 사용하는 방법(및 사용하지 않는 방법)에 대한 지침이 포함되어 있습니다.

- 단일 장치의 ACL 구문 분석 설정에 대한 자세한 내용은 [43페이지의 "구성 관리 페이지 필드"](#)를 참조하십시오.
- 장치 그룹의 ACL 구문 분석 설정에 대한 자세한 내용은 [209페이지의 "장치 일괄 편집 페이지 필드"](#)를 참조하십시오.
- ACL 검색에 대한 자세한 내용은 [652페이지의 "ACL 검색 페이지 필드"](#)를 참조하십시오.

참고: ACL 정보는 ACL 구문 분석이 활성화된 후 처음 저장되거나 또는 장치의 검사점 스냅샷이 작성된 후 사용할 수 있습니다.

ACL 보기

장치에서 ACL을 보려면

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다.
2. 인벤토리 페이지에서 ACL 구문 분석이 활성화된 장치를 선택합니다. 장치 세부사항 페이지가 열립니다. (참고: ACL을 지원하는 장치를 추가할 때 사용함 옵션이 선택되어 있는지 확인하십시오.) 장치가 검색되고 검사점 스냅샷이 작성되면 장치의 ACL을 볼 수 있습니다. (장치 추가에 대한 자세한 내용은 [137페이지의 "장치 추가"](#)를 참조하십시오.)
3. 보기 드롭다운 메뉴에서 장치 세부사항을 선택한 다음 ACL을 클릭합니다. 장치 ACL 페이지가 열립니다. [874페이지의 "장치 ACL 페이지 필드"](#)를 참조하십시오.
4. 장치 ACL 페이지에서, 나열된 ACL에 대한 ACL 옵션 보기를 클릭합니다. ACL 보기 페이지가 열립니다. [876페이지의 "ACL 보기 페이지 필드"](#)를 참조하십시오.

장치 ACL 페이지 필드

필드	설명/작업
호스트 이름	장치 호스트 이름을 표시합니다. 장치의 호스트 이름을 클릭하면 이 장치 ACL에 대한 정보를 볼 수 있는 마지막으로 방문했던 장치 세부사항 페이지가 열립니다.
장치 IP	장치 IP 주소를 표시합니다. 장치의 IP 주소를 클릭하면 이 장치의 ACL 정보를 볼 수 있는 최근 방문한 장치 세부사항 페이지가 열립니다.
마지막 스냅샷 시도	마지막으로 시도한 스냅샷의 날짜 및 시간을 표시합니다.
마지막 스냅샷 결과	"구성 변경 감지"와 같은 마지막 스냅샷 결과를 표시합니다.

필드	설명/작업
확인란	<p>왼쪽의 확인란을 통해 두 ACL을 비교할 수 있습니다. ACL을 선택한 후에 작업 드롭다운 메뉴를 클릭하고 다음 중 하나를 클릭합니다.</p> <ul style="list-style-type: none"> • 비교 — 선택한 두 ACL을 함께 비교할 수 있는 스크립트 비교 페이지가 열립니다. 차이점은 쉽게 확인할 수 있게 서로 다른 색상으로 강조 표시됩니다. <p>인접한 선택 드롭다운 메뉴를 통해 모든 장치 구성을 선택하거나 선택을 취소할 수 있습니다.</p>
ACL ID	<p>ACL ID를 표시합니다. ACL ID는 장치가 구성에서 ACL을 식별하는 방법을 참조합니다. 많은 장치가 ACL ID로 정수 인덱스를 사용하지만 모든 장치가 그런 것은 아닙니다. 결과적으로 ACL ID가 문자열로 저장됩니다.</p>
ACL 핸들	<p>ACL 핸들을 표시합니다. ACL 핸들은 정의한 ACL 이름입니다. 기본적으로 ACL 핸들은 ACL ID와 동일합니다. 특정 ACL 핸들을 제공하지 않는 경우 드라이버는 ACL ID를 사용합니다. (참고: 기본적으로 이 필드는 ACL을 정렬하는 데 사용됩니다.)</p>
ACL 유형	<p>장치에서 정의한 대로 ACL 유형을 표시합니다.</p>
마지막 수정일	<p>ACL이 마지막으로 수정된 날짜 및 시간을 표시합니다.</p>
작업	<p>선택할 수 있는 작업은 다음과 같습니다.</p> <ul style="list-style-type: none"> • ACL 편집 — ACL을 편집할 수 있는 ACL 편집 페이지를 엽니다. 자세한 내용은 878페이지의 "명령 스크립트 실행"을 참조하십시오. • ACL 보기 — ACL을 볼 수 있는 ACL 보기 페이지를 엽니다. 자세한 내용은 876페이지의 "ACL 보기 페이지 필드"를 참조하십시오. • ACL 이력 — 모든 변경 사항의 전체 감사 추적을 볼 수 있는 ACL 이력 페이지를 엽니다. ACL 이력을 사용하여 사전 구성으로 ACL을 복원하도록 지원할 수 있습니다. 이렇게 하려면 기록 ACL을 본 다음 ACL 편집 작업 링크를 클릭하십시오.

ACL 보기 페이지 필드

ACL 보기 페이지를 열려면

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다.
2. 인벤토리 페이지에서 ACL 구문 분석이 활성화된 장치를 선택합니다. 장치 세부사항 페이지가 열립니다. (참고: ACL을 지원하는 장치를 추가할 때 사용함 옵션이 선택되어 있는지 확인하십시오.) 장치가 검색되고 초기 스냅샷이 작성되면 장치의 ACL을 볼 수 있습니다.
3. 보기 드롭다운 메뉴에서 장치 세부사항을 선택한 다음 ACL을 클릭합니다. 장치 ACL 페이지가 열립니다.
4. 장치 ACL 페이지에서, 나열된 ACL에 대한 ACL 옵션 보기를 클릭합니다. ACL 보기 페이지가 열립니다.

필드	설명/작업
장치	장치의 호스트 이름 및 IP 주소를 표시합니다. 장치의 IP 주소를 클릭하면 이 장치의 ACL 정보를 볼 수 있는 최근 방문한 장치 세부사항 페이지가 열립니다.
ID	ACL ID를 표시합니다. ACL ID는 장치가 구성에서 ACL을 식별하는 방법을 참조합니다.
ACL 핸들	ACL 핸들을 표시합니다. ACL 핸들은 정의한 ACL 이름입니다.
ACL 유형	ACL 유형을 표시합니다.
마지막 수정일	ACL이 마지막으로 수정된 날짜 및 시간을 표시합니다.
마지막으로 수정한 사람	ACL을 마지막으로 수정한 사람을 표시합니다. 마지막으로 수정한 사람이 "해당 없음"일 수 있으며 이는 NA에서 ACL의 이 특정 버전의 담당자가 누구인지 인식할 수 없음을 나타냅니다. 사용자가 표시되는 경우 사용자 특성 세부사항 페이지에 링크가 제공되며, 여기서 ACL의 이 버전을 검색하기 전에 발생한 활동에 대해 NA에서 인식하는 모든 활동을 표시합니다. 사용자는 NA의 최적의 추측일 뿐이므로 다른 활동이 ACL 변경에 대해 실제 원인을 나타낼 수 있습니다.

필드	설명/작업
ACL 스크립트	<p>ACL을 정의하는 구성 스크립팅을 표시합니다. ACL 스크립트는 ACL을 정의하는 데 필요한 구성 라인을 나타냅니다. 선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 새 ACL — 기존 ACL을 템플릿으로 사용할 수 있는 명령 스크립트 실행 작업 페이지를 엽니다. (879페이지의 "ACL 생성"을 참조하십시오.) • ACL 편집 — ACL을 편집할 수 있는 명령 스크립트 실행 작업 페이지를 엽니다. (878페이지의 "명령 스크립트 실행"을 참조하십시오.) • 새 ACL 템플릿 — 기존 ACL을 템플릿으로 저장할 수 있는 새 명령 스크립트 페이지를 엽니다. (885페이지의 "ACL 템플릿 생성"을 참조하십시오.) • ACL 템플릿 편집 — 현재 ACL을 편집하는 템플릿을 생성할 수 있는 새 명령 스크립트 페이지를 엽니다. (885페이지의 "ACL 템플릿 생성"을 참조하십시오.)
ACL 응용 프로그램	<p>ACL이 적용되는 경우 ACL 응용 프로그램이 표시됩니다. ACL 응용 프로그램에는 ACL이 사용되는 장소를 정의하는 구성 명령 목록이 포함됩니다. 일부 ACL 유형에는 별도의 응용 프로그램 스크립팅이 없습니다. 이러한 ACL은 응용 프로그램 스크립트를 표시하지 않습니다. 선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • ACL 적용 — ACL을 (다시) 적용할 수 있는 새 작업 - 명령 스크립트 실행 페이지를 엽니다. (879페이지의 "ACL 생성"을 참조하십시오.) • ACL 템플릿 적용 — ACL 응용 프로그램 템플릿을 생성하는 새 명령 스크립트 페이지를 엽니다. (885페이지의 "ACL 템플릿 생성"을 참조하십시오.)
주석	<p>ACL에 대한 주석을 표시합니다. 선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 주석 편집 — ACL 편집 페이지를 엽니다. • 이력 — ACL 이력 페이지를 엽니다. • 관련 구성 보기 — 장치 구성 페이지를 엽니다. (227페이지의 "장치 구성 세부사항 페이지 필드"를 참조하십시오.)

명령 스크립트 실행

명령 스크립트 실행 작업을 사용하여 명령 스크립트를 실행할 수 있습니다. 자세한 내용은 [389페이지의 "명령 스크립트 실행 작업 페이지 필드"](#)를 참조하십시오. 명령 스크립트 실행 작업 페이지에서 다음 작업 옵션이 표시됩니다.

- 실행할 명령 스크립트 — 장치에 있는 특정 ACL에서 ACL 편집 스크립트가 실행 중임을 나타냅니다. ACL은 ID 및 핸들로 모두 식별됩니다(괄호로).
- 스크립트 유형으로 제한 — 스크립트 유형은 "ACL 편집 스크립트"로 자동으로 설정됩니다.
- 모드 — Cisco IOS 구성과 같은 장치 액세스 모드를 표시합니다.
- 스크립트 — 실행할 장치별 명령을 표시합니다. 실행할 스크립트는 기존 ACL 구성의 복사본을 제공하며 자동으로 채워집니다. 응용 프로그램으로 ACL을 편집하는 경우 ACL 구성 스크립팅 전(필요한 경우 응용 프로그램을 실행 취소하기 위해) 및 ACL 구성 스크립팅 후(ACL을 다시 적용하기 위해) 모두 ACL 응용 프로그램 스크립팅의 복사본이 제공됩니다. 많은 경우(예를 들어 IOS) 스크립트에서 지정한 구성과 ACL 구성을 정확하게 일치하도록 하려면 해당 ACL을 먼저 삭제한 다음 이를 되돌려 놓아야 합니다.

ACL 생성

기존 ACL을 템플릿으로 사용하여 새 ACL을 생성하려면

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다.
2. 활성화할 ACL 구문 분석이 있는 장치를 선택합니다. 장치 세부사항 페이지가 열립니다.
3. 보기 드롭다운 메뉴에서 장치 세부사항을 선택하고 ACL을 클릭합니다. 장치 ACL 페이지가 열립니다.
4. 작업 열에서 ACL 편집 옵션을 클릭합니다. 명령 스크립트 실행 페이지가 열립니다. 자세한 내용은 [389페이지의 "명령 스크립트 실행 작업 페이지 필드"](#)를 참조하십시오.

명령 스크립트 실행 작업 페이지에 있는 다음 필드가 자동으로 채워집니다.

- 실행할 명령 스크립트 — 스크립트(ACL 적용) 유형 및 소스 ACL을 표시합니다.
- 스크립트 유형으로 제한 — 스크립트 유형을 표시합니다(ACL 편집 스크립트).
- 모드 — 장치에서 ACL을 적용하기 위해 올바른 스크립트 모드를 표시합니다.
- 스크립트 — 기존 ACL 응용 프로그램 스크립팅의 복사본을 표시합니다. 이에 대해 철저히 확인하고 필요한 사항을 변경해야 합니다.

참고: ACL 스크립트를 라인별로 실행할 수 없습니다. ACL 스크립트는 라인별로 실행할 때 연결이 손실될 수 있습니다.

이미 존재하는 동일한 ACL ID를 사용하여 장치에 ACL을 추가할 경우 해당 장치에 기존 ACL을 실제로 편집 중입니다.

ACL 응용 프로그램 변경

ACL 응용 프로그램을 변경하려면

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다.
2. 활성화할 ACL 구문 분석이 있는 장치를 선택합니다. 장치 세부사항 페이지가 열립니다.
3. 보기 드롭다운 메뉴에서 장치 세부사항을 선택하고 ACL을 클릭합니다. 장치 ACL 페이지가 열립니다.
4. ACL 보기 옵션을 클릭합니다. ACL 보기 페이지가 열립니다. (876페이지의 "ACL 보기 페이지 필드"를 참조하십시오.)
5. ACL 적용 옵션을 클릭합니다. 명령 스크립트 실행 페이지가 열립니다. (879페이지의 "ACL 생성"을 참조하십시오.)

명령 스크립트 실행 작업 페이지에 있는 다음 필드가 자동으로 채워집니다.

- 실행할 명령 스크립트 — 스크립트(ACL 적용) 유형 및 소스 ACL을 표시합니다.
- 스크립트 유형으로 제한 — 스크립트 유형을 표시합니다(ACL 응용 프로그램 스크립트).
- 모드 — 장치에서 ACL을 적용하기 위해 올바른 스크립트 모드를 표시합니다.
- 스크립트 — 기존 ACL 응용 프로그램 스크립팅의 복사본을 표시합니다.

참고: ACL 스크립트를 라인별로 실행할 수 없습니다. ACL 스크립트는 라인별로 실행할 때 연결이 손실될 수 있습니다.

ACL 라인 일괄 삽입

ACL 라인을 일괄 배포할 수 있습니다. NA는 ACL ID 또는 ACL 핸들을 기반으로 하여 단일 또는 여러 장치에서 적절한 ACL에 필요한 라인을 자동으로 추가합니다. 다음 단계는 Cisco IOS 장치에만 해당합니다.

ACL에 라인을 일괄 삽입하려면

1. 장치의 메뉴 모음에서 장치 작업을 선택하고 ACL 라인 일괄 삽입을 클릭합니다. 새 작업 - 명령 스크립트 실행 페이지가 열립니다. (879페이지의 "ACL 생성"을 참조하십시오.)
2. 작업을 실행할 장치 또는 장치 그룹을 선택할 수 있습니다. 장치 또는 그룹 선택 시 페이지를 업데이트합니다.
3. 실행할 명령 스크립트 — 다음 중 하나를 선택합니다.
 - a) Cisco IOS에서 ACL ID로 ACL에 라인 삽입
 - 라인을 삽입할 ACL ID 위치 — 라인을 추가할 ACL ID 위치를 입력합니다. 장치 그룹을 선택한 경우 이 ACL ID와 일치하는 ACL을 포함하는 각 장치에 라인을 추가합니다.
 - 삽입할 ACL 라인 — 장치에서와 동일하게 ACL 라인을 입력합니다.
 - 라인을 추가할 위치 — 라인을 추가할 위치를 선택합니다. 옵션에는 첫 번째, 마지막 및 끝에서 두 번째가 포함됩니다.
 - 스크립트 업데이트 — 위의 변수 작업을 완료하면 클릭합니다.
 - 매개 변수 — 선택적 매개 변수.
 - 스크립트 — 이것은 ACL을 업데이트하는 실제 스크립트입니다. 실행 전 이 스크립트를 편집하는 옵션은 이 기능의 유연성을 크게 향상시킵니다.
 - b) Cisco IOS에서 핸들로 ACL에 라인 삽입
 - ACL 핸들 — 라인을 추가할 ACL 핸들 위치를 입력합니다. 장치 그룹을 선택한 경우 이 ACL 핸들과 일치하는 ACL을 포함하는 각 장치에 라인을 추가합니다.
 - 삽입할 ACL 라인('access-list {id}'포함 안 함) — "access-list ACLID"를 포함하지 않고 삽입할 ACL 라인을 입력합니다. 필요한 경우 스크립트에 이것이 배치됩니다.

- 라인을 추가할 위치 — 이 라인을 추가할 위치를 선택합니다. 옵션에는 첫 번째, 마지막 및 끝에서 두 번째가 포함됩니다.
- 스크립트 업데이트 — 위의 변수 작업을 완료하면 클릭합니다.
- 매개 변수 — 선택적 매개 변수.
- 스크립트 — 이것은 ACL을 업데이트하는 실제 스크립트입니다. 실행 전 이 스크립트를 편집하는 옵션은 이 기능의 유연성을 크게 향상시킵니다.

ACL 라인 일괄 삭제

ACL 라인을 일괄 제거할 수 있습니다. NA는 ACL ID 또는 ACL 핸들을 기반으로 하여 단일 또는 여러 장치에서 적절한 ACL에 필요한 라인을 자동으로 제거합니다. 다음 단계는 Cisco IOS 장치에만 해당합니다.

ACL에 라인을 일괄 삭제하려면

1. 장치의 메뉴 모음에서 장치 작업을 선택하고 ACL 라인 일괄 제거를 클릭합니다. 새 작업 - 명령 스크립트 실행 페이지가 열립니다. (879페이지의 "ACL 생성"을 참조하십시오.)
2. 작업을 실행할 장치 또는 장치 그룹을 선택할 수 있습니다. 장치 또는 그룹 선택 시 페이지를 업데이트합니다.
3. 실행할 명령 스크립트 — 다음 중 하나를 선택합니다.
 - a) Cisco IOS에서 ACL ID로 ACL의 라인 제거
 - 라인을 삭제할 ACL ID 위치 — 라인을 제거할 ACL ID 위치를 입력합니다. 장치 그룹을 선택한 경우 이 ACL ID와 일치하는 각 장치 ACL에서 라인을 제거합니다.
 - 삭제할 ACL 라인 — 장치에 표시되는 것과 동일하게 ACL 라인을 입력합니다. 일부 ACL 라인에는 여러 공백 문자가 있습니다. 예를 들어, `access-list 139` 및 `deny ip host 192.168.139.2 any` 는 "deny"와 "ip" 사이에 세 개의 공백이 있습니다.
 - 스크립트 업데이트 — 위의 변수를 완료하면 클릭합니다.
 - 매개 변수 — 선택적 매개 변수.

- 스크립트 — 이것은 ACL을 업데이트하는 실제 스크립트입니다. 실행 전 이 스크립트를 편집하는 옵션은 이 기능의 유연성을 크게 향상시킵니다.

b) Cisco IOS에서 핸들로 ACL의 라인 제거

- ACL 핸들 — 라인을 삭제할 ACL 핸들 위치를 입력합니다. 장치 그룹을 선택한 경우 이 ACL 핸들과 일치하는 ACL을 포함하는 각 장치에 라인을 삭제합니다.
- 삭제할 ACL 라인('access-list {id}'포함 안 함) — "access-list ACLID"를 포함하지 않고 삭제할 ACL 라인을 입력합니다. 필요한 경우 스크립트에 이것이 배치됩니다.
- 스크립트 업데이트 — 위의 변수를 완료하면 클릭합니다.
- 매개 변수 — 선택적 매개 변수.
- 스크립트 — 이것은 ACL을 업데이트하는 실제 스크립트입니다. 실행 전 이 스크립트를 편집하는 옵션은 이 기능의 유연성을 크게 향상시킵니다.

ACL 주석 처리 및 ACL 핸들 생성

NA에서는 인라인 주석 처리 기능을 ACL 주석과 통합합니다. 이는 ACL에 포함하고 다시 적용하기 위해 구성 주석에 있는 변경에 대한 주석 처리 및 구성에 포함할 ACL에 대한 주석 처리가 가능합니다.

인라인 주석 처리를 지원하는 장치에서 ACLNAME: NA 인라인 주석을 식별하는 이중 주석 문자 시퀀스 뒤에 오는 텍스트는 ACL 핸들을 나타냅니다. 인라인 주석 처리를 지원하지 않는 장치에서 구성의 ACL 주석 이동 기능은 사용할 수 없습니다. 하지만 ACL 주석 및 핸들은 ACL 내에 지속적으로 유지 관리됩니다.

주석을 입력하려면

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다.
2. 인벤토리 페이지에서 ACL 구문 분석이 활성화된 장치를 선택합니다. 장치 세부 사항 페이지가 열립니다.
3. 보기 드롭다운 메뉴에서 장치 세부사항을 선택하고 ACL을 클릭합니다. 장치 ACL 페이지가 열립니다.
4. ACL 보기 옵션을 클릭합니다. ACL 보기 페이지가 열립니다. **876페이지의 "ACL 보기 페이지 필드"**를 참조하십시오.
5. 주석 편집 옵션을 클릭합니다. ACL 편집 페이지가 열립니다.
6. 주석 필드에 주석을 입력합니다.
7. ACL 핸들을 편집합니다.
8. 저장을 클릭합니다.

NA 인라인 주석 처리를 지원하는 장치에 대해 구성에 있는 주석을 변경하면 ACL 주석에 반영됩니다.

ACL 템플릿 생성

기존 ACL을 기반으로 직접 스크립트를 생성하는 것 외에도 ACL을 사용하여 ACL 명령 스크립트 템플릿에 대해 기초를 형성할 수 있습니다. ACL 템플릿은 ACL을 편집 및 적용 하도록 생성할 수도 있습니다.

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다.
2. 인벤토리 페이지에서 ACL 구문 분석이 활성화된 장치를 선택합니다. 장치 세부 사항 페이지가 열립니다.
3. 보기 드롭다운 메뉴에서 장치 세부사항을 선택하고 ACL을 클릭합니다. 장치 ACL 페이지가 열립니다.
4. 작업 열에서 ACL 보기 옵션을 클릭합니다. ACL 보기 페이지가 열립니다.
5. ACL 스크립트의 새 ACL 템플릿 링크를 클릭합니다. 새 명령 스크립트 페이지가 열립니다. **722페이지의 "새 명령 스크립트 페이지 필드"**를 참조하십시오. 새 명령 스크립트 페이지에 있는 다음 필드가 자동으로 채워집니다.
 - 스크립트 유형 — ACL 생성 스크립트, ACL 편집 스크립트 또는 ACL 적용 스크립트를 포함하여 생성되는 ACL 스크립트 템플릿 유형을 표시합니다.
 - 모드 — 장치에서 ACL 스크립트를 실행하기 위해 올바른 스크립트 모드를 표시합니다.
 - 스크립트 — 기존 ACL 응용 프로그램 스크립팅의 복사본을 표시합니다.

참고: ACL ID가 필요하면 스크립트에 있는 예약된 변수 "\$tc_aclid_for_handle\$"를 사용할 수 있습니다. 스크립트를 실행하면 ACL 핸들에 대한 메시지가 표시됩니다. 장치에서 스크립트가 실제로 실행되면 스크립트에 있는 이 변수의 각 인스턴스는 제공하는 것과 일치하는 핸들이 있는 장치에서 ACL ID로 대체됩니다.

6. 새 ACL 생성 스크립트에 대해 이름을 입력합니다.
7. 스크립트를 편집합니다. 자세한 내용은 **878페이지의 "명령 스크립트 실행"**을 참조하십시오.
8. 완료되면 스크립트 저장을 클릭해야 합니다. 스크립트가 성공적으로 저장되면 스크립트 검색 결과(명령 스크립트) 페이지가 열립니다. 추가한 스크립트가 목록에 나타나고 강조 표시됩니다. 스크립트는 작업으로 예약될 때까지 실행되지 않습니다.
9. 작업 실행을 선택합니다.

10. 스크립트를 실행할 수 있는 장치의 호스트 이름 또는 IP 주소를 지정합니다.
11. ACL ID를 입력합니다.
12. 작업을 저장합니다. 작업이 완료되면 ACL 보기 페이지에 새 ACL이 표시됩니다.
874페이지의 "장치 ACL 페이지 필드"를 참조하십시오.

ACL 편집

ACL을 편집하려면

1. 장치 아래의 메뉴 모음에서 인벤토리를 클릭합니다.
2. 인벤토리 페이지에서 ACL 구문 분석이 활성화된 장치를 선택합니다. 장치 세부 사항 페이지가 열립니다.
3. 보기 드롭다운 메뉴에서 장치 세부사항을 선택하고 ACL을 클릭합니다. 장치 ACL 페이지가 열립니다.
4. 편집할 ACL에 대한 ACL 편집 옵션을 클릭합니다. 명령 스크립트 실행 페이지가 열립니다. 자세한 내용은 879페이지의 "ACL 생성"를 참조하십시오.

ACL 편집 링크를 클릭하면 명령 스크립트 실행 작업에 있는 다음 필드가 자동으로 채워집니다.

- 실행할 명령 스크립트 — 스크립트(ACL 편집) 유형 및 소스 ACL을 표시합니다.
- 스크립트 유형으로 제한 — 스크립트 유형을 표시합니다(ACL 편집 스크립트).
- 모드 — 장치에서 ACL을 편집하기 위해 올바른 스크립트 모드를 표시합니다.
- 스크립트 — 실행할 장치별 명령을 표시합니다. 이에 대해 철저히 확인하고 필요한 사항을 변경해야 합니다.

몇 가지 장치에 편집한 ACL을 배포하려면 ACL을 배포할 장치 그룹을 선택합니다. 자세한 내용은 389페이지의 "명령 스크립트 실행 작업 페이지 필드"를 참조하십시오.

참고: ACL 스크립트를 라인별로 실행할 수 없습니다. ACL 스크립트는 라인별로 실행할 때 연결이 손실될 수 있습니다.

ACL 삭제

ACL 관리에서 시간이 오래 걸리는 작업 중 하나가 장치에서 더 오래되고 사용되지 않은 ACL을 제거하고 있습니다. 이로 인해 새 응용 프로그램 및 ACL과 충돌하지 않도록 합니다. 단일 장치에 대해 ACL을 삭제하면 해당 장치에 있는 ACL이 나열됩니다. 장치 그룹에 대해 ACL을 삭제하면 그룹에 있는 모든 장치의 모든 ACL 핸들이 나열되고 ACL ID가 아닌 핸들에 의해 ACL이 삭제됩니다.

ACL을 삭제하려면 장치 메뉴에서 장치 작업을 선택하고 ACL 삭제를 클릭합니다. 새 작업 - ACL 삭제 페이지가 열립니다. **888페이지의 "ACL 삭제 작업 페이지"**를 참조하십시오.

장치 구성에서 ACL을 삭제하면 ACL은 더 이상 관리되는 ACL 목록에 나타나지 않습니다. ACL에 대한 검색 옵션을 사용하여 여전히 ACL 이력을 검색할 수 있지만 ACL 이력은 장치별 ACL을 볼 때 표시되지 않습니다. 장치별 인터페이스에서 삭제한 ACL에 대한 추적이 없습니다. 삭제한 ACL의 구성을 롤백하려면 해당 ACL을 검색한 다음 다시 배포하십시오.

응용 프로그램이 없는 ACL이 삭제됩니다. 하지만 응용 프로그램이 있는 ACL은 삭제되지 않습니다. 기본적으로 NA에서는 응용 프로그램 스크립트가 있는 경우 ACL을 삭제하지 않습니다. 응용 프로그램이 있는 경우에도 ACL을 강제로 삭제하는 옵션이 제공됩니다. 이 옵션을 선택하는 경우 모든 선택한 ACL이 삭제됩니다.

참고: NA에서는 장치의 구성에 있는 ACL의 모든 응용 프로그램을 찾는다고 보장하지 않습니다. ACL에 응용 프로그램 스크립트는 없지만 장치의 특정 위치에서 실제로 사용 중일 수 있습니다. 이러한 경우에는 ACL 삭제 작업에서 ACL을 삭제하려고 하므로(응용 프로그램이 없다고 인식되므로) 결과는 예기치 않은 장치 동작이 됩니다.

ACL 삭제 작업 페이지

ACL 삭제 작업을 사용하여 ACL을 삭제할 수 있습니다. ACL을 삭제하려면 장치 메뉴에서 장치 작업을 선택하고 ACL 삭제를 클릭합니다. ACL 삭제 페이지가 열립니다. 완료되면 작업 저장 버튼을 클릭합니다.

필드	설명/작업
작업 이름	ACL 삭제를 표시합니다. 적용 가능한 경우 다른 작업 이름을 입력할 수 있습니다.
적용 대상	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 장치/그룹 — 작업을 실행할 IP 주소, 호스트 이름 또는 장치 그룹 이름을 입력하거나 돋보기 아이콘을 클릭합니다. 장치 선택기 사용 방법에 대한 자세한 내용은 183페이지의 "장치 선택기"를 참조하십시오. • CSV 파일 — 이름을 입력하거나 장치의 목록이 포함된 CSV 파일을 찾습니다. CSV 파일은 CSV 파일의 각 행과 연관된 장치를 식별하는 방법을 제공해야 합니다(IP 주소 및 호스트 이름). 작업 CSV 템플릿 링크를 클릭하면 샘플 CSV 파일을 다운로드할 수 있습니다.
시작 날짜	선택할 수 있는 옵션은 다음과 같습니다. <ul style="list-style-type: none"> • 가능한 한 빨리 시작 — 기본값을 선택한 경우 여러 작업이 가능한 한 빨리 시작합니다. • 시작 위치 — 이 옵션을 선택하면 캘린더 아이콘을 클릭하여 여러 작업을 시작하기 위해 날짜 및 시간을 선택할 수 있는 캘린더를 열 수 있습니다.
우선 순위	작업 우선 순위가 표시됩니다. 1~5의 5가지 작업 우선 순위 수준이 있으며, 최고 작업 우선 순위는 1입니다. 자세한 내용은 359페이지의 "작업 예약" 을 참조하십시오.
주석	멀티 태스킹 작업에 대한 설명을 추가합니다.
작업 옵션	
세션 로그	디버깅 로그를 저장하려면 "전체 장치 세션 로그 저장" 상자를 선택합니다. 이렇게 하면 실패한 스냅샷을 디버깅할 때 유용하지만 많은 양의 데이터가 저장될 수 있습니다.

필드	설명/작업
삭제할 ACL	<p>선택할 수 있는 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 응용 프로그램 없이 ACL 표시 — 알려진 응용 프로그램 없이 ACL만 표시합니다(기본값). • 모든 ACL 표시 — 이 옵션을 선택하면 괄호 안에 핸들이 있는 ACL ID를 포함하여 모든 ACL이 표시됩니다. 목록에서 ACL의 개수를 선택할 수 있습니다. (참고: 장치 그룹에 대해 이 작업을 실행하고 있는 경우 목록에는 그룹에 있는 모든 장치에 대해 찾을 수 있는 모든 ACL이 포함됩니다. 응용 프로그램 없이 ACL으로 목록을 필터링할 옵션이 없습니다.)
응용 프로그램으로도 ACL 삭제 확인란	이 옵션을 선택하면 알려진 응용 프로그램이 있는 경우일지라도 선택한 ACL이 삭제됩니다.
추산 기간	이 작업이 실행될 대상 장치 또는 장치 그룹을 예약할 기간을 입력합니다. 기본 값은 60분입니다.

장치 자격 증명 옵션

서버 페이지의 관리 설정에서 구성된 표준 장치 자격 증명 허용, 작업별 장치 자격 증명 허용 및/또는 사용자 AAA 자격 증명 허용 옵션에 따라, 장치 자격 증명 옵션이 표시됩니다. 작업별 장치 자격 증명 허용을 활성화하면 해당 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 둘 이상의 장치 자격 증명 옵션을 활성화하면 작업을 실행할 때 사용할 옵션을 선택하라는 메시지가 표시됩니다. 장치 자격 증명 옵션을 하나만 활성화하면 해당 옵션이 자동으로 사용되며 옵션을 선택하라는 메시지가 표시되지 않습니다. 장치 자격 증명 활성화에 대한 자세한 내용은 [56페이지의 "장치 액세스 페이지 필드"](#)를 참조하십시오.

장치 자격 증명	<p>장치 액세스 페이지의 관리 설정에서 활성화된 장치 자격 증명 옵션에 따라, 다음 옵션 중 하나 이상을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • 표준 장치별 자격 증명 및 네트워크 전체 암호 규칙 사용(기본값) • 작업별 자격 증명 사용. 사용자 이름, 암호, 암호 확인, 활성화 암호, 활성화 암호 확인, SNMP 읽기 전용 커뮤니티 문자열 및 SNMP 읽기/쓰기 커뮤니티 문자열을 입력하라는 메시지가 표시됩니다. • 작업 소유자의 AAA 자격 증명 사용. 작업 소유자의 올바른 AAA 자격 증명 정의되어 있어야 합니다. (참고: 표준 암호 규칙과 장치별 암호가 사용되지만 작업 소유자의 AAA 사용자 이름과 암호가 적용됩니다.)
----------	--

필드	설명/작업
사전 작업/사후 작업 스냅샷 옵션	
스냅샷 옵션은 시스템이 구성 관리 페이지의 관리 설정에서 사용자 오버라이드를 활성화하도록 구성된 경우에만 표시됩니다. (자세한 내용은 43페이지의 "구성 관리 페이지 필드" 를 참조하십시오.)	
사전 작업 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨(기본값)
사후 작업 스냅샷	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •없음 •작업에 포함됨(기본값) •별도 작업으로 예정됨
승인 옵션	
승인 옵션은 작업이 워크플로 승인에 포함될 경우에만 표시됩니다.	
승인 요청	작업을 실행하기 위해 먼저 승인이 필요한 경우 기본적으로 이 옵션이 선택되어 있습니다. 작업이 승인될 날짜를 변경하려면 날짜 옆의 캘린더 아이콘을 클릭하여 캘린더를 열고 날짜와 시간을 선택합니다. 작업 우선 순위도 선택할 수 있습니다. 워크플로를 구성할 때 긴급 및 보통과 같은 다양한 우선 순위 값을 추가할 수 있습니다. NA 스케줄러는 이러한 값을 확인하지 않습니다. 기본적으로 우선 순위 값은 사용자가 시기 적절하게 승인이 필요한 작업을 확인할 수 있는 시각적 대기열입니다.
승인 오버라이드	작업에서 오버라이드를 허용하는 경우 승인 프로세스를 오버라이드하려면 이 옵션을 선택합니다.
드래프트로 저장	이 옵션을 선택하면 작업을 드래프트로 저장하고 나중에 처리할 수 있습니다. 작업은 드래프트 모드로 실행되지 않습니다.
예약 옵션	
재시도 수	작업이 실패하면 NA는 지정된 재시도 간격만큼 띄어 이 횟수만큼 재시도를 진행합니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> •재시도 없음(기본값) •한 번 •두 번 •세 번

필드	설명/작업
재시도 간격	다시 시도하기 전에 대기할 시간(분)을 입력합니다. 기본값은 5분입니다.
반복 옵션	작업이 위에 지정된 날짜/시간에 시작된 후 다음 기준에 따라 반복됩니다. 다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> • 한 번만 — 작업이 지정된 날짜/시간에 한 번만 발생합니다(기본값). • 주기적으로 — 반복 간격(분)을 지정합니다. • 매일 — 작업이 매일 지정된 시간에 발생합니다. • 매주 — 하나 이상의 요일을 선택합니다. 작업이 해당 요일의 지정된 시간에 발생합니다. • 매월 — 일을 선택합니다. 작업이 매월 해당 일의 지정된 시간에 한 번만 발생합니다.
반복 범위	한 번만을 제외한 반복 옵션을 선택하면 다음과 같은 반복 범위를 지정할 수 있습니다. <ul style="list-style-type: none"> • 종료 날짜 없음(기본값) • < >번 발생 후 종료 — 반복 횟수를 입력합니다. • 종료 날짜 — 캘린더 아이콘을 클릭하고 날짜와 시간을 선택합니다.

21장: 문제 해결

다음 표를 사용하면 정보를 신속하게 찾을 수 있습니다.

항목	참조
드라이버 검색 실패	894페이지의 "드라이버 검색 실패"
장치 스냅샷 실패	895페이지의 "장치 스냅샷 실패"
Syslog 통한 실시간 변경 감지 없음	896페이지의 "Syslog를 통한 실시간 변경 감지 없음"
세션 로그	897페이지의 "세션 로그"
SWIM 오류 메시지	898페이지의 "SWIM 오류 메시지"

로깅에 대한 자세한 내용은 [125페이지의 "로깅"](#)을 참조하십시오. 고객 지원 센터에 문제 해결 정보 보내기에 대한 자세한 내용은 [35페이지의 "문제 해결 보내기 페이지 필드"](#)를 참조하십시오.

드라이버 검색 실패

장치에 대해 드라이버를 검색할 수 없는 경우

1. 검색하려는 장치가 지원되는 장치 모델 및 OS 버전인지 확인합니다. 지원되는 장치에 대한 자세한 내용은 DRS(장치 릴리스 서비스) 설명서를 참조하십시오. DRS는 자동화된 새로운 드라이버 릴리스 및 전달 시스템입니다. 장치가 지원되지 않는 경우 고객 지원 센터에 문의하십시오. 장치가 지원되는 경우 2단계로 이동합니다.
2. NA 서버에서 장치에 텔넷 및/또는 SSH를 통해 연결합니다. 장치 목록 페이지에 있는 장치에 대한 텔넷 또는 SSH 링크를 클릭하면, NA가 장치에 텔넷 또는 SSH를 통해 연결할 수 있는지 쉽게 확인할 수 있습니다. 자세한 내용은 [241페이지의 "인벤토리 페이지 필드"](#)를 참조하십시오. NA는 자동으로 장치에 로그인을 시도합니다. 장치에 로그인할 수 없는 경우, 장치에 있는 잘못된 액세스 목록, 잘못된 암호 정보 또는 네트워크 연결 문제가 원인일 수 있습니다. 고객 지원 센터에 문의하십시오. 장치에 텔넷 및/또는 SSH를 통해 연결할 수 있지만 장치 검색 작업이 여전히 실패하는 경우 3단계로 이동합니다.
3. 장치에서 활성화된 읽기 전용 SNMP가 있는지 확인합니다. 읽기 전용 SNMP가 활성화되어 있다면, 이 OID를 사용하여 NA 서버에서 읽기 전용 SNMP를 통해 장치에 연락을 시도해 보십시오. NA 내에서 장치에 대해 구성된 커뮤니티 문자열을 사용하는지 확인합니다. 읽기 전용 SNMP를 활성화하지 않으려면, 장치를 추가하거나 편집할 때 드라이버 드롭다운 목록에서 드라이버를 수동으로 선택할 수 있습니다. 자세한 내용은 [230페이지의 "장치 구성 데이터 편집"](#)을 참조하십시오. 읽기 전용 SNMP를 활성화했으면, NA에 로그인하고 추가하려는 장치를 선택한 후 장치 편집을 클릭합니다. 올바른 읽기 전용 SNMP 커뮤니티 문자열이 있는 장치를 업데이트하고 드라이버 검색을 클릭합니다. 드라이버 검색 작업이 여전히 실패하는 경우 4단계로 이동합니다.
4. NA에 로그인합니다. 메뉴 모음에서 관리를 선택하고 문제 해결 옵션을 클릭합니다. 문제 해결 페이지가 열립니다. 목록 상자에서 장치/세션/로그 및 장치/드라이버/검색을 선택합니다. 추적(가장 많은 메시지)으로 수준을 설정합니다. 제출을 클릭합니다. 검색하려는 장치를 클릭한 다음 드라이버 검색을 클릭합니다. 드라이버 검색 작업이 실패했다면, 메뉴 모음에서 관리를 선택하고 문제 해결을 클릭합니다. 문제 해결 정보 보내기를 클릭합니다. 설명 섹션에서 실패 내용과 장치 모델 및 OS 버전을 지정합니다. 로깅에 대한 자세한 내용은 [125페이지의 "로깅"](#)을 참조하십시오.

장치 스냅샷 실패

장치 스냅샷이 실패한 경우

1. 스냅샷하려는 장치가 지원되는 장치 모델 및 NA용 OS 버전인지 확인합니다. 지원되는 장치에 대한 자세한 내용은 DRS(장치 릴리스 서비스) 설명서를 참조하십시오. DRS는 자동화된 새로운 드라이버 릴리스 및 전달 시스템입니다. 장치가 지원되지 않는 경우 고객 지원 센터에 문의하십시오. 장치가 지원되는 경우 2단계로 이동합니다.
2. 장치에 할당된 장치 드라이버가 있는지 확인합니다. 장치 목록 페이지에서 문제가 있는 장치를 클릭합니다. 자세한 내용은 [261페이지의 "메뉴 옵션 보기"](#)를 참조하십시오. 드라이버 이름 필드로 스크롤하고 값이 있는지 확인합니다. 드라이버가 없는 경우 고객 지원 센터에 문의하십시오. 드라이버가 있는 경우 드라이버 검색 링크를 클릭합니다. 스냅샷 작업이 여전히 실패하는 경우 3단계로 이동합니다.
3. NA 서버에서 장치에 텔넷 및/또는 SSH를 통해 연결합니다. 장치 목록 페이지에 있는 장치에 대한 텔넷 또는 SSH 링크를 클릭하면, NA가 장치에 텔넷 또는 SSH를 통해 연결할 수 있는지 쉽게 확인할 수 있습니다. 자세한 내용은 [241페이지의 "인벤토리 페이지 필드"](#)를 참조하십시오. 장치에 로그인할 수 없는 경우, 장치에 있는 잘못된 액세스 목록, 잘못된 암호 정보 또는 네트워크 연결 문제가 원인일 수 있습니다. 고객 지원 센터에 문의하십시오. 장치에 텔넷 및/또는 SSH를 통해 연결할 수 있지만 장치 검색 작업이 실패하는 경우 4단계로 이동합니다.
4. 장치에서 활성화된 읽기 전용 SNMP가 있는지 확인합니다. 장치에서 읽기 전용 SNMP가 활성화되어 있다면, 이 OID를 사용하여 NA 서버에서 읽기 전용 SNMP를 통해 장치에 연락을 시도해 보십시오. NA 내에서 장치에 대해 구성된 커뮤니티 문자열을 사용하는지 확인합니다. 읽기 전용 SNMP를 활성화하지 않으려면, 장치를 추가하거나 편집할 때 드라이버 드롭다운 목록에서 드라이버를 수동으로 선택할 수 있습니다. 자세한 내용은 [230페이지의 "장치 구성 데이터 편집"](#)을 참조하십시오. 읽기 전용 SNMP를 활성화했으면, NA에 로그인하고 추가하려는 장치를 선택한 후 장치 편집을 클릭합니다. 올바른 읽기 전용 SNMP 커뮤니티 문자열이 있는 장치를 업데이트하고 스냅샷을 클릭합니다. 스냅샷 작업이 여전히 실패할 경우 고객 지원 센터에 문의하십시오.

Syslog를 통한 실시간 변경 감지 없음

Syslog를 통한 실시간 변경 감지가 없는 경우

1. 스냅샷하려는 장치가 지원되는 장치 모델 및 NA용 OS 버전인지 확인합니다. 지원되는 장치에 대한 자세한 내용은 DRS(장치 릴리스 서비스) 설명서를 참조하십시오. DRS는 자동화된 새로운 드라이버 릴리스 및 전달 시스템입니다. 장치가 지원되지 않는 경우 고객 지원 센터에 문의하십시오. 장치가 지원되는 경우 2단계로 이동합니다.
2. Syslog 메시지가 NA 서버에 접근하기 위해 Syslog 설정이 올바르게 구성되어 있는지 확인합니다. NA에 전송되는 Syslog 변경 메시지를 트리거할 이벤트를 초기화합니다.
3. 장치/OS 조합이 Syslog를 통한 실시간 변경 감지를 지원하는지 확인합니다. 지원되는 장치에 대한 자세한 내용은 DRS(장치 릴리스 서비스) 설명서를 참조하십시오. DRS는 자동화된 새로운 드라이버 릴리스 및 전달 시스템입니다. 가능한 경우, 이 장치 및 OS에서 Syslog 변경 알림을 사용할 수 있는지 공급업체 웹 사이트에서 확인합니다. 장치에서 Syslog를 통한 실시간 변경 감지가 지원되지 않는다면, 4단계로 이동합니다.
4. AAA 로깅은 NA에서 실시간 변경 감지를 제공하는 다른 방법입니다. AAA 변경 감지가 활성화되었는지 확인합니다. 자세한 내용은 [43페이지의 "구성 관리 페이지 필드"](#)를 참조하십시오. AAA를 사용 중인 경우 장치에서 AAA를 통한 실시간 변경 감지를 지원하는지 확인합니다.

세션 로그

자동화 작업의 어려운 점은 자동화 자체가 아니라, 자동화 작업이 실패할 경우 실패 원인을 확인하는 것입니다. NA에서는 실패 이유를 신속하게 파악하고 해결할 수 있도록 자세한 문제 해결 기능을 제공합니다.

NA에서는 장치 작업에서 자세한 장치 세션 로그를 제공합니다. 이로 인해 NA가 장치에 무엇을 전송하는 중인지, 장치가 어떻게 응답하는지 알 수 있습니다.

1. NA에 로그인합니다.
2. 장치의 기본 메뉴 모음에서 새 장치 작업을 선택하고 명령 스크립트 실행을 클릭합니다. 새 작업 - 명령 스크립트 실행 페이지가 열립니다.
3. 필드에 적용에서, 구성 변경이 허용되는 장치 호스트 이름 또는 IP 주소를 입력합니다.
4. 작업 옵션 — 세션 로그의 "전체 장치 세션 로그 저장" 확인란을 선택합니다.
5. 작업 옵션 — 실행할 명령 스크립트의 드롭다운 메뉴에서 실행할 하는 명령 스크립트를 선택합니다.
6. 실행될 모드를 지정합니다. 예를 들어, IOS 장치인 경우 Cisco IOS 구성을 선택합니다.
7. 장치에 전송할 명령을 입력합니다.
8. 작업 저장 버튼을 클릭합니다.

작업이 실행되면서 NA <-> 장치 인터랙션의 출력이 표시됩니다. 다음을 확인할 수 있어야 합니다.

- NA가 장치에 무엇을 전송했는지
- NA가 장치에서 무엇을 수신하기로 예상했는지
- NA가 장치에서 실제로 무엇을 수신했는지

SWIM 오류 메시지

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM0019	데이터가 부족하여 선택한 장치에 대한 이미지 권장 사항을 수행할 수 없습니다.	데이터베이스에서 이미지 정보를 반입할 수 없습니다.	인벤토리 수집을 성공했는지 확인합니다. 선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다.
SWIM0089	선택한 장치의 Cisco.com에서 이미지 가져오기를 수행할 수 없습니다.	장치에 대해 지원되지 않는 Cisco.com에서 이미지를 추가합니다. 그 이유는 Cisco.com에서는 지원 목록의 장치 플랫폼을 찾을 수 없기 때문입니다.	없음
SWIM0092	장치에 대한 인벤토리 정보를 반입하는 동안 오류가 발생했습니다.	이 장치를 사용할 권한이 있는지 여부 및 인벤토리에 이 장치에 대한 전체 데이터가 있는지 여부를 확인합니다.	선택한 장치에 대해 OS 분석 작업을 실행합니다.
SWIM0093	Cisco.com에서 이미지 정보를 가져올 수 없습니다.	잘못된 Cisco.com 자격 증명 또는 누락된 프록시 구성으로 인해 CWNCM 서버에서 Cisco.com에 연결할 수 없습니다.	Cisco.com 자격 증명이 올바른지 확인합니다. 올바른 경우, 프록시 서버가 올바른 프록시 자격 증명으로 구성되어 있는지 확인합니다. 프록시를 구성하려면, CWNCM 홈 페이지 > 암호 변경 클릭 > 자격 증명 유형의 Cisco.com 프록시 선택 > 사용자 이름 및 암호 입력으로 이동합니다.

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM0125	예상치 못한 오류가 발생했습니다. Cisco 지원 센터에 문의하고 SWIMNG_server.log 파일을 첨부합니다.	없음	다음의 아래에서 사용할 수 있는 로그와 함께 Cisco 기술 지원 센터(TAC)에 문의하십시오. Windows: <CWNCM 설치 폴더>\server\ext\swim\log\SWIMNG_server.log Solaris 및 Linux: <CWNCM 설치 디렉터리>/server/ext/swim/log/SWIMNG_server.log
SWIM0126	예상치 못한 오류가 발생했습니다. Cisco 지원 센터에 문의하고 SWIMNG_server.log 파일을 첨부합니다.	없음	다음의 아래에서 사용할 수 있는 로그와 함께 Cisco 기술 지원 센터(TAC)에 문의하십시오. Windows: <CWNCM 설치 폴더>\server\ext\swim\log\SWIMNG_server.log Solaris 및 Linux: <CWNCM 설치 디렉터리>/server/ext/swim/log/SWIMNG_server.log
SWIM0155	사용자에게 Cisco.com에서 암호 작성 이미지를 다운로드할 권한이 없습니다.	사용자에게 Cisco.com에서 암호 작성 이미지를 다운로드할 권한이 없습니다.	Cisco.com으로 이동하여 암호 작성 약정에 서명합니다.
SWIM0156	다운로드 요청에 대해 응답 스트림을 가져오지 못했습니다.	다운로드 요청에 대해 응답 스트림을 가져오지 못했습니다.	나중에 다시 시도하거나 Cisco.com 웹 사이트에서 이미지를 직접 다운로드한 다음 시스템에 추가합니다.
SWIM1003	SNMP 에이전트는 플래시 파일 시스템에 대한 정보를 얻는 데 필요한 계층을 지원하지 않습니다.	장치에 있는 SNMP 에이전트는 CISCO-FLASH-MIB/OLD-CISCO-FLASH-MIB를 지원하지 않습니다.	장치에서 실행 중인 이미지 버전에 대해 이러한 MIB와 관련이 있는 알려진 버그를 확인합니다.
SWIM1004	장치에 있는 플래시 파일 시스템에 대한 세부사항을 가져올 수 없습니다.	장치에 있는 MIB 구현에 문제가 있을 수 있습니다.	실행 중인 이미지 버전의 알려진 문제에 대해 Cisco.com을 확인합니다.

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1005	플래시 장치 또는 파티션이 장치에 없습니다.	장치에 있는 인벤토리 데이터가 잘못되었거나 선택한 플래시 장치 또는 파티션이 잘못되었습니다.	선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다.
SWIM1006	플래시 파티션이 장치에 없습니다.	장치에 있는 인벤토리 데이터가 잘못되었거나 선택한 플래시 파티션이 잘못되었습니다.	선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다.
SWIM1027	인벤토리 정보를 반입하는 동안 오류가 발생했습니다.	선택한 작업에 필요한 데이터가 불완전하거나 인벤토리에 없습니다.	선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다.
SWIM1029	장치에 대해 필요한 인벤토리 정보를 가져올 수 없습니다.	장치에 대해 인벤토리 수집이 없거나 장치가 응답하지 않습니다.	선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다.
SWIM1030	이것은 RFF(Run From Flash) 장치이지만 응용 프로그램이 플래시에서 실행 중인 이미지를 찾을 수 없습니다.	인벤토리가 업데이트되지 않았거나 플래시 파일이 플래시에서 삭제되었습니다.	선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다.
SWIM1031	실행 중인 소프트웨어에 대해 후보 이미지를 찾을 수 없습니다.	Cisco.com이 내 기본 설정에 포함되어 있지 않거나 소프트웨어 리포지토리 또는 Cisco.com에 해당 이미지가 없습니다.	관리 > 사용자 > 사용자 이름 선택 및 연관된 '권한' 클릭 > 내 기본 설정을 선택하거나 소프트웨어 리포지토리에 이미지를 추가합니다. 소프트웨어 업그레이드 권장 사항을 다시 시작합니다.

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1032	권장에 대해 가져온 이미지가 선택한 장치의 하드웨어 및 소프트웨어 요구 사항을 충족하지 않습니다.	선택한 내 기본 설정을 기반으로 하여 후보 이미지가 필터링되었거나 장치에서 실행하는 데 필요한 플래시/RAM/BootROM을 충족하지 않습니다.	관리 > 사용자 > 사용자 이름 선택 및 연관된 '권한' 클릭 > 내 기본 설정을 선택합니다. 또는 소프트웨어 리포지토리에 이미지를 추가합니다. 소프트웨어 업그레이드 권장 사항을 다시 시작합니다.
SWIM1033	호환성 확인을 적용하여 장치에 대해 가장 적합한 이미지를 찾을 수 없습니다.	선택한 내 기본 설정을 기반으로 하여 후보 이미지가 필터링되었거나 장치에서 실행하는 데 필요한 플래시/RAM/BootROM을 충족하지 않습니다.	관리 > 사용자 > 사용자 이름 선택 및 연관된 '권한' 클릭 > 내 기본 설정을 선택하거나 소프트웨어 리포지토리에 이미지를 추가합니다. 소프트웨어 업그레이드 권장 사항을 다시 시작합니다.
SWIM1034	구성된 이미지 원본에서 장치에 대해 해당 이미지를 찾을 수 없습니다.	Cisco.com이 내 기본 설정에 포함되어 있지 않거나 소프트웨어 리포지토리 또는 Cisco.com에 해당 이미지가 없습니다.	관리 > 사용자 > 사용자 이름 선택 및 연관된 '권한' 클릭 > 내 기본 설정을 선택하거나 소프트웨어 리포지토리에 이미지를 추가합니다. 소프트웨어 업그레이드 권장 사항을 다시 시작합니다.
SWIM1035	권장 옵션을 수행하는 동안 오류가 발생했습니다. 장치에서 실행 중인 이미지의 문제로 인해 이미지를 필터링하는 동안 런타임 오류가 발견되었습니다.	없음	운행을 재시도합니다. 문제가 계속되면 Cisco 기술 지원 센터(TAC)에 디버그 로그를 보내십시오. 디버그 로그는 다음 위치에서 사용할 수 있습니다. Windows: <CWNCM 설치 폴더>\server\ext\swim\log\SWIMNG_server.log Solaris 및 Linux: <CWNCM 설치 디렉터리>/server/ext/swim/log/SWIMNG_server.log

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1036	권장 사항을 수행하는 동안 런타임 오류가 발생했습니다.	없음	운동을 재시도합니다. 문제가 계속되면 Cisco 기술 지원 센터(TAC)에 디버그 로그를 보내십시오. 디버그 로그는 다음 위치에서 사용할 수 있습니다. Windows: <CWNCM 설치 폴더>\server\ext\swim\log\SWIMNG_server.log Solaris 및 Linux: <CWNCM 설치 디렉터리>/server/ext/swim/log/SWIMNG_server.log
SWIM1037	플래시 파티션 정보를 반입하는 동안 오류가 발생했습니다.	인벤토리에서 플래시 정보를 가져올 수 없거나 장치에서 실행 중인 이미지에 문제가 있습니다.	선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다. 문제가 계속되면 실행 중인 이미지 버전의 알려진 문제에 대해 Cisco.com을 확인합니다.
SWIM1038	장치에서 읽기-쓰기 파티션을 찾을 수 없습니다.	없음	읽기-쓰기 파티션이 있는 플래시 장치를 설치하고 인벤토리를 업데이트합니다.
SWIM1039	장치에 대해 저장 권장 사항을 하지 않았습니다.	선택한 장치에는 이미지를 복사하기 위해 충분히 사용 가능한 크기의 파티션이 없을 수 있습니다.	선택한 장치에 이미지를 복사하기 위해 충분히 사용 가능한 크기의 파티션이 있는지 확인합니다.
SWIM1040	장치에 대한 플래시 정보를 가져올 수 없습니다.	인벤토리에서 플래시 정보를 가져올 수 없거나 장치에서 실행 중인 이미지에 문제가 있습니다.	선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다. 문제가 계속되면 실행 중인 이미지 버전의 알려진 문제에 대해 Cisco.com을 확인합니다.

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1041	이 장치 업그레이드는 장치에 대해 SSH/텔넷 연결 열기가 필요합니다.	암호 사용이 장치에 대해 잘못 구성되어 있습니다.	적절한 SSH/텔넷 암호가 장치에 대해 올바르게 구성되어 있는지 확인합니다.
SWIM1042	장치에 있는 부트플래시 용량이 선택한 이미지를 실행하기에 충분하지 않을 수 있습니다.	장치에 있는 부트플래시 용량이 선택한 이미지를 실행하기에 충분하지 않을 수 있습니다.	없음
SWIM1043	부트로더 이미지 검증을 수행하는 동안 런타임 오류가 발생했습니다.	선택한 이미지 버전이 표준 버전 형식이 아닐 수 있습니다.	운동을 재시도합니다. 문제가 계속되면 Cisco 기술 지원 센터(TAC)에 디버그 로그를 보내십시오. 디버그 로그는 다음 위치에서 사용할 수 있습니다. Windows: <CWNCM 설치 폴더>\server\ext\swim\log\SWIMNG_server.log Solaris 및 Linux: <CWNCM 설치 디렉터리>/server/ext/swim/log/SWIMNG_server.log
SWIM1044	새 이미지를 복사하기 전에 부트플래시 파티션이 지워집니다.	선택한 부트로더 이미지가 부트플래시의 사용 가능한 공간에 적합하지 않습니다.	사용 가능한 경우 다른 부트로더 이미지를 선택합니다.
SWIM1046	선택한 소프트웨어가 선택한 플래시 파티션에 적합하지 않습니다.	선택한 소프트웨어 이미지가 부트플래시의 사용 가능한 공간에 적합하지 않습니다.	업그레이드를 위해 다른 플래시 파티션을 선택합니다.
SWIM1048	장치에서 활성 상태인 시스템 소프트웨어가 선택한 이미지를 실행할 수 없습니다.	장치에서 활성 상태인 시스템 소프트웨어가 선택한 이미지와 호환되지 않습니다.	현재 시스템 소프트웨어로 업그레이드될 수 있는 다른 이미지를 선택하거나 소프트웨어 버전으로 시스템 소프트웨어를 업그레이드합니다.
SWIM1049	선택한 이미지에는 이미지를 업그레이드하는 동안 지워질 플래시가 필요합니다.	없음	필요한 백업을 수행했는지 확인합니다.

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1050	장치에 대해 읽기-쓰기 SNMP 커뮤니티 문자열을 사용할 수 없습니다.	장치에 대해 읽기-쓰기 SNMP 커뮤니티 문자열을 사용할 수 없습니다.	장치에 대해 읽기-쓰기 커뮤니티 문자열을 추가합니다.
SWIM1051	장치에 대해 자격 증명 정보를 가져올 수 없습니다.	장치가 CWNCM 서버에서 관리되지 않거나 장치 자격 증명에 올바르지 않거나 또는 장치 액세스 권한이 없습니다.	없음
SWIM1052	암호 사용이 장치에 대해 구성되어 있지 않습니다.	RFF(Run From Flash) 파티션 소프트웨어 업그레이드를 위해 암호 사용이 구성되어야 합니다.	장치에 대해 암호 사용을 구성합니다.
SWIM1053	선택한 MICA 이미지는 장치에서 실행 중인 이미지와 동일합니다.	이미지의 소프트웨어 버전은 장치에서 최신입니다.	없음
SWIM1054	장치의 텔넷 자격 증명을 확인하는 동안 오류가 발생했습니다.	없음	장치에 대한 텔넷 자격 증명에 올바른지 확인합니다.
SWIM1055	선택한 플래시 파티션은 읽기 전용입니다.	플래시 파티션에서 쓰기가 활성화되어 있지 않거나 읽기-쓰기 파티션이 없습니다.	읽기-쓰기 파티션이 있는지 확인합니다. 플래시 파티션에서 쓰기를 활성화로 설정합니다.
SWIM1056	선택한 저장 장치에 있는 소프트웨어를 업데이트할 방법을 알 수 없습니다.	없음	사용 가능한 경우 다른 플래시 파티션을 선택합니다.
SWIM1057	이미지 업그레이드를 위해 장치가 Rxbboot 모드로 됩니다.	없음	사용 가능한 경우 시스템 소프트웨어에 대해 다른 플래시 장치를 선택합니다.
SWIM1058	선택한 소프트웨어 버전은 플래시 MIB 옵션에 응용 프로그램이 장치에서 소프트웨어 업그레이드를 수행할 수 없도록 하는 일부 알려진 문제가 있습니다.	없음	사용 가능한 경우 장치를 수동으로 업그레이드하거나 이후 소프트웨어 버전을 선택합니다.

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1059	Dial Shelf가 새로 로드된 Router Shelf 소프트웨어 이미지와 호환되는 소프트웨어 이미지를 실행하는지 확인합니다.	Router shelf 소프트웨어 이미지가 Dial Shelf 소프트웨어 이미지와 호환되지 않습니다.	현재 Dial Shelf 소프트웨어가 호환되는지 확인하려면 Router Shelf 소프트웨어 이미지에 대한 릴리스 노트를 참조하십시오. 그렇지 않은 경우 Dial Shelf 소프트웨어를 업그레이드합니다.
SWIM1060	선택한 이미지의 파일 크기를 가져올 수 없습니다.	선택한 이미지가 Cisco.com에서 제거되었을 수 있습니다.	업그레이드를 위해 다른 이미지를 선택합니다.
SWIM1062	선택한 이미지가 장치에서 이미 실행 중입니다.	없음	이 이미지가 장치에 대해 업그레이드할 이미지인지 검증합니다.
SWIM1063	선택한 이미지의 최소 RAM 요구 사항을 확인할 수 없습니다.	장치에서 사용할 수 있는 RAM은 이 이미지를 활성화하기에 충분하지 않을 수 있습니다.	없음
SWIM1064	장치에서 사용할 수 있는 RAM은 선택한 이미지를 활성화하기에 충분히 크지 않을 수 있습니다.	장치에서 사용할 수 있는 RAM은 선택한 이미지를 활성화하기에 충분히 크지 않을 수 있습니다.	다른 이미지를 선택하거나 장치에서 RAM을 업그레이드합니다.
SWIM1065	장치에서 사용할 수 있는 RAM은 선택한 이미지를 활성화하기에 충분하지 않을 수 있습니다.	장치에서 사용할 수 있는 RAM은 선택한 이미지를 활성화하기에 충분하지 않을 수 있습니다.	업그레이드를 위해 다른 이미지를 선택합니다.
SWIM1067	선택한 이미지에 대한 검증을 수행하는 동안 런타임 오류가 발생했습니다.	없음	업그레이드를 위해 다른 이미지를 선택합니다. 문제가 해결되지 않으면 Cisco 기술 지원 센터(TAC)에 디버그 로그를 보내십시오. 디버그 로그는 다음 위치에서 사용할 수 있습니다. Windows: <CWNCM 설치 폴더> \server\ext\swim\log\SWIMNG_server.log Solaris 및 Linux: <CWNCM 설치 디렉터리>/server/ext/swim/log/SWIMNG_server.log

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1068	선택한 이미지에 업그레이드에 필요한 최소 시스템 소프트웨어 버전이 없습니다.	선택한 이미지에 업그레이드에 필요한 최소 시스템 소프트웨어 버전이 없습니다.	11.0보다 상위 버전의 다른 이미지를 선택합니다.
SWIM1069	선택한 이미지의 기능 하위 집합은 소프트웨어 기능 집합을 실행하는 하위 집합이거나 같습니다. 다른 이미지를 선택합니다.	선택한 이미지의 기능 하위 집합은 소프트웨어 기능 집합을 실행하는 하위 집합이거나 같습니다.	다른 이미지를 선택합니다.
SWIM1070	실행 중인 이미지의 기능 하위 집합을 확인할 수 없습니다. 다른 이미지를 선택합니다.	선택한 이미지의 기능 하위 집합은 소프트웨어 기능 집합을 실행하는 하위 집합이거나 같습니다.	다른 이미지를 선택합니다.
SWIM1075	부트플래시에 맞거나 더 최신인 이미지를 찾을 수 없습니다.	없음	실행 중인 이미지 버전보다 높고 부트플래시에 맞는 버전의 소프트웨어 리포지토리에 부트로더 이미지를 추가합니다.
SWIM1076	장치에서 읽기-쓰기 부트 파티션을 찾을 수 없습니다.	장치에서 읽기-쓰기 부트 파티션을 사용할 수 없습니다.	장치에 있는 읽기-쓰기 부트플래시를 삽입하고 인벤토리를 업데이트합니다.
SWIM1077	부트로더 이미지에 대한 부트플래시 파티션을 찾을 수 없습니다.	부트로더 이미지에 대해 부트플래시 파티션을 사용할 수 없습니다.	장치에 있는 읽기-쓰기 부트플래시를 삽입하고 인벤토리를 업데이트합니다.
SWIM1079	이미지 버전을 비교할 수 없습니다.	모든 이미지의 이미지 형식이 비교를 위해 호환되지 않을 수 있습니다.	버전 형식을 확인합니다. 업그레이드를 위해 다른 이미지를 선택합니다.

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1082	모뎀 이미지를 비교하는 동안 런타임 오류가 발생했습니다.	비교할 모뎀 이미지를 잘못 선택했거나 모뎀 이미지 형식이 호환되지 않습니다.	업그레이드를 위해 다른 모뎀 이미지를 선택합니다. 문제가 계속되면 Cisco 기술 지원 센터(TAC)에 디버그 로그를 보내십시오. 디버그 로그는 다음 위치에서 사용할 수 있습니다. Windows: <CWNCM 설치 폴더>\server\ext\swim\log\SWIMNG_server.log Solaris 및 Linux: <CWNCM 설치 디렉터리>/server/ext/swim/log/SWIMNG_server.log
SWIM1083	플래시에 맞거나 더 최신인 이미지를 찾을 수 없습니다.	없음	소프트웨어 리포지토리에 다른 이미지를 추가하고 운영을 재시도합니다.
SWIM1084	장치에 대해 최소 플래시 요구 사항을 찾을 수 없습니다.	장치에서 사용 가능한 플래시 공간이 선택한 이미지에 대해 충분하지 않을 수 있습니다.	이미지가 장치에 맞는 지 확인합니다.
SWIM1085	선택한 이미지에 대해 MinFlash 속성을 알 수 없습니다.	선택한 이미지가 선택한 파티션에 맞지 않습니다.	이미지가 선택한 파티션에 맞는 지 확인하거나 다른 이미지를 선택합니다.
SWIM1087	장치 표시를 가져올 수 없습니다.	인벤토리에서 장치 세부사항을 검색할 수 없습니다.	로그를 캡처하여 Cisco 기술 지원 센터(TAC)에 문의하십시오. 디버그 로그는 다음 위치에서 사용할 수 있습니다. Windows: <CWNCM 설치 폴더>\server\ext\swim\log\SWIMNG_server.log Solaris 및 Linux: <CWNCM 설치 디렉터리>/server/ext/swim/log/SWIMNG_server.log

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1092	선택한 이미지는 시스템 업그레이드에 필요한 최소 시스템 소프트웨어 버전이 없습니다.	없음	최소 지원 버전보다 상위 버전의 이미지를 선택합니다. Cisco IOS 소프트웨어용 호환성 매트릭스에 대한 문서를 참조하십시오.
SWIM1093	인벤토리에서 새시 정보를 가져올 수 없습니다.	없음	선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다.
SWIM1094	SNMP-V3 매개 변수가 잘못되었거나 장치에 대해 사용할 수 없습니다.	이에 대한 원인은 다음 중 하나일 수 있습니다. <ul style="list-style-type: none"> • SNMP-V3 암호가 잘못 구성되어 있습니다. • SNMP-V3 알고리즘이 잘못 구성되어 있습니다. • SNMP-V3 엔진 ID가 장치에 대해 구성되어 있지 않습니다. 	SNMP-V3 암호, SNMP-V3 알고리즘 및 SNMP-V3 엔진 ID가 장치에 대해 구성되어 있는지 확인합니다.
SWIM1095	장치 컨텍스트에 있는 SNMP-V3 사용자 이름을 확인하는 동안 오류가 발생했습니다.	없음	장치에 대해 SNMP-V3 자격 증명을 업데이트합니다. 선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다.
SWIM1097	선택한 부트로더 이미지는 장치에서 실행 중인 부트로더의 버전보다 하위 버전입니다.	장치에서 실행 중인 부트로더 이미지 버전이 최신입니다.	업그레이드를 위해 상위 버전을 사용할 수 있는지 확인합니다.
SWIM1098	선택한 이미지는 장치에서 실행 중인 이미지보다 하위 버전입니다.	장치에서 실행 중인 이미지 버전이 최신입니다.	장치 소프트웨어 업그레이드를 위해 상위 이미지를 선택합니다. (변경 필요 없음)

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1099	이미지 업그레이드 절차에서 실행 중인 이미지에서 MIB 계층을 기반으로 하여 SSH/텔넷-기반 접근으로 복원할 수 있습니다.	SSH/텔넷 암호가 장치에 대해 구성되지 않을 수 있습니다.	적절한 SSH/텔넷 암호가 장치에 대해 구성되어 있는지 확인합니다.
SWIM1100	장치에 대해 SNMP-V2 읽기-쓰기 커뮤니티 문자열을 찾을 수 없습니다.	SNMP-V2 자격 증명이 장치에 대해 올바르게 구성되지 않을 수 있습니다.	SNMP-V2 자격 증명이 장치에 대해 올바르게 구성되어 있는지 확인합니다.
SWIM1101	이 장치 업그레이드는 장치에 대해 SSH/텔넷 연결 열기가 필요합니다.	장치에 대한 암호 사용이 장치에 대해 구성되어 있지 않습니다.	적절한 SSH/텔넷 암호가 장치에 대해 올바르게 구성되어 있는지 확인합니다.
SWIM1102	이 장치 업그레이드는 장치에 대해 SSH/텔넷 연결 열기가 필요합니다.	장치의 자격 증명을 확인하는 동안 오류가 발생했습니다.	적절한 SSH/텔넷 암호가 장치에 대해 올바르게 구성되어 있는지 확인합니다.
SWIM1103	선택한 이미지가 장치에 호환되지 않을 수 있습니다.	이미지는 장치에서 실행 중인 이미지와 동일한 장치 제품군에 속합니다. 하지만 호환되지 않는 것으로 식별됩니다.	선택한 이미지에 대해 caveat가 식별되는지 Cisco.com 문서를 확인합니다.
SWIM1105	선택한 이미지에 대한 이미지 상태를 확인할 수 없습니다.	선택한 이미지가 지연된 상태에 있을 수 있습니다.	이미지가 지연된 상태에 있지 않은지 확인합니다. 이미지를 업그레이드하기 전에 Cisco.com에서 관련 문서를 참조하십시오.
SWIM1106	업그레이드를 위해 선택한 이미지는 .tar 형식으로 압축됩니다. 플래시는 이미지를 업그레이드하는 동안 덮어쓰게 됩니다.	없음	업그레이드하기 전에 필요한 백업 작업이 완료되었는지 확인합니다.
SWIM1107	이 옵션에는 인벤토리에 있는 devicename 데이터가 필요합니다.	필요한 장치 정보를 인벤토리에서 사용할 수 없습니다.	선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다.

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1109	선택한 이미지에 대한 이미지가 지연되거나 지원되지 않습니다.	선택한 이미지에 대한 이미지가 지연되거나 지원되지 않습니다.	CWNCM 응용 프로그램에서 이미지가 지원되는지 확인합니다. 이미지를 업그레이드하기 전에 Cisco.com에서 문서를 확인합니다.
SWIM1111	이 이미지 유형을 업그레이드하기에 사용 가능 공간이 충분하지 않습니다.	이미지를 업그레이드하기 위한 공간이 부족합니다.	다른 이미지를 선택하거나 공간을 확보합니다. 인벤토리를 업데이트하고 작업을 재시도합니다.
SWIM1112	독립적으로 관리하는 경우 이 모듈을 업그레이드할 수 없습니다.	별도의 장치로서 관리하는 경우 이 모듈을 업그레이드할 수 있습니다.	이 모듈에 독립적인 IP 주소를 할당합니다. 이 모듈을 업그레이드하려면 별도의 장치로서 관리하고 해당 장치를 선택합니다.
SWIM1116	장치 컨텍스트에서 읽기-쓰기 SNMP 커뮤니티 문자열을 반입할 수 없습니다.	장치에 대해 읽기-쓰기 커뮤니티 문자열을 사용할 수 없습니다.	장치에 대해 읽기-쓰기 커뮤니티 문자열을 추가합니다.
SWIM1118	선택한 이미지가 실행 중인 이미지의 버전보다 하위 버전입니다.	선택한 이미지가 실행 중인 이미지의 버전보다 하위 버전입니다.	없음
SWIM1119	이 장치에 대해 텔넷 자격 증명이 없습니다. 장치에 대해 자격 증명을 확인하는 동안 오류가 발생했습니다.	SSH/텔넷 암호가 장치에 대해 올바르게 구성되어 있지 않습니다.	적절한 SSH/텔넷 암호가 장치에 대해 올바르게 구성되어 있는지 확인합니다.

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1120	장치의 sysObjectID를 가져올 수 없습니다.	없음	<p>선택한 장치에 대해 OS 분석 작업을 실행합니다. 문제가 계속되면 Cisco 기술 지원 센터 (TAC)에 디버그 로그를 보내십시오. 디버그 로그는 다음 위치에서 사용할 수 있습니다.</p> <p>Windows: <CWNCM 설치 폴더> >\server\ext\swim\log\SWIMNG_server.log</p> <p>Solaris 및 Linux: <CWNCM 설치 디렉터리>/ server/ext/swim/log/ SWIMNG_server.log</p>
SWIM1122	검증하는 동안 런타임 오류가 발견되었습니다.	없음	<p>운행을 재시도합니다. 문제가 계속되면 Cisco 기술 지원 센터(TAC)에 디버그 로그를 보내십시오. 디버그 로그는 다음 위치에서 사용할 수 있습니다.</p> <p>Windows: <CWNCM 설치 폴더>\server\ext\swim\log\SWIMNG_server.log</p> <p>Solaris 및 Linux: <CWNCM 설치 디렉터리>/ server/ext/swim/log/ SWIMNG_server.log</p>
SWIM1123	이 장치에 대해 텔넷 사용자 이름이 없습니다.	없음	장치에 대해 기본 사용자 이름이 구성되어 있는지 확인합니다.
SWIM1139	bootldr을 업그레이드하기 위해 사용할 수 있는 부트 플래시 파티션을 선택합니다. bootldr을 업그레이드하기 위해 부트 플래시를 사용하는 것이 좋습니다.	이는 사용자가 배포 및 부트 플래시가 아닌 저장 위치에 대해 부트로더 이미지를 선택했을 경우 발생합니다.	<p>bootldr을 업그레이드하기 위해 사용할 수 있는 부트 플래시 파티션을 선택합니다.</p> <p><i>다음 페이지에서 계속됨</i></p>

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1162	장치에 대해 이미지를 권장하는 동안 오류가 발생했습니다.	이미지 소프트웨어 권장은 인벤토리에서 수집된 장치 ROM, RAM 및 플래시를 기반으로 합니다. 장치에 결함이 있는 하드웨어(플래시)가 있는 경우에는 인벤토리에서 사용할 수 없게 됩니다.	결함이 있는 하드웨어에 대한 장치 또는 장치 소프트웨어에 있는 버그를 확인합니다. 선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다. 문제가 계속되면 Cisco 기술 지원 센터(TAC)에 디버그 로그를 보내십시오. 디버그 로그는 다음 위치에서 사용할 수 있습니다. Windows: <CWNCM 설치 폴더>\server\ext\swim\log\SWIMNG_server.log Solaris 및 Linux: <CWNCM 설치 디렉터리>/server/ext/swim/log/SWIMNG_server.log
SWIM129	선택한 이미지가 장치의 사용 가능한 플래시 크기에 맞지 않습니다. 선택한 저장 파티션이 배포하는 동안 지워집니다.	다음과 같은 경우 업그레이드를 위해 부트 로더 이미지를 선택하거나(함께 선택한 시스템 소프트웨어 이미지가 없습니다.) 또는 복사할 부트 로더 이미지에 대해 저장 위치가 지워지지 않습니다.	업그레이드를 위해 시스템 소프트웨어를 선택하지 않았으므로 선택한 저장 파티션에 실행 중인 시스템 소프트웨어가 없는 것을 확인합니다. 실행 중인 시스템 소프트웨어를 백업하고 작업이 실패한 경우 백업한 이미지에서 장치 부팅을 확인합니다.
SWIM1501	4.1(1)보다 낮은 이미지 버전으로 감독자를 다운그레이드할 수 없습니다.	이는 4.1(1)보다 낮은 CATOS 이미지를 배포하려는 경우 발생합니다.	계속 다운그레이드하는 경우 장치 구성을 잃을 수 있습니다. 상위 버전을 사용합니다.
SWIM1525	알 수 없는 패키지 유형입니다.	없음	선택한 모듈을 지원하지 않습니다.
SWIM1529	<i>devicename</i> 에 대해 인벤토리에서 사용할 수 있는 모듈 정보가 없습니다.	<i>devicename</i> 에 대해 인벤토리에서 사용할 수 있는 모듈 정보가 없습니다.	선택한 장치에 대해 OS 분석 작업을 실행합니다.

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1530	모듈 <i>modulename</i> 에 대해 저장 권장 사항을 지원하지 않습니다.	없음	이 모듈에 대해 저장 권장 사항을 지원하지 않습니다. 모듈이 판매 종료 또는 수명 종료되었을 수 있기 때문입니다.
SWIM1532	선택한 이미지를 수용할 읽기-쓰기 파티션이 장치에 없습니다.	없음	사용 가능 공간을 충분히 확보합니다.
SWIM1542	감독자에 대한 최소 지원 버전은 3.8입니다.	없음	업그레이드할 이미지의 상위 버전을 선택합니다.
SWIM1543	선택한 이미지가 실행 중인 이미지의 버전보다 하위 버전이거나 동일합니다.	선택한 이미지가 실행 중인 이미지의 버전보다 하위 버전이거나 동일합니다.	없음
SWIM1546	장치에서 NVRAM 크기가 이미지를 실행하기에 충분히 크지 않을 수 있습니다.	장치에서 NVRAM 크기가 이미지를 실행하기에 충분히 크지 않을 수 있습니다.	다른 이미지를 선택하거나 장치에서 NVRAM을 업그레이드하고 업그레이드 옵션을 재시도합니다.
SWIM1547	선택한 이미지에서 사용할 수 있는 NVRAM 크기를 확인할 수 없습니다.	이 모듈에서 RAM 크기가 이미지를 저장하기에 충분히 크지 않을 수 있습니다.	선택한 이미지를 실행하기에 충분한 NVRAM이 모듈에 있는지 확인합니다. 그렇지 않으면 다른 이미지를 선택하거나 모듈에서 RAM을 업그레이드합니다.
SWIM1548	선택한 이미지에 대해 소프트웨어 요구 사항을 찾을 수 없습니다.	없음	다른 이미지를 선택합니다.
SWIM1549	선택한 새 소프트웨어가 호환되는지 검증합니다.	소프트웨어 관리에서 ATM 소프트웨어 기능을 확인할 수 없습니다.	이전 소프트웨어의 모든 기능을 새 소프트웨어에서 사용할 수 있는지 확인하려면 새 소프트웨어에 대한 릴리스 노트를 확인합니다.
SWIM1554	장치를 업그레이드하기 위해 선택한 이미지를 사용할 수 없습니다.	선택한 이미지를 실행할 수 있는 모듈이 장치에 없습니다.	다른 이미지를 선택합니다.

다음 페이지에서 계속됨

메시지 ID	오류 메시지	가능한 원인	가능한 작업
SWIM1560	인벤토리에서 모듈에 해당하는 슬롯 번호를 가져올 수 없습니다.	없음	선택한 장치에 대해 OS 분석 작업을 실행하고 소프트웨어 업그레이드 권장 사항을 시작합니다.
SWIM2001	장치에 연결하는 동안 텔넷 오류가 발생했습니다. 장치에 연결할 수 없습니다.	장치에 대해 잘못된 액세스 정보입니다.	장치에 대해 사용자 이름 및 암호를 검증한 다음 작업을 재시도합니다.
SWIM2002	장치에 있는 플래시 파일 시스템에 대한 세부사항을 가져올 수 없습니다.	플래시 장치를 사용할 수 없거나 플래시 정보 형식이 변경되었습니다.	플래시 장치를 확인하고 OS 분석 작업을 다시 실행합니다.
SWIM3501	선택한 장치에 대해 장치 자격 증명을 반입할 수 없습니다.	장치에 대해 자격 증명이 올바르게 구성되어 있지 않을 수 있습니다.	장치에 대해 자격 증명 구성이 되어 있는지 확인합니다.
SWIM3703	선택한 이미지에는 시스템 업그레이드에 필요한 최소 시스템 소프트웨어 버전이 없습니다.	없음	11.3(0)보다 상위 버전의 다른 이미지를 선택합니다.
SWIM5001	프로토콜을 사용하여 장치 <i>devicename</i> 에 연결할 수 없습니다.	장치에 접근할 수 없거나 장치에 대해 잘못된 액세스 정보가 있습니다.	장치에 접근할 수 있는지 그리고 자격 증명에 올바른지 검증합니다.
SWIM4800	장치에서 실행 중인 버전이 최소 지원 버전보다 낮습니다.	없음	최소 지원 버전 이상으로 장치를 수동으로 업그레이드합니다.

부록 A: 명령줄 참조

명령 창을 열려면 화면의 왼쪽에 있는 검색 탭에서 장치 IP 주소나 호스트 이름을 입력하고 연결 버튼을 클릭합니다.

또한 연결 메뉴를 사용하여 장치 세부사항 페이지에서 명령 창을 열 수도 있습니다. 명령 창 내에서 복사할 텍스트를 선택하고 Enter 키를 누르면 됩니다. 강조 표시된 텍스트가 복사 버퍼에 저장됩니다. 다음에는 이 텍스트를 다른 응용 프로그램으로 붙여 넣을 수 있습니다. 작업을 완료한 후 `exit`를 입력하여 창을 닫습니다.

참고: 텔넷/SSH 프록시를 사용하여 장치에 직접 연결하는 경우 장치를 종료해도 텔넷/SSH 프록시에 남아 있습니다. 다시 `exit`를 입력하지 않는 한 CLI 명령을 입력하여 다른 장치에 연결할 수 있습니다.

CLI 명령에 대한 도움말을 보려면 `help`를 입력하여 모든 명령 목록을 표시합니다. 특정 명령에 대해 자세한 도움말을 보려면 `help <명령 이름>`을 입력합니다.

참고: CLI는 대/소문자를 구분하지 않습니다. 대소문자 구분 없이 모든 명령과 옵션을 입력할 수 있습니다.

CLI 도움말은 다음 명령을 사용하여 온라인에서 사용할 수 있습니다.

- CLI 프롬프트에서 `help`를 입력합니다. 알파벳 순으로 거의 모든 CLI 명령 목록을 볼 수 있어야 합니다. 예를 들어, `Import` 명령에 대한 도움말을 보려면 `import`를 입력합니다. (**참고:** 도움말 또는 종료/끝내기 명령에 대한 도움말 텍스트가 없습니다.)
- 예를 들어 `Import` 명령에 대한 도움말 정보를 보려면 `help import`를 입력합니다. `help <명령 이름>` 명령은 이름, 구문, 설명 및 예를 포함하여 해당 명령에 대한 자세한 정보를 표시합니다.
- 명령줄로 완료하는 경우 `exit`를 입력합니다. 시작하는 세션 유형에 따라, 다시 종료를 입력하고 수동으로 창을 닫아야 할 수 있습니다.

참고: 동일한 첫째 단어로 시작하는 모든 명령 목록을 반환하려면 `help` 명령과 명령의 첫째 단어만 입력할 수도 있습니다.

CLI 도움말 텍스트에 사용된 유형 규칙은 특수한 의미를 가집니다. 다음 표에는 규칙 및 규칙의 의미가 나열되어 있습니다.

규칙	의미
>	단일 오른쪽 꺾쇠 괄호는 명령을 입력하는 명령 프롬프트를 나타냅니다.
-	대시는 명령 옵션 앞에 옵니다.
< >	꺾쇠 괄호를 사용하여 IP 주소와 같이 입력해야 하는 변수 텍스트를 묶습니다. 꺾쇠 괄호를 포함하지 않습니다.
[]	대괄호는 하나 이상의 선택 사항 요소를 구분합니다.
	세로 파이프는 괄호 내 인수를 구분합니다. 하나의 인수만 포함합니다.

구문 및 예를 포함한 CLI 명령의 전체 목록은 *HP Network Automation 7.60 API Reference Guide*를 참조하십시오.

부록 B: 명령 권한

사용자에게는 웹 페이지 보기 또는 명령 실행과 같은 수행할 각 작업에 해당하는 명령 권한이 명시적으로 부여되어야 합니다. 명령 권한 집합은 명령 권한 역할을 생성합니다. 그런 다음 사용자 그룹에 역할을 적용하여 지정된 사용자 그룹에 대한 명령 권한을 설정할 수 있습니다. 자세한 내용은 [337페이지의 "새 사용자 역할 페이지 필드"](#)를 참조하십시오.

참고: NA에는 명령 권한, 장치 권한 수정, 스크립트 권한 및 장치 권한 보기를 비롯하여 네 가지 유형의 권한이 포함되어 있습니다. 일부 명령 권한은 하나 이상의 다른 권한이 필요합니다. 자세한 내용은 [920페이지의 "명령 권한 정의"](#)를 참조하십시오.

명령 권한 허가

명령 권한을 부여하려면

1. 관리 아래 메뉴 모음에서 사용자 역할 및 권한을 클릭합니다. 사용자 역할 및 권한 페이지가 열립니다.
2. 페이지 맨 위에 있는 새 사용자 역할 링크를 클릭합니다. 새 사용자 역할 페이지가 열립니다. 자세한 내용은 [335페이지의 "사용자 역할 추가"](#)를 참조하십시오.

명령 목록

장치 추가	전자 메일 보고서
장치 그룹 추가	외부 인증 설정
이벤트 추가	요약 보고서 생성
SNMP 트랩 구성 추가	장치 및 암호 가져오기
관리 설정	ListSysOIDs
장치 그룹 관리	보기 나열
사용자 관리	ACL 관리
사용자 그룹 관리	명령 스크립트 관리
장치 구성 주식 처리	구성 정책 관리
동시 텔넷/SSH 세션 인증	장치 암호 규칙 관리
장치 소프트웨어 백업	진단 스크립트 관리
장치 일괄 편집	이벤트 규칙 관리
장치 암호 변경	향상된 고객 데이터 관리
구성 정책 준수 확인	배포된 시스템 관리
Syslog 구성	게이트웨이 관리
커넥터 리디렉션	IP 주소 관리
데이터 정리	라이선스 관리
중복 방지	파티션 관리
액세스 삭제	소프트웨어 준수 관리
장치 삭제	소프트웨어 수준 관리
장치 구성 삭제	소프트웨어 이미지 관리
진단 삭제	시스템 보고서 관리
드라이버 삭제	템플릿 관리
세션 삭제	사용자 관리
소프트웨어 준수 삭제	사용자 그룹 관리
소프트웨어 이미지 삭제	사용자 역할 관리
소프트웨어 수준 삭제	관리 보기
시스템 이벤트 삭제	장치 구성 수정
작업 삭제	SecurID 수정
원격 에이전트 배포	멀티 태스킹 프로젝트
소프트웨어 배포	워크플로 승인 오버라이드
네트워크 장치 감지	장치 작업 다시 로드
장치 드라이버 검색	FQDN 확인
드라이버	명령 스크립트 실행
ACL 편집	진단 실행
ACL 설명 주식	외부 응용 프로그램 실행
사용자[가 변경한] 구성 편집	ICMP 테스트 실행
장치 편집	
비활성 장치 편집	
작업 편집	
사용자 편집	

(다음 페이지에 계속)

최고 작업 우선 순위 설정
반복 작업 동기화
스냅샷 작성
텔넷/SSH 클라이언트
문제 해결
장치 주석 업데이트
장치 티켓 업데이트
워크플로 설정
ACL 보기
명령 스크립트 보기
구성 정책 이벤트 보기
배포된 소프트웨어 보기
구성 정책 보기
장치 구성 보기
장치 진단 보기

장치 정보 보기
진단 스크립트 보기
드라이버 보기
이벤트 규칙 보기
전체 장치 구성 보기
스크립트 및 진단 결과 보기
SecurID 보기
세션 보기
소프트웨어 이미지 아카이브 보기
작업 보기
템플릿 보기
사용자 정보 보기
워크플로 설정 보기

명령 권한 정의

명령 권한	설명
장치 활성화/비활성화	장치를 활성화 또는 비활성화할 수 있습니다.
장치 추가	NA 시스템에 장치를 추가할 수 있습니다. 이 권한에는 장치 마법사 추가를 통해 장치 추가가 포함되어 있습니다.
장치 그룹 추가	장치 그룹을 생성할 수 있습니다. 공용 장치 그룹을 생성하려면, 장치 그룹 관리 권한도 부여되어야 합니다.
그룹에 장치 추가	장치 그룹에 장치를 추가할 수 있습니다. 장치가 NA 데이터베이스에 이미 있어야 합니다.
이벤트 추가	편집 메뉴에서 새 메시지 옵션을 사용할 수 있습니다.
SNMP 트랩 구성 추가	SNMP 트랩을 구성할 수 있으며 "add SNMP trap config" CLI 명령(구성 옵션 "snmp/traps/global"에 차례로 추가)을 실행할 수 있습니다.
관리 설정	관리 설정을 변경할 수 있습니다. 워크플로 설정 및 외부 인증 설정과 같은 추가 권한이 필요한 관리 설정이 있습니다.
장치 그룹 관리	상위 및 공개 그룹 추가, 수정 및 제거를 포함하여 장치 그룹을 관리할 수 있습니다.
장치 구성 주석 처리	장치 구성을 주석 처리할 수 있습니다.
동시 텔넷/SSH 세션 인증	장치에 다중 프록시 연결 방지를 오버라이드할 수 있습니다.
장치 소프트웨어 백업	장치 소프트웨어 백업 작업을 실행할 수 있습니다.
장치 일괄 편집	일괄 편집 도중 다중 장치를 수정할 수 있습니다.

명령 권한	설명
장치 암호 변경	단일 장치 암호를 변경하는 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
장치 암호 변경(그룹)	장치 그룹의 암호를 변경할 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치 그룹에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
구성 정책 준수 확인	구성 정책 준수 확인 작업을 실행할 수 있습니다. 정책 준수 확인 작업을 사용하면 장치가 구성 정책 또는 소프트웨어 준수 정책을 준수하는지 확인할 수 있습니다.
장치 예약 지우기	활동 캘린더에 나타나는 장치 예약 충돌을 지울 수 있습니다.
Syslog 구성	장치 Syslog 설정을 구성하는 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
Syslog 구성(그룹)	장치 Syslog 설정 그룹을 구성하는 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치 그룹에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
커넥터 리디렉션	NNM 7.x 및 NNM 8.x에 대한 URL 작업을 리디렉션합니다. 커넥터 리디렉션에서는 NNM에서 제공하는 IP 주소에서 장치 ID를 조회합니다. 또한 커넥터 리디렉션에서는 구성 이력과 같은 장치 정보를 전달할 수 있습니다.
데이터 정리 작업	단일 장치에 대한 데이터 정리 작업을 예약할 수 있습니다. 데이터를 정리하면 사용되지 않는 파일, 진단, 이벤트 및 작업이 제거됩니다.
데이터 정리 작업(그룹)	장치 그룹에 대한 데이터 정리 작업을 예약할 수 있습니다. 데이터를 정리하면 사용되지 않는 파일, 진단, 이벤트 및 작업이 제거됩니다.

명령 권한	설명
중복 방지	단일 장치를 제거하거나 비활성화할 수 있기 때문에 장치 인터페이스가 NA 데이터베이스 내에서 한 번만 발생합니다.
중복 방지(그룹)	장치 그룹을 제거하거나 비활성화할 수 있기 때문에 장치 인터페이스가 NA 데이터베이스 내에서 한 번만 발생합니다.
액세스 삭제	장치 액세스 로그를 삭제할 수 있습니다.
장치 삭제	NA 데이터베이스에서 장치를 영구적으로 삭제할 수 있습니다.
장치 구성 삭제	장치 구성을 제거할 수 있습니다.
장치 그룹 삭제	장치 그룹을 삭제할 수 있습니다.
진단 삭제	작업에 의해 캡처된 진단 데이터를 삭제할 수 있습니다. 로그에는 진단 데이터가 캡처된 방식이 기록됩니다.
드라이버 삭제	장치에 할당된 드라이버를 지울 수 있습니다.
이벤트 규칙 삭제	이벤트 알림 및 응답 규칙을 삭제할 수 있습니다.
세션 삭제	텔넷/SSH 세션 기록을 삭제할 수 있습니다.
소프트웨어 준수 삭제	소프트웨어 준수 레코드를 삭제할 수 있습니다.
소프트웨어 이미지 삭제	NA 소프트웨어 리포지토리에서 소프트웨어 이미지를 삭제할 수 있습니다.
소프트웨어 수준 삭제	구성된 소프트웨어 수준을 삭제할 수 있습니다. NA에는 소프트웨어 수준, 기본적으로 소프트웨어 버전과 일치하는 정규 표현식을 정의하는 기능이 있습니다. 해당 정규 표현식에 소프트웨어 수준을 할당할 수 있습니다. 소프트웨어 버전이 정규 표현식과 일치하는 모든 장치는 해당 수준으로 고려됩니다.
시스템 이벤트 삭제	시스템 이벤트를 삭제할 수 있습니다.
작업 삭제	작업을 삭제할 수 있습니다.

명령 권한	설명
원격 에이전트 배포	NA 원격 에이전트를 배포할 수 있습니다. NA 원격 에이전트에는 SNMP를 처리하며 NA 코어에서 NA 관리 엔진으로 조정되는 프로세스, 로컬 장치의 Syslog 알림을 처리하는 Syslog 프로세스 및 로컬 장치에 대한 TFTP 액세스를 가능하게 하는 TFTP 프로세스가 포함됩니다. 자세한 내용은 <i>NA 7.60 Satellite User's Guide</i> 를 참조하십시오.
소프트웨어 배포	단일 장치에 장치 소프트웨어를 배포하는 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
소프트웨어 배포(그룹)	장치 그룹에 장치 소프트웨어를 배포하는 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치 그룹에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
네트워크 장치 감지	IP 주소를 스캔할 수 있으며 NA 데이터베이스에 알 수 없는 장치를 자동으로 추가할 수 있습니다.
네트워크 장치 감지(그룹)	IP 주소를 스캔할 수 있으며 NA 데이터베이스에 알 수 없는 장치 그룹을 자동으로 추가할 수 있습니다.
장치 단일 사인온	텔넷/SSH 프록시를 통해 자동으로 장치에 연결할 수 있습니다.
장치 드라이버 검색	장치 드라이버를 검색할 수 있습니다. 이 명령에는 명령이 실행되는 장치에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
장치 드라이버 검색(그룹)	장치 드라이버 그룹을 검색할 수 있습니다. 이 명령에는 명령이 실행되는 장치 그룹에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
드라이버	드라이버 페이지를 볼 수 있습니다. 드라이버 페이지는 시스템에 설치된 드라이버 목록과 현재 사용 중인 드라이버 수를 표시합니다.
ACL 편집	ACL 스크립트를 편집할 수 있습니다.
ACL 설명 주석	ACL 설명을 편집할 수 있습니다.

명령 권한	설명
사용자[가 변경한] 구성 편집	장치 구성에 대해 사용자[가 변경]를 재설정할 수 있습니다. 이 권한은 관리 사용자 전용으로 설정되는 것이 좋습니다.
장치 편집	장치 그룹 구성원, 액세스 장치 설정 및 기타 속성을 변경할 수 있습니다. 이 명령에는 명령이 실행되는 장치에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
장치 그룹 편집	장치 그룹으로 장치 추가 및 장치 그룹에서 장치 제거를 포함하여 장치 그룹을 편집할 수 있습니다.
비활성 장치 편집	비활성 장치에 대해 설명 필드를 편집할 수 있습니다.
작업 편집	예약된 작업을 편집할 수 있습니다.
사용자 편집	사용자 프로필을 편집할 수 있습니다. 기본적으로 사용자는 자신의 사용자 프로필만을 편집할 수 있습니다.
전자 메일 보고서	다양한 보고서를 실행하는 작업을 예약할 수 있으며 지정된 수신자에게 전자 메일을 보낼 수 있습니다.
외부 인증 설정	ActiveDirectory, TACACS+, SecurID 및 RADIUS와 같은 외부 인증을 설정할 수 있습니다.
요약 보고서 생성	단일 장치에 대한 요약 보고서를 생성하는 작업을 예약할 수 있습니다.
요약 보고서 생성(그룹)	장치 그룹에 대한 요약 보고서를 생성하는 작업을 예약할 수 있습니다.
장치 및 암호 가져오기	장치 및 장치 인증 정보를 가져올 수 있습니다.
SysOID 나열	지원되는 장치의 sysOID를 나열할 수 있습니다.
보기 나열	보기 나열 페이지를 볼 수 있습니다. NA의 객체를 보기 내 특정 파티션으로 분리하는 하나 이상의 파티션에 대한 보기 집합입니다.
ACL 관리	ACL 삭제를 포함하여 장치 ACL을 관리할 수 있습니다.
명령 스크립트 관리	명령 스크립트를 생성, 수정 및 삭제할 수 있습니다.

명령 권한	설명
구성 정책 관리	구성 정책을 생성, 편집 및 삭제할 수 있습니다.
장치 암호 규칙 관리	장치 암호 규칙을 생성, 편집 및 삭제할 수 있습니다.
진단 스크립트 관리	진단 스크립트를 생성, 편집 및 삭제할 수 있습니다.
배포된 시스템 관리	배포된 모니터 결과 페이지, 배포된 오류 목록 페이지, 배포된 충돌 목록 페이지, 코어 나열 페이지 등을 비롯하여 분산 시스템 페이지를 볼 수 있습니다. 분산 시스템 환경 구성에 대한 자세한 내용은 <i>HP NA 7.60 Multimaster Distributed System on Oracle User's Guide</i> 를 참조하십시오.
이벤트 규칙 관리	이벤트 알림 및 응답 규칙을 생성, 편집 및 삭제할 수 있습니다.
게이트웨이 관리	게이트웨이 목록 페이지를 보고, 게이트웨이를 편집 및 삭제하며, NA 원격 에이전트를 배포할 수 있습니다. NA 원격 에이전트에는 SNMP를 처리하며 NA 코어에서 NA 관리 엔진으로 조정되는 프로세스, 로컬 장치의 Syslog 알림을 처리하는 Syslog 프로세스 및 로컬 장치에 대한 TFTP 액세스를 가능하게 하는 TFTP 프로세스가 포함됩니다.
IP 주소 관리	장치 IP 주소를 추가, 편집 및 삭제할 수 있습니다.
라이선스 관리	NA 라이선스 정보를 보고 업데이트할 수 있습니다.
파티션 관리	파티션을 추가, 편집 및 삭제할 수 있습니다.
소프트웨어 준수 관리	소프트웨어 준수 정보를 추가 및/또는 편집할 수 있습니다.
소프트웨어 이미지 관리	소프트웨어 이미지를 추가, 편집 및 삭제할 수 있습니다.
소프트웨어 수준 관리	소프트웨어 준수를 추가하고 편집할 수 있습니다.
시스템 보고서 관리	시스템 및 사용자 보고서 순서를 변경할 수 있으며 시스템 보고서를 삭제할 수 있습니다.
템플릿 관리	스크립트 템플릿을 생성, 편집 및 삭제할 수 있습니다.
사용자 관리	NA 사용자를 생성, 편집 및 삭제할 수 있습니다.

명령 권한	설명
사용자 그룹 관리	사용자 그룹을 생성, 편집 및 삭제할 수 있습니다. 사용자 권한은 이 인터페이스를 통해 관리되기 때문에 이 권한은 주의 깊게 부여되어야 합니다.
사용자 역할 관리	사용자 역할을 추가, 편집 및 삭제할 수 있습니다.
장치 구성 수정	장치에 편집한 구성을 배포하는 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
SecurID 수정	SecurID 토큰 정보를 수정할 수 있습니다.
멀티 태스킹 프로젝트	멀티 태스킹 프로젝트를 수정할 수 있습니다.
OS 분석	OS 분석 작업을 실행할 수 있습니다. OS 분석 작업 페이지에서는 sysoid(장치 모델의 고유 식별자), OS 버전, 플래시 저장 옵션, 모듈 등에 대한 정보와 같이 장치에 대한 데이터를 수집합니다. 이 정보는 소프트웨어 권장 사항을 생성하는 데 사용됩니다.
워크플로 승인 오버라이드	워크플로 승인 프로세스를 거치지 않고 작업을 실행할 수 있습니다.
장치 작업 다시 로드	드라이버에 제공된 다시 로드 스크립트를 통해 장치를 다시 로드(재부팅)할 수 있습니다. 이 명령에는 명령이 실행되는 장치에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
FQDN 확인	장치의 정규화된 도메인 이름을 확인하는 FQDN 확인 작업을 예약할 수 있습니다.
FQDN 확인(그룹)	장치 그룹의 정규화된 도메인 이름을 확인하는 FQDN 확인 작업을 예약할 수 있습니다.
명령 스크립트 실행	지정된 장치에서 스크립트를 실행하는 명령 스크립트 실행 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다. 또한 선택한 스크립트에 대한 스크립트 권한이 필요합니다.

명령 권한	설명
명령 스크립트 실행(그룹)	지정된 장치 그룹에서 스크립트를 실행하는 명령 스크립트 실행 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치 그룹에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다. 또한 선택한 스크립트에 대한 스크립트 권한이 필요합니다.
진단 스크립트 실행	지정된 장치에서 진단 스크립트를 실행하는 진단 실행 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
진단 스크립트 실행(그룹)	지정된 장치 그룹에서 진단 스크립트를 실행하는 진단 실행 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치 그룹에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
외부 응용 프로그램 실행	사용자 정의 외부 응용 프로그램을 실행할 수 있습니다. 이 권한은 주의 깊게 부여되어야 합니다.
ICMP 테스트 실행	장치에서 ICMP 테스트를 실행하는 ICMP 테스트 실행 작업을 예약할 수 있습니다.
ICMP 테스트 실행(그룹)	장치 그룹에서 ICMP 테스트를 실행하는 ICMP 테스트 실행 작업을 예약할 수 있습니다.
최고 작업 우선 순위 설정	작업의 우선 순위를 1로 설정할 수 있습니다.
시작 및 실행 동기화	대상으로 지정된 장치에 대해 시작 및 실행 구성을 동기화하는 시작 및 실행 동기화 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치에서 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
시작 및 실행 동기화(그룹)	대상으로 지정된 장치 그룹에 대해 시작 및 실행 구성을 동기화하는 시작 및 실행 동기화 작업을 예약할 수 있습니다. 이 명령에는 명령이 실행되는 장치 그룹의 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
스냅샷 작성	장치의 구성 스냅샷을 작성하는 스냅샷 작성 작업을 예약할 수 있습니다.

명령 권한	설명
스냅샷 작성(그룹)	장치의 구성 스냅샷을 작성하는 스냅샷 작성 작업을 예약할 수 있습니다.
텔넷/SSH 클라이언트	NA 프록시 서비스를 통해 텔넷 또는 SSH를 사용하는 장치에 액세스할 수 있습니다.
문제 해결	문제 해결 페이지에 액세스할 수 있고, 전자 메일을 통해 문제 해결 정보를 보낼 수 있으며, NA 서버의 로깅 수준을 변경할 수 있습니다.
장치 주석 업데이트	장치 설명을 변경할 수 있습니다.
장치 티켓 업데이트	Remedy와 같은 타사 티켓팅 시스템과 통신하도록 NA를 구성할 수 있습니다.
ACL 보기	ACL 스크립트를 볼 수 있습니다.
명령 스크립트 보기	명령 스크립트를 볼 수 있습니다.
구성 정책 및 준수 보기	구성 정책 및 준수 정보를 볼 수 있습니다.
구성 정책 이벤트 보기	구성 정책 이벤트 세부사항을 볼 수 있습니다. 이 명령에는 명령이 실행되는 장치의 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
배포된 소프트웨어 보기	소프트웨어 아카이브와 반대로, 배포된 소프트웨어를 볼 수 있습니다.
장치 구성 보기	장치 구성을 볼 수 있습니다. 암호 및 커뮤니티 문자열과 같은 중요 정보는 마스킹됩니다.
장치 진단 보기	장치 진단을 볼 수 있습니다.
장치 정보 보기	장치와 관련된 모든 정보(장치 구성 제외)를 볼 수 있습니다.
진단 스크립트 보기	진단 스크립트 세부사항을 볼 수 있습니다.
드라이버 보기	드라이버 세부사항을 볼 수 있습니다.
이벤트 규칙 보기	이벤트 규칙 목록을 볼 수 있습니다.

명령 권한	설명
전체 장치 구성 보기	마스킹 해제된 장치 구성을 볼 수 있습니다. 이 명령에는 명령이 실행되는 장치의 명령 권한 및 해당 장치 권한 수정이 모두 필요합니다.
스크립트 및 진단 결과 보기	명령 스크립트 또는 진단 작업의 결과 세부사항을 볼 수 있습니다.
SecurID 보기	SecurID 토큰 정보를 볼 수 있습니다.
세션 보기	텔넷/SSH 세션 명령 및 응답 이력을 볼 수 있습니다.
소프트웨어 이미지 아카이브 보기	NA 아카이브에 저장된 소프트웨어 이미지를 볼 수 있습니다.
작업 보기	작업 세부사항을 볼 수 있습니다.
템플릿 보기	스크립트 템플릿 세부사항을 볼 수 있습니다.
사용자 정보 보기	사용자 정보를 볼 수 있습니다.
워크플로 설정	워크플로 승인 규칙을 구성할 수 있습니다.

부록 C: 샘플 스크립트

이 부록에는 샘플 스크립트가 포함되어 있습니다.

샘플 PERL 스크립트 #1

이 PERL 스크립트에서는 Cisco 2600s 및 7200s에서 모든 FastEthernet 인터페이스를 전이중으로 설정합니다.

```
#
# Sample Script to set all FastEthernet interfaces
# to full duplex on Cisco 2600s and 7200s
#
use Socket;
$iaddr = gethostbyname("$tc_device_ip$");
$telnet_port = 23;
$sin = sockaddr_in($telnet_port, $iaddr);
socket(DEV, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
connect(DEV, $sin) || die "Can't connect to $tc_device_hostname$: $!\n";

sendln("");
sendln("$tc_device_password$");
sendln("en");
sendln("$tc_device_enable_password$");
sendln("conf t");

for $name (split(" ", "$tc_device_port_name_list$")) {
    if ($name =~ /FastEthernet/)
        sendln("interface $name");
        sendln("duplex full");
        sendln("exit");
    }
}
sendln("exit");
sendln("exit");
sendln("");
close(DEV);
exit;
```

(다음 페이지에 계속)

```
sub sendln {
  my ($line) = @_ ;
  $line .= "\n";
  syswrite(DEV,$line,length($line));
  while (<DEV>) {
    print;
    die "Failed to execute command\n"
      if (/\/% (Unknown|Unrecognized|Invalid|.*uthorization failed)/);
    last if (/name:/ ||
             /word:/ ||
             />/ ||
             /\#/);
  }
}
```

샘플 PERL 스크립트 #2

이 PERL 스크립트에서는 모든 인터페이스를 IP에서 전달되지 않은 브로드캐스트로 설정합니다.

```
#
# Sample Script to set all interfaces
# to no ip directed broadcast
#
use Socket;

$iaddr = gethostbyname("$tc_device_ip$");
$telnet_port = 23;
$sin = sockaddr_in($telnet_port, $iaddr);
socket(DEV, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
connect(DEV, $sin) || die "Can't connect to $tc_device_hostname$: $!\n";

sendln("");
sendln("$tc_device_password$");
sendln("en");
sendln("$tc_device_enable_password$");
sendln("conf t");

for $name (split(" ", "$tc_device_port_name_list$")) {
    sendln("interface $name");
    sendln("no ip directed-broadcast");
    sendln("exit");
}
sendln("exit");
sendln("exit");
sendln("");
close(DEV);
exit;

sub sendln {
    my ($line) = @_;
    $line .= "\n";
    syswrite(DEV,$line,length($line));
    while (<DEV>) {
        print;
        die "Failed to execute command\n"
            if (/\/% (Unknown|Unrecognized|Invalid|.*uthorization failed)/);
        last if (/name:/ ||
                /word:/ ||
                />/ ||
                /\#/);
    }
}
```

샘플 Expect 스크립트

이 Expect 스크립트에서는 배너가 문자열을 포함하고 있지 않는 경우에만 지정된 문자열이 포함되도록 배너를 수정합니다.

```
#
# Sample Script to set the banner only if
# it is not already set correctly
#
spawn telnet $tc_device_ip$
set banner "****Unauthorized Access Prohibited****"
expect {
    $banner {
        puts "\nBanner is already set correctly\n"
        exit 0
    } "word:"
}
send "$tc_device_password$\r"
expect ">"
send "en\r"
expect "word:"
send "$tc_device_enable_password$\r"
expect "\#"
send "config t\r"
expect "\#"
send "banner motd /$banner/\r"
expect "\#"
send "exit"
```

용어집

이 용어집에는 HP Network Automation(NA) 용어에 대한 정의가 포함되어 있습니다. 용어는 알파벳순으로 나열됩니다.

용어	정의
게이트웨이	다른 게이트웨이로 IP 트래픽을 라우트하는 응용 프로그램입니다. NAT 장치 및 방화벽 뒤에 있는 서버를 관리할 수 있는 게이트웨이 소프트웨어. 또한 게이트웨이는 영역 간 터널에서 대역폭 제한을 지원하며 SSL 프록시 또는 TCP 포트 전달이 사용되는 곳에서 사용될 수 있습니다. 터널은 인증될 수 있으며 SSL을 사용하여 선택적으로 암호화될 수 있습니다.
규칙	다음 중 적어도 하나 이상을 검증하는 자동화된 테스트 <ul style="list-style-type: none">• 특정 구성 설정• 특정 데이터 모델 요소• 장치의 런타임 상태(일명 진단)• 장치에서 실행 중인 소프트웨어 버전
규칙 예외	규칙 예외도 규칙의 일부입니다. 하지만 규칙 예외는 장치 구성에서 일치하는 텍스트를 텍스트가 속한 규칙의 고려 대상에서 제외하는 것을 목적으로 합니다.
기본 사이트 파티션	기본 파티션의 이름은 기본 사이트입니다. NA를 처음 사용하는 경우 파티션만 기본 파티션으로 사용할 수 있습니다. 현재 NA에서 관리되는 모든 장치가 포함됩니다.

용어	정의
다중 마스터	모든 데이터의 전체 집합을 포함하는 데이터베이스가 두 개 이상 있는 시스템입니다.
단일 검색	단일 검색 옵션을 사용하면 단일 검색 결과 페이지에서 지정한 검색 기준을 포함하는 모든 이벤트를 검색할 수 있습니다.
단일 보기	단일 보기를 통해 하나의 페이지에서 모든 해당 장치 또는 단일 장치의 변경 사항을 표시하는 이벤트를 추적할 수 있습니다.
멀티 태스킹 프로젝트	멀티 태스킹 프로젝트는 단일 프로젝트 아래에 순서대로 함께 조인된 여러 다른 작업을 실행할 수 있습니다. 멀티 태스킹 프로젝트에 포함된 각 작업은 지정한 순서대로 실행됩니다.
분산 시스템	별도의 서버에서 각각 실행되는 코어가 두 개 이상 있는 시스템입니다.
사용자 그룹	사용자 관리 목적을 위한 논리적 컨테이너. 시스템 관리자는 사용자를 사용자 그룹에 할당하고, 사용자 그룹을 특정 역할에 매핑할 수 있습니다.
사용자 보기	사용자 및 사용자 그룹에 적용되는 보기
상위 그룹	NA의 장치 그룹 계층은 상위 그룹 및 리프 그룹으로 구성됩니다. 상위 그룹에는 상위 항목이 하나만 포함될 수 있습니다. 상위 그룹은 장치가 아닌 장치 그룹만 포함할 수 있습니다.
역할	역할을 사용하여 사용자를 동일한 보안 권한을 공유하는 그룹으로 나눕니다. 역할에 할당된 사용자에게는 역할별로 정의된 권한이 허가됩니다. 예를 들어, 사용자에게 장치 추가, 구성 정책 관리 또는 소프트웨어 배포와 같은 특정 운영을 수행할 수 있는 권한이 부여된 경우 NA는 리소스에 액세스할 고정 역할 ID를 사용합니다.

용어	정의
영역	네트워크 세그먼트. 일반적으로 영역은 고유한 IP 주소 집합으로 식별됩니다. 예를 들어 영역에는 10.255.111.128로 번호가 매겨진 두 개의 장치가 포함될 수 없습니다. 대신 장치는 별도의 영역으로 분리되어야 합니다. 사이트는 관리하는 NA 코어와 동일한 영역에 있지 않아도 됩니다.
워크플로	NA 워크플로 통합 및 라우팅 엔진(WIRE)은 네트워크 구성 프로세스를 관리하여, 네트워크 변경 내용이 미리 정의된 정책에 따라 올바른 순서로 완료되고 담당자에 의해 승인되도록 합니다.
작업	NA가 네트워크와 인터랙션하는 기본 메커니즘. 작업은 예약하거나 즉시 실행할 수 있는 특정 작업입니다(예: 암호 배포, 장치 다시 로드 및 작업 스냅샷).
작업 풀 초기화	NA 관리 엔진이 시작되면 엔진이 데이터베이스를 쿼리하여 작업 풀을 구성합니다. 작업이 생성, 업데이트 또는 삭제되는 경우 NA는 로컬 NA 코어에 연결된 데이터베이스만 업데이트합니다. 데이터베이스 복제 메커니즘은 원격 NA 코어에 연결된 데이터베이스의 필수 변경 사항을 처리합니다. 하지만 원격 NA 코어를 호출하여 메모리에 있는 작업 풀을 업데이트하는 일은 응용 프로그램이 담당합니다.
장치 보기	장치 및 장치 그룹에 적용되는 보기.
장치 암호 규칙	장치 그룹, IP 주소 범위 또는 호스트 이름에 동일한 사용자 이름, 암호 및 SNMP 커뮤니티 문자열을 적용할 수 있습니다.
정책	장치 구성 및 런타임 상태를 테스트하는 규칙 모음
진단	구성 파일에 캡처되지 않는 장치에 대한 정보를 수집하기 위해 장치에서 실행되는 명령어. 예를 들어, Cisco 라우터에서 진단은 NTP 상태 표시 명령의 출력을 나타냅니다.

용어	정의
코어	단일 NA 관리 엔진, 연관된 서비스(Syslog 및 TFTP) 및 단일 데이터베이스. 코어는 여러 사이트(장치 집합)를 관리할 수 있습니다.
파티션	파티션은 NA 객체의 집합입니다. NA 객체에는 장치, 사용자, 명령 스크립트, 장치 암호 규칙, 정책, 소프트웨어 이미지 등이 포함됩니다. 파티션은 또한 권한 모델, 그룹 계층, NA 코어의 장치 분산 및 네트워크 다이어그램과 함께 사용할 수 있습니다.

색인

가

- 가져오기 페이지 421
- 검색 212
 - 고급 674
 - 모듈 597
 - 인터페이스 593
 - 작업 622
 - 장치 변경 사항 671
 - 정책 601
 - 정책, 규칙 및 준수 605
 - 홈 페이지에서 354
- 게이트웨이
 - 목록 198
 - 설치 198
 - 위성 198
 - 코어 198
- 게이트웨이 메시지
 - 관리 포트 64
 - 구성 195
 - 지연 64
- 게이트웨이 목록 198
- 결과 세부사항 포함 615, 629, 640
- 계층 레이어 144, 765
- 고객 지원 센터 34
- 고급 검색 674
- 고급 권한 페이지 335
- 고급 스크립팅 72, 74, 724
- 관리 상태
 - 비활성 168
 - 사전 프로덕션 168
 - 새 장치 마법사 165
 - 활성 168
- 관리 설정 구성
 - 개요 41
 - 구성 관리 42
 - 보고 90
 - 부팅 감지 50
 - 사용자 인터페이스 80
 - 서버 67
 - 서버 모니터링 110
- 워크플로 77
- 장치 액세스 55
- 텔넷/SSH 85
- 관리 엔진 123
- 관리되는 IP 주소 편집 305
- 구성
 - 검색 610
 - 관리 222
 - 변경 감지 43
 - 변경 사항 223
 - 비교 231
 - 생성 512
 - 세부사항 227
 - 스냅샷 54
 - 시작 46
 - 실행 중인 구성에 배포 228
 - 정리 71
 - 정책 514
 - 정책 확인 47
 - 텍스트 검색 610
 - 편집 230
- 구성 검색 페이지 610
- 구성 관리 페이지 43
- 구성 규칙 예외
 - 개요 529
 - 추가 529
- 구성 규칙 예외 페이지 530
- 구성 작업 배포 페이지 234
- 구성 정책 가져오기 524
- 구성 정책 내보내기 524
- 구성 정책 생성 511
- 구성 정책 편집 페이지 557
- 구성 정책 활동 페이지 532
- 구성 준수 테스트 545
- 구성 준수 테스트 페이지 545
- 구성 템플릿 보기 페이지 708
- 구성 템플릿 페이지 703
- 구성 파일 구문 분석 227
- 구성 편집 및 배포 304
- 권한
 - 명령 337, 917
 - 보기 334
 - 사용자 339
 - 설정 337

- 스크립트 334, 337
 - 장치 보기 337
 - 장치 수정 334, 337
 - NA/SA 통합 255
- 규칙 예외 522
- 규칙 정의 172
- 규칙 조건 521
- 그룹
 - 동적 180
 - 리프 175
 - 상위 175
 - 하위 175
- 그룹 편집 페이지 207
- 기본 IP 주소 70
- 기본 VLAN ID 272

나

- 내 기본 설정 페이지 341
- 내 설정
 - 권한 338
 - 빠른 시작 338
 - 암호 338
 - 작업 공간 338
 - 프로필 338
 - 환경 설정 338
- 내 작업 공간 페이지 341
- 내 작업 페이지 491
- 내 프로필 페이지 339
- 네트워크 상태 보고서
 - 개요 748
 - 모범 사례 748
 - 모범 사례 상태 750
 - 보고서 필드 748
 - 세부사항 751
 - 이벤트 748
 - 장치 상태 748
- 네트워크 장치 감지
 - 개요 426
 - 설정 59
 - CIDR 범위 430
 - IP 주소 범위 429, 430

다

- 다시 로드
 - 드라이버 123
 - 컨텐츠 123
- 다이어그램 작성
 - 가장자리 길이 95
 - 그래프 범례 768
 - 라우트 765
 - 레이블 글꼴 크기 95
 - 색상 758
 - 아이콘 758
 - 압축성 95
 - 유형 764
 - 장치 주석 767
 - 최대 기간 95
 - 최대 노드 95
 - 출력 형식 764
 - 품질-시간 비율 95
 - 흡 765
- 단순 스크립팅 720
- 단일 검색 671
- 단일 보기
 - 개요 680
 - 관리 설정 94
 - 목록 보기 262
 - 추적할 이벤트 94
 - 추적할 진단 94
 - 페이지 681, 776, 778, 780
- 단일 사인온 87, 88, 788
- 데이터 정리 페이지 478
- 데이터베이스
 - 정리 71
- 도움말
 - 명령줄 31, 915
 - HTML 파일 31
- 도움말 메뉴
 - 문서 29
 - 지원 29
 - HP Live Network 29
 - HP Network Automation 정보 29
- 동기 작업 504, 867
- 동적 장치 그룹
 - 개요 180
 - 계산 182

생성 180
 장치 변경 이벤트 73
 재계산 73
 드라이버
 검색 139, 147, 212, 423
 다시 로드 131
 목록 139, 147, 555
 보기 131
 실행 131
 확장 디렉터리 74
 드라이버 검색 페이지 234, 375, 433
 드라이버 다시 로드 131

라

라이선스
 경고 임계값 113
 모니터 121
 라이선스 정보 보기 페이지 36
 래퍼 로그 35
 로그인한 사용자 페이지 321
 로그인 페이지
 배너 84
 사용자 지정 84
 실패 103
 로깅
 관리 129
 명령 86
 서버 129
 세션 127
 수준 125
 응답 86
 이름 126
 작업 128
 로컬 영역
 개요 193
 베이스 호스트 액세스 194
 추가 194
 콘솔 액세스 193
 NAT 액세스 193
 리프 그룹 175

마

멀티 태스킹 프로젝트

구성 489
 예약 485
 옵션 487
 멀티 태스킹 프로젝트 페이지 487
 메뉴
 보기 261
 연결 157, 316
 편집 157, 304
 프로비전 157, 314
 메모리
 순 413, 556
 여유 413, 556
 총 수 413, 556
 명령
 입력 31, 915
 정의 920
 명령 권한
 목록 918
 사용자 그룹 332
 사용자 역할 917
 정의 920
 허가 917
 명령 스크립트
 고급 713
 목록 391
 실행 389, 738
 자동 수정 523
 추가 및 편집 720
 Expect로 변환 720
 Perl로 변환 720
 Pull 변수 버튼 724, 725
 명령 스크립트 실행
 대기 옵션 392
 배포 옵션 392
 명령 스크립트 실행 작업 389
 명령 창 31, 915
 모니터
 보기 117
 상태 117
 설명 118
 모듈 검색 페이지 597
 모든 사용자 페이지 320
 모범 사례
 구성 변경 사항 750

- 소프트웨어 수준 위반 750
 - 시작과 구성 불일치 750
 - 장치 액세스 실패 750
 - 정책 규칙 위반 750
 - 모범 사례 보고서
 - 개요 752
 - 보고서 필드 752
 - 문서
 - 릴리스 노트 31
 - 사용 설명서 31
 - 업그레이드 및 설치 설명서 31
 - 온라인 도움말 31
 - CLI 도움말 31, 915
 - 문제 해결
 - 드라이버 검색 실패 894
 - 로깅 수준 130
 - 세션 로그 897
 - 스냅샷 실패 895
 - 이벤트 로깅 130
 - FAQ 801, 893
 - Syslog 895
 - 문제 해결 다운로드 페이지 35
 - 문제 해결 페이지 130, 131
- ## 바
- 방화벽 55, 256
 - 배스천 호스트
 - 개요 218
 - 구성 59, 210
 - 암호 309
 - 정의 307
 - 배포
 - 시작 구성에 228, 233
 - 실행 중인 구성에 228, 233
 - 배포 단계 292
 - 배포 테이블 414, 418
 - 변경 감지
 - 간격 43
 - 개요 51
 - 구성 스냅샷 43
 - 사용 43
 - 변수
 - 모든 이벤트 579
 - 장치 구성 이벤트 578
 - 장치 액세스 141, 149
 - 장치 컨텍스트 450
 - 보고
 - 개요 90
 - 구성 변경 92
 - 구성 불일치 92
 - 다이어그램 작성 95
 - 소프트웨어 준수 91
 - 장치 액세스 실패 92
 - 전자 메일 보고서 93, 94
 - 정책 규칙 위반 91
 - 보고 페이지 91
 - 보고서
 - 네트워크 상태 748
 - 다이어그램 작성 763
 - 모범 사례 752
 - 사용자 744
 - 소프트웨어 수준 772
 - 소프트웨어 취약점 774
 - 소프트웨어 취약점 세부사항 780
 - 시스템 744
 - 이미지 동기화 776
 - 장치 상태 755
 - 장치 소프트웨어 770
 - 중복 IP 주소 746
 - 통계 353, 757
 - NA 이벤트 778
 - 보기
 - 드라이버 목록 36
 - 라이선스 정보 36
 - 보류 중 작업 495
 - 소프트웨어 이미지 권장 사항 293
 - 시스템 구성 36
 - 실행 중인 작업 498
 - 작업 로드 506
 - 장치 관계 265
 - 장치 그룹 186, 245
 - 장치 정보 249
 - 최근 작업 361, 500, 503, 867
 - 파티션 세부사항 206
 - 보기 권한 페이지 343
 - 보기 메뉴 261
 - 보류 중 작업 495
 - 보안

- 세션 시간 초과 80
 - 스크립팅 확인 81
 - 자동 완성 기능 80
 - 장치 보기 80
 - 정책 97
 - 보안 경고 서비스 518, 540
 - 보조 IP 유형 44
 - 부울 검색
 - 구성 텍스트 587, 612
 - 인터페이스 593
 - 장치 589, 599, 612
 - 부팅 감지 50
 - 분산 시스템
 - 코어 138, 457
 - 파티션 138, 457
 - 비활성 노드 427
 - 빠른 시작
 - 개요 345
 - 관리 346
 - 구성 345
 - 설정 345
 - 추가 363
- 사**
- 사용자
 - 고급 권한 330
 - 보기 권한 334
 - 암호 323
 - 역할 319, 335
 - 작업 공간 341
 - 장치 수정 권한 333
 - 전자 메일 주소 320
 - 프로필 339
 - 현재 로그인됨 320
 - 환경 설정 341
 - 사용자 검색 결과 페이지 320
 - 사용자 검색 페이지 648
 - 사용자 그룹 추가 330
 - 사용자 그룹 페이지 330
 - 사용자 보고서 744
 - 사용자 역할 319, 917
 - 사용자 유형
 - 관리자 324
 - 전체 액세스 324
 - 제한된 액세스 324
 - 파워 324
 - 사용자 인터페이스 페이지
 - 개요 80
 - 구성 비교 81
 - 메뉴 사용자 지정 81
 - 보안 80
 - 소프트웨어 81
 - 스크립트 82
 - 확장된 사용자 지정 필드 82
 - 사용자 자동 생성 44
 - 사용자 지정 데이터
 - 모듈 695
 - 사용자 696, 697
 - 인터페이스 695
 - 장치 694
 - 장치 그룹 696
 - 진단 694
 - 추가 693
 - 텔넷/SSH 세션 697
 - 확장된 필드 82
 - 사용자 지정 데이터 설정 페이지 694, 699
 - 사용자 지정 로그인 페이지 84
 - 사용자 지정 IP 주소 310
 - 사용자 추가 319
 - 사용자 특성 세부사항 페이지 53
 - 사용자 편집 페이지 323
 - 사전 작업 스냅샷 47, 235, 393, 410, 890
 - 사후 작업 스냅샷 47, 235, 393, 410, 890
 - 상위 그룹 175
 - 상태
 - 네트워크 748
 - 시스템 117
 - 작업 297, 504, 867
 - 새 구성 규칙 예외 페이지 530
 - 새 구성 정책 페이지 514
 - 새 구성 템플릿 페이지 706
 - 새 규칙 페이지 518
 - 새 메시지 페이지 306
 - 새 명령 스크립트 페이지 722
 - 새 사용자 그룹 페이지 331
 - 새 사용자 역할 페이지 337

- 새 사용자 지정 데이터 필드 설정 페이지 700
- 새 사용자 페이지 323
- 새 상위 그룹 페이지 178
- 새 소프트웨어 수준 추가
 - 소프트웨어 수준 추가 페이지 537
 - 이미지 그룹화 537
- 새 장치 그룹 페이지 177
- 새 장치 마법사
 - 구성 166
 - 인증 166
 - 장치 생성 165
- 새 장치 템플릿 페이지 161
- 새 장치 페이지 138
- 새 전자 메일 및 이벤트 규칙 페이지 571
- 새 정책 페이지 514
- 새 준수 추가
 - 이미지 그룹화 557
 - 준수 추가 페이지 557
- 새 진단 페이지 686
- 새 파티션 페이지 203
- 새 IP 주소 페이지 313
- 새 SecurID 토큰 페이지 793
- 새로 고침 간격 82, 297, 498
- 샘플 스크립트 931
- 서버 로그 129
- 서버 모니터링
 - 개요 110
 - 구성 113
 - 페이지 필드 111
- 서버 모니터링 페이지 111, 115
- 서버 인터페이스 292
- 서버 자동화 255, 276, 292
- 서버 페이지 68, 292
- 서브넷의 인터페이스 페이지 273
- 서비스
 - 시작 123
 - 중지 123
- 서비스 시작/중지
 - 관리 엔진 123
 - 소프트웨어 이미지 서버 124
 - FTP 서버 124
 - HP Live Network 123
 - Syslog 서버 124
 - TFTP 서버 124
- 서비스 유형 50, 211, 252, 588, 669
- 설치
 - 게이트웨이 194
- 설치 마법사 107
- 성능 조정 74
- 세션 검색 페이지 631
- 세션 로그
 - 저장 372, 376, 380, 385
 - 텔넷/SSH 85
- 세션 시간 초과 80
- 셀 인터페이스
 - 개요 216
 - 제어 문자 216
- 소프트웨어
 - 배포 319, 556
 - 배포 테이블 414
 - 버전 586, 770
 - 소프트웨어 수준 편집 537
 - 수준 772
 - 수준 위반 518
 - 준수 위반 91
 - 준수 편집 543, 557
 - 취약점 518, 774
 - SecurID 토큰 라이선스 340
- 소프트웨어 리포지토리 296
- 소프트웨어 배포
 - 개요 556
 - 이미지 집합 요구 사항 554
- 소프트웨어 버전 36
- 소프트웨어 센터
 - 소프트웨어 배포 549
 - 이미지 집합 551
- 소프트웨어 수준
 - 정의 543
 - 추가 537
 - 편집 537
- 소프트웨어 수준 보고서 772
- 소프트웨어 수준 편집 페이지 543
- 소프트웨어 이미지 관리
 - 서버 설정 74
 - 서비스 포트 74
 - 서비스 호스트 74
 - 소프트웨어 이미지 권장 사항 262, 293, 295

- 이미지 권장 사항 설정 342
- 이미지 동기화 보고서 776
- 자격 증명 유형 344
- 프록시 서버 74
- 소프트웨어 이미지 백업 459
- Cisco.com 344
- Cisco.com에서 이미지 다운로드 작업 페이지 456
- 소프트웨어 이미지 집합 페이지 553
- 소프트웨어 이미지 페이지 551
- 소프트웨어 이미지 편집 페이지
 - 이미지 이름 553, 555
 - 이미지 집합 요구 사항 553, 555
 - MD5 체크섬 553, 555
- 소프트웨어 준수 페이지 540
- 소프트웨어 취약점 보고서 774
- 소프트웨어 취약점 세부사항 780
- 솔루션 링크 516, 528, 539, 544
- 스냅샷
 - 검사점 404
 - 검색 중 143
 - 구성 54
 - 사용 43
 - 사전 작업 및 사후 작업 47
 - 실패함 770
 - 인벤토리 113
- 스냅샷 구성 235, 393, 410, 890
- 스냅샷 작업 페이지 403
- 스캔 방식
 - NMAP 427, 430
 - SNMP 427, 430
- 스크립트
 - 권한 334
 - 내보내기 719
 - 언어 72, 74
 - 자동 수정 523, 726
 - 추가 및 편집 720
 - Bare metal 프로비전 714
- 스크립트 가져오기/내보내기 페이지 719
- 스크립트로 변환 옵션 86
- 스택 추적 83
- 승인 요청 863
- 승인 요청 페이지 863
- 시스템
 - 보고서 744
 - 성능 74
 - 시스템 구성 보기 페이지 37
 - 시스템 및 네트워크 이벤트 보고서 778
 - 시스템 상태
 - 개요 117
 - 마지막 확인 117
 - 시스템 상태 페이지 117, 118
 - 시스템 성능
 - 마스킹 구성 75
 - 세션 로그 75, 127
 - 실행 중인 작업 75
 - 이벤트 제한 74
 - 조정 옵션 74
 - LogMonitor 설정 112
 - NA 코어 76
 - SNMP 스캐너 스레드 58
 - 시작 날짜 466
 - 시작 동기화 페이지 408
 - 실행 중인 작업 364
- 아
 - 아이콘 758
 - 암호
 - 규칙 139, 170
 - 네트워크 전체 규칙 139, 147
 - 로컬 인증 344
 - 변경 사항 784
 - 보안 102
 - 선택 56
 - 옵션 323, 339
 - 외부 자격 증명 344
 - 장치별 140, 148
 - 장치에 연결 56
 - 재설정 210
 - 제한 102
 - 편집 171
 - AAA 325
 - NA 사용자 173
 - 암호 구성
 - 만료 326, 328
 - 사용자 시나리오 326
 - 재사용 326
 - 암호 변경 페이지 344

- 암호 시도 57
- 암호 코드 60
- 액세스 변수 141, 149
- 액세스 설정 141, 149
- 역할 319, 704
- 연결 메뉴 316
- 연결 방법
 - 콘솔 서버 142, 150
 - 텔넷 57, 142, 150
 - FTP 57
 - Rlogin 57, 142, 150
 - SCP 57
 - SNMP 57, 142, 150
 - SSH 57, 142, 150
 - TFTP 57
- 영역 191
- 오버랩되는 IP 네트워크
 - 개요 194
 - 게이트웨이 설치 194
 - 영역 194
 - NA 코어 194
- 와일드카드 216
- 외부 리소스 자격 증명 339
- 외부 응용 프로그램 실행 481
- 외부 인증
 - 설치 마법사 107
 - 장애 조치 설정 325
 - HP OO 101
 - LDAP 97, 106
 - RADIUS 100, 103
 - SA 101
 - SecurID 97
 - TACACS+ 97
- 외부 인증 페이지 102
- 요약 보고서 782
- 요약 보고서 생성 페이지 466
- 우선 순위
 - 변경 499
 - 작업 대기열 359
 - 작업 예약 359, 499
- 워크플로
 - 개요 855
 - 관리 설정 77
 - 마법사 856
- 사용 77
- 승인 요청 863
- 승인자 855
- 실행 중인 작업 78
- 우선 순위 값 78
- 이벤트 규칙 78
- 작업 승인 866
- 작업 유형 493, 861
- 작업 표시 860
- 주관자 855
- 참고 수신자 855
- 프로젝트 855
- 위성 게이트웨이 196
- 위험도 높음(빨강) 이벤트 751, 754, 756
- 이미지 동기화 보고서 776
- 이미지 집합 548, 776
- 이미지 페이지
 - 드라이버 필요 551
 - 생성 날짜 551
 - 이미지 집합 551
 - 체크섬 551
 - 추가한 사람 551
 - 파일 이름 551
- 이벤트
 - 보고서 778
 - 설명 640
- 이벤트 검색 결과 페이지 681, 776, 778, 780
- 이벤트 검색 페이지 636, 671
- 이벤트 규칙 검색 결과 페이지 570
- 이벤트 변수
 - 구성 578
 - 장치 577
 - 진단 577
- 이벤트 설명 640
- 이벤트 세부사항 변경
 - 날짜 53
 - 사용자 53
 - 장치 인터랙션 53
- 이벤트 알림 규칙 563
- 이중 데이터 수집 264
- 이중 불일치 데이터 269, 272
- 인벤토리 페이지 241
- 인증

- 사용자 암호 102
- 외부 103, 339
- 장애 조치 339
- Twist 서버 104
- 인증 장애 조치 98
- 인터페이스
 - 검색 593
 - 서브넷 268, 273
 - 세부사항 261
 - 세부사항 보기 596
 - 속도 269, 272
 - 이중 불일치 269, 272
 - 편집 593
- 인터페이스 검색 결과 페이지 596
- 인터페이스 검색 페이지 593
- 인터페이스 세부사항 페이지 268, 269, 273
- 인터페이스 편집 세부사항 페이지 271
- 임시 장치 그룹
 - 생성 358
 - 작업 실행 358
- 자**
- 자격 증명
 - 로그인 102
 - 작업별 65
 - AAA 65
- 자격 증명 유형 344
- 자동 수정
 - 샘플 스크립트 729
 - 스크립트 523
 - 스크립트 구문 726
 - 스크립트 변수 727
 - 스크립트 생성 726
 - 스크립트 실행 47
- 자동 완성 기능 80
- 자문 링크 516, 528, 539, 544
- 작업
 - 가져오기 421
 - 개요 358
 - 내 작업 페이지 492
 - 네트워크 장치 감지 426
 - 데이터 정리 478
 - 동기 504, 867
 - 드라이버 검색 375
 - 드래프트 463
 - 라운드 로빈 알고리즘 360
 - 로깅 457, 461, 480
 - 명령 스크립트 실행 389
 - 상태 504, 867
 - 새로 고침 간격 82, 297, 498
 - 스냅샷 작성 403
 - 승인 옵션 463
 - 시작 동기화 408
 - 실행 498
 - 암호 배포 370
 - 예약 237, 369, 374, 378
 - 옵션 367, 380, 437, 441, 460
 - 외부 응용 프로그램 실행 481
 - 요약 보고서 생성 466
 - 원격 에이전트 배포 472
 - 자격 증명 61, 62
 - 장치 소프트웨어 백업 459
 - 장치 소프트웨어 업데이트 413
 - 장치 재부팅 379
 - 장치 컨텍스트 448
 - 장치 프로비전 444
 - 재시도 수 464
 - 전자 메일 보고서 469
 - 정보 504, 867
 - 정책 준수 확인 462
 - 중복 방지 433
 - 진단 실행 397
 - 최근 361, 500, 503, 867
 - 추산 기간 234, 367
 - 포트 스캔 440
 - ACL 삭제 888
 - Cisco.com에서 이미지 다운로드 456
 - FQDN 확인 475
 - ICMP 테스트 실행 383
 - OS 분석 436
 - Syslog 구성 366
 - VLAN 452
 - 작업 검색 622
 - 작업 검색 페이지 622
 - 작업 대기열 359
 - 작업 로그 35, 128
 - 작업 로드 506

- 작업 상태
 - 건너뛸 504, 867
 - 경고 297, 504, 867
 - 대기 중 504, 867
 - 동기 504, 867
 - 성공함 504, 867
 - 실패함 297, 504, 867
 - 실행 499
- 작업 승인 866
- 작업 실행 중 페이지 498
- 작업 예약
 - 개요 359
 - 우선 순위 수준 359
- 작업 우선 순위 367, 375, 376, 436, 441
- 작업 정보 페이지 503, 866
- 작업 템플릿
 - 검색 623
 - 삭제 363
 - 생성 361
 - 실행 363
- 작업 풀
 - 설명 360
 - 초기화 360
 - 캐싱 360
- 잘못된 포트 개수 259
- 장치
 - 가져오기 167, 421
 - 관리되는 IP 주소 261
 - 그룹 179, 187
 - 상태 749
 - 서버 261
 - 세부사항 261
 - 암호 규칙 170
 - 액세스 변수 141, 149
 - 액세스 설정 141, 149
 - 액세스 실패 750
 - 연결 방법 56
 - 영역 191
 - 이벤트 변수 577
 - 인터페이스 267, 273
 - 임시 그룹 358
 - 자격 증명 431
 - 정보 페이지 249
 - 추가 138
 - 파티셔닝 191
 - IP 주소 261, 770
 - 장치 가동 시간 586
 - 장치 가져오기 69, 167, 421
 - 장치 검색 결과 페이지 590
 - 장치 관계
 - 보기 299
 - 보기 메뉴 265
 - 상위 및 하위 장치 300
 - 컨텍스트 관리 299
 - 피어 장치 300
 - 장치 관리
 - 개요 241
 - 그룹 보기 244
 - 장치 관찰 옵션 228, 251
 - 장치 구성 223
 - 장치 구성 비교 페이지 231
 - 장치 구성 세부사항 페이지 227
 - 장치 그룹 세부사항 페이지 188
 - 장치 그룹 페이지 179, 187, 244
 - 장치 그룹 편집 207
 - 장치 드라이버
 - 가져오기 212
 - 검색 212
 - 장치 드라이버 검색 212
 - 장치 목록 새로 고침 버튼 457
 - 장치 변경 이벤트 73
 - 장치 변수 136, 521
 - 장치 블레이드/모듈 페이지 280, 282, 283, 285, 287, 288, 289, 290, 292, 295
 - 장치 상태 보고서
 - 개요 755
 - 보고서 필드 755
 - 세부사항 756
 - 장치 선택기
 - 개요 183
 - 버튼 184
 - 장치 선택 183
 - 장치 제거 183
 - 크기 조정 185
 - 장치 세부사항
 - 모듈 289

- 서버 292
- 이벤트 266
- 인터페이스 267
- 작업 297
- 정책 290
- 텔넷/SSH 세션 303
- IP 주소 274
- MAC 주소 276
- 장치 세분화
 - 영역 191
 - 파티션 191
- 장치 세션 페이지 303
- 장치 소프트웨어 보고서 770
- 장치 소프트웨어 업데이트 페이지 413
- 장치 소프트웨어 이력 페이지 301
- 장치 암호 규칙 페이지 171
- 장치 액세스 페이지 56
- 장치 연결 방법 309, 312
- 장치 예약 246
 - 개요 246
 - 구성 78
 - 텔넷 프록시 사용 79
 - 활동 캘린더 247
 - SSH 프록시 사용 79
- 장치 이벤트 페이지 266
- 장치 인터페이스 페이지 267, 269, 271, 273
- 장치 일괄 편집 페이지 209
- 장치 자격 증명 옵션 235, 367, 376, 405, 889
- 장치 작업 페이지 297
- 장치 재부팅 페이지 379
- 장치 정책 페이지 262
- 장치 추가 137
- 장치 컨텍스트 추가 작업 페이지 448
- 장치 컨텍스트 페이지 300
- 장치 템플릿
 - 개요 668
 - 검색 668
 - 검색 결과 670
- 장치 템플릿 검색 페이지 668
- 장치 편집 페이지 146
- 장치 프로비전 작업 페이지 444
- 장치 IP 주소 페이지 274, 307
- 장치 MAC 주소 페이지 276
- 장치 VLAN 페이지 280
- 장치가 로드된 소프트웨어 페이지 300, 301
- 장치에서 관리되는 IP 주소 페이지 307
- 재설정
 - 기본 로깅 수준 130
 - 마지막으로 사용한 암호 210
- 재할당
 - 정규 표현식 패턴 70
 - IP 주소 70
- 적용된 정책 531
- 전송 프로토콜
 - FTP 142
 - SCP 142
 - SFTP 142
 - TFTP 142
- 전자 메일
 - 링크 93
 - 보내기 322
 - 서버 주소 93
 - 읽기 322
 - 작업 결과 93
 - 형식 93, 470
 - 회신 323
- 전자 메일 보고서 94
- 전자 메일 보고서 페이지 469
- 정규 표현식 521
 - 인터페이스 이름 70
 - 패턴 70
- 정책
 - 개요 601, 605
 - 검색 결과 604, 608
 - 규칙 검색 605
 - 규칙 정의 521
 - 범위 526
 - 생성 514
 - 위반 검색 601
 - 일괄 편집 512
 - 준수 검색 605
 - 준수하지 않는 장치 585
- 정책 가져오기/내보내기 페이지 524, 719, 726, 727
- 정책 검색 페이지 601
- 정책 관리자

개요 509
 규칙 510
 위험 등급 509
 적용된 정책 보기 531
 정규 표현식 511
 정책 생성 511
 정책 준수 510
 정책 테스트 546
 준수 585
 준수 테스트 545
 준수되지 않음 536
 중요도 572
 정책 규칙 위반 751
 정책 준수 페이지 534
 정책 태그 603, 607
 정책 테스트 페이지 546
 정책 페이지 512
 정책 편집 페이지 525
 정책 필드 516
 준수
 추가 557
 편집 543, 557
 준수 검색 페이지 606
 준수 센터
 개요 803
 COBIT 준수 상태 805
 COSO 준수 상태 816
 GLBA 준수 상태 825
 HIPAA 준수 상태 829
 ITIL 준수 상태 820
 Sarbanes-Oxley 803
 Visa CISP 준수 상태 838
 준수 추가 페이지 540, 545, 546
 중복 감지 71
 중복 방지
 설정 70
 작업 433
 중복 IP 주소 427
 중요도 522, 533, 544, 559
 진단
 감지 장치 부팅 263
 기본 IP 225, 263, 399
 모듈 상태 264
 보기 684

설명 263
 실행 684
 이중 데이터 수집 264
 이중 불일치 49
 인터페이스 264
 장치 정보 263, 399
 추가 687
 토폴로지 49
 토폴로지 수집 255
 NA 감지 장치 부팅 263, 399
 NA 라우팅 테이블 225, 264
 NA 모듈 상태 263, 399
 NA 인터페이스 225, 263, 399
 NA 포트 스캔 264, 618
 NA OSPF 인접 환경 225, 264
 NA VLAN 데이터 수집 399
 진단 검색 616
 진단 검색 페이지 617, 648
 진단 실행 페이지 397
 진단 편집 687

차

최근 작업 페이지 361, 500, 503, 867
 최대
 소프트웨어 토큰 수 60
 작업 길이 69
 최대 저장 규칙 57
 추가
 사용자 319
 사용자 지정 데이터 693
 소프트웨어 이미지 553
 장치 135, 205
 장치 그룹 175
 진단 687
 하위 작업 487
 추산 기간 234, 367, 376

카

컨텍스트 관리 315, 448
 코어 191, 195
 콘솔 서버 135, 311

타

타사 통합 페이지 115

텔넷

개요 213

세션 나열 215

장치 액세스 213

클라이언트 89

텔넷 프록시 예약 77

텔넷/SSH

구성 변경 217

서버 89

세션 로깅 86

프록시 86, 213, 214

텔넷/SSH 세션 페이지 215

텔넷/SSH 페이지 86

템플릿

보기 708

스크립트 생성 739

편집 708

통계

공급업체 상위 5개 353

대시보드 353, 757

OS 버전 상위 5개 353

트렁크 포트

구성 455

기본 VLAN ID 455

멤버 VLAN 455

티켓

생성 571, 576

업데이트 253

추가 571, 576

파

파일 이름 패턴 541

파티션

공유 171, 552, 570, 704

구성 195

보기 206

선택 706

장치 암호 규칙 172

장치 제한 414

장치 주석 767

장치 추가 138

적용 대상 457

파티션 편집 페이지 204

패턴 시간 초과 47

편집 메뉴 157, 304

포트

변경 258

사용 중 586

여유 586

잘못된 개수 259

포트 스캔

개요 315

작업 설정 58

포트 스캔 작업 페이지 440

프로비전 메뉴 157, 314

프로세스 105

프록시 서버 74

플래시 저장 공간 50

필터 표시 501

하

하드웨어

공급업체 144

모델 144

설명 144

항상된 사용자 지정 필드 설정 699

현재 로그인한 사용자 페이지 320

협상 속도 273

협상 이종 267, 273

홈 페이지

워크플로 승인 350

홈 상자

연결 312

정의 307, 308

활동 캘린더 247

활성 노드 426

A

AAA 63, 65, 213, 325, 340

ACL 검색 페이지 652

ACL(액세스 제어 목록)

개요 651

검색 651

구문 분석 46, 143, 151

- 삭제 888
- 스크립트 391
- 스크립트 생성 392
- 식별자 875
- 응용 프로그램 스크립트 392
- 이력 875
- 일괄 삽입 881
- 편집 46
- 핸들 875
- Active Directory
 - 개요 99
 - 외부 인증 106
 - 포트 106
- appserver.rcx 파일
 - 계층 레이어 768
 - 편집 768

B

- Bare metal 프로비전
 - 개요 153
 - 새 장치 템플릿 추가 161
 - 스크립트 714
 - 장치 템플릿 155
 - 장치 프로비전 페이지 444
 - 프로토타입 153

C

- CIDR 표기법 428, 430
- Cisco.com 74
- Cisco.com 프록시 344
- CLI
 - 도움말 31, 915
 - 명령 214
 - 코딩 규칙 915
- COBIT
 - 개요 805
 - 준수 상태 보고서 805
- Configlet 구문 분석 270
- COSO
 - 개요 816
 - 준수 상태 보고서 816
- CSV 데이터 파일
 - 기본 IP 주소 168

- 액세스 방법 168
- 호스트 이름 168
- CVE
 - 이름 528, 539, 559
 - 취약점 544, 602

D

- DRS(드라이버 릴리스 서비스) 36, 370, 894, 896

E

- Expect 엔진 713

F

- FQDN 확인 페이지 475
- FTP 모니터 111, 122
- FTP 서버 68, 123, 124

G

- GLBA
 - 개요 825
 - 준수 상태 보고서 825

H

- HIPAA
 - 개요 829
 - 준수 상태 보고서 829
- HP Live Network
 - 개요 29
 - 액세스 29
- HP OO
 - 명령 스크립트 713
 - 사용자 인증 306
 - 서비스 105
 - 언어 724
 - 포트 105
 - 호스트 이름 105
 - 흐름 713
- HTTP 모니터 112

I

- ICMP 테스트 실행 페이지 384

IP 검색 페이지 661

IP 공간

개요 197

이름 198

IP 주소

개요 661

검색 661

검색 결과 664

관리되는 305, 307

내부 662

연결 662

재할당 70

중복 보고서 746

IP를 통한 연결 313

IPv6 68

ITIL

개요 820

준수 상태 보고서 820

J

Java RMI 256

Java RMI/JRMP 프로토콜 257

JRE 214

JRMP 256

L

LDAP

검색 기준 106, 107

구성 108

설치 108

SSL 구성 108

LDAP 모니터 112

M

MAC 검색 페이지 658

MAC 주소

개요 657

검색 657

검색 결과 660

내부 659

세부사항 275

연결 659

장치 276

N

NA 게이트웨이 메시 195

NA 기능

NA 7.50 21

NA 7.60 22

NA 9.0 24

NA 9.10 26

NA 모듈 상태 225

NA 홈 페이지

검토 349

기본 설정 및 프로필 338

내 작업 공간 30, 349

사용자 설정 편집 338

사용자 지정 30, 349

장치 검색 30, 349

NA Satellite 52

NA/SA 292

NA/SA 통합

개요 254

권한 255

다이어그램 작성 764

방화벽 구성 256

서버 페이지 292

인증 101

장치 MAC 주소 페이지 276

Java RMI 256

JRMP 256

NAT

구성 141, 149

IP 주소 141, 149

NMAP

설정 58

설치 440

스캔 방식 430

옵션 58

포트 스캔 264, 440, 618

NNMi 통합

알람 115

작업 115

통합 페이지 115

O

OS 분석 작업 페이지 436

P

Perl 모듈 연결 720
 Ping
 개요 383
 ICMP 테스트 작업 383
 Pull 변수 버튼 724, 725
 Putty 213

Q

QoS 270

R

RADIUS 100, 103, 325
 RADIUS NA-IP 필드 104
 RLogin 57, 142, 150
 RSA
 서버 인증 789
 속성 파일 789

S

SA 268, 273, 764
 Sarbanes-Oxley
 개요 803
 COBIT 준수 805
 COSO 준수 816
 GLBA 준수 825
 HIPAA 준수 829
 ITIL 준수 820
 ScriptMaster 630
 SecureCRT 213
 SecurID
 개요 788
 노드 암호 798
 라이선스 사용 59
 로그인 794
 문제 해결 798
 암호 코드 수명 60
 인증 99, 788
 장치 액세스 59
 최대 소프트웨어 토큰 수 60
 토큰 59
 토큰 관리 340
 토큰 추가 793

RSA 서버 789
 SMTP 모니터 112
 SNMP
 스캐너 스레드 58
 시간 초과 설정 59
 장치 검색 212
 트랩 563, 575
 SNMP 커뮤니티 문자열
 삭제 373
 추가 373
 SNMPv3
 암호화 210
 암호화 암호 140, 148
 연결 방법 142, 150, 210
 인증 142, 150, 210
 인증 암호 140, 148
 SSH
 사용자 60
 서버 89
 세션 나열 215
 암호 60
 장치 액세스 213
 SSH 모니터 112
 SSH 장치 액세스 60
 SSH 프록시 예약 77
 SWIM 오류 메시지 898
 Syslog
 구성 143, 367
 메시지 52
 사용자 패턴 45
 시작 124
 중지 124
 패턴 52
 Syslog 구성 페이지 366, 419
 Syslog 모니터 113
 Syslog 서버 123

T

TACACS+ 암호 103
 TACACS+ 인증 100
 TCP(Transmission Control Protocol) 427
 TFTP 모니터 113, 122
 TFTP 서버 68, 123, 124
 Traceroute

개요 383
ICMP 테스트 작업 383
Twist 서버 104

U

UDP(User Datagram Protocol) 427

V

Visa CISP

개요 838
준수 상태 보고서 838
Visio 764

VLAN

개요 278
검색 665
검색 결과 667
기본 272
생성 282
장치 280
트렁크 포트 272
편집 282
포트 284
VLAN 작업 페이지 452
VTP 세부사항 285
VTP 주석 767
VLAN 검색 페이지 665
VLAN 세부사항 페이지 283
VLAN 작업 페이지 452
VRF 270
VTP 도메인 페이지 287
VTP 세부사항
클라이언트 모드 285
투명 모드 285
VTP 세부사항 페이지 262, 285

