



CommandCenter Secure Gateway

관리자 설명서

Release 4.0

Copyright © 2008 Raritan, Inc.

CCA-0H-K

2008년 7월

255-80-5140-00

이 문서에는 저작권으로 보호되는 독점 정보가 포함되어 있습니다. All rights reserved. 이 문서의 어떠한 부분도 Raritan, Inc.의 명시적인 사전 서면 승인 없이는 다른 언어로 복사, 복제 또는 번역할 수 없습니다.

© Copyright 2008 Raritan, Inc., CommandCenter®, Dominion®, Paragon® 및 Raritan 회사 로고는 Raritan, Inc.의 상표 또는 등록 상표입니다. All rights reserved. Java®는 Sun Microsystems, Inc.의 등록 상표입니다. Internet Explorer®는 Microsoft Corporation 의 등록 상표입니다. Netscape® 및 Netscape Navigator®는 Netscape Communication Corporation 의 등록 상표입니다. 다른 모든 상표 또는 등록 상표는 해당 소유자의 재산입니다.

FCC 정보

이 장비는 A급 디지털 장비에 대한 제한사항 및 FCC 규정 Part 15를 준수함을 검증 받았습니다. 이러한 제한사항은 상업적 설치 시 유해한 간섭으로부터 장비를 적절히 보호하기 위해 고안되었습니다. 이 장비는 무선 주파수 에너지를 생성, 사용 및 방사하므로, 지침에 따라 설치하여 사용하지 않는 경우 무선 통신에 유해한 간섭을 일으킬 수 있습니다. 주거 환경에서 이 장비를 작동할 경우 유해한 간섭을 일으킬 수 있습니다.

VCCI 정보(일본)

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan 은 사고, 재해, 오용, 남용, Raritan 에서 수행하지 않은 제품 개조 또는 그 밖에 Raritan 의 적절한 통제를 벗어난 상황 또는 정상 작동 조건에서 일어나지 않는 상황으로 인한 제품 손상에 대해 책임을 지지 않습니다.



목차

CC-SG 관리자 설명서의 새로운 내용	xv
------------------------------	-----------

방법: CC-SG 기본 기능	xvi
------------------------	------------

강력한 암호 구성 및 적용.....	xvi
CC-SG를 새 펌웨어 버전으로 업그레이드.....	xvii
노드 그룹에 대한 전원 제어 및 전원 제어 작업 모니터링.....	xix
노드 그룹 전원 제어.....	xix
전원 상태 메시지.....	xx
제한 시간 내에 여러 장치 업그레이드.....	xx
모든 사용자에게 대해 노드의 기본 사용자 정의 보기 할당.....	xxii

개요	1
-----------	----------

전제조건.....	1
용어/약어.....	2
클라이언트 브라우저 요구사항.....	4

CC-SG 액세스	5
------------------	----------

CC-SG Admin 클라이언트를 통한 브라우저 기반 액세스.....	5
JRE 비호환성.....	6
썬 클라이언트 액세스.....	6
썬 클라이언트 설치.....	6
썬 클라이언트 사용.....	8

CC-SG Admin 클라이언트	8
시작하기	10
IP 주소 확인.....	10
CC-SG 서버 시간 설정	10
호환성 매트릭스 확인.....	12
애플리케이션 버전 확인 및 업그레이드.....	12
설정 안내서를 사용하여 CC-SG 구성	14
설정 설명서를 사용하기 전에	14
설정 안내서의 연관체	15
범주 및 요소 생성	15
장치 설정	15
장치 검색 및 추가	16
그룹 생성	17
장치 그룹 및 노드 그룹 추가.....	17
사용자 관리	20
사용자 그룹 및 사용자 추가.....	20
연관체, 범주 및 요소	22
연관체 정보	22
연관체 용어	22
연관체-범주 및 요소 정의	23
연관체 생성 방법	24
연관체 관리자.....	24
범주 추가.....	24
범주 편집.....	25
범주 삭제.....	25
요소 추가.....	25
요소 편집.....	26
요소 삭제.....	26
장치, 장치 그룹 및 포트	27
장치 보기	28
장치 탭	28
장치 및 포트 아이콘	28
포트 정렬 옵션.....	29
장치 프로필 화면	30
분포도 보기	30
장치 탭에서 옵션을 마우스 오른쪽 버튼으로 클릭합니다.....	31

장치 검색.....	31
검색을 위한 와일드카드.....	31
와일드카드 예제.....	31
장치 검색.....	32
장치 추가.....	33
KVM 또는 직렬 장치 추가.....	33
전원 탭 장치 추가.....	35
Dominion PX 장치 추가.....	35
장치 편집.....	36
전원 탭 장치 또는 Dominion PX 장치 편집.....	36
장치 프로필에 메모 추가.....	37
장치 프로필에 위치 및 연락처 추가.....	37
장치 삭제.....	38
포트 구성.....	38
직렬 포트 구성.....	38
KVM 포트 구성.....	39
포트 구성에 의해 생성된 노드.....	40
포트 편집.....	40
포트 삭제.....	41
장치 범주 및 요소 대량 복사.....	42
장치 업그레이드.....	42
장치 구성 백업.....	43
장치 구성 복원.....	44
장치 구성 복원(KX, KSX, KX101, SX, IP-Reach).....	44
네트워크 설정을 제외한 모든 구성 데이터를 KX2, KSX2 또는 KX2-101 장치로 복원합니다.....	45
장치 설정 또는 사용자 및 사용자 그룹 데이터만 KX2, KSX2 또는 KX2-101 장치로 복원.....	45
모든 구성 데이터를 KX2, KSX2 또는 KX2-101 장치로 복원.....	46
장치 백업 파일의 저장, 업로드 및 삭제.....	46
장치 구성 복사.....	47
장치 다시 시작.....	47
장치 핑.....	48
장치에 대한 CC-SG의 관리 일시 중지.....	48
관리 다시 시작.....	48
장치 전원 관리자.....	49
장치의 관리 페이지 실행.....	49
사용자 연결 해제.....	50
Paragon II 시스템 장치로의 특별 액세스.....	50
P2-SC(Paragon II System Controller).....	50
IP-Reach 및 UST-IP 관리.....	51
장치 그룹 관리자.....	51
장치 그룹 추가.....	51
장치 그룹 편집.....	54
장치 그룹 삭제.....	55

관리된 전원 탭 56

CC-SG에서 다른 장치가 관리하는 전원 탭 구성.....57

KX, KX2, KX2-101, KSX2 및 P2SC에 연결된 전원 탭 구성58

 KX, KX2, KX2-101, KSX2 또는 P2SC 장치에 연결된 전원 탭 장치 추가58

 KX, KX2, KX2-101, KSX2 또는 P2SC의 전원 탭을 다른 포트에 이동.....58

 KX, KX2, KX2-101, KSX2 또는 P2SC 장치에 연결된 전원 탭 장치 삭제59

SX 3.0 및 KSX에 연결된 전원 탭 구성.....59

 SX 3.0 또는 KSX 장치에 연결된 전원 탭 추가.....59

 SX 3.0 또는 KSX 장치에 연결된 전원 탭 삭제.....60

 전원 탭의 장치 또는 포트 연관체 변경(SX 3.0, KSX).....60

SX 3.1에 연결된 전원 탭 구성61

 SX 3.1 장치에 연결된 전원 탭 추가.....61

 SX 3.1의 전원 탭을 다른 포트에 이동.....62

 SX 3.1 장치에 연결된 전원 탭 삭제.....62

전원 탭의 콘센트 구성.....62

노드, 노드 그룹 및 인터페이스 64

노드 및 인터페이스 개요65

 노드 정보.....65

 노드 이름.....65

 인터페이스 정보.....65

노드 보기.....66

 노드 탭.....66

 노드 프로필.....67

 노드 및 인터페이스 아이콘.....68

서비스 계정.....69

 서비스 계정 개요.....69

 서비스 계정 추가, 편집 및 삭제.....70

 서비스 계정의 암호 변경.....71

 인터페이스에 서비스 계정 지정.....71

노드 추가, 편집 및 삭제.....72

 노드 추가.....72

 포트 구성에 의해 생성된 노드.....73

 노드 편집.....73

 노드 삭제.....73

노드 프로필에 위치 및 연락처 추가.....74

노드 프로필에 메모 추가.....74

CC-SG에서 가상 인프라 구성.....75

 가상 인프라 용어.....75

 가상 노드 개요.....76

 가상 호스트 및 가상 시스템이 있는 제어 시스템 추가.....76

 가상 시스템이 있는 가상 호스트 추가.....78

제어 시스템, 가상 호스트 및 가상 시스템 편집.....	80
제어 시스템 및 가상 호스트 삭제.....	82
가상 시스템 노드 삭제.....	82
가상 인프라 삭제.....	82
CC-SG와 가상 인프라 동기화.....	83
가상 인프라 동기화.....	83
가상 인프라의 일일 동기화 활성화 또는 비활성화.....	83
가상 호스트 노드의 재부팅 또는 강제 재부팅.....	84
가상 분포도 보기 액세스.....	84
노드 연결.....	85
노드 핑.....	85
인터페이스 추가, 편집 및 삭제.....	86
인터페이스 추가.....	86
인터페이스 편집.....	93
인터페이스 삭제.....	94
인터페이스 책갈피 설정.....	94
노드에 직접 포트 액세스 구성.....	95
노드 범주 및 요소 대량 복사.....	95
채팅 사용.....	96
노드 그룹 추가, 편집 및 삭제.....	97
노드 그룹 개요.....	97
노드 그룹 추가.....	97
노드 그룹 편집.....	101
노드 그룹 삭제.....	101

사용자 및 사용자 그룹 102

사용자 탭.....	103
기본 사용자 그룹.....	104
CC 수퍼 사용자 그룹.....	104
시스템 관리자 그룹.....	104
CC 사용자 그룹.....	104
사용자 그룹 추가, 편집 및 삭제.....	105
사용자 그룹 추가.....	105
사용자 그룹 편집.....	106
사용자 그룹 삭제.....	107
사용자 그룹에 대한 액세스 감사 구성.....	107
사용자 추가, 편집 및 삭제.....	108
사용자 추가.....	108
사용자 편집.....	109
사용자 삭제.....	110
그룹에 사용자 지정.....	110
그룹에서 사용자 삭제.....	111
사용자 프로필.....	111
암호 변경.....	111

기본 검색 기본 설정 변경	112
CC-SG 기본 글꼴 크기 변경	112
이메일 주소 변경	112
CC-SG 슈퍼 사용자의 사용자 이름 변경	113
사용자 로그아웃	113
사용자 대량 복사	114

액세스 제어 규정 115

규정 추가	116
규정 편집	117
규정 삭제	118
가상 매체 지원	119
사용자 그룹에 규정 지정	119

장치 및 노드의 사용자 정의 보기 120

사용자 정의 보기 유형	120
범주별 보기	120
노드 그룹별 필터	120
장치 그룹별 필터	120
Admin 클라이언트에서 사용자 정의 보기 사용	121
노드 사용자 정의 보기	121
장치 사용자 정의 보기	124

원격 인증 128

인증 및 허가(AA) 개요	128
인증 흐름	128
사용자 계정	129
LDAP 및 AD의 DN(구분 이름)	129
AD의 DN 지정	129
LDAP의 DN 지정	130
AD의 사용자 이름 지정	130
기본 DN 지정	130
인증 및 허가에 대한 모듈 지정	130
외부 AA 서버의 순서 설정	131
AD 및 CC-SG 개요	131
CC-SG에 AD 모듈 추가	131
AD 일반 설정	132
AD 고급 설정	133
AD 그룹 설정	134
AD Trust(트러스트) 설정	135

AD 모듈 편집 136

AD 사용자 그룹 가져오기 137

AD와 CC-SG 동기화 138

 AD와 모든 사용자 그룹 동기화..... 139

 모든 AD 모듈 동기화 140

 모든 AD 모듈의 일일 동기화 활성화 또는 비활성화 140

 일일 AD 동기화 시간 변경 141

LDAP 및 CC-SG 정보..... 141

CC-SG에 LDAP(Netscape) 모듈 추가..... 141

 LDAP 일반 설정 141

 LDAP 고급 설정 142

 Sun One LDAP(iPlanet) 구성 설정..... 144

 OpenLDAP(eDirectory) 구성 설정..... 144

TACACS+ 및 CC-SG 정보 145

TACACS+ 모듈 추가 145

 TACACS+ 일반 설정 145

RADIUS 및 CC-SG 정보 146

RADIUS 모듈 추가 146

 RADIUS 일반 설정 146

 RADIUS를 이용한 Two-Factor 인증..... 147

보고서 **148**

보고서 사용 148

 보고서 데이터 정렬 148

 보고서 열 너비 크기 조정 148

 보고서 내역 보기 149

 여러 페이지 보고서 탐색 149

 보고서 인쇄 149

 보고서를 파일로 저장..... 149

 CC-SG에서 보고서 데이터 제거..... 150

 보고서 필터 숨기기 또는 표시 150

감사 추적 보고서	151
오류 로그 보고서	152
액세스 보고서.....	152
가용성 보고서.....	153
활성 사용자 보고서.....	154
잠긴 사용자 보고서.....	154
모든 사용자 데이터 보고서.....	154
사용자 데이터 보고서.....	155
장치 자산 보고서	156
장치 그룹 데이터 보고서	156
질의 포트 보고서	156
노드 자산 보고서	158
활성 노드 보고서	159
노드 생성 보고서	159
노드 그룹 데이터 보고서	159
AD 사용자 그룹 보고서.....	160
예약된 보고서.....	160
장치 펌웨어 업그레이드 보고서.....	161
CC-NOC 동기화 보고서	161

시스템 정비 **162**

정비 모드.....	162
예약된 작업 및 정비 모드	162
정비 모드 시작.....	162
정비 모드 종료.....	163
CC-SG 백업	163
백업 파일 저장 및 삭제	164
백업 파일 저장.....	165
백업 파일 삭제.....	165
CC-SG 복원	165
CC-SG 재설정.....	166
CC-SG 다시 시작	169
CC-SG 업그레이드.....	169
브라우저 캐시 지우기.....	171
Java 캐시 지우기	171
CC-SG 종료	172
종료 후 CC-SG 다시 시작.....	172
CC-SG 전원 끄기	172
CC-SG 세션 종료	173
CC-SG에서 로그아웃.....	173
CC-SG 종료	173

고급 관리	174
오늘의 메시지 구성.....	174
노드 액세스를 위한 애플리케이션 구성.....	175
노드 액세스를 위한 애플리케이션 정보.....	175
애플리케이션 버전 확인 및 업그레이드.....	175
애플리케이션 추가.....	176
애플리케이션 삭제.....	177
기본 애플리케이션 구성.....	177
기본 애플리케이션 정보.....	177
기본 애플리케이션 지정 보기.....	177
인터페이스 또는 포트 유형에 대한 기본 애플리케이션을 선택합니다.....	178
장치 펌웨어 관리.....	178
펌웨어 업로드.....	178
펌웨어 삭제.....	179
CC-SG 네트워크 구성.....	179
네트워크 설정 정보.....	179
CC-SG LAN 포트 정보.....	179
기본/백업 모드란 무엇입니까?.....	180
활성/활성 모드란 무엇입니까?.....	183
CC-SG에 대한 권장 DHCP 구성.....	185
로그 활동 구성:.....	185
CC-SG의 내부 로그 제거.....	186
CC-SG 서버 시간 및 날짜 구성.....	186
연결 모드: 직접 및 프록시.....	187
연결 모드 정보.....	187
모든 클라이언트 연결에 대해 직접 모드 구성.....	188
모든 클라이언트 연결에 대해 프록시 모드 구성.....	188
직접 모드 또는 프록시 모드의 조합 구성.....	188
장치 설정.....	189
사용자 정의 JRE 설정 구성.....	190
SNMP 구성.....	191
MIB 파일.....	192
CC-SG 클러스터 구성.....	193
CC-SG 클러스터란 무엇입니까?.....	193
CC-SG 클러스터의 요구 사항.....	193
CC-SG 클러스터 및 CC-NOC 정보.....	193
클러스터 생성.....	194
보조 CC-SG 노드 제거.....	195
기본 CC-SG 노드 제거.....	195
실패한 CC-SG 노드 복구.....	195
고급 클러스터 설정.....	196
보안 관리자.....	196
원격 인증.....	196

AES 암호화.....	197
브라우저 연결 프로토콜 구성: HTTP 또는 HTTPS/SSL.....	198
CC-SG에 SSH 액세스를 위한 포트 번호 설정.....	198
로그인 설정.....	198
비활동 타이머 구성.....	201
초기 화면.....	202
인증서.....	203
액세스 제어 목록.....	206
통지 관리자.....	208
외부 SMTP 서버 구성.....	208
작업 관리자.....	209
작업 유형.....	209
순차적 작업 예약.....	209
작업에 대한 이메일 통지.....	209
예약된 보고서.....	210
작업 찾기 및 보기.....	210
작업 예약.....	211
장치 펌웨어 업그레이드 예약.....	213
예약된 작업 변경.....	215
작업 재예약.....	215
다른 작업과 비슷한 작업 예약.....	216
작업 삭제.....	216
CommandCenter NOC.....	216
CC-NOC 추가.....	216
CC-NOC 편집.....	218
CC-NOC 실행.....	218
CC-NOC 삭제.....	218
CC-SG에 대한 SSH 액세스.....	219
SSH 명령에 대한 도움말 얻기.....	220
SSH 명령 및 매개변수.....	221
명령 팁.....	224
직렬 가능 장치에 SSH 연결 생성.....	225
SSH를 사용하여 대역외 직렬 인터페이스를 통해 노드에 연결.....	226
SSH 연결 종료.....	227
직렬 관리 포트.....	227
터미널 애플리케이션 프로그램 정보.....	228
CC-SG 일련 번호 찾기.....	228
Web Services API.....	228

진단 콘솔 231

진단 콘솔 액세스.....	231
VGA/키보드/마우스 포트를 통한 진단 콘솔 액세스.....	231
SSH를 통한 진단 콘솔 액세스.....	231
상태 콘솔.....	233
상태 콘솔 정보.....	233

상태 콘솔 액세스.....	233
관리자 콘솔.....	233
관리자 콘솔 정보.....	233
관리자 콘솔 액세스.....	234
관리자 콘솔 탐색.....	234
진단 콘솔 구성 편집.....	235
네트워크 인터페이스 구성 편집(네트워크 인터페이스).....	235
IP 주소 ping.....	237
Traceroute 사용.....	238
정적 루트 편집.....	239
진단 콘솔에서 로그 파일 보기.....	241
진단 콘솔로 CC-SG 다시 시작.....	245
진단 콘솔로 CC-SG 재부팅.....	246
진단 콘솔에서 CC-SG 시스템 전원 끄기.....	247
진단 콘솔로 CC 슈퍼 사용자 암호 재설정.....	248
CC-SG 출고 시 구성(Admin) 재설정.....	249
진단 콘솔 암호 설정.....	251
진단 콘솔 계정 구성.....	253
원격 시스템 모니터링 구성.....	255
이력 데이터 추세 구성.....	256
디스크 상태 표시.....	257
진단 콘솔로 상단 부분 표시 보기.....	257
NTP 상태 표시.....	258
V1 및 E1 사양	260
V1 모델.....	260
V1 일반 사양.....	260
V1 환경 요구사항.....	260
E1 모델.....	261
E1 일반 사양.....	261
E1 환경 요구사항.....	261
CC-SG 및 네트워크 구성	263
CC-SG 네트워크를 위한 필수 개방 포트: 요약.....	263
CC-SG 통신 채널.....	264
CC-SG 및 Raritan 장치.....	264
CC-SG 클러스터링.....	265
인프라 서비스 액세스.....	266
PC 클라이언트 및 CC-SG.....	266
PC 클라이언트 및 노드.....	267
CC-SG 및 IPMI, iLO/RILOE, DRAC, RSA용 클라이언트.....	268
CC-SG 및 SNMP.....	268
CC-SG 및 CC-NOC.....	268

CC-SG 내부 포트	269
NAT 사용 방화벽을 통한 CC-SG 액세스	270
노드에 대한 RDP 액세스	270
노드에 대한 VNC 액세스	270
노드에 대한 SSH 액세스	270
원격 시스템 모니터링 포트	270
사용자 그룹 권한	271
<hr/>	
SNMP 트랩	279
<hr/>	
문제 해결	281
<hr/>	
두 요소 인증	282
두 요소 인증을 위한 지원 환경	282
두 요소 인증 설정 요구사항	282
두 요소 인증의 알려진 문제	283
자주 묻는 질문	284
일반 FAQ	284
인증 FAQ	286
보안 FAQ	287
회계 FAQ	288
성능 FAQ	289
그룹화 FAQ	289
상호 운용성 FAQ	290
인증 FAQ	291
사용자 경험 FAQ	291
키보드 단축키	293
<hr/>	
명명 규칙	294
<hr/>	
색인	295
<hr/>	

CC-SG 관리자 설명서의 새로운 내용

장비 및/또는 설명서에 대한 개선 사항 및 변경 사항을 기초로 다음 섹션이 변경되었거나 CommandCenter Secure Gateway 관리자 설명서에 정보가 추가되었습니다.

- **JRE 비호환성** (p. 6)
- **Dominion PX 장치 추가** (p. 35)
- **전원 탭 장치 또는 Dominion PX 장치 편집** (p. 36)
- **장치 프로필에 메모 추가** (p. 37)
- **장치 프로필에 위치 및 연락처 추가** (p. 37)
- **CC-SG에서 다른 장치가 관리하는 전원 탭 구성** (p. 57)
- **서비스 계정** (p. 69)
- **노드 프로필에 위치 및 연락처 추가** (p. 74)
- **노드 프로필에 메모 추가** (p. 74)
- **CC-SG에서 가상 인프라 구성** (p. 75)
- **CC-SG와 가상 인프라 동기화** (p. 83)
- **가상 호스트 노드의 재부팅 또는 강제 재부팅** (p. 84)
- **가상 분포도 보기 액세스** (p. 84)
- **대역내 연결을 위한 인터페이스** (p. 88)
- **인터페이스 삭제** (p. 94)
- **사용자 그룹에 대한 액세스 감사 구성** (p. 107)
- **CC-SG 업그레이드** (p. 169)
- **CC-SG 재설정** (p. 166)
- **장치 설정** (p. 189)
- **사용자 정의 JRE 설정 구성** (p. 190)
- **SNMP 구성** (p. 191)
- **원격 시스템 모니터링 구성** (p. 255)
- **이력 데이터 추세 구성** (p. 256)
- **CC-SG 통신 채널** (p. 264)

이 버전의 CommandCenter Secure Gateway 에 적용된 변경 사항에 대한 자세한 설명은 Release Notes 를 참조하십시오.

방법: CC-SG 기본 기능

이 장에서는 사용자가 CC-SG의 실제적인 사용에 빠르게 익숙해지도록 도와주는 가장 일반적인 몇 가지의 사용 사례를 포함하고 있습니다. 이 섹션에서는 일반적인 예제를 제공하지만 실제 구성 및 작업에 따라 다를 수 있습니다.

이 장에서

강력한 암호 구성 및 적용	xvi
CC-SG를 새 펌웨어 버전으로 업그레이드	xvii
노드 그룹에 대한 전원 제어 및 전원 제어 작업 모니터링	xix
제한 시간 내에 여러 장치 업그레이드	xx
모든 사용자에게 대해 노드의 기본 사용자 정의 보기 할당	xxii

강력한 암호 구성 및 적용

1. 관리 > 보안을 선택합니다.
2. 로그인 설정 탭을 클릭합니다.
3. 모든 사용자에게 강력한 암호 필요 확인란을 선택합니다.
4. 최대 암호 길이를 선택합니다. 암호는 최대 문자 수보다 적어야 합니다.
5. 암호 기록 수준을 선택합니다. 숫자는 기록에 남아 있어 재사용할 수 없는 이전 암호 수를 지정합니다. 예를 들어, 암호 기록 수준이 5로 설정된 경우 사용자는 이전 5개의 암호를 다시 사용할 수 없습니다.
6. 암호 만료 빈도를 선택합니다. 모든 암호는 설정된 일 수 이후에 만료됩니다. 암호가 만료된 후 사용자는 다음에 로그인할 때 새 암호를 선택해야 합니다.
7. 강력한 암호 요구사항 선택:
 - 암호에는 한 개 이상의 소문자가 포함되어야 합니다.
 - 암호에는 한 개 이상의 대문자가 포함되어야 합니다.

- 암호에 한 개 이상의 숫자가 포함되어야 합니다.
 - 암호는 한 개 이상의 특수 문자(예: 느낌표 또는 앰퍼샌드)를 포함해야 합니다.
8. 업데이트를 클릭하여 변경 사항을 저장합니다.

로그인 보안에 대한 자세한 내용은 **로그인 설정** (p. 198)을 참조하십시오.

CC-SG를 새 펌웨어 버전으로 업그레이드

CC-SG의 펌웨어는 새 버전이 출시될 때 업그레이드할 수 있습니다. Raritan 웹 사이트의 지원 섹션에서 펌웨어 파일을 찾을 수 있습니다.

CC-SG 버전 4.0은 G1 하드웨어와 호환되지 않습니다. CC-SG G1 장치를 버전 4.0으로 업그레이드하지 마십시오.

펌웨어 파일을 자신의 클라이언트 PC에 다운로드하여 업그레이드를 진행합니다.

CC 설정 및 제어 권한을 가진 사용자만 CC-SG를 업그레이드할 수 있습니다.

업그레이드하기 전에 CC-SG를 백업해야 합니다.

CC-SG 클러스터가 작동하는 경우 업그레이드 전에 먼저 클러스터를 제거해야 합니다. 각 CC-SG 노드를 개별적으로 업그레이드하고 클러스터를 다시 생성하십시오.

중요: CC-SG 및 장치 또는 장치 그룹을 업그레이드 해야 할 경우 CC-SG 업그레이드를 먼저 수행한 다음 장치 업그레이드를 수행합니다.

CC-SG는 업그레이드 프로세스의 일부로서 재부팅됩니다. 업그레이드 동안 프로세스를 중단하거나 장치를 수동으로 재부팅하거나 장치의 전원을 끄거나 켜다가 켜지 마십시오.

▶ **CC-SG를 업그레이드하려면:**

1. 클라이언트 PC에 펌웨어 업그레이드 파일을 다운로드합니다.
2. CC 설정 및 제어 권한을 가진 계정을 이용하여 CC-SG Admin 클라이언트에 로그인합니다.
3. 정비 모드를 시작합니다. **정비 모드 시작** (p. 162)을 참조하십시오.

4. CC-SG 가 정비 모드가 되면 시스템 정비 > 업그레이드를 선택합니다.
5. 찾아보기를 클릭합니다. CC-SG 펌웨어 파일(.zip)을 탐색하여 선택한 다음 열기를 클릭합니다.
6. 확인을 클릭하여 펌웨어 파일을 CC-SG 로 업로드합니다.
펌웨어 파일이 CC-SG 로 업로드된 후 CC-SG 가 업그레이드 프로세스를 시작했음을 나타내는 성공 메시지가 표시됩니다. 이제 모든 사용자는 CC-SG 에서 연결 해제됩니다.
7. 확인을 클릭하여 CC-SG 를 종료합니다.
8. 브라우저 캐시를 지운 다음 브라우저 창을 닫습니다. **브라우저 캐시 지우기** (p. 171)를 참조하십시오.
9. Java 캐시를 지웁니다. **Java 캐시 지우기** (p. 171)를 참조하십시오.
10. CC-SG 에 다시 로그인하기 전에 업그레이드가 완료될 때까지 기다려야 합니다. 진단 콘솔에서 업그레이드를 모니터링할 수 있습니다.
 - a. admin 계정을 이용해 진단 콘솔을 액세스합니다. **관리자 콘솔 액세스** (p. 234)를 참조하십시오.
 - b. 관리자 > 시스템 로그파일 뷰어를 선택합니다. 업그레이드 로그를 보려면 **sg/upgrade.log** 를 선택한 다음 보기를 선택합니다.
 - c. 업그레이드 프로세스가 실행될 때까지 기다립니다. 업그레이드 프로세스가 완료되면 업그레이드 로그에 "업그레이드 완료" 메시지가 표시됩니다.
 - d. 서버를 재부팅해야 합니다. 재부팅 프로세스가 시작되면 업그레이드 로그에 "Linux 재부팅" 메시지가 표시됩니다. 서버가 종료되고 재부팅됩니다.
11. CC-SG 가 재부팅되는 동안 몇 초 기다린 후 새 웹 브라우저 창을 실행합니다.
12. CC 설정 및 제어 권한을 가진 계정을 이용하여 CC-SG Admin 클라이언트에 로그인합니다.
13. 도움말 > Raritan Secure Gateway 정보를 선택합니다.
업그레이드가 성공했는지 검증하기 위해 버전 번호를 확인합니다.
 - 버전이 업그레이드되지 않았으면 이전 단계를 반복합니다.
 - 업그레이드가 완료되었으면 다음 단계를 진행합니다.
14. 정비 모드를 종료합니다. **정비 모드 종료** (p. 163)를 참조하십시오.
CC-SG를 백업합니다. **CC-SG 백업** (p. 163)을 참조하십시오.

노드 그룹에 대한 전원 제어 및 전원 제어 작업 모니터링

노드 그룹 전원 제어

연관된 전원 인터페이스가 있는 노드 그룹의 모든 노드 전원을 켜고, 끄고, 켜다가 다시 켜고, 정상적으로 종료할 수 있습니다.

이 명령은 노드가 장착된 랙을 설치할 수 있도록 노드 그룹의 모든 노드 전원을 꺼야 하는 경우 또는 노드 그룹에서 다른 유형의 유지 보수를 수행해야 하는 경우에 유용할 수 있습니다.

둘 이상의 전원 제어 인터페이스를 이용한 노드의 전원 제어 작업 설정에 대한 자세한 내용은 다중 인터페이스를 이용해 노드의 전원을 제어하기 위한 설명(**CC-SG 사용자 설명서**에서)을 참조하십시오.

1. 노드 탭을 클릭합니다.
2. 노드 > 그룹 전원 제어를 선택합니다. 그룹 전원 제어 화면이 나타납니다.
3. 노드 그룹 드롭다운 화살표를 클릭하고 목록에서 전원을 제어할 노드 그룹을 선택합니다.
4. 사용 가능 목록에서 전원 제어를 수행할 특정 인터페이스를 선택한 다음 추가를 클릭하여 인터페이스를 선택 목록으로 이동합니다. 선택 목록에 필요한 인터페이스를 모두 추가할 때까지 이 단계를 반복하십시오. 인터페이스를 제거해야 하는 경우 선택 목록에서 인터페이스를 선택한 다음 제거를 클릭합니다.
5. CC-SG 가 전원 작업을 수행하는 순서로 인터페이스를 선택 목록에 배치합니다. 선택 목록에서 인터페이스를 선택한 다음 위쪽 및 아래쪽 화살표를 클릭하여 인터페이스를 원하는 순서로 이동합니다.
6. 작업 드롭다운 화살표를 클릭하고 목록에서 전원 켜기, 전원 끄기, 전원 주기, 정상 종료 또는 일시 정지를 선택합니다.
7. 작동 필드에서 전원 켜기, 전원 끄기, 정상 종료 또는 일시 정지를 선택하고 순서 간격(초) 필드에 인터페이스 간에 경과해야 하는 초(0-120)를 입력합니다.
8. 확인을 클릭하여 선택한 인터페이스를 통해 전원 작업 요청을 보냅니다. 확인 메시지가 나타납니다.
9. 전원 상태 메시지 창은 전원 제어 작업의 상태를 보여주기 위해 열립니다. 전원 제어 작업에 대한 새 정보가 수신될 때 메시지가 창에 표시됩니다. 진행 상황을 모니터링할 수 있도록 전원 제어 작업이 완료될 때까지 이 창을 열어 두어야 합니다.

CC-SG가 전원 제어 작업의 성공 및 실패에 대해 경고하는 방법에 대한 자세한 내용은 **전원 상태 메시지** (p. xx)를 참조하십시오.

전원 상태 메시지

전원 상태 메시지 창은 전원 제어 작업을 시작할 때 열립니다. 전원 제어 작업이 완료될 때까지 이 창을 열어 두어야 합니다.

전원 상태 메시지 창을 크기 조정, 최소화 또는 최대화할 수 있습니다. 창의 텍스트를 선택하고 복사 및 붙여넣기 할 수 있습니다.

전원 상태 메시지 창의 메시지는 전원 제어 작업 상태에 관해 새 정보가 수신될 때 업데이트됩니다.

다음과 같은 경우 전원 상태 메시지 창에 새 메시지가 표시됩니다.

- 전원 제어 작업 요청이 전송된 경우
- 전원 제어 작업이 실패한 경우
- 전원 제어 작업이 성공적으로 완료된 경우
- 모든 요청된 전원 제어 작업이 성공적으로 완료된 경우

▶ **전원 상태 메시지 창을 닫을 경우 상태를 업데이트하는 방법:**

- 전원 제어 작업이 실패할 경우 경고 메시지가 실패한 작업에 대한 정보와 함께 표시됩니다.
- 전체 작업이 성공적으로 완료될 경우 브라우저 창의 맨 아래 상태 표시줄에 경고 메시지가 표시됩니다.
- 경고 메시지는 작업이 실패한 경우에만 표시됩니다. 경고 메시지는 작업이 성공한 경우 표시되지 않습니다.

제한 시간 내에 여러 장치 업그레이드

장치 그룹 안에서 KX 또는 SX와 같은 동일 유형의 다중 장치를 업그레이드하도록 작업을 예약할 수 있습니다. 작업이 시작되면 보고서 > 예약된 보고서 메뉴에서 장치 펌웨어 업그레이드 보고서를 받아 실시간으로 업그레이드 상태를 볼 수 있습니다. 통지 탭에서 옵션을 지정한 경우 이 보고서가 이메일로도 전송됩니다.

예상 업그레이드 시간은 각 장치에 대한 Raritan 사용자 설명서를 참조하십시오.

▶ **장치 펌웨어 업그레이드를 예약하려면:**

1. 관리 > 작업을 선택합니다.

2. 새로 만들기를 클릭합니다.
3. 메인 탭에서 작업의 이름 및 설명을 입력합니다. 선택한 이름은 작업 및 작업과 연관된 보고서를 식별하기 위해 사용됩니다.
4. 작업 데이터 탭을 클릭합니다.
5. 장치 업그레이드 내역을 지정합니다.
 - a. 작업 실행: 장치 펌웨어 업그레이드를 선택합니다.
 - b. 장치 그룹: 업그레이드할 장치를 포함하는 장치 그룹을 선택합니다.
 - c. 장치 유형: 업그레이드할 장치 유형을 선택합니다. 둘 이상의 장치 유형을 업그레이드해야 할 경우 각 유형에 대해 작업을 예약해야 합니다.
 - d. 동시 업그레이드: 업그레이드의 파일 전송 부분을 동시에 시작해야 하는 장치 수를 지정합니다. 최대 10입니다. 각 파일 전송이 완료되면 새 파일 전송이 시작되어 한 번에 최대 동시 전송 수만큼 발생하도록 보장합니다.
 - e. 파일 업그레이드: 업그레이드할 펌웨어 버전을 선택합니다. 선택된 장치 유형에 적합한 이용 가능 업그레이드 파일만 옵션으로 표시됩니다.
6. 업그레이드 기간을 지정합니다.
 - a. 시작 날짜/시간: 작업이 시작될 날짜 및 시간을 선택합니다. 시작 날짜/시간은 현재 날짜/시간보다 커야 합니다.
 - b. 업그레이드 시간대 및 최종 업그레이드 날짜/시간 제한: 지정된 시간대 안에 모든 업그레이드를 완료해야 할 경우 이 필드를 사용하여 그 이후에는 새 업그레이드가 시작될 수 없는 날짜 및 시간을 지정합니다. 최종 업그레이드 시작 날짜/시간 필드를 활성화하기 위해 업그레이드 시간대 제한을 선택합니다.
7. 업그레이드할 장치 및 순서를 지정합니다. 우선순위가 높은 장치를 목록 맨 위에 배치합니다.
 - a. 사용 가능 목록에서 업그레이드할 각 장치를 선택하고 추가를 클릭하여 선택 목록으로 이동합니다.
 - b. 선택 목록에서 장치를 선택하고 화살표 버튼을 사용하여 업그레이드를 진행할 순서로 장치를 이동합니다.
8. 실패한 업그레이드를 재시도할 것인지 여부를 지정합니다.
 - a. 재시도 탭을 클릭합니다.

- b. 재시도 횟수: CC-SG 가 실패한 업그레이드를 재시도하는 횟수를 입력합니다.
 - c. 재시도 간격: 재시도 사이의 경과 시간을 입력합니다. 기본 시간은 30, 60 및 90 분입니다. 이것이 최적의 재시도 간격입니다.
9. 성공 및 실패 통지를 받을 이메일 주소를 지정합니다. 기본적으로 현재 로그인된 사용자의 이메일 주소를 사용할 수 있습니다. 사용자 이메일 주소는 사용자 프로필에 구성되어 있습니다.
- a. 통지 탭을 클릭합니다.
 - b. 추가를 클릭하여 열리는 창에 이메일 주소를 입력한 다음 확인을 클릭합니다.
 - c. 업그레이드가 실패할 경우 이메일이 전송되기 원하면 실패 시를 선택합니다.
 - d. 모든 업그레이드가 성공적으로 완료될 때 이메일이 전송되기 원하면 성공 시를 선택합니다.
10. 확인을 클릭하여 변경 사항을 저장합니다.

작업이 실행을 시작하면 예약된 기간 동안 언제든지 장치 펌웨어 업그레이드 보고서를 열어 업그레이드 상태를 볼 수 있습니다. **장치 펌웨어 업그레이드 보고서** (p. 161)를 참조하십시오.

모든 사용자에게 대해 노드의 기본 사용자 정의 보기 할당

CC 설정 및 제어 권한이 있는 경우 모든 사용자에게 대해 기본 사용자 정의 보기를 할당할 수 있습니다.

▶ **모든 사용자에게 대해 노드의 기본 사용자 정의 보기를 지정하려면:**

1. 노드 탭을 클릭합니다.
2. 노드 > 보기 변경 > 사용자 정의 보기 생성을 선택합니다.
3. 이름 드롭다운 화살표를 클릭하고 시스템 전체 기본 보기로 지정하고자 하는 사용자 정의 보기를 선택합니다.
4. 시스템 전체 확인란을 선택한 다음 저장을 클릭합니다.

CC-SG 에 로그인하는 모든 사용자는 선택한 사용자 정의 보기에 따라 정렬된 노드 탭을 볼 수 있습니다. 사용자는 사용자 정의 보기를 변경할 수 있습니다.

사용자 정의 보기 유형 및 생성 지침에 대한 자세한 내용은 **사용자 정의 보기** (참조 "장치 및 노드의 사용자 정의 보기" p. 120)를 참조하십시오.

CommandCenter Secure Gateway(CC-SG) 관리자 설명서는 CC-SG의 관리 및 유지를 위한 지침을 제공합니다.

이 설명서는 일반적으로 사용 가능한 모든 권한을 갖는 관리자를 대상으로 합니다.

관리자가 아닌 사용자는 Raritan의 **CommandCenter Secure Gateway 사용자 설명서**를 참조하십시오.

이 장에서

전제조건	1
용어/약어	2
클라이언트 브라우저 요구사항	4

전제조건

이 설명서의 절차에 따라 CC-SG를 구성하기 전에 CC-SG에서 관리하는 Raritan 장치의 배치에 대한 포괄적인 지침은 Raritan의 **CommandCenter Secure Gateway 배치 설명서**를 참조하십시오.

용어/약어

이 설명서에 나오는 용어 및 약어는 다음과 같습니다.

액세스 클라이언트 - CC-SG 에서 관리하는 노드에 액세스해야 하는 일반 액세스 사용자가 사용하는 HTML 기반 클라이언트입니다. 액세스 클라이언트에서는 관리 기능을 사용할 수 없습니다.

Admin 클라이언트 - 일반 액세스 사용자와 관리자가 사용할 수 있는 CC-SG 용 Java 기반 클라이언트입니다. 관리를 허용하는 클라이언트만 해당됩니다.

연관체- 범주 간, 범주의 요소 간, 포트 또는 장치 혹은 둘 간의 관계입니다. 예를 들어, "위치" 범주를 장치와 연관시키려면 CC-SG 에서 장치 및 포트를 추가하기 전에 먼저 연관체를 생성합니다.

범주 - 세트 값이나 요소를 포함하는 변수입니다. 범주의 예로는 위치가 있으며 이 범주는 "New York City", "Philadelphia" 또는 "Data Center 1"과 같은 요소를 가질 수 있습니다. CC-SG 에 장치 및 포트를 추가하면 이 정보가 연관됩니다. 장치 및 포트를 추가하기 전에 먼저 연관체를 정확하게 설정하는 것이 좋습니다. 범주의 또 다른 예로는 "OS 유형"이 있으며 "Windows", "Unix" 또는 "Linux"와 같은 요소를 가질 수 있습니다.

CIM(컴퓨터 인터페이스 모듈) - 대상 서버와 Raritan 장치를 연결하는데 사용되는 하드웨어입니다. 각 대상에는 CIM 이 필요하지만 하나의 대상에 직접 연결되어 CIM 이 필요하지 않은 Dominion KX101 은 제외됩니다. 대상 서버의 전원이 켜져 있고 CIM 에 연결되어야 하며 CIM 은 CC-SG 에서 포트를 추가하기 전에 Raritan 장치에 연결되어야 합니다. 그렇지 않으면 빈 CIM 이름이 CC-SG 포트 이름을 덮어씁니다. CIM 에 연결한 후 서버를 재부팅해야 합니다.

CommandCenter NOC(CC-NOC) - 서버, 장비 및 CC-SG 가 관리하는 Raritan 장치의 상태를 감사 및 모니터링하는 네트워크 모니터링 어플라이언스입니다.

장치 그룹 - 사용자가 액세스할 수 있는 정의된 장치 그룹입니다. 그룹의 장치에 대한 액세스를 제어하는 규정을 생성할 때 장치 그룹이 사용됩니다.

장치 - Dominion KX, Dominion KX II, Dominion SX, Dominion KSX, IP-Reach, Paragon II System Controller 및 USTIP 가 포함된 Paragon II UMT832 등과 같이 CC-SG 에서 관리하는 Raritan 제품입니다. 이 장치는 연결된 대상 서버 및 시스템 또는 "노드"를 제어합니다. 지원 장치 목록은 Raritan 지원 웹 사이트에서 CC-SG 호환성 매트릭스를 확인하십시오.

요소 - 범주의 값입니다. 예를 들어, "New York City" 요소는 "위치" 범주에 속하며 "Windows" 요소는 "OS 유형"에 속합니다.

Ghost 포트 - Paragon 장치를 관리하는 경우, CIM 또는 대상 서버가 시스템에서 제거되거나 수동 또는 사고에 의해 전원이 꺼지면 Ghost 포트가 발생할 수 있습니다. **Raritan**의 **Paragon II 사용자 설명서**를 참조하십시오.

호스트 이름 - DNS 서버 지원이 활성화된 경우 사용할 수 있습니다. **네트워크 설정 정보** (p. 179)를 참조하십시오.

호스트 이름과 완전한 도메인 이름(FQDN = 호스트 이름 + 접미사)은 257 자를 초과할 수 없습니다. 이것은 "."으로 구분되는 많은 구성요소로 구성될 수 있습니다.

각 구성요소의 최대 크기는 63 자이고 첫 번째 문자는 알파벳이어야 합니다. 나머지 문자는 영문자, 숫자 또는 "-"(하이픈 또는 마이너스)가 될 수 있습니다.

구성요소의 마지막 문자는 "-"가 될 수 없습니다.

시스템에 입력된 문자의 대소문자를 구분하지만 FQDN 을 사용할 때는 대소문자가 구분되지 않습니다.

iLO/RILOE - CC-SG 가 관리할 수 있는 Hewlett Packard 의 Integrated Lights Out/Remote Insight Lights Out 서버입니다. iLO/RILOE 장치의 대상이 직접 전원 켜기/끄기가 되거나 재순환됩니다. iLO/RILOE 장치는 CC-SG 로 검색할 수 없으며 직접 노드로 추가되어야 합니다.

대역내 액세스 - 네트워크에서 대상을 수정하거나 문제 해결하기 위해 TCP/IP 네트워크를 통해 액세스합니다. KVM 및 직렬 장치는 RemoteDesktop Viewer, SSH Client, RSA Client, VNC Viewer 와 같은 대역내 애플리케이션을 통해 액세스할 수 있습니다.

IPMI 서버 - CC-SG 에서 제어할 수 있는 Intelligent Platform Management Interface 서버입니다. IPMI 를 자동으로 발견하거나 수동으로 추가할 수 있습니다.

대역외 액세스 - Raritan Remote Console(RRC), Raritan Console(RC) 또는 Multi-Platform Client(MPC) 등의 애플리케이션을 사용하여 KVM 또는 네트워크의 직렬 관리 노드를 수정하거나 문제를 해결합니다.

정책 - CC-SG 네트워크 내에서 사용자 그룹의 액세스를 정의합니다. 규정은 사용자 그룹에 적용되며 액세스 날짜 및 시간과 같은 제어 레벨을 판별하기 위한 몇 가지 제어 매개변수를 갖습니다.

노드 - CC-SG 사용자가 액세스할 수 있는 서버, 데스크탑 PC 또는 기타 네트워크 장비와 같은 대상 시스템입니다.

1: 개요

인터페이스 - **Dominion KX2** 연결과 같은 대역외 솔루션 또는 **VNC** 서버와 같은 대역내 솔루션을 통해 노드를 액세스할 수 있는 방법입니다.

노드 그룹 - 사용자가 액세스할 수 있는 정의된 노드 그룹입니다. 그룹의 노드에 대한 액세스를 제어하는 규정을 생성할 때 노드 그룹이 사용됩니다.

포트 - **Raritan** 장치와 노드 간의 연결점입니다. 포트는 **Raritan** 장치에만 존재하며 해당 장치에서 노드까지의 경로를 확인합니다.

SASL(Simple Authentication and Security Layer) - 연결 기반 프로토콜에 인증 지원을 추가하는 방법입니다.

SSH - PuTTY 또는 **OpenSSH** 와 같이 **CC-SG** 에 대한 명령줄 인터페이스를 제공하는 클라이언트입니다. **CC-SG** 명령의 하위 세트만 **SSH** 를 통해 제공되어 장치 및 **CC-SG** 자체를 관리합니다.

사용자 그룹 - 동일 수준의 액세스 및 권한을 공유하는 사용자 세트입니다.

클라이언트 브라우저 요구사항

지원되는 브라우저의 전체 목록은 **Raritan** 지원 웹 사이트의 호환성 매트릭스를 참조하십시오.

다음 여러 방법으로 CC-SG 에 액세스할 수 있습니다.

- 브라우저: CC-SG 는 많은 웹 브라우저를 지원합니다. 지원되는 브라우저의 전체 목록은 Raritan 지원 웹 사이트의 호환성 매트릭스를 참조하십시오.
- 썬 클라이언트: 클라이언트 컴퓨터에서 Java Web Start 썬 클라이언트를 설치할 수 있습니다. 썬 클라이언트는 브라우저-기반 클라이언트와 기능이 동일합니다.
- SSH: 직렬 포트를 통해 연결된 원격 장치는 SSH 를 사용하여 액세스할 수 있습니다.
- 진단 콘솔: 긴급 수리 및 진단만 제공하며, CC-SG를 구성하고 작동하기 위한 브라우저 기반 GUI에 대한 교체는 아닙니다. **진단 콘솔** (p. 231)을 참조하십시오.:

참고: 사용자는 CC-SG 에 액세스하는 동안 브라우저, 썬 클라이언트 및 SSH 를 사용하여 동시에 연결할 수 있습니다.

이 장에서

CC-SG Admin 클라이언트를 통한 브라우저 기반 액세스	5
썬 클라이언트 액세스.....	6
CC-SG Admin 클라이언트	8

CC-SG Admin 클라이언트를 통한 브라우저 기반 액세스

CC-SG Admin 클라이언트는 권한에 따라 관리 및 액세스 작업 모두에 대한 GUI 를 제공하는 Java 기반 클라이언트입니다.

1. 지원되는 인터넷 브라우저를 사용하여 CC-SG의 URL 을 입력한 후 /admin: `https://IP 주소/admin` 을 입력합니다(예: **`https://10.0.3.30/admin`** (`https://10.0.3.30/admin`)).

JRE 비호환성 경고 창이 표시되는 경우 클라이언트 컴퓨터에 적합한 JRE 버전을 선택하여 설치합니다. JRE가 설치되면 이 절차를 다시 시도합니다. JRE 비호환성 (p. 6)을 참조하십시오.

또는 새 JRE 버전을 설치하지 않고 계속할 수 있습니다.

2. 제한된 서비스 계약이 표시되는 경우 계약 텍스트를 읽은 후 제한된 서비스 계약을 읽고 동의합니다 확인란을 선택합니다.
3. 사용자 이름 및 암호를 입력하고 로그인을 클릭합니다.
4. 로그인이 올바르면 CC-SG Admin 클라이언트가 열립니다.

JRE 비호환성

클라이언트 컴퓨터에 JRE 의 최소 요구 버전이 설치되지 않은 경우 CC-SG Admin 클라이언트에 액세스하기 전에 경고 메시지가 표시됩니다. CC-SG 에서 클라이언트 컴퓨터에 필요한 JRE 파일을 찾을 수 없을 경우 JRE 비호환성 경고 창이 열립니다.

JRE 비호환성 경고 창이 표시되면 클라이언트에 적합한 JRE 버전을 선택하여 설치하거나 새 JRE 버전을 설치하지 않고 계속할 수 있습니다.

JRE 가 설치되면 CC-SG 를 다시 실행해야 합니다.

관리자는 권장되는 JRE 최소 버전 및 비호환성 경고 창에 표시되는 메시지를 구성할 수 있습니다. *사용자 정의 JRE 설정 구성* (p. 190)을 참조하십시오.

썬 클라이언트 액세스

CC-SG 썬 클라이언트는 웹 브라우저를 통해 애플릿을 실행하지 않고 Java Web Start 를 시작하여 CC-SG 로 연결할 수 있도록 해줍니다. 브라우저 대신 썬 클라이언트를 사용하면 속도 및 효율성 측면에서 브라우저를 훨씬 능가한다는 장점이 있습니다.

썬 클라이언트 설치

▶ **CC-SG 에서 썬 클라이언트를 다운로드하려면:**

1. 웹 브라우저를 실행하고 다음 URL 을 입력합니다.
http(s)://<IP_address>/install, 여기서 <IP_address>는 CC-SG 의 IP 주소입니다.
 - 보안 경고 메시지가 나타나면 시작을 클릭하여 다운로드를 시작합니다.
 - 클라이언트 컴퓨터에서 Java 버전 1.4 가 실행되고 있는 경우, 데스크탑 통합 창이 열립니다. Java 가 바탕 화면에 썬 클라이언트의 단축 아이콘을 추가하게 하려면 예를 클릭합니다.
2. 다운로드가 완료되면, CC-SG IP 주소를 지정할 수 있는 새 창이 열립니다.
3. 연결 IP 필드에 액세스하려는 CC-SG 장치의 IP 주소를 입력합니다. 연결되면 이 주소는 연결 IP 드롭다운 목록에 표시됩니다. IP 주소는 데스크탑에 저장된 등록정보 파일에 저장됩니다.

4. 안전한 브라우저 연결을 위해 CC-SG 가 구성된 경우, 보안 소켓 층(SSL) 확인란을 선택해야 합니다. 안전한 브라우저 연결을 위해 CC-SG 가 구성되지 않은 경우, 보안 소켓 층(SSL) 확인란을 선택 취소해야 합니다. 이 설정이 올바르지 않으면 씹 클라이언트가 CC-SG 에 연결될 수 없습니다.
5. CC-SG 의 설정을 확인하려면: 관리 > 보안을 선택합니다. 암호화 탭에서 브라우저 연결 프로토콜 옵션을 확인합니다. HTTPS/SSL 옵션이 선택된 경우 씹 클라이언트의 IP 주소 사양 창에서 보안 소켓 층 SSL 확인란을 선택해야 합니다. HTTP 옵션이 선택된 경우 씹 클라이언트의 IP 주소 사양 창에서 보안 소켓 층 SSL 확인란을 선택 취소해야 합니다.
6. 시작을 클릭합니다.
 - 지원되지 않는 Java Runtime Environment(JRE) 버전을 사용하면 경고 메시지가 나타납니다. 프롬프트에 따라 지원되는 Java 버전을 다운로드하거나 현재 설치된 버전을 계속 사용합니다.
7. 로그인 화면이 나타납니다.
8. 제한된 서비스 계약을 활성화한 경우 계약 텍스트를 읽은 다음 제한된 서비스 계약을 읽고 동의합니다 확인란을 선택합니다.
9. 해당 필드에 사용자 이름 및 암호를 입력한 다음 로그인을 클릭합니다.

썩 클라이언트 사용

썩 클라이언트가 설치되면, 사용하는 Java 버전에 따라 두 가지 방법으로 클라이언트 컴퓨터에서 썩 클라이언트에 액세스합니다.

▶ Java 1.4x

클라이언트 컴퓨터가 Java 버전 1.4.x 를 실행하고 썩 클라이언트를 설치할 때 데스크탑 통합 창에서 예를 클릭한 경우, 바탕화면의 단축 아이콘을 더블 클릭하여 썩 클라이언트를 시작하고 CC-SG 에 액세스할 수 있습니다.

단축 아이콘이 없다면, 언제든지 생성할 수 있습니다. 클라이언트 컴퓨터에서 AMcc.jnlp 를 검색하고 해당 파일에 대한 단축 아이콘을 생성합니다.

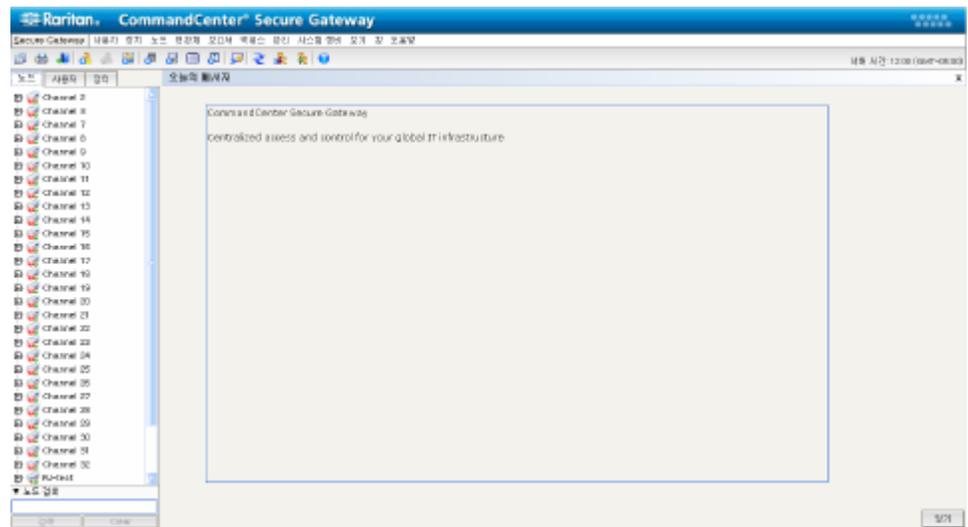
▶ Java 1.5

클라이언트 컴퓨터가 Java 버전 1.5 를 실행할 경우 다음을 수행할 수 있습니다.

- Java 제어판의 Java 애플리케이션 캐시 뷰어(Cache Viewer)에서 썩 클라이언트를 시작합니다.
- Java 제어판의 Java 애플리케이션 캐시 뷰어(Cache Viewer)를 사용하여 데스크탑에서 썩 클라이언트를 위한 단축 아이콘을 설치합니다.

CC-SG Admin 클라이언트

로그인이 올바르면 CC-SG Admin 클라이언트가 나타납니다.



- **노드 탭:** 알려진 모든 대상 노드를 트리 보기에 표시하려면 노드 탭을 클릭합니다. 노드 프로필을 보려면 노드를 클릭합니다. 인터페이스는 상위 노드에서 그룹화되어 있습니다. 트리를 확장하거나 축소하려면 +와 - 기호를 클릭합니다. 인터페이스를 마우스 오른쪽 버튼으로 클릭하고 연결을 선택하여 해당 인터페이스에 연결합니다. 노드 이름(영문자) 또는 노드 상태(사용 가능, 사용 중, 사용 불가)를 기준으로 노드를 정렬할 수 있습니다. 트리 보기를 마우스 오른쪽 버튼으로 클릭하고 노드 정렬 옵션을 선택한 다음 노드 이름별 또는 노드 상태별을 선택합니다.
- **사용자 탭:** 사용자 탭을 클릭하여 등록된 모든 사용자 및 그룹을 트리 보기에 표시합니다. 트리를 확장하거나 축소하려면 +와 - 기호를 클릭합니다.
- **장치 탭:** 장치 탭을 클릭하여 알려진 모든 Raritan 장치를 트리 보기에 표시합니다. 장치 유형에 따라 각각 다른 아이콘이 있습니다. 포트는 상위 장치에서 그룹화되어 있습니다. 트리를 확장하거나 축소하려면 +와 - 기호를 클릭합니다. 포트 프로필을 보려면 포트를 클릭합니다. 포트를 마우스 오른쪽 버튼으로 클릭하고 연결을 선택하여 해당 포트에 연결합니다. 포트 이름(영문자) 또는 포트 상태(사용 가능, 사용 중, 사용 불가)를 기준으로 포트를 정렬할 수 있습니다. 트리 보기를 마우스 오른쪽 버튼으로 클릭하고 포트 정렬 옵션을 선택한 다음 노드 이름별 또는 노드 상태별을 선택합니다.
- **빠른 명령 도구모음:** 이 도구모음은 자주 사용하는 명령을 실행하기 위한 단축 버튼을 제공합니다.
- **작동 및 구성 메뉴모음:** 이러한 메뉴에는 CC-SG 를 작동하고 구성하기 위한 명령이 포함되어 있습니다. 노드, 사용자 및 장치 선택 탭에서 아이콘을 마우스 오른쪽 버튼으로 클릭하여 이 명령 중 일부에 액세스할 수도 있습니다. 표시되는 메뉴와 메뉴 항목은 사용자 액세스 권한에 따라 결정됩니다.
- **서버 시간:** 구성 관리자의 CC-SG에 구성되어 있는 현재 시간 및 시간대입니다. 이 시간은 작업 관리자에서 작업을 예약할 때 사용됩니다. **작업 관리자** (p. 209)를 참조하십시오. 이 시간은 클라이언트에서 사용하는 시간과 다를 수 있습니다.

먼저 CC-SG 에 로그인하여 IP 주소를 확인하고 CC-SG 서버 시간을 설정한 다음 펌웨어 및 설치된 애플리케이션 버전을 확인합니다. 펌웨어 및 애플리케이션을 업그레이드해야 할 수도 있습니다.

최초 구성을 완료하면 설정 안내서로 진행합니다. **설정 안내서를 사용하여 CC-SG 구성** (p. 14)을 참조하십시오.

이 장에서

IP 주소 확인	10
CC-SG 서버 시간 설정	10
호환성 매트릭스 확인	12
애플리케이션 버전 확인 및 업그레이드	12

IP 주소 확인

1. 관리 > 구성을 선택합니다.
2. 네트워크 설정 탭을 클릭합니다.
3. 네트워크 설정이 올바른지 확인하거나 필요한 경우 네트워크 설정을 변경합니다. **네트워크 설정 정보** (p. 179)를 참조하십시오. 옵션입니다.
4. 구성 업데이트를 클릭하여 변경 사항을 제출합니다.
5. 설정을 확인하고 CC-SG 를 다시 시작하려면 지금 다시 시작을 클릭합니다.

CC-SG 서버 시간 설정

장치 관리 기능에 신뢰성을 제공하려면 CC-SG 의 시간 및 날짜가 정확하게 유지되어야 합니다.

중요: 시간/날짜 구성은 작업 관리자에서 작업을 예약할 때 사용됩니다. **작업 관리자** (p. 209)를 참조하십시오. 클라이언트 PC에서 설정된 시간은 CC-SG에서 설정된 시간과 다를 수 있습니다.

비슷한 권한을 갖는 CC 슈퍼 사용자 및 사용자만 시간 및 날짜를 구성할 수 있습니다.

클러스터 구성에서는 시간대 변경을 사용할 수 없습니다.

▶ **CC-SG 서버 시간 및 날짜를 구성하려면:**

1. 관리 > 구성을 선택합니다.
2. 시간/날짜 탭을 클릭합니다.
 - a. 날짜와 시간을 수동으로 설정하려면 다음을 수행하십시오.
 - 날짜 - 드롭다운 화살표를 클릭하여 월을 선택하고 위로 및 아래로 화살표를 사용하여 연도를 선택한 다음 달력 영역에서 일을 클릭합니다.
 - 시간 - 위로 및 아래로 화살표를 사용하여 시, 분 및 초를 설정한 후 시간대 드롭다운 화살표를 클릭하여 CC-SG 가 작동하는 시간대를 선택합니다.
 - a. NTP 를 통해 시간 및 날짜를 설정하려면 다음을 수행하십시오. 창 맨 아래에 있는 네트워크 시간 프로토콜 활성화 확인란을 선택한 다음 해당 필드에 기본 NTP 서버 및 보조 NTP 서버의 IP 주소를 입력합니다.

참고: 네트워크 시간 프로토콜(NTP)은 연결된 컴퓨터의 날짜 및 시간 데이터를 참조 NTP 서버와 동기화하는 데 사용되는 프로토콜입니다. CC-SG 가 NTP 로 구성된 경우 CC-SG 는 공개적으로 사용 가능한 NTP 참조 서버와 해당 시간을 동기화하여 정확하고 일정한 시간을 유지할 수 있습니다.

3. 구성 업데이트를 클릭하여 CC-SG 에 시간 및 날짜 변경 사항을 적용합니다.
4. 새로 고침을 클릭하여 현재 시간 필드에 새 서버 시간을 다시 로드합니다.

시스템 정비 > 다시 시작을 선택하여 CC-SG 를 다시 시작합니다.

호환성 매트릭스 확인

호환성 매트릭스는 현재 버전의 CC-SG 와 호환 가능한 Raritan 장치의 펌웨어 버전 및 애플리케이션의 소프트웨어 버전을 나열합니다. CC-SG 는 장치를 추가하고 장치 펌웨어를 업그레이드하거나 사용할 애플리케이션을 선택할 때마다 이 데이터에 대해 확인합니다. 펌웨어 또는 소프트웨어 버전이 호환되지 않는 경우 CC-SG 는 계속 진행하기 전에 사용자에게 경고하는 메시지를 표시합니다. CC-SG 의 각 버전은 Raritan 장치를 출시할 때 현재 및 이전 펌웨어 버전만 지원합니다. Raritan 지원 웹 사이트에서 호환성 매트릭스를 볼 수도 있습니다.

▶ **호환성 매트릭스를 확인하려면:**

- 관리 > 호환성 매트릭스를 선택합니다.

애플리케이션 버전 확인 및 업그레이드

Raritan Console(RC) 및 Raritan Remote Client(RRC)와 같은 CC-SG 애플리케이션을 확인 및 업그레이드합니다.

▶ **애플리케이션 버전을 확인하려면:**

1. 관리 > 애플리케이션을 선택합니다.
2. 목록에서 애플리케이션 이름을 선택합니다. 버전 필드의 번호를 메모합니다. 일부 애플리케이션은 버전 번호를 자동으로 표시하지 않습니다.

▶ **애플리케이션을 업그레이드하려면:**

애플리케이션이 최신 버전이 아닌 경우 애플리케이션을 업그레이드해야 합니다. Raritan 웹 사이트에서 애플리케이션 업그레이드 파일을 다운로드할 수 있습니다. 지원되는 애플리케이션 버전의 전체 목록은 Raritan 지원 웹 사이트의 호환성 매트릭스를 참조하십시오.

애플리케이션을 업그레이드하기 전에 정비 모드를 시작하는 것이 좋습니다. **정비 모드 시작** (p. 162)을 참조하십시오.

1. 클라이언트 PC 에 애플리케이션 파일을 저장합니다.
2. 애플리케이션 이름 드롭다운 화살표를 클릭하고 목록에서 업그레이드해야 하는 애플리케이션을 선택합니다. 애플리케이션이 목록에 없을 경우 먼저 추가해야 합니다. **애플리케이션 추가** (p. 176)를 참조하십시오.

3. 찾아보기를 클릭하고 표시된 대화 상자에서 애플리케이션 업그레이드 파일을 찾아 선택한 다음 열기를 클릭합니다.
4. 애플리케이션 이름이 애플리케이션 관리자 화면의 새 애플리케이션 파일 필드에 표시됩니다.
5. 업로드를 클릭합니다. 진행률 창이 새로운 애플리케이션이 업로드 중임을 표시합니다. 완료되면 새 창에 애플리케이션이 **CC-SG** 데이터베이스에 추가되었고 사용할 수 있다는 내용이 표시됩니다.
6. 버전 필드가 자동으로 업데이트되지 않을 경우 버전 필드에 새 버전 번호를 입력합니다. 일부 애플리케이션의 경우 버전 필드가 자동으로 업데이트됩니다.
7. 업데이트를 클릭합니다.

*참고: 업그레이드 동안 로그인한 사용자는 새 버전의 애플리케이션이 실행하기 위해 **CC-SG** 를 로그아웃한 다음 다시 로그인해야 합니다.*

네트워크 구성이 완료되면 설정 안내서가 초기 CC-SG 구성 작업을 완료할 수 있는 간단한 방법을 제공합니다. 설정 안내서 인터페이스는 연관체를 정의하고 장치를 검색하여 CC-SG에 추가하고 장치 그룹 및 노드 그룹을 생성하며 사용자 그룹을 생성하고 사용자 그룹에 규정 및 권한을 지정하며 사용자를 추가하는 프로세스를 수행하도록 도와줍니다. 설정 안내서를 완료하면 항상 개별적으로 구성을 편집할 수 있습니다.

설정 안내서는 다음 네 개의 작업으로 나누어집니다.

- **연관체** - 장비를 구성하기 위해 사용할 범주 및 요소를 정의합니다. *설정 안내서의 연관체* (p. 15)를 참조하십시오.
- **장치 설정** - 네트워크에서 장치를 검색하여 CC-SG에 추가합니다. 장치 포트를 구성합니다. *장치 설정* (p. 15)을 참조하십시오.
- **그룹 생성** - CC-SG가 관리하는 관리하는 장치 및 노드들 그룹으로 분류하고 각 그룹에 대한 전체 액세스 규정을 생성합니다. *그룹 생성* (p. 17)을 참조하십시오.
- **사용자 관리** - CC-SG에 사용자 및 사용자 그룹을 추가하고 CC-SG 내에서 그리고 장치 및 노드에 대한 사용자 액세스를 제어할 규정 및 권한을 선택합니다. *사용자 관리* (p. 20)를 참조하십시오.

이름 길이에 대한 CC-SG의 자세한 규정에 대해서는 *명명 규칙* (p. 294)을 참조하십시오.

이 장에서

설정 설명서를 사용하기 전에	14
설정 안내서의 연관체.....	15
장치 설정.....	15
그룹 생성.....	17
사용자 관리.....	20

설정 설명서를 사용하기 전에

CC-SG 구성을 시작하기 전에 시스템 구성을 완료해야 합니다.

- IP 주소를 할당하여 Dominion 시리즈 및 IP-Reach 어플라이언스(직렬 및 KVM 장치 모두)를 구성하고 설치합니다.

설정 안내서의 연관체

범주 및 요소 생성

▶ **설정 안내서에서 범주 및 요소를 생성하려면:**

1. 설정 안내서 창에서 연관체를 클릭한 다음 왼쪽 패널의 범주 생성을 클릭하여 범주 생성 패널을 엽니다.
2. 범주 이름 필드에 장비를 구성할 범주의 이름을 입력합니다(예: "위치").
3. 적용 대상 필드에 장치, 노드 또는 두 가지 모두에 범주를 사용할 것인지 여부를 나타낼 수 있습니다. 적용 대상 드롭다운 메뉴를 클릭한 다음 목록에서 값을 선택합니다.
4. 요소 표에서 범주 내의 요소 이름을 입력합니다(예: "Raritan US").
 - 새 행 추가 아이콘을 클릭하여  요소 표에 행을 추가합니다.
 - 요소를 삭제하려면 행을 선택한 다음 행 삭제 아이콘을 클릭합니다 .
5. 요소 표에 범주 내의 요소를 모두 추가할 때까지 이 단계를 반복합니다.
6. 다른 범주를 생성하려면 적용을 클릭하여 이 범주를 저장한 다음 이 섹션의 단계를 반복하여 범주를 추가합니다. **옵션입니다.**
7. 범주 및 요소 생성을 완료하면 확인을 클릭합니다. 연관체 요약 패널은 생성한 범주 및 요소의 목록을 표시합니다.
8. 다음 작업인 장치 설정을 시작하려면 계속을 클릭합니다. 다음 섹션의 단계를 따릅니다.

장치 설정

설정 안내서의 두 번째 작업은 장치 설정입니다. 장치 설정을 사용하여 네트워크에 있는 장치를 검색하고 CC-SG에 해당 장치를 추가할 수 있습니다. 장치를 추가할 때 장치와 연관시킬 범주당 요소 하나를 선택할 수 있습니다.

중요: CC-SG 구성 중 다른 사용자가 장치에 로그인되지 않았는지 확인하십시오.

장치 검색 및 추가

연관체 작업을 마친 후 계속을 클릭하면 장치 검색 패널이 열립니다. 장치 설정을 클릭한 다음 왼쪽 패널에 있는 안내된 작업 트리 보기에서 장치 검색을 클릭하여 장치 검색 패널을 열 수도 있습니다.

▶ 설정 안내서에서 장치를 검색하고 추가하려면:

1. 발신 주소 및 수신 주소 필드에 장치를 검색할 IP 주소 범위를 입력합니다.
2. 마스크 필드에 장치를 검색할 서브넷 마스크를 입력합니다.
3. 지정한 범위 내에서 검색할 장치 유형을 장치 유형 목록에서 선택합니다. 여러 장치 유형을 선택하려면 **Ctrl** 키를 누른 상태에서 장치 유형을 클릭합니다.
4. **CC-SG** 가 있는 동일한 서브넷에서 장치를 검색하고 있는 경우 방송 검색을 클릭합니다. 모든 서브넷에서 장치를 검색하려면 방송 검색 확인란을 선택 취소합니다.
5. 검색을 클릭합니다.
6. 검색이 완료되면 확인 메시지가 표시됩니다. 확인을 클릭합니다.
7. **CC-SG** 가 지정한 주소 범위에서 지정한 유형의 장치를 검색하면 장치 검색 패널의 아래쪽 섹션에 있는 표에 장치가 표시됩니다. 패널 맨 위에 있는 검정색 화살표를 클릭하여 맨 위 섹션을 숨기면 패널의 아래쪽 섹션에 있는 검색 결과의 보기를 확장할 수 있습니다.
8. 검색된 장치의 표에서 **CC-SG** 에 추가할 장치를 선택한 다음 추가를 클릭합니다. 장치 추가 패널이 열립니다. 장치 추가 패널은 추가하고 있는 장치의 유형에 따라 약간 다릅니다.
9. 해당 필드에 새 정보를 입력하여 장치 이름 및 설명을 변경할 수 있습니다.
10. **CC-SG** 에 추가할 장치를 준비할 때 지정한 IP 주소가 장치 IP 또는 호스트 이름 필드에 표시되는지 확인하거나 필요한 경우 해당 필드에 정확한 주소를 입력합니다.
11. TCP 포트 번호 필드가 장치 유형에 따라 자동으로 입력됩니다.
12. 해당 필드에 **CC-SG** 에 추가할 장치를 준비할 때 생성한 사용자 이름 및 암호를 입력합니다.
13. 하트비트 시간 제한 필드에 장치와 **CC-SG** 사이의 시간 제한이 발생하기 전까지 경과하는 시간(초)을 입력합니다.

14. Dominion SX 장치를 추가할 경우 장치에 대한 로컬 액세스를 허용하려면 직접 장치 액세스 허용 확인란을 선택합니다. 장치에 대한 로컬 액세스를 허용하지 않으려면 로컬 액세스: 허용 확인란을 선택 취소합니다.
15. 전원 탭 장치를 수동으로 추가하는 경우 포트 수 드롭다운 화살표를 클릭하고 전원 탭에 포함된 콘센트 수를 선택합니다.
16. IPMI 서버를 추가하는 경우 해당 필드에 가용성을 확인하는데 사용되는 간격 및 IPMI 서버에 구성되어 있는 사항과 일치해야 하는 인증 방법을 입력합니다.
17. 장치에 사용 가능한 모든 포트를 구성하려면 모든 포트 구성 확인란을 선택합니다. CC-SG 는 장치의 모든 포트를 CC-SG 에 추가하고 각 포트에 대한 노드를 생성합니다.
18. 패널의 아래쪽에 있는 장치 연관체 섹션에서 장치에 지정할 각 범주에 해당하는 요소 열의 드롭다운 화살표를 클릭한 다음 목록에서 장치와 연관시킬 요소를 선택합니다.
19. 요소를 장치 및 장치에 연결된 노드에 적용하려면 노드에 적용 확인란을 선택합니다.
20. 다른 장치를 추가하고자 할 경우 적용을 클릭하여 이 장치를 저장하고 이 단계를 반복합니다. **옵션입니다.**
21. 장치 추가를 완료하면 확인을 클릭합니다. 장치 요약 패널은 추가한 장치의 목록을 표시합니다.
22. 다음 작업인 그룹 생성을 시작하려면 계속을 클릭합니다. 다음 섹션의 단계를 따릅니다.

그룹 생성

설정 안내서의 세 번째 작업은 그룹 생성입니다. 그룹 생성을 사용하여 장치 그룹과 노드 그룹을 정의하고 각 그룹에 포함된 장치 또는 노드 세트를 지정할 수 있습니다. 관리자는 각 장치나 노드를 개별적으로 관리하는 대신 비슷한 장치와 노드 그룹을 관리하여 시간을 절약할 수 있습니다.

장치 그룹 및 노드 그룹 추가

▶ **설정 안내서에서 장치 그룹 및 노드 그룹을 추가하려면:**

1. 장치 설정 작업을 마친 후 계속을 클릭하면 장치 그룹 관리자 패널이 열립니다. 그룹 생성을 클릭한 다음 왼쪽 패널에 있는 안내된 작업 트리 보기에서 장치 그룹 추가를 클릭하여 장치 그룹 관리자 패널을 열 수 있습니다.

2. 그룹 이름 필드에 생성할 장치 그룹의 이름을 입력합니다.
3. 그룹에 장치를 추가할 수 있는 두 방법은 장치 선택 및 장치 설명을 선택하는 것입니다. 장치 선택 탭을 사용하면 사용 가능한 장치의 목록에서 장치를 선택하여 그룹에 지정할 장치를 선택할 수 있습니다. 장치 설명 탭을 사용하면 장치를 설명하는 규칙을 지정할 수 있으며 매개변수가 해당 규칙을 따르는 장치가 그룹에 추가됩니다.

장치 선택

- a. 장치 그룹 추가 패널에서 장치 선택 탭을 클릭합니다.
- b. 사용 가능 목록에서 그룹에 추가할 장치를 선택한 다음 추가를 클릭하여 선택 목록으로 장치를 이동합니다. 선택 목록의 장치가 그룹에 추가됩니다.
 - 그룹에서 장치를 제거하려면 선택 목록에서 장치 이름을 선택한 다음 제거를 클릭합니다.
 - 사용 가능 또는 선택 목록에서 장치를 검색할 수 있습니다. 목록 아래의 필드에 검색 용어를 입력한 다음 이동을 클릭합니다.

장치 설명

- a. 장치 그룹 추가 패널에서 장치 설명 탭을 클릭합니다. 장치 설명 탭에서 그룹에 지정할 장치를 설명하는 규칙 표를 생성합니다.
 - b. 새 행 추가 아이콘을 클릭하여  표에 행을 추가합니다.
 - c. 각 열에 생성된 셀을 더블 클릭하여 드롭다운 메뉴를 활성화합니다. 각 목록에서 사용할 규칙 구성요소를 선택합니다.
1. 항상 제어 권한을 사용하여 그룹에 있는 모든 노드와 장치에 대한 액세스를 허용하는 이 장치 그룹의 규정을 생성하려면 그룹의 전체 액세스 규정 생성 확인란을 선택합니다.
 2. 다른 장치 그룹을 추가하려면 적용을 클릭하여 이 그룹을 저장하고 이 단계를 반복합니다. **옵션입니다.**
 3. 장치 그룹 추가를 완료하면 확인을 클릭합니다. 노드 그룹 관리자 패널이 열립니다. 그룹 생성을 클릭한 다음 왼쪽 패널에 있는 안내된 작업 트리 보기에서 노드 그룹 추가를 클릭하여 노드 그룹 관리자 패널을 열 수 있습니다.
 4. 그룹 이름 필드에 생성할 노드 그룹의 이름을 입력합니다.

5. 그룹에 노드를 추가할 수 있는 두 가지 방법은 노드 선택 및 노드 설명입니다. 노드 선택 섹션을 사용하면 사용 가능한 노드의 목록에서 노드를 선택하여 그룹에 지정할 노드를 선택할 수 있습니다. 노드 설명 섹션을 사용하면 노드를 설명하는 규칙을 지정할 수 있으며 매개변수가 해당 규칙을 따르는 노드가 그룹에 추가됩니다.

노드 선택

- a. 노드 그룹 추가 패널에서 노드 선택 탭을 클릭합니다.
- b. 사용 가능 목록에서 그룹에 추가할 노드를 선택한 다음 추가를 클릭하여 선택 목록으로 노드를 이동합니다. 선택 목록의 노드가 그룹에 추가됩니다.
- c. 그룹에서 노드를 제거하려면 선택 목록에서 노드 이름을 선택한 다음 제거를 클릭합니다.
- d. 사용 가능 또는 선택 목록에서 노드를 검색할 수 있습니다. 목록 아래의 필드에 검색 용어를 입력한 다음 이동을 클릭합니다.

노드 설명

- a. 노드 그룹 추가 패널에서 노드 설명 탭을 클릭합니다. 노드 설명 탭에서 그룹에 지정할 노드를 설명하는 규칙 표를 생성합니다.
 - b. 새 행 추가 아이콘을 클릭하여  표에 행을 추가합니다.
 - c. 각 열에 생성된 셀을 더블 클릭하여 드롭다운 메뉴를 활성화합니다. 각 목록에서 사용할 규칙 구성요소를 선택합니다. **액세스 제어 규정** (p. 115)을 참조하십시오.
 - d. 항상 제어 권한을 사용하여 그룹에 있는 모든 노드에 대한 액세스를 허용하는 이 노드 그룹의 규정을 생성하려면 그룹의 전체 액세스 규정 생성 확인란을 선택 취소합니다.
 - e. 다른 노드 그룹을 추가하려면 적용을 클릭하여 이 그룹을 저장하고 이 단계를 반복합니다. **옵션입니다.**
1. 노드 그룹 추가를 완료하면 확인을 클릭합니다. 그룹 요약 패널은 추가한 그룹의 목록을 표시합니다.
 2. 다음 작업인 사용자 관리를 시작하려면 계속을 클릭합니다. 다음 섹션의 단계를 따릅니다.

사용자 관리

설정 안내서의 네 번째 작업은 사용자 관리입니다. 사용자 관리를 사용하여 사용자 그룹의 액세스와 활동을 제어하는 권한 및 규정을 선택할 수 있습니다. 권한은 사용자 그룹의 구성원이 CC-SG에서 수행할 수 있는 활동을 지정합니다. 규정은 사용자 그룹의 구성원이 보고 수정할 수 있는 장치와 노드를 지정합니다. 규정은 범주와 요소를 기반으로 합니다. 사용자 그룹을 생성하면 개별 사용자를 정의하고 사용자 그룹에 추가할 수 있습니다.

사용자 그룹 및 사용자 추가

그룹 생성 작업을 마친 후 계속을 클릭하면 사용자 그룹 추가 패널이 열립니다. 사용자 관리를 클릭한 다음 왼쪽 패널에 있는 안내된 작업 트리 보기에서 사용자 그룹 추가를 클릭하여 사용자 그룹 추가 패널을 열 수도 있습니다.

▶ **설정 안내서에서 사용자 그룹 및 사용자를 추가하려면:**

1. 사용자 그룹 이름 필드에 생성할 사용자 그룹의 이름을 입력합니다. 사용자 그룹 이름은 최대 32자를 포함할 수 있습니다.
2. 설명 필드에 사용자 그룹의 설명을 입력합니다.
3. 권한 탭을 클릭한 다음 사용자 그룹에 지정할 권한 또는 CC-SG 활동에 유형에 해당하는 확인란을 선택합니다.
4. 노드 액세스 섹션에서 사용자 그룹이 대역내 및 대역외 노드와 전원 관리 기능에 액세스할 수 있는지 여부를 지정할 수 있습니다. 그룹에 지정할 액세스 유형에 해당하는 확인란을 선택합니다.
5. 규정 탭을 클릭합니다.
6. 모든 규정 목록에서 사용자 그룹에 지정할 규정을 선택한 다음 추가를 클릭하여 선택된 규정 목록으로 규정을 이동합니다. 선택된 규정 목록의 규정이 사용자 그룹에 지정됩니다. 이 단계를 반복하여 사용자 그룹에 규정을 추가합니다.
7. 사용자 그룹에서 규정을 제거하려면 선택된 규정 목록에서 규정 이름을 선택한 다음 제거를 클릭합니다.
8. 인증된 사용자를 Active Directory 모듈과 원격으로 연관시키려면 Active Directory 연관체 탭을 클릭합니다. 사용자 그룹과 연관시키려는 각 Active Directory 모듈에 해당하는 확인란을 선택합니다.

9. 다른 사용자 그룹을 추가하려면 적용을 클릭하여 이 그룹을 저장하고 단계를 반복합니다. **옵션입니다.**
10. 사용자 그룹 추가를 완료하면 확인을 클릭합니다. 사용자 추가 패널이 열립니다. 사용자 관리를 클릭한 다음 왼쪽 패널에 있는 안내된 작업 트리 보기에서 사용자 추가를 클릭하여 사용자 추가 패널을 열 수도 있습니다.
11. 사용자 이름 필드에서 추가할 사용자가 CC-SG 에 로그인하는 데 사용할 이름을 입력합니다.
12. 사용자가 CC-SG 에 로그인할 수 있도록 하려면 로그인 활성 확인란을 선택합니다.
13. TACACS+, RADIUS, LDAP 또는 AD 와 같은 외부 서버에서 사용자를 인증하려는 경우에만 원격 인증 확인란을 선택합니다. 원격 인증을 사용하는 경우 암호가 필요 없습니다. 원격 인증을 선택하면 새 암호 및 새 암호 재입력 필드가 비활성화됩니다.
14. 새 암호 및 새 암호 재입력 필드에 사용자가 CC-SG 에 로그인하는 데 사용할 암호를 입력합니다.
15. 사용자가 나중에 로그인할 때 강제로 지정된 암호를 변경하게 하려면 다음 로그인에서 암호 변경 실행 확인란을 선택합니다.
16. 사용자가 강제로 암호를 변경하는 빈도를 지정하려면 주기적 암호 변경 실행 확인란을 선택합니다.
17. 만료 기간(일) 필드에 사용자가 강제로 암호를 변경하기 전에 같은 암호를 사용할 수 있는 기간(일)을 입력합니다.
18. 이메일 주소 필드에 사용자의 이메일 주소를 입력합니다.
19. 사용자 그룹 드롭다운 화살표를 클릭하고 목록에서 사용자를 지정할 사용자 그룹을 선택합니다.
20. 다른 사용자를 추가하려면 적용을 클릭하여 이 사용자를 저장한 다음 이 섹션의 단계를 반복하여 사용자를 추가합니다.
21. 사용자 추가를 완료하면 확인을 클릭합니다. 사용자 요약 패널은 추가한 사용자 그룹 및 사용자의 목록을 표시합니다. **옵션입니다.**

이 장에서

연관체 정보.....	22
연관체 관리자.....	24

연관체 정보

연관체를 설정하여 CC-SG가 관리하는 장비를 구성하는 데 도움을 줄 수 있습니다. 각 연관체에는 최상위 조직 그룹인 범주와 범주의 하위 집합인 관련 요소가 있습니다. 예를 들어, 미국, 아시아 태평양 및 유럽의 데이터 센터에서 대상 서버를 관리하는 Raritan 장치를 가지고 있을 수 있습니다. 이 장비를 위치별로 구성하는 연관체를 설정할 수 있습니다. 그런 다음 CC-SG를 사용자 정의하여 CC-SG 인터페이스에 선택한 범주-위치 및 그 연관된 요소(예: 미국, 아시아 태평양 및 유럽)에 따라 Raritan 장치 및 노드를 표시할 수 있습니다. CC-SG를 사용자 정의하여 원하는 대로 서버를 구성하고 표시할 수 있습니다.

연관체 용어

- 연관체 - 범주, 범주의 요소 그리고 노드 및 장치 사이의 관계입니다.
- 범주 - 요소라는 세트 값을 포함하는 변수입니다. 범주의 예로는 위치로서 "미국" 및 "아시아 태평양"과 같은 요소를 가질 수 있습니다. 범주의 또 다른 예로는 "OS 유형"이 있으며 "Windows", "Unix" 또는 "Linux"와 같은 요소를 가질 수 있습니다.
- 요소 - 범주의 값. 예를 들어, "미국" 요소는 "위치" 범주에 속합니다.

연관체--범주 및 요소 정의

Raritan 장치 및 노드는 범주 및 요소로 구성됩니다. 각 범주/요소 쌍은 장치나 노드 또는 둘 다에 지정됩니다. 따라서 CC-SG 에 Raritan 장치를 추가하기 전에 범주 및 요소를 정의해야 합니다.

범주는 유사한 요소의 그룹입니다. 예를 들어, Raritan 장치를 위치별로 그룹화하려면 New York, Philadelphia 및 New Orleans 와 같은 요소 세트를 포함하는 위치라는 범주를 정의합니다.

또한 규정은 범주 및 요소를 사용하여 서버에 대한 사용자 액세스를 제어합니다. 예를 들어, 위치/New York 과 같은 범주/요소 쌍은 New York 의 서버에 대한 사용자 액세스를 제어하는 규정을 생성하는 데 사용할 수 있습니다.

범주 및 요소의 일반적인 연관체 구성의 다른 예는 다음과 같습니다.

범주	요소
위치	New York City, Philadelphia, New Orleans
OS 유형	Unix, Windows, Linux
부서	영업부, IT, 엔지니어링

연관체 구성은 서버/포트 조직 목표 및 사용자 액세스 목표를 달성하기 위해 간단하게 되어 있어야 합니다. 노드는 범주의 단일 요소에만 지정될 수 있습니다. 예를 들어, 대상 서버는 위의 OS 유형 범주의 Windows 요소와 Unix 요소 모두에 지정될 수 없습니다.

서버가 유사하고 임의로 구성해야 하는 경우 시스템을 구성하는 유용한 방법은 다음과 같습니다.

범주	요소
usergroup1	usergroup1node
usergroup2	usergroup2node
usergroup3	usergroup3node

CC-SG 에 장치 및 노드를 추가하면 사전 정의된 범주 및 요소에 연결됩니다. 노드 및 장치 그룹을 생성하고 이 그룹에 규정을 지정할 경우 범주 및 요소를 사용하여 각 그룹에 속하는 노드 및 장치를 정의합니다.

연관체 생성 방법

연관체를 생성할 수 있는 방법은 설정 안내서 및 연관체 관리자입니다.

- 설정 안내서는 자동화된 인터페이스로 많은 구성 작업을 결합합니다. 설정 안내서는 초기 **CC-SG** 구성에 권장됩니다. 설정 안내서를 완료하면 항상 개별적으로 구성을 편집할 수 있습니다. **설정 안내서를 사용하여 CC-SG 구성** (p. 14)을 참조하십시오.
- 연관체 관리자는 연관체와의 상호 작용만 허용하며 구성 작업을 자동화하지 않습니다. 연관체 관리자를 사용하여 설정 안내서를 사용한 후 연관체를 편집할 수도 있습니다. **연관체 관리자** (p. 24)를 참조하십시오.

연관체 관리자

연관체 관리자를 사용하여 범주 및 요소를 추가, 편집 또는 삭제할 수 있습니다.

범주 추가

▶ **범주를 추가하려면:**

1. 연관체 > 연관체를 선택합니다.
2. 추가를 클릭합니다. 범주 추가 창이 열립니다.
3. 범주 이름 필드에 범주 이름을 입력합니다. 이름 길이에 대한 **CC-SG** 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.
4. 요소에 대한 데이터 유형을 선택합니다.
 - 값을 텍스트로 읽을 경우 문자열을 선택합니다.
 - 값을 숫자로 읽을 경우 정수를 선택합니다.
5. 적용 대상 필드에서 다음 중 이 범주의 적용 대상을 선택합니다. 장치, 노드 또는 장치 및 노드.
6. 확인을 클릭하여 새 범주를 생성합니다. 새 범주 이름이 범주 이름 필드에 나타납니다.

범주 편집

문자열 값을 정수 값으로 변경하거나 정수 값을 문자열 값으로 변경할 수 없습니다. 이 유형의 변경이 필요한 경우, 범주를 삭제하고 새 범주를 추가합니다.

▶ 범주를 편집하려면:

1. 연관체 > 연관체를 선택합니다.
2. 범주 이름 드롭다운 화살표를 클릭하고 편집할 범주를 선택합니다.
3. 범주를 편집하려면 화면의 범주 패널에서 편집을 클릭합니다. 범주 편집 창이 열립니다.
4. 범주 이름 필드에 새 범주 이름을 입력합니다.
5. 적용 대상 드롭다운 화살표를 클릭하여 장치, 노드 또는 둘 모두에 이 범주를 적용할 것인지 여부를 변경합니다.
6. 확인을 클릭하여 변경 사항을 저장합니다. 업데이트된 범주 이름이 범주 이름 필드에 나타납니다.

범주 삭제

범주를 삭제하면 해당 범주 내에 생성된 모든 요소가 삭제됩니다. 화면을 새로 고침하거나 사용자가 로그아웃한 후 CC-SG에 다시 로그인하면 삭제된 범주가 노드 또는 장치 트리에 더 이상 나타나지 않습니다.

▶ 범주를 삭제하려면:

1. 연관체 > 연관체를 선택합니다.
2. 범주 이름 드롭다운 화살표를 클릭하고 삭제할 범주를 선택합니다.
3. 범주를 삭제하려면 화면의 범주 패널에서 삭제를 클릭합니다. 범주 삭제 창이 열립니다.
4. 예를 클릭하여 범주를 삭제합니다.

요소 추가

▶ 요소를 추가하려면:

1. 연관체 > 연관체를 선택합니다.

5: 연관체, 범주 및 요소

2. 범주 이름 드롭다운 화살표를 클릭하고 새 요소를 추가할 범주를 선택합니다.
3. 새 행 추가 아이콘을 클릭합니다.
4. 빈 행에 새 요소 이름을 입력합니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오. 요소 이름은 대소문자를 구분합니다.
5. 확인을 클릭하여 변경 사항을 저장합니다.

요소 편집

▶ 요소를 편집하려면:

1. 연관체 > 연관체 관리자를 선택합니다.
2. 범주 이름 드롭다운 화살표를 클릭하고 편집할 요소의 범주를 선택합니다.
3. 범주 요소 목록에서 편집할 요소를 선택하고 범주 요소 패널에서 편집을 클릭합니다. 요소 편집 창이 열립니다.
4. 새로운 요소 값 입력 필드에 새 요소의 이름을 입력합니다. 요소 이름은 대소문자를 구분합니다.
5. 확인을 클릭하여 요소를 업데이트하거나 취소를 클릭하여 창을 닫습니다. 새 요소 이름은 범주 요소 목록에 표시됩니다.

요소 삭제

요소를 삭제하면 모든 연관체에서 해당 요소가 제거되고 연관체 필드는 공백으로 남습니다.

▶ 요소를 삭제하려면:

1. 연관체 > 연관체를 선택합니다.
2. 범주 이름 드롭다운 화살표를 클릭하고 요소를 삭제할 범주를 선택합니다.
3. 요소 목록에서 삭제할 요소를 선택한 다음 행 제거 아이콘을 클릭합니다.
4. 확인을 클릭하여 변경 사항을 저장합니다.

다른 Raritan 장치에 연결된 Raritan 전원 탭 장치를 CC-SG로 연결하려면 **관리된 전원 탭** (p. 56)을 참조하십시오.

참고: iLO/RILOE 장치, IPMI 장치, Dell DRAC 장치, IBM RSA 장치 또는 기타 비 Raritan 장치를 구성하려면 노드 추가 메뉴를 사용하여 이러한 항목을 인터페이스로서 추가합니다. 노드, 노드 그룹 및 인터페이스 (p. 64)를 참조하십시오.

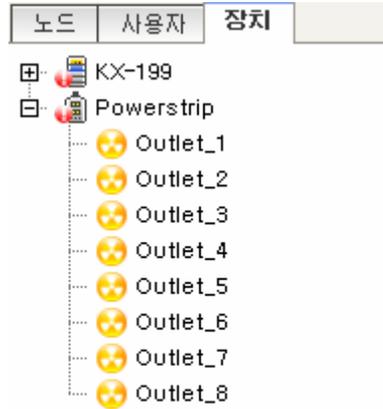
이 장에서

장치 보기.....	28
장치 검색.....	31
장치 검색.....	32
장치 추가.....	33
장치 편집.....	36
전원 탭 장치 또는 Dominion PX 장치 편집.....	36
장치 프로필에 메모 추가.....	37
장치 프로필에 위치 및 연락처 추가.....	37
장치 삭제.....	38
포트 구성.....	38
포트 편집.....	40
포트 삭제.....	41
장치 범주 및 요소 대량 복사.....	42
장치 업그레이드.....	42
장치 구성 백업.....	43
장치 구성 복원.....	44
장치 구성 복사.....	47
장치 다시 시작.....	47
장치 핑.....	48
장치에 대한 CC-SG의 관리 일시 중지.....	48
관리 다시 시작.....	48
장치 전원 관리자.....	49
장치의 관리 페이지 실행.....	49
사용자 연결 해제.....	50
Paragon II 시스템 장치로의 특별 액세스.....	50
장치 그룹 관리자.....	51

장치 보기

장치 탭

CC-SG 관리 아래에 모든 장치를 표시하려면 장치 탭을 클릭합니다.



각 장치의 구성된 포트는 포트가 속한 장치 아래에 중첩됩니다. 구성된 포트가 있는 장치는 옆에 + 기호가 있는 목록에 나타납니다. 포트의 목록을 확장하거나 축소하려면 + 또는 -를 클릭합니다.

장치 및 포트 아이콘

간편한 식별을 위해 KVM, 직렬 및 전원 장치는 장치 트리에서 서로 다른 아이콘을 사용합니다. 장치 또는 포트에 대한 정보를 포함하는 도구 설명을 보려면 장치 트리의 아이콘 위에 마우스 포인터를 갖다 댍니다.

아이콘	의미
	장치 사용 가능
	KVM 포트 사용 가능 또는 연결됨
	KVM 포트 비활성
	직렬 포트 사용 가능
	직렬 포트 사용 불가능

아이콘	의미
	Ghost 포트(Ghosting 모드에 대해서는 Paragon II 사용자 설명서 참조)
	장치 일시 중지
	장치 사용 불가능
	전원 탭
	콘센트 포트

포트 정렬 옵션

구성된 포트는 장치 탭에서 상위 장치 아래에 중첩됩니다. 포트의 정렬 방법을 변경할 수 있습니다. 상태별로 정렬한 포트는 연결 상태 분류 내에서 알파벳순으로 정렬됩니다. 장치도 항상 알파벳순으로 정렬됩니다.

▶ 장치 탭의 포트를 정렬하려면:

1. 장치 > 포트 정렬 옵션을 선택합니다.
2. 이름이나 가용성 상태를 기준으로 영문자 순서로 장치 내의 포트를 정렬하려면 포트 이름별 또는 포트 상태별을 선택합니다.

장치 프로필 화면

장치 탭에서 장치를 클릭하면 선택한 장치에 대한 정보를 표시하는 장치 프로필 화면이 나타납니다.

장치가 작동하지 않는 상태일 경우 장치 프로필 화면의 정보는 읽기 전용입니다. 작동하지 않는 상태의 장치는 삭제할 수 있습니다. **장치 삭제** (p. 38)를 참조하십시오.

장치 프로필에는 장치에 관한 정보를 포함하고 있는 탭이 있습니다.

▶ 연관체 탭

연관체 탭은 노드에 지정된 모든 범주 및 요소를 포함하고 있습니다. 다른 사항을 선택하여 연관체를 변경할 수 있습니다. **연관체, 범주 및 요소** (p. 22)를 참조하십시오.

▶ 위치 & 연락처 탭

위치 & 연락처 탭에는 전화 번호와 같이 장치를 이용할 때 필요한 장치 위치 및 연락처 정보에 대한 정보가 포함됩니다. 새 정보를 입력하여 이 필드의 정보를 변경할 수 있습니다. **장치 프로필에 위치 및 연락처 추가** (p. 37)를 참조하십시오.

▶ 메모 탭

메모 탭에는 사용자가 장치에 대한 메모를 남겨 다른 사용자가 읽을 수 있도록 할 수 있는 도구가 있습니다. 모든 메모는 메모를 추가한 날짜, 사용자 이름 및 사용자의 IP 주소와 함께 탭에 표시됩니다.

장치, 포트 및 노드 관리 권한이 있을 경우 지우기를 클릭하여 노드 프로필에서 모든 메모를 지울 수 있습니다.

장치 프로필에 메모 추가 (p. 37)를 참조하십시오.

분포도 보기

분포도 보기는 구성 내에서 연결되어 있는 모든 어플라이언스의 구조를 표시합니다.

분포도 보기를 닫을 때까지 이 보기는 장치를 선택할 때 일반적으로 나타나는 장치 프로필 화면을 대체합니다.

▶ 분포도 보기를 열려면:

1. 장치 탭을 클릭하고 분포도 보기를 보려는 장치를 선택합니다.

2. 장치 > 장치 관리자 > 분포도 보기를 선택합니다. 선택된 장치에 대한 분포도 보기가 나타납니다.
 - 보기를 확대하거나 축소하려면 + 또는 - 기호를 클릭합니다.

장치 탭에서 옵션을 마우스 오른쪽 버튼으로 클릭합니다.

선택된 장치나 포트에 이용할 수 있는 명령어 메뉴를 표시하기 위해 장치 탭에서 장치나 포트를 마우스 오른쪽 버튼으로 클릭할 수 있습니다.

장치 검색

장치 탭은 트리 내에서 장치를 검색하는 기능을 제공합니다. 검색은 결과로 장치만 반환하고 포트 이름을 포함하지 않습니다. 검색 방법은 내 프로필에서 구성할 수 있습니다. **기본 검색 기본 설정 변경** (p. 112)을 참조하십시오.

▶ 장치를 검색하려면:

- 장치 탭의 아래쪽에서 장치 검색 필드에 검색 문자열을 입력한 다음 ENTER 키를 누릅니다.
- 검색 문자열에는 와일드카드가 지원됩니다. **검색을 위한 와일드카드** (p. 31)를 참조하십시오.

검색을 위한 와일드카드

와일드카드	설명
?	모든 문자를 나타냅니다.
[]	범위 안의 문자를 나타냅니다.
*	0 개 이상의 문자를 나타냅니다.

와일드카드 예제

예	설명
KX?	KX1 및 KXZ 를 찾지만 KX1Z 은 찾지 않습니다.
KX*	KX1, KX, KX1 및 KX1Z 를 찾습니다.
KX[0-9][0-9]T	KX95T, KX66T 는 찾지만 KXZ 및 KX5PT 는 찾지 않습니다.

장치 검색

장치 검색은 네트워크에 있는 모든 장치의 검색을 개시합니다. 검색된 장치가 아직 관리되고 있지 않은 경우 **CC-SG**에 추가할 수 있습니다.

▶ 장치를 검색하려면:

1. 장치 > 장치 검색을 선택합니다.
2. 장치가 검색될 것으로 예상되는 IP 주소의 범위를 발신 주소 및 수신 주소 필드에 입력합니다. 수신 주소가 발신 주소보다 커야 합니다. 적용할 마스크를 범위에 지정합니다. 마스크가 지정되지 않은 경우 방송 주소 **255.255.255.255**가 전송되어 모든 로컬 네트워크에 방송됩니다. 서브넷에서 장치를 검색하려면 마스크를 지정해야 합니다.
3. **CC-SG**가 있는 동일한 서브넷에서 장치를 검색하고 있는 경우 방송 검색을 클릭합니다. 여러 서브넷에 걸쳐 장치를 검색하려면 방송 검색을 지웁니다.
4. 특정 장치 유형을 검색하려면 장치 유형 목록에서 유형을 선택합니다. 기본적으로 모든 장치 유형이 강조 표시됩니다. **CTRL+클릭**을 사용하여 두 개 이상의 장치 유형을 선택합니다.
5. **IPMI** 전원 제어를 제공하는 대상을 찾으려면 **IPMI** 에이전트 포함 확인란을 선택합니다.
6. 검색을 시작하려면 검색을 클릭합니다. 검색하는 동안 언제든지 중지를 클릭하여 검색 프로세스를 중단할 수 있습니다. 검색된 장치가 목록에 나타납니다.
7. **CC-SG**에 한 개 이상의 검색된 장치를 추가하려면 목록에서 장치를 선택하고 추가를 클릭합니다. 장치 추가 화면이 이미 일부 데이터가 입력된 상태로 표시됩니다.
추가할 두 개 이상의 장치를 선택한 경우 화면 아래쪽에 있는 이전 및 건너뛰기를 클릭하여 장치 추가 화면을 통해 추가할 장치를 탐색할 수 있습니다.
8. 장치 추가 페이지는 장치 유형에 따라 다릅니다. **CC-SG**가 검색한 각 장치 유형 추가에 대한 지침을 참조하십시오.
 - **KVM** 또는 직렬 장치의 경우 **KVM 또는 직렬 장치 추가** (p. 33)를 참조하십시오.
 - 전원 탭의 경우 **전원 탭 장치 추가** (p. 35)를 참조하십시오.
 - IP 네트워크의 **Dominion PX** 전원 탭의 경우 **Dominion PX 장치 추가** (p. 35)를 참조하십시오.

9. 검색된 장치를 추가하고 다음 검색된 장치를 계속하려면 적용을 클릭하십시오. 현재 검색된 장치를 추가하고 검색된 장치 추가 프로세스를 중단하려면 확인을 누르십시오.

장치 추가

CC-SG에 장치를 추가해야 포트를 구성하거나 포트에 연결된 노드에 액세스를 제공하는 인터페이스를 추가할 수 있습니다. 장치 추가 화면은 속성을 알고 있고 CC-SG에 제공할 수 있는 장치를 추가하는데 사용됩니다. 추가할 장치를 검색하려면 장치 검색 옵션을 사용합니다. **장치 검색** (p. 32)을 참조하십시오.

다른 Raritan 장치에서 CC-SG로 연결되는 Raritan 전원 탭 장치를 추가할 경우 **관리된 전원 탭** (p. 56)을 참조하십시오.

▶ CC-SG 에 장치 추가:

1. 장치 > 장치 관리자 > 장치 추가를 선택합니다.
2. 장치 유형 드롭다운 화살표를 클릭한 다음 목록에서 추가하고 있는 장치의 유형을 선택합니다. 선택하는 장치 유형에 따라 약간 다른 장치 추가 페이지가 나타납니다.
 - KVM 또는 직렬 장치 추가에 대한 지침은 **KVM 또는 직렬 장치 추가** (p. 33)를 참조하십시오.
 - 전원 탭 장치 추가에 대한 지침은 **전원 탭 장치 추가** (p. 35)를 참조하십시오.
 - Dominion PX 장치 추가에 대한 지침은 **Dominion PX 장치 추가** (p. 35)를 참조하십시오.

KVM 또는 직렬 장치 추가

KVM 및 직렬 장치는 256 비트 AES 암호화를 지원하지만 CC-SG 는 이 수준의 암호화를 지원하지 않습니다. 장치가 기본 암호화 모드인 "자동 감지"로 설정되어 있는지 확인하십시오. 장치는 CC-SG 에서 작동하기 위해 128 비트 수준으로 하향 조정됩니다.

1. 장치 이름 필드에 장치의 이름을 입력합니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.
2. 장치 IP 주소 또는 호스트 이름 필드에 장치 IP 또는 호스트 이름을 입력합니다. 호스트 이름 규칙을 보려면 **용어/약어** (p. 2)를 참조하십시오.
3. TCP 포트 번호 필드에 장치와 통신하는데 사용되는 TCP 통신 포트 번호를 입력합니다. 최대 길이는 5 자리 문자입니다. 대다수 Raritan 장치의 기본 포트 번호는 5000 입니다.

4. 사용자 이름 필드에 이 장치에 로그인할 때 사용한 이름을 입력합니다. 사용자가 관리 액세스 권한을 가지고 있어야 합니다.
5. 암호 필드에 이 장치에 액세스할 때 필요한 암호를 입력합니다. 사용자가 관리 액세스 권한을 가지고 있어야 합니다.
6. 하트비트 시간 제한(초) 필드에 새 장치와 CC-SG 사이의 시간 제한이 발생하기 전에 경과하는 시간(초)을 입력합니다.
7. Dominion SX 장치를 추가할 경우 직접 장치 액세스 허용 확인란을 이용하여 장치에 대한 로컬 포트 액세스를 허용하거나 거부할 수 있습니다. 사용자가 CC-SG에서 관리하는 이 장치에 직접 액세스할 수 있도록 하려면 확인란을 선택합니다.
8. 설명 필드에 이 장치에 대한 간단한 설명을 입력합니다.
옵션입니다.
9. 장치 탭에 이 장치의 모든 포트를 자동으로 추가하고 노드 탭에 이 장치의 각 포트에 대한 노드를 생성하려면 모든 포트 구성 확인란을 선택합니다.
 - 해당 노드 및 포트는 일치하는 이름으로 구성됩니다.
 - 각 포트에 대한 새 노드가 생성되고 대역의 인터페이스가 해당 노드에 대해 생성됩니다.
10. 이 장치 및 이에 연결된 노드를 자세히 설명하고 구성하도록 범주 및 요소의 목록을 구성할 수 있습니다. **연관체, 범주 및 요소 (p. 22)**를 참조하십시오.
11. 나열된 각 범주의 경우 요소 드롭다운 메뉴를 클릭하고 목록에서 장치에 적용할 요소를 선택합니다. 사용하지 않으려는 각 범주의 경우 요소 필드에서 빈 항목을 선택합니다.

장치뿐만 아니라 관련 노드에 요소를 지정하려면 노드에 적용 확인란을 선택합니다.
12. 사용할 범주 또는 요소 값이 나타나지 않는 경우 연관체 메뉴를 통해 추가할 수 있습니다. **연관체, 범주 및 요소 (p. 22)**를 참조하십시오.
13. 이 장치의 구성을 완료하면 적용을 클릭하여 이 장치를 추가하고 장치를 계속 추가할 수 있는 비어 있는 새 장치 추가 화면을 열거나 확인을 클릭하여 새 장치 추가 화면을 계속하지 않고 이 장치를 추가합니다.
14. 장치의 펌웨어 버전이 CC-SG와 호환되지 않는 경우 메시지가 표시됩니다. 예를 클릭하여 CC-SG에 장치를 추가합니다. CC-SG에 장치를 추가한 후 장치 펌웨어를 업그레이드할 수 있습니다. **장치 업그레이드 (p. 42)**를 참조하십시오.

전원 탭 장치 추가

전원 탭 장치를 CC-SG에 추가하는 프로세스는 전원 탭이 물리적으로 연결된 Raritan 장치에 따라 달라집니다. **관리된 전원 탭** (p. 56)을 참조하십시오.

다른 Raritan 장치에 연결되지 않은 Dominion PX를 추가하는 경우 **Dominion PX 장치 추가** (p. 35)를 참조하십시오.

Dominion PX 장치 추가

Dominion PX 장치는 IP 네트워크에만 연결된 전원 탭입니다. Dominion PX 장치는 다른 Raritan 장치에 의해 관리되지 않습니다. 다른 Raritan 장치가 관리하는 전원 탭을 추가하는 절차는 다릅니다. **관리된 전원 탭** (p. 56)을 참조하십시오.

1. 장치 이름 필드에 장치의 이름을 입력합니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.
2. 장치 IP 주소 또는 호스트 이름 필드에 장치 IP 또는 호스트 이름을 입력합니다. 호스트 이름 규칙을 보려면 **용어/약어** (p. 2)를 참조하십시오.
3. 사용자 이름 필드에 이 장치에 로그인할 때 사용한 이름을 입력합니다. 사용자가 관리 액세스 권한을 가지고 있어야 합니다.
4. 암호 필드에 이 장치에 액세스할 때 필요한 암호를 입력합니다. 사용자가 관리 액세스 권한을 가지고 있어야 합니다.

경고: PX 에 대한 암호를 변경할 경우 CC-SG 에서 PX 장치를 삭제하고 다시 추가해야 합니다. CC-SG 는 사용자 이름 또는 암호가 변경될 경우 Dominion PX 장치와의 연결이 끊깁니다.

5. 설명 필드에 이 장치에 대한 간단한 설명을 입력합니다. 옵션입니다.
6. Dominion PX 의 모든 콘센트를 장치 탭에 자동으로 추가하려면 모든 콘센트 구성 확인란을 선택합니다.
7. 이 장치를 자세히 설명하고 구성하도록 범주 및 요소의 목록을 구성할 수 있습니다.
 - 나열된 각 범주의 경우 목록에서 장치에 적용할 요소를 선택합니다. 사용하지 않으려는 각 범주의 경우 요소 필드에서 빈 항목을 선택합니다.
 - 사용할 범주 또는 요소 값이 나타나지 않는 경우 다른 것을 추가할 수 있습니다. **연관제, 범주 및 요소** (p. 22)를 참조하십시오.

- 이 장치의 구성을 완료하면 적용을 클릭하여 이 장치를 추가하고 장치를 계속 추가할 수 있는 비어 있는 새 장치 추가 화면을 열거나 확인을 클릭하여 새 장치 추가 화면을 계속하지 않고 이 장치를 추가합니다.

장치 편집

장치를 편집하여 장치의 이름을 바꾸고 속성을 수정할 수 있습니다.

▶ **장치를 편집하려면:**

- 장치 탭을 클릭하고 편집할 장치를 선택합니다.
- 장치 프로필 화면에서 필요에 따라 매개변수를 변경합니다.
- 확인을 클릭하여 변경 사항을 저장합니다.

전원 탭 장치 또는 Dominion PX 장치 편집

관리된 전원 탭 장치 및 Dominion PX 장치를 편집하여 해당 장치의 이름을 바꾸고 속성을 수정하며 콘센트 구성 상태를 볼 수 있습니다.

▶ **전원 탭 장치를 편집하려면:**

- 장치 탭을 클릭하고 편집할 전원 탭 장치를 선택합니다.
- 이 화면의 해당 필드에 새로운 장치 속성을 입력합니다. 필요한 경우 이 장치와 연관된 범주 및 요소를 편집합니다.
- 콘센트 탭을 클릭하여 이 전원 탭의 모든 콘센트를 봅니다.
- 콘센트가 노드와 연결되어 있는 경우 노드 하이퍼링크를 클릭하여 노드 프로필을 열 수 있습니다.
- 콘센트가 노드와 연결되어 있는 경우 콘센트를 선택한 다음 전원 제어를 클릭하여 연결된 노드에 대한 전원 제어 화면을 열 수 있습니다.
- 콘센트를 제거하려면 콘센트 이름 옆의 확인란을 선택 취소합니다.
- 콘센트를 구성하려면 콘센트 이름 옆의 확인란을 선택합니다.
- 확인을 클릭하여 변경 사항을 저장합니다. 장치가 수정되면 메시지가 표시됩니다.

장치 프로필에 메모 추가

메모 탭에는 다른 사용자가 읽을 수 있도록 장치에 대한 메모를 추가할 수 있습니다. 모든 메모는 메모를 추가한 날짜, 사용자 이름 및 사용자의 IP 주소와 함께 탭에 표시됩니다.

장치, 포트 및 노드 관리 권한이 있을 경우 메모 탭에 표시되는 모든 메모를 지울 수 있습니다.

▶ 장치 프로필에 메모를 추가하려면:

1. 장치 탭에서 장치를 선택합니다. 장치 프로필 페이지가 열립니다.
2. 메모 탭을 클릭합니다.
3. 새 메모 필드에 메모를 입력합니다.
4. 추가를 클릭합니다. 메모가 메모 목록에 표시됩니다.

▶ 모든 메모를 지우려면:

1. 메모 탭을 클릭합니다.
2. 메모 지우기를 클릭합니다.
3. 예를 클릭하여 확인합니다. 모든 메모가 메모 탭에서 삭제됩니다.

장치 프로필에 위치 및 연락처 추가

장치의 위치 및 장치를 관리하거나 사용하는 사람에 대한 연락처 정보에 대한 자세한 내용을 입력합니다.

▶ 장치 프로필에 위치 및 연락처를 추가하려면:

1. 장치 탭에서 장치를 선택합니다. 장치 프로필 페이지가 열립니다.
2. 위치 & 연락처 탭을 클릭합니다.
3. 위치 정보를 입력합니다.
 - 부서: 최대 64 문자입니다.
 - 사이트: 최대 64 문자입니다.
 - 위치: 최대 128 문자입니다.
4. 연락처 정보를 입력합니다.
 - 기본 연락처 이름 및 보조 연락처 이름: 최대 64 문자입니다.
 - 전화 번호 및 핸드폰 번호: 최대 32 문자입니다.

5. 확인을 클릭하여 변경 사항을 저장합니다.

장치 삭제

장치를 삭제하여 CC-SG 관리에서 해당 장치를 제거할 수 있습니다.

중요: 장치를 삭제하면 해당 장치에 대해 구성된 모든 포트가 제거됩니다. 해당 포트와 연관된 모든 인터페이스가 노드에서 제거됩니다. 이러한 노드에 다른 인터페이스가 존재하지 않는 경우 노드도 **CC-SG**에서 제거됩니다.

참고: CC-SG 에서 성공적으로 삭제하려면 먼저 KSX 장치를 일시 중지해야 합니다. KSX 장치를 일시 중지하려면 장치 탭에서 장치를 마우스 오른쪽 버튼으로 클릭한 다음 관리 일시 중지를 클릭합니다. 확인 메시지에서 예를 클릭합니다. KSX 장치가 다시 시작됩니다. 장치를 일시 중지하면 CC-SG 에서 해당 장치를 삭제할 수 있습니다.

▶ **장치를 삭제하려면:**

1. 장치 탭을 클릭하고 삭제할 장치를 선택합니다.
2. 장치 > 장치 관리자 > 장치 삭제를 선택합니다.
3. 확인을 클릭하여 장치를 삭제합니다. 장치가 삭제되면 메시지가 표시됩니다.

포트 구성

장치를 추가할 때 모든 포트 구성을 선택하여 장치의 모든 포트가 자동으로 추가되지 않을 경우, 포트 구성 화면을 이용하여 장치의 개별 포트 또는 포트 세트를 CC-SG 에 추가합니다.

포트를 구성하면 각 포트의 CC-SG에 노드가 생성되고 기본 인터페이스도 생성됩니다. *포트 구성에 의해 생성된 노드* (p. 40)를 참조하십시오.

직렬 포트 구성

▶ **직렬 포트를 구성하려면:**

1. 장치 탭을 클릭하고 직렬 장치를 선택합니다.
2. 장치 > 포트 관리자 > 포트 구성을 선택합니다.

열 헤더를 클릭하여 해당 속성별로 오름차순으로 포트를 정렬합니다. 열 헤더를 다시 클릭하면 포트가 내림차순으로 정렬됩니다.

3. 구성하려는 직렬 포트에 해당하는 구성 버튼을 클릭합니다.
4. 포트 이름 필드에 이름을 입력합니다. 쉽게 사용하기 위해 포트에 연결되어 있는 대상 다음에 포트의 이름을 지정합니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.
5. 노드 이름 필드에 노드 이름을 입력하여 이 포트에서 대역외 인터페이스를 사용한 새 노드를 생성합니다. 쉽게 사용하기 위해 포트에 연결되어 있는 대상 다음에 노드의 이름을 지정합니다. 따라서 포트 이름 및 노드 이름 필드에 동일한 이름을 입력하게 됩니다.
6. 액세스 애플리케이션 드롭다운 메뉴를 클릭하고 목록에서 이 포트에 연결할 때 사용할 애플리케이션을 선택합니다. CC-SG 에서 브라우저 기반의 올바른 애플리케이션을 자동으로 선택할 수 있도록 하려면 자동 탐지를 선택합니다.
7. 확인을 클릭하여 포트를 추가합니다.

KVM 포트 구성

▶ KVM 포트를 구성하려면:

1. 장치 탭을 클릭하고 KVM 장치를 선택합니다.
2. 장치 > 포트 관리자 > 포트 구성을 선택합니다.
 - 열 헤더를 클릭하여 해당 속성별로 오름차순으로 포트를 정렬합니다. 열 헤더를 다시 클릭하면 포트가 내림차순으로 정렬됩니다.
3. 구성하려는 KVM 포트에 해당하는 구성 버튼을 클릭합니다.
4. 포트 이름 필드에 포트 이름을 입력합니다. 쉽게 사용하기 위해 포트에 연결되어 있는 대상 다음에 포트의 이름을 지정합니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.
5. 노드 이름 필드에 노드 이름을 입력하여 이 포트에서 대역외 인터페이스를 사용한 새 노드를 생성합니다. 쉽게 사용하기 위해 포트에 연결되어 있는 대상 다음에 노드의 이름을 지정합니다. 따라서 포트 이름 및 노드 이름 필드에 동일한 이름을 입력하게 됩니다.

6. 액세스 애플리케이션 드롭다운 메뉴를 클릭하고 목록에서 이 포트에 연결할 때 사용할 애플리케이션을 선택합니다. CC-SG 에서 브라우저에 기반한 애플리케이션을 자동으로 선택할 수 있도록 하려면 자동 탐지를 선택합니다.
7. 확인을 클릭하여 포트를 추가합니다.

포트 구성에 의해 생성된 노드

장치의 포트를 구성할 수 있을 경우 노드는 자동으로 각 포트에 대해 생성됩니다. 인터페이스도 각 노드에 대해 생성됩니다.

노드가 자동으로 생성될 때 연관된 포트와 동일한 이름이 부여됩니다. 노드 이름이 이미 존재할 경우 확장 번호가 노드 이름에 추가됩니다. 예를 들어, Channel1(1)입니다. 확장 번호는 괄호 안의 숫자입니다. 이 확장 번호는 노드 이름의 문자 수에 포함되지 않습니다. 노드 이름을 편집할 경우 새 이름은 최대 문자 수로 제한됩니다. **명명 규칙** (p. 294)을 참조하십시오.

포트 편집

포트를 편집하여 포트 이름, 액세스 애플리케이션 또는 직렬 포트 설정과 같은 다양한 매개변수를 변경할 수 있습니다. 변경할 수 있는 사항은 포트 유형 및 장치 유형에 따라 다릅니다.

▶ **KVM 또는 직렬 포트 이름, 액세스 애플리케이션을 편집하려면:**

일부 포트는 하나의 액세스 애플리케이션만 지원하기 때문에 액세스 애플리케이션 기본 설정을 변경할 수 없습니다.

1. 장치 탭을 클릭하고 편집할 포트를 선택합니다.
2. 필요한 경우 포트 이름 필드에 포트의 새 이름을 입력합니다.
3. 액세스 애플리케이션 드롭다운 메뉴를 클릭하고 목록에서 이 포트에 연결할 때 사용할 애플리케이션을 선택합니다. CC-SG 에서 브라우저에 기반한 애플리케이션을 자동으로 선택할 수 있도록 하려면 자동 탐지를 선택합니다.
4. 확인을 클릭하여 변경 사항을 저장합니다.

▶ **전송 속도, 흐름 제어 또는 패리티/데이터 비트와 같은 KSX2 또는 KSX 직렬 포트의 설정을 편집하려면:**

1. 장치 탭을 클릭하고 편집할 직렬 포트를 선택하거나 편집할 포트를 포함하고 있는 장치를 선택합니다.

2. 장치 > 장치 관리자 > 관리 시작을 선택합니다. 장치 관리 페이지가 열립니다.
3. 포트 구성을 클릭합니다.
4. 편집한 직렬 포트를 클릭합니다.
5. 포트 설정을 편집하려면:
6. 확인을 클릭하여 변경 사항을 저장합니다. 관리 페이지를 닫고 CC-SG 로 돌아갑니다.

▶ **전송 속도, 흐름 제어 또는 패리티/데이터 비트와 같은 SX 직렬 포트의 설정을 편집하려면:**

1. 장치 탭을 클릭하고 편집할 포트를 선택합니다. 포트 프로필 페이지가 열립니다.
2. 포트 설정을 편집합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.

포트 삭제

포트를 삭제하여 장치에서 포트 항목을 제거합니다. 포트가 작동하지 않는 상태일 경우 포트 프로필 화면의 정보는 읽기 전용입니다. 작동하지 않는 상태의 포트는 삭제할 수 있습니다.

중요: 노드와 연관된 포트를 삭제하면 포트에서 제공한 연관된 대역의 KVM 또는 직렬 인터페이스가 노드에서 제거됩니다. 노드에 다른 인터페이스가 없는 경우 노드도 CC-SG에서 제거됩니다.

▶ **포트를 삭제하려면:**

1. 장치 탭을 클릭하고 포트를 삭제할 장치를 선택합니다.
2. 장치 > 포트 관리자 > 포트 삭제를 선택합니다.
3. 삭제할 포트의 확인란을 선택합니다.
4. 확인을 클릭하여 선택한 포트를 삭제합니다. 포트가 삭제되면 메시지가 표시됩니다.

장치 범주 및 요소 대량 복사

대량 복사 명령을 사용하면 한 장치에 지정된 범주와 요소를 다른 여러 장치로 복사할 수 있습니다. 이 프로세스에서 복사되는 속성은 범주와 요소 뿐입니다.

▶ **장치 범주 및 요소를 대량 복사하려면:**

1. 장치 탭을 클릭하고 장치 트리에서 장치를 선택합니다.
2. 장치 > 장치 관리자 > 대량 복사를 선택합니다.
3. 모든 장치 목록에서 장치 이름 필드에 있는 장치의 범주 및 요소를 복사할 장치를 선택합니다.
4. >을 클릭하여 장치를 선택한 장치 목록에 추가합니다.
5. 장치를 선택하고 <을 클릭하여 선택한 장치 목록에서 제거합니다.
6. 확인을 클릭하여 대량 복사합니다. 장치 범주 및 요소가 복사되면 메시지가 표시됩니다.

장치 업그레이드

새 버전의 장치 펌웨어가 있으면 장치를 업그레이드할 수 있습니다.

중요: 새 장치 펌웨어 버전이 **CC-SG** 펌웨어 버전과 호환되는지 확인하려면 호환성 매트릭스를 확인하십시오. **CC-SG** 및 장치 또는 장치 그룹을 업그레이드 해야 할 경우 **CC-SG** 업그레이드를 먼저 수행한 다음 장치 업그레이드를 실시합니다.

▶ **장치를 업그레이드하려면:**

1. 장치 탭을 클릭하고 장치 트리에서 장치를 선택합니다.
2. 장치 > 장치 관리자 > 장치 업그레이드를 선택합니다.
3. 펌웨어 이름: 목록에서 적절한 펌웨어를 선택합니다. 이 정보는 **Raritan** 또는 대리점에서 제공합니다.
4. 확인을 클릭하여 장치를 업그레이드합니다.
 - **SX** 및 **KX** 장치를 업그레이드하려면 20 분 정도 소요됩니다.
 - 장치의 펌웨어 버전이 **CC-SG** 와 호환되지 않는 경우 메시지가 표시됩니다. 예를 클릭하여 장치를 업그레이드합니다. 아니오를 클릭하여 업그레이드를 취소합니다.
5. 메시지가 나타납니다. 예를 클릭하여 장치를 다시 시작합니다. 장치가 업그레이드되었을 때 메시지가 표시됩니다.

6. 브라우저가 모든 업그레이드 파일을 로드하는지 확인하려면 브라우저 창을 닫은 다음 새 브라우저 창에서 CC-SG 에 로그인합니다.

장치 구성 백업

선택한 장치의 모든 사용자 구성 및 시스템 구성 파일을 백업할 수 있습니다. 장치에 문제가 발생하는 경우 생성한 백업 파일을 사용하여 CC-SG 에서 이전 구성을 복원할 수 있습니다.

CC-SG에 저장할 수 있는 최대 백업 파일 수는 장치 당 3 개입니다. 더 많은 백업 파일이 필요할 경우 백업 파일을 네트워크에 저장한 다음 CC-SG에서 삭제할 수 있습니다. 또는 CC-SG가 오래된 백업 파일을 삭제하도록 선택할 수 있습니다. 이 옵션은 네 번째 백업을 시도할 때 경고를 표시합니다. **모든 구성 데이터를 KX2, KSX2 또는 KX2-101 장치로 복원** (p. 46)을 참조하십시오.

각 장치가 구성의 서로 다른 구성 요소를 백업할 수 있습니다. 백업할 장치에 대한 자세한 내용은 사용자 설명서를 참조하십시오.

참고: SX 3.0.1 장치를 백업할 경우 연결된 전원 탭 구성은 백업되지 않습니다. 백업에서 SX 3.0.1 장치를 복원할 경우 전원 탭을 다시 구성해야 합니다.

▶ 장치 구성을 백업하려면:

1. 장치 탭을 클릭하고 백업할 장치를 선택합니다.
2. 장치 > 장치 관리자 > 구성 > 백업을 선택합니다.
3. 백업 이름 필드에 이름을 입력하여 이 백업을 식별합니다.
4. 설명 필드에 이 백업에 대한 간단한 설명을 입력합니다.
옵션입니다.
5. 확인을 클릭하여 장치 구성을 백업합니다. 장치 구성이 백업되었을 때 메시지가 표시됩니다.

장치 구성 복원

다음 장치 유형을 사용하여 장치 구성의 전체 백업을 복원할 수 있습니다.

- KX
- KSX
- KX101
- SX
- IP-Reach

KX2, KSX2 및 KX2-101 장치를 사용하여 장치로 복원할 백업 구성 요소를 선택할 수 있습니다.

- 보호됨: 선택한 백업 파일에서 네트워크 설정(개인 패키지)을 제외한 전체 내용이 장치로 복원됩니다. 보호됨 옵션을 사용하여 한 장치의 백업을 동일 모델의 다른 장치로 복원할 수 있습니다(KX2, KSX2 및 KX2-101 전용).
- 전체: 선택한 백업 파일의 전체 내용이 장치로 복원됩니다.
- 사용자 정의: 장치 설정, 사용자 및 사용자 그룹 데이터 설정 또는 두 가지 모두를 복원할 수 있습니다.

장치 구성 복원(KX, KSX, KX101, SX, IP-Reach)

전체 백업 구성을 KX, KSX, KX101, SX 및 IP-Reach 장치로 복원할 수 있습니다.

▶ **전체 백업 장치 구성을 복원하려면:**

1. 장치 탭을 클릭하고 백업 구성으로 복원할 장치를 선택합니다.
2. 장치 > 장치 관리자 > 구성 > 복원을 선택합니다.
3. 사용 가능한 백업 표에서 장치로 복원할 백업 구성을 선택합니다.
4. 확인을 클릭합니다.
5. 예를 클릭하여 장치를 다시 시작합니다. 모든 데이터가 복원되었을 때 메시지가 표시됩니다.

네트워크 설정을 제외한 모든 구성 데이터를 KX2, KSX2 또는 KX2-101 장치로 복원합니다.

보호됨 복원 옵션을 사용하여 네트워크 설정을 제외하고 백업 파일의 모든 구성 데이터를 KX2, KSX2 또는 KX2-101 장치로 복원할 수 있습니다. 보호됨 옵션을 사용하여 한 장치의 백업을 동일 모델의 다른 장치로 복원할 수 있습니다(KX2, KSX2 및 KX2-101 전용).

▶ 네트워크 설정을 제외한 모든 구성 데이터를 KX2, KSX2 또는 KX2-101 장치로 복원하려면:

1. 장치 탭을 클릭하고 백업 구성으로 복원할 장치를 선택합니다.
2. 장치 > 장치 관리자 > 구성 > 복원을 선택합니다.
3. 사용 가능한 백업 표에서 장치로 복원할 백업 구성을 선택합니다.
4. 복원 유형: 보호됨을 선택합니다.
5. 확인을 클릭합니다.
6. 예를 클릭하여 장치를 다시 시작합니다. 모든 사용자 및 시스템 구성 데이터가 복원되었을 때 메시지가 표시됩니다.

장치 설정 또는 사용자 및 사용자 그룹 데이터만 KX2, KSX2 또는 KX2-101 장치로 복원

사용자 정의 복원 옵션을 사용하여 장치 설정, 사용자 및 사용자 그룹 설정 또는 두 가지 모두를 복원할 수 있습니다.

▶ 장치 설정 또는 사용자 및 사용자 그룹 데이터만 KX2, KSX2 또는 KX2-101 장치로 복원하려면:

1. 장치 탭을 클릭하고 백업 구성으로 복원할 장치를 선택합니다.
2. 장치 > 장치 관리자 > 구성 > 복원을 선택합니다.
3. 사용 가능한 백업 표에서 장치로 복원할 백업 구성을 선택합니다.
4. 복원 유형: 사용자 정의를 선택합니다.
5. 복원 옵션: 장치로 복원할 다음 구성 요소를 선택합니다. 장치 설정, 사용자 및 사용자 그룹 데이터.
6. 확인을 클릭합니다.
7. 예를 클릭하여 장치를 다시 시작합니다. 데이터가 복원되었을 때 메시지가 표시됩니다.

모든 구성 데이터를 KX2, KSX2 또는 KX2-101 장치로 복원

전체 복원 옵션을 사용하여 백업 파일의 모든 구성 데이터를 KX2, KSX2 또는 KX2-101 장치로 복원할 수 있습니다.

▶ **모든 구성 데이터를 KX2, KSX2 또는 KX2-101 장치로 복원하려면:**

1. 장치 탭을 클릭하고 백업 구성으로 복원할 장치를 선택합니다.
2. 장치 > 장치 관리자 > 구성 > 복원을 선택합니다.
3. 사용 가능한 백업 표에서 장치로 복원할 백업 구성을 선택합니다.
4. 복원 유형: 전체를 선택합니다.
5. 확인을 클릭합니다.
6. 예를 클릭하여 장치를 다시 시작합니다. 모든 사용자 및 시스템 구성 데이터가 복원되었을 때 메시지가 표시됩니다.

장치 백업 파일의 저장, 업로드 및 삭제

장치 구성 복원 페이지에서 장치 백업 파일을 네트워크 또는 로컬 시스템의 위치로 저장할 수 있습니다. 새 백업을 CC-SG 로 복원하기 위해 공간이 필요할 경우 장치 백업 파일을 삭제할 수 있습니다. 또한 네트워크에 저장된 장치 백업 파일을 CC-SG 로 업로드하여 장치 구성을 복원하는데 사용할 수 있습니다.

▶ **CC-SG 에서 장치 백업 파일 저장:**

1. 장치 탭을 클릭하고 장치를 선택합니다.
2. 장치 > 장치 관리자 > 구성 > 복원을 선택합니다.
3. 저장할 장치 백업 파일을 선택합니다. 파일에 저장을 클릭합니다.
4. 파일을 저장할 위치를 탐색합니다. 저장을 클릭합니다.

▶ **CC-SG 에서 장치 백업 파일 삭제:**

1. 장치 탭을 클릭하고 장치를 선택합니다.
2. 장치 > 장치 관리자 > 구성 > 복원을 선택합니다.
3. 삭제할 장치 백업 파일을 선택합니다. 삭제를 클릭합니다.
4. 예를 클릭하여 확인합니다.

▶ **CC-SG 로 장치 백업 파일 업로드:**

1. 장치 탭을 클릭하고 장치를 선택합니다.
2. 장치 > 장치 관리자 > 구성 > 복원을 선택합니다.

- 업로드를 클릭합니다. 장치 백업 파일을 탐색하여 선택합니다. 파일 유형은 .rfp 입니다. 열기를 클릭합니다.
장치 백업 파일이 CC-SG 로 업로드되고 페이지에 표시됩니다.

장치 구성 복사

하나의 Dominion SX 장치에서 하나 이상의 다른 SX 장치로 구성을 복사할 수 있습니다.

구성은 SX 장치 사이에만 복사할 수 있습니다. SX 장치는 각각 동일한 수의 포트를 가져야 합니다.

▶ Dominion SX 장치 구성을 복사하려면:

- 장치 탭을 클릭하고 장치 트리에서 다른 장치로 복사하려는 구성을 가진 장치를 선택합니다.
- 장치 > 장치 관리자 > 구성 > 구성 복사를 선택합니다.
- 이 장치에서 장치 백업 옵션을 사용하면 대신에 저장된 구성을 선택한 다음 저장된 구성 드롭다운 메뉴에서 구성을 선택하여 해당 구성을 복사할 수 있습니다.
- 이 구성을 복사하려는 장치를 사용 가능한 장치 열에서 강조 표시하고 오른쪽 화살표를 클릭하여 선택한 장치를 구성 복사 대상 열로 이동합니다. 왼쪽 화살표는 선택한 장치를 구성 복사 대상 열로 이동합니다.
- 확인을 클릭하여 구성을 구성 복사 대상 열의 장치로 복사합니다.
- 다시 시작 메시지가 나타나면 예를 클릭하여 장치를 다시 시작합니다. 장치 구성이 복사되었을 때 메시지가 표시됩니다.

장치 다시 시작

장치 다시 시작 기능을 사용하여 장치를 다시 시작합니다.

▶ 장치를 다시 시작하려면:

- 장치 탭을 클릭하고 다시 시작할 장치를 선택합니다.
- 장치 > 장치 관리자 > 장치 다시 시작을 선택합니다.
- 확인을 클릭하여 장치를 다시 시작합니다.
- 예를 클릭하여 장치에 액세스하는 모든 사용자가 로그오프되도록 확인합니다.

장치 핑

장치를 핑하면 장치가 네트워크에서 사용 가능한지를 판별할 수 있습니다.

▶ **장치에 핑하려면:**

1. 장치 탭을 클릭하고 핑할 장치를 선택합니다.
2. 장치 > 장치 관리자 > 장치 핑을 선택합니다. 장치 핑 화면이 나타나서 핑 결과를 보여줍니다.

장치에 대한 CC-SG의 관리 일시 중지

CC-SG 에 저장된 구성 데이터를 유실하지 않고 CC-SG 제어를 일시적으로 중지하기 위해 장치를 일시 중지할 수 있습니다.

▶ **장치에 대한 CC-SG 관리를 일시 중지하려면:**

1. 장치 탭을 클릭하고 CC-SG 관리를 일시 중지할 장치를 선택합니다.
2. 장치 > 장치 관리자 > 관리 일시 중지를 선택합니다. 장치 트리의 장치 아이콘은 장치의 일시 중지된 상태를 나타냅니다.

관리 다시 시작

일시 중지된 장치의 CC-SG 관리를 다시 시작하여 CC-SG 에서 다시 제어되도록 할 수 있습니다.

▶ **일시 중지된 장치에 대한 CC-SG 관리를 다시 시작하려면:**

1. 장치 탭을 클릭하고 장치 트리에서 일시 중지한 장치를 선택합니다.
2. 장치 > 장치 관리자 > 관리 다시 시작을 선택합니다. 장치 트리의 장치 아이콘은 장치의 활성 상태를 나타냅니다.

장치 전원 관리자

장치 전원 관리자는 전원 탭 장치의 모든 전원 콘센트를 관리하고 전압, 전류 및 온도를 포함하여 전원 탭 장치의 상태를 확인하는데 사용됩니다. 장치 전원 관리자는 콘센트에 대한 전원 탭 중심 보기를 제공합니다.

장치 전원 관리자를 사용하기 전에 전원 탭을 **Dominion SX** 또는 **Dominion KSX** 장치와 실제로 연결해야 합니다. 전원 탭 장치를 추가할 때 연결을 제공하는 **Raritan** 장치를 정의해야 합니다. 이 경우 전원 탭 장치는 전원 탭의 관리를 제공하는 **SX** 직렬 포트 또는 **KSX** 전용 전원 포트와 연결됩니다.

▶ 장치 전원 관리자를 보려면:

1. 장치 탭에서 전원 탭 장치를 선택합니다.
2. 장치 > 장치 전원 관리자를 선택합니다.
3. 콘센트는 콘센트 상태 패널에 나열됩니다. 모든 콘센트를 보려면 스크롤해야 하는 경우도 있습니다.
 - 각 콘센트에 해당하는 켜짐 또는 꺼짐 라디오 버튼을 클릭하면 콘센트 전원이 켜지거나 꺼집니다.
 - 콘센트에 연결된 장치를 다시 시작하려면 재순환을 클릭합니다.

장치의 관리 페이지 실행

선택된 장치에 사용 가능한 경우 관리 시작 명령은 장치의 관리자 인터페이스에 대한 액세스를 제공합니다.

▶ 장치의 관리 페이지를 실행하려면:

1. 장치 탭을 클릭하고 관리자 인터페이스를 시작할 장치를 선택합니다.
2. 장치 > 장치 관리자 > 관리 시작을 선택합니다. 선택한 장치의 관리자 인터페이스가 나타납니다.

사용자 연결 해제

관리자는 장치에 대한 모든 사용자의 세션을 종료할 수 있습니다. 여기에는 포트에 연결하거나 장치 구성을 백업하거나 장치 구성을 복원하거나 장치의 펌웨어를 업그레이드하는 등 장치에 대한 모든 작업을 수행하는 사용자가 포함됩니다.

장치에 대한 사용자 세션이 종료되기 전에 펌웨어 업그레이드와 장치 구성 백업 및 복원을 완료할 수 있습니다. 다른 모든 작업이 즉시 종료됩니다.

Dominion SX 장치의 경우에만 장치에 직접 로그인된 사용자 뿐 아니라 CC-SG 를 통해 장치에 연결된 사용자를 연결 해제할 수 있습니다.

▶ **장치에서 사용자를 연결 해제하려면:**

1. 장치 탭을 클릭하고 사용자를 연결 해제할 장치를 선택합니다.
2. 장치 > 장치 관리자 > 사용자 연결 해제를 선택합니다.
3. 사용자 연결 해제 표에서 세션을 연결 해제할 세션의 사용자를 선택합니다.
4. 연결 해제를 클릭하여 장치에서 사용자를 연결 해제합니다.

Paragon II 시스템 장치로의 특별 액세스

P2-SC(Paragon II System Controller)

Paragon II 시스템 통합 사용자는 P2-SC 장치를 CC-SG 장치 트리에 추가하고 CC-SG 내에서 P2-SC 관리 애플리케이션을 구성할 수 있습니다. P2-SC 관리를 사용하는 방법에 대한 자세한 내용은 Raritan 의 **Paragon II System Controller 사용자 설명서**를 참조하십시오.

Paragon 시스템 장치(Paragon 시스템에는 P2-SC 장치, 연결된 UMT 장치, 연결된 IP-Reach 장치 등이 포함됨)를 CC-SG 에 추가하면 장치 트리에 표시됩니다.

▶ **Cc-SG 에서 Paragon II System Controller 에 액세스하려면:**

1. 장치 탭을 클릭하고 Paragon II System Controller 를 선택합니다.
2. Paragon II System Controller 를 마우스 오른쪽 버튼으로 클릭한 다음 관리 시작을 클릭하여 새 브라우저 창에서 Paragon II System Controller 애플리케이션을 시작합니다. 그런 다음 PII UMT 장치를 구성할 수 있습니다.

IP-Reach 및 UST-IP 관리

CC-SG 인터페이스에서 Paragon 시스템 설정으로 직접 연결된 IP-Reach 및 UST-IP 장치에서 관리 진단 프로그램을 실행할 수도 있습니다.

Paragon 시스템 장치를 CC-SG 에 추가하면 장치 트리에 표시됩니다.

▶ 원격 사용자 스테이션 관리 액세스:

1. 장치 탭을 클릭하고 Paragon II System Controller 를 선택합니다.
2. Paragon II System Controller 를 마우스 오른쪽 버튼으로 클릭하고 원격 사용자 스테이션 관리를 클릭합니다. 원격 사용자 스테이션 관리 화면이 나타나 연결된 모든 IP-Reach 및 UST-IP 장치를 나열합니다.
3. 작업하려는 장치 행에 있는 관리 시작을 클릭하여 Raritan 원격 콘솔을 활성화하고 새로운 창에 파란색 장치 구성 화면을 시작합니다.

장치 그룹 관리자

장치 그룹 관리자 화면을 사용하여 장치 그룹을 추가, 편집 및 제거합니다. 새 장치 그룹을 추가할 때 그룹에 대한 전체 액세스 규정을 생성할 수 있습니다. **액세스 제어 규정** (p. 115)을 참조하십시오.

장치 그룹 추가

▶ 장치 그룹을 추가하려면:

1. 연관계 > 장치 그룹을 선택합니다. 장치 그룹 관리자 창이 열립니다. 기존의 장치 그룹은 왼쪽 패널에 표시됩니다.
2. 도구 모음에서  새 그룹 아이콘을 클릭합니다. 장치 그룹: 새 패널이 나타납니다.
3. 그룹 이름 필드에 생성할 장치 그룹의 이름을 입력합니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.

4. 그룹에 장치를 추가할 수 있는 두 방법은 장치 선택 및 장치 설명입니다. 장치 선택 탭을 사용하면 사용 가능한 장치의 목록에서 장치를 선택하여 그룹에 지정할 장치를 선택할 수 있습니다. 장치 설명 탭을 사용하면 장치를 설명하는 규칙을 지정할 수 있으며 매개변수가 해당 규칙을 따르는 장치가 그룹에 추가됩니다.

▶ **장치 선택**

- a. 장치 선택 탭을 클릭합니다.
- b. 사용 가능 목록에서 그룹에 추가할 장치를 선택한 다음 추가를 클릭하여 선택 목록으로 장치를 이동합니다. 선택 목록의 장치가 그룹에 추가됩니다.
 - 그룹에서 장치를 제거하려면 선택 목록에서 장치 이름을 선택한 다음 제거를 클릭합니다.
 - 사용 가능 또는 선택 목록에서 장치를 검색할 수 있습니다. 목록 아래의 필드에 검색 용어를 입력한 다음 이동을 클릭합니다.

▶ **장치 설명**

- a. 장치 그룹: 새 패널에서 장치 설명 탭을 클릭합니다. 장치 설명 탭에서 그룹에 지정할 장치를 설명하는 규칙 표를 생성합니다.
- b. 새 행 추가 아이콘을 클릭하여  표에 행을 추가합니다.
- c. 각 열에 생성된 셀을 더블 클릭하여 드롭다운 메뉴를 활성화합니다. 각 목록에서 사용할 규칙 구성요소를 선택합니다.
 - 접두어 - 비워 두거나 **NOT** 을 선택합니다. **NOT** 을 선택한 경우 이 규칙은 나머지 수식과 반대값으로 필터링됩니다.
 - 범주 - 규칙에서 평가되는 속성을 선택합니다. 연관체 관리자에서 생성한 모든 범주를 여기서 사용할 수 있습니다.
 - 연산자 - 범주와 요소 항목 사이에서 수행할 비교 작업을 선택합니다. 사용 가능한 연산자는 =(같음), LIKE(이름으로 요소를 찾는데 사용) 및 <>(같지 않음)입니다.
 - 요소 - 비교할 범주 속성의 값을 선택합니다. 선택한 범주와 연관된 요소만 여기에 표시됩니다(예: "부서" 범주를 평가하는 경우 "위치" 요소가 여기에 나타나지 않음).
 - 규칙 이름- 이 행에서 규칙에 지정된 이름입니다. 편집할 수 없으며 약식 표현 필드에 설명을 입력하는 데 사용됩니다.

- 다른 규칙을 추가하려면 새 행 추가를 클릭하고 필요한 구성을 설정합니다. 여러 규칙을 구성하면 장치를 평가하는 여러 기준을 제공하여 보다 정확한 설명이 가능해집니다.
- 규칙 표는 노드를 평가하는 기준에만 사용할 수 있습니다. 장치 그룹에 대한 설명을 입력하려면 약식 표현 필드에 규칙 이름별로 규칙을 추가합니다. 설명에 한 가지 규칙만 필요한 경우 해당 필드에 해당 규칙의 이름을 입력합니다. 여러 규칙을 평가하는 경우 서로 연관된 규칙을 설명하는 데 논리 연산자 세트를 사용하여 해당 필드에 규칙을 입력합니다.
- & - AND 연산자. 노드는 설명(또는 설명의 해당 섹션)을 true(참)로 평가하려면 이 연산자의 양쪽에 있는 규칙을 충족해야 합니다.
- | - OR 연산자. 설명(또는 설명의 해당 섹션)이 true(참)로 평가되려면 장치가 이 연산자의 양쪽에 있는 규칙 중 한 가지만 충족하면 됩니다.
- (and) - 그룹화 연산자. 괄호 안에 포함된 하위 섹션으로 설명을 나눕니다. 나머지 설명을 노드와 비교하기 전에 먼저 괄호 안의 섹션을 평가합니다. 삽입 그룹은 다른 삽입 그룹 안에 중첩될 수 있습니다.
- 예제 1: 엔지니어링 부서에 속하는 장치를 설명하려면 **Department = Engineering** 이라는 규칙을 생성합니다. 이 규칙은 **Rule0** 이 됩니다. 약식 표현 필드에 **Rule0** 을 입력합니다.
- 예제 2: 엔지니어링 부서에 속하거나 Philadelphia 에 있으며 모든 시스템의 메모리가 1GB 가 되도록 지정하는 장치 그룹을 설명하려면 세 가지 규칙을 생성해야 합니다. **Department = Engineering(Rule0) Location = Philadelphia(Rule1) Memory = 1GB(Rule2)**. 이러한 규칙은 서로 연관된 상태로 정렬되어야 합니다. 장치는 엔지니어링 부서에 속하거나 Philadelphia 에 있을 수 있기 때문에 OR 연산자 |를 사용하여 다음과 같이 두 규칙을 연결합니다. **Rule0|Rule1**. 괄호로 닫아 이 비교를 먼저 설정합니다. **(Rule0|Rule1)**. 장치는 이 비교를 만족하고 1GB 의 메모리를 포함해야 하기 때문에 AND 커넥터인 &을(를) 사용하여 이 섹션을 **Rule2: (Rule0|Rule1)&Rule2** 와 연결합니다. 약식 표현 필드에 이 마지막 수식을 입력합니다.
- 표에서 행을 제거하려면 행을 선택하고 선택한 행 제거 아이콘  을 클릭합니다.

- 매개변수가 정의한 규칙을 따르는 장치의 목록을 보려면 장치 보기를 클릭합니다.
 - a. 약식 표현 필드에 설명을 입력할 때 확인을 클릭합니다. 설명이 잘못 구성되면 경고 메시지가 나타납니다. 설명이 올바르게 구성되면 정규 형식의 수식이 정규 수식 필드에 나타납니다.
 - b. 이 수식을 충족하는 노드를 보려면 장치 보기를 클릭합니다. 현재 수식에 의해 그룹화된 장치를 표시하는 장치 그룹의 장치 결과 창이 나타납니다. 이 창은 설명이 올바르게 입력되었는지 확인하는 데 사용할 수 있습니다. 설명이 올바르게 입력되지 않은 경우 규칙 표 또는 약식 표현 필드로 돌아가서 설명을 조정할 수 있습니다.
 - c. 항상 제어 권한을 사용하여 그룹에 있는 모든 장치에 대한 액세스를 허용하는 이 장치 그룹의 규정을 생성하려면 그룹의 전체 액세스 규정 생성 확인란을 선택합니다.
 - d. 다른 장치 그룹을 추가하려면 적용을 클릭하여 이 그룹을 저장하고 단계를 반복합니다. **옵션입니다.**
 - e. 장치 그룹 추가를 완료하면 확인을 클릭하여 변경 사항을 저장합니다.

설명 방법 대 선택 방법

그룹이 범주 및 요소와 같은 노드 또는 장치의 몇 가지 속성을 기초로하기 원할 경우 설명 방법을 사용합니다. 설명 방법의 이점은 설명된 것과 동일한 속성을 가진 장치나 노드를 추가할 경우 자동으로 그룹에 추가된다는 것입니다.

특정 노드의 그룹을 수동으로 만들기 원할 경우 선택 방법을 사용합니다. CC-SG 에 추가된 새 노드 및 장치는 이 그룹에 자동으로 추가되지 않습니다. CC-SG 에 추가한 후에 그룹에 새 노드나 장치를 수동으로 추가해야 합니다.

이 두 방법은 조합할 수 없습니다.

그룹이 하나의 방법으로 생성되면 동일한 방법을 사용하여 편집해야 합니다. 방법을 전환하면 현재 그룹 설정을 덮어 씩니다.

장치 그룹 편집

▶ 장치 그룹을 편집하려면:

1. 연관체 > 장치 그룹을 선택합니다. 장치 그룹 관리자 창이 열립니다.

2. 기존의 장치 그룹은 왼쪽 패널에 표시됩니다. 이름을 편집할 장치 그룹을 선택합니다. 장치 그룹 내역 패널이 나타납니다.
3. 그룹 이름 필드에 장치 그룹에 대한 새 이름을 입력합니다.
옵션입니다.
4. 장치 선택 또는 장치 설명 탭을 사용하여 장치 그룹의 포함된 장치를 편집합니다. **장치 그룹 추가** (p. 51)를 참조하십시오.
5. 확인을 클릭하여 변경 사항을 저장합니다.

장치 그룹 삭제

▶ **장치 그룹을 삭제하려면:**

1. 연관체 > 장치 그룹을 선택합니다. 장치 그룹 관리자 창이 열립니다.
2. 기존의 장치 그룹은 왼쪽 패널에 표시됩니다. 삭제할 장치 그룹을 선택합니다. 장치 그룹 내역 패널이 나타납니다.
3. 그룹 > 삭제를 선택합니다.
4. 장치 그룹 삭제 패널이 나타납니다. 삭제를 클릭합니다.
5. 확인 메시지에서 예를 클릭합니다.

CC-SG 에서 전원 탭을 이용하여 전원 제어를 구성하는 방법은 두 가지가 있습니다.

1. 지원되는 모든 Raritan 브랜드 전원 탭은 다른 Raritan 장치에 연결될 수 있으며 전원 탭 장치로 CC-SG에 추가할 수 있습니다. Raritan 브랜드 전원 탭에는 Dominion PX 및 RPC 전원 탭이 있습니다. 지원되는 버전에 대해서는 호환성 매트릭스를 확인합니다. CC-SG에서 이 유형의 관리되는 전원 탭을 구성하려면 전원 탭이 물리적으로 연결된 Raritan 장치를 알아야 합니다. **CC-SG에서 다른 장치가 관리하는 전원 탭 구성** (p. 57)을 참조하십시오.
2. Dominion PX 전원 탭은 IP 네트워크에 직접 연결되어 PX 장치로서 CC-SG 에 추가될 수 있습니다. IP 네트워크에 직접 연결된 PX 전원 탭은 다른 Raritan 장치에 연결할 필요가 없습니다.

두 가지 방법 모두 콘센트와 전원이 공급되는 노드 사이에 전원 연관체를 생성하기 위해 관리되는 전원 탭 인터페이스를 노드에 추가해야 합니다. **관리된 전원 연결을 위한 인터페이스** (참조 "관리된 전원 탭 연결을 위한 인터페이스" p. 89)를 참조하십시오.

▶ Dominion PX 에 대한 특별한 메모

PX 를 구성하기 위해 선택한 방법과 상관 없이 단일 방법, 즉 관리되는 장치의 전원 탭 또는 PX로서 단일 방법을 사용하여 모든 전원 연관체를 구성해야 하며 두 가지 방법을 모두 사용할 수는 없습니다.

또한 PX 를 장치 관리에 연결하여 전원 연관체를 구성할 수 있으며 동일한 PX 장치를 IP 네트워크에 연결하여 전원 데이터를 보고 수집하기 위해 PX 웹 클라이언트를 사용할 수 있습니다. 펌웨어 및 설명서 아래에 있는 Raritan 웹 사이트의 지원 섹션에 있는 **Raritan Dominion PX 사용자 설명서**를 참조하십시오.

이 장에서

CC-SG에서 다른 장치가 관리하는 전원 탭 구성	57
KX, KX2, KX2-101, KSX2 및 P2SC에 연결된 전원 탭 구성	58
SX 3.0 및 KSX에 연결된 전원 탭 구성.....	59
SX 3.1 에 연결된 전원 탭 구성	61
전원 탭의 콘센트 구성.....	62

CC-SG에서 다른 장치가 관리하는 전원 탭 구성

CC-SG 에서 관리되는 전원 탭은 다음 장치 중 하나에 연결할 수 있습니다.

- Dominion KX
- Dominion KX2
- Dominion KX2-101
- Dominion SX 3.0
- Dominion SX 3.1
- Dominion KSX
- Dominion KX2
- Paragon II/Paragon II System Controller(P2SC)

관리되는 전원 탭이 물리적으로 연결된 Raritan 장치를 알아야 합니다.

참고: IP 네트워크에 연결되지만 다른 Raritan 장치에 연결되지 않는 Dominion PX 전원 탭을 가질 수도 있습니다. 이러한 전원 탭에 대한 전원 제어를 구성하는 자세한 내용은 관리되는 전원 탭 (참조 "관리된 전원 탭" p. 56)을 참조하십시오.

▶ CC-SG 에서 관리되는 전원 탭을 구성하려면:

1. 장치, 전원 탭 및 전원 탭이 전원을 공급하는 노드 사이를 모두 물리적으로 연결합니다. 전원 탭, 장치 및 노드 사이의 물리적 연결에 대한 자세한 내용은 RPC 빠른 설정 안내서, Dominion PX 빠른 설정 안내서 및 CC-SG 배치 설명서를 참조하십시오.
2. CC-SG 에 관리 중인 장치를 추가합니다. 이 절차는 Raritan 장치에 따라 다릅니다. 전원 탭이 연결된 장치와 관련된 섹션을 참조하십시오.
 - **KX, KX2, KX2-101, KSX2 및 P2SC에 연결된 전원 탭 구성** (p. 58)
 - **SX 3.0 및 KSX에 연결된 전원 탭 구성** (p. 59)
 - **SX 3.1 에 연결된 전원 탭 구성** (p. 61).
3. 콘센트를 구성합니다. **전원 탭에 콘센트 구성** (참조 "전원 탭의 콘센트 구성" p. 62)을 참조하십시오.
4. 각 콘센트를 전원이 공급되는 노드와 연결합니다. **관리된 전원 연결을 위한 인터페이스** (참조 "관리된 전원 탭 연결을 위한 인터페이스" p. 89)를 참조하십시오.

KX, KX2, KX2-101, KSX2 및 P2SC에 연결된 전원 탭 구성

CC-SG 는 KX, KX2, KX2-101, KSX2 및 P2SC 장치에 연결된 전원 탭을 자동으로 탐지합니다. CC-SG 에서 다음 작업을 수행하여 이러한 장치에 연결된 전원 탭을 구성하고 관리할 수 있습니다.

- **KX, KX2, KX2-101, KSX2 또는 P2SC 장치에 연결된 전원 탭 장치 추가** (p. 58)
- **KX, KX2, KX2-101, KSX2 또는 P2SC의 전원 탭을 다른 포트로 이동** (p. 58)
- **KX, KX2, KX2-101, KSX2 또는 P2SC 장치에 연결된 전원 탭 장치 삭제** (p. 59)

KX, KX2, KX2-101, KSX2 또는 P2SC 장치에 연결된 전원 탭 장치 추가

전원 탭에 연결된 KX, KX2, KX2-101, KSX2 또는 P2SC 장치를 CC-SG 에 추가할 경우 전원 탭이 자동으로 추가됩니다. 전원 탭은 연결된 장치 아래의 장치 탭에 표시됩니다.

다음 단계:

1. 콘센트를 구성합니다. **전원 탭에 콘센트 구성** (참조 "전원 탭의 콘센트 구성" p. 62)을 참조하십시오.
2. 각 콘센트를 전원이 공급되는 노드와 연결합니다. **관리된 전원 연결을 위한 인터페이스** (참조 "관리된 전원 탭 연결을 위한 인터페이스" p. 89)를 참조하십시오.

KX, KX2, KX2-101, KSX2 또는 P2SC의 전원 탭을 다른 포트로 이동

하나의 KX, KX2, KX2-101, KSX2 또는 P2SC 장치나 포트에서 전원 탭을 다른 KX, KX2, KX2-101, KSX2 또는 P2SC 장치나 포트에 물리적으로 이동할 경우 CC-SG 는 전원 탭을 자동으로 탐지하여 올바른 장치로 연관체를 업데이트합니다. 전원 탭을 CC-SG 에 별도로 추가할 필요는 없습니다.

참고: P2SC 포트에서 전원 탭을 물리적으로 제거하지만 다른 포트에 연결하지 않을 경우 CC-SG 는 이전 포트에서 전원 탭을 제거하지 않습니다. 장치 탭에서 전원 탭을 제거하기 위해서는 전원 탭이 연결된 UMT 의 부분 또는 전체 데이터베이스 재설정을 수행해야 합니다. **Raritan P2SC 사용자 설명서**를 참조하십시오.

KX, KX2, KX2-101, KXS2 또는 P2SC 장치에 연결된 전원 탭 장치 삭제

KX, KX2, KX2-101, KXS2 또는 P2SC 장치에 연결된 전원 탭을 CC-SG 에서 삭제할 수 없습니다. CC-SG 에서 전원 탭을 삭제하려면 장치에서 전원 탭을 물리적으로 연결 해제해야 합니다. 장치에서 전원 탭을 물리적으로 연결 해제할 경우 전원 탭 및 모든 구성된 콘센트가 장치 탭에서 사라집니다.

SX 3.0 및 KSX에 연결된 전원 탭 구성

CC-SG 에서 다음 작업을 수행하여 SX3.0 및 KSX 장치에 연결된 전원 탭을 구성하고 관리할 수 있습니다.

참고: 전원 탭은 전원 포트 또는 KSX 장치에 물리적으로 연결되어야 합니다.

- **SX 3.0 또는 KSX 장치에 연결된 전원 탭 추가** (p. 59)
- **SX 3.0 또는 KSX 장치에 연결된 전원 탭 삭제** (p. 60)
- **전원 탭의 장치 또는 포트 연관체 변경(SX 3.0, KSX)** (p. 60)

SX 3.0 또는 KSX 장치에 연결된 전원 탭 추가

1. SX 3.0 또는 KSX 장치를 CC-SG에 추가합니다. **KVM 또는 직렬 장치 추가** (p. 33)를 참조하십시오.
2. 장치 > 장치 관리자 > 장치 추가를 선택합니다.
3. 장치 유형 드롭다운 메뉴를 클릭하고 전원 탭 선택을 선택합니다.
4. 전원 탭 이름 필드에 전원 탭의 이름을 입력합니다. 커서를 필드 위에 놓으면 이름에서 허용된 문자 수가 표시됩니다. 공백은 허용되지 않습니다.
5. 콘센트 수 드롭다운 메뉴를 클릭하고 이 전원 탭에 있는 콘센트 수를 선택합니다.
6. 장치 관리 드롭다운 메뉴를 클릭하고 이 전원 탭에 연결되어 있는 SX 3.0 또는 KSX 장치를 선택합니다.
7. 포트 관리 드롭다운 메뉴를 클릭하고 이 전원 탭이 연결되어 있는 SX 3.0 또는 KSX 장치의 포트를 선택합니다.
8. 설명 필드에 이 전원 탭에 대한 간단한 설명을 입력합니다. 옵션입니다.

9. 장치 탭에 이 전원 탭의 각 콘센트를 자동으로 추가하려면 모든 콘센트 구성을 선택합니다. 지금 모든 콘센트를 구성하지 않을 경우 나중에 구성할 수 있습니다. **전원 탭에 콘센트 구성** (참조 "전원 탭의 콘센트 구성" p. 62)을 참조하십시오. **옵션입니다.**
10. 나열된 각 범주의 경우 요소 드롭다운 메뉴를 클릭하고 장치에 적용할 요소를 선택합니다. 사용하지 않으려는 각 범주의 경우 요소 필드에서 빈 항목을 선택합니다. **연관체, 범주 및 요소** (p. 22)를 참조하십시오. **옵션입니다.**
11. 이 전원 탭의 구성을 완료하면 적용을 클릭하여 이 장치를 추가하고 장치를 계속 추가할 수 있는 비어 있는 새 장치 추가 화면을 열어 장치를 추가하거나 확인을 클릭하여 새 장치 추가 화면을 계속하지 않고 이 전원 탭을 추가합니다.

다음 단계:

1. 콘센트를 구성합니다. **전원 탭에 콘센트 구성** (참조 "전원 탭의 콘센트 구성" p. 62)을 참조하십시오.
2. 각 콘센트를 전원이 공급되는 노드와 연결합니다. **관리된 전원 연결을 위한 인터페이스** (참조 "관리된 전원 탭 연결을 위한 인터페이스" p. 89)를 참조하십시오.

SX 3.0 또는 KSX 장치에 연결된 전원 탭 삭제

전원 탭이 물리적으로 연결되어 있더라도 SX 3.0, KSX 또는 P2SC 장치에 연결된 전원 탭을 시각적으로 삭제할 수 있습니다. 연결된 SX 3.0, KSX 또는 P2SC 장치에서 전원 탭을 물리적으로 연결 해제하더라도 해당 전원 탭이 해당 장치 아래 장치 탭에는 계속 표시됩니다. 표시되지 않도록 제거하려면 전원 탭을 삭제해야 합니다.

1. 장치 탭에서 삭제할 전원 탭을 선택합니다.
2. 장치 > 장치 관리자 > 장치 삭제를 선택합니다.
3. 전원 탭을 삭제하려면 확인을 클릭합니다. 전원 탭이 삭제되었을 때 메시지가 표시됩니다. 전원 탭 아이콘이 장치 탭에서 제거됩니다.

전원 탭의 장치 또는 포트 연관체 변경(SX 3.0, KSX)

전원 탭이 하나의 SX 3.0 또는 KSX 장치나 포트에서 다른 SX 3.0 또는 KSX 장치나 포트로 물리적으로 이동할 경우 CC-SG의 전원 탭 프로필에서 연관체를 변경해야 합니다.

1. 장치 탭에서 이동할 전원 탭을 선택합니다.
2. 장치 관리 드롭다운 메뉴를 클릭하고 이 전원 탭에 연결되어 있는 SX 3.0 또는 KSX 장치를 선택합니다.

3. 포트 관리 드롭다운 메뉴를 클릭하고 이 전원 탭이 연결되어 있는 SX 3.0 또는 KSX 장치의 포트를 선택합니다.
4. 확인을 클릭합니다.

SX 3.1 에 연결된 전원 탭 구성

CC-SG 에서 다음 작업을 수행하여 SX 3.1 장치에 연결된 전원 탭을 구성하고 관리할 수 있습니다.

- **SX 3.1 장치에 연결된 전원 탭 추가** (p. 61)
- **SX 3.1 의 전원 탭을 다른 포트로 이동** (p. 62)
- **SX 3.1 장치에 연결된 전원 탭 삭제** (p. 62)

SX 3.1 장치에 연결된 전원 탭 추가

SX 3.1 장치에 연결된 전원 탭의 추가 절차는 SX 3.1 장치가 CC-SG 에 추가되었는지 여부에 따라 달라집니다.

전원 탭이 **SX 3.1** 장치에 연결되어 있으며 장치가 아직 **CC-SG**에 추가되지 않은 경우:

1. SX 3.1 장치를 CC-SG에 추가합니다. **KVM 또는 직렬 장치 추가** (p. 33)를 참조하십시오.
2. CCSG 는 전원 탭을 삭제하고 자동으로 추가합니다. 전원 탭은 연결된 SX 3.1 장치 아래의 장치 탭에 표시됩니다.

SX 3.1 장치가 이미 **CC-SG**에 추가되어 있으며 전원 탭이 나중에 장치에 연결되는 경우:

1. SX 3.1 장치를 CC-SG에 추가합니다. **KVM 또는 직렬 장치 추가** (p. 33)를 참조하십시오.
2. SX 3.1 장치의 포트를 구성합니다. **포트 구성** (p. 38)을 참조하십시오.
3. 장치 탭에서 전원 탭이 연결된 SX 3.1 장치를 선택합니다.
4. 포트의 목록을 확장하려면 장치 아이콘 옆에 +를 클릭합니다.
5. 전원 탭이 연결된 SX 3.1 포트를 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 전원 탭 추가를 선택합니다.
6. 전원 탭이 가지고 있는 콘센트 수를 입력한 다음 확인을 클릭합니다.

다음 단계:

1. 콘센트를 구성합니다. **전원 탭에 콘센트 구성** (참조 "전원 탭의 콘센트 구성" p. 62)을 참조하십시오.
2. 각 콘센트를 전원이 공급되는 노드와 연결합니다. **관리된 전원 연결을 위한 인터페이스** (참조 "관리된 전원 탭 연결을 위한 인터페이스" p. 89)를 참조하십시오.

SX 3.1의 전원 탭을 다른 포트로 이동

하나의 SX 3.1 장치나 포트에서 다른 SX 3.1 장치나 포트에 전원 탭을 물리적으로 이동할 경우 이전 SX 3.1 포트에서 전원 탭을 삭제하고 새 SX 3.1 포트에 추가해야 합니다. **SX 3.1 장치에 연결된 전원 탭 삭제** (p. 62) 및 **SX 3.1 장치에 연결된 전원 탭 장치 추가** (참조 "SX 3.1 장치에 연결된 전원 탭 추가" p. 61)를 참조하십시오.

SX 3.1 장치에 연결된 전원 탭 삭제

전원 탭이 물리적으로 연결되어 있더라도 SX 3.1 장치에 연결된 전원 탭을 시각적으로 삭제할 수 있습니다. 연결된 SX 3.1 장치에서 전원 탭을 물리적으로 연결 해제하더라도 해당 전원 탭은 해당 장치 아래 장치 탭에 계속 표시됩니다. 표시하지 않도록 제거하려면 전원 탭을 삭제해야 합니다.

▶ **SX 3.1 장치에 연결된 전원 탭을 삭제하려면:**

1. 장치 탭에서 삭제할 전원 탭을 선택합니다.
2. 장치 > 장치 관리자 > 장치 삭제를 선택합니다.
3. 전원 탭을 삭제하려면 확인을 클릭합니다. 전원 탭이 삭제되었을 때 메시지가 표시됩니다. 전원 탭 아이콘이 장치 탭에서 제거됩니다.

전원 탭의 콘센트 구성

전원 탭 콘센트를 노드와 연결하기 전에 노드에 관리되는 전원 탭 인터페이스를 추가하여 콘센트를 구성해야 합니다. **관리되는 전원 탭 연결을 위한 인터페이스** (참조 "관리된 전원 탭 연결을 위한 인터페이스" p. 89)를 참조하십시오.

▶ **전원 탭 프로필에서 콘센트를 구성하려면:**

1. 장치 탭에서 전원 탭에 연결된 장치 옆의 +를 클릭합니다.
2. 구성할 콘센트가 있는 전원 탭을 선택합니다.
3. 장치 프로필: 전원 탭 화면에서 콘센트 탭을 선택합니다.

4. 구성할 각 콘센트에 대한 확인란을 선택한 다음 확인을 클릭합니다.

콘센트가 장치 탭의 전원 탭 아이콘 아래에 표시됩니다.

▶ **포트 구성 화면에서 콘센트를 구성하려면:**

1. 장치 탭에서 전원 탭에 연결된 장치 옆의 +를 클릭합니다.
2. 구성할 콘센트가 있는 전원 탭을 선택합니다.
3. 장치 > 포트 관리자 > 포트 구성을 선택합니다.
 - 화면에 표시된 기본 이름으로 여러 콘센트를 구성하려면 구성할 각 콘센트에 대한 확인란을 선택한 다음 확인을 클릭하여 기본 이름으로 각 콘센트를 구성합니다.
 - 각 콘센트를 개별적으로 구성하려면 콘센트 옆의 구성 버튼을 클릭한 다음 포트 이름 필드에 콘센트의 이름을 입력합니다. 포트를 구성하려면 확인을 클릭합니다.

▶ **콘센트를 삭제하려면:**

1. 장치 탭에서 전원 탭에 연결된 장치 옆의 +를 클릭합니다.
2. 전원 탭 옆의 +를 클릭합니다.
3. 장치 > 포트 관리자 > 포트 삭제를 선택합니다.
4. 삭제할 각 콘센트에 대한 확인란을 선택한 다음 확인을 클릭하여 콘센트를 삭제합니다.

이 섹션에서는 노드 및 연관된 인터페이스를 보고 구성하며 편집하는 방법과 노드 그룹 생성 방법을 설명합니다. 노드에 대한 연결은 간략하게 다루어집니다. 노드에 연결하는 방법에 대한 자세한 내용은 Raritan의 **CommandCenter Secure Gateway 사용자 설명서**를 참조하십시오.

이 장에서

노드 및 인터페이스 개요	65
노드 보기	66
서비스 계정	69
노드 추가, 편집 및 삭제	72
노드 프로필에 위치 및 연락처 추가	74
노드 프로필에 메모 추가	74
CC-SG에서 가상 인프라 구성	75
CC-SG와 가상 인프라 동기화	83
가상 호스트 노드의 재부팅 또는 강제 재부팅	84
가상 분포도 보기 액세스	84
노드 연결	85
노드 ping	85
인터페이스 추가, 편집 및 삭제	86
인터페이스 책갈피 설정	94
노드에 직접 포트 액세스 구성	95
노드 범주 및 요소 대량 복사	95
채팅 사용	96
노드 그룹 추가, 편집 및 삭제	97

노드 및 인터페이스 개요

노드 정보

각 노드는 대역내(직접 IP) 또는 대역외(Raritan 장치에 연결됨) 방법을 사용하여 CC-SG 를 통해 액세스할 수 있는 대상을 나타냅니다. 예를 들어, 노드는 Raritan KVM over IP 장치에 연결된 랙의 서버, HP iLO 카드를 사용한 서버, VNC 를 실행하는 네트워크상의 PC 또는 원격 직렬 관리 연결을 사용한 네트워크 인프라일 수 있습니다.

연결되어 있는 장치를 추가한 후 CC-SG 에 노드를 수동으로 추가할 수 있습니다. 또한 노드는 장치를 추가할 때 장치 추가 화면에 있는 모든 포트 구성 확인란을 선택하여 자동으로 생성할 수 있습니다. 이 옵션을 사용하여 CC-SG 에서 모든 장치 포트를 자동으로 추가하고 각 포트의 대역외 KVM 또는 직렬 인터페이스와 노드를 추가할 수 있습니다. 이 노드, 포트 및 인터페이스를 언제든지 편집할 수 있습니다.

노드 이름

노드 이름은 고유해야 합니다. 기존의 노드 이름을 사용하여 노드를 수동으로 추가할 경우 CC-SG 에서 옵션을 표시합니다. CC-SG 에서 노드를 자동으로 추가하면 번호 지정 시스템에서 노드 이름이 고유한지 확인합니다.

이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.

인터페이스 정보

CC-SG 에서 노드는 인터페이스를 통해 액세스합니다. 새로운 각 노드에 한 개 이상의 인터페이스를 추가해야 합니다. 노드 유형에 따라 다른 액세스를 제공하기 위해 노드에 대역외 KVM, 직렬, 전원 제어 또는 대역내 SSH/RDP/VNC, DRAC/RSA/ILO 와 같은 여러 유형의 인터페이스를 추가할 수 있습니다.

노드는 여러 인터페이스를 가질 수 있지만 하나의 대역외 직렬 또는 KVM 인터페이스만 가질 수 있습니다. 예를 들어, Windows Server 는 키보드, 마우스, 모니터 포트 및 서버가 연결된 콘센트를 관리하는 전원 인터페이스에 대해 한 개의 대역외 KVM 인터페이스를 가질 수 있습니다.

노드 보기

CC-SG 에서 노드 탭의 모든 노드를 보고 노드를 선택하여 자세한 노드 프로필을 볼 수 있습니다.

노드 탭

노드 탭을 클릭하면 액세스할 수 있는 모드 노드가 트리 구조로 표시됩니다.

노드는 이름별로 영문자 순서로 표시되거나 가용성 상태별로 그룹화됩니다. 가용성 상태별로 그룹화된 노드는 가용성 그룹 내에서 영문자 순서로 정렬됩니다. 정렬 방법을 전환하려면 트리를 마우스 오른쪽 버튼으로 클릭하고 노드 정렬 옵션을 클릭한 다음 노드 이름별 또는 노드 상태별을 클릭합니다.

노드 탭을 보는 여러 가지 방법에 대한 자세한 정보는 **장치 및 노드에 대한 사용자 정의 보기** (참조 "장치 및 노드의 사용자 정의 보기" p. 120)를 참조하십시오.

노드 프로필

노드 탭에서 노드를 선택하여 노드 프로필 페이지를 엽니다. 노드 프로필 페이지에는 노드에 대한 정보를 포함하는 탭이 있습니다.

▶ 인터페이스 탭

인터페이스 탭에는 노드의 모든 인터페이스가 있습니다. 이 탭을 추가, 편집 및 삭제하고 기본 인터페이스를 선택할 수 있습니다. 가상 매체를 지원하는 노드는 가상 매체가 활성화 또는 비활성화인지 표시하는 추가 열을 포함합니다.

▶ 연관체 탭

연관체 탭은 노드에 지정된 모든 범주 및 요소를 포함하고 있습니다. 다른 사항을 선택하여 연관체를 변경할 수 있습니다.

연관체, 범주 및 요소 (p. 22)를 참조하십시오.

▶ 위치 & 연락처 탭

위치 & 연락처 탭에는 전화 번호와 같이 장치를 이용할 때 필요한 장치 위치 및 연락처 정보에 대한 정보가 포함됩니다. 새 정보를 입력하여 이 필드에서 정보를 변경할 수 있습니다.

노드 프로필에 위치 및 연락처 추가 (p. 74)를 참조하십시오.

▶ 메모 탭

메모 탭에는 사용자가 장치에 대한 메모를 남겨 다른 사용자가 읽을 수 있도록 할 수 있는 도구가 있습니다. 모든 메모는 메모를 추가한 날짜, 사용자 이름 및 사용자의 IP 주소와 함께 탭에 표시됩니다.

장치, 포트 및 노드 관리 권한이 있을 경우 노드 프로필에서 모든 메모를 지울 수 있습니다. 지우기 버튼을 클릭합니다.

노드 프로필에 메모 추가 (p. 74)를 참조하십시오.

▶ 감사 탭

감사 탭에서 노드를 액세스한 이유를 볼 수 있습니다. 사용자 그룹에 대한 노드 감사가 활성화된 경우에는 노드에 연결하기 전에 액세스 이유를 입력해야 합니다.

감사 탭은 기능이 비활성화될 때 또는 액세스 이유가 입력되지 않았을 때 숨겨집니다.

사용자 그룹에 대한 액세스 감사 구성 (p. 107)을 참조하십시오.

▶ **제어 시스템 데이터 탭**

VMware의 Virtual Center와 같은 제어 시스템 서버 노드에는 제어 시스템 데이터 탭이 있습니다. 제어 시스템 데이터 탭에는 탭이 열릴 때 새로 고쳐지는 제어 시스템 서버의 정보가 포함됩니다. 가상 인프라의 분포도 보기에 액세스하거나 연관된 노드 프로필에 연결하거나 제어 시스템에 연결하고 요약 탭을 열 수 있습니다.

▶ **가상 호스트 데이터 탭**

VMware의 ESX 서버와 같은 가상 호스트 노드에는 가상 호스트 데이터 탭이 있습니다. 가상 호스트 데이터 탭에는 탭이 열릴 때 새로 고쳐지는 가상 호스트 서버의 정보가 포함됩니다. 가상 인프라의 분포도 보기에 액세스하거나 연관된 노드 프로필에 연결하거나 가상 호스트에 연결하고 요약 탭을 열 수 있습니다. 장치, 포트 및 노드 관리 권한이 있을 경우 가상 호스트 서버를 재부팅 및 강제 재부팅할 수 있습니다.

▶ **가상 시스템 데이터 탭**

VMware의 Virtual Machines와 같은 가상 시스템 노드에는 가상 시스템 데이터 탭이 있습니다. 가상 시스템 데이터 탭에는 탭이 열릴 때 새로 고쳐지는 가상 시스템의 정보가 포함됩니다. 가상 인프라의 분포도 보기에 액세스하거나 연관된 노드 프로필에 연결하거나 가상 호스트에 연결하고 요약 탭을 열 수 있습니다.

노드 및 인터페이스 아이콘

간편한 식별을 위해 노드는 노드 트리에서 서로 다른 아이콘을 사용합니다. 노드에 대한 정보를 포함하는 도구 설명을 보려면 노드 트리의 아이콘 위에 마우스 포인터를 갖다 댍니다.

아이콘	의미
	노드 사용 가능 - 노드에 사용 가능한 인터페이스가 한 개 이상 있습니다.
	노드 사용 불가 - 노드에 사용 가능한 인터페이스가 없습니다.

서비스 계정

서비스 계정 개요

서비스 계정은 여러 인터페이스에 지정할 수 있는 특별한 로그인 자격 증명입니다. 자주 암호 변경이 필요한 인터페이스 세트에 서비스 계정을 지정하여 시간을 절약할 수 있습니다. 서비스 계정의 로그인 자격 증명을 업데이트할 수 있으며 이 변경 사항은 서비스 계정을 사용하는 모든 인터페이스에 반영됩니다.

서비스 계정은 대역외 인터페이스 또는 관리되는 전원 탭 인터페이스에 사용할 수 없습니다.

- DRAC, iLO 및 RSA 인터페이스의 경우 로그인 자격 증명은 기반 OS가 아니라 내장 프로세서 카드에 적용됩니다.
- RDP, SSH 및 Telnet 인터페이스의 경우 로그인 자격 증명은 OS에 적용됩니다.
- VNC 인터페이스의 경우 로그인 자격 증명은 VNC 서버에 적용됩니다.
- 웹 브라우저 인터페이스의 경우 로그인 자격 증명은 인터페이스에 지정된 URL에 이용 가능한 형식에 적용됩니다.

▶ 서비스 계정을 보려면:

- 노트 > 서비스 계정을 선택합니다. 서비스 계정 대화상자가 나타납니다.

필드	설명
서비스 계정 이름	이 이름은 인터페이스 대화 상자 및 서비스 계정 지정 페이지에서 서비스 계정을 식별하는데 사용됩니다.
사용자 이름	이 사용자 이름은 서비스 계정을 인터페이스에 지정할 때 로그인 자격 증명의 일부로서 사용됩니다.
암호	이 암호는 서비스 계정이 인터페이스에 지정될 때 로그인 자격 증명의 일부로서 사용됩니다.
암호 다시 입력	이 필드는 암호를 올바르게 입력했는지 확인하기 위해 사용됩니다.
설명	이 설명에는 서비스 계정에 대해 추가하고자 하는 추가 정보가 포함될 수 있습니다.

서비스 계정 추가, 편집 및 삭제

▶ 서비스 계정을 추가하려면:

1. 노드 > 서비스 계정을 선택합니다. 서비스 계정 대화상자가 나타납니다.
2. 행 추가 아이콘  을 클릭하여 표에 행을 추가합니다.
3. 서비스 계정 이름 필드에 이 서비스 계정의 이름을 입력합니다.
4. 사용자 이름 필드에 사용자 이름을 입력합니다.
5. 암호 필드에 암호를 입력합니다.
6. 암호 다시 입력 필드에 암호를 다시 입력합니다.
7. 설명 필드에 이 서비스 계정에 대한 설명을 입력합니다.
8. 확인을 클릭합니다.

▶ 서비스 계정을 편집하려면:

1. 노드 > 서비스 계정을 선택합니다. 서비스 계정 대화상자가 나타납니다.
2. 편집할 서비스 계정을 찾습니다.
3. 필드를 편집합니다. 서비스 계정 이름은 편집할 수 없습니다.

참고: CC-SG 는 사용자 이름이나 암호를 변경할 때 새 로그인 자격 증명을 사용하기 위해 서비스 계정을 사용하는 모든 인터페이스를 업데이트합니다.

4. 확인을 클릭합니다.

▶ 서비스 계정을 삭제하려면:

1. 노드 > 서비스 계정을 선택합니다. 서비스 계정 대화상자가 나타납니다.
2. 삭제할 서비스 계정을 선택합니다.
3. 행 삭제 버튼을 클릭합니다. 
4. 확인을 클릭합니다.

서비스 계정의 암호 변경

▶ 서비스 계정의 암호를 변경하려면:

1. 노드 > 서비스 계정을 선택합니다. 서비스 계정 대화상자가 나타납니다.
2. 변경할 암호의 서비스 계정을 찾습니다.
3. 암호 필드에 새 암호를 입력합니다.
4. 암호 다시 입력 필드에 암호를 다시 입력합니다.
5. 확인을 클릭합니다.

참고: CC-SG 는 사용자 이름이나 암호를 변경할 때 새 로그인 자격 증명을 사용하기 위해 서비스 계정이 사용하는 모든 인터페이스를 업데이트합니다.

인터페이스에 서비스 계정 지정

서비스 계정을 여러 인터페이스에 지정할 수 있습니다. 서비스 계정이 지정된 각 인터페이스는 연결을 위해 동일한 로그인 정보를 사용합니다.

CC-SG 는 사용자 이름이나 암호를 변경할 때 새 로그인 자격 증명을 사용하기 위해 서비스 계정이 사용하는 모든 인터페이스를 업데이트합니다.

인터페이스를 구성할 때 서비스 계정을 선택할 수도 있습니다.

인터페이스 추가, 편집 및 삭제 (p. 86)를 참조하십시오.

서비스 계정을 인터페이스에 지정하려면 장치, 포트 및 노드 관리 권한이 있어야 합니다. **사용자 그룹 추가, 편집 및 삭제** (p. 105)를 참조하십시오.

▶ 서비스 계정을 인터페이스에 지정하려면:

1. 노드 > 서비스 계정 지정을 선택합니다. 서비스 계정 지정 페이지가 열립니다.
2. 서비스 계정 이름 필드에서 노드에 지정할 서비스 계정을 선택합니다.
3. 사용 가능 목록에서 서비스 계정을 지정할 인터페이스를 선택합니다. **Ctrl+클릭** 또는 **Shift+클릭**을 사용하여 한 번에 여러 인터페이스를 선택합니다.

팁: 찾기 필드에 노드 이름을 입력하면 목록에서 강조 표시됩니다. 목록에서 비슷한 모든 이름을 강조 표시하려면 이름 일부 뒤에 *를 입력합니다.

목록을 알파벳 순서로 정렬하려면 열 헤더를 클릭합니다.

4. 선택한 인터페이스를 선택 목록으로 이동하려면 추가를 클릭합니다.
5. 확인을 클릭합니다. 서비스 계정은 선택 목록의 모든 노드에 지정됩니다.

참고: CC-SG 는 사용자 이름이나 암호를 변경할 때 새 로그인 자격 증명을 사용하기 위해 서비스 계정이 사용하는 모든 인터페이스를 업데이트합니다.

노드 추가, 편집 및 삭제

노드 추가

▶ **CC-SG 에 노드를 추가하려면:**

1. 노드 탭을 클릭합니다.
2. 노드 > 노드 추가를 선택합니다.
3. 노드 이름 필드에 노드의 이름을 입력합니다. CC-SG의 모든 노드 이름은 고유해야 합니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.
4. 설명 필드에 이 노드에 대한 간단한 설명을 입력합니다.
옵션입니다.
5. 한 개 이상의 인터페이스를 구성해야 합니다. 노드 추가 화면의 인터페이스 영역에서 추가를 클릭하여 인터페이스를 추가합니다.
인터페이스 추가 (p. 86)를 참조하십시오.
6. 이 노드를 자세히 설명하고 구성하도록 범주 및 요소의 목록을 구성할 수 있습니다. **연관체, 범주 및 요소** (p. 22)를 참조하십시오.
옵션입니다.
 - 나열된 각 범주의 경우 요소 드롭다운 메뉴를 클릭하고 목록에서 노드에 적용할 요소를 선택합니다.
 - 사용하지 않으려는 각 범주의 경우 요소 필드에서 빈 항목을 선택합니다.

- 사용할 범주 또는 요소 값이 나타나지 않는 경우 연관체 메뉴를 통해 추가할 수 있습니다. **연관체, 범주 및 요소** (p. 22)를 참조하십시오.
7. 확인을 클릭하여 변경 사항을 저장합니다. 노드 목록에 노드가 추가됩니다.

포트 구성에 의해 생성된 노드

장치의 포트를 구성할 수 있을 경우 노드는 자동으로 각 포트에 대해 생성됩니다. 인터페이스도 각 노드에 대해 생성됩니다.

노드가 자동으로 생성될 때 연관된 포트와 동일한 이름이 부여됩니다. 노드 이름이 이미 존재할 경우 확장 번호가 노드 이름에 추가됩니다. 예를 들어, Channel1(1)입니다. 확장 번호는 괄호 안의 숫자입니다. 이 확장 번호는 노드 이름의 문자 수에 포함되지 않습니다. 노드 이름을 편집할 경우 새 이름은 최대 문자 수로 제한됩니다. **명명 규칙** (p. 294)을 참조하십시오.

노드 편집

노드의 이름, 설명, 인터페이스, 기본 인터페이스 또는 연관체를 변경하여 노드를 편집할 수 있습니다.

▶ 노드 편집:

1. 노드 탭을 클릭하고 편집할 노드를 선택합니다. 노드 프로필이 나타납니다.
2. 필요한 경우 필드를 편집합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.

노드 삭제

노드를 삭제하면 노드 탭에서 노드를 제거합니다. 노드는 더 이상 사용자가 액세스할 수 없게 됩니다. 노드를 삭제할 때 모든 인터페이스, 연관체 및 연관된 포트가 삭제됩니다.

▶ 노드 삭제:

1. 노드 탭에서 삭제할 노드를 선택합니다.
2. 노드 > 노드 삭제를 선택합니다. 노드 삭제 화면이 표시됩니다.
3. 노드를 삭제하려면 확인을 클릭합니다.
4. 예를 클릭하여 노드를 삭제하면 모든 인터페이스 및 연관된 포트도 삭제함을 확인합니다. 삭제가 완료되면 삭제된 항목의 목록이 표시됩니다.

노드 프로필에 위치 및 연락처 추가

노드의 위치 및 노드를 관리하거나 사용하는 사람에 대한 연락처 정보에 대한 자세한 내용을 입력합니다.

▶ **노드 프로필에 위치 및 연락처를 추가하려면:**

1. 노드 탭에서 노드를 선택합니다. 노드 프로필 페이지가 열립니다.
2. 위치 & 연락처 탭을 클릭합니다.
3. 위치 정보를 입력합니다.
 - 부서: 최대 64 문자입니다.
 - 사이트: 최대 64 문자입니다.
 - 위치: 최대 128 문자입니다.
4. 연락처 정보를 입력합니다.
 - 기본 연락처 이름 및 보조 연락처 이름: 최대 64 문자입니다.
 - 전화 번호 및 핸드폰 번호: 최대 32 문자입니다.
5. 확인을 클릭하여 변경 사항을 저장합니다.

노드 프로필에 메모 추가

메모 탭에는 다른 사용자가 읽을 수 있도록 노드에 대한 메모를 추가할 수 있습니다. 모든 메모는 메모를 추가한 날짜, 사용자 이름 및 IP 주소가 포함되어 탭에 표시됩니다.

장치, 포트 및 노드 관리 권한이 있을 경우 메모 탭에 표시되는 모든 메모를 지울 수 있습니다.

▶ **노드 프로필에 메모를 추가하려면:**

1. 노드 탭에서 노드를 선택합니다. 노드 프로필 페이지가 열립니다.
2. 메모 탭을 클릭합니다.
3. 새 메모 필드에 메모를 입력합니다.
4. 추가를 클릭합니다. 메모가 메모 목록에 표시됩니다.

▶ **모든 메모를 지우려면:**

1. 메모 탭을 클릭합니다.
2. 메모 지우기를 클릭합니다.
3. 예를 클릭하여 확인합니다. 모든 메모가 메모 탭에서 삭제됩니다.

CC-SG에서 가상 인프라 구성

가상 인프라 용어

CC-SG 는 가상 인프라 구성요소에 대해 다음 용어를 사용합니다.

용어	정의	예
제어 시스템	제어 시스템은 관리 서버입니다. 제어 시스템은 하나 이상의 가상 호스트를 관리합니다.	VMware 의 Virtual Center
가상 호스트	가상 호스트는 하나 이상의 가상 시스템이 있는 물리적 하드웨어입니다.	VMware ESX
가상 시스템	가상 시스템은 가상 호스트에 있는 가상 "서버"입니다. 가상 시스템은 하나의 가상 호스트에서 다른 가상 호스트로 이동할 수 있습니다.	VMware 가상 시스템 또는 VM
VI 클라이언트 인터페이스	제어 시스템 노드 및 가상 호스트 노드에는 가상화 시스템의 인프라 클라이언트 애플리케이션에 대한 액세스를 제공하는 VI 클라이언트 인터페이스가 있습니다.	VMware 의 가상 인프라 웹 액세스
VMW 뷰어 인터페이스	가상 시스템 노드에는 가상 시스템의 뷰어 애플리케이션에 액세스를 제공하는 VMW 뷰어 인터페이스가 있습니다.	VMware 의 가상 시스템 원격 콘솔
VMW 전원 인터페이스	가상 시스템 노드에는 CC-SG 를 통해 노드에 대한 전원 제어를 제공하는 VMW 전원 인터페이스가 있습니다.	해당 사항 없음

가상 노드 개요

CC-SG 에서 액세스할 가상 인프라를 구성할 수 있습니다. 가상화 페이지가 제공하는 두 개의 마법사 도구인 제어 시스템 추가 마법사와 가상 호스트 추가 마법사는 제어 시스템, 가상 호스트 및 가상 시스템을 올바르게 추가하는데 도움을 줍니다.

구성을 완료하면 모든 제어 시스템, 가상 호스트 및 가상 시스템을 CC-SG 의 노드에서 액세스할 수 있습니다. 각 유형의 가상 노드는 액세스용 인터페이스 및 전원용 인터페이스로 구성됩니다.

- 제어 시스템 노드 및 가상 호스트 노드는 VI 클라이언트 인터페이스로 구성됩니다. VI 클라이언트 인터페이스는 가상화 시스템의 인프라 클라이언트에 대한 액세스를 제공합니다. VMware 제어 센터의 경우 VI 클라이언트 인터페이스는 VMware 가상 인프라 웹 액세스를 통해 제어 센터 서버에 대한 액세스를 제공합니다. VMware ESX 서버의 경우 VI 클라이언트 인터페이스는 VMware 가상 인프라 웹 액세스를 통해 ESX 서버에 대한 액세스를 제공합니다.
- 가상 시스템 노드는 VMW 뷰어 인터페이스 및 VMW 전원 인터페이스로 구성됩니다. VMW 뷰어 인터페이스는 가상 시스템의 뷰어 애플리케이션에 대한 액세스를 제공합니다. VMware 가상 시스템의 경우 VMW 뷰어 인터페이스는 가상 시스템 원격 콘솔에 대한 액세스를 제공합니다. VMW 전원 인터페이스는 CC-SG 를 통해 노드에 대한 전원 제어를 제공합니다.

가상 호스트 및 가상 시스템이 있는 제어 시스템 추가

제어 시스템을 추가할 때 마법사는 제어 시스템에 포함된 가상 호스트 및 가상 시스템을 추가하는 과정을 안내합니다.

▶ 가상 호스트 및 가상 시스템을 갖춘 제어 시스템을 추가하려면:

1. 노드 > 가상화를 선택합니다.
2. 제어 시스템 추가를 클릭합니다.
3. 호스트 이름/IP 주소: 제어 시스템에 대한 IP 주소 또는 호스트 이름을 입력합니다. 최대 64 문자입니다.
4. 연결 프로토콜: 제어 시스템과 CC-SG 간의 HTTP 또는 HTTPS 통신을 지정합니다.
5. TCP 포트: TCP 포트를 입력합니다. 기본 포트는 443 입니다.
6. 확인 간격(초): 제어 시스템과 CC-SG 간에 시간 제한을 발생시키는 경과 시간(초)을 입력합니다.
7. 인증 정보를 입력합니다.

- 인증을 위해 서비스 계정을 사용하려면 서비스 계정 자격 증명 사용 확인란을 선택합니다. 서비스 계정 이름 메뉴에서 사용할 서비스 계정을 선택합니다.
- 또는
- 인증할 사용자 이름 및 암호를 입력합니다. 각각 최대 64 문자입니다.
8. 이 제어 시스템에 액세스하는 사용자가 자동으로 VI 클라이언트 인터페이스에 로그인할 수 있도록 하려면 VI 클라이언트용 단일 로그인 사용 확인란을 선택합니다. **옵션입니다.**
 9. 다음을 클릭합니다. **CC-SG**는 제어 시스템의 가상 호스트 및 가상 시스템을 검색합니다.
 10. 각 가상 시스템 옆의 구성 확인란을 선택하여 가상 시스템을 **CC-SG**에 추가합니다. 각 연관된 가상 호스트도 구성됩니다. 각각의 가상 시스템에 대해 하나의 노드가 생성됩니다. 가상 호스트는 여러 가상 시스템과 연결될 수 있지만 하나의 가상 호스트 노드만 추가됩니다.
 11. **VNC, RDP** 또는 **SSH** 인터페이스를 가상 호스트 노드 및 가상 시스템 노드에 추가하려면 각 가상 시스템 옆의 확인란을 선택합니다. **옵션입니다.**
 12. 다음을 클릭합니다. **CC-SG**는 추가될 인터페이스 유형 목록을 표시합니다. 각 유형에 대한 이름 및 로그인 자격 증명을 추가할 수 있습니다.
 13. 각 인터페이스 유형에 대해 이름 및 로그인 자격 증명을 입력합니다. 이름 및 로그인 자격 증명은 각 구성된 가상 시스템 노드 및 가상 호스트 노드에 추가된 모든 인터페이스가 공유합니다. **옵션입니다.**

각 인터페이스에 대해 개별적으로 이름 및 로그인 자격 증명을 추가하려면 이 필드를 비어 두십시오.

인터페이스는 필드가 비어 있을 경우 노드 이름을 가집니다.

- a. 인터페이스의 이름을 입력합니다. 최대 32 문자입니다.
 - 가상 호스트 VI 클라이언트 인터페이스
 - VMware 뷰어 인터페이스
 - 가상 전원 인터페이스
 - 지정된 경우 RDP, VNC 및 SSH 인터페이스
- b. 필요한 경우 로그인 자격 증명을 입력합니다. 일부 인터페이스 유형은 로그인 자격 증명을 요구하지 않습니다.

- 서비스 계정을 사용하려면 서비스 계정 자격 증명 사용 확인란을 선택한 다음 서비스 계정의 이름을 선택합니다.

또는

- 인터페이스 유형에 대한 사용자 이름 및 암호를 입력합니다. 각각 최대 64 문자입니다.

14. 확인을 클릭합니다.

CC-SG 는 다음을 생성합니다.

- 하나의 가상 시스템에 대해 하나의 노드가 생성됩니다. 각 가상 시스템 노드는 VMW 뷰어 인터페이스, VMW 전원 인터페이스 및 기타 지정된 대역내 인터페이스를 가집니다. 가상 시스템 노드에는 가상 호스트 시스템의 가상 시스템 이름이 지정됩니다.
- 각 가상 호스트에 대해 하나의 노드. 각 가상 호스트는 VI 클라이언트 인터페이스를 가집니다. 가상 호스트 노드에는 IP 주소나 호스트 이름이 지정됩니다.
- 제어 시스템에 대해 하나의 노드. 제어 시스템 노드는 하나의 VI 클라이언트 인터페이스를 가집니다. 제어 시스템 노드는 VMware Virtual Center 로 이름이 지정됩니다.

가상 시스템이 있는 가상 호스트 추가

가상 호스트를 추가할 때 마법사는 가상 호스트에 포함된 가상 시스템의 추가를 안내합니다.

▶ 가상 시스템이 있는 가상 호스트를 추가하려면:

1. 노드 > 가상화를 선택합니다.
2. 가상 호스트 추가를 클릭합니다.
3. 노드 > 가상화를 선택합니다.
4. 가상 호스트 추가를 클릭합니다.
5. 호스트 이름/IP 주소: 가상 호스트에 대한 IP 주소 또는 호스트 이름을 입력합니다. 최대 64 문자입니다.
6. 연결 프로토콜: 가상 호스트와 CC-SG 사이에 HTTP 또는 HTTPS 통신을 지정합니다.
7. TCP 포트: TCP 포트를 입력합니다. 기본 포트는 443 입니다.
8. 확인 간격(초): 가상 호스트와 CC-SG 간에 시간 제한을 발생시키는 경과 시간(초)을 입력합니다.
9. 인증 정보를 입력합니다.

- 인증을 위해 서비스 계정을 사용하려면 서비스 계정 자격 증명 사용 확인란을 선택합니다. 서비스 계정 이름 메뉴에서 사용할 서비스 계정을 선택합니다.
- 또는
- 인증할 사용자 이름 및 암호를 입력합니다. 각각 최대 64 문자입니다.
10. 이 가상 호스트에 액세스하는 사용자가 자동으로 VI 클라이언트 인터페이스에 로그인할 수 있도록 하려면 VI 클라이언트용 단일 로그인 사용 확인란을 선택합니다. **옵션입니다.**
 11. 다음을 클릭합니다. **CC-SG** 는 가상 호스트의 가상 시스템을 검색합니다.
 12. 각 가상 시스템 옆의 구성 확인란을 선택하여 가상 시스템을 **CC-SG** 에 추가합니다. 각 연관된 가상 호스트도 구성됩니다. 하나의 가상 시스템에 대해 하나의 노드가 추가됩니다. 가상 호스트는 여러 가상 시스템과 연결될 수 있지만 하나의 가상 호스트 노드만 추가됩니다.
 13. **VNC, RDP** 또는 **SSH** 인터페이스를 가상 호스트 노드 및 가상 시스템 노드에 추가하려면 각 가상 시스템 옆의 확인란을 선택합니다. **옵션입니다.**
 14. 다음을 클릭합니다. **CC-SG** 는 추가될 인터페이스 유형 목록을 표시합니다. 각 유형에 대한 이름 및 로그인 자격 증명을 추가할 수 있습니다.
 15. 각 인터페이스 유형에 대해 이름 및 로그인 자격 증명을 입력합니다. 이름 및 로그인 자격 증명은 각 구성된 가상 시스템 노드 및 가상 호스트 노드에 추가된 모든 인터페이스가 공유합니다. **옵션입니다.**

각 인터페이스에 대해 개별적으로 이름 및 로그인 자격 증명을 추가하고자 할 경우 이 필드를 비어 두십시오.

인터페이스는 필드가 비어 있을 경우 노드 이름을 가집니다.

- a. 인터페이스의 이름을 입력합니다. 최대 32 문자입니다.
 - VI 클라이언트 인터페이스
 - VMware 뷰어 인터페이스
 - 가상 전원 인터페이스
 - 지정된 경우 RDP, VNC 및 SSH 인터페이스
- b. 필요할 경우 로그인 자격 증명을 입력합니다. 일부 인터페이스 유형은 로그인 자격 증명을 요구하지 않습니다.

- 서비스 계정을 사용하려면 서비스 계정 자격 증명 사용 확인란을 선택한 다음 서비스 계정의 이름을 선택합니다.

또는

- 인터페이스 유형에 대한 사용자 이름 및 암호를 입력합니다. 각각 최대 64 문자입니다.

16. 확인을 클릭합니다.

CC-SG 는 다음을 생성합니다.

- 하나의 가상 시스템에 대해 하나의 노드 각 가상 시스템 노드는 VMW 뷰어 인터페이스, VMW 전원 인터페이스 및 기타 지정된 대역내 인터페이스를 가집니다. 가상 시스템 노드는 가상 호스트 시스템에서 가상 시스템 이름으로 이름이 지정됩니다.
- 각 가상 호스트에 대해 하나의 노드. 각 가상 호스트는 VI 클라이언트 인터페이스를 가집니다. 가상 호스트 노드는 IP 주소나 호스트 이름으로 이름이 지정됩니다.

제어 시스템, 가상 호스트 및 가상 시스템 편집

CC-SG 에서 구성된 제어 시스템, 가상 호스트 및 가상 시스템을 편집하여 해당 등록 정보를 변경할 수 있습니다. 가상 시스템에 대한 구성 확인란을 선택 취소하여 CC-SG 에서 가상 시스템 노드를 삭제할 수 있습니다.

▶ 제어 시스템, 가상 호스트 및 가상 시스템을 편집하려면:

1. 노드 > 가상화를 선택합니다.
2. 편집할 제어 시스템이나 가상 호스트를 선택합니다.
3. 편집을 클릭합니다.
4. 필요한 경우 정보를 변경합니다. 전체 필드 설명에 대해서는 **가상 호스트 및 가상 시스템이 있는 제어 시스템 추가** (p. 76) 및 **가상 시스템이 있는 가상 호스트 추가** (p. 78)를 참조하십시오.
5. 다음을 클릭합니다.
6. CC-SG 에서 가상 시스템을 삭제하려면 구성 확인란을 선택 취소합니다. VNC, RDP 또는 SSH 인터페이스를 가상 호스트 노드 및 가상 시스템 노드에 추가하려면 각 가상 시스템 옆의 확인란을 선택합니다.

이 페이지에서 가상 시스템 노드 또는 가상 호스트 노드로부터 SSH, VNC 및 RDP 인터페이스를 제거할 수 없습니다. 노드 프로필에서 인터페이스를 삭제해야 합니다. 인터페이스 삭제 (p. 94)를 참조하십시오.

7. 다음을 클릭합니다. 가상 시스템 삭제를 선택한 경우 경고 메시지가 표시됩니다.
8. 각 인터페이스 유형에 대해 이름 및 로그인 자격 증명을 입력합니다. 이름 및 로그인 자격 증명은 각 구성된 가상 시스템 노드 및 가상 호스트 노드에 추가된 모든 인터페이스가 공유합니다. **옵션입니다.** 각 인터페이스에 대해 개별적으로 이름 및 로그인 자격 증명을 추가하고자 할 경우 이 필드를 비어 두십시오.
 - a. 인터페이스의 이름을 입력합니다(최대 32 자).
 - 가상 호스트 VI 클라이언트 인터페이스
 - VMware 뷰어 인터페이스
 - 가상 전원 인터페이스
 - 지정된 경우 RDP, VNC 및 SSH 인터페이스
 - b. 로그인 자격 증명을 입력합니다.
 - 서비스 계정을 사용하려면 서비스 계정 자격 증명 사용 확인란을 선택한 다음 서비스 계정의 이름을 선택합니다.

또는

 - 인터페이스 유형에 대한 사용자 이름 및 암호를 입력합니다. 각각 최대 64 문자입니다.
9. 확인을 클릭합니다.

제어 시스템 및 가상 호스트 삭제

CC-SG 에서 제어 시스템 및 가상 호스트를 삭제할 수 있습니다.

제어 시스템을 삭제할 경우 이와 연결된 가상 호스트 및 가상 시스템은 삭제되지 않습니다.

가상 호스트를 삭제할 경우 이와 연결된 제어 시스템 및 가상 시스템은 삭제되지 않습니다.

가상 시스템 노드는 연관된 제어 시스템이나 가상 호스트가 삭제될 때 자동으로 삭제되지 않습니다. **가상 시스템 노드 삭제** (p. 82)를 참조하십시오.

▶ **제어 시스템 및 가상 호스트를 삭제하려면:**

1. 노드 > 가상화를 선택합니다.
2. 목록에서 삭제할 제어 시스템 및 가상 호스트를 삭제합니다. 여러 항목을 삭제하려면 **Ctrl+클릭**을 사용합니다.
3. 삭제를 클릭합니다.

가상 시스템 노드 삭제

가상 시스템 노드를 삭제하는 방법에는 두 가지가 있습니다.

- 노드 삭제 기능을 사용합니다. **노드 삭제** (p. 73)를 참조하십시오.
- 가상 시스템에 대한 구성 확인란을 선택 취소합니다. **제어 시스템, 가상 호스트 및 가상 시스템 편집** (p. 80)을 참조하십시오.

가상 인프라 삭제

다음 단계에 따라 제어 시스템, 가상 호스트 및 가상 시스템을 포함한 전체 가상 인프라를 CC-SG 에서 삭제합니다.

▶ **가상 인프라를 삭제하려면:**

1. 각 가상 시스템에 대한 구성 확인란을 선택 취소하여 모든 가상 시스템 노드를 삭제합니다. **제어 시스템, 가상 호스트 및 가상 시스템 편집** (p. 80)을 참조하십시오.
2. 제어 시스템 및 가상 호스트를 삭제합니다. **제어 시스템 및 가상 호스트 삭제** (p. 82)를 참조하십시오.

제어 시스템 노드, 가상 호스트 노드 및 가상 시스템 노드와 인터페이스를 포함한 가상 인프라의 모든 구성요소가 삭제됩니다.

CC-SG와 가상 인프라 동기화

동기화를 하면 CC-SG에는 가상 인프라에 대한 가장 최신 정보가 저장됩니다. 동기화를 하면 각 가상 시스템 노드 및 가상 인프라 분포도 정보와 관련된 정보가 업데이트합니다.

모든 제어 시스템 및 구성된 가상 호스트에 대해 자동 일일 동기화를 구성할 수 있습니다. 언제든지 선택된 제어 시스템과 가상 호스트의 동기화도 수행할 수 있습니다.

가상 인프라 동기화

가상 인프라와 CC-SG의 동기화를 수행할 수 있습니다.

동기화를 위해 제어 시스템을 선택한 경우 가상 호스트의 선택 여부와 관계 없이 연관된 가상 호스트도 동기화됩니다.

▶ 가상 인프라를 동기화하려면:

1. 노드 > 가상화를 선택합니다.
2. 노드 목록에서 동기화할 노드를 선택합니다. 여러 항목을 삭제하려면 Ctrl+클릭을 사용합니다.
3. 동기화를 클릭합니다. 가상 인프라가 마지막 동기화 이후 변경된 경우 CC-SG에 정보가 업데이트됩니다.
 - Secure Gateway에서 구성 열에는 CC-SG에 구성된 가상 시스템이나 호스트의 수가 표시됩니다.
 - 마지막 동기화 날짜는 동기화 날짜 및 시간을 표시합니다.
 - 노드 상태 열은 가상 노드의 상태를 표시합니다.

가상 인프라의 일일 동기화 활성화 또는 비활성화

가상 인프라와 CC-SG의 자동 동기화를 구성할 수 있습니다. 자동 동기화는 지정한 시간에 매일 진행됩니다.

▶ 가상 인프라의 일일 동기화를 활성화하려면:

1. 노드 > 가상화를 선택합니다.
2. 일일 자동 동기화 활성화 확인란을 선택합니다.
3. 시작 시간 필드에 일일 동기화가 발생할 시간을 입력합니다.
4. 업데이트를 클릭합니다.

▶ 가상 인프라의 일일 동기화를 비활성화하려면:

1. 노드 > 가상화를 선택합니다.
2. 일일 자동 동기화 활성화 확인란을 선택 취소합니다.
3. 업데이트를 클릭합니다.

가상 호스트 노드의 재부팅 또는 강제 재부팅

가상 호스트 서버를 재부팅 또는 강제 재부팅할 수 있습니다. 재부팅 작업은 정비 모드에 있을 때 가상 호스트 서버의 정상적인 재부팅을 수행합니다. 강제 재부팅 작업은 정비 모드에 있지 않을 경우 가상 호스트 서버를 강제로 재부팅합니다.

이 명령에 액세스하려면 노드 대역내 액세스 및 노드 전원 제어 권한을 가지고 있어야 합니다. 재부팅 또는 강제 재부팅할 노드에 액세스하는 규정이 지정된 사용자 그룹에도 속해 있어야 합니다.

▶ 가상 호스트 노드를 재부팅 또는 강제 재부팅하려면:

1. 재부팅 또는 강제 재부팅할 가상 호스트 노드를 선택합니다.
2. 가상 호스트 데이터 탭을 클릭합니다.
3. 재부팅 또는 강제 재부팅을 클릭합니다.

가상 분포도 보기 액세스

분포도 보기는 트리 구조로서 선택한 노드와 연관된 제어 시스템, 가상 호스트 및 가상 시스템의 관계를 보여줍니다.

분포도 보기를 열려면 장치, 포트 및 노드 관리 권한이 있어야 합니다.

▶ 가상 노드 프로필에서 분포도 보기를 엽니다.

1. 노드 프로필에서 노드에 대한 가상화 정보를 포함하고 있는 다음 탭을 클릭합니다. 노드 유형에 따라 가상 시스템 데이터 탭, 가상 호스트 데이터 탭 또는 제어 시스템 탭이 해당됩니다.
2. 분포도 보기 링크를 클릭합니다. 분포도 보기가 새 창에 열립니다. CC-SG 에 구성된 가상 노드가 링크로 표시됩니다.
 - 가상 노드에 대한 노드 프로필을 열려면 노드 링크를 더블 클릭합니다.
 - 노드에 연결할 인터페이스 링크를 더블 클릭합니다.

- 노드에 대한 전원 제어 페이지를 열려면 가상 전원 인터페이스 링크를 더블 클릭합니다.

노드 연결

노드에 인터페이스가 있는 경우 여러 방법으로 인터페이스를 통해 해당 노드에 연결할 수 있습니다. Raritan의 **CommandCenter Secure Gateway 사용자 설명서**를 참조하십시오.

▶ 노드에 연결하려면:

1. 노드 탭을 클릭합니다.
2. 연결할 노드를 선택하고
 - 인터페이스 표에서 연결할 인터페이스의 이름을 클릭합니다.
 또는
 - 노드 탭에서 연결할 노드 바로 밑에 있는 인터페이스의 목록을 확장합니다. 연결할 인터페이스의 이름을 더블 클릭하거나 인터페이스를 마우스 오른쪽 버튼으로 클릭하고 연결을 선택합니다.

노드 핑

CC-SG에서 노드를 핑하면 연결이 활성 상태인지 확인할 수 있습니다.

▶ 노드에 핑하려면:

1. 노드 탭을 클릭하고 핑할 노드를 선택합니다.
2. 노드 > 노드 핑을 선택합니다. 화면에 핑 결과가 나타납니다.

인터페이스 추가, 편집 및 삭제

인터페이스 추가

*참고: 제어 시스템, 가상 호스트 및 가상 시스템과 같은 가상 노드에 대한 인터페이스는 노드 > 가상화 아래의 가상화 도구를 사용하여만 추가할 수 있습니다. **CC-SG**에서 가상 인프라 구성 (p. 75)을 참조하십시오.*

▶ 인터페이스를 추가하려면:

1. 기존 노드의 경우: 노드 탭을 클릭하고 인터페이스를 추가할 노드를 선택합니다. 노드 프로필 화면이 나타나면 인터페이스 섹션에서 추가를 클릭합니다.

새 노드를 추가할 경우: 노드 추가 화면의 인터페이스 섹션에서 추가를 클릭합니다.

인터페이스 추가 창이 열립니다.

2. 인터페이스 유형 드롭다운 메뉴를 클릭하고 노드에 대한 연결 유형을 선택합니다.

대역내 연결:

- 대역내 - DRAC KVM: DRAC 인터페이스를 통해 Dell DRAC 서버에 대한 KVM 연결을 생성하려면 이 항목을 선택합니다. 나중에 DRAC 전원 인터페이스를 구성해야 합니다.
- 대역내 - iLO 프로세서 KVM: iLO 또는 RILOE 인터페이스를 통해 HP 서버에 대한 KVM 연결을 생성하려면 이 항목을 선택합니다.
- 대역내 - RDP: Remote Desktop Protocol 을 사용하여 노드에 대한 KVM 연결을 생성하려면 이 항목을 선택합니다(예: Windows 서버의 원격 데스크탑 연결).
- 대역내 - RSA KVM: RSA 인터페이스를 통해 IBM RSA 서버에 대한 KVM 연결을 생성하려면 이 항목을 선택합니다. 나중에 RSA 전원 인터페이스를 구성해야 합니다.
- 대역내 - SSH: 노드에 대한 SSH 연결을 생성하려면 이 항목을 선택합니다.
- 대역내 - VNC: VNC 서버 소프트웨어를 통해 노드에 대한 KVM 연결을 생성하려면 이 항목을 선택합니다.

대역내 연결을 위한 인터페이스 (p. 88)를 참조하십시오.

대역외 연결:

- 대역외 - KVM: Raritan KVM 장치(KX, KX101, KSX, IP-Reach, Paragon II)를 통해 노드에 대한 KVM 연결을 생성하려면 이 항목을 선택합니다.
- 대역외 - 직렬: Raritan 직렬 장치(SX, KSX)를 통해 노드에 대한 직렬 연결을 생성하려면 이 항목을 선택합니다.
대역외 KVM 대역외 직렬 연결을 위한 인터페이스 (참조 "대역외 KVM, 대역외 직렬 연결을 위한 인터페이스" p. 88)를 참조하십시오.

전원 제어 연결:

- 전원 제어 - DRAC: Dell DRAC 서버에 대한 전원 제어 연결을 생성하려면 이 항목을 선택합니다.
- 전원 제어 - iLO 프로세서: HP iLO/RILOE 서버에 대한 전원 제어 연결을 생성하려면 이 항목을 선택합니다.
- 전원 제어 - IPMI: IPMI 연결을 통해 노드에 대한 전원 제어 연결을 생성하려면 이 항목을 선택합니다.
- 전원 제어 - RSA: RSA 서버에 대한 전원 제어 연결을 생성하려면 이 항목을 선택합니다.

DRAC, RSA 및 ILO 프로세서 전원 제어 연결을 위한 인터페이스 (p. 89) 및 **IPMI 전원 제어 연결을 위한 인터페이스** (p. 90)를 참조하십시오.

관리된 전원 탭 연결:

- 관리된 전원 탭: Raritan 전원 탭 또는 Dominion PX 장치를 통해 전원을 제공한 노드에 대한 전원 제어 연결을 생성하려면 이 항목을 선택합니다.

관리된 전원 연결을 위한 인터페이스 (참조 "관리된 전원 탭 연결을 위한 인터페이스" p. 89)를 참조하십시오.

웹 브라우저 연결:

- 웹 브라우저: 이 항목을 선택하여 내장 웹 서버를 가진 장치에 대한 연결을 생성합니다.

웹 브라우저 인터페이스 (p. 91)를 참조하십시오.

3. 기본 이름은 선택한 인터페이스 유형에 따라 이름 필드에 표시됩니다. 이름을 변경할 수 있습니다. 이 이름은 노드 목록의 인터페이스 옆에 나타납니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.

대역내 연결을 위한 인터페이스

대역내 연결에는 RDP, VNC, SSH, RSA KVM, iLO 프로세서 KVM, DRAC KVM 및 TELNET 이 있습니다.

Telnet 은 안전한 액세스 방법이 아닙니다. 모든 사용자 이름, 암호 및 트래픽이 일반 텍스트로 전송됩니다.

▶ 대역내 연결을 위한 인터페이스를 추가하려면:

1. IP 주소/호스트 이름 필드에 이 인터페이스의 IP 주소 또는 호스트 이름을 입력합니다.
2. 필요한 경우 TCP 포트 필드에 이 연결의 TCP 포트를 입력합니다. **옵션입니다.**
3. RDP 인터페이스의 경우 콘솔 또는 원격 사용자를 선택합니다. 콘솔 사용자가 노드에 액세스할 때 다른 모든 사용자는 연결 해제됩니다. 여러 원격 사용자는 동시에 노드를 액세스할 수 있습니다.
4. 인증 정보를 입력합니다.
 - 인증을 위해 서비스 계정을 사용하려면 서비스 계정 자격 증명 사용 확인란을 선택합니다. 서비스 계정 이름 메뉴에서 사용할 서비스 계정을 선택합니다.또는
 - 인증할 사용자 이름 및 암호를 입력합니다. VNC 인터페이스의 경우 암호만 필요합니다.
5. 해당 언어의 키보드 레이아웃을 선택합니다.
6. 설명 필드에 이 인터페이스의 설명을 입력합니다. **옵션입니다.**
7. 확인을 클릭하여 변경 사항을 저장합니다.

대역외 KVM, 대역외 직렬 연결을 위한 인터페이스

▶ 대역외 KVM 또는 대역외 직렬 연결을 위한 인터페이스를 추가하려면:

1. 애플리케이션 이름: 목록에서 인터페이스를 가진 노드에 연결하는데 사용할 애플리케이션을 선택합니다. CC-SG 에서 브라우저에 기반한 애플리케이션을 자동으로 선택할 수 있도록 하려면 자동 탐지를 선택합니다.

2. **Raritan 장치 이름:** 이 노드에 대한 액세스를 제공하는 Raritan 장치를 선택합니다. 장치를 이 목록에 표시하려면 먼저 CC-SG에 추가해야 합니다.
3. **Raritan 포트 이름:** 이 노드에 대한 액세스를 제공하는 Raritan 장치의 포트를 선택합니다. 포트는 이 목록에 나타내기 전에 CC-SG에 구성되어야 합니다. 직렬 연결에서 전송 속도, 패리티 및 흐름 제어 값은 포트의 구성에 따라 입력됩니다.
4. 설명 필드에 이 인터페이스의 설명을 입력합니다. **옵션입니다.**
5. 확인을 클릭하여 변경 사항을 저장합니다.

DRAC, RSA 및 ILO 프로세서 전원 제어 연결을 위한 인터페이스

▶ DRAC, RSA 및 ILO 프로세서 전원 제어 연결을 위한 인터페이스를 추가하려면:

1. IP 주소/호스트 이름 필드에 이 인터페이스의 IP 주소 또는 호스트 이름을 입력합니다.
2. 필요한 경우 TCP 포트 필드에 이 연결의 TCP 포트를 입력합니다. **옵션입니다.**
3. 인증 정보를 입력합니다.
 - 인증을 위해 서비스 계정을 사용하려면 서비스 계정 자격 증명 사용 확인란을 선택합니다. 서비스 계정 이름 메뉴에서 사용할 서비스 계정을 선택합니다.
- 또는
 - 인증할 사용자 이름 및 암호를 입력합니다.
4. 설명 필드에 이 인터페이스의 설명을 입력합니다. **옵션입니다.**
5. 확인을 클릭하여 변경 사항을 저장합니다.

관리된 전원 탭 연결을 위한 인터페이스

KX를 관리 장치로서 지정하는 관리된 전원 탭을 생성할 경우 지정하는 콘센트는 연관된 노드 이름으로 바뀝니다

▶ 관리된 전원 탭 연결을 위한 인터페이스를 추가하려면:

1. 관리 장치:
 - 전원 탭이 연결된 Raritan 장치를 선택합니다. 장치는 CC-SG에 추가되어야 합니다.
- 또는

- 이 전원 제어 인터페이스가 다른 Raritan 장치에 연결되지 않은 IP 네트워크의 PX 장치를 사용하는 경우 Dominion PX 를 선택합니다.
2. 관리 포트: 전원 탭이 연결된 Raritan 장치의 포트를 선택합니다. 이 필드는 관리 장치로 PX 를 선택하면 비활성화됩니다.
 3. 전원 탭 이름: 노드에 전원을 공급하는 전원 탭 또는 PX 장치를 선택합니다. 전원 탭 또는 PX 장치는 CC-SG 에 구성되어야 이 목록에 표시됩니다.
 4. 콘센트 이름: 노드가 연결된 콘센트 이름을 선택합니다.
옵션입니다.
 5. 설명 필드에 이 인터페이스의 설명을 입력합니다.
 6. 확인을 클릭하여 변경 사항을 저장합니다.

IPMI 전원 제어 연결을 위한 인터페이스

▶ IPMI 전원 제어 연결을 위한 인터페이스를 추가하려면:

1. IP 주소/호스트 이름 필드에 이 인터페이스의 IP 주소 또는 호스트 이름을 입력합니다.
 2. UDP 포트 필드에 이 인터페이스의 UDP 포트 번호를 입력합니다.
 3. 인증: 이 인터페이스에 연결하기 위한 인증 시스템을 선택합니다.
 4. 확인 간격(초) 필드에 이 인터페이스의 확인 간격을 입력합니다.
 5. 인증 정보를 입력합니다.
 - 인증을 위해 서비스 계정을 사용하려면 서비스 계정 자격 증명 사용 확인란을 선택합니다. 서비스 계정 이름 메뉴에서 사용할 서비스 계정을 선택합니다.
- 또는
- 인증할 사용자 이름 및 암호를 입력합니다. **옵션입니다.**
6. 설명 필드에 이 인터페이스의 설명을 입력합니다.
 7. 확인을 클릭하여 변경 사항을 저장합니다.

웹 브라우저 인터페이스

Dominion PX와 같이 내장 웹 브라우저를 가진 장치에 연결을 생성하기 위해 웹 브라우저 인터페이스를 추가할 수 있습니다. **예제: PX 노드에 웹 브라우저 인터페이스 추가** (p. 93)를 참조하십시오. 웹 브라우저 인터페이스는 RSA, DRAC 또는 ILO 프로세서 카드와 연관된 웹 애플리케이션과 같은 모든 웹 애플리케이션에 연결하는데 사용할 수도 있습니다.

웹 브라우저 인터페이스는 웹 애플리케이션이 세션 ID와 같이 사용자 이름 및 암호 이외의 정보를 요구할 경우 자동 로그인할 수 없습니다.

사용자는 웹 브라우저 인터페이스에 액세스하기 위해 노드 대역내 액세스 권한을 가지고 있어야 합니다.

구성된 DNS를 가지고 있어야 하며 그렇지 않을 경우 URL이 해석되지 않습니다. IP 주소를 위해 구성된 DNS를 가지고 있을 필요가 없습니다.

▶ 웹 브라우저 인터페이스를 추가하려면:

1. 웹 브라우저 인터페이스의 기본 이름은 Web Browser(웹 브라우저)입니다. 이름 필드에서 이름을 변경할 수 있습니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.
2. 웹 애플리케이션을 위한 URL이나 도메인 이름을 URL 필드에 입력합니다. 웹 애플리케이션이 사용자 이름과 암호를 읽을 것으로 기대되는 URL을 입력해야 한다는 점을 기억하십시오. 최대 길이는 120 문자입니다. 올바른 형식은 다음 예제를 따르십시오.
 - http(s)://192.168.1.1/login.asp
 - http(s)://www.example.com/cgi/login
 - http(s)://example.com/home.html
3. 인증 정보를 입력합니다. **옵션입니다.**
 - 인증을 위해 서비스 계정을 사용하려면 서비스 계정 자격 증명 사용 확인란을 선택합니다. 서비스 계정 이름 메뉴에서 사용할 서비스 계정을 선택합니다.

또는

- 인증할 사용자 이름 및 암호를 입력합니다. 이 인터페이스에 액세스할 수 있는 사용자 이름과 암호를 입력합니다.

참고: DRAC, ILO 및 RSA 웹 애플리케이션에 대한 사용자 인증 정보를 입력하십시오. 그렇지 않으면 연결이 실패합니다.

4. 사용자 이름 필드 및 암호 필드에서 웹 애플리케이션의 로그인 화면에서 사용된 사용자 이름 및 암호 필드에 대한 필드 이름을 입력합니다. 필드 레이블이 아니라 필드 이름을 찾으려면 로그인 화면의 HTML 소스를 봐야 합니다. **웹 브라우저 인터페이스 추가를 위한 팁** (p. 92)을 참조하십시오.
5. 설명 필드에 이 인터페이스의 설명을 입력합니다. 옵션입니다.
6. 확인을 클릭하여 변경 사항을 저장합니다.

웹 브라우저 인터페이스 추가를 위한 팁

웹 브라우저 인터페이스를 구성하려면 사용자 이름 및 암호 필드의 실제 필드 이름을 식별할 수 있도록 HTML 소스로부터 일부 정보를 수집해야 합니다. 모든 공급업체는 이 인증 필드를 다르게 구현하며 이 필드의 이름은 특정 장치에 대한 펌웨어 버전들 사이에서 뿐만 아니라 장치에 따라 다릅니다. 이러한 이유로 필드 이름을 찾는 간단한 방법은 없습니다. 하나의 가능한 방법은 아래 절차를 참조하십시오.

소프트웨어 엔지니어 또는 시스템 관리자의 도움을 받아 적절한 필드 이름을 찾아 식별할 수 있습니다.

▶ 필드 이름을 찾기 위한 팁:

1. 웹 애플리케이션의 로그인 페이지 HTML 소스 코드에서 사용자 이름 및 암호와 같은 필드 레이블을 검색합니다.
2. 필드 레이블을 찾은 경우 인접 코드에서 다음과 같은 태그를 찾습니다. `name="user"`

따옴표 안의 단어가 필드 이름입니다.

예제: PX 노드에 웹 브라우저 인터페이스 추가

Dominion PX 관리된 전원 탭이 CC-SG 에 노드로서 추가될 수 있습니다. 그런 다음 사용자가 Dominion PX 의 웹 기반 관리 애플리케이션에 액세스할 수 있도록 하는 웹 브라우저 인터페이스를 노드에 추가할 수 있습니다.

▶ **Dominion PX 노드를 위한 웹 브라우저 인터페이스를 추가하려면 다음 값을 사용하십시오.**

URL: <DOMINION PX IP ADDRESS>/auth.asp

사용자 이름: Dominion PX 관리자의 사용자 이름

암호: Dominion PX 관리자의 암호

Username 필드 = login

Password 필드 = password

인터페이스 추가 결과

노드에 인터페이스를 추가하면 인터페이스는 인터페이스 표 및 노드 추가 또는 노드 프로필 화면의 기본 인터페이스 드롭다운 메뉴에 표시됩니다. 드롭다운 메뉴를 클릭하면 노드에 연결할 때 사용할 기본 인터페이스를 선택할 수 있습니다.

노드 추가 또는 노드 프로필 화면의 변경 사항을 저장하면 인터페이스의 이름도 노드 목록에 표시되어 액세스를 제공하는 노드 아래에 중첩됩니다.

KX 를 관리 장치로서 지정하는 관리된 전원 탭을 추가할 경우 지정하는 콘센트는 연관된 노드 이름으로 바뀝니다

인터페이스 편집

▶ **인터페이스 편집:**

1. 노드 탭을 클릭하고 편집할 인터페이스가 있는 노드를 선택합니다. 노드 프로필 페이지가 열립니다.
2. 인터페이스 탭에서 편집할 인터페이스의 행을 선택합니다.
3. 편집을 클릭합니다.
4. 필요한 경우 필드를 편집합니다. 필드의 자세한 내용은 **인터페이스 추가** (p. 86)를 참조하십시오. 일부 필드는 읽기 전용입니다.

5. 확인을 클릭하여 변경 사항을 저장합니다.

인터페이스 삭제

가상 시스템 노드에서 VMW 뷰어 인터페이스 또는 VMW 전원 인터페이스를 삭제할 수 없습니다.

▶ **노드에서 인터페이스 삭제:**

1. 노드 탭을 클릭합니다.
2. 삭제할 인터페이스를 사용한 노드를 클릭합니다.
3. 인터페이스 표에서 삭제할 인터페이스의 행을 클릭합니다.
4. 삭제를 클릭합니다. 확인 메시지가 나타납니다.
5. 예를 클릭하여 인터페이스를 삭제합니다.

인터페이스 책갈피 설정

특정 인터페이스를 통해 노드에 자주 액세스하는 경우 책갈피로 설정하여 브라우저에서 쉽게 이용할 수 있습니다.

▶ **브라우저에서 인터페이스를 책갈피로 설정하려면:**

1. 노드 탭에서 책갈피로 설정할 인터페이스를 선택합니다.
인터페이스를 보기 위해 노드를 확장해야 합니다.
2. 노드 > 노드 인터페이스 책갈피 설정을 선택합니다.
3. URL 을 클립보드에 복사합니다.
4. 확인을 클릭합니다. URL 이 클립보드에 복사됩니다.
5. 새 브라우저 창을 열고 URL 을 주소 필드로 붙여넣기합니다.
6. URL 에 연결하려면 ENTER 키를 누릅니다.
7. URL 을 브라우저에 책갈피로 추가합니다(즐겨찾기라고도 함).

▶ **Internet Explorer 에서 인터페이스를 책갈피 설정하려면(인터페이스를 즐겨찾기에 추가하기):**

1. 노드 탭에서 책갈피로 설정할 인터페이스를 선택합니다.
인터페이스를 보기 위해 노드를 확장해야 합니다.
2. 노드 > 노드 인터페이스 책갈피 설정을 선택합니다.
3. 책갈피 추가(IE 전용)을 선택합니다.

4. 책갈피의 기본 이름이 책갈피 이름 필드에 표시됩니다. 이 이름을 변경할 수 있으며, Internet Explorer의 즐겨찾기 목록에 표시됩니다.
5. 확인을 클릭합니다. 즐겨찾기 추가 창이 열립니다.
6. 즐겨찾기 목록에 책갈피를 추가하려면 확인을 클릭합니다.

▶ **책갈피 설정된 인터페이스를 액세스하려면:**

1. 브라우저 창을 엽니다.
2. 브라우저의 책갈피 목록에서 책갈피 설정된 인터페이스를 선택합니다.
3. CC-SG 액세스 클라이언트가 나타날 때 인터페이스에 액세스 권한이 있는 사용자로 로그인합니다. 인터페이스 연결이 열립니다.

▶ **모든 노드에 대한 즐겨찾기 URL을 가져오려면:**

- 노드 자산 보고서에서 모든 노드에 대한 즐겨찾기 URL을 가져올 수 있습니다. **노드 자산 보고서** (p. 158)를 참조하십시오.

노드에 직접 포트 액세스 구성

즐거찾기 노드 인터페이스 기능을 이용하여 노드에 직접 포트 액세스를 구성할 수 있습니다.

인터페이스 책갈피 설정 (p. 94)을 참조하십시오.

노드 범주 및 요소 대량 복사

대량 복사 명령을 사용하면 한 노드에 지정된 범주와 요소를 다른 여러 노드로 복사할 수 있습니다. 이 프로세스에서 복사되는 속성은 범주와 요소뿐입니다.

▶ **노드 범주 및 요소를 대량 복사하려면:**

1. 노드 탭을 클릭하고 노드를 선택합니다.
2. 노드 > 대량 복사를 선택합니다.
3. 모든 노드 목록에서 노드 이름 필드에 있는 노드의 범주 및 요소를 복사할 노드를 선택합니다.
 - 오른쪽 화살표 버튼을 클릭하여 선택 노드 목록에 노드를 추가합니다.
 - 선택 노드 목록에서 노드를 선택하고 왼쪽 화살표를 클릭하여 목록에서 제거합니다.

4. 확인을 클릭하여 대량 복사합니다. 노드 범주 및 요소가 복사되었을 때 메시지가 표시됩니다.

채팅 사용

채팅은 동일한 노드에 연결된 사용자들이 서로 통신할 수 있는 방법을 제공합니다. 해당 노드의 채팅 세션을 시작하려면 노드에 연결되어 있어야 합니다. 동일한 노드에 있는 사용자만 서로 채팅할 수 있습니다.

▶ **채팅 세션을 시작하려면:**

1. 노드 > 채팅 > 채팅 세션 시작을 선택합니다.
2. 왼쪽 아래 필드에 메시지를 입력하고 보내기를 클릭합니다. 왼쪽 위 필드에 모든 사용자가 볼 수 있는 메시지가 표시됩니다.

▶ **이미 진행 중인 채팅 세션에 참가하려면:**

- 노드 > 채팅 > 채팅 세션 표시를 선택합니다.

▶ **채팅 세션을 종료하려면:**

1. 채팅 세션에서 닫기를 클릭합니다. 확인 메시지가 나타납니다.
 - 모든 참가자에 대한 채팅 세션을 닫으려면 예를 클릭합니다.
 - 채팅 세션을 종료하지만 다른 참가자에 대한 세션은 놔두려면 아니오를 클릭합니다.

노드 그룹 추가, 편집 및 삭제

노드 그룹 개요

노드 그룹은 노드를 세트로 구성하는 데 사용됩니다. 노드 그룹은 이 특정 노드 세트에 대한 액세스를 허용하거나 거부하는 규정의 기본이 됩니다. **규정 추가** (p. 116)를 참조하십시오. 노드는 선택 방법을 이용하여 수동으로 또는 설명 방법을 사용하여 일반적인 속성 세트를 설명하는 Boolean 식을 생성하여 그룹화할 수 있습니다.

설정 안내서를 사용하여 노드의 범주 및 요소를 생성한 경우 일반적인 속성에 따라 노드를 구성하기 위한 몇 가지 방법이 생성됩니다. CC-SG는 이러한 요소를 기반으로 기본 액세스 규정을 자동 생성합니다. 범주 및 요소 생성에 대한 자세한 내용은 **연관체, 범주 및 요소** (p. 22)를 참조하십시오.

▶ 노드 그룹을 보려면:

- 연관체 > 노드 그룹을 선택합니다. 노드 그룹 관리자 창이 나타납니다. 기존의 노드 그룹 목록은 왼쪽에 표시되고 선택한 노드 그룹에 대한 상세 내용은 기본 패널에 표시됩니다.
 - 기존의 노드 그룹 목록이 왼쪽에 표시됩니다. 노드 그룹을 클릭하여 노드 그룹 관리자에서 그룹의 상세 내용을 봅니다.
 - 그룹이 임의로 구성된 경우 그룹에 있는 노드와 그룹에 없는 노드의 목록을 보여 주는 노드 선택 탭이 표시됩니다.
 - 그룹이 일반적인 속성을 기반으로 구성된 경우 그룹의 노드 선택을 제어하는 규칙을 보여 주는 노드 설명 탭이 표시됩니다.
 - 노드 그룹 목록에서 노드를 검색하려면 목록 맨 아래의 검색 필드에 문자열을 입력하고 검색을 클릭합니다. 검색 방법은 내 프로필 화면을 통해 구성됩니다. **사용자 및 사용자 그룹** (p. 102)을 참조하십시오.
 - 속성을 기반으로 그룹을 보는 경우 노드 보기를 클릭하여 현재 노드 그룹에 있는 노드의 목록을 표시합니다. 노드와 모든 속성을 표시하는 노드 그룹에 있는 노드 창이 열립니다.

노드 그룹 추가

▶ 노드 그룹 편집:

1. 연관체 > 노드 그룹을 선택합니다. 노드 그룹 관리자 창이 나타납니다.

2. 그룹 > 추가를 선택합니다. 노드 그룹의 템플릿이 나타납니다.
3. 그룹 이름 필드에 생성할 노드 그룹의 이름을 입력합니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.
4. 그룹에 노드를 추가할 수 있는 두 가지 방법은 노드 선택 및 노드 설명입니다. 노드 선택 방법을 사용하면 사용 가능한 노드의 목록에서 노드를 선택하여 그룹에 노드를 임의로 지정할 수 있습니다. 노드 설명 방법을 사용하면 노드를 설명하는 규칙을 지정할 수 있습니다. 설명과 일치하는 노드는 그룹에 포함됩니다.

설명 방법 대 선택 방법

그룹이 범주 및 요소와 같은 노드 또는 장치의 몇 가지 속성을 기초로하기 원할 경우 설명 방법을 사용합니다. 설명 방법의 이점은 설명된 것과 동일한 속성을 가진 장치나 노드를 추가할 경우 자동으로 그룹에 추가된다는 것입니다.

특정 노드의 그룹을 수동으로 만들기 원할 경우 선택 방법을 사용합니다. CC-SG 에 추가된 새 노드 및 장치는 이 그룹에 자동으로 추가되지 않습니다. CC-SG 에 추가한 후에 그룹에 새 노드나 장치를 수동으로 추가해야 합니다.

이 두 방법은 조합할 수 없습니다.

그룹이 하나의 방법으로 생성되면 동일한 방법을 사용하여 편집해야 합니다. 방법을 전환하면 현재 그룹 설정을 덮어 씩니다.

노드 선택

▶ 노드 선택 옵션을 사용하여 노드 그룹을 추가하려면:

1. 노드 선택 탭을 클릭합니다.
2. 장치 이름 드롭다운 메뉴를 클릭하고 해당 장치에서 인터페이스를 가진 노드만 표시하도록 사용 가능 목록을 필터링할 장치를 선택합니다.
3. 사용 가능 목록에서 그룹에 추가할 장치를 선택한 다음 추가를 클릭하여 선택 목록으로 장치를 이동합니다. 선택 목록의 노드가 그룹에 추가됩니다.
4. 그룹에서 노드를 제거하려면 선택 목록에서 노드 이름을 선택한 다음 제거를 클릭합니다.
5. 사용 가능 또는 선택 목록에서 노드를 검색할 수 있습니다. 목록 아래의 필드에 검색 용어를 입력한 다음 이동을 클릭합니다.

6. 언제든지 이 그룹에 있는 노드에 대한 액세스를 허용하는 규정을 생성하려면 이 그룹의 전체 액세스 규정 생성을 선택합니다.
7. 그룹에 노드를 추가하고 나면 추가를 클릭하여 노드 그룹을 생성합니다. 그룹은 왼쪽에 있는 노드 그룹 목록에 추가됩니다.

노드 설명

▶ 노드 설명 옵션을 사용하여 노드 그룹을 추가하려면:

1. 노드 선택 탭을 클릭합니다.
2. 새 행 추가를 클릭하여 새 규칙에 대한 표에 행을 추가합니다. 규칙에는 노드를 비교할 수 있는 수식 형식이 적용됩니다.
3. 행에서 각 열을 더블 클릭하여 적절한 셀을 드롭다운 메뉴로 바꾼 다음 각 구성요소의 적절한 값을 선택합니다.
 - 접두어 - 비워 두거나 **NOT** 을 선택합니다. **NOT** 을 선택한 경우 이 규칙은 나머지 수식과 반대값으로 필터링됩니다.
 - 범주 - 규칙에서 평가되는 속성을 선택합니다. 연관체 관리자에서 생성한 모든 범주를 여기서 사용할 수 있습니다. 노드 이름 및 인터페이스도 포함됩니다.
 - 연산자 - 범주와 요소 항목 사이에서 수행할 비교 작업을 선택합니다. 사용 가능한 연산자는 = (같음), LIKE (이름으로 요소를 찾는 데 사용) 및 <>(같지 않음).
 - 요소 - 비교할 범주 속성의 값을 선택합니다. 선택한 범주와 연관된 요소만 여기에 표시됩니다(예: "부서" 범주를 평가하는 경우 "위치" 요소가 여기에 나타나지 않음).

규칙 이름- 이 행에서 규칙에 지정된 이름입니다. 이러한 값은 편집할 수 없습니다. 약식 표현 필드에 설명을 입력하려면 이러한 값을 사용합니다.

예제 규칙으로는 **Department = Engineering** 이 있을 수 있으며, 여기서 이 규칙은 범주 "Department"가 "Engineering"으로 설정된 모든 노드를 설명하고 있음을 의미합니다. 이것은 노드 추가 작업 중에 연관체를 구성할 때 발생한 문제입니다.
4. 다른 규칙을 추가하려면 새 행 추가를 다시 클릭하고 필요한 구성을 설정합니다. 여러 규칙을 구성하면 노드를 평가하는 여러 기준을 제공하여 보다 정확한 설명이 가능해 집니다.
 - 규칙을 제거하려면 표에서 규칙을 강조 표시한 다음 행 제거를 클릭합니다.

5. 규칙 표는 노드를 평가하는 기준에만 사용할 수 있습니다. 노드 그룹에 대한 설명을 입력하려면 약식 표현 필드에 규칙 이름별로 규칙을 추가합니다. 설명에 한 가지 규칙만 필요한 경우 해당 필드에 해당 규칙의 이름을 입력합니다. 여러 규칙을 평가하는 경우 서로 연관된 규칙을 설명하는 데 논리 연산자 세트를 사용하여 해당 필드에 규칙을 입력합니다.

- **& - AND** 연산자. 노드는 설명(또는 설명의 해당 섹션)을 true(참)로 평가하려면 이 연산자의 양쪽에 있는 규칙을 충족해야 합니다.
- **| - OR** 연산자. 노드는 설명(또는 설명의 해당 섹션)을 true(참)로 평가하려면 이 연산자의 양쪽에 있는 규칙 중 한 가지만 충족해야 합니다.
- **(and)**- 그룹화 연산자입니다. 괄호 안에 포함된 하위 섹션으로 설명을 나눕니다. 나머지 설명을 노드와 비교하기 전에 먼저 괄호 안의 섹션을 평가합니다. 삽입 그룹은 다른 삽입 그룹 안에 중첩될 수 있습니다.

예제 1: 엔지니어링 부서에 속하는 노드를 설명하려면 **Department = Engineering** 이라는 규칙을 생성합니다. 이 규칙은 **Rule0** 이 됩니다. 그리고 나서 약식 표현 필드에 **Rule0** 을 입력합니다.

예제 2: 엔지니어링 부서에 속하거나 Philadelphia 에 있으며 모든 시스템의 메모리가 1GB 가 되도록 지정하는 장치 그룹을 설명하는 경우 세 가지 규칙을 생성해야 합니다. **Department = Engineering(Rule0) Location = Philadelphia(Rule1) Memory = 1GB(Rule2)**. 이러한 규칙은 서로 연관된 상태로 정렬되어야 합니다. 장치는 엔지니어링 부서에 속하거나 Philadelphia 에 있을 수 있기 때문에 **OR** 연산자 **|**를 사용하여 다음과 같이 두 규칙을 연결합니다. **Rule0|Rule1**. 괄호로 닫아 이 비교를 먼저 설정합니다. **(Rule0|Rule1)**. 장치는 이 비교를 만족하고(**AND**) **1GB** 의 메모리를 포함해야 하기 때문에 **&**을(를) 사용하여 이 섹션을 **Rule2: (Rule0|Rule1)&Rule2**. 약식 표현 필드에 이 마지막 수식을 입력합니다.

6. 약식 표현 필드에 설명을 입력할 때 확인을 클릭합니다. 설명이 잘못 구성되면 경고가 나타납니다. 설명이 올바르게 구성되면 정규 형식의 수식이 정규 수식 필드에 나타납니다.
7. 이 수식을 충족하는 노드를 보려면 노드 보기를 클릭합니다. 현재 수식에 의해 그룹화되는 노드를 표시하는 노드 그룹의 노드 창이 나타납니다. 이 창은 설명이 올바르게 입력되었는지 확인하는 데 사용할 수 있습니다. 설명이 올바르게 입력되지 않은 경우 규칙 표 또는 약식 표현 필드로 돌아가서 설명을 조정할 수 있습니다.

- 언제든지 이 그룹에 있는 노드에 대한 액세스를 허용하는 규정을 생성하려면 이 그룹의 전체 액세스 규정 생성을 선택합니다.
- 이 그룹에 속하는 노드의 설명을 완료하면 추가를 클릭하여 노드 그룹을 생성합니다. 그룹은 왼쪽에 있는 노드 그룹 목록에 추가됩니다.

노드 그룹 편집

노드 그룹을 편집하여 그룹의 구성원 또는 설명을 변경합니다.

▶ **노드 그룹 편집:**

- 연관체 > 노드 그룹을 선택합니다. 노드 그룹 관리자 창이 열립니다.
- 노드 그룹 목록에서 편집할 노드를 클릭합니다. 노드 그룹 창에 해당 노드의 상세 내용이 나타납니다.
- 노드 그룹을 구성하는 방법에 대한 자세한 내용은 노드 선택 또는 노드 설명 섹션의 지침을 참조하십시오.
- 확인을 클릭하여 변경 사항을 저장합니다.

노드 그룹 삭제

▶ **노드 그룹을 삭제하려면:**

- 연관체 > 노드 그룹을 선택합니다. 노드 그룹 관리자 창이 열립니다.
- 왼쪽에 있는 노드 그룹 목록에서 삭제할 노드를 선택합니다.
- 그룹 > 삭제를 선택합니다.

사용자 계정을 생성하여 사용자에게 CC-SG에 액세스하기 위한 사용자 이름 및 암호를 지정할 수 있습니다.

사용자 그룹은 구성원의 권한 세트를 정의합니다. 사용자 자신에게 권한을 지정할 수 없으며 사용자 그룹에만 지정할 수 있습니다. 모든 사용자는 최소한 하나의 사용자 그룹에 속해야 합니다.

CC-SG는 인증 및 허가를 위해 중앙 집중화된 사용자 목록과 사용자 그룹 목록을 관리합니다.

외부 인증을 사용하도록 CC-SG를 구성할 수도 있습니다. **원격 인증** (p. 128)을 참조하십시오.

사용자 그룹에 지정할 수 있는 액세스 규정도 생성해야 합니다. **액세스 제어 규정** (p. 115)을 참조하십시오.

이 장에서

사용자 탭.....	103
기본 사용자 그룹.....	104
사용자 그룹 추가, 편집 및 삭제.....	105
사용자 그룹에 대한 액세스 감사 구성.....	107
사용자 추가, 편집 및 삭제.....	108
그룹에 사용자 지정.....	110
그룹에서 사용자 삭제.....	111
사용자 프로필.....	111
사용자 로그아웃.....	113
사용자 대량 복사.....	114

사용자 탭

사용자 탭을 클릭하여 CC-SG 에 모든 사용자 그룹 및 사용자를 표시합니다.



사용자는 속한 사용자 그룹 아래에 중첩됩니다. 지정된 사용자가 있는 사용자 그룹은 옆에 + 기호가 있는 목록에 나타납니다. 목록을 확대하거나 축소하려면 + 또는 -를 클릭합니다. CC-SG 에 현재 로그인된 활성 사용자는 굵은 글씨체로 표시됩니다.

사용자 탭은 트리 내에서 사용자를 검색하는 기능을 제공합니다.

기본 사용자 그룹

CC-SG 는 다음과 같은 3 개의 기본 사용자 그룹으로 구성됩니다.
CC-수퍼 사용자, 시스템 관리자 및 CC 사용자

CC 수퍼 사용자 그룹

CC 수퍼 사용자 그룹은 전체 관리 및 액세스 권한을 갖습니다. 사용자 한 명만 이 그룹의 구성원이 될 수 있습니다. 기본 사용자 이름은 admin 입니다. 기본 사용자 이름은 변경할 수 있습니다. CC-수퍼 사용자 그룹은 삭제할 수 없습니다. CC-수퍼 사용자 그룹에 지정된 권한을 변경하거나 그룹에 구성원을 추가하거나 그룹에서 사용자만 삭제할 수 없습니다. 강력한 암호는 항상 CC-수퍼 사용자 그룹의 구성원에게 적용됩니다. 강력한 암호 요구사항:

- 암호에는 한 개 이상의 소문자가 포함되어야 합니다.
- 암호에는 한 개 이상의 대문자가 포함되어야 합니다.
- 암호에 한 개 이상의 숫자가 포함되어야 합니다.
- 암호는 한 개 이상의 특수 문자(예: 느낌표 또는 앰퍼샌드)를 포함해야 합니다.

시스템 관리자 그룹

시스템 관리자 그룹은 전체 관리 및 액세스 권한을 갖습니다. CC-수퍼 사용자 그룹과 달리 권한을 변경하고 구성원을 추가하거나 삭제할 수 있습니다.

CC 사용자 그룹

CC 사용자 그룹은 대역내 및 대역외 노드 액세스 권한을 갖습니다. 권한을 변경하고 구성원을 추가하거나 삭제할 수 있습니다.

중요: 먼저 적절한 사용자 그룹 또는 사용자를 선택하지 않으면 많은 메뉴 항목을 선택할 수 없습니다.

사용자 그룹 추가, 편집 및 삭제

사용자 그룹 추가

먼저 사용자 그룹을 생성하면 사용자를 추가할 때 사용자를 구성하는데 도움이 됩니다. 사용자 그룹이 생성되면 권한이 해당 사용자 그룹에 지정됩니다. 그룹에 할당된 사용자는 그러한 권한을 상속합니다. 예를 들어 그룹을 생성하고 해당 그룹에 사용자 관리 권한을 지정하면 해당 그룹에 지정된 모든 사용자는 사용자 관리자 메뉴에서 명령을 보고 실행할 수 있습니다. **사용자 그룹 권한** (p. 271)을 참조하십시오.

사용자 그룹을 구성하려면 다음과 같은 기본 단계를 수행해야 합니다.

- 그룹의 이름을 지정하고 그룹에 대한 설명을 제공합니다.
- 사용자 그룹이 부여받을 권한을 선택합니다.
- 사용자 그룹이 노드에 액세스하는 데 사용할 수 있는 인터페이스 유형을 선택합니다.
- 사용자 그룹이 액세스할 수 있는 노드를 지정하는 규정을 선택합니다.

▶ 사용자 그룹을 추가하려면:

1. 사용자 > 사용자 그룹 관리자 > 사용자 그룹 추가를 선택합니다. 사용자 그룹 추가 화면이 나타납니다.
2. 사용자 그룹 이름 필드에 사용자 그룹의 이름을 입력합니다. 사용자 그룹 이름은 고유해야 합니다. 이름 길이에 대한 **CC-SG** 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.
3. 설명 필드에 이 그룹에 대한 간단한 설명을 입력합니다. **옵션입니다.**
4. 권한 탭을 클릭합니다.
5. 사용자 그룹에 지정할 각 권한에 해당하는 확인란을 선택합니다.
6. 아래 권한 표는 다음 세 종류의 노드 액세스에 대한 권한이 있는 노드 액세스 영역입니다. 노드 대역외 액세스, 노드 대역내 액세스 및 노드 전원 제어 사용자 그룹에 지정할 각 노드 액세스 유형에 해당하는 확인란을 선택합니다.
7. 장치/노드 규정 탭을 클릭합니다. 규정 표가 나타납니다.

모든 규정 표는 **CC-SG**에서 사용할 수 있는 모든 규정을 나열합니다. 각 규정은 노드 그룹에 대한 액세스를 허용 또는 거부하는 규칙을 나타냅니다. 규정 및 규정 생성 방법에 대한 자세한 내용은 **액세스 제어 규정** (p. 115)을 참조하십시오.

- 모든 규정 목록에서 사용자 그룹에 지정할 규정을 선택한 다음 추가를 클릭하여 선택된 규정 목록으로 해당 규정을 이동합니다. 선택된 규정 목록의 규정은 이 규정으로 제어되는 노드 또는 장치에 대한 액세스를 허용하거나 거부합니다.

이 단계를 반복하여 사용자 그룹에 규정을 추가합니다.

- 이 그룹이 사용 가능한 모든 노드에 액세스할 수 있도록 하려면 규정 추가 목록에서 전체 액세스 규정을 선택한 다음 추가를 클릭합니다.
 - 사용자 그룹에서 규정을 제거하려면 선택된 규정 목록에서 규정 이름을 선택한 다음 제거를 클릭합니다.
- 그룹에 대한 규정을 구성했으면 적용을 클릭하여 이 그룹을 저장하고 다른 그룹을 생성합니다. 사용자 그룹을 추가하려면 이 섹션의 단계를 반복합니다. **옵션입니다.**
 - 확인을 클릭하여 변경 사항을 저장합니다.

사용자 그룹 편집

사용자 그룹을 편집하여 해당 그룹의 기존 권한 및 규정을 변경할 수 있습니다.

참고: CC-수퍼 사용자 그룹의 권한 또는 규정을 편집할 수 없습니다.

▶ **사용자 그룹을 편집하려면:**

- 사용자 탭을 클릭합니다.
- 사용자 탭에서 사용자 그룹을 클릭합니다. 사용자 그룹 프로필이 나타납니다.
- 사용자 그룹 이름 필드에 사용자 그룹의 새 이름을 입력합니다. **옵션입니다.**
- 설명 필드에 사용자 그룹에 대한 새 설명을 입력합니다. **옵션입니다.**
- 권한 탭을 클릭합니다.
- 사용자 그룹에 지정할 각 권한에 해당하는 확인란을 선택합니다. 권한을 선택 취소하여 그룹에서 제거합니다.
- 노드 액세스 영역에서 이 그룹이 액세스할 각 인터페이스의 드롭다운 메뉴를 클릭하고 제어를 선택합니다.
- 이 그룹이 액세스하지 않을 각 인터페이스의 드롭다운 메뉴를 클릭하고 거부를 선택합니다.
- 규정 탭을 클릭합니다. 두 개의 규정 표가 나타납니다.

10. 그룹에 추가할 각 규정의 경우 모든 규정에서 규정을 선택한 다음 추가를 클릭하여 선택된 규정 목록으로 규정을 이동합니다.
선택된 규정 목록의 규정은 이 규정으로 제어되는 노드 또는 장치에 대한 사용자 액세스를 허용하거나 거부합니다.
11. 사용자 그룹에서 제거하려는 각 규정에 대해 선택된 규정 목록에서 규정 이름을 선택한 다음 제거를 클릭합니다.
12. 확인을 클릭하여 변경 사항을 저장합니다.

사용자 그룹 삭제

구성원이 없는 사용자 그룹은 삭제할 수 있습니다.

▶ 사용자 그룹 삭제:

1. 사용자 탭을 클릭합니다.
2. 삭제할 사용자 그룹을 클릭합니다.
3. 사용자 > 사용자 그룹 관리자 > 사용자 그룹 제거를 선택합니다.
4. 확인을 클릭하여 사용자 그룹을 삭제합니다.

사용자 그룹에 대한 액세스 감사 구성

액세스 허용 전에 사용자 그룹의 구성원이 노드에 액세스하는 이유를 입력하도록 요구할 수 있습니다. 선택한 사용자 그룹의 모든 사용자에게 대화 상자가 표시됩니다. 사용자는 노드 연결이 이루어지기 전에 액세스에 대한 이유를 입력해야 합니다. 이 기능은 전원 제어를 포함하여 모든 인터페이스 유형을 가진 모든 액세스 유형에 적용됩니다.

액세스 이유는 감사 추적 및 노드 프로필의 감사 탭에 기록됩니다.

▶ 사용자 그룹에 대한 액세스 감사를 구성하려면:

1. 사용자 > 노드 감사를 선택합니다.
2. 노드 연결 시 사용자에게 대해 액세스 정보 입력 요구 확인란을 선택합니다.
3. 사용자에게 대한 메시지 필드에서 사용자가 노드에 액세스하려고 할 때 표시되는 메시지를 입력합니다. 기본 메시지가 제공됩니다. 최대 256 자입니다.
4. 그룹에 대한 액세스 감사가 가능하도록 화살표 버튼을 클릭하여 사용자 그룹을 선택 목록으로 이동합니다. 여러 항목을 삭제하려면 **Ctrl+클릭**을 사용합니다.

팁: 찾기 필드에 사용자 그룹의 이름을 입력하면 목록에 강조 표시됩니다. 목록에서 비슷한 모든 이름을 강조 표시하려면 이름 일부 뒤에 * 를 입력합니다.

목록을 알파벳 순서로 정렬하려면 열 헤더를 클릭합니다.

5. 업데이트를 클릭합니다.

사용자 추가, 편집 및 삭제

사용자 추가

CC-SG 에 사용자를 추가할 경우 사용자 그룹에 지정된 액세스 권한을 사용자에게 부여하기 위해 사용자 그룹을 지정해야 합니다.

▶ **사용자 추가:**

1. 사용자 탭에서 사용자를 추가할 그룹을 선택합니다.
2. 사용자 > 사용자 관리자 > 사용자 추가를 선택합니다.
3. 사용자 이름 필드에서 추가할 사용자의 사용자 이름을 입력합니다. 이 이름을 사용하여 CC-SG에 로그인합니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.
4. 사용자가 CC-SG 에 로그인할 수 있도록 하려면 로그인 활성 확인란을 선택합니다.
5. TACACS+, RADIUS, LDAP 또는 AD 와 같은 외부 서버에서 사용자를 인증하려는 경우에만 원격 인증 확인 확인란을 선택합니다. 원격 인증을 사용하는 경우 암호가 필요하지 않으며 새 암호 및 새 암호 다시 입력 필드가 비활성화됩니다.
6. 새 암호 및 새 암호 재입력 필드에 사용자가 CC-SG 에 로그인하는 데 사용할 암호를 입력합니다.

참고: 암호 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙** (p. 294)을 참조하십시오.

강력한 암호가 활성화되면 입력한 암호가 설정된 규칙에 맞아야 합니다. 화면 맨 위의 알림 표시줄에 암호 요구사항을 지원하기 위한 메시지가 표시됩니다. 강력한 암호에 대한 자세한 내용은 **고급 관리** (p. 174)를 참조하십시오.

7. 사용자가 나중에 로그인할 때 강제로 지정된 암호를 변경하게 하려면 다음 로그인에서 암호 변경 실행 확인란을 선택합니다.

8. 사용자가 강제로 암호를 변경하는 빈도를 지정하려면 주기적 암호 변경 실행 확인란을 선택합니다.
9. 선택할 경우 만료 기간(일) 필드에 사용자가 강제로 암호를 변경하기 전에 같은 암호를 사용할 수 있는 기간(일)을 입력합니다.
10. 이메일 주소 필드에 사용자의 이메일 주소를 입력합니다. 이메일 주소는 사용자 통지를 보낼 때 사용됩니다.
11. 전화 번호 필드에 사용자의 전화 번호를 입력합니다.
12. 사용자 그룹 드롭다운 메뉴를 클릭하고 사용자가 추가될 그룹을 선택합니다.
13. 이 사용자의 구성을 완료하면 적용을 클릭하여 이 사용자를 추가하고 다른 사용자를 생성하거나 확인을 클릭하여 사용자를 생성하지 않고 추가합니다. 생성한 사용자는 속한 사용자 그룹 아래에 중첩되어 사용자 탭에 표시됩니다.

사용자 편집

속한 그룹을 변경하기 위해 사용자를 편집할 수 없습니다. **그룹에 사용자 지정** (p. 110)을 참조하십시오.

▶ 사용자 편집:

1. 사용자 탭에서 + 기호를 클릭하여 편집할 사용자를 포함하는 사용자 그룹을 확장한 다음 사용자를 선택합니다. 사용자 프로필이 나타납니다.
2. 이 사용자가 CC-SG에 로그인하지 못하도록 하려면 로그인 활성화 확인란을 선택 취소합니다. 이 사용자가 CC-SG에 로그인하도록 하려면 로그인 활성화 확인란을 선택합니다.
3. TACACS+, RADIUS, LDAP 또는 AD와 같은 외부 서버에서 사용자를 인증하려는 경우에만 원격 인증 확인란만 선택합니다. 원격 인증을 사용하는 경우 암호가 필요하지 않으며 새 암호 및 새 암호 다시 입력 필드가 비활성화됩니다.
4. 새 암호 및 새 암호 다시 입력 필드에 새 암호를 입력하여 이 사용자의 암호를 변경합니다.

*참고: 강력한 암호가 활성화되면 입력한 암호가 설정된 규칙에 맞아야 합니다. 화면 맨 위의 알림 표시줄은 암호 요구사항을 지원합니다. 강력한 암호에 대한 자세한 내용은 **고급 관리** (p. 174)를 참조하십시오.*

5. 사용자가 나중에 로그인할 때 강제로 지정된 암호를 변경하게 하려면 다음 로그인에서 암호 변경 실행 확인란을 선택합니다.

6. 이메일 주소 필드에 새 이메일 주소를 입력하여 사용자의 구성된 이메일 주소를 추가하거나 변경합니다. 이메일 주소는 사용자 통지를 보낼 때 사용됩니다.
7. 확인을 클릭하여 변경 사항을 저장합니다.

사용자 삭제

사용자를 완전히 삭제하면 **CC-SG** 에서 사용자가 제거됩니다. 이 명령은 더 이상 필요 없는 계정을 제거하는 데 유용합니다.

이 절차는 사용자가 여러 사용자 그룹에 존재하더라도 사용자의 모든 인스턴스를 삭제합니다. **CC-SG**에서 사용자를 삭제하지 않고 그룹에서 사용자를 제거하려면 **그룹에서 사용자 제거** (참조 "그룹에서 사용자 삭제" p. 111)를 참조하십시오.

▶ 사용자 삭제:

1. 사용자 탭에서 + 기호를 클릭하여 삭제할 사용자를 포함하는 사용자 그룹을 확장한 다음 사용자를 선택합니다. 사용자 프로필이 나타납니다.
2. 사용자 > 사용자 관리자, 사용자 삭제를 선택합니다.
3. 확인을 클릭하여 **CC-SG** 에서 사용자를 영구적으로 삭제합니다.

그룹에 사용자 지정

이 명령을 사용하여 기존 사용자를 다른 그룹에 지정합니다. 이 방법으로 지정된 사용자는 이전에 지정된 그룹에 존재하면서 새 그룹에 추가됩니다. 사용자를 이동하려면 그룹에서 사용자 삭제와 함께 이 명령을 사용합니다.

▶ 그룹에 사용자 지정:

1. 사용자 탭에서 사용자를 지정할 사용자 그룹을 선택합니다.
2. 사용자 > 사용자 그룹 관리자 > 그룹에 사용자 지정을 선택합니다.
3. 선택한 사용자 그룹은 사용자 그룹 이름 필드에 표시됩니다.
4. 대상 그룹에 지정되지 않은 사용자는 그룹에 없는 사용자 목록에 나타납니다.
 - 이 목록에서 추가할 사용자를 선택한 다음 >을 클릭하여 선택한 사용자를 그룹에 있는 사용자 목록으로 이동합니다.
 - >> 버튼을 클릭하여 그룹에 없는 모든 사용자를 그룹에 있는 사용자 목록으로 이동합니다.

- 그룹에 있는 사용자 목록에서 제거할 사용자를 선택한 다음 < 버튼을 클릭하여 제거합니다.
 - << 버튼을 클릭하여 그룹에 있는 사용자 목록에서 모든 사용자를 제거합니다.
5. 모든 사용자가 적절한 열로 이동되었으면 확인을 클릭합니다. 그룹에 있는 사용자 목록의 사용자는 선택한 사용자 그룹에 추가됩니다.

그룹에서 사용자 삭제

그룹에서 사용자를 삭제할 경우 사용자는 지정된 그룹에서만 제거됩니다. 사용자는 기타 모든 지정된 그룹에는 남아 있습니다. 그룹에서 사용자를 삭제해도 CC-SG 에서 사용자를 삭제하지 않습니다.

사용자가 하나의 그룹에만 속해 있는 경우 해당 그룹에서 사용자를 삭제할 수 없습니다. CC-SG 에서만 해당 사용자를 삭제할 수 있습니다.

▶ 그룹에서 사용자 삭제:

1. 사용자 탭에서 + 기호를 클릭하여 그룹에서 삭제할 사용자를 포함하는 사용자 그룹을 확장한 다음 사용자를 선택합니다. 사용자 프로필이 나타납니다.
2. 사용자 > 사용자 관리자 > 그룹에서 사용자 삭제를 선택합니다. 사용자 삭제 화면이 나타납니다.
3. 확인을 클릭하여 그룹에서 사용자를 삭제합니다.

사용자 프로필

모든 사용자는 내 프로필을 사용하여 계정에 대한 내역을 볼 수 있으며 일부 상세 내용을 변경하고 가용성 설정을 사용자 정의할 수 있습니다. 계정 이름을 변경하기 위한 유일한 방법은 CC 수퍼 사용자 계정을 사용하는 것입니다.

▶ 프로필을 편집하려면:

Secure Gateway > 내 프로필을 선택합니다. 계정에 대한 상세 내용을 표시하는 내 프로필 변경 화면이 나타납니다.

암호 변경

1. Secure Gateway > 내 프로필을 선택합니다.

2. 암호 변경(로컬 인증 전용) 확인란을 선택합니다.
3. 이전 암호 필드에 현재 암호를 입력합니다.
4. 새 암호 필드에 새로운 암호를 입력합니다. 강력한 암호가 필요한 경우 메시지가 나타납니다.
5. 새 암호 다시 입력 필드에 새 암호를 다시 입력합니다.
6. 확인을 클릭하여 변경 사항을 저장합니다.

기본 검색 기본 설정 변경

1. Secure Gateway > 내 프로필을 선택합니다.
2. 검색 기본 설정 영역에서 원하는 방법을 선택하여 노드, 사용자 및 장치를 검색합니다.
 - 검색 결과로 필터링 - 와일드카드의 사용을 허용하며 노드, 사용자 또는 장치의 표시를 검색 기준이 포함된 모든 이름으로 제한합니다.
 - 일치하는 문자열 찾기 - 와일드카드의 사용을 지원하지 않으며 입력한 노드, 사용자 또는 장치와 가장 일치하는 항목을 강조 표시합니다. 목록은 검색을 클릭한 후 검색 기준이 포함된 해당 항목으로 제한됩니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.

CC-SG 기본 글꼴 크기 변경

1. Secure Gateway > 내 프로필을 선택합니다.
2. 글꼴 크기 드롭다운 메뉴를 클릭하여 표준 CC-SG 클라이언트에서 사용하는 글꼴 크기를 조정합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.

이메일 주소 변경

1. Secure Gateway > 내 프로필을 선택합니다.
2. 이메일 주소 필드에 새 주소를 입력하여 CC-SG 에서 통지를 보내는 데 사용할 주소를 추가하거나 변경합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.

CC-SG 슈퍼 사용자의 사용자 이름 변경

CC 슈퍼 사용자의 사용자 이름을 변경하려면 CC-SG 슈퍼 사용자 계정을 사용하여 CC-SG 에 로그인해야 합니다. 기본 CC 슈퍼 사용자 이름은 *admin* 입니다.

1. Secure Gateway > 내 프로필을 선택합니다.
2. 사용자 이름 필드에 새 이름을 입력합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.

사용자 로그아웃

개별적으로 또는 사용자 그룹별로 CC-SG 로부터 활성 사용자를 기록할 수 있습니다.

▶ 사용자 로그아웃:

1. 사용자 탭에서 + 기호를 클릭하여 CC-SG 에서 로그아웃할 사용자를 포함하는 사용자 그룹을 확장한 다음 사용자를 선택합니다.
 - 여러 사용자를 선택하려면 Shift 키를 누른 상태에서 추가 사용자를 클릭합니다.
2. 사용자 > 사용자 관리자 > 사용자 로그아웃을 선택합니다. 선택한 사용자의 목록과 함께 사용자 로그아웃 화면이 나타납니다.
3. CC-SG 에서 사용자를 로그아웃하려면 확인을 클릭합니다.

▶ 사용자 그룹의 모든 사용자 로그아웃:

1. 사용자 탭에서 CC-SG 에서 로그아웃할 사용자 그룹을 선택합니다.
 - 여러 사용자 그룹을 로그아웃하려면 Shift 키를 누른 상태에서 추가 사용자 그룹을 클릭합니다.
2. 사용자 > 사용자 그룹 관리자 > 사용자 로그아웃을 선택합니다. 선택한 그룹의 활성 사용자 목록과 함께 사용자 로그아웃 화면이 나타납니다.
3. CC-SG 에서 사용자를 로그아웃하려면 확인을 클릭합니다.

사용자 대량 복사

한 사용자의 사용자 그룹 관계를 다른 사용자 또는 사용자 목록으로 복사하려면 사용자 대량 복사를 사용할 수 있습니다. 관계가 할당되는 사용자가 기존 그룹 관계를 가지고 있는 경우 기존 관계가 제거됩니다.

▶ **사용자 대량 복사를 수행하려면:**

1. 사용자 탭에서 복사할 규정 및 권한을 가진 사용자를 포함하는 사용자 그룹을 확장하려면 + 기호를 클릭한 다음 사용자를 선택합니다.
2. 사용자 > 사용자 관리자 > 대량 복사를 선택합니다. 사용자 이름 필드는 복사하는 규정 및 권한을 가진 사용자를 표시합니다.
3. 모든 사용자 목록에서 사용자 이름 필드에 나열된 사용자의 규정 및 권한을 받는 사용자를 선택합니다.
 - >을 클릭하여 사용자 이름을 선택한 사용자 목록으로 이동합니다.
 - >>을 클릭하여 모든 사용자를 선택된 사용자 목록으로 이동합니다.
 - 선택된 사용자 목록의 사용자를 선택한 다음 <을 클릭하여 사용자를 제거합니다.
 - <<을 클릭하여 그룹에 있는 사용자 목록에서 모든 사용자를 제거합니다.
4. 확인을 클릭하여 복사합니다.

규정은 해당하는 경우 사용자가 액세스할 수 있는 노드 및 장치, 액세스할 수 있을 때 그리고 가상 매체 권한이 활성화되어 있는지 여부 등을 정의하는 규칙입니다. 규정을 생성하는 가장 쉬운 방법은 노드 및 장치를 노드 그룹 및 장치 그룹으로 분류한 다음 각 그룹에서 노드 및 장치에 액세스를 허용 및 거부하는 규정을 생성하는 것입니다. 규정을 생성한 후 이를 사용자 그룹에 지정합니다. **사용자 그룹에 규정 지정** (p. 119)을 참조하십시오.

CC-SG 는 전체 액세스 규정을 포함합니다. 항상 모든 노드 및 장치에 대한 모든 사용자 액세스를 제공하려면 모든 사용자 그룹에 전체 액세스 규정을 지정합니다.

설정 안내서를 완료한 경우 많은 기본 규정이 이미 생성되었을 수 있습니다. **설정 안내서를 사용하여 CC-SG 구성** (p. 14)을 참조하십시오.

▶ **규정을 사용하여 액세스를 제어하려면:**

- 노드 그룹을 생성하여 액세스 규칙을 생성할 노드 구성 **노드 그룹 추가** (p. 97)를 참조하십시오.
- 장치 그룹을 생성하여 액세스 규칙을 생성할 장치를 구성합니다. **장치 그룹 추가** (p. 51)를 참조하십시오.
- 해당 노드 또는 장치 그룹에 액세스할 때를 지정하는 노드 또는 장치에 대한 규정을 생성합니다. **규정 추가** (p. 116)를 참조하십시오.
- 사용자 그룹에 규정을 적용합니다. **사용자 그룹에 규정 지정** (p. 119)을 참조하십시오.

이 장에서

규정 추가.....	116
규정 편집.....	117
규정 삭제.....	118
가상 매체 지원	119
사용자 그룹에 규정 지정	119

규정 추가

노드 그룹 또는 장치 그룹에 대한 액세스(거부)를 거부하는 규정을 생성하는 경우 선택한 노드 그룹 또는 장치 그룹에 대한 액세스(제어)를 허용하는 규정도 생성해야 합니다. 거부 규정이 적용되지 않으면 사용자에게 제어 권한이 자동으로 부여되지 않습니다.

참고: CC-SG가 프록시 모드 또는 두 가지 모드 모두에 있을 경우 가상 매체에 대한 사용자 액세스 권한을 부여할 수 없습니다. **연결 모드: 직접 및 프록시 (p. 187)**를 참조하십시오.

▶ **규정을 추가하려면:**

1. 연관체 > 규정을 선택합니다. 규정 관리자 창이 열립니다.
2. 추가를 클릭합니다. 규정 이름을 요청하는 대화 창이 나타납니다.
3. 규정 이름 입력 필드에 새 규정 이름을 입력합니다. 이름 길이에 대한 CC-SG 규정의 자세한 내용은 **명명 규칙 (p. 294)**을 참조하십시오.
4. 확인을 클릭합니다. 규정 관리자 화면의 규정 이름 목록에 새 규정이 추가됩니다.
5. 장치 그룹 드롭다운 화살표를 클릭하고 이 규정을 통해 액세스가 제어되는 장치 그룹을 선택합니다.
6. 노드 그룹 드롭다운 화살표를 클릭하고 이 규정을 통해 액세스가 제어되는 노드 그룹을 선택합니다.
7. 규정이 한 개의 그룹 유형에만 적용될 경우 해당 유형의 값만 선택합니다.
8. 요일 드롭다운 화살표를 클릭하고 다음과 같이 이 규정이 적용되는 요일을 선택합니다. 매일, 주중(월요일부터 금요일만) 및 주말(토요일 및 일요일만) 또는 사용자 정의(특정 요일 선택)
9. 사용자 정의를 선택하여 사용자 자신의 요일 세트를 선택합니다. 개별 요일 확인란이 활성화됩니다.
10. 이 규정을 적용할 각 요일에 해당하는 확인란을 선택합니다.
11. 시작 시간 필드에 이 규정이 적용되는 시간을 입력합니다. 시간은 24 시간 형식이어야 합니다.
12. 종료 시간 필드에 이 규정의 적용이 끝나는 시간을 입력합니다. 시간은 24 시간 형식이어야 합니다.

13. 장치/노드 액세스 권한 필드에서 제어를 선택하여 지정된 시간과 요일에 선택한 노드 또는 장치 그룹에 대한 액세스를 허용하는 규정을 정의합니다. 거부를 선택하여 지정된 시간과 요일에 선택한 노드 또는 장치 그룹에 대한 액세스를 거부하는 이 규정을 정의합니다.
14. 장치/노드 액세스 권한 필드에서 제어를 선택한 경우 가상 매체 권한 섹션이 활성화됩니다. 가상 매체 권한 필드에서 지정된 시간 및 일 동안 선택된 노드 또는 장치 그룹에서 이용 가능한 가상 매체에 대한 액세스를 허용 또는 거부하는 옵션을 선택합니다.
 - 읽기-쓰기는 가상 매체에 대한 읽기 및 쓰기 권한을 허용합니다.
 - 읽기 전용은 가상 매체에 대한 읽기 권한만 허용합니다.
 - 거부는 가상 매체에 대한 모든 액세스를 거부합니다.
15. 업데이트를 클릭하여 **CC-SG**에 새 규정을 추가하고 나타나는 확인 메시지에서 예를 클릭합니다.

규정 편집

규정을 편집할 경우 변경 사항은 **CC-SG**에 현재 로그인된 사용자에게 적용되지 않습니다. 변경 사항은 다음에 로그인할 때 적용됩니다.

변경 사항이 곧 적용되도록 하려면 먼저 정비 모드를 시작하고 규정을 편집합니다. 정비 모드에 들어가면 사용자가 다시 로그인하여 정비 모드를 종료할 때까지 현재 모든 사용자는 **CC-SG**에서 로그아웃됩니다. **정비 모드** (p. 162)를 참조하십시오.

▶ 규정 편집:

1. 연관체 메뉴에서 규정을 클릭합니다. 규정 관리자 창이 열립니다.
2. 규정 이름 드롭다운 화살표를 클릭하고 목록에서 편집할 규정을 선택합니다.
3. 규정 이름을 편집하려면 편집을 클릭합니다. 규정 편집 창이 열립니다. 해당 필드에 규정의 새 이름을 입력한 다음 확인을 클릭하여 규정 이름을 변경합니다. **옵션입니다.**
4. 장치 그룹 드롭다운 화살표를 클릭하고 이 규정이 액세스를 제어하는 장치 그룹을 선택합니다.
5. 노드 그룹 드롭다운 화살표를 클릭하고 이 규정이 액세스를 제어하는 노드 그룹을 선택합니다.
6. 규정이 한 개의 그룹 유형에만 적용될 경우 해당 유형의 값만 선택합니다.

7. 요일 드롭다운 화살표를 클릭하고 다음과 같이 이 규정이 적용되는 요일을 선택합니다. 모두(매일), 주중(월요일부터 금요일만) 및 주말(토요일 및 일요일만) 또는 사용자 정의(특정 요일 선택)
8. 사용자 정의를 선택하여 사용자 자신의 요일 세트를 선택합니다. 개별 요일 확인란이 활성화됩니다.
9. 이 규정을 적용할 각 요일에 해당하는 확인란을 선택합니다.
10. 시작 시간 필드에 이 규정이 적용되는 시간을 입력합니다. 시간은 24 시간 형식이어야 합니다.
11. 종료 시간 필드에 이 규정의 적용이 끝나는 시간을 입력합니다. 시간은 24 시간 형식이어야 합니다.
 - 장치/노드 액세스 권한 필드에서:
 - 제어를 선택하여 지정된 시간과 요일에 선택한 노드 또는 장치 그룹에 대한 액세스를 허용하는 이 규정을 정의합니다.
 - 거부를 선택하여 지정된 시간과 요일에 선택한 노드 또는 장치 그룹에 대한 액세스를 거부하는 이 규정을 정의합니다.
12. 장치/노드 액세스 권한 필드에서 제어를 선택한 경우 가상 매체 권한 섹션이 활성화됩니다. 가상 매체 권한 필드에서 지정된 시간 및 일 동안 선택된 노드 또는 장치 그룹에서 이용 가능한 가상 매체에 대한 액세스를 허용 또는 거부하는 옵션을 선택합니다.
 - 읽기-쓰기는 가상 매체에 대한 읽기 및 쓰기 권한을 허용합니다.
 - 읽기 전용은 가상 매체에 대한 읽기 권한만 허용합니다.
 - 거부는 가상 매체에 대한 모든 액세스를 거부합니다.
13. 업데이트를 클릭하여 변경 사항을 저장합니다.
14. 확인 메시지에서 예를 클릭합니다.

규정 삭제

더 이상 필요하지 않은 규정은 삭제할 수 있습니다.

▶ **규정 삭제:**

1. 연관체 > 규정을 선택합니다. 규정 관리자 창이 열립니다.
2. 규정 이름 드롭다운 화살표를 클릭하고 목록에서 삭제할 규정을 선택합니다.
3. 삭제를 클릭합니다.

4. 확인 메시지에서 예를 클릭합니다.

가상 매체 지원

CC-SG 는 가상 매체를 지원하는 KX2, KSX2 및 KX2-101 장치에 연결된 노드에 대해 원격 가상 매체 지원을 제공합니다. 장치를 이용해 가상 매체에 액세스하는 자세한 지침은 다음을 참조하십시오.

- **Dominion KX II** 사용자 설명서
- **Dominion KSX II** 사용자 설명서
- **Dominion KXII-101** 사용자 설명서

CC-SG에서 사용자 그룹에 가상 매체 권한을 지정하는 규정의 생성 방법에 대한 자세한 내용은 **규정 추가** (p. 116)를 참조하십시오.

사용자 그룹에 규정 지정

규정은 적용되기 전에 사용자 그룹에 지정되어야 합니다. 규정이 사용자 그룹에 지정되면 그룹의 구성원은 해당 규정으로 제어되는 액세스 권한을 갖게 됩니다. 사용자 그룹에 규정을 지정하는 방법에 대한 자세한 내용은 **사용자 및 사용자 그룹** (p. 102)을 참조하십시오.

사용자 정의 보기를 사용하여 왼쪽 패널에 노드를 표시하는 다른 방법(범주, 노드 및 장치 그룹을 이용하여)을 지정할 수 있습니다.

이 장에서

사용자 정의 보기 유형.....	120
Admin 클라이언트에서 사용자 정의 보기 사용.....	121

사용자 정의 보기 유형

사용자 정의 보기에는 범주별 보기, 노드 그룹별 필터 및 장치 그룹별 필터의 세 가지 유형이 있습니다.

범주별 보기

범주별 보기 사용자 정의 보기가 적용될 때 지정된 범주에 의해 기술된 모든 노드 및 장치가 노드나 장치 목록에 표시됩니다. 할당된 범주가 없는 노드나 장치는 "연관되지 않음"으로도 표시됩니다.

노드 그룹별 필터

노드 그룹별 필터링 사용자 정의 보기가 적용될 때 지정된 노드 그룹만 노드 목록에 표시됩니다. 첫 번째 조직 수준은 노드 그룹 이름입니다. 노드가 사용자 정의 보기에 정의된 하나 이상의 노드 그룹에 속할 경우 노드는 목록에 여러 번 나타날 수 있습니다. 사용자 정의 보기에 의해 지정된 노드 그룹에 속하지 않은 노드는 목록에 표시되지 않습니다.

장치 그룹별 필터

장치 그룹별 필터링 사용자 정의 보기가 적용될 때 지정된 장치 그룹만 장치 목록에 표시됩니다. 첫 번째 조직 수준은 장치 그룹 이름입니다. 장치가 사용자 정의 보기에 정의된 둘 이상의 장치 그룹에 속할 경우 장치는 목록에 여러 번 나타날 수 있습니다. 사용자 정의 보기에 의해 지정된 장치 그룹에 속하지 않은 장치는 목록에 표시되지 않습니다.

Admin 클라이언트에서 사용자 정의 보기 사용

노드 사용자 정의 보기

노드의 사용자 정의 보기 추가

▶ 노드의 사용자 정의 보기를 추가하려면:

1. 노드 탭을 클릭합니다.
2. 노드 > 보기 변경 > 사용자 정의 보기 생성을 선택합니다. 사용자 정의 보기 화면이 나타납니다.
3. 사용자 정의 보기 패널에서 추가를 클릭합니다. 사용자 정의 보기 추가 창이 열립니다.
4. 사용자 정의 이름 보기 필드에서 새 사용자 정의 보기의 이름을 입력합니다.
5. 사용자 정의 보기 유형 섹션에서:
 - 지정한 노드 그룹만 표시하는 사용자 정의 보기를 생성하려면 노드 그룹별 필터링을 선택하십시오.
 - 지정한 범주에 따라 노드를 표시하는 사용자 정의 보기를 생성하려면 범주별 보기를 선택하십시오.
6. 확인을 클릭합니다.
7. 사용자 정의 내역 보기 섹션에서:
 - a. 사용 가능 목록에서 사용자 정의 보기에 추가할 항목을 선택한 다음 추가를 클릭하여 목록에 항목을 추가합니다. 이 단계를 반복하여 원하는 수의 항목을 추가합니다.
 - b. 각 그룹을 노드 탭에 표시하려는 순서로 선택 목록에 항목을 배치합니다. 항목을 선택한 다음 위로 및 아래로 화살표를 클릭하여 항목을 원하는 순서로 이동합니다.
 - c. 목록에서 항목을 제거해야 하는 경우 항목을 선택하고 제거를 클릭합니다.
8. 저장을 클릭합니다. 사용자 정의 보기가 추가되었음을 확인하는 메시지가 표시됩니다.
9. 새 사용자 정의 보기를 적용하려면 현재 설정을 클릭합니다.

노드의 사용자 정의 보기 적용

▶ **노드 목록에 사용자 정의 보기를 적용하려면:**

1. 노드 > 보기 변경 > 사용자 정의 보기를 선택합니다. 사용자 정의 보기 화면이 나타납니다.
2. 이름 드롭다운 화살표를 클릭하고 목록에서 사용자 정의 보기를 선택합니다.
3. 보기 적용을 클릭합니다.

또는

- 노드 > 보기 변경을 선택합니다. 모든 정의된 사용자 정의 보기는 팝업 메뉴에서 옵션입니다. 적용할 사용자 정의 보기를 선택합니다.

노드의 사용자 정의 보기 변경

1. 노드 탭을 클릭합니다.
2. 노드 > 보기 변경 > 사용자 정의 보기 생성을 선택합니다. 사용자 정의 보기 화면이 나타납니다.
3. 이름 드롭다운 화살표를 클릭하고 목록에서 사용자 정의 보기를 선택합니다. 포함된 항목의 내역과 순서가 사용자 정의 내역 보기 패널에 나타납니다.

▶ **사용자 정의 보기 이름을 변경하려면:**

1. 사용자 정의 보기 패널에서 편집을 클릭합니다. 사용자 정의 보기 편집 창이 열립니다.
2. 사용자 정의 보기의 새 이름 입력 필드에 사용자 정의 보기의 새 이름을 입력한 다음 확인을 클릭합니다. 사용자 정의 보기 화면의 이름 필드에 새 보기 이름이 나타납니다.

▶ **사용자 정의 보기의 내용을 변경하려면:**

1. 사용자 정의 내역 보기 섹션에서:
 - a. 사용 가능 목록에서 사용자 정의 보기에 추가할 항목을 선택한 다음 추가를 클릭하여 목록에 항목을 추가합니다. 이 단계를 반복하여 원하는 수의 항목을 추가합니다.
 - b. 각 그룹을 노드 탭에 표시하려는 순서로 선택 목록에 항목을 배치합니다. 항목을 선택한 다음 위로 및 아래로 화살표를 클릭하여 항목을 원하는 순서로 이동합니다.

- c. 목록에서 항목을 제거해야 하는 경우 항목을 선택하고 제거를 클릭합니다.
- 2. 저장을 클릭합니다. 사용자 정의 보기가 추가되었음을 확인하는 메시지가 표시됩니다.
- 3. 새 사용자 정의 보기를 적용하려면 현재 설정을 클릭합니다.

노드의 사용자 정의 보기 삭제

▶ **노드의 사용자 정의 보기를 삭제하려면:**

1. 노드 탭을 클릭합니다.
2. 노드 > 보기 변경 > 사용자 정의 보기 생성을 선택합니다. 사용자 정의 보기 화면이 나타납니다.
3. 이름 드롭다운 화살표를 클릭하고 목록에서 사용자 정의 보기를 선택합니다. 포함된 항목의 내역과 순서가 사용자 정의 내역 보기 패널에 나타납니다.
4. 사용자 정의 보기 패널에서 삭제를 클릭합니다. 사용자 정의 보기 삭제 확인 메시지가 나타납니다.
5. 예를 클릭합니다.

노드의 기본 사용자 정의 보기 할당

▶ **노드의 기본 사용자 정의 보기를 지정하려면:**

1. 노드 탭을 클릭합니다.
2. 노드 > 보기 변경 > 사용자 정의 보기 생성을 선택합니다. 사용자 정의 보기 화면이 나타납니다.
3. 이름 드롭다운 화살표를 클릭하고 목록에서 사용자 정의 보기를 선택합니다.
4. 사용자 정의 보기 패널에서 기본으로 설정을 클릭합니다. 다음 번 로그인할 때 선택된 사용자 정의 보기가 기본으로 사용됩니다.

모든 사용자에게 대해 노드의 기본 사용자 정의 보기 할당

CC 설정 및 제어 권한이 있는 경우 모든 사용자에게 대해 기본 사용자 정의 보기를 할당할 수 있습니다.

▶ **모든 사용자에게 대해 노드의 기본 사용자 정의 보기를 지정하려면:**

1. 노드 탭을 클릭합니다.

2. 노드 > 보기 변경 > 사용자 정의 보기 생성을 선택합니다.
3. 이름 드롭다운 화살표를 클릭하고 시스템 전체 기본 보기로 지정하고자 하는 사용자 정의 보기를 선택합니다.
4. 시스템 전체 확인란을 선택한 다음 저장을 클릭합니다.

CC-SG에 로그인하는 모든 사용자는 선택한 사용자 정의 보기에 따라 정렬된 노드 탭을 볼 수 있습니다. 사용자는 사용자 정의 보기를 변경할 수 있습니다.

장치 사용자 정의 보기

장치의 사용자 정의 보기 추가

▶ 장치의 사용자 정의 보기를 추가하려면:

1. 장치 탭을 클릭합니다.
2. 장치 > 보기 변경 > 사용자 정의 보기 생성을 선택합니다. 사용자 정의 보기 화면이 나타납니다.
3. 사용자 정의 보기 패널에서 추가를 클릭합니다. 사용자 정의 보기 추가 창이 나타납니다.
4. 사용자 정의 이름 보기 필드에서 새 사용자 정의 보기의 이름을 입력합니다.
5. 사용자 정의 보기 유형 섹션에서:
 - 지정한 장치 그룹만 표시하는 사용자 정의 보기를 생성하려면 장치 그룹별 필터링을 선택합니다.
 - 지정한 범주에 따라 장치를 표시하는 사용자 정의 보기를 생성하려면 범주별 보기를 선택합니다.
6. 확인을 클릭합니다.
7. 사용자 정의 내역 보기 섹션에서:
 - a. 사용 가능 목록에서 사용자 정의 보기에 추가할 항목을 선택한 다음 추가를 클릭하여 목록에 항목을 추가합니다. 이 단계를 반복하여 원하는 수의 항목을 추가합니다.
 - b. 각 그룹을 노드 탭에 표시하려는 순서로 선택 목록에 항목을 배치합니다. 항목을 선택한 다음 위로 및 아래로 화살표를 클릭하여 항목을 원하는 순서로 이동합니다.
 - c. 목록에서 항목을 제거해야 하는 경우 항목을 선택하고 제거를 클릭합니다.

8. 저장을 클릭합니다. 사용자 정의 보기가 추가되었음을 확인하는 메시지가 표시됩니다.
9. 새 사용자 정의 보기를 적용하려면 현재 설정을 클릭합니다.

장치의 사용자 정의 보기 적용

▶ 장치 목록에 사용자 정의 보기를 적용하려면:

1. 장치 > 보기 변경 > 사용자 정의 보기를 선택합니다. 사용자 정의 보기 화면이 나타납니다.
2. 이름 드롭다운 화살표를 클릭하고 목록에서 사용자 정의 보기를 선택합니다.
3. 현재 설정을 클릭하여 사용자 정의 보기를 적용합니다.

또는

장치 > 보기 변경을 선택합니다. 모든 정의된 사용자 정의 보기는 팝업 메뉴에서 옵션입니다. 적용할 사용자 정의 보기를 선택합니다.

장치의 사용자 정의 보기 변경

1. 장치 탭을 클릭합니다.
2. 장치 > 보기 변경 > 사용자 정의 보기 생성을 선택합니다. 사용자 정의 보기 화면이 나타납니다.
3. 이름 드롭다운 화살표를 클릭하고 목록에서 사용자 정의 보기를 선택합니다. 포함된 항목의 내역과 순서가 사용자 정의 내역 보기 패널에 나타납니다.

▶ 사용자 정의 보기 이름을 변경하려면:

1. 사용자 정의 보기 패널에서 편집을 클릭합니다. 사용자 정의 보기 편집 창이 열립니다.
2. 사용자 정의 보기의 새 이름 입력 필드에 사용자 정의 보기의 새 이름을 입력한 다음 확인을 클릭합니다. 사용자 정의 보기 화면의 이름 필드에 새 보기 이름이 나타납니다.

▶ 사용자 정의 보기의 내용을 변경하려면:

1. 사용자 정의 내역 보기 섹션에서:
 - a. 사용 가능 목록에서 사용자 정의 보기에 추가할 항목을 선택한 다음 추가를 클릭하여 목록에 항목을 추가합니다. 이 단계를 반복하여 원하는 수의 항목을 추가합니다.

11: 장치 및 노드의 사용자 정의 보기

- b. 각 그룹을 노드 탭에 표시하려는 순서로 선택 목록에 항목을 배치합니다. 항목을 선택한 다음 위로 및 아래로 화살표를 클릭하여 항목을 원하는 순서로 이동합니다.
 - c. 목록에서 항목을 제거해야 하는 경우 항목을 선택하고 제거를 클릭합니다.
2. 저장을 클릭합니다. 사용자 정의 보기가 추가되었음을 확인하는 메시지가 표시됩니다.
3. 새 사용자 정의 보기를 적용하려면 현재 설정을 클릭합니다.

장치의 사용자 정의 보기 삭제

▶ 장치의 사용자 정의 보기를 삭제하려면:

1. 장치 탭을 클릭합니다.
2. 장치 > 보기 변경 > 사용자 정의 보기 생성을 선택합니다. 사용자 정의 보기 화면이 나타납니다.
3. 이름 드롭다운 화살표를 클릭하고 목록에서 사용자 정의 보기를 선택합니다. 포함된 항목의 내역과 순서가 사용자 정의 내역 보기 패널에 나타납니다.
4. 사용자 정의 보기 패널에서 삭제를 클릭합니다. 사용자 정의 보기 삭제 확인 메시지가 나타납니다.
5. 예를 클릭합니다.

장치의 기본 사용자 정의 보기 지정

▶ 장치의 기본 사용자 정의 보기를 지정하려면:

1. 장치 탭을 클릭합니다.
2. 장치 > 보기 변경 > 사용자 정의 보기 생성을 선택합니다. 사용자 정의 보기 화면이 나타납니다.
3. 이름 드롭다운 화살표를 클릭하고 목록에서 사용자 정의 보기를 선택합니다.
4. 사용자 정의 보기 패널에서 기본으로 설정을 클릭합니다. 다음 번 로그인할 때 선택된 사용자 정의 보기가 기본으로 사용됩니다.

모든 사용자에게 대해 장치의 기본 사용자 정의 보기 할당

장치, 포트 및 노드 관리 권한이 있는 경우 모든 사용자에게 대해 기본 사용자 정의 보기를 지정할 수 있습니다.

▶ **모든 사용자에게 대해 장치의 기본 사용자 정의 보기를 지정하려면:**

1. 장치 탭을 클릭합니다.
2. 장치 > 보기 변경 > 사용자 정의 보기 생성을 선택합니다.
3. 이름 드롭다운 화살표를 클릭하고 시스템 전체 기본 보기로 할당하고자 하는 사용자 정의 보기를 선택합니다.
4. 시스템 전체 확인란을 선택한 다음 저장을 클릭합니다.

CC-SG 에 로그인하는 모든 사용자는 선택한 사용자 정의 보기에 따라 정렬된 장치 탭을 볼 수 있습니다. 사용자는 사용자 정의 보기를 변경할 수 있습니다.

이 장에서

인증 및 허가(AA) 개요.....	128
LDAP 및 AD의 DN(구분 이름).....	129
인증 및 허가에 대한 모듈 지정	130
외부 AA 서버의 순서 설정	131
AD 및 CC-SG 개요.....	131
CC-SG에 AD 모듈 추가.....	131
AD 모듈 편집.....	136
AD 사용자 그룹 가져오기.....	137
AD와 CC-SG 동기화.....	138
LDAP 및 CC-SG 정보	141
CC-SG에 LDAP(Netscape) 모듈 추가	141
TACACS+ 및 CC-SG 정보	145
TACACS+ 모듈 추가.....	145
RADIUS 및 CC-SG 정보.....	146
RADIUS 모듈 추가.....	146

인증 및 허가(AA) 개요

CC-SG의 사용자는 CC-SG에서 로컬로 인증 및 권한 부여되거나 다음의 지원되는 디렉터리 서버를 사용하여 원격으로 인증됩니다.

- Microsoft Active Directory(AD)
- Netscape Lightweight Directory Access Protocol(LDAP)
- TACACS+
- RADIUS

외부 인증을 위해 임의의 수의 원격 서버를 사용할 수 있습니다. 예를 들어, AD 서버 3대, iPlanet(LDAP) 서버 2대 및 RADIUS 서버 3대를 구성할 수 있습니다.

AD만 사용자의 원격 인증을 위해 사용할 수 있습니다.

LDAP 구현은 LDAP v3을 사용합니다.

인증 흐름

원격 인증이 활성화되면 인증 및 허가는 다음 단계를 따릅니다.

1. 사용자는 적절한 사용자 이름과 암호를 사용하여 CC-SG에 로그인합니다.

2. CC-SG 는 외부 서버에 연결하고 사용자 이름 및 암호를 전송합니다.
3. 사용자 이름과 암호는 승인되거나 거부되어 반송됩니다. 인증이 거부되면 결과적으로 로그인 시도는 실패로 돌아갑니다.
4. 인증에 성공한 경우 허가가 수행됩니다. CC-SG 는 입력한 사용자 이름이 CC-SG 에 생성되었거나 AD 에서 가져온 그룹과 일치하는지 확인하고 지정된 규정별로 권한을 부여합니다.

원격 인증이 비활성화되면 인증과 허가가 모두 CC-SG 에서 로컬로 수행됩니다.

사용자 계정

원격 인증을 위해 사용자 계정이 인증 서버에 추가되어야 합니다. 인증과 허가 모두를 위해 AD를 사용하는 경우를 제외하고, 모든 원격 인증 서버에서는 CC-SG에서 사용자를 생성해야 합니다. 인증 서버와 CC-SG의 사용자 이름은 동일해야 하지만 암호는 다를 수 있습니다. 로컬 CC-SG 암호는 원격 인증이 비활성화된 경우에만 사용됩니다. 원격으로 인증되는 사용자를 추가하는 방법에 대한 자세한 내용은 **사용자 및 사용자 그룹** (p. 102)을 참조하십시오.

참고: 원격 인증을 사용할 경우, 원격 서버에서 암호를 변경하려면 사용자는 관리자에게 문의해야 합니다. 원격으로 인증된 사용자의 경우 CC-SG 에서 암호를 변경할 수 없습니다.

LDAP 및 AD의 DN(구분 이름)

LDAP 또는 AD 서버에서 원격으로 인증된 사용자를 구성할 경우 사용자 이름 및 검색을 DN(구분 이름) 형식으로 입력해야 합니다. 전체 구분 이름(DN) 형식은 RFC2253(<http://www.rfc-editor.org/rfc/rfc2253.txt>)에 기술되어 있습니다.

CC-SG 를 구성하려면 DN 을 입력하는 방법 및 DN 의 각 구성요소가 나열되는 순서를 알아야 합니다.

AD의 DN 지정

AD 의 DN 은 이 구조를 따라야 합니다. 공통 이름 및 조직 단위를 지정할 필요는 없습니다.

- common name (cn), organizational unit (ou), domain component (dc)

LDAP의 DN 지정

Netscape LDAP 및 eDirectory LDAP 의 DN 은 이 구조를 따라야 합니다.

- user id (uid), organizational unit (ou), organization (o)

AD의 사용자 이름 지정

사용자 이름에 `cn=administrator,cn=users,dc=xyz,dc=com` 을 지정하여 AD 서버에서 CC-SG 사용자를 인증할 때 CC-SG 사용자가 가져온 AD 그룹과 연관되는 경우 이 자격 증명에 대한 액세스가 부여됩니다. 둘 이상의 공통 이름, 조직 단위 및 도메인 구성요소를 지정할 수 있습니다.

기본 DN 지정

DN(구분 이름)을 입력하여 사용자에게 대한 검색이 시작되는 위치를 지정합니다. 기본 DN 필드에 DN 을 입력하여 사용자를 찾을 수 있는 AD 컨테이너를 지정합니다. 예를 들어, `ou=DCAdmins,ou=IT,dc=xyz,dc=com` 은 `xyz.com` 도메인 아래의 DCAdmins 및 IT 조직 단위에서 모든 사용자를 검색합니다.

인증 및 허가에 대한 모듈 지정

모든 외부 서버를 CC-SG 에 모듈로 추가하면 CC-SG 가 인증, 허가 또는 이 모두에 대해 각 모듈을 사용하게 할지를 지정합니다.

▶ 인증 및 허가를 위해 모듈을 지정하려면:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다. 모든 구성된 외부 허가 및 인증 서버가 표에 표시됩니다.
3. 각 나열된 서버에 대해:
 - a. CC-SG 가 사용자 인증을 위해 서버를 사용하도록 할 경우 인증 확인란을 선택합니다.
 - b. CC-SG 가 사용자 허가를 위해 서버를 사용하도록 할 경우 허가 확인란을 선택합니다. 인증에는 AD 서버만 사용할 수 있습니다.
4. 업데이트를 클릭하여 변경 사항을 저장합니다.

외부 AA 서버의 순서 설정

CC-SG 는 지정한 순서로 구성된 외부 허가 및 인증 서버를 조회합니다. 처음 선택한 옵션을 사용할 수 없으면 CC-SG 는 두 번째 옵션을 시도하고 그 다음 세 번째 옵션을 시도하여 성공할 때까지 계속합니다.

▶ CC-SG 가 외부 인증 및 허가 서버를 사용하는 순서를 설정하려면:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다. 모든 구성된 외부 허가 및 인증 서버가 표에 표시됩니다.
3. 목록에서 서버를 선택하고 위로 및 아래로 화살표를 클릭하여 배치의 우선 순위를 결정합니다.
4. 업데이트를 클릭하여 변경 사항을 저장합니다.

AD 및 CC-SG 개요

CC-SG 는 사용자를 CC-SG 에서 로컬로 정의할 필요 없이 AD 도메인 컨트롤러에서 가져온 사용자의 인증 및 허가를 지원합니다. 따라서 AD 서버에서만 사용자를 유지할 수 있습니다. AD 서버가 CC-SG 에서 모듈로 구성되면 CC-SG 는 지정된 도메인의 모든 도메인 컨트롤러를 질의할 수 있습니다. CCSG 가 AD 사용자 그룹에 대한 최신 허가 정보를 갖도록 CC-SG 의 AD 모듈과 AD 서버를 동기화할 수 있습니다.

중복 AD 모듈을 추가하지 마십시오. 사용자가 로그인을 시도할 때 "그룹의 구성원이 아닙니다."라는 메시지를 나타낼 경우 중복 AD 모듈을 구성했을 수 있습니다. 중첩 도메인 영역을 기술하는지 보려면 구성된 모듈을 확인하십시오.

CC-SG에 AD 모듈 추가

중요: 이 프로세스를 시작하기 전에 적절한 AD 사용자 그룹을 생성하고 해당 그룹에 AD 사용자를 지정합니다. 또한 구성 관리자에 CC-SG DNS 및 도메인 접미사를 구성했는지 확인합니다. CC-SG *네트워크 구성* (p. 179)을 참조하십시오.

▶ CC-SG 에 AD 모듈 추가:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다.

3. 추가를 클릭하여 모듈 추가 창을 엽니다.
4. 모듈 유형 드롭다운 메뉴를 클릭하고 목록에서 AD 를 선택합니다.
5. 모듈 이름 필드에 AD 서버의 이름을 입력합니다.
 - 최대 문자 수는 31 입니다.
 - 모든 인쇄 가능 문자가 사용될 수 있습니다.
 - 모듈 이름은 선택 사항이며 CC-SG 에 구성하는 다른 서버 모듈과 이 AD 서버 모듈을 구별하기 위해 지정됩니다. 이름은 실제 AD 서버 이름에 연결되지 않습니다.
6. 다음을 클릭하여 계속 진행합니다. 일반 탭이 열립니다.

AD 일반 설정

일반 탭에서 CC-SG 가 AD 서버를 질의할 수 있도록 하는 정보를 추가합니다.

중복 AD 모듈을 추가하지 마십시오. 사용자가 로그인을 시도할 때 "그룹의 구성원이 아닙니다."라는 메시지를 보게 될 경우 중복 AD 모듈을 구성했을 수 있습니다. 중첩 도메인 영역을 기술하는지 보려면 구성된 모듈을 확인하십시오.

1. 도메인 필드에 질의할 AD 도메인을 입력합니다. 예를 들어, AD 도메인이 xyz.com 도메인에 설치된 경우 도메인 필드에 xyz.com 을 입력합니다. 질의할 CC-SG 및 AD 서버는 서로 신뢰하는 동일한 도메인 또는 서로 다른 도메인에 구성되어야 합니다.

참고: CC-SG 는 지정된 도메인의 알려진 모든 도메인 컨트롤러를 질의합니다.

2. DNS 서버 IP 주소 필드에 DNS 서버의 IP 주소를 입력하거나 기본 CC-SG DNS 사용 확인란을 선택하여 CC-SG의 구성 관리자 섹션에 구성된 DNS를 사용합니다. **고급 관리** (p. 174)를 참조하십시오.
3. 사용자 이름 및 암호를 지정하지 않고 AD 서버에 연결할 경우 익명 바인드 확인란을 선택합니다. 이 옵션을 사용하면 AD 서버에서 익명 질의를 허용해야 합니다.

참고: 기본적으로 Windows 2003 에서는 익명 질의를 허용하지 않습니다. Windows 2000 서버에서는 질의 결과가 각 개체의 권한을 기준으로 하는 특정 익명 작업을 허용합니다.

4. 익명 바인드를 사용하지 않을 경우 "사용자 이름" 필드에 AD 서버를 질의하는데 사용할 사용자 계정의 사용자 이름을 입력합니다. 필요한 형식은 AD 버전 및 구성에 따라 다릅니다. 다음 형식 중 하나를 사용합니다.

raritan.com 도메인에서 UserN 이라는 로그인 이름을 가진 User Name 이란 사용자는 다음과 같이 입력할 수 있습니다.

- cn=UserName,cn=users,dc=Raritan,dc=com
- UserName@raritan.com
- Raritan/UserName

참고: 지정된 사용자는 AD 도메인에서 검색 질의를 실행하는 권한이 있어야 합니다. 예를 들어, 사용자는 그룹 범위가 전역으로 설정되어 있고 그룹 유형이 보안으로 설정되어 있는 AD 내의 그룹에 속해 있을 수 있습니다.

5. 암호 및 암호 확인 필드에 AD 서버를 질의하는 데 사용할 사용자 계정의 암호를 입력합니다. 최대 길이는 32 자입니다.
6. 지정된 매개변수를 사용하여 AD 서버에 연결을 테스트하려면 연결 테스트를 클릭합니다. 연결 성공에 대한 확인을 받아야 합니다. 확인을 받지 않은 경우, 설정을 검토하여 오류를 확인하고 다시 시도합니다.
7. 다음을 클릭하여 계속 진행합니다. 고급 탭이 열립니다.

AD 고급 설정

▶ 고급 AD 설정을 구성하려면:

1. 고급 탭을 클릭합니다.
2. AD 서버가 수신하는 포트 번호를 입력합니다. 기본 포트는 389 입니다. LDAP 의 보안 연결을 사용하는 경우 이 포트를 변경해야 합니다. 보안 LDAP 연결의 표준 포트는 636 입니다.
3. 연결에 보안 채널을 사용할 경우 LDAP 의 보안 연결 확인란을 선택합니다. 선택한 경우 CC-SG 는 SSL 을 통한 LDAP 을 사용하여 AD 에 연결합니다. 이 옵션은 AD 구성에서 지원되지 않을 수 있습니다.
4. 인증 검색 질의를 실행할 기본 DN(디렉터리 수준/항목)을 지정합니다. CC-SG 는 이 기본 DN 에서 재귀 검색을 수행할 수 있습니다.

예	설명
dc=raritan,dc=com	전체 디렉터리 구조에서 사용자 항목에 대한 검색 질의가 작성됩니다.
cn=Administrators,cn=Users,dc=raritan,dc=com	사용자 항목에 대한 검색 질의는 관리자 하위 디렉터리(항목)에서만 수행됩니다.

5. 필터 필드에 사용자의 속성을 입력하면 검색 질의는 이 기준에 맞는 항목으로만 제한됩니다. 기본 필터는 `objectclass=user`이며, 이는 사용자 유형의 항목만 검색됨을 의미합니다.
6. 사용자 항목에 대해 검색 질의가 수행될 방식을 지정합니다.
 - 애플릿에서 로그인하는 사용자가 AD 서버에서 검색 질의를 수행하는 권한을 가진 경우 바인드 사용을 선택합니다. 그러나 사용자 이름 유형이 바인드 사용자 이름 유형에서 지정된 경우 유형은 애플릿에 제공된 사용자 이름과 병합되고 AD 서버에 연결하는 데 병합된 사용자 이름이 사용됩니다.
 예제: `cn={0},cn=Users,dc=raritan,dc=com` 을 지정하고 `TestUser` 가 애플릿에 제공된 경우 `CC-SG` 는 AD 서버에 연결하기 위해 `cn=TestUser,cn=Users,dc=raritan,dc=com` 을 사용합니다.
 - 검색 후 바인드 사용 확인란을 선택하고 일반 탭에 지정된 사용자 이름과 암호를 사용하여 AD 서버에 연결합니다. 이 항목은 지정된 기본 DN 에서 검색되고 지정된 필터링 기준을 충족하고 "samAccountName" 속성이 애플릿에 입력된 사용자 이름과 동일한 경우에 검색됩니다. 그런 다음 애플릿에 제공된 사용자 이름 및 암호를 사용하여 두 번째 연결이 시도됩니다. 이 두 번째 바인드는 사용자가 올바른 암호를 제공했는지 확인합니다.
7. 다음을 클릭하여 계속 진행합니다. 그룹 탭이 열립니다.

AD 그룹 설정

그룹 탭에서 AD 사용자 그룹을 가져올 정확한 위치를 지정할 수 있습니다.

중요: AD에서 그룹을 가져오기 전에 그룹 설정을 지정해야 합니다.

1. 그룹 탭을 클릭합니다.

- 인증될 사용자를 포함하는 그룹이 검색될 기본 DN(디렉터리 수준/항목)을 지정합니다.

예	설명
dc=raritan,dc=com	전체 디렉터리 구조에서 그룹의 사용자에 대한 검색 질의가 작성됩니다.
cn=Administrators,cn=Users,dc=raritan,dc=com	그룹의 사용자에 대한 검색 질의는 관리자 하위 디렉터리(항목)에서만 수행됩니다.

- 필터 필드에 사용자의 속성을 입력하면 해당 그룹에 있는 사용자의 검색 질의는 이 기준에 맞는 항목으로만 제한됩니다.

예를 들어, cn=Groups,dc=raritan,dc=com 을 기본 DN 으로 지정하고 (objectclass=group)을 필터로 지정할 경우 그룹 항목에 있고 유형 그룹에 속하는 모든 항목이 반환됩니다.

- 다음을 클릭하여 계속 진행합니다. 트러스트 탭이 열립니다.

AD Trust(트러스트) 설정

Trusts(트러스트) 탭에서, 새로운 AD 도메인과 기존의 도메인 간에 신뢰 관계를 설정할 수 있습니다. 인증된 사용자는 신뢰 관계를 통해 도메인에서 리소스에 액세스할 수 있습니다. 신뢰 관계는 들어오고, 나갈 수 있으며, 양방향성이거나 비활성화될 수 있습니다. AD 모듈이 서로의 정보에 액세스할 수 있도록 AD 에서 상이한 포리스트를 나타내게 하려면 신뢰 관계를 설정해야 합니다. CC-SG 에서 구성된 트러스트는 AD 에서 구성된 트러스트와 일치해야 합니다.

- 트러스트(Trusts) 탭을 클릭합니다. 두 개 이상의 AD 도메인을 구성한 경우, 다른 모든 도메인이 트러스트(Trusts) 탭에 나열됩니다.
- Trust Partner(트러스트 파트너) 열의 각 도메인에서, Trust Direction(트러스트 방향) 드롭다운 메뉴를 클릭하고 도메인 간에 설정하고자 하는 트러스트의 방향을 선택합니다. 트러스트 방향은 한 개의 AD 모듈에 대해 변경할 때 모든 AD 모듈에서 업데이트됩니다.
 - 들어오기: 도메인에서 들어오는 정보가 신뢰됩니다.
 - 나가기: 선택한 도메인으로 나가는 정보가 신뢰됩니다.
 - 양방향: 각 도메인의 양 방향에서 정보가 신뢰됩니다.
 - 비활성: 도메인 간에는 정보가 교환되지 않습니다.

3. 적용을 클릭하여 변경 사항을 저장한 다음 확인을 클릭하여 AD 모듈을 저장하고 창을 종료합니다.
새 AD 모듈이 외부 AA 서버 아래의 보안 관리자 화면에 표시됩니다.
4. CC-SG가 사용자 인증을 위해 AD 모듈을 사용하도록 할 경우 인증 확인란을 선택합니다. CC-SG가 사용자 허가를 위해 AD 모듈을 사용하도록 할 경우 허가 확인란을 선택합니다.
5. 업데이트를 클릭하여 변경 사항을 저장합니다.

AD 모듈 편집

AD 모듈을 구성한 후에는 언제든지 AD 모듈을 편집할 수 있습니다.

▶ **AD 모듈을 편집하려면:**

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다. 모든 구성된 외부 허가 및 인증 서버가 표에 표시됩니다.
3. 편집할 AD 모듈을 선택하고 편집을 클릭합니다.
4. 구성된 설정을 보려면 모듈 편집 창에서 각 탭을 클릭합니다. 필요한 경우 내용을 변경합니다. **AD 일반 설정** (p. 132), **AD 고급 설정** (p. 133), **AD 그룹 설정** (p. 134) 및 **AD 트러스트 설정** ("AD Trust(트러스트) 설정" p. 135)을 참조하십시오.
5. 연결 정보를 변경하려면 연결 테스트를 클릭하여 주어진 매개변수를 이용하여 AD 서버에 대한 연결을 테스트합니다. 연결 성공에 대한 확인을 받아야 합니다. 확인을 받지 않은 경우, 설정을 검토하여 오류를 확인하고 다시 시도합니다.
6. 확인을 클릭하여 변경 사항을 저장합니다.
7. 변경한 AD 사용자 그룹을 동기화해야 합니다. 또는 모든 AD 모듈을 동기화하여 모든 모듈의 모든 그룹 및 사용자를 동기화할 수 있습니다. **AD와 모든 사용자 그룹 동기화** (p. 139) 및 **모든 AD 모듈 동기화** (p. 140)를 참조하십시오.

AD 사용자 그룹 가져오기

AD 서버에서 그룹을 가져오기 전에 AD 모듈에서 그룹 설정을 지정해야 합니다. **AD 그룹 설정** (p. 134)을 참조하십시오.

가져온 그룹 또는 사용자를 변경한 후, 가져온 그룹이 AD의 적절한 그룹과 매핑되도록 변경한 AD 사용자 그룹을 동기화하고 모든 모듈에서 모든 그룹 및 사용자를 동기화하기 위해 모든 AD 모듈을 동기화해야 합니다. **AD와 모든 사용자 그룹 동기화** (p. 139) 및 **모든 AD 모듈 동기화** (p. 140)를 참조하십시오.

AD에서 중첩된 그룹을 가져올 수 있습니다.

참고: AD 사용자 그룹을 가져오기 전에 구성 관리자에서 CC-SG DNS 및 도메인 접미사를 구성했는지 확인하십시오. 고급 관리 (p. 174)를 참조하십시오.

▶ AD 사용자 그룹을 가져오려면:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다. 모든 구성된 허가 및 인증 서버가 표에 표시됩니다.
3. AD 사용자 그룹을 가져오려는 AD 서버를 선택합니다.
4. AD 사용자 그룹 가져오기를 클릭하여 AD 서버에 저장된 사용자 그룹 값의 목록을 검색합니다. CC-SG에서 사용할 준비가 되지 않은 사용자 그룹이 있는 경우 여기로 가져오기를 하여 액세스 규정을 지정할 수 있습니다.
5. CC-SG에 가져올 그룹을 선택합니다.
 - 가져온 사용자 그룹 이름은 최대 64자를 포함할 수 있습니다.
 - 사용자 그룹을 검색하려면 사용 그룹 검색 필드에 검색 문자열을 입력하고 이동을 클릭합니다.
 - 열 헤더를 클릭하여 해당 열의 정보별로 사용자 그룹의 목록을 정렬합니다.
 - 모두 선택을 클릭하여 가져올 모든 사용자 그룹을 선택합니다.
 - 모두 선택 취소를 클릭하여 선택된 모든 사용자 그룹을 선택 취소합니다.
6. 규정 열에서, 목록에서 CC-SG 액세스 규정을 선택하여 선택한 그룹에 규정을 지정합니다.
7. 선택한 사용자 그룹을 가져오려면 가져오기를 클릭합니다.

탭: 그룹을 제대로 가져왔는지 확인하고 방금 가져온 그룹의 권한을 보려면 사용자 탭을 클릭하고 가져온 그룹을 선택하여 사용자 그룹 프로필 화면을 엽니다. 권한 및 장치/노드 규정 탭의 정보를 확인합니다. 사용자 그룹과 연관된 AD 모듈의 정보를 보려면 Active Directory 연관체 탭을 클릭합니다.

AD와 CC-SG 동기화

CC-SG의 정보를 AD 서버의 정보와 동기화하는 방법은 여러 가지가 있습니다.

- 모든 모듈의 일일 동기화: CC-SG가 언제든지 매일 모든 AD 모듈과 동기화할 수 있도록 예약된 동기화를 활성화할 수 있습니다. **모든 AD 모듈 동기화** (p. 140)를 참조하십시오. 이 동기화는 허가를 위해 AD를 사용할 경우에만 필요합니다.
- 온 디맨드 동기화: 선택할 경우 두 가지 유형의 동기화를 수행할 수 있습니다.
 1. **모든 Active Directory 모듈:** 이 옵션은 모든 모듈의 일일 동기화와 동일한 작업을 수행하지만 언제든지 필요 시 동기화하기 위해 사용할 수 있습니다. 이 동기화는 허가를 위해 AD를 사용할 경우에만 필요합니다. **모든 AD 모듈 동기화** (p. 140)를 참조하십시오.
 2. **모든 사용자 그룹:** 사용자 그룹을 변경한 경우 이 옵션을 사용합니다. 모든 사용자 그룹을 동기화하면 가져온 사용자 그룹 및 로컬 사용자 그룹을 AD 모듈의 일부로 식별된 사용자 그룹에 매핑할 수 있습니다. 사용자 그룹을 동기화해도 CC-SG의 액세스 정보를 업데이트하지 않습니다. 액세스 정보를 업데이트하려면 모든 일일 동기화 실행을 기다리거나 모든 모듈의 필요 시 동기화를 실행하여 모든 AD 모듈을 동기화해야 합니다. **AD와 모든 사용자 그룹 동기화** (p. 139)를 참조하십시오.

AD와 모든 사용자 그룹 동기화

사용자 그룹을 하나의 AD 모듈에서 다른 AD 모듈로 이동하는 것과 같이 사용자 그룹을 변경하면 모든 사용자 그룹을 동기화해야 합니다. (사용자 그룹의 AD 연관체도 사용자 그룹 프로필, Active Directory 연관체 탭에서 수동으로 변경할 수 있습니다.)

사용자나 도메인 컨트롤러를 변경한 경우 모든 AD 모듈을 동기화해야 합니다. **모든 AD 모듈 동기화** (p. 140)를 참조하십시오.

AD 사용자 그룹을 동기화할 때, CC-SG는 선택한 AD 모듈에 대한 그룹을 검색하여 AD에서 가져온 사용자 그룹과 해당 이름을 비교하고 서로 일치하는지 확인합니다. CC-SG는 일치 결과를 표시하며 CC-SG와 연결할 AD의 그룹을 선택할 수 있습니다. 이 작업은 CC-SG에서 사용자 액세스 정보를 업데이트하지 않습니다. AD 사용자 그룹 동기화는 AD의 그룹 이름만 CC-SG에 매핑합니다.

▶ AD와 모든 사용자 그룹을 동기화하려면:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다. 모든 구성된 허가 및 인증 서버가 표에 표시됩니다.
3. CC-SG의 사용자 그룹과 동기화하려는 사용자 그룹이 있는 AD 서버를 선택합니다.
4. 온 디맨드 동기화 목록에서 모든 사용자 그룹을 선택하고 화살표 버튼을 클릭합니다.
5. 이름이 CC-SG의 사용자 그룹과 일치하는 AD 모듈에서 발견된 모든 사용자 그룹 목록이 표시됩니다. 동기화하려는 사용자 그룹을 선택한 다음 확인을 클릭합니다.

선택한 모듈의 가져온 모든 사용자 그룹이 성공적으로 동기화되면 확인 메시지가 나타납니다.

모든 AD 모듈 동기화

AD 에서 사용자 그룹을 변경 또는 삭제할 때마다, AD 에서 사용자 권한을 변경할 때마다 또는 도메인 컨트롤러에 변경 작업을 할 때마다 모든 AD 모듈을 동기화해야 합니다.

모든 AD 모듈을 동기화하면, CC-SG 는 구성된 모든 AD 모듈에 대한 사용자 그룹을 검색하여 CC-SG 로 가져오거나 CC-SG 의 AD 모듈과 연관된 사용자 그룹과 해당 이름을 비교한 후 CC-SG 로컬 캐시를 새로 고칩니다. CC-SG 로컬 캐시는 각 도메인에 대한 모든 도메인 컨트롤러, CC-SG 의 모듈과 연관된 모든 사용자 그룹 및 알려진 AD 사용자에 대한 사용자 정보를 포함합니다. 사용자가 그룹이 AD 모듈에서 삭제된 경우, CC-SG 는 또한 해당 로컬 캐시에서 삭제된 그룹에 대한 모든 연관체를 제거합니다. 이렇게 하면 CC-SG 가 가장 최신의 AD 사용자 그룹 정보를 갖게 됩니다.

▶ 모든 AD 모듈을 동기화하려면:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다. 모든 구성된 허가 및 인증 서버가 표에 표시됩니다.
3. 온 디맨드 동기화 목록에서 모든 Active Directory 모듈을 선택하고 화살표 버튼을 클릭합니다. 모든 AD 모듈이 성공적으로 동기화되면 확인 메시지가 나타납니다.

모든 AD 모듈의 일일 동기화 활성화 또는 비활성화

▶ 모든 AD 모듈의 일일 동기화를 활성화하려면:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다. 모든 구성된 허가 및 인증 서버가 표에 표시됩니다.
3. 모든 모듈의 일일 동기화 확인란을 선택합니다.
4. 동기화 시간 필드에서 위로 및 아래로 화살표를 클릭하여 CC-SG 가 모든 AD 모듈에 대해 일일 동기화를 수행하려는 시간을 선택합니다.
5. 업데이트를 클릭하여 변경 사항을 저장합니다.

▶ 모든 AD 모듈의 일일 동기화를 비활성화하려면:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다. 모든 구성된 허가 및 인증 서버가 표에 표시됩니다.

3. 모든 모듈의 일일 동기화 확인란을 선택 취소합니다.
4. 업데이트를 클릭하여 변경 사항을 저장합니다.

일일 AD 동기화 시간 변경

일일 동기화가 활성화되면 자동 동기화가 발생하는 시간을 지정할 수 있습니다. 기본적으로 일일 동기화는 23:30에 발생합니다.

▶ 일일 AD 동기화 시간을 변경하려면:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 선택합니다. 모든 모듈의 일일 동기화 확인란이 선택되었는지 확인합니다.
3. 화면 맨 아래의 동기화 시간 필드에서 위로 및 아래로 화살표를 클릭하여 CC-SG가 모든 AD 모듈에 대해 일일 동기화를 수행하려는 시간을 선택합니다.
4. 업데이트를 클릭하여 변경 사항을 저장합니다.

LDAP 및 CC-SG 정보

CC-SG가 시작되고 사용자 이름과 암호가 입력되면, 질의는 CC-SG를 통해 또는 LDAP 서버로 직접 전달됩니다. 사용자 이름 및 암호가 LDAP 디렉터리의 이름 및 암호와 일치하면 사용자가 인증됩니다. 그런 다음 사용자가 LDAP 서버의 로컬 사용자 그룹으로 인증됩니다.

CC-SG에 LDAP(Netscape) 모듈 추가

▶ CC-SG에 LDAP(Netscape) 모듈을 추가하려면:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다.
3. 추가...를 클릭하여 모듈 추가 창을 엽니다.
4. 모듈 유형 드롭다운 메뉴를 클릭하고 목록에서 LDAP을 선택합니다.
5. 모듈 이름 필드에 LDAP 서버의 이름을 입력합니다.
6. 다음을 클릭하여 계속 진행합니다. 일반 탭이 열립니다.

LDAP 일반 설정

1. 일반 탭을 클릭합니다.

2. LDAP 서버의 IP 주소 또는 호스트 이름을 IP 주소/호스트 이름 필드에 입력합니다. 호스트 이름 규칙을 보려면 **용어/약어** (p. 2)를 참조하십시오.
3. 포트 필드에 포트 값을 입력합니다. 기본 포트는 389입니다.
4. 보안 LDAP 서버를 사용하는 경우 LDAP의 보안 연결을 선택합니다.
5. LDAP 서버에서 익명 질의를 허용하는 경우 익명 바인드를 선택합니다. 익명 바인드로 사용자 이름 및 암호를 입력할 필요가 없습니다.

참고: 기본적으로 Windows 2003에서는 익명 질의를 허용하지 않습니다. Windows 2000 서버에서는 질의 결과가 각 개체의 권한을 기준으로 하는 특정 익명 작업을 허용합니다.

6. 익명 바인드를 사용하지 않는 경우, 사용자 이름 필드에 사용자 이름을 입력합니다. DN(구분 이름)을 입력하여 LDAP 서버에 질의하는 데 사용된 자격 증명을 지정합니다. DN의 경우 공통 이름, 조직 단위 및 도메인을 입력합니다. 예를 들어, `uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot`를 입력합니다. 값을 쉼표로 구분하지만 쉼표 앞뒤에는 공백을 사용하지 마십시오. Command Center와 같이 값에 공백이 포함될 수 있습니다.
7. 암호 및 암호 확인 필드에 암호를 입력합니다.
8. 사용자 검색을 시작하는 위치를 지정하려면 기본 DN에 구분 이름을 입력합니다. 예를 들어, `ou=Administrators,ou=TopologyManagement,o=NetscapeRoot`는 도메인 아래 모든 조직 단위를 검색합니다.
9. 특정 유형의 개체로 검색 범위를 좁히려면 필터 필드에 값을 입력합니다. 예를 들어, `(objectclass=person)`은 사람 개체만으로 검색 범위를 좁힙니다.
10. 연결 테스트를 클릭하여 주어진 매개변수를 사용하여 LDAP 서버를 테스트합니다. 연결 성공에 대한 확인을 받아야 합니다. 확인을 받지 않았으면 설정을 검토하여 오류를 확인하고 다시 시도합니다.
11. LDAP 서버의 고급 구성 옵션을 설정하기 위해 고급 탭으로 진행하려면 다음을 클릭합니다.

LDAP 고급 설정

1. 고급 탭을 클릭합니다.

2. 암호화된 LDAP 서버에 암호를 전송하려면 **Base 64** 를 선택합니다. LDAP 서버에 일반 텍스트로 암호를 전송하려면 일반 텍스트를 선택합니다.
3. 기본 개요: 사용자 암호의 기본 암호화를 선택합니다.
4. 사용자 속성 및 그룹 구성원 자격 속성 필드에 사용자 속성 및 그룹 구성원 자격 매개변수를 입력합니다. 이 값은 LDAP 디렉터리 스키마에서 가져와야 합니다.
5. 바인드 유형을 바인드 사용자 이름 유형 필드에 입력합니다.
 - **CC-SG** 가 로그인할 때 입력한 사용자 이름 및 암호 인증을 위해 LDAP 서버로 보내도록 하려면 바인드 사용을 선택합니다. 바인드 사용을 선택하지 않으면, **CC-SG** 가 LDAP 서버에서 사용자 이름을 검색하여 발견한 경우 LDAP 개체를 검색하고 관련 암호와 입력한 암호를 로컬에서 비교합니다.
 - 일부 LDAP 서버에서는 암호를 LDAP 개체의 일부로 검색할 수 없습니다. **CC-SG** 가 암호를 LDAP 개체로 다시 바인드하고 인증을 위해 서버로 다시 보내도록 하려면 검색 후 바인드 사용 확인란을 선택합니다.
6. 확인을 클릭하여 변경 사항을 저장합니다. 새 LDAP 모듈이 외부 AA 서버 아래의 보안 관리자 화면에 표시됩니다.
7. **CC-SG** 가 사용자 인증을 위해 LDAP 모듈을 사용하도록 할 경우 인증 확인란을 선택합니다.
8. 업데이트를 클릭하여 변경 사항을 저장합니다.

Sun One LDAP(iPlanet) 구성 설정

원격 인증을 위해 Sun One LDAP 서버를 사용하는 경우 매개변수 설정에 대해 다음 예를 사용합니다.

매개변수 이름	SUN One LDAP 매개변수
IP 주소/호스트 이름	<디렉터리 서버 IP 주소>
사용자 이름	CN=<유효 사용자 id>
암호	<암호>
기본 DN	O=<조직>
필터	(objectclass=person)
암호(고급 화면)	일반 텍스트
암호 기본값 개요(고급)	SHA
바인드 사용	선택 취소됨
검색 후 바인드 사용	선택됨

OpenLDAP(eDirectory) 구성 설정

원격 인증을 위해 OpenLDAP 서버를 사용하는 경우 다음 예를 사용합니다.

매개변수 이름	Open LDAP 매개변수
IP 주소/호스트 이름	<디렉터리 서버 IP 주소>
사용자 이름	CN=<유효 사용자 ID>, O=<조직>
암호	<암호>
사용자 기준	O=계정, O=<조직>
사용자 필터	(objectclass=person)
암호(고급 화면)	Base64
암호 기본값 개요(고급)	Crypt
바인드 사용	선택 취소됨
검색 후 바인드 사용	선택됨

TACACS+ 및 CC-SG 정보

TACACS+ 서버에서 원격으로 인증된 CC-SG 사용자를 TACACS+ 서버 및 CC-SG에서 생성해야 합니다. TACACS+ 서버와 CC-SG의 사용자 이름이 동일해야 하지만 암호는 다를 수 있습니다. **사용자 및 사용자 그룹 생성** ("사용자 및 사용자 그룹" p. 102)을 참조하십시오.

TACACS+ 모듈 추가

▶ TACACS+ 모듈을 추가하려면:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다.
3. 추가를 클릭하여 모듈 추가 창을 엽니다.
4. 모듈 유형 > TACACS+를 선택합니다.
5. 모듈 이름 필드에 TACACS+ 서버의 이름을 입력합니다.
6. 다음을 클릭합니다. 일반 탭이 열립니다.

TACACS+ 일반 설정

1. TACACS+ 서버의 IP 주소 또는 호스트 이름을 IP 주소/호스트 이름 필드에 입력합니다. 호스트 이름 규칙을 보려면 **용어/약어** (p. 2)를 참조하십시오.
2. TACACS+ 서버가 청취하는 포트 번호를 포트 번호 필드에 입력합니다. 기본 포트 번호는 49입니다.
3. 인증 포트 필드에 인증 포트를 입력합니다.
4. 공유 키를 공유 키 및 공유 키 확인 필드에 입력합니다. 최대 길이는 128자입니다.
5. 확인을 클릭하여 변경 사항을 저장합니다. 새 TACACS+ 모듈이 외부 AA 서버 아래의 보안 관리자 화면에 표시됩니다.
6. CC-SG가 사용자 인증을 위해 TACACS+ 모듈을 사용하도록 할 경우 인증 확인란을 선택합니다.
7. 업데이트를 클릭하여 변경 사항을 저장합니다.

RADIUS 및 CC-SG 정보

RADIUS 서버에서 원격으로 인증되는 CC-SG 사용자를 RADIUS 서버와 CC-SG에서 생성해야 합니다. RADIUS+ 서버와 CC-SG의 사용자 이름이 동일해야 하지만 암호는 다를 수 있습니다. **사용자 및 사용자 그룹 생성** ("사용자 및 사용자 그룹" p. 102)을 참조하십시오.

RADIUS 모듈 추가

▶ RADIUS 모듈을 추가하려면:

1. 관리 > 보안을 선택합니다.
2. 인증 탭을 클릭합니다.
3. 추가를 클릭하여 모듈 추가 창을 엽니다.
4. 모듈 유형 드롭다운 메뉴를 클릭하고 목록에서 RADIUS 를 선택합니다.
5. 모듈 이름 필드에 RADIUS 서버의 이름을 입력합니다.
6. 다음을 클릭하여 계속 진행합니다. 일반 탭이 열립니다.

RADIUS 일반 설정

1. 일반 탭을 클릭합니다.
2. RADIUS 서버의 IP 주소나 호스트 이름을 IP 주소/호스트 이름 필드에 입력합니다. 호스트 이름 규칙을 보려면 **용어/약어** (p. 2)를 참조하십시오.
3. 포트 번호 필드에 포트 번호를 입력합니다. 기본 포트 번호는 1812입니다.
4. 인증 포트 필드에 인증 포트를 입력합니다.
5. 공유 키를 공유 키 및 공유 키 확인 필드에 입력합니다.
6. 확인을 클릭하여 변경 사항을 저장합니다.
7. 새 RADIUS 모듈이 외부 AA 서버 아래의 보안 관리자 화면에 표시됩니다. CC-SG가 사용자 인증을 위해 RADIUS 모듈을 사용하도록 할 경우 인증 확인란을 선택합니다.
8. 업데이트를 클릭하여 변경 사항을 저장합니다.

RADIUS를 이용한 Two-Factor 인증

CC-SG 는 RSA 인증 관리자와 연계된 two-factor 인증을 지원하는 RSA RADIUS 를 사용하여 동적 토큰을 갖는 two-factor 인증 시스템을 이용할 수 있습니다.

이러한 환경에서, 사용자는 우선 사용자 이름 필드에 사용자 이름을 입력하여 CC-SG 에 로그인한 다음 암호 필드에 고정 암호 및 동적 토큰 값을 입력합니다.

CC-SG의 구성은 위에 설명된 표준 RADIUS 원격 인증과 동일합니다. **두 요소 인증 (p. 282)**을 참조하십시오.

이 장에서

보고서 사용	148
감사 추적 보고서	151
오류 로그 보고서	152
액세스 보고서	152
가용성 보고서	153
활성 사용자 보고서	154
잠긴 사용자 보고서	154
모든 사용자 데이터 보고서	154
사용자 데이터 보고서	155
장치 자산 보고서	156
장치 그룹 데이터 보고서	156
질의 포트 보고서	156
노드 자산 보고서	158
활성 노드 보고서	159
노드 생성 보고서	159
노드 그룹 데이터 보고서	159
AD 사용자 그룹 보고서	160
예약된 보고서	160
장치 펌웨어 업그레이드 보고서	161
CC-NOC 동기화 보고서	161

보고서 사용

보고서 데이터 정렬

- 열 헤더를 클릭하여 해당 열에서 값에 따라 보고서 데이터를 정렬합니다. 데이터는 알파벳 순서, 숫자 순서 또는 시간적 순서에 따라 오름차순으로 고쳐집니다.
- 열 헤더를 다시 클릭하면 내림차순으로 정렬됩니다.

보고서 열 너비 크기 조정

선택한 열 너비가 다음에 로그인해서 보고서를 실행할 때 기본 보고서 보기가 됩니다.

1. 마우스 포인터가 이중 화살표 모양이 될 때까지 헤더 열의 열 경계선에 마우스 포인터를 놓습니다.
2. 화살표를 왼쪽 또는 오른쪽으로 클릭하여 끌어서 열 너비를 조절합니다.

보고서 내역 보기

- 보고서의 내역을 보려면 행을 더블 클릭합니다.
- 행이 강조 표시되면 ENTER 키를 눌러 내역을 봅니다.

여러 페이지 보고서 탐색

- 보고서의 맨 아래에 있는 화살표 아이콘을 클릭하여 여러 페이지의 보고서를 탐색합니다.

보고서 인쇄

CC-SG에는 두 개의 인쇄 옵션이 있습니다. 보고서 페이지를 화면에 표시되는 것처럼 인쇄(스크린샷 인쇄)하거나 각 항목의 모든 내역을 포함하여 전체 보고서를 인쇄할 수 있습니다.

참고: 인쇄 옵션은 모든 CC-SG 페이지에 작동합니다.

▶ 보고서의 스크린샷을 인쇄하려면:

1. 인쇄할 보고서를 생성합니다.
2. Secure Gateway > 화면 인쇄를 선택합니다.

▶ 모든 보고서 내역을 인쇄하려면:

1. 인쇄할 보고서를 생성합니다. 표시할 항목 필드에서 모두를 선택하십시오.
2. Secure Gateway > 인쇄를 선택합니다.

보고서를 파일로 저장

보고서를 Excel에서 열 수 있는 .CSV 파일로 저장할 수 있습니다. 보고서를 파일로 저장하면 보고서 화면에서 볼 수 있는 내역뿐만 아니라 모든 보고서 내역이 저장됩니다.

1. 파일로 저장할 보고서를 생성합니다.
2. 파일에 저장을 클릭합니다. 또는 보고서 데이터 관리를 클릭한 다음 저장을 클릭합니다).
3. 파일의 이름을 입력하고 저장할 위치를 선택합니다.
4. 저장을 클릭합니다.

CC-SG에서 보고서 데이터 제거

감사 추적 및 오류 로그 보고서에 표시되는 레코드를 제거할 수 있습니다. 보고서를 제거하면 사용된 검색 기준에 맞는 모든 데이터가 삭제됩니다. 예를 들어, 2008년 3월 26일부터 2008년 3월 27일까지 모든 감사 추적 항목을 검색할 경우 해당 레코드만 제거됩니다. 3월 26일 이전 또는 3월 27일 이후 항목은 감사 추적에 그대로 유지됩니다.

제거된 데이터는 CC-SG에서 영구 제거됩니다.

▶ **CC-SG에서 보고서 데이터를 제거하려면:**

1. CC-SG에서 삭제할 데이터의 보고서를 생성합니다.
2. 제거를 클릭합니다.
3. 예를 클릭하여 확인합니다.

보고서 필터 숨기기 또는 표시

일부 보고서는 보고서 화면의 맨 위에 필터링 기준 세트를 제공합니다. 필터링 섹션을 숨겨서 보고서 영역을 확장할 수 있습니다.

▶ **보고서 필터를 표시하거나 숨기려면:**

- 필터링 섹션을 숨기려면 화면의 맨 위에 필터 도구 모음을 클릭합니다.
- 필터링 섹션을 표시하려면 필터 도구 모음을 다시 클릭합니다.

감사 추적 보고서

감사 추적 보고서는 CC-SG 의 감사 로그와 액세스를 표시합니다. 이 보고서는 장치 또는 포트의 추가, 편집, 삭제, 기타 수정 등과 같은 활동을 포착합니다.

CC-SG 는 다음과 같은 활동의 감사 추적을 관리합니다.

- CC-SG 가 시작될 경우
- CC-SG 가 중지될 경우
- 사용자가 CC-SG 에 로그인할 경우
- 사용자가 CC-SG 에서 로그아웃할 경우
- 사용자가 노드 연결을 시작할 경우

▶ 감사 추적 보고서를 생성하려면:

1. 보고서 > 감사 추적을 선택합니다.
2. 시작 날짜와 시간 및 종료 날짜와 시간 필드에서 보고서의 날짜 범위를 설정합니다. 기본 날짜의 각 구성요소(월, 일, 연도, 시, 분)를 클릭하여 선택하고 위로 및 아래로 화살표를 클릭하여 원하는 숫자를 선택합니다.
3. 메시지 유형, 메시지, 사용자 이름 및 사용자 IP 주소 필드에 추가 매개변수를 입력하여 보고서에 포함할 데이터를 제한할 수 있습니다. 이 필드에 와일드카드를 사용할 수 있습니다.
 - 하나의 메시지 유형으로 보고서를 제한하려면 메시지 유형 필드에서 유형을 선택합니다.
 - 활동과 연관된 메시지 텍스트에 따라 보고서를 제한하려면 메시지 필드에 텍스트를 입력합니다.
 - 특정 사용자의 활동으로 보고서를 제한하려면 사용자 이름 필드에 사용자의 이름을 입력합니다.
 - 특정 IP 주소의 활동으로 보고서를 제한하려면 사용자 IP 주소 필드에 사용자의 IP 주소를 입력합니다.
4. 표시할 항목 필드에서 보고서 화면에 표시할 항목 번호를 선택합니다.
5. 적용을 클릭하여 보고서를 생성합니다.
 - 보고서의 레코드를 제거하려면 제거를 클릭합니다. **CC-SG에서 보고서 데이터 제거** (p. 150)를 참조하십시오.

오류 로그 보고서

CC-SG 는 시스템 문제를 해결하는 데 액세스 및 사용할 수 있는 일련의 오류 로그 파일에 오류 메시지를 보관합니다. 오류 로그는 오류 조건과 연관된 감사 추적 항목의 하위 세트를 포함합니다.

▶ **오류 로그 보고서를 생성하려면:**

1. 보고서 > 오류 로그를 선택합니다.
2. 시작 날짜와 시간 및 종료 날짜와 시간 필드에서 보고서의 날짜 범위를 설정합니다. 기본 날짜의 각 구성요소(월, 일, 연도, 시, 분)를 클릭하여 선택하고 위로 및 아래로 화살표를 클릭하여 원하는 숫자를 선택합니다.
3. 메시지, 사용자 이름 및 사용자 IP 주소 필드에 추가 매개변수를 입력하여 보고서에 포함할 데이터를 제한할 수 있습니다. 이 필드에 와일드카드를 사용할 수 있습니다.
 - 활동과 연관된 메시지 텍스트에 따라 보고서를 제한하려면 메시지 필드에 텍스트를 입력합니다.
 - 특정 사용자의 활동으로 보고서를 제한하려면 사용자 이름 필드에 사용자의 이름을 입력합니다.
 - 특정 IP 주소의 활동으로 보고서를 제한하려면 사용자 IP 주소 필드에 사용자의 IP 주소를 입력합니다.
4. 표시할 항목 필드에서 보고서 화면에 표시할 항목 번호를 선택합니다.
5. 적용을 클릭하여 보고서를 생성합니다.
 - 오류 로그를 삭제하려면 **제거** (참조 "CC-SG에서 보고서 데이터 제거" p. 150)를 클릭합니다. **CC-SG에서 보고서 데이터 제거** (p. 150)를 참조하십시오.

액세스 보고서

액세스한 장치 및 노드, 액세스한 시간 및 액세스한 사용자에 대한 정보를 보려면 액세스 보고서를 생성합니다.

▶ **액세스 보고서를 생성하려면:**

1. 보고서 > 액세스 보고서를 선택합니다.
2. 장치 또는 노드를 선택합니다.

3. 시작 날짜와 시간 및 종료 날짜와 시간 필드에서 보고서의 날짜와 시간 범위를 설정합니다. 기본 날짜의 각 구성요소(월, 일, 연도, 시, 분)를 클릭하여 선택하고 위로 및 아래로 화살표를 클릭하여 원하는 숫자를 선택합니다.
4. 장치 이름, 노드 이름, 사용자 이름 및 사용자 IP 주소 필드에 추가 매개변수를 입력하여 보고서에 포함할 데이터를 제한할 수 있습니다.
 - 특정 장치로 보고서를 제한하려면 장치 이름 필드에 장치 이름을 입력합니다.
 - 특정 노드로 보고서를 제한하려면 노드 이름 필드에 포트 이름을 입력합니다.
 - 특정 사용자의 활동으로 보고서를 제한하려면 사용자 이름 필드에 사용자의 이름을 입력합니다.
 - 특정 IP 주소의 활동으로 보고서를 제한하려면 사용자 IP 주소 필드에 사용자의 IP 주소를 입력합니다.
5. 표시할 항목 필드에서 보고서 화면에 표시할 항목 번호를 선택합니다.
6. 적용을 클릭하여 보고서를 생성합니다.

가용성 보고서

가용성 보고서는 장치나 노드에 대한 모든 연결 상태를 표시합니다. 이 보고서는 CC-SG 관리 네트워크에서 모든 장치 또는 노드에 대한 모든 가용성 정보를 제공합니다.

▶ **가용성 보고서를 생성하려면:**

1. 보고서 > 가용성 보고서를 선택합니다.
2. 노드 또는 장치를 선택합니다.
3. 적용을 클릭합니다.

활성 사용자 보고서

현재 사용자 보고서에는 현재 사용자의 사용자 세션이 표시됩니다. 보고서에서 활성 사용자를 선택하고 CC-SG 에서 해당 사용자를 연결 해제할 수 있습니다.

▶ **활성 사용자 보고서를 생성하려면:**

- 보고서 > 사용자 > 활성 사용자를 선택합니다.

▶ **CC-SG 의 활성 세션에서 사용자를 연결 해제하려면:**

1. 활성 사용자 보고서에서 연결 해제할 사용자 이름을 선택합니다.
2. 로그아웃을 클릭합니다.

잠긴 사용자 보고서

잠긴 사용자 보고서는 여러 번 로그인을 실패했기 때문에 현재 CC-SG에서 잠겨 있는 사용자를 표시합니다. 보고서로부터 사용자의 잠금을 해제할 수 있습니다. **로그아웃 설정** (참조 "잠금 설정" p. 200)을 참조하십시오.

▶ **잠긴 사용자 보고서를 생성하려면:**

- 보고서 > 사용자 > 잠긴 사용자를 선택합니다.

▶ **CC-SG 에서 잠긴 사용자를 잠금 해제하려면:**

- 잠금 해제할 사용자를 선택하고 사용자 잠금 해제를 클릭합니다.

모든 사용자 데이터 보고서

사용자 데이터 보고서는 CC-SG 데이터베이스의 모든 사용자에 대한 특정 데이터를 표시합니다.

▶ **모든 사용자 데이터 보고서를 생성하려면:**

- 보고서 > 사용자 > 모든 사용자 데이터를 선택합니다.
 - 사용자 이름 필드는 모든 CC-SG 사용자의 사용자 이름을 표시합니다.

- 활성 필드는 사용자 프로필에서 로그인 활성 옵션이 선택되었는지 여부에 따라 사용자가 CC-SG에 로그인할 수 있는 경우 true(참)로 표시되고 사용자가 CC-SG에 로그인할 수 없는 경우 false(거짓)로 표시됩니다. **사용자 추가** (p. 108)를 참조하십시오.
- 암호 만료 기간 필드는 사용자가 강제로 암호를 변경하기 전에 동일한 암호를 사용할 수 있는 기간(일)을 표시합니다. **사용자 추가** (p. 108)를 참조하십시오.
- 그룹 필드에는 사용자가 속한 사용자 그룹이 표시됩니다.
- 권한 필드는 사용자에게 지정된 CC-SG 권한을 표시합니다. **사용자 그룹 권한** (p. 271)을 참조하십시오.
- 이메일 필드는 사용자 프로필에 지정된 사용자의 이메일 주소를 표시합니다.
- 사용자 유형 필드는 사용자의 액세스 방법에 따라 로컬 또는 원격을 표시합니다.

사용자 데이터 보고서

사용자 그룹 데이터 보고서에는 사용자와 사용자가 연관된 그룹에 대한 데이터가 표시됩니다.

▶ **사용자 그룹 데이터 보고서를 생성하려면:**

1. 보고서 > 사용자 > 사용자 그룹 데이터를 선택합니다.
2. 지정된 규정을 보려면 사용자 그룹을 더블 클릭합니다.

장치 자산 보고서

장치 자산 보고서는 CC-SG 에서 현재 관리하는 장치에 대한 데이터를 표시합니다.

▶ 장치 자산 보고서를 생성하려면:

- 보고서 > 장치 > 장치 자산 보고서를 선택합니다. 보고서는 모든 장치에 대해 생성됩니다.

▶ 장치 유형별로 보고서 데이터를 필터링하려면:

- 장치 유형을 선택한 다음 적용을 클릭합니다. 선택한 필터가 적용된 보고서가 다시 생성됩니다.
 - 버전이 호환성 매트릭스를 준수하지 않는 장치는 장치 이름 필드에 빨간색 텍스트로 표시됩니다.

장치 그룹 데이터 보고서

장치 그룹 데이터 보고서는 장치 그룹 정보를 표시합니다.

▶ 장치 그룹 데이터 보고서를 생성하려면:

1. 보고서 > 사용자 > 장치 그룹 데이터를 선택합니다.
2. 그룹의 장치 목록을 표시하려면 행을 더블 클릭합니다.

질의 포트 보고서

질의 포트 보고서는 포트 상태에 따라 모든 포트를 표시합니다.

▶ 질의 포트 보고서를 생성하려면:

1. 보고서 > 포트 > 질의 포트를 선택합니다.
2. 포트 상태/가용성 섹션에서 보고서에 포함할 포트 상태를 선택합니다. 둘 이상의 확인란을 선택하면 모든 선택된 상태를 가진 포트가 포함됩니다. 상태 옵션이 지정될 때 최소한 하나의 가용성 옵션을 선택해야 합니다.

상태 유형	포트 상태	정의
	모두	모든 포트
상태:		

상태 유형	포트 상태	정의
	업	
	다운	장치가 다운되어 사용할 수 없으므로 포트에 연결할 수 없습니다.
가용성:		
	유휴 상태	포트가 구성되었으며 포트에 연결할 수 있습니다.
	연결됨	
	사용 중	사용자가 이 포트에 연결되어 있습니다.
	전원 켜기	
	전원 끄기	
구성되지 않음:		
	새로 만들기	포트가 대상 서버에 연결되었지만 구성되지는 않았습니다.
	사용되지 않음	포트가 대상 서버에 연결되지 않았으며 구성되지 않았습니다.

3. Ghost화된 포트를 포함하려면 Ghost 포트를 선택합니다. Ghost 포트는 CIM 또는 대상 서버가 Paragon 시스템에서 제거되거나 전원이 꺼질 때(직접 또는 우연히) 발생합니다. Raritan의 **Paragon II 사용자 설명서**를 참조하십시오. **옵션입니다.**
4. 일시 중지되거나 잠긴 포트를 포함하려면 일시 중지된 포트 또는 잠긴 포트를 선택합니다. 일시 중지된 포트는 장치의 CC-SG 관리가 일시 중지될 때 발생합니다. 잠긴 포트는 장치가 잠길 때 발생합니다. **옵션입니다.**
5. 표시할 항목 필드에서 보고서 화면에 표시할 데이터의 행 번호를 선택합니다.

참고: 이 기본 설정은 작업으로 보고서를 생성할 때 적용되지 않습니다.

6. 적용을 클릭하여 보고서를 생성합니다.

노드 자산 보고서

노드 자산 보고서는 노드 이름, 인터페이스 이름 및 유형, 장치 이름 및 유형, **CC-SG** 에서 관리하는 모든 노드의 노드 그룹을 표시합니다. 또한 지정된 노드 그룹, 인터페이스 유형, 장치 유형 또는 장치에 해당하는 노드에 대한 데이터만 포함하도록 보고서를 필터링할 수 있습니다.

▶ 노드 자산 보고서를 생성하려면:

1. 보고서 > 노드 > 노드 자산 보고서를 선택합니다.
2. 보고서, 모든 노드, 노드 그룹, 장치 그룹 또는 장치에 적용할 필터링 기준을 선택합니다.
 - 노드 그룹, 인터페이스 유형 또는 장치 그룹을 선택한 경우 해당 메뉴에서 매개변수를 선택합니다.
 - 장치를 선택한 경우 보고서에 포함할 노드 자산이 있는 사용 가능 목록에서 장치를 선택하고 추가를 클릭하여 해당 장치를 선택 목록으로 이동합니다.
3. 적용을 클릭하여 보고서를 생성합니다. 노드 자산 보고서가 생성됩니다.

▶ 노드에 대한 책갈피 URL 을 가져오려면:

1. 노드 자산 보고서를 생성하고 내역 대화 상자를 보려면 노드를 더블 클릭합니다.
2. 파일에 저장을 클릭합니다. 모든 보고서 정보가 **.csv** 파일에 저장됩니다.
3. **URL** 열에는 각 노드에 대한 직접 링크가 포함됩니다. 각 노드를 개별적으로 책갈피 설정하는 대신 이 정보를 사용하여 각 노드에 대한 링크가 있는 웹 페이지를 생성할 수 있습니다. **인터페이스 책갈피 설정** (p. 94)을 참조하십시오.

활성 노드 보고서

활성 노드 보고서에는 각 활성 인터페이스의 이름 및 유형, 연결 모드, 연관된 장치, 타임스탬프, 현재 사용자 및 활성 연결을 갖는 각 노드의 사용자 IP 주소가 포함됩니다. 활성 노드 목록을 보고 이 보고서에서 노드를 연결 해제할 수 있습니다.

▶ **활성 노드 보고서를 생성하려면:**

- 보고서 > 노드 > 활성 노드를 선택합니다. 현재 활성 노드가 있는 경우 활성 노드 보고서가 생성됩니다.

▶ **활성 세션에서 노드를 연결 해제하려면:**

- 활성 노드 보고서에서 연결 해제할 노드를 선택한 다음 연결 해제를 클릭합니다.

노드 생성 보고서

노드 생성 보고서는 지정된 시간 내에 성공하거나 실패한 모든 노드 생성 시도를 나열합니다. 모든 노드 생성 시도를 볼 것인지 또는 잠재적 중복 노드만 볼지 여부를 지정할 수 있습니다.

▶ **노드 생성 보고서를 생성하려면:**

1. 보고서 > 노드 > 노드 생성을 선택합니다.
2. 모든 노드 또는 잠재 중복을 선택합니다. 잠재 중복은 보고서를 잠재 중복으로 플래그 설정된 노드로만 제한합니다.
3. 모든 노드를 선택한 경우 시작 날짜와 시간 및 종료 날짜와 시간 필드에서 보고서의 날짜 범위를 설정합니다. 기본 날짜의 각 구성요소(월, 일, 연도, 시, 분)를 클릭하여 선택하고 위로 및 아래로 화살표를 클릭하여 원하는 숫자를 선택합니다.
4. 적용을 클릭합니다. 노드 생성 보고서가 생성됩니다.
 - 결과 필드는 성공, 실패 또는 잠재 중복을 표시하여 노드 생성 시도의 결과를 설명합니다.

노드 그룹 데이터 보고서

노드 그룹 데이터 보고서에는 노드 그룹 정보가 표시됩니다.

▶ **노드 그룹 데이터 보고서를 생성하려면:**

1. 보고서 > 사용자 > 노드 그룹 데이터를 선택합니다.

2. 그룹의 노드 목록을 표시하려면 행을 더블 클릭합니다.

AD 사용자 그룹 보고서

AD 사용자 그룹 보고서는 인증 및 허가에 대해 구성된 AD 서버에서 CC-SG 로 가져온 그룹의 모든 사용자를 표시합니다. 보고서는 CC-SG 를 통해 로컬로 AD 사용자 그룹에 추가된 사용자를 포함하지 않습니다.

▶ AD 사용자 그룹 보고서를 생성하려면:

1. 보고서 > Active Directory > AD 사용자 그룹 보고서를 선택합니다.
2. AD 서버 목록은 인증 및 허가 모두에 대해 CC-SG 에 구성된 모든 AD 서버를 포함합니다. 보고서에 포함할 각 AD 서버에 해당하는 확인란을 선택합니다.
3. AD 사용자 그룹 섹션에서 사용 가능 목록은 AD 서버 목록에서 선택한 AD 서버로부터 CC-SG 로 가져온 모든 사용자 그룹을 포함합니다. 보고서에 포함할 사용자 그룹을 선택하고 추가를 클릭하여 사용자 그룹을 선택 목록으로 이동합니다.
4. 적용을 클릭하여 보고서를 생성합니다.

예약된 보고서

예약된 보고서는 작업 관리자에 예약된 보고서를 표시합니다. 예약된 보고서 화면에서 장치 펌웨어 업그레이드 보고서 및 장치 다시 시작 보고서를 찾을 수 있습니다. 예약된 보고서는 HTML 형식으로만 볼 수 있습니다. **작업 관리자** (p. 209)를 참조하십시오.

▶ 예약된 보고서에 액세스하려면:

1. 보고서 > 예약된 보고서를 선택합니다.
2. 보고서 유형을 선택합니다.
3. 보고서 소유자를 선택합니다.
4. 이름에서 필터링할 보고서 이름을 입력합니다. 전체 이름 또는 일부 이름을 입력할 수 있습니다. 일치하는 결과는 대소문자를 구분하지 않습니다. 와일드카드를 허용되지 않습니다.
5. 시작 날짜와 시간 및 종료 날짜와 시간 필드에서 보고서의 날짜 범위를 설정합니다. 기본 날짜의 각 구성요소(월, 일, 연도, 시, 분)를 클릭하여 선택하고 위로 및 아래로 화살표를 클릭하여 원하는 숫자를 선택합니다.
6. 적용을 클릭합니다. 예약된 보고서 목록이 생성됩니다.

▶ **예약된 보고서를 보려면:**

1. 목록에서 보고서를 선택합니다.
2. 보고서 보기를 클릭합니다.

▶ **예약된 보고서를 삭제하려면:**

1. 삭제할 보고서를 선택합니다. 여러 보고서를 삭제하려면 **Ctrl+클릭** 및 **Shift+클릭**을 사용합니다.
2. 보고서 삭제를 클릭합니다.
3. 예를 클릭하여 확인합니다.

장치 펌웨어 업그레이드 보고서

장치 펌웨어 업그레이드 보고서는 예약된 보고서 목록에서 찾을 수 있습니다. 이 보고서는 장치 펌웨어 업그레이드 작업이 실행 중일 때 생성됩니다. 작업에 대한 실시간 상태 정보를 얻으려면 보고서를 봅니다. 작업이 완료되면 보고서 정보가 변하지 않습니다.

보고서를 보는 방법에 대한 자세한 내용은 **예약된 보고서** (p. 160)를 참조하십시오.

CC-NOC 동기화 보고서

CC-NOC 동기화 보고서에는 CC-SG가 가입하고 특정 검색 날짜에 CC-NOC에서 모니터링하는 IP 주소와 함께 모든 대상이 나열됩니다. 구성된 범위에서 검색되는 새 대상도 여기에 표시됩니다. **CC-NOC 추가 (p. 216)**를 참조하십시오. 이 보고서의 CC-SG 데이터베이스에서 대상을 제거할 수도 있습니다.

▶ **CC-NOC 동기화 보고서를 생성하려면:**

1. 보고서 > CC-NOC 동기화를 선택합니다.
2. 마지막 발견 날짜를 선택하고 대상 가져오기를 클릭합니다. 마지막 발견 날짜 이전에 발견된 대상은 발견된 대상에 표시됩니다.
 - CC-SG 데이터베이스에서 대상을 제거하려면 제거할 대상을 선택하고 제거를 클릭합니다.
 - CC-SG 데이터베이스에서 대상의 전체 목록을 제거하려면 모두 제거를 클릭합니다.

이 장에서

정비 모드.....	162
정비 모드 시작	162
정비 모드 종료	163
CC-SG 백업	163
백업 파일 저장 및 삭제	164
CC-SG 복원	165
CC-SG 재설정	166
CC-SG 다시 시작.....	169
CC-SG 업그레이드	169
CC-SG 종료	172
종료 후 CC-SG 다시 시작.....	172
CC-SG 전원 끄기	172
CC-SG 세션 종료.....	173

정비 모드

정비 모드에서는 관리자가 중단 없이 CC-SG 업그레이드와 같은 다양한 작업을 수행할 수 있도록 CC-SG 에 대한 액세스를 제한합니다.

정비 모드를 시작하고 있는 관리자를 제외한 현재 사용자는 구성 가능 기간이 만료된 후 변경되고 로그아웃됩니다. 정비 모드 상태에서 다른 관리자는 CC-SG 에 로그인할 수 있지만 관리자가 아닌 사용자는 로그인되지 않습니다. CC-SG 가 정비 모드를 시작하거나 종료할 때마다 SNMP 트랩이 생성됩니다.

참고: 정비 모드는 클러스터 구성에 포함되지 않은 독립형 CC-SG 장치에서만 사용할 수 있습니다. 정비 모드를 시작할 때까지 CC-SG 를 업그레이드할 수 없습니다.

예약된 작업 및 정비 모드

CC-SG가 정비 모드인 동안에는 예약된 작업을 실행할 수 없습니다. **작업 관리자** (p. 209)를 참조하십시오. CC-SG가 정비 모드를 종료하면 일정 잡힌 작업이 가능한 빨리 실행됩니다.

정비 모드 시작

1. 시스템 정비 > 정비 모드 > 정비 모드 시작을 선택합니다.

2. 암호: 암호를 입력합니다. CC 설정 및 제어 권한을 가진 사용자만 정비 모드를 시작할 수 있습니다.
3. 방송 메시지: CC-SG 에서 로그아웃할 사용자에게 표시할 메시지를 입력합니다.
4. 정비 모드 시작 시간(분): 0-30 분까지 CC-SG 가 정비 모드를 시작하기 전에 경과 시간을 입력합니다. 정비 모드를 즉시 시작하려면 0(영)을 입력합니다.
5. 확인을 클릭합니다.
6. 확인 대화 상자에서 확인을 클릭합니다.

정비 모드 종료

1. 시스템 정비 > 정비 모드 > 정비 모드 종료를 선택합니다.
2. 정비 모드를 종료하려면 확인을 클릭합니다.
3. CC-SG 가 정비 모드를 종료할 때 메시지가 표시됩니다. 모든 사용자는 CC-SG 에 정상적으로 액세스할 수 있습니다.

CC-SG 백업

CC-SG 를 백업하려면 정비 모드를 시작하는 것이 좋습니다. 정비 모드를 시작하면 백업되는 동안 데이터베이스에 변경이 이루어지지 않도록 보장합니다.

▶ CC-SG 를 백업하려면:

1. 시스템 정비 > 백업을 선택합니다.
2. 백업 이름 필드에 이 백업의 이름을 입력합니다.
3. 설명 필드에 이 백업에 대한 간단한 설명을 입력합니다.
옵션입니다.
4. 백업 유형을 선택합니다.
 - 사용자 정의 - 아래의 백업 옵션 영역에서 선택하여 백업에 추가할 구성 요소를 지정할 수 있습니다. 다음 중 백업에 포함할 각 항목을 선택합니다.
 - 데이터 - CC-SG 구성, 장치 및 노드 구성, 사용자 데이터(표준).
 - 로그 - CC-SG 에 저장된 오류 로그 및 이벤트 보고서
 - CC-SG 펌웨어 파일 - CC-SG 서버를 업데이트하기 위해 사용하는 저장된 펌웨어 파일.

- 장치 펌웨어 파일 - **CC-SG** 에서 관리하는 **Raritan** 장치를 업데이트하기 위해 사용하는 저장된 펌웨어 파일.
 - 애플리케이션 파일 - **CC-SG** 에서 노드에 사용자를 연결하기 위해 사용하는 저장된 애플리케이션.
 - 전체 - **CC-SG** 에 저장된 모든 데이터, 로그, 펌웨어 및 애플리케이션 파일의 백업을 생성합니다. 대용량 백업 파일이 만들어집니다.
 - 표준 - **CC-SG** 의 중요한 데이터의 백업만 생성합니다. 이 백업은 **CC-SG** 구성 정보, 장치 및 노드 구성, 사용자 구성을 포함합니다. 가장 작은 백업 파일을 생성합니다.
5. 이 백업 파일의 복사본을 외부 서버에 저장하려면 원격 위치로 백업 확인란을 선택합니다. **옵션입니다.**
 6. 원격 서버에 연결할 때 사용하는 프로토콜인 **FTP** 또는 **SFTP** 를 선택합니다.
 7. 서버의 **IP** 주소나 호스트 이름을 호스트 이름 필드에 입력합니다.
 8. 선택한 프로토콜(**FTP: 21, SFTP: 22**)의 기본 포트를 사용하지 않는 경우 포트 번호 필드에 사용한 통신 포트를 입력합니다.
 9. 사용자 이름 필드에 원격 서버의 사용자 이름을 입력합니다.
 10. 암호 필드에 원격 서버의 암호를 입력합니다.
 11. 디렉터리 필드에 백업을 원격 서버에 저장할 때 사용하는 디렉터리를 지정합니다. 디렉터리의 절대 경로를 지정해야 합니다.
 12. 확인을 클릭합니다.

백업이 완료되면 메시지가 나타납니다. 백업 파일은 **CC-SG** 파일 시스템에 저장되며 원격 위치로 백업 필드에서 지정된 경우 원격 서버에도 저장됩니다. 이 백업은 나중에 복원할 수 있습니다.

CC-SG 복원 (p. 165)을 참조하십시오.

백업 파일 저장 및 삭제

CommandCenter 복원 화면을 사용하여 **CC-SG** 에 저장된 백업을 저장하고 삭제합니다. 백업을 저장하면 다른 **PC** 에서 백업 파일의 사본을 유지할 수 있습니다. 백업 파일의 아카이브를 생성할 수 있습니다. 다른 위치에 저장된 백업 파일은 다른 **CC-SG** 장치로 업로드할 수 있으며, 그런 다음 하나의 **CC-SG** 에서 다른 위치로 구성을 복사하기 위해 복원할 수 있습니다.

필요하지 않은 백업을 삭제하면 **CC-SG** 의 공간이 절약됩니다.

백업 파일 저장

1. 시스템 정비 > Command Center 복원을 선택합니다.
2. 사용 가능한 백업 표에서 PC 에 저장할 백업을 선택합니다.
3. 파일에 저장을 클릭합니다. 저장 대화 상자가 나타납니다.
4. 파일의 이름을 입력하고 저장할 위치를 선택합니다.
5. 지정된 위치로 백업 파일을 복사하려면 저장을 클릭합니다.

백업 파일 삭제

1. 사용 가능한 백업 표에서 삭제할 백업을 선택합니다.
2. 삭제를 클릭합니다. 확인 대화 상자가 나타납니다.
3. 확인을 클릭하여 CC-SG 시스템에서 백업을 삭제합니다.

CC-SG 복원

생성한 백업 파일을 사용하여 CC-SG 를 복원할 수 있습니다.

▶ CC-SG 를 복원하려면:

1. 시스템 정비 > 복원을 선택합니다. CommandCenter 복원 화면이 나타나고 CC-SG 에 이용 가능한 백업 파일 목록을 표시합니다. 백업 유형, 백업 날짜, 설명, 표가 만들어진 CC-SG 버전 및 백업 파일의 크기를 볼 수 있습니다.
2. CC-SG 시스템에 저장된 백업에서 복원하려면 먼저 백업 파일을 CC-SG 로 업로드해야 합니다. **옵션입니다.**
 - a. 업로드를 클릭합니다.
 - b. 백업 파일을 찾고 대화 창에서 선택합니다. 클라이언트의 네트워크를 통해 어디에서든지 파일을 검색할 수 있습니다.
 - c. 열기를 클릭하여 이 파일을 CC-SG 에 업로드합니다. 완료되면 백업 파일이 사용 가능한 백업 표에 나타납니다.
3. 사용 가능한 백업 표에서 복원할 백업 파일을 선택합니다.
4. 해당하는 경우 이 백업에서 수행할 복원의 종류를 선택합니다.
 - 표준 - 중요한 데이터만 CC-SG 로 복원합니다. 여기에는 CC-SG 구성 정보, 장치 및 노드 구성, 사용자 구성이 포함됩니다.

- 전체 - 백업 파일에 저장된 모든 데이터, 로그, 펌웨어 및 애플리케이션 파일을 복원합니다. 파일에 대한 전체 백업을 만들어야 합니다.
 - 사용자 정의 - 복원 옵션 영역에서 선택하여 **CC-SG** 로 복원할 백업의 구성 요소를 지정할 수 있습니다. 복원에 포함할 다음 각 항목을 선택합니다.
 - 데이터 - **CC-SG** 구성, 장치 및 노드 구성, 사용자 데이터
 - 로그 - **CC-SG** 에 저장된 오류 로그 및 이벤트 보고서
 - **CC** 펌웨어 파일 - **CC-SG** 서버를 업데이트하는 데 사용하는 저장된 펌웨어 파일.
 - 장치 펌웨어 파일 - **CC-SG** 에서 관리하는 **Raritan** 장치를 업데이트하기 위해 사용하는 저장된 펌웨어 파일.
 - 애플리케이션 파일 - **CC-SG** 에서 노드에 사용자를 연결하기 위해 사용하는 저장된 애플리케이션.
5. "복원 시간(분)" 필드에서 복원 작업을 수행하기 전에 **CC-SG** 가 대기하는 시간(분)을 입력합니다. 이 시간은 **0-60** 분입니다. 사용자가 작업을 완료하고 로그아웃하는 시간입니다.
 6. 방송 메시지 필드에서 다른 **CC-SG** 사용자에게 복원이 시작됨을 알리는 메시지를 입력합니다.
 7. 복원을 클릭합니다. **CC-SG** 는 선택한 백업에서 해당 구성을 복원하기 전에 지정된 시간 동안 대기합니다. 복원이 시작되면 다른 모든 사용자는 로그아웃됩니다.

CC-SG 재설정

데이터베이스를 제거하거나 다른 구성 요소를 출하 시 기본 설정으로 재설정하기 위해 **CC-SG** 를 재설정할 수 있습니다. 재설정 옵션을 사용하기 전에 백업을 수행하고 다른 위치로 백업 파일을 저장해야 합니다.

선택된 기본 옵션을 사용하는 것이 좋습니다.

옵션	설명
전체 데이터베이스	<p>이 옵션을 선택하면 기존의 CC-SG 데이터베이스가 제거되고 모든 출고 시 기본값으로 새 버전이 빌드됩니다. 네트워크 설정, SNMP 설정, 펌웨어 및 진단 콘솔 설정은 CC-SG 데이터베이스와 관계가 없습니다.</p> <p>IP-ACL 설정은 IP ACL 표 옵션의 선택과 상관 없이 전체 데이터베이스 재설정으로 재설정됩니다.</p> <p>데이터베이스가 제거되면, 모든 장치, 노드 및 사용자가 제거됩니다. 모든 원격 인증 및 허가 서버가 제거됩니다.</p> <p>CC 슈퍼 사용자 계정이 기본값으로 재설정됩니다. 재설정 작업이 완료된 후 기본 사용자 이름 및 암호인 admin/raritan 으로 로그인해야 합니다.</p>
개인 설정 저장 시도	<p>이 옵션은 전체 CC-SG 데이터베이스 재설정을 선택했을 때 활성화됩니다.</p> <p>CC-SG 데이터베이스가 재구축되기 때문에 이전에 구성된 일부 옵션이 저장됩니다.</p> <ul style="list-style-type: none"> ▪ PC 클라이언트와 CC-SG 간의 보안 통신 ▪ 강력한 암호 강제 실행 ▪ 대역외 노드에 대한 직접 대 프록시 연결 ▪ 비활동 타이머 설정
네트워크 설정	<p>이 옵션은 네트워크 설정을 출고 시 기본값으로 변경합니다.</p> <ul style="list-style-type: none"> ▪ 호스트 이름: CommandCenter ▪ 도메인 이름: localdomain ▪ 모드: 기본/백업 ▪ 구성: 정적 ▪ IP 주소: 192.168.0.192 ▪ 넷마스크: 255.255.255.0 ▪ 게이트웨이: 없음 ▪ 기본 DNS: 없음 ▪ 보조 DNS: 없음 ▪ 어댑터 속도: 자동

옵션	설명
SNMP 구성	이 옵션은 SNMP 설정을 출고 시 기본값으로 재설정합니다. <ul style="list-style-type: none"> ▪ 포트: 161 ▪ 읽기 전용 커뮤니티: public ▪ 읽기-쓰기 커뮤니티: private ▪ 시스템 담당자, 이름, 위치: 없음 ▪ SNMP 트랩 구성 ▪ SNMP 트랩 대상
기본 펌웨어	이 옵션은 모든 장치 펌웨어 파일을 출하 시 기본값으로 재설정합니다. 이 옵션은 CC-SG 데이터베이스를 변경하지 않습니다.
재설정 후 DB 로 펌웨어 업로드	이 옵션은 현재 CC-SG 버전의 펌웨어 파일을 CC-SG 데이터베이스로 로드합니다.
진단 콘솔	이 옵션은 진단 콘솔 설정을 출고 시 기본값으로 복원합니다.
IP-ACL 표	이 옵션은 IP-ACL 표에서 모든 항목을 제거합니다. IP-ACL 설정은 IP ACL 표 옵션을 선택하든 안하든 간에 전체 데이터베이스 재설정으로 재설정됩니다.

▶ **CC-SG 를 재설정하려면:**

1. 재설정하기 전에 CC-SG를 백업하고 백업 파일을 원격 위치로 저장합니다. **CC-SG 백업** (p. 163)을 참조하십시오.
2. 시스템 정비 > 재설정을 참조하십시오.
3. 재설정 옵션을 선택합니다.
4. CC-SG 암호를 입력합니다.
5. 방송 메시지: CC-SG 에서 로그오프할 사용자에게 표시할 메시지를 입력합니다.
6. 0-720 분까지 CC-SG 가 재설정 작업을 수행하기 전에 경과 시간을 입력합니다.
7. 확인을 클릭합니다. 재설정을 확인하는 메시지가 표시됩니다.

CC-SG 다시 시작

다시 시작 명령은 CC-SG 소프트웨어를 다시 시작하는 데 사용됩니다. CC-SG 를 다시 시작하면 CC-SG 의 모든 활성 사용자가 로그아웃됩니다.

다시 시작은 CC-SG 의 전원을 껐다가 다시 켜지 않습니다. 전체 재부팅을 실행하려면 CC-SG 장치의 전원 스위치 또는 진단 콘솔에 액세스해야 합니다.

1. 시스템 정비 > 다시 시작을 선택합니다.
2. 암호 필드에 암호를 입력합니다.
3. 방송 메시지: CC-SG 에서 로그오프할 사용자에게 표시할 메시지를 입력합니다.
4. 다시 시작 시간(분): 0-30 분까지 CC-SG 가 다시 시작하기 전에 경과 시간을 입력합니다.
5. 확인을 클릭하여 CC-SG 를 다시 시작합니다.

CC-SG 업그레이드

CC-SG 의 펌웨어는 새 버전이 출시될 때 업그레이드할 수 있습니다. Raritan 웹 사이트의 지원 섹션에서 펌웨어 파일을 찾을 수 있습니다.

CC-SG 버전 4.0 은 G1 하드웨어와 호환되지 않습니다. CC-SG G1 장치를 버전 4.0 으로 업그레이드하지 마십시오.

펌웨어 파일을 자신의 클라이언트 PC 에 다운로드하여 업그레이드를 진행합니다.

CC 설정 및 제어 권한을 가진 사용자만 CC-SG 를 업그레이드할 수 있습니다.

업그레이드하기 전에 CC-SG 를 백업해야 합니다.

CC-SG 클러스터가 작동하는 경우 업그레이드 전에 먼저 클러스터를 제거해야 합니다. 각 CC-SG 노드를 개별적으로 업그레이드하고 클러스터를 다시 생성하십시오.

중요: CC-SG 및 장치 또는 장치 그룹을 업그레이드 해야 할 경우 CC-SG 업그레이드를 먼저 수행한 다음 장치 업그레이드를 수행합니다.

CC-SG는 업그레이드 프로세스의 일부로서 재부팅됩니다. 업그레이드 동안 프로세스를 중단하거나 장치를 수동으로 재부팅하거나 장치의

전원을 끄거나 켜다가 켜지 마십시오.

▶ **CC-SG 를 업그레이드하려면:**

1. 클라이언트 PC 에 펌웨어 업그레이드 파일을 다운로드합니다.
2. CC 설정 및 제어 권한을 가진 계정을 이용하여 CC-SG Admin 클라이언트에 로그인합니다.
3. 정비 모드를 시작합니다. **정비 모드 시작** (p. 162)을 참조하십시오.
4. CC-SG 가 정비 모드가 되면 시스템 정비 > 업그레이드를 선택합니다.
5. 찾아보기를 클릭합니다. CC-SG 펌웨어 파일(.zip)을 탐색하여 선택한 다음 열기를 클릭합니다.
6. 확인을 클릭하여 펌웨어 파일을 CC-SG 로 업로드합니다.
 펌웨어 파일이 CC-SG 로 업로드된 후 CC-SG 가 업그레이드 프로세스를 시작했음을 나타내는 성공 메시지가 표시됩니다. 이제 모든 사용자는 CC-SG 에서 연결 해제됩니다.
7. 확인을 클릭하여 CC-SG 를 종료합니다.
8. 브라우저 캐시를 지운 다음 브라우저 창을 닫습니다. **브라우저 캐시 지우기** (p. 171)를 참조하십시오.
9. Java 캐시를 지웁니다. **Java 캐시 지우기** (p. 171)를 참조하십시오.
10. CC-SG 에 다시 로그인하기 전에 업그레이드가 완료될 때까지 기다려야 합니다. 진단 콘솔에서 업그레이드를 모니터링할 수 있습니다.
 - a. admin 계정을 이용해 진단 콘솔을 액세스합니다. **관리자 콘솔 액세스** (p. 234)를 참조하십시오.
 - b. 관리자 > 시스템 로그파일 뷰어를 선택합니다. 업그레이드 로그를 보려면 **sg/upgrade.log** 를 선택한 다음 보기를 선택합니다.
 - c. 업그레이드 프로세스가 실행될 때까지 기다립니다. 업그레이드 프로세스가 완료되면 업그레이드 로그에 "업그레이드 완료" 메시지가 표시됩니다.
 - d. 서버를 재부팅해야 합니다. 재부팅 프로세서가 시작되면 업그레이드 로그에 "Linux 재부팅" 메시지가 표시됩니다. 서버가 종료되고 재부팅됩니다.
11. CC-SG 가 재부팅되는 동안 몇 초 기다린 후 새 웹 브라우저 창을 실행합니다.
12. CC 설정 및 제어 권한을 가진 계정을 이용하여 CC-SG Admin 클라이언트에 로그인합니다.

13. 도움말 > Raritan Secure Gateway 정보를 선택합니다.
업그레이드가 성공했는지 검증하기 위해 버전 번호를 확인합니다.
 - 버전이 업그레이드되지 않았으면 이전 단계를 반복합니다.
 - 업그레이드가 완료되었으면 다음 단계를 진행합니다.
14. 정비 모드를 종료합니다. **정비 모드 종료** (p. 163)를 참조하십시오.
15. CC-SG를 백업합니다. **CC-SG 백업** (p. 163)을 참조하십시오.

브라우저 캐시 지우기

이 명령은 브라우저 버전에 따라 약간 다를 수 있습니다.

▶ Internet Explorer 6.0 에서 브라우저 캐시를 지우려면:

1. 도구 > 인터넷 옵션을 선택합니다.
2. 일반 탭에서 파일 삭제를 클릭한 다음 확인을 클릭하여 확인합니다.

▶ FireFox 2.0 에서:

1. 도구 > 개인 데이터 지우기를 선택합니다.
2. 캐시를 선택한 다음 지금 개인 데이터 지우기를 클릭합니다.

Java 캐시 지우기

이 명령은 Java 및 운영 체제 버전에 따라 약간 다를 수 있습니다.

▶ Java 1.6 이 설치된 Windows XP 에서:

1. 제어판 > Java 를 선택합니다.
2. 일반 탭에서 설정을 클릭합니다.
3. 열리는 대화 상자에서 파일 삭제를 클릭합니다.
4. 애플리케이션 및 애플릿 확인란을 선택한 다음 확인을 클릭합니다.

CC-SG 종료

CC-SG 를 종료하면 CC-SG 소프트웨어는 종료되지만 CC-SG 장치의 전원은 꺼지지 않습니다.

CC-SG 가 종료된 후 모든 사용자가 로그아웃됩니다. 진단 콘솔을 통하거나 CC-SG 전원을 껐다가 켜서 CC-SG 를 다시 시작할 때까지 사용자는 다시 로그인할 수 없습니다.

▶ **CC-SG 를 종료하려면:**

1. 시스템 정비 > CommandCenter 종료를 선택합니다.
2. 암호 필드에 암호를 입력합니다.
3. 기본 메시지를 승인하거나 방송 메시지 필드에 현재 온라인으로 연결되어 있는 모든 사용자에게 표시할 메시지를 입력합니다(예를 들어, 사용자에게 CC-SG 의 작업을 완료할 잠깐의 시간을 주고 시스템이 다시 작동할 것으로 예상되는 시간을 알려줍니다).
CC-SG 를 종료할 때 모든 사용자가 연결 해제됩니다.
4. 종료 시간(분) 필드에 CC-SG 를 종료할 때까지 경과하는 시간(분)을 입력합니다. 이 시간은 0-60 분입니다.
5. 확인을 클릭하여 CC-SG 를 종료합니다.

종료 후 CC-SG 다시 시작

CC-SG 를 종료한 후 다음 두 가지 방법 중 하나를 사용하여 장치를 다시 시작합니다.

- 진단 콘솔을 사용합니다. **진단 콘솔** (p. 231)을 참조하십시오.:
- CC-SG 장치 전원을 껐다가 다시 켭니다.

CC-SG 전원 끄기

CC-SG 를 설치하고 실행하는 동안 AC 전원이 끊기는 경우 마지막 전원 상태를 기억합니다. AC 전원이 복원되면 CC-SG 가 자동으로 재부팅됩니다. 그러나 꺼져 있는 상태에서 CC-SG 가 AC 전원을 잃게 되면 AC 전원이 복원되어도 전원이 꺼져 있게 됩니다.

중요: POWER 버튼을 눌러 CC-SG의 전원을 강제로 끄지 마십시오. CC-SG의 전원을 끄는 방법은 다음 절차를 따르십시오.

▶ **CC-SG 의 전원을 끄려면 다음을 수행하십시오.**

1. 베젤을 제거하고 전원 버튼을 꼭 누릅니다.

2. CC-SG 의 전원이 정상적으로 꺼질 때까지 약 1 분간 기다립니다.

참고: 진단 콘솔을 통해 CC-SG 에 로그인한 사용자는 CC-SG 장치의 전원을 끌 때 간단한 방송 메시지를 수신하게 됩니다. 웹 브라우저나 SSH 를 통해 CC-SG 에 로그인한 사용자는 CC-SG 장치의 전원을 끌 때 메시지를 수신하지 않습니다.

3. AC 전원 코드를 제거해야 하는 경우 전원 코드를 제거하기 전에 전원 끄기 프로세스가 완전히 완료되도록 합니다. 이 프로세스는 CC-SG 에서 모든 트랜잭션을 완료하고 데이터베이스를 종료하고 전원 제거를 위해 디스크 드라이브를 안전한 상태로 만드는 데 필요합니다.

CC-SG 세션 종료

CC-SG 세션을 종료하는 방법은 두 가지가 있습니다.

- 클라이언트 창이 열려 있는 동안 로그아웃하여 세션을 종료합니다. **CC-SG에서 로그아웃** (p. 173)을 참조하십시오.
- 종료로 세션을 종료하고 클라이언트 창을 닫습니다. **CC-SG 종료** (p. 173)를 참조하십시오.

CC-SG에서 로그아웃

1. Secure Gateway > 로그아웃을 선택합니다. 로그아웃 창이 열립니다.
2. CC-SG 에서 로그아웃하려면 예를 클릭합니다. 로그아웃하면 CC-SG 로그인 창이 열립니다.

CC-SG 종료

1. Secure Gateway > 종료를 선택합니다.
2. 예를 클릭하여 CC-SG 를 종료합니다.

이 장에서

오늘의 메시지 구성	174
노드 액세스를 위한 애플리케이션 구성.....	175
기본 애플리케이션 구성	177
장치 펌웨어 관리.....	178
CC-SG 네트워크 구성.....	179
로그 활동 구성:.....	185
CC-SG 서버 시간 및 날짜 구성	186
연결 모드: 직접 및 프록시	187
장치 설정.....	189
사용자 정의 JRE 설정 구성	190
SNMP 구성	191
CC-SG 클러스터 구성.....	193
보안 관리자.....	196
통지 관리자.....	208
작업 관리자.....	209
CommandCenter NOC	216
CC-SG에 대한 SSH 액세스.....	219
직렬 관리 포트	227
CC-SG 일련 번호 찾기.....	228
Web Services API.....	228

오늘의 메시지 구성

오늘의 메시지를 이용하여 모든 사용자가 로그인 시에 보는 메시지를 제공할 수 있습니다. 오늘의 메시지를 구성하려면 CC 설정 및 제어 권한이 있어야 합니다.

▶ **오늘의 메시지를 구성하려면:**

1. 관리 > 오늘의 메시지 설정을 선택합니다.
2. 로그인 후 모든 사용자에게 메시지를 표시하려면 모든 사용자에게 오늘의 메시지 표시를 선택합니다. **옵션입니다.**
3. CC-SG 에 메시지를 입력하려면 오늘의 메시지 내용 확인란을 선택하고 기존 파일에서 메시지를 로드하려면 오늘의 메시지 파일 확인란을 선택합니다.
 - 오늘의 메시지 내용을 선택한 경우:
 - a. 대화 상자에 메시지를 입력합니다.

- b. 글꼴 이름 드롭다운 메뉴를 클릭하고 메시지 텍스트의 글꼴을 선택합니다.
 - c. 글꼴 크기 드롭다운 메뉴를 클릭하고 메시지 텍스트의 글꼴 크기를 선택합니다.
 - 오늘의 메시지 파일을 선택한 경우:
 - a. 찾아보기를 클릭하여 메시지 파일을 찾습니다.
 - b. 열리는 대화 창에서 파일을 선택하고 열기를 클릭합니다.
 - c. 미리 보기를 클릭하여 파일의 내용을 검토합니다.
4. 확인을 클릭하여 변경 사항을 저장합니다.

노드 액세스를 위한 애플리케이션 구성

노드 액세스를 위한 애플리케이션 정보

CC-SG 는 노드에 액세스하기 위해 사용할 수 있는 여러 가지 애플리케이션을 제공합니다. 애플리케이션 관리자를 사용하여 애플리케이션을 보고, 새 애플리케이션을 추가하며, 애플리케이션을 삭제하고 각 장치 유형에 대한 기본 애플리케이션을 설정할 수 있습니다.

▶ CC-SG 에서 이용 가능한 애플리케이션을 보려면:

1. 관리 > 애플리케이션을 선택합니다.
2. 애플리케이션 이름 드롭다운 메뉴를 클릭하고 CC-SG 에서 이용할 수 있는 애플리케이션 목록을 봅니다.

애플리케이션 버전 확인 및 업그레이드

Raritan Console(RC) 및 Raritan Remote Client(RRC)와 같은 CC-SG 애플리케이션을 확인 및 업그레이드합니다.

▶ 애플리케이션 버전을 확인하려면:

1. 관리 > 애플리케이션을 선택합니다.
2. 목록에서 애플리케이션 이름을 선택합니다. 버전 필드의 번호를 메모합니다. 일부 애플리케이션은 버전 번호를 자동으로 표시하지 않습니다.

▶ 애플리케이션을 업그레이드하려면:

애플리케이션이 최신 버전이 아닌 경우 애플리케이션을 업그레이드해야 합니다. Raritan 웹 사이트에서 애플리케이션 업그레이드 파일을 다운로드할 수 있습니다. 지원되는 애플리케이션 버전의 전체 목록은 Raritan 지원 웹 사이트의 호환성 매트릭스를 참조하십시오.

애플리케이션을 업그레이드하기 전에 정비 모드를 시작하는 것이 좋습니다. **정비 모드 시작** (p. 162)을 참조하십시오.

1. 클라이언트 PC 에 애플리케이션 파일을 저장합니다.
2. 애플리케이션 이름 드롭다운 화살표를 클릭하고 목록에서 업그레이드해야 하는 애플리케이션을 선택합니다. 애플리케이션이 목록에 없을 경우 먼저 추가해야 합니다. **애플리케이션 추가** (p. 176)를 참조하십시오.
3. 찾아보기를 클릭하고 표시된 대화 상자에서 애플리케이션 업그레이드 파일을 찾아 선택한 다음 열기를 클릭합니다.
4. 애플리케이션 이름이 애플리케이션 관리자 화면의 새 애플리케이션 파일 필드에 표시됩니다.
5. 업로드를 클릭합니다. 진행률 창이 새로운 애플리케이션이 업로드 중임을 표시합니다. 완료되면 새 창에 애플리케이션이 **CC-SG** 데이터베이스에 추가되었고 사용할 수 있다는 내용이 표시됩니다.
6. 버전 필드가 자동으로 업데이트되지 않을 경우 버전 필드에 새 버전 번호를 입력합니다. 일부 애플리케이션의 경우 버전 필드가 자동으로 업데이트됩니다.
7. 업데이트를 클릭합니다.

*참고: 업그레이드 동안 로그인한 사용자는 새 버전의 애플리케이션이 실행하기 위해 **CC-SG** 를 로그아웃한 다음 다시 로그인해야 합니다.*

애플리케이션 추가

CC-SG 에 애플리케이션을 추가할 경우 애플리케이션이 작동할 장치 유형을 지정해야 합니다. 장치가 **KVM** 및 직렬 액세스를 제공하는 경우 장치는 각 방법당 한 번씩 두 번 나열됩니다.

▶ 애플리케이션을 추가하려면:

1. 관리 > 애플리케이션을 선택합니다.
2. 추가를 클릭합니다. 애플리케이션 추가 대화 창이 열립니다.
3. 애플리케이션 이름 필드에 애플리케이션의 이름을 입력합니다.

4. 사용 가능 목록에서 애플리케이션이 작동할 **Raritan** 장치를 선택하고 추가를 클릭하여 선택 목록에 해당 장치를 추가합니다.
 - 애플리케이션을 사용한 장치를 제거하려면 선택 목록에서 장치를 선택하고 제거를 클릭합니다.
5. 확인을 클릭합니다. 열기 대화 상자가 나타납니다.
6. 애플리케이션 파일(보통 .jar 또는 .cab 파일)을 탐색하고 선택한 다음 열기를 클릭합니다.
7. 선택된 애플리케이션이 CC-SG 에 로드됩니다.

애플리케이션 삭제

▶ 애플리케이션을 삭제하려면:

1. 관리 > 애플리케이션을 선택합니다.
2. 애플리케이션 이름 드롭다운 메뉴에서 애플리케이션을 선택합니다.
3. 삭제를 클릭합니다. 확인 대화 상자가 나타납니다.
4. 예를 클릭하여 애플리케이션을 삭제합니다.

기본 애플리케이션 구성

기본 애플리케이션 정보

CC-SG 가 각 장치 유형에 대해 기본적으로 사용할 애플리케이션을 지정할 수 있습니다.

기본 애플리케이션 지정 보기

▶ 기본 애플리케이션 지정을 보려면:

1. 관리 > 애플리케이션을 선택합니다.
2. 기본 애플리케이션 탭을 클릭하여 다양한 인터페이스 및 포트 유형에 대한 현재 기본 애플리케이션을 보고 편집합니다. 여기에 나열된 애플리케이션은 선택한 인터페이스를 통해 액세스를 허용하도록 노드를 구성할 때 기본 선택 사항이 됩니다.

인터페이스 또는 포트 유형에 대한 기본 애플리케이션을 선택합니다.

▶ **인터페이스 또는 포트 유형에 대한 기본 애플리케이션을 설정하려면:**

1. 관리 > 애플리케이션을 선택합니다.
2. 기본 애플리케이션 탭을 클릭합니다.
3. 설정할 기본 애플리케이션에 대한 인터페이스 또는 포트 유형을 선택합니다.
4. 해당 행에 나열된 애플리케이션 화살표를 더블 클릭합니다. 값은 드롭다운 메뉴가 됩니다. 회색으로 된 값은 변경할 수 없습니다.
5. 선택된 인터페이스나 포트 유형에 연결할 때 사용할 기본 애플리케이션을 선택합니다.
 - 자동 탐지: CC-SG 는 클라이언트 브라우저를 기반으로 적절한 애플리케이션을 자동 선택합니다.
6. 업데이트를 클릭하여 변경 사항을 저장합니다.

장치 펌웨어 관리

CC-SG는 Raritan 장치의 펌웨어를 저장하여 제어하는 장치를 업데이트하는 데 사용할 수 있습니다. 펌웨어 관리자는 CC-SG에 대해 장치 펌웨어 파일을 업로드 및 삭제하는 데 사용됩니다. 펌웨어 파일이 업로드되면 장치 업그레이드를 수행하기 위해 액세스할 수 있습니다. **장치 업그레이드** (p. 42)를 참조하십시오.

펌웨어 업로드

다른 버전의 장치 펌웨어를 CC-SG 에 업로드할 수 있습니다. 새 펌웨어 버전이 공개되면 Raritan 웹 사이트에 게시됩니다.

▶ **CC-SG 로 펌웨어를 업로드하려면:**

1. 관리 > 펌웨어를 선택합니다.
2. 추가를 클릭하여 새 펌웨어 파일을 추가합니다. 검색 창이 열립니다.
3. CC-SG 에 업로드할 펌웨어 파일을 탐색하고 선택한 다음 열기를 클릭합니다. 업로드가 완료되면 새 펌웨어가 펌웨어 이름 필드에 나타납니다.

펌웨어 삭제

▶ 펌웨어를 삭제하려면:

1. 관리 > 펌웨어를 선택합니다.
2. 펌웨어 이름 드롭다운 화살표를 클릭하고 삭제할 펌웨어를 선택합니다.
3. 삭제를 클릭합니다. 확인 메시지가 나타납니다.
4. 예를 클릭하여 펌웨어를 삭제합니다.

CC-SG 네트워크 구성

구성 관리자에서 CC-SG 관리 네트워크의 네트워크 설정을 구성할 수 있습니다.

네트워크 설정 정보

CC-SG 는 두 가지 모드의 네트워크 설정을 제공합니다.

- 기본/백업 모드: *기본/백업 모드란 무엇입니까?* (p. 180) 참조
- 활성/활성 모드: *활성/활성 모드란 무엇입니까?* (p. 183) 참조

CC-SG는 정적 또는 DHCP-할당 IP 주소도 허용합니다. CC-SG의 DHCP 사용에 대한 모범 사례는 **CC-SG에 대한 권장 DHCP 구성** (p. 185)을 참조하십시오.

CC-SG LAN 포트 정보

CC-SG 는 두 개의 기본 LAN 포트를 제공합니다. 기본 LAN 및 보조 LAN. 기본/백업 및 활성/활성 모드에서는 다른 방법으로 CC-SG LAN 포트에 연결해야 합니다.

CC-SG 모델의 기본 및 보조 LAN 포트 위치를 확인하려면 아래 표를 참조하십시오.

▶ V1 LAN 포트:

모델	기본 LAN 이름	기본 LAN 위치	보조 LAN 이름	보조 LAN 위치
V1	LAN1	왼쪽 LAN 포트	LAN2	오른쪽 LAN 포트

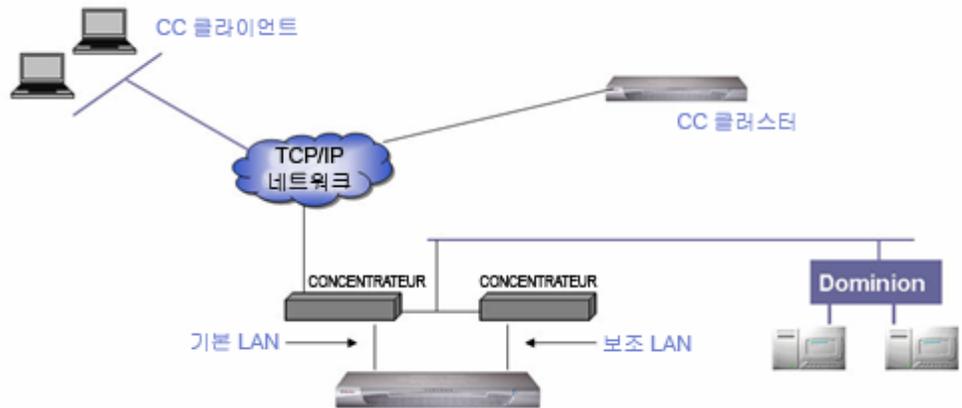
▶ E1 LAN 포트:

모델	기본 LAN 이름	기본 LAN 위치	보조 LAN 이름	보조 LAN 위치
E1	레이블되지 않음	장치 후면 패널의 중앙에 2 개의 포트가 세트 구성된 곳에서 상단 LAN 포트	레이블되지 않음	장치 후면 패널의 중앙에 2 개의 포트가 세트 구성된 곳에서 하단 LAN 포트

기본/백업 모드를 무엇입니까?

기본/백업 모드에서 두 개의 CC-SG LAN 포트를 사용하여 네트워크 장애 복구 및 중복성을 구현할 수 있습니다. 이 모드에서 하나의 LAN 포트만 한 번에 활성이 됩니다.

각 CC-SG 모델에 대한 기본 LAN 및 보조 LAN 포트의 위치에 대해서는 **CC-SG LAN 포트 정보** (p. 179)를 참조하십시오.



기본 LAN 이 연결되어 있고 링크 무결성 신호를 수신하는 경우 CC-SG 는 모든 통신에서 이 LAN 포트를 사용합니다. 기본 LAN 이 링크 무결성을 잃게 되고 보조 LAN 이 연결되면 CC-SG 는 할당된 IP 주소를 보조 LAN 으로 장애 복구합니다. 보조 LAN 은 기본 LAN 이 서비스를 복원할 때까지 사용됩니다. 기본 LAN 이 다시 서비스를 제공할 때 CC-SG 는 자동으로 기본 LAN 사용으로 복원됩니다.

하나의 LAN 연결이 실행되고 있는 한 클라이언트는 장애 중의 서비스 중단을 알지 못합니다.

▶ 기본/백업 모드의 설정:

CC-SG 네트워크에 대한 기본/백업 모드를 구현할 때:

- 두 개의 CC-SG LAN 포트가 동일한 LAN 하위 네트워크에 연결되어야 합니다.
- 신뢰성을 위해 각 LAN 포트를 동일한 하위 네트워크의 다른 스위치 또는 허브에 연결할 수 있습니다. **옵션입니다.**

▶ CC-SG 에서 기본/백업 모드를 구성하려면:

1. 관리 > 구성을 선택합니다.
2. 네트워크 설정 탭을 클릭합니다.
3. 기본/백업 모드를 선택합니다.
4. CC-SG 호스트 이름을 호스트 이름 필드에 입력합니다. 호스트 이름 규칙을 보려면 **용어/약어** (p. 2)를 참조하십시오. 구성을 저장하기 위해 구성 업데이트를 클릭하면 DNS와 도메인 접미부가 구성된 경우 FQDN(완전한 도메인 이름)을 반영하도록 호스트 이름 필드가 업데이트됩니다.
5. 구성 드롭다운 화살표를 클릭하고 DHCP 또는 정적을 선택합니다.

DHCP:

- DHCP 를 선택한 경우 이 네트워크 설정을 저장하고 CC-SG 를 다시 시작하면 기본 DNS, 보조 DNS, 도메인 접미사, IP 주소, 서브넷 마스크 및 기본 게이트웨이 필드가 자동으로 채워집니다(DHCP 서버가 이 정보를 제공하도록 구성된 경우).
- DHCP 서버가 제공하는 정보를 사용하여 CC-SG 에서 동적 업데이트를 승인하는 경우 DNS 서버에 동적으로 자체 등록합니다.
- **CC-SG 에 대한 권장 DHCP 구성** (p. 185)을 참조하십시오.

정적:

- 정적을 선택한 경우, 적절한 필드에 기본 DNS, 보조 DNS, 도메인 접미사, IP 주소, 서브넷 마스크 및 기본 게이트웨이를 입력합니다.
6. 어댑터 속도 드롭다운 화살표를 클릭하고 목록에서 회선 속도를 선택합니다. 선택 사항이 스위치의 어댑터 포트 설정과 일치하는지 확인하십시오. 스위치가 1Giga 회선 속도를 사용하는 경우 자동으로 선택합니다.
 7. 어댑터 속도 필드에서 자동으로 선택한 경우, 어댑터 모드 필드는 비활성화되고 전이중이 자동으로 선택됩니다. 자동 이외의 어댑터 속도를 지정한 경우 어댑터 모드 드롭다운 화살표를 클릭하고 목록에서 이중 모드를 선택합니다.
 8. 구성 업데이트를 클릭하여 변경 사항을 저장합니다. 변경 사항을 적용하려면 CC-SG 를 다시 시작해야 합니다.
 - CC-SG 를 자동으로 다시 시작하려면 지금 다시 시작을 클릭합니다.
 - 나중에 수동으로 CC-SG를 다시 시작하려면 나중에 나중에 다시 시작을 클릭합니다. **CC-SG 다시 시작** (p. 169)을 참조하십시오.
 - 변경 사항을 저장하지 않고 네트워크 설정 패널로 복귀하려면 취소를 클릭합니다. 변경 사항을 저장하려면 구성 업데이트를 클릭한 다음 지금 다시 시작 또는 나중에 다시 시작을 클릭해야 합니다.

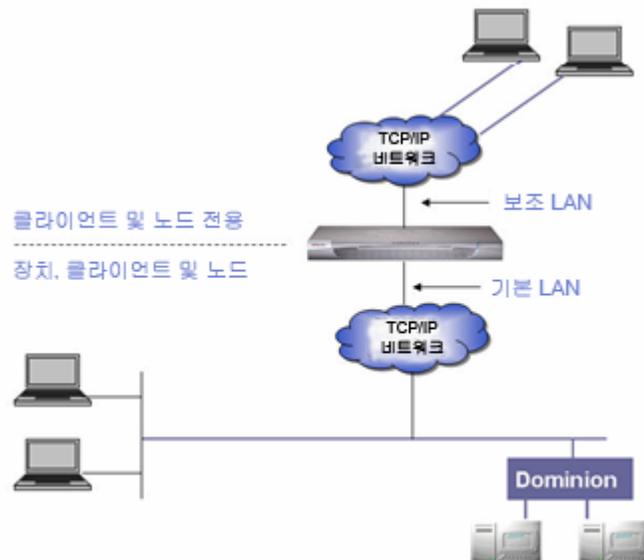
참고: CC-SG 가 DHCP 로 구성된 경우 DNS 서버에 성공적으로 등록된 후 호스트 이름을 통해 CC-SG 에 액세스할 수 있습니다.

활성/활성 모드란 무엇입니까?

활성/활성 모드에서 CC-SG 를 사용하여 두 개의 별개 네트워크에 있는 장치 및 노드를 관리할 수 있습니다. 이 모드에서 CC-SG 는 두 개의 별도 IP 도메인 사이에 트래픽을 관리합니다. 활성/활성 모드는 장애 복구를 제공하지 않습니다. LAN 연결에 장애가 생길 경우 사용자는 액세스할 수 없습니다.

각 CC-SG 모델에 대한 기본 LAN 및 보조 LAN 포트의 위치에 대해서는 **CC-SG LAN 포트 정보** (p. 179)를 참조하십시오.

참고: 활성/활성 모드를 사용하는 경우 클러스터링을 구성할 수 없습니다.



▶ **활성/활성 모드 설정:**

CC-SG 네트워크에 대해 활성/활성 모드를 구현할 때:

- 각 CC-SG LAN 포트는 다른 하위 네트워크에 연결되어야 합니다.
- Raritan 장치는 기본 LAN에만 연결되어야 합니다.
- 클라이언트 및 노드는 기본 LAN 또는 보조 LAN에 연결될 수 있습니다.
- CC-SG의 네트워크 설정 패널에서 최대 하나의 기본 게이트웨이를 지정합니다. 필요할 경우 진단 콘솔을 사용하여 정적 루트를 추가합니다. **정적 루트 편집** (p. 239)을 참조하십시오.

▶ **CC-SG에서 활성/활성 모드를 구성하려면:**

1. 관리 > 구성을 선택합니다.
2. 네트워크 설정 탭을 클릭합니다.
3. 활성/활성 모드를 선택합니다.
4. CC-SG 호스트 이름을 호스트 이름 필드에 입력합니다. 호스트 이름 규칙을 보려면 **용어/약어** (p. 2)를 참조하십시오. 구성을 저장하기 위해 구성 업데이트를 클릭하면 DNS와 도메인 접미부가 구성된 경우 FQDN(완전한 도메인 이름)을 반영하도록 호스트 이름 필드가 업데이트됩니다.
5. 왼쪽 열에 기본 LAN을 구성하고 오른쪽 열에는 보조 LAN을 구성합니다.
6. 구성 드롭다운 화살표를 클릭하고 DHCP 또는 정적을 선택합니다.

DHCP:

- DHCP를 선택한 경우 이 네트워크 설정을 저장하고 CC-SG를 다시 시작하면 기본 DNS, 보조 DNS, 도메인 접미사, IP 주소, 서브넷 마스크 및 기본 게이트웨이 필드가 자동으로 채워집니다(DHCP 서버가 이 정보를 제공하도록 구성된 경우).
- DHCP 서버가 제공하는 정보를 사용하여 CC-SG에서 동적 업데이트를 승인하는 경우 DNS 서버에 동적으로 자체 등록합니다.
- **CC-SG에 대한 권장 DHCP 구성** (p. 185)을 참조하십시오.

정적:

- 정적을 선택한 경우, 적절한 필드에 기본 DNS, 보조 DNS, 도메인 접미사, IP 주소 및 서브넷 마스크를 입력합니다.
- 둘 모두가 아니라 하나의 기본 게이트웨이만 지정합니다.

7. 어댑터 속도 드롭다운 화살표를 클릭하고 목록에서 회선 속도를 선택합니다. 선택 사항이 스위치의 어댑터 포트 설정과 일치하는지 확인하십시오. 스위치가 1 Gig 회선 속도를 사용하는 경우 자동으로 선택합니다.
8. 어댑터 속도 필드에서 자동으로 선택한 경우, 어댑터 모드 필드는 비활성화되고 전이중이 자동으로 선택됩니다. 자동 이외의 어댑터 속도를 지정한 경우 어댑터 모드 드롭다운 화살표를 클릭하고 목록에서 이중 모드를 선택합니다.
9. 구성 업데이트를 클릭하여 변경 사항을 저장합니다. CC-SG 가 다시 시작됩니다.

CC-SG에 대한 권장 DHCP 구성

다음 권장 DHCP 구성을 검토합니다. DHCP 를 사용하기 위해 CC-SG 를 구성하기 전에 DHCP 서버가 적절히 설정되었는지 확인합니다.

- CC-SG 의 IP 주소를 정적으로 할당하려면 DHCP 를 구성합니다.
- DHCP 가 CC-SG 에 IP 주소를 할당할 때 DNS 에 CC-SG 를 자동으로 등록하도록 DHCP 및 DNS 서버를 구성합니다.
- CC-SG 로부터 비인증 동적 도메인 이름 체계(DDNS) 등록 요청을 받도록 DNS 를 구성합니다.

로그 활동 구성:

외부 로깅 서버에 보고하고 각 로그에 보고된 메시지 수준을 지정하기 위해 CC-SG 를 구성할 수 있습니다.

▶ CC-SG 로그 활동을 구성하려면:

1. 관리 > 구성을 선택합니다.
2. 로그 탭을 클릭합니다.
3. CC-SG 에서 사용할 외부 로그 서버를 지정하려면 기본 서버 아래의 서버 주소 필드에 IP 주소를 입력합니다.
4. 전송 수준 드롭다운 화살표를 클릭하고 이벤트 심각도 수준을 선택합니다. 이 수준 이상의 모든 이벤트는 로그 서버로 전송됩니다.
5. 두 번째 외부 로그 서버를 구성하려면 보조 서버 아래의 필드에 대해 3-4 단계를 반복합니다.
6. CommandCenter 로그에서 전송 수준 드롭다운 메뉴를 클릭하고 심각도 수준을 선택합니다. 이 수준 이상의 모든 이벤트는 CC-SG 의 고유 내부 로그에서 보고됩니다.

7. 구성 업데이트를 클릭하여 변경 사항을 저장합니다.

CC-SG의 내부 로그 제거

CC-SG의 외부 로그를 제거할 수 있습니다. 이 작업은 외부 로그 서버에 기록된 이벤트를 삭제하지 않습니다.

참고: 감사 추적 및 오류 로그 보고서는 CC-SG의 내부 로그에 기반합니다. CC-SG의 내부 로그를 제거하면 이러한 두 개의 보고서도 제거됩니다. 이 보고서를 개별적으로 제거할 수도 있습니다.

CC-SG에서 보고서 데이터 제거 (p. 150)를 참조하십시오.

▶ **CC-SG의 내부 로그를 제거하려면:**

1. 관리 > 구성을 선택합니다.
2. 로그 탭을 클릭합니다.
3. 제거를 클릭합니다.
4. 예를 클릭합니다.

CC-SG 서버 시간 및 날짜 구성

장치 관리 기능에 신뢰성을 제공하려면 CC-SG의 시간 및 날짜가 정확하게 유지되어야 합니다.

중요: 시간/날짜 구성은 작업 관리자에서 작업을 예약할 때 사용됩니다. *작업 관리자 (p. 209)*를 참조하십시오. 클라이언트 PC에서 설정된 시간은 **CC-SG**에서 설정된 시간과 다를 수 있습니다.

비슷한 권한을 갖는 CC 슈퍼 사용자 및 사용자만 시간 및 날짜를 구성할 수 있습니다.

클러스터 구성에서는 시간대 변경을 사용할 수 없습니다.

▶ **CC-SG 서버 시간 및 날짜를 구성하려면:**

1. 관리 > 구성을 선택합니다.
2. 시간/날짜 탭을 클릭합니다.
 - a. 날짜와 시간을 수동으로 설정하려면 다음을 수행하십시오.
 - 날짜 - 드롭다운 화살표를 클릭하여 월을 선택하고 위로 및 아래로 화살표를 사용하여 연도를 선택한 다음 달력 영역에서 일을 클릭합니다.

- 시간 - 위로 및 아래로 화살표를 사용하여 시, 분 및 초를 설정한 후 시간대 드롭다운 화살표를 클릭하여 CC-SG가 작동하는 시간대를 선택합니다.
- a. NTP를 통해 시간 및 날짜를 설정하려면 다음을 수행하십시오. 창 맨 아래에 있는 네트워크 시간 프로토콜 활성화 확인란을 선택한 다음 해당 필드에 기본 NTP 서버 및 보조 NTP 서버의 IP 주소를 입력합니다.

참고: 네트워크 시간 프로토콜(NTP)은 연결된 컴퓨터의 날짜 및 시간 데이터를 참조 NTP 서버와 동기화하는 데 사용되는 프로토콜입니다. CC-SG가 NTP로 구성된 경우 CC-SG는 공개적으로 사용 가능한 NTP 참조 서버와 해당 시간을 동기화하여 정확하고 일정한 시간을 유지할 수 있습니다.

3. 구성 업데이트를 클릭하여 CC-SG에 시간 및 날짜 변경 사항을 적용합니다.
4. 새로 고침을 클릭하여 현재 시간 필드에 새 서버 시간을 다시 로드합니다.
5. 시스템 정비 > 다시 시작을 선택하여 CC-SG를 다시 시작합니다.

연결 모드: 직접 및 프록시

연결 모드 정보

CC-SG는 대역내 및 대역외 연결을 위해 세 가지 연결 모드를 제공합니다. 직접, 프록시 및 둘 모두

- 직접 모드에서 CC-SG를 통해 데이터를 전달하지 않고 직접 노드나 포트에 연결할 수 있습니다. 직접 모드는 일반적으로 더 빠른 연결을 제공합니다.
- 프록시 모드에서 CC-SG를 통해 데이터를 전달하여 노드나 포트에 연결할 수 있습니다. 프록시 모드는 CC-SG 서버에 부하를 증가시켜 연결이 느려질 수 있습니다. 그러나 연결의 보안을 더 고려할 경우 프록시 모드가 권장됩니다. CC-SG TCP 포트(80, 443 및 2400)만 방화벽에서 열어 놓아야 합니다. 프록시 모드는 AES가 KXII 장치에서 활성화된 경우 KVM 데이터에 대해 CC-SG와 KXII 장치 사이에 SSL을 사용하지 않습니다.
- 두 모드 모두에서 직접 모드와 프록시 모드를 조합하여 CC-SG를 구성할 수 있습니다. 두 모드 모두에서 프록시 모드가 기본이지만 지정된 범위에서 클라이언트 IP 주소를 사용하여 연결한 경우 직접 모드를 사용하도록 CC-SG를 구성할 수 있습니다.

중요: CC-SG가 프록시 모드 또는 둘 모두 모드에 있을 경우

사용자에게 가상 매체에 액세스 권한을 부여할 수 없습니다.

모든 클라이언트 연결에 대해 직접 모드 구성

▶ 모든 클라이언트 연결에 대해 직접 모드를 구성하려면:

1. 관리 > 구성을 선택합니다.
2. 연결 모드 탭을 클릭합니다.
3. 직접 모드를 선택합니다.
4. 구성 업데이트를 클릭합니다.

모든 클라이언트 연결에 대해 프록시 모드 구성

▶ 모든 클라이언트 연결에 대해 프록시 모드를 구성하려면:

1. 관리 > 구성을 선택합니다.
2. 연결 모드 탭을 클릭합니다.
3. 프록시 모드를 선택합니다.
4. 구성 업데이트를 클릭합니다.

직접 모드 또는 프록시 모드의 조합 구성

직접 모드와 프록시 모드의 조합을 사용하도록 CC-SG 를 구성할 경우 프록시 모드가 기본 연결 모드가 되며 직접 모드는 지정한 클라이언트 IP 주소에 대해 사용됩니다.

▶ 직접 모드 또는 프록시 모드의 조합을 구성하려면:

1. 관리 > 구성을 선택합니다.
2. 연결 모드 탭을 클릭합니다.
3. 둘 모두를 선택합니다.
4. 넷 주소 및 넷 마스크 필드에서 직접 모드를 통해 노드 및 포트에 연결해야 하는 클라이언트 IP 주소 범위를 지정한 다음 추가를 클릭합니다.
5. 구성 업데이트를 클릭합니다.

장치 설정

모든 장치에 적용할 일부 설정을 구성하고 각 장치 유형의 기본 포트 번호를 구성할 수 있습니다.

▶ 장치에 대한 기본 포트 번호를 구성하려면:

1. 관리 > 구성을 선택합니다.
2. 장치 설정 탭을 클릭합니다.
3. 표에서 장치 유형을 선택하고 기본 포트 값을 더블 클릭합니다.
4. 새 기본 포트 값을 입력합니다.
5. 구성 업데이트를 클릭하여 변경 사항을 저장합니다.

▶ 장치의 시간 제한 기간을 구성하려면:

1. 관리 > 구성을 선택합니다.
2. 장치 설정 탭을 클릭합니다.
3. 하트비트(초) 필드에 새 시간 제한 기간을 입력합니다. 올바른 범위는 30 초에서 50,000 초입니다.
4. 구성 업데이트를 클릭하여 변경 사항을 저장합니다.

▶ 모든 전원 작업에 대해 경고 메시지를 활성화 또는 비활성화하려면:

요청된 전원 작업이 발생하기 전에 사용자에게 경고하는 경고 메시지를 활성화하려면 모든 전원 작업에 경고 메시지 표시 확인란을 선택합니다. 전원 작업을 실행한 사용자만 메시지를 볼 수 있습니다. 사용자는 메시지에서 예 또는 아니오를 클릭하여 전원 작업을 취소하거나 확인할 수 있습니다.

1. 관리 > 구성을 선택합니다.
2. 장치 설정 탭을 클릭합니다.
3. 경고 메시지를 활성화하려면 모든 전원 작업에 경고 메시지 표시 확인란을 선택합니다. 경고 메시지를 비활성화하려면 확인란을 선택 취소합니다.
4. 구성 업데이트를 클릭하여 변경 사항을 저장합니다.

사용자 정의 JRE 설정 구성

CC-SG 는 CC-SG 에 액세스를 시도하는 사용자가 지정한 최소 JRE 버전이 없는 경우 경고 메시지를 표시합니다. JRE 의 최소 지원 버전에 대해서는 호환성 매트릭스를 확인합니다. 관리 > 호환성 매트릭스를 선택합니다.

CC-SG 에 로그인을 시도하는 사용자가 지정된 JRE 버전을 설치하지 않은 경우 JRE 비호환성 경고 창이 열립니다. 이 창에는 기본적인 최소 JRE 버전을 다운로드하기 위한 여러 옵션이 있습니다. 다운로드 옵션에 텍스트 및 링크를 포함하여 메시지를 변경할 수 있습니다. 사용자는 새 버전의 JRE 를 다운로드하거나 현재 설치된 JRE 버전으로 CC-SG 에 계속 액세스할 수 있습니다.

▶ 로그인을 위한 사용자 정의 JRE 를 활성화 또는 비활성화하려면:

1. 이 기능을 활성화 또는 비활성화하기 전에 CC-SG 를 백업하고 백업 파일을 원격 위치로 저장합니다. **CC-SG 백업** (p. 163) 을 참조하십시오.
2. 관리 > 구성을 선택합니다.
3. 사용자 JRE 탭을 클릭합니다.
4. 옵션을 활성화하려면 로그인을 위해 사용자 정의 JRE 활성화 확인란을 선택합니다. 옵션을 비활성화하려면 확인란을 선택 취소합니다.
5. 최소 JRE 필요 필드에 필요한 최소 JRE 버전을 입력합니다. 최소 3 개의 부분을 포함한 전체 버전 번호를 입력해야 합니다. 예를 들어, 1.6.0 은 올바른 버전 번호입니다. 1.6 은 올바르지 않은 버전 번호입니다. JRE "업데이트" 버전의 경우 밑줄 문자를 사용하십시오. 예를 들어, 1.6.0_5 은 JRE 버전 1.6.0 업데이트 5 에 대한 올바른 버전 번호입니다.
6. 업데이트를 클릭합니다.

▶ JRE 비호환성 경고 창의 메시지를 사용자 정의하려면:

1. 관리 > 구성을 선택합니다.
2. 사용자 JRE 탭을 클릭합니다.
3. HTML 코드를 이용하여 JRE 비호환성 경고 창에 표시할 메시지를 입력합니다.
4. 업데이트를 클릭합니다.

▶ 기본 메시지 및 최소 JRE 버전을 복원하려면:

1. 관리 > 구성을 선택합니다.
2. 사용자 JRE 탭을 클릭합니다.
3. 기본값 복원을 클릭합니다.
4. 업데이트를 클릭합니다.

▶ 기본 메시지 및 최소 JRE 버전을 지우려면:

1. 관리 > 구성을 선택합니다. 사용자 JRE 탭을 클릭합니다.
2. 지우기를 클릭합니다.

SNMP 구성

SNMP(Simple Network Management Protocol)를 사용하여 CC-SG 는 SNMP 트랩(이벤트 통지)을 네트워크의 기존 SNMP 관리자로 보낼 수 있습니다. CC-SG 가 SNMP 와 함께 작동하도록 구성하려면 SNMP 인프라 처리 교육을 받아야 합니다.

또한 CC-SG 는 HP OpenView 와 같은 타사 솔루션을 사용하여 SNMP GET/SET 작업을 지원합니다. 조작을 지원하려면 sysContact, sysName 및 sysLocation 등의 MIB-II System Group 개체와 같은 SNMP 에이전트 ID 정보를 제공해야 합니다. 이 ID 는 관리 노드에 대한 연락처, 관리 및 위치 정보를 제공합니다. 자세한 내용은 RFC 1213 을 참조하십시오.

▶ CC-SG 에서 SNMP 를 구성하려면:

1. 관리 > 구성을 선택합니다.
2. SNMP 탭을 클릭합니다.
3. SNMP 작동을 활성화하려면 SNMP 데몬 활성화 확인란을 선택합니다.
4. CC-SG 에서 실행하는 SNMP 에이전트를 타사 엔터프라이즈 관리 솔루션과 구분하기 위해 에이전트 구성 아래에 에이전트 정보를 제공합니다. 에이전트의 포트를 입력합니다(기본값: 161). 읽기 전용 커뮤니티 문자열(기본값: public) 및 읽기-쓰기 커뮤니티 문자열(기본값: private)을 입력합니다. 여러 개의 커뮤니티 문자열이 허용되며 쉼표로 구분됩니다. 시스템 담당자, 시스템 이름 및 시스템 위치를 입력하여 관리 노드에 대한 정보를 제공합니다.
5. 에이전트 구성 업데이트를 클릭하여 변경 사항을 저장합니다.

6. SNMP 트랩 활성화 확인란을 선택하여 CC-SG 에서 SNMP 호스트로 SNMP 트랩 보내기를 활성화합니다.
7. CC-SG 가 SNMP 호스트에게 보내도록 하려는 트랩 앞의 확인란을 선택합니다. 트랩 소스 아래에는 SNMP 트랩 목록이 다음과 같은 두 개의 다른 범주로 그룹화됩니다. 하드 디스크 오류와 같은 CC 장치의 상태에 대한 통지를 포함하는 시스템 로그 트랩 및 사용자 계정 수정과 같이 CC 애플리케이션의 이벤트가 생성한 통지용 애플리케이션 로그 트랩 유형별로 트랩을 활성화하려면 시스템 로그 및 애플리케이션 로그로 표시된 상자를 선택합니다. 확인란을 선택하여 개별 트랩을 활성화 또는 비활성화할 수 있습니다. 모든 트랩을 활성화하려면 모두 선택 및 모두 지우기를 사용하고 그렇지 않으면 모든 확인란을 선택 취소합니다. 제공되는 SNMP 트랩 목록은 MIB 파일을 참조하십시오. 자세한 내용은 MIB 파일을 참조하십시오.
8. 트랩 대상 패널에서 SNMP 호스트가 사용하는 트랩 대상 호스트 IP 주소 및 포트 번호를 입력합니다. 기본 포트는 162 입니다.
9. 트랩 대상 패널에서 SNMP 호스트가 사용하는 커뮤니티 문자열 및 버전(v1 또는 v2)을 입력합니다.
10. 추가를 클릭하여 대상 호스트를 구성된 호스트 목록에 추가합니다. 이 목록에 설정할 수 있는 관리자의 수에는 제한이 없습니다.
11. 트랩 구성 업데이트를 클릭하여 변경 사항을 저장합니다.

MIB 파일

CC-SG가 일련의 자체적인 Raritan 트랩을 보내기 때문에 Raritan SNMP 트랩 정의를 포함하는 사용자 정의 MIB 파일을 사용하여 모든 SNMP를 업데이트해야 합니다. **SNMP 트랩** (p. 279)을 참조하십시오. 사용자 정의 MIB 파일은 Raritan 지원 웹 사이트에서 찾을 수 있습니다.

CC-SG 클러스터 구성

CC-SG 클러스터란 무엇입니까?

CC-SG 클러스터는 기본 노드가 실패하는 경우 백업 보안을 위해 두 가지 CC-SG 노드, 즉 기본 노드와 보조 노드를 사용합니다. 이 두 가지 노드는 활성 사용자와 활성 연결의 공통 데이터를 공유하며 두 노드 사이의 모든 상태 데이터가 복사됩니다.

CC-SG 클러스터의 장치는 기본 노드에게 상태 변경 이벤트를 알릴 수 있도록 기본 CC-SG 노드의 IP 를 알고 있어야 합니다. 기본 노드가 중지되면 보조 노드가 즉시 기본 노드의 모든 기능을 수행하게 됩니다. 이를 위해서는 CC-SG 애플리케이션과 사용자 세션(기본 CC-SG 노드에서 유래한 기존의 모든 세션은 종료됨)이 초기화되어야 합니다. 기본 노드에 연결된 장치는 기본 노드가 응답하지 않고 보조 노드의 요청에 응답한다는 것을 알게 됩니다.

CC-SG 클러스터의 요구 사항

- 클러스터의 기본 노드와 보조 노드는 동일한 버전의 하드웨어(V1 또는 E1)에서 동일한 버전의 펌웨어를 실행하고 있어야 합니다.
- CC-SG 네트워크는 클러스터링을 위해 사용하려면 기본/백업 모드에 있어야 합니다. 클러스터링은 활성/활성 구성과 상호 작용하지 않습니다. **About Network 네트워크 설정 정보** ("네트워크 설정 정보" p. 179)를 참조하십시오.
- 날짜, 시간 및 시간대 설정은 기본 노드에서 보조 노드로 복제되지 않습니다. 클러스터를 생성하기 전에 이러한 설정을 각 CC-SG 에 구성해야 합니다.

CC-SG 클러스터 및 CC-NOC 정보

클러스터 구성에서 기본 노드만 CC-NOC 와 통신합니다. CC-SG 는 기본 노드가 될 때마다 해당 IP 주소 및 보조 노드의 IP 주소를 CC-NOC 에 전송합니다.

클러스터 생성

장애 복구 시 관리자가 모든 **CC-SG** 사용자에게 이메일을 전송하여 새 기본 **CC-SG** 노드의 IP 주소를 사용할 것을 통지합니다.

기본 노드와 보조 노드 간의 통신이 끊기면 보조 노드가 기본 노드의 역할을 수행합니다. 연결이 재개되면 두 개의 기본 노드를 가질 수 있습니다. 그러면 기본 노드를 제거하고 보조 노드로 재설정해야 합니다.

중요: 클러스터를 생성하기 전에 두 개의 **CC-SG** 장치 모두에 대한 구성을 백업해야 합니다.

▶ 1. 기본 **CC-SG** 노드 설정:

1. 관리 > 클러스터 구성을 선택합니다.
2. **CommandCenters** 찾기를 클릭하여 현재 사용 중인 것과 동일한 하위 세트에서 모든 **CC-SG** 어플라이언스를 검색하여 표시합니다. 또는 창 맨 아래의 **CommandCenter** 주소에서 IP 주소를 지정하고 **CommandCenter** 추가를 클릭하여 다른 서브넷으로부터 **CC-SG** 를 추가할 수 있습니다.
3. 이 클러스터의 이름을 클러스터 이름 필드에 입력합니다. 지금 이름을 제공하지 않으면 클러스터를 생성할 때 **cluster192.168.51.124** 와 같은 기본 이름이 제공됩니다.
4. 클러스터 생성을 클릭합니다. 메시지가 나타납니다.
5. 예를 클릭합니다. 현재 사용 중인 **CC-SG** 가 기본 노드가 됩니다.

▶ 2. 보조 **CC-SG** 노드 설정:

1. **CommandCenters** 찾기를 클릭하여 현재 사용 중인 것과 동일한 하위 세트에서 모든 **CC-SG** 어플라이언스를 검색하여 표시합니다. 또는 창 맨 아래의 **CommandCenter** 주소에서 IP 주소를 지정하여 다른 서브넷으로부터 **CC-SG** 를 추가할 수 있습니다. **CommandCenter** 추가를 클릭합니다.
2. 보조 노드 또는 백업 **CC-SG** 노드를 추가하려면 클러스터 구성 표에서 독립형 상태의 **CC-SG** 장치를 선택합니다. 버전 번호가 기본 노드의 버전과 일치해야 합니다.
3. 백업 사용자 이름 및 암호 필드에 백업 노드의 올바른 사용자 이름 및 암호를 입력합니다.
4. "백업" 노드 조인을 클릭합니다.
5. 확인 메시지가 나타납니다. 예를 클릭하여 선택한 노드에 보조 상태를 지정합니다.

중요: 조인 프로세스를 시작하면 조인 프로세스가 완료될 때까지 CC-SG의 다른 기능을 수행하지 마십시오.

6. 새로 선택한 보조 노드가 다시 시작됩니다. 이 프로세스는 몇 분이 걸립니다. 다시 시작이 완료되면 확인 메시지가 표시됩니다.
7. 업데이트된 클러스터 구성 표를 보려면 관리 > 클러스터 구성을 선택합니다.

보조 CC-SG 노드 제거

보조 또는 백업 노드를 제거하면 보조 노드의 지정을 제거합니다. 구성에서 보조 CC-SG 장치는 삭제되지 않습니다.

▶ CC-SG 장치에서 보조 노드 상태를 제거하려면:

1. 클러스터 구성 표에서 보조 CC-SG 노드를 선택합니다.
2. "백업" 노드 제거를 클릭합니다.
3. 예를 클릭하여 보조 노드 상태를 제거합니다.

기본 CC-SG 노드 제거

클러스터 삭제를 클릭해도 구성에서 기본 CC-SG 장치가 삭제되지 않으며 기본 노드의 지정만 제거됩니다. 백업 노드가 없을 경우에만 클러스터 삭제를 사용할 수 있습니다.

▶ CC-SG 장치에서 기본 노드 상태를 제거하려면:

1. 클러스터 구성 표에서 기본 CC-SG 노드를 선택합니다.
2. 클러스터 제거를 클릭합니다.
3. 예를 클릭하여 기본 노드 상태를 제거합니다.

실패한 CC-SG 노드 복구

노드가 실패하고 장애 복구가 시작되면 실패한 노드가 대기 상태로 복구됩니다. 노드가 대기 상태가 되면 독립형 모드 또는 백업 모드에서 시작할 수 있습니다.

▶ 실패한 CC-SG 노드를 복구하려면:

1. 클러스터 구성 표에서 대기 노드를 선택합니다.
2. "대기" 노드 조인을 클릭하여 해당 노드를 백업 노드로 추가합니다.

3. 확인 메시지가 나타납니다. 예를 클릭하여 선택한 노드에 보조 상태를 지정합니다.
4. 보조 노드가 다시 시작됩니다. 이 프로세스는 몇 분이 걸립니다. 다시 시작이 완료되면 확인 메시지가 표시됩니다.

고급 클러스터 설정

클러스터 구성에서는 시간대를 변경할 수 없습니다.

▶ **고급 클러스터 설정을 구성하려면:**

1. 기본 노드를 선택합니다.
2. 고급을 클릭합니다. 고급 설정 창이 열립니다.
3. 시간 간격의 경우, **CC-SG** 가 다른 노드와의 연결을 확인하는 빈도를 입력합니다.

참고: 시간 간격을 짧게 설정하면 하트비트 확인으로 생성된 네트워크 트래픽이 증가합니다. 서로 멀리 떨어진 노드가 있는 클러스터를 보다 높은 시간 간격으로 설정할 수도 있습니다.

4. 오류 임계값의 경우, **CC-SG** 노드의 오류가 밝혀지기 전에 응답하지 않고 통과해야 하는 연속적인 하트비트의 수를 입력해야 합니다.
5. 복구 시간의 경우, 실패한 연결이 복구된 것으로 간주되기 전에 성공적으로 반환되어야 하는 연속적인 하트비트의 수를 입력합니다.
6. 확인을 클릭하여 변경 사항을 저장합니다.

보안 관리자

보안 관리자는 **CC-SG** 가 사용자에게 액세스를 제공하는 방법을 관리하는 데 사용됩니다. 보안 관리자에서 인증 방법, **SSL** 액세스, **AES** 암호화, 강력한 암호 규칙, 잠금 규칙, 로그인 포털, 인증서 및 액세스 제어 목록을 구성할 수 있습니다.

원격 인증

원격 인증 서버를 구성하는 방법에 대한 자세한 지침은 **원격 인증** (p. 128)을 참조하십시오.

AES 암호화

클라이언트와 CC-SG 서버 사이에 AES 128 암호화가 필요하도록 CC-SG 를 구성할 수 있습니다. AES 암호화가 필요할 경우 모든 사용자는 AES 사용 클라이언트를 사용하여 CC-SG 에 액세스해야 합니다. AES 암호화가 필요하고 비 AES 브라우저를 이용하여 CC-SG 를 액세스하려는 경우 CC-SG 에 연결할 수 없게 됩니다.

브라우저의 AES 암호화 확인

브라우저가 AES 를 사용하는지 알 수 없는 경우 브라우저 제조업체에게 확인하십시오.

확인하고자 하는 암호화가 지원되는 브라우저를 사용하여 다음 웹 사이트에서 탐색을 시도할 수도 있습니다.

<https://www.fortify.net/sslcheck.html>

<https://www.fortify.net/sslcheck.html>. 이 웹 사이트는 브라우저의 암호화 방법을 탐지하여 보고서를 표시합니다. Raritan은 이러한 웹 사이트와 아무 관계도 없습니다.

클라이언트와 CC-SG 사이에 AES 암호화가 필요합니다.

보안 관리자에서 클라이언트와 CC-SG 서버 사이에 AES 암호화가 필요하도록 CC-SG 를 구성할 수 있습니다.

1. 관리 > 보안을 선택합니다.
2. 암호화 탭을 엽니다.
3. 클라이언트와 서버 간 AES 암호화 필요 확인란을 선택합니다.
4. 이 옵션이 선택되면 클라이언트가 CC-SG 에 연결하기 위해 AES 암호화가 필요하다는 경고 메시지가 표시됩니다. 확인을 클릭하여 확인합니다.
 - 키 길이 필드는 128 을 표시하며 클라이언트와 CC-SG 서버 사이에는 128 비트 암호화가 필요합니다.
 - 브라우저 연결 프로토콜 필드는 선택된 HTTPS/SSL 을 표시합니다.
5. 업데이트를 클릭하여 변경 사항을 저장합니다.

브라우저 연결 프로토콜 구성: HTTP 또는 HTTPS/SSL

보안 관리자에서 클라이언트로부터의 정규 HTTP 연결을 사용하거나 HTTPS/SSL 연결을 요구하기 위해 CC-SG 를 구성할 수 있습니다. 이 설정의 변경 사항을 적용하려면 CC-SG 를 다시 시작해야 합니다.

▶ 브라우저 연결 프로토콜을 구성하려면:

1. 관리 > 보안을 선택합니다.
2. 암호화 탭을 엽니다.
3. HTTP 또는 HTTPS/SSL 옵션을 선택하여 CC-SG 에 연결할 때 클라이언트에서 사용할 브라우저 연결 프로토콜을 지정합니다.
4. 업데이트를 클릭하여 변경 사항을 저장합니다.

CC-SG에 SSH 액세스를 위한 포트 번호 설정

보안 관리자에서 CC-SG에 대한 SSH 액세스를 위해 사용할 포트 번호를 설정할 수 있습니다. **CC-SG에 대한 SSH 액세스** (p. 219)를 참조하십시오.

▶ CC-SG 에 대한 SSH 액세스를 위한 포트 번호를 설정하려면:

1. 관리 > 보안을 선택합니다.
2. 암호화 탭에서 SSH 서버 포트 필드에 SSH 를 통해 CC-SG 에 액세스하기 위한 포트 번호를 입력합니다.
3. 업데이트를 클릭하여 변경 사항을 저장합니다.

로그인 설정

로그인 설정 탭에서 강력한 암호 설정 및 잠금 설정을 구성할 수 있습니다.

로그인 설정 보기

1. 관리 > 보안을 선택합니다.
2. 로그인 설정 탭을 클릭합니다.

모든 사용자에게 강력한 암호가 필요함

1. 관리 > 보안을 선택합니다.
2. 로그인 설정 탭을 클릭합니다.
3. 모든 사용자에게 강력한 암호 필요 확인란을 선택합니다.

4. 최대 암호 길이를 선택합니다. 암호는 최대 문자 수보다 적어야 합니다.
5. 암호 기록 수준을 선택합니다. 숫자는 기록에 남아 있어 재사용할 수 없는 이전 암호 수를 지정합니다. 예를 들어, 암호 기록 수준이 5로 설정된 경우 사용자는 이전 5개의 암호를 다시 사용할 수 없습니다.
6. 암호 만료 빈도를 선택합니다. 모든 암호는 설정된 일 수 이후에 만료됩니다. 암호가 만료된 후 사용자는 다음에 로그인할 때 새 암호를 선택해야 합니다.
7. 강력한 암호 요구사항 선택:
 - 암호에는 한 개 이상의 소문자가 포함되어야 합니다.
 - 암호에는 한 개 이상의 대문자가 포함되어야 합니다.
 - 암호에 한 개 이상의 숫자가 포함되어야 합니다.
 - 암호는 한 개 이상의 특수 문자(예: 느낌표 또는 앰퍼샌드)를 포함해야 합니다.
8. 업데이트를 클릭하여 변경 사항을 저장합니다.

CC-SG 암호 정보

모든 암호는 관리자가 구성하는 모든 기준을 만족해야 합니다. 강력한 암호 규칙을 구성한 후 향후 모든 암호는 이 기준을 만족해야 합니다. 새 기준이 이전 기준보다 더 강력할 경우 모든 기존 사용자는 다음 로그인 시에 암호를 변경해야 합니다. 강력한 암호 규칙은 로컬에 저장된 사용자 프로필에만 적용됩니다. 인증 서버의 암호 규칙은 인증 서버에서 관리해야 합니다.

또한 사용자 이름 및 암호에서 4개의 인접 문자는 일치할 수 없습니다.

강력한 암호 규칙은 사용자가 암호를 만들 때 엄격한 지침을 따라야 하므로 암호를 짐작하는 것을 더욱 어렵게 함으로써 더욱 더 안전을 기할 수 있습니다. 기본적으로 강력한 암호는 CC-SG에서 활성화되지 않습니다. 모든 강력한 암호 매개변수를 포함하는 강력한 암호는 CC 수퍼 사용자에게 항상 요구됩니다.

강력한 암호 규칙의 변경 시기와 새 기준 정보에 대한 고급 통지를 사용자에게 제공하기 위해 오늘의 메시지 기능을 사용할 수 있습니다.

잠금 설정

지정된 횟수의 로그인 시도에 실패하면 관리자가 CC-SG, CC-NOC 사용자 및 SSH 사용자를 잠글 수 있습니다. 로컬 인증된 사용자, 원격 인증된 사용자 또는 모든 사용자에게 이 기능을 활성화할 수 있습니다.

참고: 기본적으로 로그인 시도에 3 번 실패하면 5 분 동안 admin 계정이 잠깁니다. admin 의 경우 잠금 전후의 로그인 시도 실패 횟수를 구성할 수 없습니다.

▶ 잠금을 활성화하려면:

1. 관리 > 보안을 선택합니다.
2. 로그인 설정 탭을 클릭합니다.
3. 로컬 인증 사용자에게 대한 잠금을 활성화하기 위해 로컬 사용자의 잠금 활성화 확인란을 선택합니다. 원격 인증 사용자에게 대한 잠금을 활성화하기 위해 원격 사용자의 잠금 활성화 확인란을 선택합니다.
4. 시도한 로그인 실패 횟수가 세 번이면 사용자가 잠깁니다. 1 에서 10 까지 숫자를 입력하여 이 값을 변경할 수 있습니다.
5. 잠금 전략을 선택합니다.
 - 일정 기간 동안 잠금 사용자가 다시 로그인할 수 있을 때까지 잠기는 시간(분)을 지정합니다. 기본 숫자는 5 분입니다. 1 분에서 1440 분(24 시간)까지 기간을 지정할 수 있습니다. 기간이 만료되면 사용자가 다시 로그인할 수 있습니다. 잠금 기간 중 언제라도 관리자가 이 값을 덮어쓰고 사용자가 CC-SG 로 다시 로그인하도록 허용할 수 있습니다.
 - 관리자가 액세스를 허용할 때까지 잠금: 사용자는 관리자가 사용자 계정을 잠금 해제할 때까지 잠깁니다.
6. 잠금 통지 이메일 필드에 이메일 주소를 입력합니다. 잠금이 발생할 때 이 이메일 주소로 통지가 전송됩니다. 필드가 비어 있으면 통지가 전송되지 않습니다. **옵션입니다.**
7. 관리자의 전화 번호 필드에 전화 번호를 입력합니다. 전화 번호는 잠금이 발생할 때 전송되는 통지 이메일에 표시됩니다. **옵션입니다.**
8. 업데이트를 클릭하여 변경 사항을 저장합니다.

▶ 잠금을 비활성화하려면:

잠금을 비활성화할 경우 현재 CC-SG 에 잠겨 있는 모든 사용자가 로그인할 수 있습니다.

1. 관리 > 보안을 선택합니다.
2. 로그인 설정 탭을 엽니다.
3. 로컬 인증 사용자에게 대한 잠금을 비활성화하기 위해 로컬 사용자의 잠금 활성화 확인란을 선택 취소합니다. 원격 인증 사용자에게 대한 잠금을 비활성화하기 위해 원격 사용자의 잠금 활성화 확인란을 선택 취소합니다.
4. 업데이트를 클릭하여 변경 사항을 저장합니다.

사용자 이름당 동시 로그인 허용

동일한 사용자 이름으로 CC-SG 에서 둘 이상의 동시 세션을 허용합니다.

1. 관리 > 보안을 선택합니다.
2. 로그인 설정 탭을 클릭합니다.
 - CC 슈퍼 사용자 계정에 대해 둘 이상의 동시 로그인을 허용하려면 슈퍼 사용자 확인란을 선택합니다.
 - 시스템 관리자 사용자 그룹의 사용자에게 의한 동시 로그인을 허용하려면 시스템 관리자 확인란을 선택합니다.
 - 다른 모든 사용자에게 의한 동시 로그인을 허용하려면 다른 사용자 확인란을 선택합니다.
3. 업데이트를 클릭하여 변경 사항을 저장합니다.

비활동 타이머 구성

비활동 타이머를 구성하여 CC-SG 에서 사용자가 잠기게 되는 CC-SG 세션의 비활동 시간을 지정할 수 있습니다.

사용자가 열려진 노드에 연결한 경우 세션은 활동으로 간주되며 사용자는 비활동 타이머가 만료될 때 잠기지 않습니다.

▶ 비활동 타이머를 구성하려면:

1. 관리 > 보안 선택
2. 로그인 설정 탭을 클릭합니다.
3. 비활동 타이머 필드에 원하는 시간 한도를 입력합니다.

- 업데이트를 클릭하여 변경 사항을 저장합니다.

초기 화면

관리자는 포털 설정을 사용하여 사용자가 CC-SG에 액세스할 때 환영하는 로고 및 액세스 계약을 구성할 수 있습니다.

▶ 포털 설정에 액세스하려면:

- 관리 > 보안을 선택합니다.
- 포털 탭을 엽니다.

로고

로그인 페이지에서 배너 역할을 할 작은 그래픽 파일을 CC-SG에 업로드할 수 있습니다. 로고의 최대 크기는 998 x 170 픽셀입니다.

▶ 로고를 업로드하려면:

- 포털 탭의 로고 영역에서 찾아보기를 클릭합니다. 열기 대화 상자가 나타납니다.
- 대화 상자에서 로고로 사용할 그래픽 파일을 선택하고 열기를 클릭합니다.
- 로고를 미리 보려면 미리 보기를 클릭합니다. 선택한 그래픽 파일이 오른쪽에 나타납니다.
- 업데이트를 클릭하여 변경 사항을 저장합니다.

제한된 서비스 계약

로그인 화면에 있는 로그인 필드의 왼쪽에 메시지가 나타나도록 구성할 수 있습니다. 이 메시지는 제한된 서비스 계약으로 사용하거나 사용자가 CC-SG에 액세스하는 것을 동의함을 나타냅니다. 로그 파일 및 감사 추적 보고서에 사용자가 제한된 서비스 계약을 승인했다는 내용이 언급되어 있습니다.

▶ 제한된 서비스 계약을 CC-SG 로그인 화면에 추가하려면:

- 사용자가 로그인 정보를 입력하기 전에 로그인 화면의 계약 상자를 선택하도록 하려면 제한된 서비스 계약의 승인 필요 확인란을 선택합니다.
- 메시지를 입력합니다.
 - 배너 텍스트를 직접 입력하려면 제한된 서비스 계약 메시지를 선택합니다.

- 제공된 텍스트 필드에 계약 메시지를 입력합니다. 텍스트 메시지의 최대 길이는 10,000 자입니다.
 - 글꼴 드롭다운 메뉴를 클릭하고 메시지의 글꼴을 선택합니다.
 - 크기 드롭다운 메뉴를 클릭하여 메시지의 글꼴 크기를 선택합니다.
- b. 텍스트(.TXT) 파일에서 메시지를 로드하려면 제한된 서비스 계약 메시지 파일을 선택합니다.
- 찾아보기를 클릭합니다. 대화 창이 열립니다.
 - 대화 창에서 사용할 메시지가 있는 텍스트 파일을 선택하고 열기를 클릭합니다. 텍스트 메시지의 최대 길이는 10,000 자입니다.
 - 미리 보기를 클릭하여 파일에 포함된 텍스트의 미리 보기를 수행합니다. 위의 배너 메시지 필드에 미리 보기가 나타납니다.
3. 업데이트를 클릭하여 변경 사항을 저장합니다. 업데이트는 다음에 사용자가 CC-SG 에 액세스할 때 로그인 화면에 표시됩니다.

인증서

인증서 탭에서 디지털 ID 인증서를 신청하거나, 자체 서명 인증서를 생성하거나, 인증서 및 그 개인 키의 가져오기 및 내보내기를 수행하기 위해 전송되는 인증서 서명 요청(CSR)을 생성할 수 있습니다.

인증서 작업

참고: 화면 맨 아래의 버튼은 선택한 인증서 옵션에 따라 내보내기에서 가져오기로, 다시 생성으로 변경됩니다.

▶ 현재 인증서 및 개인 키를 내보내기하려면:

1. 관리 > 보안을 선택합니다.
2. 인증서 탭을 클릭합니다.
3. 현재 인증서 및 개인 키 내보내기를 선택합니다.
4. 내보내기를 클릭합니다. 인증서 패널에 인증서가 나타나고 개인 키 패널에 개인 키가 나타납니다..
5. 각 패널에서 텍스트를 선택하고 **Ctrl+C** 를 눌러 복사합니다. 그런 다음 텍스트를 필요한 곳에 붙여넣을 수 있습니다.

▶ **인증서 서명 요청을 생성하고 붙여넣기된 인증서 및 개인 키를 가져오려면:**

CSR 은 서명 인증서를 발행할 인증 서버에 제출됩니다. 루트 인증서도 인증 서버에서 내보내져 파일로 저장됩니다. 인증 서명 기관에서 서명 인증서를 수신하면 서명 인증서, 루트 인증서 및 개인 키를 가져올 수 있습니다.

1. 관리 > 보안을 선택합니다.
2. 인증서 탭을 클릭합니다.
3. 인증서 서명 요청 생성을 클릭하고 생성을 클릭합니다. 인증서 서명 요청 생성 창이 열립니다.
4. 요청된 데이터를 필드에 입력합니다.
 - a. 암호화 모드: 클라이언트와 서버 간 AES 암호화 필요가 관리 >보안> 암호화에서 선택된 경우 AES-128 이 기본입니다. AES 가 필요하지 않을 경우 3DES 가 기본입니다.
 - b. 개인 키 길이: 기본값은 1024 입니다.
 - c. 유효 기간(일): 최대 4 자리 숫자입니다.
 - d. 국가 코드: CSR 태그는 국가 이름입니다.
 - e. 시/도: 최대 64 문자입니다. 전체 주 또는 지역 이름을 입력합니다. 약어를 사용하지 마십시오.
 - f. 도시/지역: CSR 태그는 지역 이름입니다. 최대 64 문자입니다.
 - g. 등록된 회사 이름: CSR 태그는 조직 이름입니다. 최대 64 문자입니다.
 - h. 부서/조직 이름: CSR 태그는 조직 단위 이름입니다. 최대 64 문자입니다.
 - i. 정규화된 도메인 이름: CSR 태그는 공통 이름입니다. 등록된 회사 이름은 CSR 에 대한 도메인 이름을 소유해야 합니다. 이 서명 서비스는 등록된 회사가 도메인 이름을 소유하고 있지 않을 경우 요청을 거부합니다.
 - j. 챌린지 암호: 최대 64 문자입니다.
 - k. 관리자 이메일 주소: 인증서 요청에 책임을 맡고 있는 관리자의 이메일 주소를 입력합니다.
5. CSR 을 생성하려면 확인을 클릭합니다. CSR 및 개인 키가 인증서 화면의 해당 필드에 나타납니다.
6. 인증서 요청 상자에서 텍스트를 선택한 다음 Ctrl+C 를 눌러 복사합니다. 메모장과 같은 ASCII 편집기를 사용하여 CSR 을 파일에 붙여넣고 .cer 확장자로 저장합니다.

7. 개인 키 상자에서 텍스트를 선택한 다음 **Ctrl+C** 를 눌러 복사합니다. 메모장과 같은 **ASCII** 편집기를 사용하여 개인 키를 파일에 붙여넣고 **.txt** 확장자로 저장합니다.
8. 서명 인증서를 받기 위해 **.cer** 파일을 인증 서버에 제출합니다.
9. 인증 서버에서 루트 인증서를 다운로드하거나 내보내고 **.cer** 확장자의 파일에 저장합니다. 이것은 다음 단계에서 인증 서버에서 발행할 서명 인증서와는 다릅니다.
10. **CA** 파일 옆의 찾아보기를 클릭하고 루트 인증서 파일을 선택합니다.
11. 인증 서버에서 서명 인증서를 수신하면 붙여넣은 인증서 및 개인 키 가져오기를 선택합니다.
12. 서명 인증서의 텍스트를 복사한 다음 **Ctrl+V** 를 눌러 인증서 상자로 붙여넣습니다.
13. 이전에 **.txt** 파일로 저장된 개인 키의 텍스트를 복사한 다음 **Ctrl+V** 를 눌러 개인 키 상자로 붙여넣습니다.
14. **CSR** 이 **CC-SG** 에 의해 생성된 경우 암호 필드에서 **raritan** 를 입력합니다. 다른 애플리케이션에서 **CSR** 을 생성했으면 해당 애플리케이션에 대해 해당 암호를 사용합니다.

*참고: 가져온 인증서를 루트 및 하위 루트 **CA**(인증 기관)에서 서명하는 경우 루트 또는 하위 루트 인증서만 사용할 수 없습니다. 이 문제를 해결하려면 루트와 하위 루트 인증서를 모두 하나의 파일에 복사하여 붙여넣은 다음 가져옵니다.*

▶ **자체 서명 인증서 요청을 생성하려면:**

1. 관리 > 보안을 선택합니다.
2. 인증서 탭을 클릭합니다.
3. 자체 서명 인증서 생성을 선택한 다음 생성을 클릭합니다. 자체 서명 인증서 생성 창이 열립니다.
4. 요청된 데이터를 필드에 입력합니다.
 - a. 암호화 모드: 클라이언트와 서버 간 **AES** 암호화 필요가 관리 >보안> 암호화에서 선택된 경우 **AES-128** 이 기본입니다. **AES** 가 필요하지 않을 경우 **3DES** 가 기본입니다.
 - b. 개인 키 길이: 기본값은 **1024** 입니다.
 - c. 유효 기간(일): 최대 **4** 자리 숫자입니다.
 - d. 국가 코드: **CSR** 태그는 국가 이름입니다.

- e. 시/도: 최대 64 문자입니다. 전체 주 또는 지역 이름을 입력합니다. 약어를 사용하지 마십시오.
 - f. 도시/지역: CSR 태그는 지역 이름입니다. 최대 64 문자입니다.
 - g. 등록된 회사 이름: CSR 태그는 조직 이름입니다. 최대 64 문자입니다.
 - h. 부서/조직 이름: CSR 태그는 조직 단위 이름입니다. 최대 64 문자입니다.
 - i. 정규화된 도메인 이름: CSR 태그는 공통 이름입니다. 등록된 회사 이름은 CSR 에 대한 도메인 이름을 소유해야 합니다. 이 서명 서비스는 등록된 회사가 도메인 이름을 소유하고 있지 않을 경우 요청을 거부합니다.
 - j. 챌린지 암호: 최대 64 문자입니다.
 - k. 관리자 이메일 주소: 인증서 요청에 책임을 맡고 있는 관리자의 이메일 주소를 입력합니다.
5. 인증서를 생성하려면 확인을 클릭합니다. 인증서 화면의 해당 필드에 암호화된 인증서 및 개인 키가 나타납니다.

액세스 제어 목록

IP 액세스 제어 목록은 CC-SG 에 액세스를 거부 또는 허용할 클라이언트 IP 주소 범위를 지정합니다. 액세스 제어 목록의 각 항목은 특정 IP 주소를 가진 특정 그룹의 사용자가 CC-SG 에 액세스할 수 있는지 여부를 결정하는 규칙이 됩니다. 운영 체제 수준에서 전체 CC-SG 시스템에 적용할 규칙을 설정할 수도 있습니다(사용자 그룹 대신 시스템 선택). 규칙을 생성하면 적용되는 순서를 지정하기 위해 목록에 배열할 수 있습니다. 목록의 맨 위에 있는 규칙은 아래의 규칙보다 우선합니다.

▶ **액세스 제어 목록을 보려면:**

1. 관리 > 보안을 선택합니다.
2. 액세스 제어 목록 탭을 클릭합니다.

▶ **액세스 제어 목록에 규칙을 추가하려면:**

1. 관리 > 보안을 선택합니다.
2. 액세스 제어 목록 탭을 클릭합니다.

3. 행 추가 아이콘  을 클릭하여 표에 행을 추가합니다.

4. 시작 IP 값을 시작 IP 필드에 입력하고 종료 IP 값을 종료 IP 필드에 입력하여 규칙을 적용할 IP 주소 범위를 지정합니다.
5. 그룹 드롭다운 화살표를 클릭하여 규칙을 적용할 사용자 그룹을 선택합니다. 시스템을 선택하면 전체 CC-SG 시스템에 규칙이 적용됩니다.
6. 작업 드롭다운 화살표를 클릭하고 IP 범위에서 지정된 사용자가 CC-SG에 액세스할 수 있는지 지정하기 위해 허용 또는 거부를 선택합니다.
7. 업데이트를 클릭하여 변경 사항을 저장합니다.

▶ **운영 체제 수준에서 액세스를 허용하거나 거부하기 위해 액세스 제어 목록에 규칙을 추가하려면:**

1. 관리 > 보안을 선택합니다.
2. 액세스 제어 목록 탭을 클릭합니다.
3. 행 추가 아이콘  을 클릭하여 표에 행을 추가합니다.
4. 시작 IP 값을 시작 IP 필드에 입력하고 종료 IP 값을 종료 IP 필드에 입력하여 규칙을 적용할 IP 주소 범위를 지정합니다.
5. 그룹 > 시스템을 선택합니다.
6. 작업 드롭다운 화살표를 클릭하고 IP 범위에서 지정된 사용자가 CC-SG에 액세스할 수 있는지 지정하기 위해 허용 또는 거부를 선택합니다.
7. 업데이트를 클릭하여 변경 사항을 저장합니다.

▶ **CC-SG가 규칙을 적용할 순서를 변경하려면:**

1. 관리 > 보안을 선택합니다.
2. 액세스 제어 목록 탭을 클릭합니다.
3. 목록에서 위 또는 아래로 이동할 규칙을 선택합니다.
4. 규칙이 제자리에 배치될 때까지 위로 또는 아래로 화살표를 클릭합니다.
5. 업데이트를 클릭하여 변경 사항을 저장합니다.

▶ **액세스 제어 목록에서 규칙을 제거하려면:**

1. 관리 > 보안을 선택합니다.
2. 액세스 제어 목록 탭을 클릭합니다.

3. 제거할 규칙을 선택하고 행 제거 아이콘을 클릭합니다.
4. 업데이트를 클릭하여 변경 사항을 저장합니다.



통지 관리자

통지 관리자를 사용하여 CC-SG에서 통지를 보낼 수 있도록 외부 SMTP 서버를 구성합니다. 통지는 예약된 보고서를 이메일로 보내고 사용자가 잠긴 경우 보고서를 이메일로 보내고 실패하거나 성공한 예약된 작업의 상태를 이메일로 보내는 데 사용됩니다. **작업 관리자** (p. 209)를 참조하십시오. SMTP 서버를 구성한 후에 지정된 수신자에게 테스트 이메일을 보내고 테스트 결과를 수신자에게 알릴 수 있습니다.

외부 SMTP 서버 구성

1. 관리 > 통지를 선택합니다.
2. SMTP 통지 사용 확인란을 선택합니다.
3. SMTP 호스트 필드에 SMTP 호스트를 입력합니다. 호스트 이름 규칙을 보려면 **용어/약어** (p. 2)를 참조하십시오.
4. SMTP 포트 필드에 올바른 SMTP 포트 번호를 입력합니다.
5. 계정 이름 필드에 SMTP 서버에 로그인하는 데 사용할 수 있는 올바른 계정 이름을 입력합니다.
6. 암호 및 암호 다시 입력 필드에 계정 이름의 암호를 입력합니다.
7. 메시지가 CC-SG 에서 전송된 것인지 여부를 식별할 올바른 이메일 주소를 보낸 사람 필드에 입력합니다.
8. 보내기 프로세스에 실패할 경우 보내기 재시도 필드에 이메일을 다시 보낼 횟수를 입력합니다.
9. 보내기 재시도 간격(분) 필드에 보내기 재시도 사이의 경과 시간(분)을 입력합니다. 이 시간은 1-60 분입니다.
10. SSL(Secure Sockets Layer)을 통해 이메일을 안전하게 전송하려는 경우 SSL 사용을 선택합니다.
11. 테스트 구성을 클릭하여 지정된 SMTP 계정으로 테스트 이메일을 전송합니다. 이메일이 도착하는지 확인해야 합니다.
12. 구성 업데이트를 클릭하여 변경 사항을 저장합니다.

작업 관리자

작업 관리자를 사용하여 매일, 매주, 매월 또는 매년의 단위로 CC-SG 작업을 예약합니다. 작업을 지정된 요일에 한 번만 실행되거나 지정된 간격으로 주기적으로 실행되도록 예약할 수 있습니다. 예를 들어, 3 주마다 금요일에 장치 백업을 예약하거나 매주 월요일 특정 보고서가 여러 명의 수신인에게 이메일로 전송되도록 예약할 수 있습니다.

참고: 작업 관리자는 CC-SG 에 설정된 서버 시간을 사용하여 예약하며, 클라이언트 PC 의 시간을 사용하지 않습니다. 서버 시간은 각 CC-SG 화면의 오른쪽 맨 위 모서리에 표시됩니다.

작업 유형

다음과 같은 작업을 예약할 수 있습니다.

- CC-SG 백업
- 장치 구성 백업(개별 장치 또는 장치 그룹)
- 장치 구성 복사(개별 장치 또는 장치 그룹)
- 그룹 전원 제어
- 콘센트 전원 제어
- 로그 제거
- 장치 다시 시작
- 장치 구성 복원(장치 그룹에 적용되지 않음)
- 장치 펌웨어 업그레이드(개별 장치 또는 장치 그룹)
- 모든 보고서 생성

순차적 작업 예약

작업을 순차적으로 예약하여 예상한 동작이 수행되었는지 확인할 수 있습니다. 예를 들어, 해당 장치 그룹에 대한 장치 펌웨어 업그레이드 작업을 예약한 다음 올바른 버전의 펌웨어가 업그레이드된 직후에 자산 관리 보고서를 예약할 수 있습니다.

작업에 대한 이메일 통지

작업 완료 시 지정된 수신자에게 이메일 메시지를 전송할 수 있습니다. 이메일 수신 위치를 지정하고 통지 관리자에서 SSL을 통해 안전하게 이메일을 보내도록 선택할 수 있습니다. **통지 관리자** (p. 208)를 참조하십시오.

예약된 보고서

예약된 보고서가 이메일을 통해 지정한 수신자에게 전송됩니다. 이메일 전송된 보고서의 버전에 대해 CSV 또는 HTML 을 지정할 수 있습니다.

완료 상태인 모든 보고서는 CC-SG에 30 일 동안 HTML 형식으로 보관됩니다. 보고서 메뉴의 예약된 보고서를 선택할 경우에만 완료된 보고서를 HTML 형식으로 볼 수 있습니다. **예약된 보고서** (p. 160)를 참조하십시오.

작업 찾기 및 보기

선택한 범주에 따라 필터링된 목록에서 작업을 볼 수 있습니다. 각 작업에 대한 내역 및 이력을 볼 수 있습니다.

참고: 작업이 변경되거나 업데이트되면 이전 기록이 적용되지 않으며 최근 실행 날짜가 공백이 됩니다.

▶ **작업을 보려면 다음을 수행하십시오.**

1. 관리 > 작업을 선택합니다.
2. 작업을 검색하려면 위로 및 아래로 버튼을 사용하여 보려는 작업의 날짜 범위를 선택합니다.
3. 각 목록에서 하나 이상의(Ctrl+클릭) 작업, 상태 또는 소유자를 선택하여 목록을 추가로 필터링할 수 있습니다.
4. 작업 보기를 클릭하여 작업 목록을 봅니다.

▶ **작업 이력을 보려면:**

- 작업을 선택하고 작업 이력을 클릭합니다.

▶ **작업 내역을 보려면:**

- 작업을 더블 클릭하여 작업 내역이 포함된 대화 상자를 엽니다.

작업 예약

이 섹션에서는 예약할 수 있는 대부분의 작업을 다루고 있습니다. 장치 펌웨어 업그레이드 예약에 대한 자세한 내용은 **장치 펌웨어 업그레이드 예약** (p. 213)을 참조하십시오.

▶ 작업을 예약하려면:

1. 관리 > 작업을 선택합니다.
2. 새로 만들기를 클릭합니다.
3. 메인 탭에서 작업의 이름(1-32 자, 영숫자 또는 밑줄, 공백 없음) 및 설명을 입력합니다.
4. 작업 데이터 탭을 클릭합니다.
5. 작업 실행 드롭다운 메뉴를 클릭하고 예약할 작업을 선택합니다. 데이터가 필요한 필드는 선택한 작업마다 다릅니다. 각 작업에 대한 자세한 내용은 다음 섹션을 참조하십시오.
 - **CommandCenter 백업: CC-SG 백업** (p. 163) 참조
 - **장치 구성 백업: 장치 구성 백업** (p. 43) 참조
 - **장치 구성 복사: 장치 구성 복사** (p. 47) 참조
 - **그룹 전원 제어: 노드 그룹 전원 제어** (p. xix) 참조
 - **콘센트 전원 제어: CC-SG 사용자 설명서** 참조
 - **로그 제거: 로그 활동 구성** (참조 "로그 활동 구성:" p. 185)을 참조하십시오.
 - **장치 다시 시작: 장치 다시 시작** (p. 47) 참조
 - **장치 구성 복원: 장치 구성 복원** (p. 44) 참조(장치 그룹에 적용되지 않음)
 - **장치 펌웨어 업그레이드(개별 장치 또는 장치 그룹): 장치 펌웨어 업그레이드 예약** (p. 213)을 참조하십시오.
 - **모든 보고서 생성: 보고서** (p. 148)를 참조하십시오.
6. 재발생 탭을 클릭합니다. 재발생 탭은 장치 펌웨어 업그레이드 작업 동안에 비활성화됩니다.
7. 기간 필드에 예약된 작업이 반복되는 기간에 해당하는 라디오 버튼을 클릭합니다.
 - a. 한 번: 위로 및 아래로 화살표를 사용하여 작업을 시작해야 하는 시작 시간을 선택합니다.

- b. 주기적: 위로 및 아래로 화살표를 사용하여 작업을 시작해야 하는 시작 시간을 선택합니다. 반복 횟수 필드에 작업을 실행해야 하는 횟수를 입력합니다. 반복 간격 필드에 반복 간격과 시간을 입력합니다. 드롭다운 메뉴를 클릭하고 목록에서 시간 단위를 선택합니다.
 - c. 매일: 작업을 매일 반복하려면 매일 라디오 버튼을 클릭합니다. 작업을 월요일에서 금요일까지 매일 반복하려면 주중 매일 라디오 버튼을 클릭합니다.
 - d. 매주: 위로 및 아래로 화살표를 사용하여 작업 실행 간격과 주를 선택하고 작업을 실행하는 각 주에 반복해야 하는 각 요일 옆의 확인란을 선택합니다.
 - e. 매월: 일 필드에 작업을 실행해야 하는 날짜를 입력하고 지정된 날짜에서 작업을 반복해야 하는 각 월 옆의 확인란을 선택합니다.
 - f. 매년: 드롭다운 메뉴를 클릭하고 목록에서 작업을 실행해야 하는 월을 선택합니다. 위로 및 아래로 화살표를 사용하여 작업을 실행해야 하는 해당 월의 날짜를 선택합니다.
8. 매일, 매주, 매월 및 매년 작업의 경우 재발생 범위 섹션에 작업의 시작 시간 및 종료 시간을 추가해야 합니다. 위로 및 아래로 화살표를 사용하여 시작 시간 및 시작 날짜를 선택합니다. 작업이 지정된 대로 무한정 반복해야 하는 경우 종료 날짜 없음 옆의 라디오 버튼을 클릭하거나 종료 날짜 옆의 라디오 버튼을 클릭한 다음 위로 및 아래로 화살표를 사용하여 작업 실행을 중지해야 하는 날짜를 선택합니다.
9. 재시도 탭을 클릭합니다.
10. 작업에 실패할 경우 **CC-SG**는 재시도 탭에 지정된 대로 나중에 작업을 다시 시도할 수 있습니다. 재시도 필드에 **CC-SG**가 작업을 다시 실행해야 하는 횟수를 입력합니다. 재시도 간격 필드에 재시도 간격과 시간을 입력합니다. 드롭다운 메뉴를 클릭하고 목록에서 시간 단위를 선택합니다.

중요: SX 또는 KX 장치를 업그레이드하도록 작업을 예약하는 경우 재시도 간격을 20 분 이상으로 설정합니다. 이러한 장치를 업그레이드하려면 20 분 정도 소요되기 때문입니다.

11. 통지 탭을 클릭합니다.

12. 작업의 성공 또는 실패에 대한 통지를 보내야 하는 이메일 주소를 지정할 수 있습니다. 기본적으로 현재 로그인된 사용자의 이메일 주소를 사용할 수 있습니다. 사용자 이메일 주소는 사용자 프로필에 구성되어 있습니다. 다른 이메일 주소를 추가하려면 추가를 클릭하고 열린 창에 이메일 주소를 입력한 다음 확인을 클릭합니다. 기본적으로 작업이 완료되었으면 이메일이 전송됩니다. 작업 실패를 수신자에게 통지하려면 실패 시를 선택합니다.
13. 확인을 클릭하여 변경 사항을 저장합니다.

장치 펌웨어 업그레이드 예약

장치 그룹 안에서 **KX** 또는 **SX** 와 같은 동일 유형의 다중 장치를 업그레이드하도록 작업을 예약할 수 있습니다. 작업이 시작되면 보고서 > 예약된 보고서 메뉴에서 장치 펌웨어 업그레이드 보고서를 받아 실시간으로 업그레이드 상태를 볼 수 있습니다. 통지 탭에서 옵션을 지정한 경우 이 보고서가 이메일로도 전송됩니다.

예상 업그레이드 시간은 각 장치에 대한 **Raritan** 사용자 설명서를 참조하십시오.

▶ 장치 펌웨어 업그레이드를 예약하려면:

1. 관리 > 작업을 선택합니다.
2. 새로 만들기를 클릭합니다.
3. 메인 탭에서 작업의 이름 및 설명을 입력합니다. 선택한 이름은 작업 및 작업과 연관된 보고서를 식별하기 위해 사용됩니다.
4. 작업 데이터 탭을 클릭합니다.
5. 장치 업그레이드 내역을 지정합니다.
 - a. 작업 실행: 장치 펌웨어 업그레이드를 선택합니다.
 - b. 장치 그룹: 업그레이드할 장치를 포함하는 장치 그룹을 선택합니다.
 - c. 장치 유형: 업그레이드할 장치 유형을 선택합니다. 둘 이상의 장치 유형을 업그레이드해야 할 경우 각 유형에 대해 작업을 예약해야 합니다.
 - d. 동시 업그레이드: 업그레이드의 파일 전송 부분을 동시에 시작해야 하는 장치 수를 지정합니다. 최대 10입니다. 각 파일 전송이 완료되면 새 파일 전송이 시작되어 한 번에 최대 동시 전송 수만큼 발생하도록 보장합니다.

- e. 파일 업그레이드: 업그레이드할 펌웨어 버전을 선택합니다. 선택된 장치 유형에 적합한 이용 가능 업그레이드 파일만 옵션으로 표시됩니다.
6. 업그레이드 기간을 지정합니다.
- a. 시작 날짜/시간: 작업이 시작될 날짜 및 시간을 선택합니다. 시작 날짜/시간은 현재 날짜/시간보다 커야 합니다.
 - b. 업그레이드 시간대 및 최종 업그레이드 날짜/시간 제한: 지정된 시간대 안에 모든 업그레이드를 완료해야 할 경우 이 필드를 사용하여 그 이후에는 새 업그레이드가 시작될 수 없는 날짜 및 시간을 지정합니다. 최종 업그레이드 시작 날짜/시간 필드를 활성화하기 위해 업그레이드 시간대 제한을 선택합니다.
7. 업그레이드할 장치 및 순서를 지정합니다. 우선순위가 높은 장치를 목록 맨 위에 배치합니다.
- a. 사용 가능 목록에서 업그레이드할 각 장치를 선택하고 추가를 클릭하여 선택 목록으로 이동합니다.
 - b. 선택 목록에서 장치를 선택하고 화살표 버튼을 사용하여 업그레이드를 진행할 순서로 장치를 이동합니다.
8. 실패한 업그레이드를 재시도할 것인지 여부를 지정합니다.
- a. 재시도 탭을 클릭합니다.
 - b. 재시도 횟수: **CC-SG** 가 실패한 업그레이드를 재시도하는 횟수를 입력합니다.
 - c. 재시도 간격: 재시도 사이의 경과 시간을 입력합니다. 기본 시간은 **30, 60** 및 **90** 분입니다. 이것이 최적의 재시도 간격입니다.
9. 성공 및 실패 통지를 받을 이메일 주소를 지정합니다. 기본적으로 현재 로그인된 사용자의 이메일 주소를 사용할 수 있습니다. 사용자 이메일 주소는 사용자 프로필에 구성되어 있습니다.
- a. 통지 탭을 클릭합니다.
 - b. 추가를 클릭하여 열리는 창에 이메일 주소를 입력한 다음 확인을 클릭합니다.
 - c. 업그레이드가 실패할 경우 이메일이 전송되기 원하면 실패 시를 선택합니다.
 - d. 모든 업그레이드가 성공적으로 완료될 때 이메일이 전송되기 원하면 성공 시를 선택합니다.
10. 확인을 클릭하여 변경 사항을 저장합니다.

작업이 실행을 시작하면 예약된 기간 동안 언제든지 장치 펌웨어 업그레이드 보고서를 열어 업그레이드 상태를 볼 수 있습니다.
장치 펌웨어 업그레이드 보고서 (p. 161)를 참조하십시오.

예약된 작업 변경

예약된 작업은 실행 전에 변경할 수 있습니다.

▶ **예약된 작업을 변경하려면:**

1. 변경할 작업을 선택합니다.
2. 편집을 클릭합니다.
3. 필요한 경우 작업 사양을 변경합니다. 탭 설명에 대해서는 **작업 예약** (p. 211) 및 **장치 펌웨어 업그레이드 예약** (p. 213)을 참조하십시오.
4. 업데이트를 클릭하여 변경 사항을 저장합니다.

작업 재예약

작업 관리자의 다른 이름으로 저장 기능을 이용하여 다시 실행할 완료된 작업을 재예약할 수 있습니다. 이 작업은 완료된 작업과 비슷한 새 작업을 생성할 경우에도 편리한 방법입니다.

▶ **작업을 재예약하려면:**

1. 관리 > 작업을 선택합니다.
2. 작업 관리자 페이지에서 재예약할 작업을 선택합니다. 필터링 기준을 사용하여 작업을 검색합니다.
3. 다른 이름으로 저장을 클릭합니다.
4. 열린 다른 이름으로 작업 저장 창에서 탭은 이전에 구성된 작업의 정보로 채워집니다.
5. 필요한 경우 작업 사양을 변경합니다. 탭 설명에 대해서는 **작업 예약** (p. 211) 및 **장치 펌웨어 업그레이드 예약** (p. 213)을 참조하십시오.
6. 확인을 클릭하여 변경 사항을 저장합니다.

다른 작업과 비슷한 작업 예약

비슷한 사양의 새 작업을 예약하기 위해 이전에 구성된 작업을 "템플릿"으로 사용할 수 있습니다.

▶ **다른 작업과 비슷한 작업을 예약하려면:**

- **작업 재예약** (p. 215)을 참조하십시오.

작업 삭제

작업 관리자에서 작업을 제거하여 삭제할 수 있습니다. 현재 실행 중인 작업은 삭제할 수 없습니다.

▶ **작업을 삭제하려면:**

- 작업을 선택하고 삭제를 클릭합니다.

CommandCenter NOC

설정에 CommandCenter NOC(CC-NOC)를 추가하면 직렬 및 KVM 대상 시스템에 대한 모니터링, 보고 및 경고 서비스를 제공함으로써 대상 관리 기능이 확장됩니다. CC-NOC 설치 및 작동에 대한 자세한 내용은 Raritan CommandCenter NOC 설명서를 참조하십시오.

유효한 연결을 생성하려면 CC-SG 와 CC-NOC 사이의 시간 설정을 동기화해야 합니다. NTP 서버를 사용하려면 CC-NOC 및 CC-SG 를 구성해야 합니다.

CC-NOC 추가

CC-NOC 관리자에게 생성된 암호문을 제공하고 해당 관리자는 5 분 내에 CC-NOC 에서 암호문을 구성해야 합니다. 자동화된 시스템의 방해받지 않으려면 이메일이나 기타 전자 방식으로 암호문을 전송하지 마십시오. 신뢰할 수 있는 두 당사자 간에 전화나 서면으로 암호문을 교환하는 것이 자동화된 방해받지 않는 좋은 방법입니다.

1. 액세스 메뉴에서 CC-NOC 구성을 클릭합니다.
2. 추가를 클릭합니다.
3. 추가할 CC-NOC 의 소프트웨어 버전을 선택하고 다음을 클릭합니다. 버전 5.1 에는 5.2 보다 통합 기능이 적게 들어 있으며 이름과 IP 주소를 추가해야 합니다. CC-NOC 5.1 에 대한 자세한 내용은 Raritan 지원 웹 사이트를 참조하십시오.
4. CC-NOC 에 대한 설명 이름을 이름 필드에 입력합니다. 최대 길이는 영숫자 50 자입니다.

5. CC-NOC의 IP 주소 또는 호스트 이름을 CC-NOC IP/호스트 이름 필드에 입력합니다. 이것은 필수 필드입니다. 호스트 이름 규칙을 보려면 **용어/약어** (p. 2)를 참조하십시오.
6. CC-NOC 데이터베이스에서 대상에 대한 일일 정보를 검색하려면 IP 범위 시작 및 IP 범위 끝 필드에 검색 범위를 입력합니다. CC-SG 는 CC-NOC 가 이 IP 범위에서 장치에 대한 이벤트를 CC-SG 로 전송하도록 요청합니다. 이 범위는 CC-NOC 에 구성된 검색 범위와 관련되어 있습니다. Raritan 의 **CommandCenter NOC 관리자 설명서**를 참조하십시오. 다음과 같은 규칙을 준수하며 범위를 입력합니다.

IP 주소 범위	설명
여기에 입력된 CC-SG 범위가 CC-NOC 에 구성된 범위의 하위 세트인 경우...	CC-NOC 는 이 범위의 알려진 모든 대상 장치 정보를 반환합니다.
여기에 입력된 CC-SG 범위가 CC-NOC 에 구성된 범위의 부분 목록(Null 이 아닌 교차점)을 포함하는 경우...	CC-NOC 는 교차 범위 내의 알려진 모든 대상 장치 정보를 반환합니다.
CC-SG 범위가 CC-NOC 에 구성된 범위의 상위 세트인 경우...	CC-NOC 는 이 범위의 알려진 모든 대상 장치 정보를 반환합니다. 기본적으로, CC-NOC 에서는 CC-NOC 범위에 정의된 대상을 리턴합니다.
CC-SG 범위가 CC-NOC 에 구성된 범위와 겹치지 않는 경우...	CC-NOC 는 대상 장치 정보를 반환하지 않습니다.

참고: CC-NOC 동기화 보고서를 사용하여 CC-SG가 가입 중인 대상을 표시합니다. 보고서에는 CC-NOC에서 검색한 새 대상도 표시됩니다. CC-NOC 동기화 보고서 (p. 161)를 참조하십시오

1. 동기화 시간을 지정하여 CC-NOC 데이터베이스에서 대상 정보가 검색되는 시간을 예약합니다. 그러면 대상이 검색되거나 관리되지 않음 상태가 되면서 새로 고침됩니다. 기본값은 클라이언트 시스템에 설정된 현재 시간입니다. 동기화가 다른 프로세스의 성능에 영향을 주지 않도록 한가한 시간에 동기화 일정을 정할 수 있습니다.
2. 하트비트 간격 필드에 CC-SG에서 CC-NOC로 하트비트 메시지를 전송하는 빈도(초)를 입력합니다. 그러면 CC-NOC가 아직 설치되어 사용 가능한지 확인됩니다. 기본값은 60 초입니다. 올바른 범위는 30-120 초입니다.

3. 하트비트 시도 실패 필드에서 **CC-NOC** 노드가 사용 불가능한 것으로 간주되기 전에 응답하지 않고 통과해야 하는 연속적인 하트비트의 수를 입력합니다. 기본값은 2 하트비트입니다. 올바른 범위는 2-4 하트비트입니다.
4. 다음을 클릭합니다.
5. **CC-NOC** 관리자이거나 **CC-NOC** 관리자에게 두 개의 암호문을 제출하는 경우 **CC-NOC** 필드에 암호문을 입력합니다.

중요: 보안을 강화하려면 **CC-SG**를 생성한 시간으로부터 **5분** 내에 **CC-NOC**에 암호문을 입력해야 합니다. 그러면 침입자가 강제 공격으로 시스템을 파괴할 수 있는 기회의 창이 최소화됩니다. 구두 혹은 서면으로 암호문을 교환합니다.

인증 교환 프로세스가 완료되면 **CC-NOC**와 **CC-SG** 사이에 안전한 채널이 설정됩니다. **CC-NOC** 데이터가 **CC-SG**로 복사됩니다. 확인을 클릭하여 프로세스를 완료합니다. 프로세스가 5분 내에 완료되지 않으면 시간이 초과되어 데이터가 **CC-SG**에 저장되지 않으며 저장된 인증서는 삭제됩니다. 절차를 반복해야 합니다.

참고: **CommandCenter NOC**는 독립형 **CC-SG** 장치 또는 기본 노드의 클러스터된 **CC-SG** 장치에만 추가할 수 있습니다.

CC-NOC 편집

▶ **CC-NOC**를 편집하려면

1. 액세스 > **CC-NOC** 구성을 선택합니다.
2. 목록에서 **CC-NOC**를 선택하고 편집을 클릭합니다.
3. 필요한 경우 구성을 변경합니다.

CC-NOC 실행

▶ **CC-SG**에서 **CC-NOC**를 실행하려면 다음을 수행하십시오.

1. 액세스 > **CC-NOC** 구성을 선택합니다.
2. **CC-NOC** 구성 화면에서 사용 가능한 **CC-NOC**를 선택합니다.
3. 실행을 클릭합니다. 그러면 구성된 **CC-NOC**로 연결됩니다.

CC-NOC 삭제

1. 액세스 > **CC-NOC** 구성을 선택합니다.

2. CC-SG 에서 삭제할 CC-NOC 를 선택하고 삭제를 클릭합니다. 확인 메시지가 나타납니다.
3. 예를 클릭하여 CC-NOC 를 삭제합니다. CC-NOC 가 삭제되었을 때 메시지가 표시됩니다.

CC-SG에 대한 SSH 액세스

Putty 또는 OpenSSH Client 와 같은 SSH(Secure Shell) 클라이언트를 사용하여 CC-SG 에서 SSH(v2) 서버에 대한 명령줄 인터페이스에 액세스합니다. CC-SG 명령의 하위 세트만 SSH 를 통해 제공되어 장치 및 CC-SG 자체를 관리합니다.

SSH 클라이언트 사용자는 CC-SG 에서 인증되며 여기서는 기존의 인증 및 허가 규정이 SSH 클라이언트에 적용됩니다. SSH 클라이언트가 사용할 수 있는 명령은 SSH 클라이언트 사용자가 속하는 사용자 그룹에 대한 권한으로 판별됩니다.

SSH 를 사용하여 CC-SG 에 액세스하는 관리자는 CC 수퍼 사용자 SSH 사용자를 로그아웃시킬 수 없지만 시스템 관리자를 포함하여 다른 모든 SSH 클라이언트 사용자는 로그아웃시킬 수 있습니다.

▶ SSH 를 통한 CC-SG 액세스:

1. PuTTY 와 같은 SSH 클라이언트를 실행합니다.
2. CC-SG 의 IP 주소를 지정합니다.
3. SSH 포트 번호를 지정합니다. 기본은 22 입니다. 보안 관리자에서 SSH 액세스를 위한 포트를 구성할 수 있습니다. **보안 관리자** (p. 196)를 참조하십시오.
4. 연결을 엽니다.
5. CC-SG 사용자 이름과 암호로 로그인합니다.
6. 셸 프롬프트가 표시됩니다.

▶ 모든 SSH 명령을 표시하려면:

- 셸 프롬프트에서 ls 를 입력하여 사용 가능한 모든 명령을 표시합니다.

```

192.168.32.58 - PuTTY
login as: admin
admin@192.168.32.58's password:
Welcome to CC-SG

[CommandCenter admin]$ ls
?          activeports      activeusers
backupdevice  clear           connect
console_cmd  copydevice      disconnect
entermaint   exit            exitmaint
grep         help            list_interfaces
list_nodes   list_ports      listbackups
listdevices  listfirmwares  listinterfaces
listnodes    listports       logoff
ls           more            pingdevice
restartcc    restartdevice   restoredevice
shutdowncc   ssh             su
ul           upgradedevice   user_list
[CommandCenter admin]$
  
```

SSH 명령에 대한 도움말 얻기

모든 명령에 대한 제한된 도움말을 한 번에 얻을 수 있습니다. 또한 한 번에 하나의 명령에 대한 자세한 도움말을 얻을 수도 있습니다.

▶ 단일 SSH 명령에 대한 도움말을 얻으려면:

1. 셸 프롬프트에서 도움말을 원하는 명령을 입력하고 공백 다음에 -h 를 입력합니다. 예:
connect -h
2. 명령, 매개변수 및 사용법에 대한 정보가 화면에 표시됩니다.

▶ 모든 SSH 명령에 대한 도움말을 얻으려면:

1. 셸 프롬프트에서 다음 명령을 입력합니다.
help
2. 각 SSH 명령에 대한 간략한 설명과 예제가 화면에 표시됩니다.

SSH 명령 및 매개변수

다음 표에는 SSH 에서 사용할 수 있는 모든 명령이 나열됩니다. 각 명령에 액세스하려면 CC-SG 에 적절한 권한을 지정해야 합니다.

일부 명령은 실행하기 위해 입력해야 하는 추가적인 매개변수가 있습니다. 명령 입력 방법에 대한 자세한 정보는 **명령 팁** (p. 224)을 참조하십시오.

▶ 활성 포트를 나열하려면:

```
activeports
```

▶ 활성 사용자를 나열하려면:

```
activeusers
```

▶ 장치 구성을 백업하려면:

```
backup device <[-host <호스트>] | [-id <device_id>]>  
backup_name [설명]
```

▶ 화면을 지우려면:

```
clear
```

▶ 직렬 포트에 대한 연결을 설정하려면:

<port_name> 또는 <device_name>에 공백이 있는 경우 해당 이름을 따옴표로 묶어야 합니다.

```
connect [-d <device_name>] [-e <escape_char>] <[-i  
<interface_id>] | [-n <port_name>] | [port_id]>
```

▶ 하나의 장치에서 다른 장치로 장치 구성을 복사하려면: 동일 포트 수를 가진 SX 장치 전용:

```
copydevice <[-b <backup_id>] | [source_device_host]>  
target_device_host
```

▶ 포트 연결을 닫으려면:

```
disconnect <[-u <username>] [-p <port_id>] [-id  
<connection_id>]>
```

▶ 정비 모드를 시작하려면:

```
entermaint minutes [message]
```

- ▶ 정비 모드를 종료하려면:

```
exitmaint
```

- ▶ 파이프된 출력 흐름에서 텍스트를 검색하려면:

```
grep search_term
```

- ▶ 모든 명령에 대한 도움말 화면을 보려면:

```
help
```

- ▶ 사용 가능한 장치 구성 백업을 나열하려면:

```
listbackups <[-id <device_id>] | [호스트]>
```

- ▶ 사용 가능한 장치를 나열하려면:

```
listdevices
```

- ▶ 업그레이드에 사용할 수 있는 펌웨어 버전을 나열하려면:

```
listfirmwares [[-id <device_id>] | [호스트]]
```

- ▶ 모든 인터페이스를 나열하려면:

```
listinterfaces [-id <node_id>]
```

- ▶ 모든 노드를 나열하려면:

```
listnodes
```

- ▶ 모든 포트를 나열하려면:

```
listports [[-id <device_id>] | [호스트]]
```

- ▶ 사용자를 로그오프시키려면:

```
logoff [-u <사용자 이름>] 메시지
```

- ▶ 모든 명령을 나열하려면:

```
ls
```

- ▶ 페이지를 지정하려면:

```
more [-p <page_size>]
```

- ▶ 장치에 핑하려면:

```
pingdevice <[-id <device_id>] | [호스트]>
```

▶ **CC-SG** 를 다시 시작하려면:

```
restartcc minutes [message]
```

▶ 장치를 다시 시작하려면:

```
restartdevice <[-id <device_id>] | [호스트]>
```

▶ 장치 구성을 복원하려면:

```
restoredevice <[-host <호스트>] | [-id <device_id>]>  
[backup_id]
```

▶ **CC-SG** 를 종료하려면:

```
shutdowncc minutes [message]
```

▶ **SX** 장치에 대한 **SSH** 연결을 열려면:

```
ssh [-e <escape_char>] <[-id <device_id>] | [호스트]>
```

▶ 사용자를 변경하려면:

```
su [-u <user_name>]
```

▶ 장치 펌웨어를 업그레이드하려면:

```
upgradedevice <[-id <device_id>] | [호스트]>
```

▶ 모든 현재 사용자를 나열하려면:

```
userlist
```

▶ **SSH** 세션을 종료하려면:

```
exit
```

명령 팁

- upgradedevice와 같이 IP 주소를 전달하는 명령의 경우 IP 주소에 대신 호스트 이름을 사용할 수 있습니다. 호스트 이름 규칙을 보려면 **용어/약어** (p. 2)를 참조하십시오.
- copydevice 및 restartdevice 명령은 일부 Raritan 장치에만 적용됩니다. Dominion SX 및 IPMI 서버는 이 명령을 지원하지 않습니다.
- 각괄호 안에 있는 명령의 일부는 옵션입니다. 이 명령의 일부를 사용할 필요는 없습니다.
- 일부 명령에는 "Or" 기호로 분리된 두 개의 세그먼트가 있습니다.
|
명령의 나열된 부분 중 하나는 반드시 입력해야 하지만 둘 모두를 입력할 필요는 없습니다.
- 각괄호에 있는 명령의 일부는 입력해야 하는 텍스트를 보여줍니다. 각괄호는 입력하지 않습니다. 예:

명령 구문	장치 ID 값	다음을 입력합니다.
ssh -id <device_id>	100	ssh -id 100

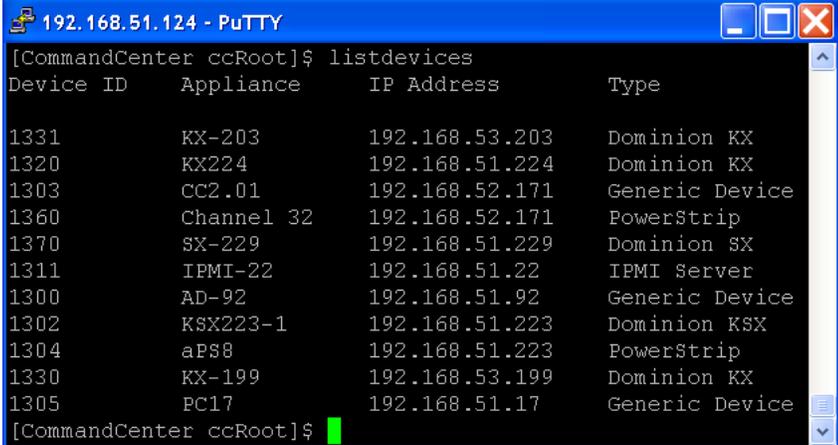
- 기본 escape 문자는 tilde 기호 뒤에 마침표가 옵니다. 예:
~.
escape 문자 및 exit 명령 사용에 대한 자세한 내용은 **SSH 연결 종료** (p. 227)를 참조하십시오.

직렬 가능 장치에 SSH 연결 생성

직렬 가능 장치에 대한 SSH 연결을 생성하여 장치에 대한 관리 조작을 수행할 수 있습니다. 연결되면 직렬 가능 장치에서 지원하는 관리 명령을 사용할 수 있습니다.

참고: 연결하기 전에 직렬 가능 장치가 CC-SG 에 추가되어야 합니다.

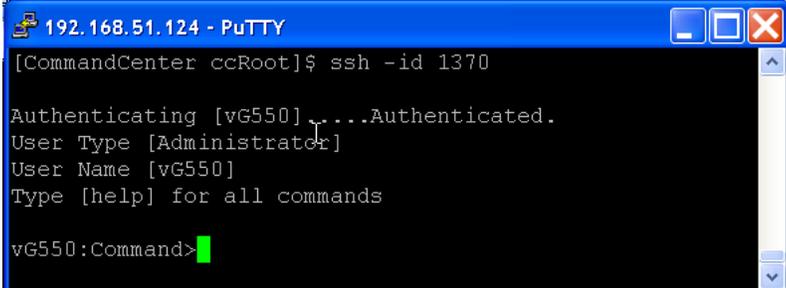
1. listdevices 를 입력하여 직렬 가능 장치가 CC-SG 에 추가되었는지 확인합니다.



```

[CommandCenter ccRoot]$ listdevices
Device ID      Appliance      IP Address      Type
-----
1331           KX-203         192.168.53.203  Dominion KX
1320           KX224          192.168.51.224  Dominion KX
1303           CC2.01         192.168.52.171  Generic Device
1360           Channel 32     192.168.52.171  PowerStrip
1370           SX-229         192.168.51.229  Dominion SX
1311           IPMI-22        192.168.51.22   IPMI Server
1300           AD-92          192.168.51.92   Generic Device
1302           KSX223-1       192.168.51.223  Dominion KSX
1304           aPS8           192.168.51.223  PowerStrip
1330           KX-199         192.168.53.199  Dominion KX
1305           PC17           192.168.51.17   Generic Device
[CommandCenter ccRoot]$
  
```

2. ssh -id <device_id> 를 입력하여 장치에 연결합니다.
예를 들어, 위 그림 사용하면 ssh-id1370 을 입력하여 **SX-229** 에 연결할 수 있습니다.



```

[CommandCenter ccRoot]$ ssh -id 1370
Authenticating [vG550]...Authenticated.
User Type [Administrator]
User Name [vG550]
Type [help] for all commands
vG550:Command>
  
```

SSH를 사용하여 대역외 직렬 인터페이스를 통해 노드에 연결

SSH를 사용하여 연관된 대역외 직렬 인터페이스를 통해 노드에 연결할 수 있습니다. SSH 연결은 프록시 모드입니다.

1. listinterfaces를 입력하여 노드 ID 및 연관된 인터페이스를 봅니다.

```

192.168.32.58 - PuTTY
[CommandCenter admin]$
[CommandCenter admin]$ listinterfaces
Interface ID  Interface name  Interface type  Node ID  Node name
-----
100          Serial Target 1  Serial interface  100     Serial Target 1
136          Admin           Serial interface  100     Serial Target 1
140          Serial Target 4  Serial interface  131     Serial Target 4
104          Serial Target 3  Serial interface  104     Serial Target 3
103          Admin           Serial interface  103     Admin
108          Serial Target 2  Serial interface  108     Serial Target 2
[CommandCenter admin]$
  
```

2. connect -i <interface_id>를 입력하여 인터페이스와 연관된 노드에 연결합니다.

```

192.168.32.58 - PuTTY
100          Serial Target 1  Serial interface  100     Serial Target 1
136          Admin           Serial interface  100     Serial Target 1
140          Serial Target 4  Serial interface  131     Serial Target 4
104          Serial Target 3  Serial interface  104     Serial Target 3
103          Admin           Serial interface  103     Admin
108          Serial Target 2  Serial interface  108     Serial Target 2
[CommandCenter admin]$ connect -i 100
Connecting to port ...
  
```

3. 표시되는 프롬프트에 특정 명령 또는 별칭을 입력할 수 있습니다.

명령	별명	설명
quit	q	연결을 종료하고 SSH 프롬프트로 돌아갑니다.
get_write	gw	쓰기 액세스를 가져옵니다. SSH 사용자가 대상 서버에서 명령을 실행할 수 있고 브라우저 사용자는 진행 과정만 관찰할 수 있습니다.
get_history	gh	기록을 가져옵니다. 대상 서버에서 마지막 몇 가지 명령과 결과를 표시합니다.
send_break	sb	중단을 전송합니다. 브라우저 사용자가 시작한 대상 서버의 루프를 중단합니다.
help	?, h	도움말 화면을 인쇄합니다.

SSH 연결 종료

CC-SG 에 대한 SSH 연결만 만들거나 CC-SG 에 대한 연결을 만들고 CC-SG 가 관리하는 포트, 장치 또는 노드에 대한 연결을 만들 수 있습니다. 이 연결을 종료하는 방법은 종료할 부분에 따라 여러 가지가 있습니다.

▶ CC-SG 에 대한 전체 SSH 연결을 종료하려면:

이 명령은 CC-SG 를 통해 만든 포트, 장치 또는 노드 연결을 포함하여 전체 SSH 연결을 종료합니다.

- 프롬프트에서 다음 명령을 입력하고 Enter 키를 누릅니다.

```
exit
```

▶ CC-SG 에 연결된 동안 포트, 장치 또는 노드에 대한 연결을 종료하려면:

CC-SG 에 대한 SSH 연결을 유지하면서 포트, 장치 또는 노드에 대한 연결을 종료하기 위해 **escape** 문자를 사용할 수 있습니다.

기본 **escape** 문자는 틸드 기호 뒤에 마침표가 옵니다.

- 프롬프트에서 다음 명령을 입력하고 Enter 키를 누릅니다.

```
~.
```

직렬 관리 포트

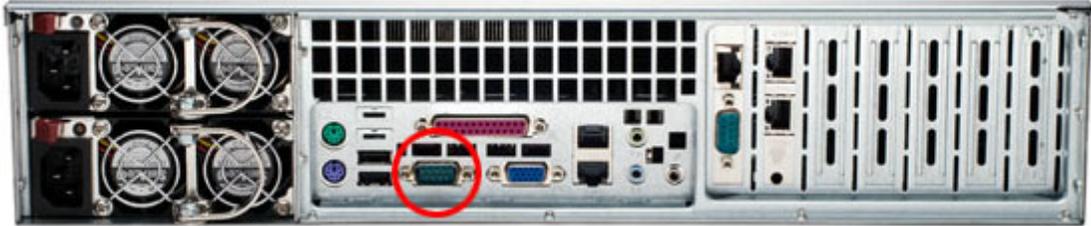
CC-SG 의 직렬 **admin** 포트는 Dominion SX 또는 KSX 와 같은 Raritan 직렬 장치에 직접 연결할 수 있습니다.

HyperTerminal 이나 PuTTY 와 같은 터미널 애플리케이션 프로그램을 사용하여 IP 주소를 통해 SX 나 KSX 에 연결할 수 있습니다. 터미널 애플리케이션 프로그램에서 전송 속도를 SX 또는 KSX 전송 속도와 일치하도록 설정합니다.

▶ V1 직렬 관리 포트:



▶ E1 직렬 관리 포트:



터미널 에뮬레이션 프로그램 정보

HyperTerminal 은 대부분 Windows OS 에서 이용할 수 있습니다.
HyperTerminal 이 Windows Vista 에는 없습니다.

PuTTY 는 인터넷에서 다운로드할 수 있는 무료 프로그램입니다.

CC-SG 일련 번호 찾기

▶ **CC-SG 일련 번호를 찾으려면:**

1. Admin 클라이언트에 로그인합니다.
2. 도움말 > Raritan Secure Gateway 정보를 선택합니다.
3. CC-SG 일련 번호를 사용하여 새 창을 엽니다.

Web Services API

Web Services 애플리케이션 프로그래밍 인터페이스(WS API)는 현재 활성화할 수 없습니다. 이 기능에 대한 업데이트 정보는 <http://www.raritan.com/web-services-api> 를 참조하십시오.

Web Services API 클라이언트를 CC-SG 에 추가하기 전에 최종 사용자 계약에 동의해야 합니다. 최대 5 개의 WS-API 클라이언트를 추가할 수 있습니다. API 사용에 대한 자세한 내용은 CC-SG Web Services SDK 설명서를 참조하십시오.

▶ **Web Services API 를 추가하려면:**

1. 액세스 > Web Services API 추가를 선택합니다. 이 옵션은 CC 설정 및 제어 권한이 있는 사용자만 이용할 수 있습니다.
2. 최종 사용자 계약을 읽으십시오.
 - 저장할 텍스트를 복사하여 붙여넣기하거나 Secure Gateway > 인쇄를 선택할 수 있습니다.

- 구성을 완료한 후 이 계약은 액세스 메뉴에서도 이용할 수 있습니다.
3. 동의를 클릭합니다. 새 **Web Services API** 구성 창이 열립니다.
 4. 웹 서비스 클라이언트에 대해 요청된 데이터를 입력합니다.
 - **Web Services** 클라이언트 이름: 최대 64 문자입니다.
 - IP 주소/호스트 이름: 최대 64 문자입니다.
 - **HTTPS** 웹 서비스 포트: 읽기 전용 필드. **CC-SG** 는 트러스트 설정이 생성된 경우 **9443** 를 사용합니다.
 - 라이선스 있는 공급업체 이름: 최대 64 문자입니다.
 - 공급업체 이름 인증: **Raritan** 공급업체 인증 페이지를 엽니다.
 - 클라이언트 애플리케이션 URL: URL 이 지정될 경우 **CC-SG** 에서 웹 서비스 애플리케이션에 액세스하기 위해 메뉴 항목을 이용할 수 있습니다.
 5. 자체 서명 인증서를 생성합니다.
 - a. 암호화 모드: 클라이언트와 서버 간 **AES** 암호화 필요가 관리 >보안> 암호화에서 선택된 경우 **AES-128** 이 기본입니다. **AES** 가 필요하지 않을 경우 **3DES** 가 기본입니다.
 - b. 개인 키 길이: 기본값은 **1024** 입니다.
 - c. 유효 기간(일): 최대 **4** 자리 숫자입니다.
 - d. 국가 코드: **CSR** 태그는 국가 이름입니다.
 - e. 시/도: 최대 **64** 문자입니다. 전체 주 또는 지역 이름을 입력합니다. 약어를 사용하지 마십시오.
 - f. 도시/지역: **CSR** 태그는 지역 이름입니다. 최대 **64** 문자입니다.
 - g. 등록된 회사 이름: **CSR** 태그는 조직 이름입니다. 최대 **64** 문자입니다.
 - h. 부서/조직 이름: **CSR** 태그는 조직 단위 이름입니다. 최대 **64** 문자입니다.
 - i. 정규화된 도메인 이름: **CSR** 태그는 공통 이름입니다. 등록된 회사 이름은 **CSR** 에 대한 도메인 이름을 소유해야 합니다. 이 서명 서비스는 등록된 회사가 도메인 이름을 소유하고 있지 않을 경우 요청을 거부합니다.
 - j. 챌린지 암호: 최대 **64** 문자입니다.
 - k. 관리자 이메일 주소: 인증서 요청에 책임을 맡고 있는 관리자의 이메일 주소를 입력합니다.
 6. 인증서 생성을 클릭합니다. 인증서 상자에 텍스트가 표시됩니다.

15: 고급 관리

7. 파일로 저장을 클릭하여 인증서를 .P12 파일로 저장합니다.
8. 추가를 클릭하여 변경 사항을 저장합니다.

진단 콘솔은 그래픽이 아닌 인터페이스로 CC-SG에 대한 로컬 액세스를 제공합니다. 직렬 또는 KVM 포트에서 진단 콘솔을 액세스할 수 있습니다. **VGA/키보드/마우스 포트를 통한 진단 콘솔 액세스** (p. 231)를 참조하십시오. 또는 PuTTY나 OpenSSH 클라이언트와 같은 SSH(Secure Shell) 클라이언트에서 진단 콘솔에 액세스할 수 있습니다. **SSH를 통한 진단 콘솔 액세스** (p. 231)를 참조하십시오.

진단 콘솔에는 두 개의 인터페이스가 있습니다.

1. 상태 콘솔: **상태 콘솔 정보** (p. 233)를 참조하십시오.
2. 관리자 콘솔: **관리자 콘솔 정보** (p. 233)를 참조하십시오.

참고: SSH를 통해 진단 콘솔에 액세스할 경우 상태 콘솔 및 관리자 콘솔은 SSH 클라이언트 및 키보드 바인딩의 모양 설정을 상속받습니다. 이러한 모양 설정은 이 설명서의 내용과 다를 수 있습니다.

이 장에서

진단 콘솔 액세스.....	231
상태 콘솔.....	233
관리자 콘솔.....	233

진단 콘솔 액세스

VGA/키보드/마우스 포트를 통한 진단 콘솔 액세스

1. VGA 모니터, PS2 키보드 및 마우스를 CC-SG 장치의 후면에 연결합니다.
2. 화면에 로그인 프롬프트를 표시하려면 **Enter** 키를 누릅니다.

SSH를 통한 진단 콘솔 액세스

1. CC-SG에 네트워크로 연결되어 있는 클라이언트 PC에서 PuTTY와 같은 SSH 클라이언트를 시작합니다.
2. IP 주소를 지정하거나 CC-SG가 DNS 서버에 등록된 경우에는 CC-SG의 IP 호스트 이름을 지정합니다. 포트에 대해 23을 지정합니다.
3. 연결할 수 있는 버튼을 클릭합니다. 창이 열리면 로그인 프롬프트가 표시됩니다.

▶ 상태 콘솔에 액세스하려면:

상태 콘솔에 액세스할 경우에는 암호가 필요 없지만 암호를 사용할 수도 있습니다.

- 로그인 프롬프트에서 **status** 를 입력합니다. 읽기 전용 상태 콘솔이 나타납니다.

```

+-----+
|Mon Dec 11 EST      CommandCenter Secure Gateway      22:27:58|
|+ Message of the Day: |-----+
|: CommandCenter Secure Gateway |
|: |
|: Centralized access and control for your global IT infrastructure |
|: |
|: |
|+-----+
|: System Information: |
|: Host Name       : CommandCenter.localdomain |
|: CC-SG Version  : 3.1.0.5.1      Model      : CC-SG-U1 |
|: CC-SG Serial # : ACC6500009     Host ID   : 00304856F118 |
|: Server Information: |
|: CC-SG Status   : Up              DB Status  : Responding |
|: Web Status     : Responding/Unsecured |
|: Cluster Status : standalone      Cluster Peer : Not Configured |
|: Network Information: |
|: Dev Link Auto  Speed Duplex      IPAddr   RX Pkts  TX Pkts |
|: eth0 yes on    100Mb/s Full      192.168.0.192  55285   11 |
|: eth1 no on    Unknown! Unknown! |
|: |
|: |
|: Help: <F1> Exit: <ctl+Q> or <ctl+C> |
+-----+
    
```

이 화면에는 시스템의 상태 및 CC-SG 와 하위 구성요소가 작동 중인지 여부에 대한 정보가 동적으로 표시됩니다.

화면의 오른쪽 상단 모서리에 있는 시간은 CC-SG 데이터가 폴링된 마지막 시간입니다.

이 화면의 정보는 약 5 초마다 업데이트됩니다.

- **Ctrl-L** 을 눌러 현재 화면을 지우고 업데이트된 정보를 다시 로드합니다. 초당 최대 한 번씩 화면을 업데이트할 수 있습니다.
- **Ctrl-Q** 또는 **Ctrl-C** 를 누르면 화면이 종료됩니다.
- 상태 콘솔은 다른 입력이나 화면 탐색을 허용하지 않습니다. 다른 모든 입력은 무시됩니다.

다음 표는 CC-SG 및 CC-SG 데이터베이스의 상태를 설명합니다.

상태	설명
CC-SG Status(상태) 업	CC-SG 가 사용 가능합니다.
CC-SG Status(상태) 다운	CC-SG 는 재부팅 중일 수 있습니다. 작동 안 함 상태가 지속되는 경우 CC-SG 를 다시 시작합니다.

상태	설명
CC-SG Status(상태) Restarting(다시 시작하는 중)	CC-SG 는 다시 시작하는 중일 수 있습니다.
DB Status(상태) Responding(응답 중)	CC-SG 데이터베이스가 사용 가능합니다.
DB Status(상태) 다운	CC-SG 는 재부팅 중일 수 있습니다.

상태 콘솔

상태 콘솔 정보

상태 콘솔을 사용하여 CC-SG 의 상태, CC-SG 가 사용하는 여러 서비스 및 연결된 네트워크를 확인할 수 있습니다.

기본적으로 상태 콘솔은 암호가 필요 없습니다.

상태 콘솔 액세스

▶ 상태 콘솔에 액세스하려면:

1. 로그인 프롬프트에서 **status** 를 입력합니다.
2. 현재 시스템 정보가 표시됩니다.

관리자 콘솔

관리자 콘솔 정보

관리자 콘솔을 사용하여 몇 가지 초기 매개변수를 설정하고, 초기 네트워킹 구성을 제공하며, 로그 파일을 디버그하며, 몇 가지 제한된 진단 및 CC-SG 다시 시작을 수행할 수 있습니다.

관리자 콘솔의 기본 로그인:

- 사용자 이름: admin
- 암호: raritan

진단 콘솔 admin 계정은 Java 기반 CC-SG 관리자 클라이언트 및 html 기반 액세스 클라이언트에서 사용하는 CC-SG 슈퍼 사용자 admin 계정 및 암호와 다릅니다. 이러한 암호 중 하나를 변경해도 다른 암호에는 적용되지 않습니다.

관리자 콘솔 액세스

관리자 콘솔에 표시된 모든 정보는 정적입니다. **CC-SG GUI** 또는 진단 콘솔을 통해 구성이 변경되는 경우 변경사항이 적용된 후에 **Administrator Console** 에 다시 로그인하여 관리자 콘솔의 변경사항을 확인해야 합니다.

▶ 관리자 콘솔에 액세스하려면:

1. 로그인 프롬프트에서 **admin** 을 입력합니다.
2. **CC-SG** 암호를 입력합니다. 기본 암호는 **raritan**입니다. 첫 로그인에서 이 암호는 만료되므로 새 암호를 선택해야 합니다. 이 암호를 입력하고 프롬프트가 표시되면 새 암호를 입력합니다. 암호 길이 설정에 대한 정보는 **진단 콘솔 암호 설정** (p. 251)을 참조하십시오.

기본 관리자 콘솔 화면이 나타납니다.

관리자 콘솔 탐색

관리자 콘솔을 탐색하려면 키보드 조합을 사용합니다. 일부 세션의 경우 마우스를 사용하여 탐색할 수도 있습니다. 그러나 마우스는 모든 **SSH** 클라이언트 또는 **KVM** 콘솔에서 작동하지 않을 수 있습니다.

누름	목적
Ctrl+C 또는 Ctrl+Q	진단 콘솔을 종료합니다.
Ctrl+L	화면을 지우고 정보를 다시 가져옵니다(그러나 정보 자체는 업데이트되거나 새로 고쳐지지 않습니다).
Tab	사용 가능한 다음 옵션으로 이동합니다.
Space bar	현재 옵션을 선택합니다.
Enter	현재 옵션을 선택합니다.
화살표 키	옵션 내에서 다른 필드로 이동합니다.

진단 콘솔 구성 편집

진단 콘솔은 직렬 포트(COM1), VGA/키보드/마우스(KVM) 포트를 통해 또는 SSH(Secure Shell) 클라이언트에서 액세스할 수 있습니다. 각 포트 유형에 대해 status 또는 admin 로그인을 허용할지 여부를 구성하고 필드 지원이 포트에서 진단 콘솔에 액세스할 수 있는지 여부도 구성할 수 있습니다. SSH 클라이언트의 경우 다른 CC-SG 서비스가 원하는 포트를 사용하지 않을 때 사용해야 하는 포트 번호를 구성할 수도 있습니다.

중요: 모든 관리자 또는 필드 지원 액세스를 잠그지 않도록 주의하십시오.

▶ 진단 콘솔 구성을 편집하려면:

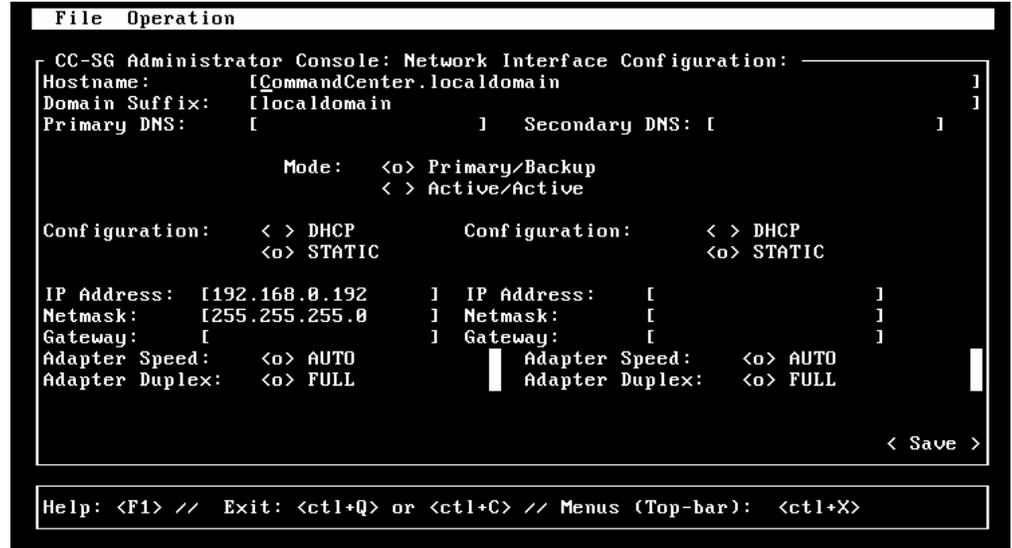
1. 작업 > 진단 콘솔 구성을 선택합니다.
2. 진단 콘솔을 구성하고 액세스하는 방법을 결정합니다.
네 가지의 진단 콘솔 액세스 메커니즘이 있습니다. 직렬 포트(COM1), KVM 콘솔, SSH(IP 네트워크) 및 웹 진단 콘솔은 다음과 같은 세 가지 서비스를 제공합니다. 상태 표시, 관리 콘솔, Raritan 필드 지원. 이 화면에서 다양한 액세스 메커니즘을 통해 서비스를 선택할 수 있습니다.
3. 포트 필드에 진단 콘솔에 대한 SSH 액세스를 위해 설정할 포트 번호를 입력합니다. 기본 포트는 23입니다.
4. 저장을 클릭합니다.

네트워크 인터페이스 구성 편집(네트워크 인터페이스)

네트워크 인터페이스 구성에서 CC-SG의 호스트 이름 및 IP 주소와 같은 초기 설정 작업을 수행할 수 있습니다.

1. 작업 > 네트워크 인터페이스 > 네트워크 인터페이스 구성을 선택합니다.

2. 네트워크 인터페이스가 이미 구성되었으면 CC-SG GUI(Admin 클라이언트)를 사용하여 인터페이스를 구성해야 한다는 경고 메시지가 표시됩니다. 계속 진행하려면 예를 클릭합니다.



3. 호스트 이름 필드에 호스트 이름을 입력합니다. 저장한 후 알려진 정규화된 도메인 이름(FQDN)을 반영하도록 이 필드가 업데이트됩니다. 호스트 이름 규칙을 보려면 **용어/약어** (p. 2)를 참조하십시오.
4. 모드 필드에서 기본/백업 모드 또는 활성/활성 모드를 선택합니다. **네트워크 설정 정보** (p. 179)를 참조하십시오.
 - 구성 필드에서 DHCP 또는 정적을 선택합니다.
 - DHCP 를 선택하고 DHCP 서버가 올바르게 구성된 경우, 저장하고 Admin 콘솔을 종료하고 다시 들어가면 DNS 정보, 도메인 접미사, IP 주소, 기본 게이트웨이 및 서브넷 마스크가 자동으로 채워집니다.
 - 정적을 선택한 경우 IP 주소(필수), 넷마스크(필수), 기본 게이트웨이(옵션), 기본 DNS(옵션), 보조 DNS(옵션) 및 도메인 접미사의 도메인 이름(옵션)을 입력합니다.
 - 인터페이스의 IP 구성을 결정하기 위해 DHCP 를 사용하더라도 올바른 형식의 IP 주소 및 넷마스크를 입력해야 합니다.
5. 어댑터 속도에서 회선 속도를 선택합니다. 다른 값 10, 100 및 1000Mbps 는 스크롤할 수 있는 목록(한 개의 값만 주어진 시간에 볼 수 있음)에 있으며 화살표 키는 이 값을 탐색하는데 사용됩니다. Space bar 키를 눌러 표시된 옵션을 선택합니다. 1GB 회선 속도의 경우 AUTO 를 선택합니다.

6. 어댑터 속도에 대해 자동으로 선택하지 않은 경우 어댑터 이중을 클릭하고 화살표 키를 사용하여 해당하는 경우 목록에서 이중 모드(전 또는 반)를 선택합니다. 이중 모드는 언제든지 선택할 수 있지만 의미만 갖고 있으며 어댑터 속도가 자동으로 아닌 경우에 적용됩니다.
7. 활성/활성 모드를 선택한 경우, 두 번째 네트워크 인터페이스에 대해 이 단계를 반복합니다.
8. 저장을 클릭합니다. CC-SG 를 다시 시작하면 모든 CC-SG GUI 사용자가 로그아웃되고 세션이 종료됩니다. 필요한 네트워크 재구성 및 연관된 CC-SG GUI 사용자에게 대한 영향을 알려주는 경고 화면이 나타납니다. <예>를 선택하여 계속 진행합니다.

진단 콘솔 상태 화면에서 시스템 진행 상황을 모니터링할 수 있습니다. KVM 포트에서 Alt+F2 를 누르고 status 로 로그인하여 다른 터미널 세션을 선택할 수 있습니다. Alt+F1 을 눌러 원래 터미널 세션으로 복귀할 수 있습니다. F1 부터 F6 까지 6 개의 가능한 터미널 세션이 있습니다.

IP 주소 핑

핑을 사용하여 CC-SG 컴퓨터와 특정 IP 주소 사이의 연결이 올바르게 작동하는지 확인합니다.

참고: 일부 사이트는 핑 요청을 명시적으로 차단합니다. 핑이 실패할 경우 대상 및 작동 중인 네트워크를 통해 핑할 수 있는지 확인합니다.

1. 작업 > 네트워크 인터페이스 > 핑을 선택합니다.
2. 대상 핑 필드에 확인할 대상의 IP 주소 또는 호스트 이름(DNS 가 CC-SG 에 적절하게 구성된 경우)을 입력합니다.
3. 선택: 옵션입니다.

옵션	설명
Show other received ICMP packets	Verbose 출력으로 ECHO_RESPONSE 패킷 이외에도 수신한 다른 ICMP 패킷을 나열합니다. 거의 표시되지 않습니다.
No DNS Resolution	주소를 호스트 이름으로 해석하지 않습니다.
Record Route	라우트를 기록합니다. IP 기록 라우트 옵션을 설정합니다. 패킷의 라우트가 IP 헤더에 저장됩니다.
Use Broadcast Address	방송 메시지 핑을 허용합니다.

옵션	설명
Adaptive Timing	적응적 핑. Interpacket 간격이 왕복 시간으로 적응되어 네트워크에 둘 이상의 미응답 프로브가 존재하지 않도록 합니다. 최소 간격은 200msec 입니다.

4. 핑 명령이 실행되는 시간(초), 전송되는 핑 요청의 수 및 핑 패킷 크기(기본값은 56 으로서 8 바이트의 ICMP 헤더 데이터와 결합되면 64 ICMP 데이터 바이트로 번역됨)의 값을 입력합니다. 공백으로 두면 기본값이 사용됩니다. **옵션입니다.**
5. 핑을 클릭합니다. 결과에 일련의 응답이 표시되는 경우 연결이 작동하는 것입니다. 시간은 연결 속도를 표시합니다. 응답 대신에 "timed out" 오류가 표시되면 컴퓨터와 도메인 사이에 연결이 작동하지 않는 것입니다. **정적 루트 편집 (p. 239)**을 참조하십시오.
6. Ctrl+C 를 눌러 세션을 종료합니다.

참고: Ctrl+Q 를 누르면 지금까지 세션에 대한 통계 요약이 표시되고 대상을 계속 ping합니다.

Traceroute 사용

Traceroute 는 주로 네트워크 문제점 해결에 사용됩니다. 통과하는 라우터 목록을 표시하면 컴퓨터에서 사용한 경로를 확인하여 네트워크에서 특정 대상에 도달할 수 있습니다. 대상에 도달하거나 실패하여 폐기될 때까지 통과하는 모든 라우터를 나열합니다. 또한 라우터에서 라우터로의 각 '홉'이 걸리는 시간을 알려줍니다. 그러면 사이트에 대한 액세스를 차단할 수 있는 라우팅 문제 또는 방화벽을 식별할 수 있습니다.

▶ IP 주소 또는 호스트 이름에서 traceroute 수행:

1. 작업 > 네트워크 인터페이스 > Traceroute 를 선택합니다.
2. 확인하려는 대상의 IP 주소 또는 호스트 이름을 Traceroute 대상 필드에 입력합니다.
3. 선택: **옵션입니다.**

옵션	설명
Verbose	Verbose 출력으로 TIME_EXCEEDED 및 UNREACHABLE 이외에 수신한 ICMP 패킷을 나열합니다.

옵션	설명
No DNS Resolution	주소를 호스트 이름으로 해석하지 않습니다.
Use ICMP (vs. normal UDP)	UDP 데이터그램 대신 ICMP ECHO 를 사용합니다.

4. `traceroute` 명령이 나가는 프로브 패킷에서 사용하는 홉 수(기본값은 30), 프로브에 사용할 UDP 대상 포트(기본값은 33434) 및 `traceroute` 패킷 크기의 값을 입력합니다. 공백으로 두면 기본값이 사용됩니다.
5. 창의 오른쪽 맨 아래 모서리에서 Traceroute 를 클릭합니다. 옵션입니다.
6. `Ctrl+C` 또는 `Ctrl+Q` 를 눌러 `traceroute` 세션을 종료합니다. 복귀? 프롬프트가 나타나면 `Enter` 키를 눌러 Traceroute 메뉴로 복귀합니다. “destination reached” 또는 “hop count exceeded” 이벤트가 발생하여 Traceroute 가 종료될 때도 복귀? 프롬프트가 표시됩니다.

정적 루트 편집

정적 라우트에서 현재 IP 라우팅 표를 보고 라우트를 수정, 추가 또는 삭제할 수 있습니다. 정적 라우트를 주의해서 사용하고 배치하면 실제로 네트워크의 성능을 향상시킬 수 있으므로 중요한 비즈니스 애플리케이션의 대역폭을 보존할 수 있으며 각 인터페이스가 별도의 IP 도메인에 연결되어 있는 활성/활성 네트워크 설정에 유용할 수 있습니다. **네트워크 설정 정보** (p. 179)를 참조하십시오. 마우스로 클릭하거나 `Tab` 및 화살표 키를 사용하여 이동하고 `Enter` 키를 눌러 값을 선택합니다.

▶ 정적 라우트 보기 또는 변경:

1. 작업 > 네트워크 인터페이스 > 정적 루트를 선택합니다.

- 현재 IP 라우팅 표 페이지가 열립니다. 호스트 또는 네트워크 라우트를 추가하거나 라우트를 삭제할 수 있습니다. 새로 고침 버튼을 사용하여 표의 라우팅 정보를 업데이트합니다.

```
File Operation

CC-SG Administrator Console: Static Routes:
This screen allows you to manage your IP routing table.
You can see the routes currently in effect, add routes,
and delete routes.
```

Destination	Gateway	Netmask	Interface	Flags
192.168.51.0	*	255.255.255.0	eth0	U
<default>	192.168.51.126	0.0.0.0	eth0	UG

```

< Add Host Route > < Add Network Route > < Delete Route > < Refresh >

Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>

```

진단 콘솔에서 로그 파일 보기

LogViewer 를 통해 하나 이상의 로그 파일을 동시에 볼 수 있습니다. 여기서는 한 번에 몇 개의 파일을 찾아보고 시스템 활동을 검토할 수 있습니다.

로그 파일 목록은 연관된 목록이 활성화 상태가 되거나(예: 사용자가 로그 파일 목록 영역을 사용할 때) 새 정렬 옵션을 선택한 경우에만 업데이트됩니다. 파일 이름 앞에는 로그 파일이 얼마나 최근에 새 데이터를 받았는지 또는 로그 파일의 파일 크기를 나타내는 타임스탬프가 옵니다.

▶ 타임스탬프 및 파일 크기 약어:

타임스탬프:

- s = 초
- m = 분
- h = 시간
- d = 일

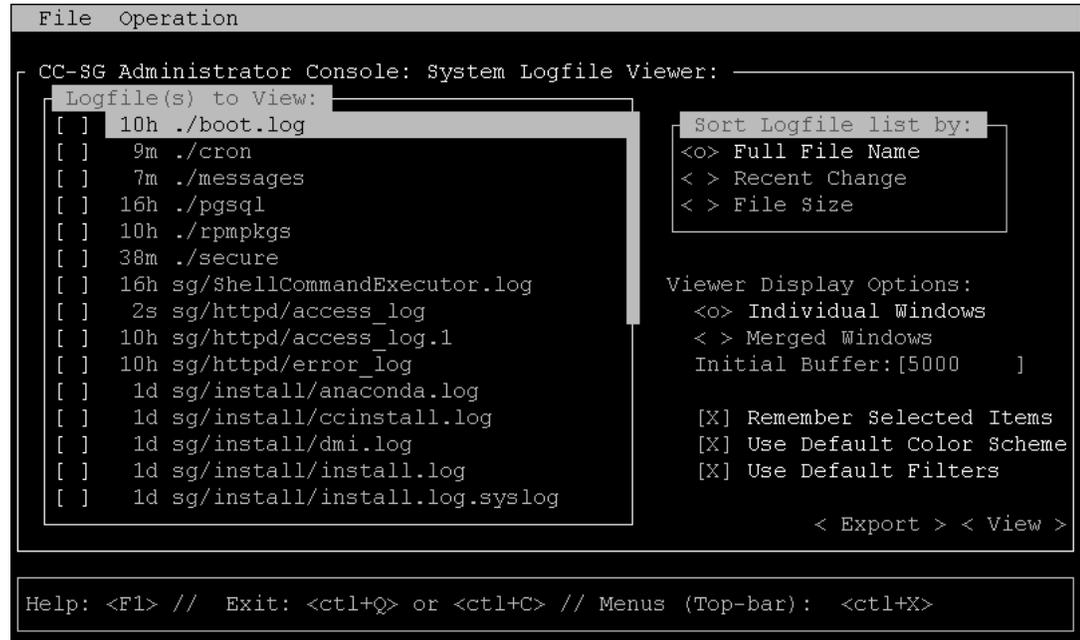
파일 크기:

- B = 바이트
- K = 킬로바이트(1,000 바이트)
- M = 메가바이트(1,000,000 바이트)
- G = 기가바이트(1,000,000,000 바이트)

▶ 로그 파일 보기:

1. 작업 > 관리자 > 시스템 로그파일 뷰어를 선택합니다.
2. Logviewer 화면은 4 개의 기본 영역으로 나누어집니다.
 - 시스템에서 현재 사용할 수 있는 로그 파일의 목록. 목록이 표시 창보다 긴 경우 화살표 키를 사용하여 목록을 스크롤할 수 있습니다.
 - 기준에 맞게 정렬한 로그 파일의 목록. 로그 파일은 전체 파일 이름, 최근에 변경된 로그 파일 또는 가장 큰 로그 파일 크기에 따라 정렬할 수 있습니다.
 - 뷰어 표시 옵션.
 - 내보내기/보기 선택기.

3. 마우스로 클릭하거나 화살표 키를 사용하여 탐색하고 Space bar 를 눌러 로그 파일을 선택하여 X로 표시합니다. 한 번에 둘 이상의 로그 파일을 볼 수 있습니다.



▶ 볼 로그 파일 목록을 정렬하려면:

로그 파일 목록 정렬 기준 옵션은 로그 파일이 볼 로그 파일 목록에 표시되는 순서를 제어합니다.

옵션	설명
Individual Windows	별도의 보조 창에 선택한 로그를 표시합니다.
Merged Windows	선택한 로그를 하나의 표시 창으로 병합합니다.
Initial Buffer	초기 버퍼 또는 기록 크기를 설정합니다. 기본값은 5000 입니다. 이 시스템은 함께 제공되는 모든 새 정보를 버퍼링하도록 구성됩니다.
Remember Selected Items	이 상자를 선택하면 현재 로그 파일 선택 사항(있을 경우)이 기억됩니다. 그렇지 않으면 새 로그 파일 목록이 생성될 때마다 선택 사항이 재설정됩니다. 파일 전체를 단계별로 실행하는 데 유용합니다.
Use Default Color Scheme	이 상자를 선택하면 표준 색 구성표로 일부 로그 파일을 봅니다. 참고: multital 명령은 로그 파일을 볼 때 색 구성표를 변경하는 데 사용할 수 있습니다.

옵션	설명
Use Default Filters	이 상자를 선택하면 일부 로그 파일에 자동 필터가 적용됩니다.
내보내기	이 옵션은 선택한 모든 로그 파일을 패키지로 만들고 웹 액세스를 통해 사용할 수 있도록 하므로 이 파일을 검색하고 Raritan 기술 지원 센터에 전송할 수 있습니다. 고객은 이 패키지의 내용물에 액세스할 수 없습니다. 내보낸 로그 파일은 최대 10일 동안 사용할 수 있으며 기간이 만료될 경우 시스템에서 자동으로 이 로그 파일을 삭제합니다.
보기	선택한 로그를 봅니다.

개별 창에 대해 보기가 선택되면 LogViewer가 표시됩니다.

```

15:30:54,366 INFO [ChannelSocket] JK: ajp13 listening on /0.0.0.0:8009
15:30:54,378 INFO [JkMain] Jk running ID=0 time=0/26 config=null
15:30:54,480 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-9443
15:30:54,756 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-0.0.0.0-8080
15:30:54,801 INFO [Server] JBoss (MX MicroKernel) [4.0.3 (build: CVSTag=JBoss_4.0.3 date=200510042324)] started in 57s:149ms
00] sg/jboss/console.log F1/<CTRL>+<h>: help 118KB - 2006/12/13 15:32:54
3/bin ; USER=root ; COMMAND=/data/raritan/jboss/ccscripts/root-scripts/iptables_ports.sh
Dec 13 15:30:55 CommandCenter httpd: httpd startup succeeded
Dec 13 15:30:55 CommandCenter MonitorCC[14617]: Starting httpd: ^[[60G[ ^[[0:32mOK^[[0:39m
Dec 13 15:30:56 CommandCenter MonitorCC[14617]: startAll: Done -- JBoss:47 HTTPD:1
01] ./messages *Press F1/<CTRL>+<h> for help* 935KB - 2006/12/13 15:32:54
02] sg/httpd/access_log F1/<CTRL>+<h>: help 538KB - 2006/12/13 15:32:54

```

- 로그 파일을 보는 동안 Q, Ctrl-Q 또는 Ctrl+C를 눌러 이전 화면으로 돌아갑니다.

- 중요한 항목을 강조 표시하기 위해 로그 파일에서 색상을 변경할 수 있습니다. 로그 파일의 색상을 변경하려면 C를 입력하고 목록에서 로그를 선택합니다.

```
C Toggle colors: select window
C 00 sg/jboss/console.log
C 01 ./messages
C 02 sg/httpd/access_log
Press ^G to abort
```

- 시스템 정보를 표시하려면 I를 입력합니다.

참고: 이 관리 콘솔 세션의 시작 부분에서 시스템 로드는 정적입니다. TOP 유틸리티를 사용하여 시스템 자원을 동적으로 모니터링합니다.

▶ 정규식을 이용하여 로그 파일을 필터링하려면:

1. 정규식을 추가하거나 편집하려면 e를 입력하고 여러 항목을 보려고 선택한 경우 목록에서 로그를 선택합니다.

```
Select window (reg.exp. editi
)00 sg/jboss/console.log
01 ./messages
02 sg/httpd/access_log
Press ^G to abort
```

2. 정규식을 추가하려면 A를 입력합니다. 예를 들어, sg/jboss/console.log 로그 파일의 WARN 메시지에서 정보를 표시하려면 WARN을 입력하고 match를 선택합니다.

참고: 또한 이 화면은 대부분의 Java 힙 메시지를 제거하는 console.log 에 대한 기본 필터 시스템을 표시합니다.

```

50064K->45311K(324096K), 0.4177820 secs]
Edit reg.exp.
sg/jboss/console.log
add, edit, delete, quit, move Down, move Up, reset counter
nv Unloading class |Full GC |\[GC 601
00] s 46:02
Dec 1 HTTP
D:1
I
01] . 46:02
Edit regular expression:
WARN
Usage of regexp? (match, v do not match
Color, Bell, bell + colorize, execute)
02] s 46:02

```

진단 콘솔로 CC-SG 다시 시작

CC-SG 를 다시 시작하면 모든 현재 CC-SG 사용자가 로그아웃되고 원격 대상 서버에 대한 세션이 종료됩니다.

중요: 진단 콘솔에서 **CC-SG**를 반드시 다시 시작할 필요가 없다면, **Admin** 클라이언트에서 **CC-SG**를 다시 시작하는 것이 좋습니다. **CC-SG 다시 시작 (p. 169)**을 참조하십시오. 진단 콘솔에서 **CC-SG**를 다시 시작해도 사용자에게 다시 시작하고 있음을 알리지 않습니다.

▶ 진단 콘솔로 CC-SG 를 다시 시작하려면:

1. 작업 > 관리자 > CC-SG 다시 시작을 선택합니다.

2. CC-SG 애플리케이션 다시 시작을 클릭하거나 Enter 키를 누릅니다. 다음 화면에서 다시 시작을 확인하여 계속 진행합니다.

```

File  Operation

CC-SG Administrator Console: CC-SG Restart: _____
CC-SG Restart.

This operation will restart the CC-SG Application.

This will log-off all currently active CC-SG GUI users of the system
and terminate any sessions to remote targets that they might have.

They will get no notification that this event will happen.

[It is better to use the CC-SG GUI to do this -- it will provide a
count-down timer and notification of session termination.]

< Restart CC-SG Application > < Cancel >

Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>

```

진단 콘솔로 CC-SG 재부팅

이 옵션을 사용하여 전체 CC-SG 를 재부팅하고 전원 주기를 시뮬레이션할 수 있습니다. 사용자는 통지를 수신하지 않습니다. CC-SG, SSH 및 진단 콘솔 사용자(이 세션 포함)는 로그아웃됩니다. 원격 대상 서버에 대한 연결도 종료됩니다.

▶ CC-SG 를 재부팅하려면:

1. 작업 > 관리자 > CC-SG 시스템 다시 시작을 선택합니다.

2. 시스템 재부팅을 클릭하거나 Enter 키를 눌러 CC-SG 를 재부팅합니다. 다음 화면에서 재부팅을 확인하여 계속 진행합니다.

```

File Operation

CC-SG Administrator Console: CC-SG System Reboot:
CC-SG System Reboot.

This operation will reboot the entire system (simulating a power cycle).

This will log-off all currently active CC-SG GUI, CC-SG SSH and Diagnostic
Console users (including this session) to this system and terminate any
sessions to remote targets that they might have. This could also impact
cluster operations (if so configured).

Users will get no notification that this event will happen.

< REBOOT System > < Cancel >

Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>

```

진단 콘솔에서 CC-SG 시스템 전원 끄기

이 옵션은 CC-SG 장치의 전원을 끕니다. 로그인된 사용자는 통지를 받지 않습니다. CC-SG, SSH 및 진단 콘솔 사용자(이 세션 포함)는 로그오프됩니다. 원격 대상 서버에 대한 연결도 종료됩니다.

장치의 전면 패널에 있는 전원 버튼을 눌러야만 CC-SG 장치의 전원을 다시 켤 수 있습니다.

▶ CC-SG 전원 끄기:

1. 작업 > 관리자 > CC-SG 시스템 전원 끄기를 선택합니다.

2. CC-SG 전원 끄기를 클릭하거나 Enter 키를 눌러 CC-SG 에서 AC 전원을 제거합니다. 다음 화면에서 전원 끄기 작업을 확인하여 계속 진행합니다.

```

File Operation

CC-SG Administrator Console: Power OFF: _____
CC-SG Power OFF.

This operation will turn the AC Power OFF for this CC-SG Unit.

The only way to bring the unit back online is by pressing the
Front Panel Power Button.

All active sessions will be terminated and no notification will given.

The system may take a couple of minutes before it actually powers off.
Please be patient!

< Power OFF the CC-SG > < Cancel >

Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>
    
```

진단 콘솔로 CC 슈퍼 사용자 암호 재설정

이 옵션은 CC-SG 슈퍼 사용자 계정의 암호를 출고 시 값으로 재설정합니다.

출고 시 암호: raritan

참고: 이것은 진단 콘솔 관리자 사용자의 암호가 아닙니다. 진단 콘솔 암호 설정 (p. 251) 을 참조하십시오.

▶ **CC-SG GUI 관리자 암호 재설정:**

1. 작업 > 관리자 > CC-SG 관리자 암호 재설정을 선택합니다.

2. CC-SG GUI 관리자 암호 재설정을 클릭하거나 Enter 키를 눌러 관리자 암호를 출고 시 기본값으로 변경합니다. 다음 화면에서 암호 재설정을 확인하여 계속 진행합니다.

```

File Operation

CC-SG Administrator Console: CC-SG ADMIN Password Reset:
CC-SG Administrator Password Reset.

This operation will reset the password for the ADMIN account of the
CC-SG GUI to the initial Factory Default value.

[Note: This is *NOT* the admin password for Diagnostic Console!
See: ADMIN->DiagCon Passwords->Account Configuration to
change the Diagnostic Console admin password.]

< Reset CC-SG GUI Admin Password > < Cancel >

Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>

```

CC-SG 출고 시 구성(Admin) 재설정

이 옵션은 CC-SG 시스템의 전체 또는 일부를 출고 시 기본값으로 재설정합니다. 모든 활성 CC-SG 사용자는 통지 없이 로그아웃되며 SNMP 처리는 중지됩니다.

선택된 기본 옵션을 사용하는 것이 좋습니다.

옵션	설명
Full CC-SG Database Reset	이 옵션을 선택하면 기존의 CC-SG 데이터베이스가 제거되고 모든 출고 시 기본값으로 새 버전이 빌드됩니다. 네트워크 설정, SNMP 설정, 펌웨어 및 진단 콘솔은 CC-SG 데이터베이스 일부가 아닙니다. IP-ACL 설정은 IP ACL 표 옵션을 선택하든 안하든 간에 전체 데이터베이스 재설정으로 재설정됩니다.

옵션	설명
Preserve CC-SG Personality during Reset	<p>이 옵션은 전체 CC-SG 데이터베이스 재설정을 선택했을 때 활성화됩니다.</p> <p>CC-SG 데이터베이스가 재구축되기 때문에 일부 이전에 구성된 옵션이 저장됩니다.</p> <ul style="list-style-type: none"> ▪ PC 클라이언트와 CC-SG 간의 보안 통신 ▪ 강력한 암호 강제 실행 ▪ 대역외 노드에 대한 직접 대 프록시 연결 ▪ 비활동 타이머 설정
Network Reset	<p>이 옵션은 네트워크 설정을 출고 시 기본값으로 변경합니다.</p> <ul style="list-style-type: none"> ▪ 호스트 이름: CommandCenter ▪ 도메인 이름: localdomain ▪ 모드: 기본/백업 ▪ 구성: 정적 ▪ IP 주소: 192.168.0.192 ▪ 넷마스크: 255.255.255.0 ▪ 게이트웨이: 없음 ▪ 기본 DNS: 없음 ▪ 보조 DNS: 없음 ▪ 어댑터 속도 자동
SNMP Reset	<p>이 옵션은 SNMP 설정을 출고 시 기본값으로 재설정합니다.</p> <ul style="list-style-type: none"> ▪ 포트: 161 ▪ 읽기 전용 커뮤니티: public ▪ 읽기-쓰기 커뮤니티: private ▪ 시스템 담당자, 이름, 위치: 없음 ▪ SNMP 트랩 구성 ▪ SNMP 트랩 대상
Firmware Reset	<p>이 옵션은 모든 장치 펌웨어 파일을 시 기본값으로 재설정합니다. 이 옵션은 CC-SG 데이터베이스를 변경하지 않습니다.</p>
Install Firmware into CC-SG DB	<p>이 옵션은 현재 CC-SG 버전의 펌웨어 파일을 CC-SG 데이터베이스로 로드합니다.</p>
Diagnostic Console Reset	<p>이 옵션은 진단 콘솔 설정을 출고 시 기본값으로 복원합니다.</p>

옵션	설명
IP 액세스 제어 목록 재설정	<p>이 옵션은 IP-ACL 표에서 모든 항목을 제거합니다.</p> <p>IP-ACL 설정은 IP 액세스 제어 목록 재설정 옵션을 선택하든 안하든간에 전체 데이터베이스 재설정으로 재설정됩니다.</p> <p>액세스 제어 목록 (p. 206)을 참조하십시오.</p>

▶ **CC-SG 를 출고 시 구성으로 재설정하려면:**

1. 작업 > 관리자 > 출고 시 재설정을 선택합니다.
2. 재설정 옵션을 선택합니다.
3. 시스템 재설정을 클릭합니다.

진단 콘솔 암호 설정

이 옵션은 암호의 강도(status 및 admin)를 구성하는 기능을 제공하고, 계정 구성 메뉴를 통해 수행해야 하며 암호를 변경하기 전에 경과해야 하는 최대 일 수의 설정 등 암호 속성을 구성할 수 있습니다. 이러한 메뉴의 작업은 진단 콘솔 계정(상태 및 관리자) 및 암호에만 적용됩니다. 일반 CC-SG GUI 계정 또는 암호에는 영향이 없습니다.

▶ **진단 콘솔 암호를 구성하려면:**

1. 작업 > 관리자 > DiagCon 암호 > 암호 구성을 선택합니다.

2. 암호 기록 수준 필드에 기억할 암호 수를 입력합니다. 기본 설정은 5입니다.

```

File Operation

CC-SG Administrator Console: Password Settings:
Use this screen to update how all subsequent Diagnostic Console (only!)
password operations will work. You can set the type of passwords (regular,
strong or random) that the system will let the user use on any subsequent
password change operation. Also, the number of passwords henceforth that
the system will remember and not let the user duplicate or reuse.

Password Configuration:

Password History Depth: [5 ]

Password Type & Parameters:
<o> Regular
< > Random Size:[20 ] Retries:[10 ]
< > Strong Retries:[3 ] DiffOK:[4 ] MinLEN:[9 ]
Digits: [-1 ] Upper: [-1 ] Lower: [-1 ] Other:[-1 ]

< Update >

Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>
    
```

3. admin 및 status 암호의 경우(사용 가능한 경우) Regular, Random 또는 Strong 을 선택합니다.

암호 설정	설명
Regular	표준입니다. 암호는 약간 제한되며 4 자 이상이어야 합니다. 이것은 시스템 기본 암호 구성입니다.
Random	무작위로 생성된 암호를 제공합니다. 비트 단위의 최대 암호 크기(최대값은 14, 최소값은 70, 기본값은 20)를 구성하며 재시도 횟수(기본값은 10)는 새 암호를 승인하려는 경우 확인해야 하는 횟수입니다. 무작위 암호를 승인하거나(새 암호를 두 번 입력) 거부합니다. 사용자 자신의 암호를 설정할 수 없습니다.

암호 설정	설명
Strong	<p>강력한 암호를 강제 실행합니다.</p> <p>재시도는 오류 메시지가 나타나기 전에 프롬프트가 표시되는 횟수입니다.</p> <p>DiffOK 는 이전 암호와 동일한 새 암호의 문자 수입니다.</p> <p>MinLEN 는 암호에 필요한 최소 문자 길이입니다. 암호에 필요한 숫자, 대문자, 소문자 및 기타(특수) 문자를 지정합니다.</p> <p>양수는 이 문자 클래스의 최대 “credit” 수가 “simplicity” 수가 됨을 의미합니다.</p> <p>음수는 암호가 지정된 이 클래스의 문자 수 이상이 되어야 함을 의미합니다. 따라서 -1 은 모든 암호가 1 개 이상의 숫자를 가지고 있어야 함을 의미합니다.</p>

진단 콘솔 계정 구성

기본적으로 **status** 계정은 암호를 필요로 하지 않지만 필요하면 구성할 수는 있습니다. **admin** 암호와 다르게 구성할 수 있으며 필드 지원 계정을 활성화하거나 비활성화할 수 있습니다.

▶ 계정을 구성하려면:

1. 작업 > 관리자 > DiagCon 암호 > 계정 구성을 선택합니다.

2. 나타난 화면에 각 계정의 설정이 표시됩니다. Status, Admin, FS1 및 FS2

```

File Operation

CC-SG Administrator Console: Account Settings:
Account Configuration:
Field: \ User: Status:      Admin:      FS1:      FS2:
User Name:      status      admin      fs1       fs2
Last Changed:   Dec 12, 2006 Dec 12, 2006 Dec 13, 2006 Dec 13, 2006
Expire:         Never       Never      Never     Never

Mode:           < > Disabled      < > Disabled  <o> Disabled
                < > Enabled      <o> Enabled   < > Enabled
                <o> NoPassword

Min Days:       [0      ]      [0      ]
Max Days:       [99999 ]      [99999 ]
Warn:           [7      ]      [7      ]
Max # Logins:   [-1     ]      [2      ]      [1      ]      [0      ]
Update Param:   <UPDATE>   <UPDATE>   <UPDATE>   <UPDATE>
New Password:   <New Password> <New Password>

                < RESET to Factory Password Configuration >

Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>
    
```

이 화면은 세 개의 주요 영역으로 나뉩니다.

- 상단 부분은 시스템의 계정에 대한 읽기 전용 정보를 보여줍니다.
- 중간 부분은 각 ID와 관련된 다양한 매개변수와 버튼 집합을 보여주며, 계정에 대해 새 암호를 제공하거나 매개변수를 업데이트할 수 있습니다.
- 하단 부분은 암호 구성을 출고 시 기본값(또는 처음에 시스템이 제공된 상태)으로 복원합니다.

3. Status 계정의 암호가 필요하다면 그 아래에 있는 사용을 선택합니다.

4. Admin 및 Status 계정의 경우 다음과 같이 구성할 수 있습니다.

설정	설명
User \ User Name	(읽기 전용). 이것은 이 계정에 대한 현재 사용자 이름 또는 ID입니다.
Last Changed	(읽기 전용). 이것은 이 계정에 대한 최근 암호 변경 날짜입니다.
Expire	(읽기 전용). 이 계정에서 암호를 변경해야 하는 날짜를 알려줍니다.

설정	설명
Mode	계정이 비활성화된 경우(로그인 금지), 활성화된 경우(인증 토큰 필요) 또는 액세스가 가능하고 암호가 필요하지 않은 경우 구성 가능한 옵션. (Admin 및 FS1 계정을 동시에 잠그지 마십시오. 그렇지 않으면 진단 콘솔을 사용할 수 없습니다.)
Min Days	암호를 다시 변경하기 전에 암호 변경 이후의 최소 일 수입니다. 기본값은 0입니다.
Max Days	암호가 그대로 유지되는 최대 일 수입니다. 기본값은 99999입니다.
경고	암호가 만료되기 전에 경고 메시지를 보내는 일 수입니다.
Max # of Logins	계정이 허용하는 최대 동시 로그인 수입니다. 음수는 제한 사항 없음을 나타냅니다(-1은 status 로그인의 기본값입니다). 0은 로그인할 수 있는 사용자가 없음을 의미합니다. 양수는 로그인할 수 있는 동시 사용자 수를 정의합니다(2는 admin 로그인의 기본값입니다).
UPDATE	해당 ID에 대한 모든 변경 사항을 저장합니다.
새 암호	계정에 대한 새 암호를 입력합니다.

원격 시스템 모니터링 구성

GKrellM 도구를 사용하여 원격 시스템 모니터링 기능을 활성화할 수 있습니다. GKrellM 도구는 CC-SG 장치에 대한 자원 활용 내용을 그래픽으로 제공합니다. 이 도구는 Windows 작업 관리자의 성능 탭과 유사합니다.

▶ 1: CC-SG 장치에 대한 원격 시스템 모니터링 활성화:

1. 작업 > 유틸리티 > 원격 시스템 모니터링을 선택합니다.
2. 원격 모니터링 서비스에 활성화 필드를 선택합니다.
3. CC-SG 장치를 모니터링할 클라이언트 PC의 IP 주소를 허용된 원격 모니터링 IP 주소 필드에 입력합니다. 3개의 IP 주소까지 입력할 수 있습니다.
4. GKrellM 도구의 기본 포트는 19150이며 포트를 변경할 수 있습니다.
5. 제출을 선택합니다.

▶ **2: 원격 시스템 모니터링 클라이언트 소프트웨어 다운로드:**

1. www.gkrellm.net 로 이동합니다.
2. 클라이언트 PC 에 맞는 패키지를 다운로드하여 설치합니다.

▶ **3: CC-SG 와 작동하도록 원격 시스템 모니터링 클라이언트 구성:**

CC-SG 장치를 모니터링할 대상으로 설정하려면 Read Me 파일의 지침을 따르십시오.

Windows 사용자는 명령줄을 사용하여 Gkrellm 설치 디렉토리를 찾아 Read 에 지정된 명령을 실행해야 합니다.

이력 데이터 추세 구성

CPU 활용, 메모리 활용, 로그 파일 크기 및 시스템 및 각 폴더에 대한 디스크 공간에 대한 정보를 모으기 위해 이력 데이터 추세를 사용할 수 있습니다. 이 정보는 보고서로 변환되어 CC-SG 에서 웹 페이지로 볼 수 있습니다. 보고서에는 CC-SG 의 상태 및 이력 데이터에 대한 링크가 있습니다.

▶ **1: 이력 데이터 추세 활성화:**

1. 작업 > 진단 콘솔 구성을 선택합니다.
2. 포트 목록에서 웹을 선택합니다.
3. 상태 목록에서 웹 옆의 상태 확인란을 선택합니다.
4. 저장을 클릭합니다.

▶ **2: 이력 데이터 추세 보고서 보기:**

1. 지원되는 인터넷 브라우저를 사용하여 이 URL https://<IP_address>/status, 여기서 <IP_address>는 CC-SG 의 IP 주소입니다. 예를 들어, <https://10.0.3.30/status> 입니다.
2. 상태 페이지가 열립니다. 이 페이지에는 상태 콘솔과 동일한 정보가 포함됩니다. **상태 콘솔** (p. 233)을 참조하십시오.
 - CPU 활용, 메모리 활용, 로그 파일 크기, 시스템 및 각 폴더에 대한 디스크 공간에 대한 정보를 보려면 이력 CC-SG 모니터 링크를 클릭합니다. 각 그래프를 클릭하여 새 페이지에서 내역을 표시합니다.

디스크 상태 표시

이 옵션을 사용하여 디스크 크기, 활성 및 가동 상태, RAID-1 의 상태, 다양한 파일 시스템에서 현재 사용되는 공간 크기 등 CC-SG 디스크의 상태를 표시합니다.

▶ CC-SG 의 디스크 상태 표시:

1. 작업 > 유틸리티 > 디스크 상태를 선택합니다.
2. 새로 고침을 클릭하거나 Enter 키를 눌러 표시를 새로 고칩니다. 화면 새로고침 기능은 특히, 업그레이드나 설치 시 또는 RAID 디스크를 새로 작성하거나 동기화할 때 진행 과정을 보는 경우 유용하게 사용됩니다.

```

File Operation

CC-SG Administrator Console: Disk Status:
Personalities : [raid1]
md1 : active raid1 sdb2[1] sda2[0]
      78043648 blocks [2/2] [UU]

md0 : active raid1 sdb1[1] sda1[0]
      104320 blocks [2/2] [UU]

Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/svg-root  4.9G  115M  4.5G   3% /
/dev/md0         99M   9.0M   85M  10% /boot
/dev/mapper/svg-opt  5.8G  334M  5.2G   6% /opt
/dev/mapper/svg-sg   2.9G  195M  2.6G   7% /sg
/dev/mapper/svg-DB   8.7G  286M  8.0G   4% /sg/DB
/dev/mapper/svg-tmp  2.0G  339M  1.6G  18% /tmp
/dev/mapper/svg-usr  2.0G  580M  1.3G  31% /usr
/dev/mapper/svg-var  7.7G  133M  7.2G   2% /var

< Refresh >

Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>

```

참고: 디스크 드라이브는 완전 동기화되고 전체 RAID-1 보호는 위와 같은 화면이 표시될 때 사용할 수 있습니다. md0 및 md1 어레이의 상태는 [UU]입니다.

진단 콘솔로 상단 부분 표시 보기

상단 부분 표시를 이용하여 현재 실행 중인 프로세스의 목록 및 그 속성과 전체 시스템 상태를 볼 수 있습니다.

▶ CC-SG 에서 실행 중인 프로세스를 표시하려면:

1. 작업 > 유틸리티 > 상단 부분 표시를 선택합니다.

2. 전체 실행, 중지, 총 수 및 중지된 프로세스를 봅니다.

```
top - 20:19:27 up 1 day, 23:33, 6 users, load average: 0.55, 0.27, 0.20
Tasks: 117 total, 1 running, 116 sleeping, 0 stopped, 0 zombie
Cpu(s): 5.6% us, 8.6% sy, 0.0% ni, 85.7% id, 0.0% wa, 0.0% hi, 0.0% si
Mem: 2076088k total, 1351804k used, 724284k free, 245720k buffers
Swap: 2031608k total, 0k used, 2031608k free, 795588k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
20271	sg	16	0	275m	26m	11m	S	1.7	1.3	0:14.09	jsvc
4990	root	23	0	5452	3460	1780	S	0.3	0.2	4:30.55	status-poller.p
12634	admin	16	0	2584	960	748	R	0.3	0.0	0:00.01	top
1	root	16	0	2280	544	468	S	0.0	0.0	0:00.79	init
2	root	34	19	0	0	0	S	0.0	0.0	0:00.24	ksoftirqd/0
3	root	5	-10	0	0	0	S	0.0	0.0	0:00.68	events/0
4	root	5	-10	0	0	0	S	0.0	0.0	0:00.00	khelper
5	root	15	-10	0	0	0	S	0.0	0.0	0:00.00	kacpid
25	root	5	-10	0	0	0	S	0.0	0.0	0:00.00	kblockd/0
35	root	15	0	0	0	0	S	0.0	0.0	0:00.12	pdflush
36	root	15	0	0	0	0	S	0.0	0.0	0:01.13	pdflush
38	root	13	-10	0	0	0	S	0.0	0.0	0:00.00	aio/0
26	root	15	0	0	0	0	S	0.0	0.0	0:00.00	khubd
37	root	15	0	0	0	0	S	0.0	0.0	0:00.02	kswapd0
111	root	25	0	0	0	0	S	0.0	0.0	0:00.00	kseriod
181	root	5	-10	0	0	0	S	0.0	0.0	0:00.00	ata/0
183	root	22	0	0	0	0	S	0.0	0.0	0:00.00	scsi_eh_0

3. 상단 명령에 대한 도움말 화면을 보려면 h를 입력합니다.
 도움말을 위한 F1 키가 여기서는 쓰이지 않습니다.

NTP 상태 표시

CC-SG 에서 구성되어 있고 실행 중인 NTP 시간 디먼의 상태를 표시할 수 있습니다. NTP 디먼은 CC-SG 관리자의 GUI 인 Admin 클라이언트에서만 구성할 수 있습니다.

▶ **CC-SG 에 NTP 디먼의 상태 표시:**

1. 작업 > 유틸리티 > NTP 상태 표시를 선택합니다.

- NTP 가 활성화되지 않았거나 적절히 구성되지 않았습니다.

```
File Operation
CC-SG Administrator Console: NTP Status: _____

NTP Daemon does not appear to be running

< Refresh >

Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>
```

- NTP 가 적절히 구성되고 실행 중입니다.

```
File Operation
CC-SG Administrator Console: NTP Status: _____
NTP Daemon PID=17735
synchronised to NTP server (81.0.239.181) at stratum 3
time correct to within 143 ms
polling server every 64 s

-----

client 127.127.1.0
client 81.0.239.181
client 152.118.24.8

remote local st poll reach delay offset disp
=====
=127.127.1.0 127.0.0.1 10 64 377 0.00000 0.000000 0.03061
*81.0.239.181 192.168.51.40 2 64 377 0.13531 -0.026990 0.05887
=152.118.24.8 192.168.51.40 3 64 377 0.39163 -0.039222 0.07307

< Refresh >

Help: <F1> // Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar): <ctl+X>
```

A

V1 및 E1 사양

이 장에서

V1 모델	260
E1 모델	261

V1 모델

V1 일반 사양

폼 팩터	1U
크기(깊이 x 너비 x 높이)	24.21"x 19.09" x 1.75"615 mm x 485 mm x 44 mm
무게	10.80kg
전원	단일 공급 장치(1 x 300watt)
작동 온도	10° - 35° (50° - 95°)
평균 고장 간격 (MTBF)	36,354 시간
KVM 관리 포트	(DB15 + PS2 또는 USB 키보드/마우스)
직렬 관리 포트	DB9
콘솔 포트	(2) USB 2.0 포트

V1 환경 요구사항

작동 중	
습도	8% - 90% RH
고도	모든 고도에서 올바르게 작동 0 ~ 3,048m, 보관 12,192m(예상치)
진동	5-55-5HZ, 0.38 mm, 1 주기당 1 분; 각 축(X,Y,Z)의 경우 30 분
충격	해당 사항 없음
비작동	
온도	-40° - +60° (-40°-140°)

작동 중	
습도	5% - 95% RH
고도	모든 고도에서 올바르게 작동 0 ~ 3,048m, 보관 12,192m(예상치)
진동	5-55-5HZ, 0.38mm, 1 주기당 1 분 각 축(X,Y,Z)의 경우 30 분
충격	해당 사항 없음

E1 모델

E1 일반 사양

폼 팩터	2U
크기(깊이 x 너비 x 높이)	27.05"x 18.7" x 3.46"-687 mm x 475 mm x 88 mm
무게	44.09 lbs-20 kg
전원	SP502-2S 핫스왑 500W 2U 전원 공급 장치
작동 온도	0-50° C
평균 고장 간격(MTBF)	53,564 시간
KVM 관리 포트	PS/2 키보드 및 마우스 포트, 1 VGA 포트
직렬 관리 포트	Fast UART 16550 직렬 포트
콘솔 포트	(2) USB 2.0 포트

E1 환경 요구사항

작동 중	
습도	5-90%, 비응결
고도	해발 213,360.00 cm
진동	각 수직 축(X, Y, Z)에서 1 시간 동안 0.5g 의 일정 가속도로 10Hz - 500Hz 발생
충격	각 수직 축(X, Y, Z)에서 ½ sine 파장과 함께 11ms 동안 5 g

작동 중	
비작동	
온도	-40°-70° C
습도	5-90%, 비응결
고도	해발 12,192m
진동	각 수직 축(X, Y, Z)에서 1 시간 동안 2g 의 일정 가속도로 10Hz - 300Hz 발생
충격	각 수직 축(X, Y, Z)에서 ½ sine 파장과 함께 11ms 동안 30g

B

CC-SG 및 네트워크 구성

이 부록에서는 일반적인 CC-SG 배치의 네트워크 요구사항(주소, 프로토콜, 포트 등)을 설명합니다. 이 부록에는 외부 액세스와 내부 보안 및 라우팅 규정 적용을 위해 네트워크를 구성하는 방법에 대한 정보가 포함되어 있습니다. TCP/IP 네트워크 관리자에게 도움되는 자세한 내용이 제공됩니다. TCP/IP 관리자의 역할 및 책임은 CC-SG 관리자의 역할 및 책임 이상으로 확장할 수 있습니다. 이 부록은 관리자가 CC-SG 및 그 구성요소를 사이트의 보안 액세스 및 라우팅 규정에 포함시키는데 도움을 줍니다.

다음의 표는 CC-SG 및 연관된 구성 요소에 필요한 프로토콜 및 포트를 나타냅니다.

이 장에서

CC-SG 네트워크를 위한 필수 개방 포트: 요약.....	263
CC-SG 통신 채널.....	264

CC-SG 네트워크를 위한 필수 개방 포트: 요약

다음 포트는 열려 있어야 합니다.

포트 번호	프로토콜	용도	내역
80	TCP	CC-SG 에 대한 HTTP 액세스	암호화되지 않음
443	TCP	CC-SG 에 대한 HTTPS(SSL) 액세스	SSL/AES128 암호화됨
8080	TCP	CC-SG - PC 클라이언트	구성된 경우 SSL/AES128 암호화됨
2400	TCP	노드 액세스(프록시 모드)	구성된 경우 SSL/AES128 암호화됨
5000	TCP	노드 액세스(직접 모드)	이러한 포트는 외부 액세스할 Raritan 장치별로 열어야 합니다. 표의 다른 포트는 CC-SG 에 액세스할 경우에만 열어야 합니다. 구성된 경우 AES128 암호화됨

포트 번호	프로토콜	용도	내역
제어 시스템 노드의 경우 80 및 443 가상 호스트 및 가상 시스템 노드의 경우 80, 443, 902 및 903	TCP	가상 노드 액세스	해당 사항 없음
51000	TCP	SX 대상 액세스(직접 모드)	구성된 경우 AES128 암호화됨

▶ 필수 열림 포트에 대한 예외:

포트 80은 CC-SG에 대한 모든 액세스가 HTTPS 주소를 통해 이루어지는 경우 닫을 수 있습니다.

포트 5000 및 51000은 CC-SG 프록시 모드를 방화벽에서 연결하는데 사용하는 경우 닫을 수 있습니다.

CC-SG 통신 채널

각 통신 채널이 문서화됩니다. 각 통신 채널의 경우 표에 다음 사항이 포함됩니다.

- 통신 당사자가 사용하는 심볼 IP 주소 이러한 주소는 개체 사이의 통신 경로에서 허용되어야 합니다.
- 통신이 시작되는 방향 이것은 특정 사이트 규정에 중요할 수 있습니다. 지정된 CC-SG 역할의 경우 해당 통신 당사자 사이의 경로를 사용할 수 있어야 하며 네트워크가 중단되는 경우 대체 리라우트 경로를 사용할 수 있습니다.
- CC-SG에서 사용하는 포트 번호 및 프로토콜
- 포트 구성 가능 여부는 Admin 클라이언트 또는 진단 콘솔이 네트워크에 있는 다른 애플리케이션과의 충돌 때문에 또는 보안상의 이유로 나열된 기본값과 다른 값으로 포트 번호를 변경할 수 있는 필드를 제공함을 의미합니다.
- 통신 방법에 대한 자세한 내용, 통신 채널을 통해 전달되는 메시지 또는 메시지의 암호화

CC-SG 및 Raritan 장치

CC-SG의 기본 역할은 Dominion KX II와 같은 Raritan 장치를 관리 및 제어하는 것입니다. 일반적으로 CC-SG는 TCP/IP 네트워크(로컬, WAN 또는 VPN)에서 이러한 장치와 통신하며 TCP 및 UDP 프로토콜은 다음과 같이 사용됩니다.

통신 방향	포트 번호	프로토콜	구성 가능성	내역
CC-SG → 로컬 방송	5000	UDP	예	하트비트
CC-SG → 원격 LAN IP	5000	UDP	예	하트비트
CC-SG → Raritan 장치	5000	TCP	예	RDM 프로토콜 RC4/AES128 암호화됨
Raritan 장치 → CC-SG	5001	UDP	no	하트비트
CC-SG - Dominion PX	623	UDP	no	

CC-SG 클러스터링

옵션 CC-SG 클러스터링 기능을 사용할 때 다음 포트가 하위 네트워크를 상호 연결하기 위해 사용할 수 있어야 합니다. 옵션 클러스터링 기능이 사용되지 않을 경우 이러한 포트는 열릴 필요가 없습니다.

클러스터의 각 CC-SG 는 별도의 LAN 에 있을 수 있습니다. 그러나 장치 사이의 상호 연결은 안정적이어야 하며 정제되지 않아야 합니다.

통신 방향	포트 번호	프로토콜	구성 가능성	내역
CC-SG → 로컬 방송	10000	UDP	no	하트비트
CC-SG → 원격 LAN IP	10000	UDP	no	하트비트
CC-SG → CC-SG	5432	TCP	no	기본의 HA-JDBC 에서 백업 PostgreSQL DB 서버로 암호화되지 않음
CC-SG → CC-SG	8732	TCP	no	기본-백업 서버 동기화 클러스터링 제어 데이터 교환 MD5 암호화됨
CC-SG → CC-SG	3232	TCP	no	기본-백업 SNMP 동기화 구성 변경 포워딩 암호화되지 않음

인프라 서비스 액세스

CC-SG 는 DHCP, DNS, NTP 등의 여러 업계 표준 서비스를 사용하도록 구성할 수 있습니다. CC-SG 는 이러한 옵션 서버와 통신하기 위해 다음의 포트 및 프로토콜을 사용합니다.

통신 방향	포트 번호	프로토콜	구성 가능성	내역
DHCP 서버 → CC-SG	68	UDP	no	IPv4 DHCP 표준
CC-SG → DHCP 서버	67	UDP	no	IPv4 DHCP 표준
NTP 서버 → CC-SG	123	UDP	no	NTP 표준
CC-SG → DNS	53	UDP	no	DNS 표준

PC 클라이언트 및 CC-SG

PC 클라이언트는 다음 세 가지 모드 중 하나로 CC-SG 에 연결합니다.

- 웹 브라우저를 통한 관리자 또는 액세스 클라이언트 CC-SG 는 브라우저 연결을 위해 SSL v2, SSL v3 및 TLS v1 을 지원합니다. 브라우저에서 이 암호화 방법을 구성할 수 있습니다.
- SSH 를 통한 명령줄 인터페이스(CLI)
- 진단 콘솔

통신 방향	포트 번호	프로토콜	구성 가능성	내역
PC 클라이언트 - CC-SG	443	TCP	no	클라이언트-서버 통신 구성된 경우 SSL/AES128 암호화됨
PC 클라이언트 - CC-SG	80	TCP	no	클라이언트-서버 통신 구성된 경우 SSL/AES128 암호화됨
PC 클라이언트 - CC-SG	8080	TCP	no	클라이언트-서버 통신 구성된 경우 SSL/AES128 암호화됨
PC 클라이언트 → CLI SSH	22	TCP	예	클라이언트-서버 통신 구성된 경우 SSL/AES128 암호화됨

통신 방향	포트 번호	프로토콜	구성 가능성	내역
PC 클라이언트 → 진단 콘솔	23	TCP	예	클라이언트-서버 통신 구성된 경우 SSL/AES128 암호화됨

PC 클라이언트 및 노드

CC-SG 의 다른 중요한 역할은 PC 클라이언트를 다양한 노드에 연결하는 것입니다. 이러한 노드는 Raritan 장치에 대한 직렬 또는 KVM 콘솔 연결(대역외 연결이라고 함)일 수 있습니다. 또 다른 모드는 VNC, RDP 또는 SSH 와 같은 대역내 액세스 방법을 사용하는 것입니다.

PC 클라이언트와 노드 통신의 또 다른 면은 다음과 같습니다.

- PC 클라이언트가 Raritan 장치 또는 대역내 액세스를 통해 노드에 직접 연결합니다. 이를 직접 모드라고 합니다.
- 애플리케이션 방화벽 역할을 하는 CC-SG 를 통해 PC 클라이언트를 대상에 연결합니다. 이것을 프록시 모드라고 합니다.

통신 방향	포트 번호	프로토콜	구성 가능성	내역
클라이언트 → 프록시를 통한 CC-SG → 노드	2400 (CC-SG 에서)	TCP	no	클라이언트-서버 통신 구성된 경우 SSL/AES128 암호화됨
클라이언트 → Raritan 장치 → 대역외 KVM 노드 (직접 모드)	5000 (Raritan 장치에서)	TCP	예	클라이언트-서버 통신 구성된 경우 SSL/AES128 암호화됨
클라이언트 → Raritan Dominion SX 장치 → 대역외 직렬 노드 (직접 모드)	51000 (Raritan 장치에서)	TCP	예	클라이언트-서버 통신 구성된 경우 SSL/AES128 암호화됨

CC-SG 및 IPMI, iLO/RILOE, DRAC, RSA용 클라이언트

CC-SG의 다른 중요한 역할은 iLO/RILOE, Hewlett Packard의 Integrated Lights Out/Remote Insight Lights Out 서버와 같은 타사 장치를 관리하는 것입니다. iLO/RILOE 장치의 대상 전원은 직접 켜지거나 꺼지거나 꺼졌다 켜집니다. IPMI(Intelligent Platform Management Interface) 서버도 CC-SG에서 제어할 수 있습니다. Dell DRAC 및 RSA 대상도 CC-SG에서 관리할 수 있습니다.

통신 방향	포트 번호	프로토콜	구성 가능성	내역
CC-SG → IPMI	623	TCP	no	IPMI 표준
CC-SG → iLO/RILOE(HTTP 포트 사용)	80 또는 443	TCP	no	공급업체 표준
CC-SG ↔ DRAC	80 또는 443	TCP	no	공급업체 표준
CC-SG ↔ RSA	80 또는 443	TCP	no	공급업체 표준

CC-SG 및 SNMP

SNMP(Simple Network Management Protocol)를 사용하여 CC-SG는 SNMP 트랩(이벤트 통지)을 네트워크의 기존 SNMP 관리자로 보낼 수 있습니다. 또한 CC-SG는 HP OpenView와 같은 타사 엔터프라이즈 관리 솔루션을 사용하여 SNMP GET/SET 조작을 지원합니다.

통신 방향	포트 번호	프로토콜	구성 가능성	내역
SNMP 관리자 → CC-SG	161	UDP	예	SNMP 표준
CC-SG → SNMP 관리자	162	UDP	예	SNMP 표준

CC-SG 및 CC-NOC

CC-NOC는 CC-SG와 함께 배치할 수 있는 옵션 어플라이언스입니다. CC-NOC는 서버, 장비 및 CC-SG가 관리하는 Raritan 장치의 상태를 감사 및 모니터링하는 네트워크 모니터링 어플라이언스입니다.

통신 방향	포트 번호	프로토콜	구성 가능성	내역
CC-SG → CC-NOC	9443	TCP	no	NOC 웹 서비스 SSL/AES128 암호화됨

CC-SG 내부 포트

CC-SG 는 이러한 포트에 대한 액세스를 차단하는 내부 기능 및 로컬 방화벽 기능을 위해 여러 포트를 사용합니다. 그러나 일부의 외부 스캐너는 이러한 포트를 "차단됨" 또는 "필터링됨"으로 감지할 수 있습니다. 이러한 포트에 대한 외부 액세스는 필요하지 않으며 차단될 수 있습니다. 현재 사용 중인 포트는 다음과 같습니다.

- 1088
- 1098
- 2222
- 4444
- 4445
- 8009
- 8083
- 8093

이러한 포트 이외에도 CC-SG 는 32xxx(또는 이상) 범위에서 TCP 및 UDP 포트를 열 수 있습니다. 이러한 포트에 대한 외부 액세스는 필요하지 않으며 차단될 수 있습니다.

NAT 사용 방화벽을 통한 CC-SG 액세스

방화벽에서 PAT(Port Address Translation)와 함께 NAT(Network Address Translation)를 사용하는 경우 이 방화벽을 사용하는 모든 연결에 프록시 모드를 사용해야 합니다. 또한 PC 클라이언트가 이러한 포트에서 세션을 시작하기 때문에 포트 80(비 SSL) 또는 443(SSL), 8080 및 2400에 대한 외부 연결을 CC-SG에 전송하도록 방화벽을 구성해야 합니다.

참고: 방화벽을 통해 비 SSL 트래픽을 실행하는 것은 좋지 않습니다.

방화벽을 사용하는 연결은 프록시 모드를 사용하도록 구성해야 합니다. **연결 모드: 직접 및 프록시** (p. 187)를 참조하십시오. CC-SG는 PC 클라이언트 요청 대신 다양한 대상에 연결합니다. 그러나 CC-SG는 방화벽을 통한 PC 클라이언트와 대상 TCP/IP 연결을 종료합니다.

노드에 대한 RDP 액세스

포트 3389는 노드에 대한 RDP 액세스를 위해 열려 있어야 합니다.

노드에 대한 VNC 액세스

포트 5800 또는 5900은 노드에 대한 VNC 액세스를 위해 열려 있어야 합니다.

노드에 대한 SSH 액세스

포트 22는 노드에 대한 SSH 액세스를 위해 열려 있어야 합니다.

원격 시스템 모니터링 포트

원격 시스템 모니터링 기능이 활성화된 경우 포트 19150은 기본적으로 열려 있습니다. **원격 시스템 모니터링 구성** (p. 255)을 참조하십시오.

C

사용자 그룹 권한

이 표는 CC-SG 메뉴 항목에 액세스하는 사용자에게 지정되어야 하는 권한을 보여줍니다.

*없음은 특정 권한이 필요하지 않음을 의미합니다. CC-SG 에 대한 액세스 권한이 있는 사용자는 이러한 메뉴 및 명령을 보고 이에 액세스할 수 있습니다.

메뉴 > 하위 메뉴	메뉴 항목	필수 권한	설명
Secure Gateway	이 메뉴는 모든 사용자가 사용할 수 있습니다.		
	내 프로필	없음*	
	오늘의 메시지	없음*	
	인쇄	없음*	
	로그아웃	없음*	
	종료	없음*	
사용자	이 메뉴와 사용자 트리는 사용자 관리 권한을 가진 사용자만 사용할 수 있습니다.		
> 사용자 관리자	> 사용자 추가	사용자 관리	
	(사용자 편집)	사용자 관리	사용자 프로필 사용
	> 사용자 삭제	사용자 관리	
	> 그룹에서 사용자 삭제	사용자 관리	
	> 사용자 로그아웃	사용자 관리	
	> 대량 복사	사용자 관리	
> 사용자 그룹 관리자	> 사용자 그룹 추가	사용자 관리	
	(사용자 그룹 편집)	사용자 관리	사용자 그룹 프로필을 통해
	> 사용자 그룹 삭제	사용자 관리	
	> 그룹에 사용자 할당	사용자 관리	

C: 사용자 그룹 권한

메뉴 > 하위 메뉴	메뉴 항목	필수 권한	설명
	> 사용자 로그아웃	사용자 관리	
	노드 감사	사용자 관리	
장치	이 메뉴와 장치 트리는 다음 권한 중 하나를 가진 사용자만 사용할 수 있습니다. 장치, 포트 및 노드 관리 장치 구성 및 업그레이드 관리		
	장치 검색	장치, 포트 및 노드 관리	
> 장치 관리자	> 장치 추가	장치, 포트 및 노드 관리	
	(장치 편집)	장치, 포트 및 노드 관리	장치 프로필 사용
	> 장치 삭제	장치, 포트 및 노드 관리	
	> 대량 복사	장치, 포트 및 노드 관리	
	> 장치 업그레이드	장치 구성 및 업그레이드 관리	
>> 구성	>> 백업	장치 구성 및 업그레이드 관리	
	>> 복원	장치 구성 및 업그레이드 관리	
	>> 구성 복사	장치 구성 및 업그레이드 관리	
	> 장치 다시 시작	장치, 포트 및 노드 관리 또는 장치 구성 및 업그레이드 관리	
	> 장치 핑	장치, 포트 및 노드 관리 또는 장치 구성 및 업그레이드 관리	
	> 관리 일시 중지	장치, 포트 및 노드 관리 또는 장치 구성 및 업그레이드 관리	
	> 장치 전원 관리자	장치, 포트 및 노드 관리	

메뉴 > 하위 메뉴	메뉴 항목	필수 권한	설명
	> 관리 시작	장치, 포트 및 노드 관리 또는 장치 구성 및 업그레이드 관리	
	> 사용자 스테이션 관리 시작		
	> 사용자 연결 해제	장치, 포트 및 노드 관리 또는 장치 구성 및 업그레이드 관리	
	> 분포도 보기	장치, 포트 및 노드 관리	
> 보기 변경	> 사용자 정의 보기 생성	장치, 포트 및 노드 관리 또는 장치 구성 및 업그레이드 관리	
	> 트리 보기	장치, 포트 및 노드 관리 또는 장치 구성 및 업그레이드 관리	
> 포트 관리자	> 연결	장치, 포트 및 노드 관리	
	> 포트 구성	장치, 포트 및 노드 관리	
	> 책갈피 포트	장치, 포트 및 노드 관리	
	> 포트 연결 해제	장치, 포트 및 노드 관리	
	> 대량 복사	장치, 포트 및 노드 관리	
	> 포트 삭제	장치, 포트 및 노드 관리	
> 포트 정렬 옵션	> 포트 이름별	장치, 포트 및 노드 관리 또는 장치 구성 및 업그레이드 관리	
	> 포트 상태별	장치, 포트 및 노드 관리 또는 장치 구성 및 업그레이드 관리	

C: 사용자 그룹 권한

메뉴 > 하위 메뉴	메뉴 항목	필수 권한	설명
노드	이 메뉴와 노드 트리는 다음 권한 중 하나를 가진 사용자만 사용할 수 있습니다. 장치, 포트 및 노드 관리 대역내 노드 액세스 대역외 노드 액세스 노드 전원 제어		
	노드 추가	장치, 포트 및 노드 관리	
	(노드 편집)	장치, 포트 및 노드 관리	노드 프로필 사용
	노드 삭제	장치, 포트 및 노드 관리	
	<interfaceName>	대역내 액세스 대역외 액세스	
	연결 해제	대역내 액세스 대역외 액세스	
	가상화	장치, 포트 및 노드 관리	
	대량 복사	장치, 포트 및 노드 관리	
	전원 제어	전원 제어	
	그룹 전원 제어	전원 제어	
	서비스 계정	장치, 포트 및 노드 관리	
	서비스 계정 지정	장치, 포트 및 노드 관리	
> 노드 정렬 옵션	> 노드 이름별	다음 권한 중 하나: 장치, 포트 및 노드 관리 또는 대역내 액세스 대역외 액세스 또는 전원 제어	

메뉴 > 하위 메뉴	메뉴 항목	필수 권한	설명
	> 노드 상태별	다음 권한 중 하나: 장치, 포트 및 노드 관리 또는 대역내 노드 액세스 또는 대역외 노드 액세스 또는 노드 전원 제어	
> 채팅	> 채팅 시작	대역내 노드 액세스 또는 대역외 노드 액세스 또는 노드 전원 제어	
	> 채팅 세션 표시	대역내 노드 액세스 또는 대역외 노드 액세스 또는 노드 전원 제어	
	> 채팅 세션 종료	대역내 노드 액세스 또는 대역외 노드 액세스 또는 노드 전원 제어	
> 보기 변경	> 사용자 정의 보기 생성	다음 권한 중 하나: 장치, 포트 및 노드 관리 또는 대역내 노드 액세스 또는 대역외 노드 액세스 또는 노드 전원 제어	
	> 트리 보기	다음 권한 중 하나: 장치, 포트 및 노드 관리 또는 대역내 노드 액세스 또는 대역외 노드 액세스 또는 노드 전원 제어	
연관체	이 메뉴는 사용자 보안 관리 권한을 가진 사용자만 사용할 수 있습니다.		

C: 사용자 그룹 권한

메뉴 > 하위 메뉴	메뉴 항목	필수 권한	설명
	> 연관체	사용자 보안 관리	추가, 수정 및 삭제 기능 포함
	> 장치 그룹	사용자 보안 관리	추가, 수정 및 삭제 기능 포함
	> 노드 그룹	사용자 보안 관리	추가, 수정 및 삭제 기능 포함
	> 규정	사용자 보안 관리	추가, 수정 및 삭제 기능 포함
보고서	이 메뉴는 모든 사용자가 사용할 수 있습니다.		
	감사 추적	CC 설정 및 제어	
	오류 로그	CC 설정 및 제어	
	액세스 보고서	장치, 포트 및 노드 관리	
	가용성 보고서	장치, 포트 및 노드 관리 또는 장치 구성 및 업그레이드 관리	
> 사용자	> 활성 사용자	사용자 관리	
	> 잠겨 있는 사용자	CC 설정 및 제어	
	> 모든 사용자 데이터	모든 사용자 데이터 보기: 사용자 관리 사용자 자신의 사용자 데이터 보기: 없음	
	> 사용자 그룹 데이터	사용자 관리	
> 장치	> 장치 자산 보고서	장치, 포트 및 노드 관리	
	> 장치 그룹 데이터	장치, 포트 및 노드 관리	
	> 질의 포트	장치, 포트 및 노드 관리	
> 노드	> 노드 자산 보고서	장치, 포트 및 노드 관리	
	> 활성 노드	장치, 포트 및 노드 관리	

메뉴 > 하위 메뉴	메뉴 항목	필수 권한	설명
	> 노드 생성	장치, 포트 및 노드 관리	
	> 노드 그룹 데이터	장치, 포트 및 노드 관리	
> Active Directory	AD 사용자 그룹 보고서		
	예약된 보고서	CC 설정 및 제어	
	CC-NOC 동기화	CC 설정 및 제어	
액세스			
	CC-NOC 구성	CC 설정 및 제어	
	웹 서비스 API 추가	CC 설정 및 제어	
관리	이 메뉴는 다음 권한 중 하나를 가진 사용자만 사용할 수 있습니다. CC 설정 및 제어 장치, 포트 및 노드 관리, 사용자 관리, 사용자 보안 관리의 조합		
	설정 안내	다음 권한 모두: 장치, 포트 및 노드 관리, 사용자 관리, 사용자 보안 관리	
	오늘의 메시지 설정	CC 설정 및 제어	
	애플리케이션	CC 설정 및 제어	
	펌웨어	장치, 포트 및 노드 관리	
	구성	CC 설정 및 제어	
	보안	CC 설정 및 제어	
	통지	CC 설정 및 제어	
	작업	CC 설정 및 제어	
	호환성 매트릭스	장치 구성 및 업그레이드 관리	
시스템 정비			
	백업	CC 설정 및 제어	
	복원	CC 설정 및 제어	

C: 사용자 그룹 권한

메뉴 > 하위 메뉴	메뉴 항목	필수 권한	설명
	재설정	CC 설정 및 제어	
	다시 시작	CC 설정 및 제어	
	업그레이드	CC 설정 및 제어	
	종료	CC 설정 및 제어	
> 정비 모드	> 정비 모드 시작	CC 설정 및 제어	
	> 정비 모드 종료	CC 설정 및 제어	
보기		없음*	
창		없음*	
도움말		없음*	

D

SNMP 트랩

CC-SG 는 다음과 같은 SNMP 트랩을 제공합니다.

SNMP 트랩	설명
ccUnavailable	CC-SG 애플리케이션을 사용할 수 없습니다.
ccAvailable	CC-SG 애플리케이션이 사용 가능합니다.
ccUserLogin	CC-SG 사용자가 로그인했습니다.
ccUserLogout	CC-SG 사용자가 로그아웃했습니다.
ccPortConnectionStarted	CC-SG 세션이 시작되었습니다.
ccPortConnectionStopped	CC-SG 세션이 중지되었습니다.
ccPortConnectionTerminated	CC-SG 세션이 종료되었습니다.
ccImageUpgradeStarted	CC-SG 이미지 업그레이드가 시작되었습니다.
ccImageUpgradeResults	CC-SG 이미지 업그레이드 결과입니다.
ccUserAdded	CC-SG 에 새 사용자가 추가되었습니다.
ccUserDeleted	CC-SG 에서 사용자가 삭제되었습니다.
ccUserModified	CC-SG 사용자가 수정되었습니다.
ccUserAuthenticationFailure	CC-SG 사용자 인증에 실패했습니다.
ccLanCardFailure	CC-SG 가 LAN 카드 오류를 탐지했습니다.
ccHardDiskFailure	CC-SG 가 하드 디스크 오류를 탐지했습니다.
ccLeafNodeUnavailable	CC-SG 가 리프 노드에 대한 연결 장애를 탐지했습니다.
ccLeafNodeAvailable	CC-SG 가 도달할 수 있는 리프 노드를 탐지했습니다.
ccIncompatibleDeviceFirmware	CC-SG 가 호환되지 않는 펌웨어로 장치를 탐지했습니다.
ccDeviceUpgrade	CC-SG 가 장치의 펌웨어를 업그레이드했습니다.
ccEnterMaintenanceMode	CC-SG 가 정비 모드를 시작했습니다.
ccExitMaintenanceMode	CC-SG 가 정비 모드를 종료했습니다.
ccUserLockedOut	CC-SG 사용자가 잠겼습니다.
ccDeviceAddedAfterCCNOCNotification	CC-NOC 에서 통지를 수신한 후 CC-SG 가 장치를 추가했습니다.

D: SNMP 트랩

SNMP 트랩	설명
ccScheduledTaskExecutionFailure	예약된 작업이 실패한 이유입니다.
ccDiagnosticConsoleLogin	사용자가 CC-SG 진단 콘솔에 로그인했습니다.
ccDiagnosticConsoleLogout	사용자가 CC-SG 진단 콘솔을 로그아웃했습니다.
ccNOCAvailable	CC-SG 에서 CC-NOC 가 사용 가능함을 탐지했습니다.
ccNOCUnavailable	CC-SG 에서 CC-NOC 가 사용 불가능함을 탐지했습니다.
ccUserGroupAdded	CC-SG 에 새 사용자 그룹이 추가되었습니다.
ccUserGroupDeleted	CC-SG 사용자 그룹이 삭제되었습니다.
ccUserGroupModified	CC-SG 사용자 그룹이 수정되었습니다.
ccSuperuserNameChanged	CC-SG 슈퍼 사용자 이름이 변경되었습니다.
ccSuperuserPasswordChanged	CC-SG 슈퍼 사용자 암호가 변경되었습니다.
ccLoginBannerChanged	CC-SG 로그인 배너가 변경되었습니다.
ccMOTDChanged	CC-SG 오늘의 메시지(MOTD)가 변경되었습니다.
ccDominionPXReplaced	Dominion PX 장치가 다른 Dominion PX 장치로 대체되었습니다.
ccSystemMonitorNotification	CC-SG 의 메모리가 부족합니다.

E

문제 해결

웹 브라우저에서 CC-SG 를 시작하려면 Java 플러그인이 필요합니다. 시스템 버전이 잘못된 경우 CC-SG 가 설치 단계를 안내합니다. 시스템에 Java 플러그인이 없으면 CC-SG 가 자동으로 시작되지 않습니다. 이런 경우 기존 Java 버전을 제거하거나 비활성화하고 CC-SG 에 대한 직접 포트 연결을 제공하여 정상적인 작동이 가능하도록 합니다.

- CC-SG 가 로드되지 않은 경우 웹 브라우저 설정을 확인합니다.
 - Internet Explorer 에서 Java(Sun)가 활성화되었는지 확인합니다.
 - 제어판에서 Java 플러그인을 열고 브라우저의 설정을 조정합니다.
- 장치 추가에 문제가 있는 경우 장치에 올바른 펌웨어 버전이 있는지 확인합니다.
- 장치와 CC-SG 간의 네트워크 인터페이스 케이블이 연결되어 있지 않으면 하드비트 간격(분)이 구성되기를 기다렸다가 네트워크 인터페이스 케이블을 다시 플러그인합니다. 하드비트 간격을 구성하는 중에 장치는 독립형 모드에서 작동하며 RRC, MPC, RC 등을 통해 액세스할 수 있습니다.
- 클라이언트 버전이 서버 버전과 다르고 예상치 않은 동작이 수행되었다는 메시지가 표시되면 브라우저의 캐시 및 Java 캐시를 지우고 브라우저를 시작해야 합니다. *브라우저의 캐시 지우기* (참조 "브라우저 캐시 지우기" p. 171) 및 *Java 캐시 지우기* (p. 171)를 참조하십시오.

F

두 요소 인증

CC-SG 는 연관된 RSA 인증 관리자를 통해 두 요소 인증을 지원하는 RSA RADIUS 서버를 가리키도록 구성할 수 있습니다. CC-SG 는 RADIUS 클라이언트 역할을 하며 사용자 인증 요청을 RSA RADIUS 서버에 보냅니다. 인증 요청에는 사용자 id, 고정 암호 및 동적 코드가 포함됩니다.

이 장에서

두 요소 인증을 위한 지원 환경	282
두 요소 인증 설정 요구사항.....	282
두 요소 인증의 알려진 문제.....	283

두 요소 인증을 위한 지원 환경

다음 RSA 두 요소 인증 구성요소는 CC-SG 와 상호 작용하는 것으로 알려져 있습니다.

- Windows Server 2003 의 RSA RADIUS Server 6.1
- Windows Server 2003 의 RSA Authentication Manager 6.1
- RSA Secure ID SID700 하드웨어 토큰

또한 이전 RSA 제품 버전은 CC-SG 와 상호 작용해야 하지만 확인되지 않았습니다.

두 요소 인증 설정 요구사항

두 요소 인증 설정을 위해 다음 작업을 완료해야 합니다. RSA 설명서를 참조하십시오.

1. 토큰을 가져옵니다.
2. CC-SG 사용자를 생성하고 사용자에게 토큰을 지정합니다.
3. 사용자 암호를 생성합니다.
4. RADIUS 서버의 에이전트 호스트를 생성합니다.
5. CC-SG 의 에이전트 호스트(유형: 통신 서버)를 생성합니다.
6. RADIUS CC-SG 클라이언트를 생성합니다.

두 요소 인증의 알려진 문제

챌린지 암호/PIN 이 필요한 RSA RADIUS "새 사용자 번호" 모드가 작동하지 않습니다. 대신 이 시스템의 모든 사용자에게 고정 암호를 지정해야 합니다.

G

자주 묻는 질문

이 장에서

일반 FAQ	284
인증 FAQ	286
보안 FAQ	287
회계 FAQ	288
성능 FAQ	289
그룹화 FAQ.....	289
상호 운용성 FAQ.....	290
인증 FAQ	291
사용자 경험 FAQ.....	291

일반 FAQ

질문	답변
일반	
CC-SG 란 무엇입니까?	CC-SG 는 일반적으로 데이터 센터에 배치되고 Raritan IP 를 사용한 제품에 연결된 다중 서버와 네트워크 장비를 집계하여 통합하기 위한 네트워크 관리 장치입니다.
CC-SG 가 필요한 이유는 무엇입니까?	더 많은 데이터 센터 서버와 장치를 배치할수록 이들에 대한 관리는 상당히 복잡해집니다. CC-SG 를 사용하여 시스템 관리자나 매니저는 모든 서버, 장비, 사용자를 단일 장치에서 액세스하고 관리할 수 있습니다.
CommandCenter NOC 란?	CommandCenter NOC 는 감사용 장치를 모니터링하고 CC-SG 가 액세스를 제공하는 서버, 장비 및 Raritan 장치의 상태를 모니터링하는 네트워크입니다.
CC-SG 가 지원하는 Raritan 제품은 무엇입니까?	Raritan 웹 사이트의 펌웨어 및 설명서 아래의 지원 섹션에서 호환성 매트릭스를 참조하십시오.
CC-SG 는 다른 Raritan 제품과 어떻게 통합됩니까?	CC-SG 는 알려진 네트워크 주소가 있는 선택된 Raritan 장치를 식별하고 연결하는 고유의 검색 및 발견 기술을 사용합니다. 일단 CC-SG 가 연결 및 구성되면 CC-SG 에 연결된 장치는 명백하고 작동과 관리가 매우 단순해집니다.

질문	답변
CC-SG 의 상태는 Proxy 해주는 장치의 상태의 제한을 받습니까?	아니오. CC-SG 소프트웨어는 전용 서버에 상주하기 때문에 CC-SG 가 프록시를 제공하는 장치가 꺼진 경우에도 여전히 CC-SG 에 액세스할 수 있습니다.
새 CC-SG 소프트웨어 버전이 사용 가능하게 되면 새 버전으로 업데이트할 수 있습니까?	예. 공인 Raritan 대리점이나 Raritan, Inc.에 직접 문의하시기 바랍니다.
몇 대의 대상 장치(포트) 및/또는 Dominion 장치, IP-Reach 장치를 CC-SG 에 연결할 수 있습니까?	연결할 수 있는 노드 및/또는 Dominion, IP-Reach 장치의 수에는 제한이 없지만 무제한 허용되는 것은 아닙니다. 프로세서 성능과 호스팅 서버의 메모리 양에 따라 실제로 연결할 수 있는 노드 수가 결정됩니다.
Microsoft Internet Explorer 가 기본 웹 브라우저인 경우 그 성능을 최적화할 방법이 있습니까?	콘솔에 액세스할 때 Microsoft IE 의 성능을 높이려면 Java JIT 컴파일러 사용(시스템 재시작 필요), Java 사용 기록 남김 및 Java 콘솔 사용(시스템 재시작 필요) 옵션을 비활성화해야 합니다. 기본 메뉴 모음에서 도구 > 인터넷 옵션 > 고급을 선택합니다. 위 항목이 보일 때까지 아래로 스크롤한 후 해당 항목이 선택 해제되었는지 확인합니다.
콘솔/직렬 포트를 CC-SG 에 추가할 수 없는 경우 어떻게 해야 합니까?	콘솔/직렬 장치가 Dominion 이라고 가정할 때 다음 조건에 부합하는지 확인하십시오 - Dominion 장치가 활성화 상태입니다. - Dominion 장치가 구성된 사용자 계정의 최대 수에 도달하지 않았습니다.
Raritan CC-SG 는 어떤 버전의 Java 를 지원합니까?	Raritan 웹 사이트의 펌웨어 및 설명서 아래에 지원 섹션에서 호환성 매트릭스를 참조하십시오.
관리자가 새 노드를 CC-SG 데이터베이스에 추가하고 나에게 지정했습니다. 내 포트 트리에서 새 포트를 볼 수 있습니까?	트리를 업데이트하여 새로 지정된 노드를 보려면 도구 모음에서 새로 고침 단축 버튼을 클릭합니다. CC-SG 를 새로 고치면 모든 현재 콘솔 세션이 닫힌다는 점을 기억하십시오.

G: 자주 묻는 질문

질문	답변
Windows 데스크탑은 앞으로 어떻게 지원될 예정입니까?	<p>방화벽에 올바른 포트를 구성하여 방화벽 외부에서 CC-SG 에 액세스할 수 있습니다. 표준 포트는 다음과 같습니다.</p> <p>80: 웹 브라우저를 통한(HTTP) 액세스의 경우 443: 웹 브라우저를 통한 HTTPS 액세스의 경우 8080: CC-SG 서버 작업의 경우 2400: 프록시 모드 연결용 5001: IPR/DKSX/DKX/ P2-SC 이벤트 통지용</p> <p>두 클러스터 노드 사이에 방화벽이 있는 경우, 다음 포트는 클러스터가 올바르게 작동할 수 있도록 열려 있어야 합니다.</p> <p>8732: 클러스터 노드 하트비트의 경우 5432: 클러스터 노드 DB 복제용</p>
대규모 시스템을 위한 설계 지침은 무엇입니까? 제한이나 전제가 있습니까?	<p>Raritan 은 서버 확장성을 위해 데이터 센터 모델과 네트워크 모델이라는 두 가지 모델을 제공합니다.</p> <p>데이터 센터 모델은 Paragon 을 사용하여 단일 데이터 센터에서 수천 개 시스템으로 확장합니다. 이것은 단일 위치를 확장하는 가장 효과적이고 비용 효율적인 방법입니다. IP-Reach 및 IP User Station (UST-IP) 이 있는 네트워크 모델도 지원됩니다.</p> <p>네트워크 모델은 TCP/IP 네트워크 사용을 통해 확장하며 CC-SG 를 통해 액세스를 집계합니다. 따라서 사용자는 IP 주소나 액세스 장치의 분포도를 몰라도 됩니다. 또한 단일 사용승인(SSO)의 편리성도 제공합니다.</p>

인증 FAQ

질문	답변
인증	

질문	답변
CC-SG 에 몇 개의 사용자 계정을 만들 수 있습니까?	라이선스 제한을 확인하십시오. CC-SG 에 만들 수 있는 사용자 계정의 수에 지정된 제한은 없지만 무제한 허용되는 것은 아닙니다. 데이터베이스 크기, 프로세서 성능, 호스팅 서버의 메모리 양에 따라 실제로 만들 수 있는 사용자 계정 수가 결정됩니다.
특정 노드 액세스를 특정 사용자에게 배정할 수 있습니까?	예, 관리자 권한이 있으면 가능합니다. 관리자는 각 사용자에게 특정 노드를 배정할 수 있습니다.
사용자가 1,000 명 이상 있는 경우 어떻게 관리합니까? Active Directory 를 지원합니까?	CC-SG 는 Microsoft Active Directory, Sun iPlanet 또는 Novell eDirectory 와 작동합니다. 사용자 계정이 인증 서버에 이미 존재하면 CC-SG 는 AD/TACACS+ /RADIUS/LDAP 인증을 사용하여 원격 인증을 지원합니다.
디렉터리 서비스 및 LDAP, AD, RADIUS 등과 같은 보안 도구를 사용한 인증에는 어떤 옵션을 사용할 수 있습니까?	CC-SG 는 원격 인증뿐 아니라 로컬 인증도 허용합니다. 지원되는 원격 인증 서버에는 다음이 포함됩니다: AD, TACACS+, RADIUS 및 LDAP.

보안 FAQ

질문	답변
보안	
로그온할 때 사용자 이름 및 암호를 정확하게 입력했는데도 "로그인이 올바르지 않다"는 메시지가 나타납니다. 왜 그렇습니까?	CC-SG 에 로그온을 시작할 때마다 전송되는 세션 고유의 ID 가 있습니다. 이 ID 에는 시간 제한 기능이 있으므로 시간 초과가 발생하기 전에 장치에 로그온하지 않으면 세션 ID 는 유효하지 않게 됩니다. Shift-다시 로드를 수행하여 CC-SG 에서 페이지를 새로고침하거나 현재 브라우저를 닫은 후 새 브라우저를 열고 다시 로그온합니다. 그러면 추가 보안 기능이 제공되어 다른 사람이 웹 캐시에 저장된 정보를 재호출하여 장치에 액세스할 수 없게 됩니다.
암호 보안은 어떻게 유지됩니까?	암호는 일방 해시인 MD5 암호화를 사용하여 암호화됩니다. 이 암호화는 권한이 없는 사용자가 암호 목록에 액세스하지 못하도록 방지하는 추가 보안을 제공합니다.

G: 자주 묻는 질문

질문	답변
얼마간 워크스테이션을 사용하지 않다가 CC-SG의 메뉴를 클릭했을 때 가끔 "No longer logged in (더 이상 로그인되지 않음)"이라는 메시지가 나타납니다. 왜 그렇습니까?	CC-SG times each user session. 사전 정의된 기간 동안 활동이 발생하지 않으면 CC-SG는 사용자를 로그아웃 처리합니다. 시간의 길이는 60분으로 사전 설정되어 있지만 재구성할 수 있습니다. 사용자가 세션을 종료할 때 CC-SG를 종료하는 것이 좋습니다.
Raritan이 서버에 루트 액세스가 가능하므로 정부 기관과 문제가 발생할 수 있습니다. 고객도 루트 액세스가 가능합니까? 또는 Raritan이 감사/회계 방법을 제공합니까?	장치가 Raritan, Inc.에서 출고된 후에는 아무도 서버에 루트 액세스할 수 없습니다.
SSL 암호화는 외부적인 동시에 내부적입니까(WAN 뿐 아니라 LAN에도 적용됩니까)?	둘 다 적용됩니다. 세션은 소스(LAN 또는 WAN)에 상관 없이 암호화됩니다.
CC-SG는 CRL 목록(유효하지 않은 인증서의 LDAP 목록)을 지원합니까?	아니요
CC-SG는 클라이언트 인증서 요청을 지원합니까?	아니요

회계 FAQ

질문	답변
회계	
감사 추적 보고서의 이벤트 시간은 부정확한 것처럼 보입니다. 왜 그렇습니까?	로그 이벤트 시간은 클라이언트 컴퓨터의 시간 설정에 따라 로그됩니다. 컴퓨터의 시간 및 날짜 설정을 조정할 수 있습니다.
감사/로그 기능은 전원 플러그의 스위치를 켜거나 끈 사람을 추적할 수 있습니까?	직접 전원 스위치 끄기는 로그되지 않지만 CC-SG를 통한 전원 제어는 감사 로그에 로그될 수 있습니다.

성능 FAQ

질문	답변
성능	
CC-SG 관리자로서 500 개 이상의 노드를 추가하고 모두 자신에게 배정했습니다. 이제는 CC-SG 에 로그인하는 데 시간이 오래 걸립니다.	관리자가 많은 노드를 자신에게 배정한 경우 CC-SG 는 로그인 프로세스 중에 모든 노드에 대한 전체 포트 정보를 다운로드하므로 프로세스가 상당히 느려집니다. CC-SG 구성/설정 관리에 주로 사용하는 관리자 계정에는 많은 노드를 배정하지 않는 것이 좋습니다.
클라이언트당 대역폭 사용은 어떻게 됩니까?	TCI/IP 를 통한 직렬 콘솔 원격 액세스는 텔넷 세션과 대체로 동일한 수준의 네트워크 활동입니다. 하지만 콘솔 포트 자체의 RS232 대역폭 및 SSL/TCP/IP 오버헤드에 제한됩니다. Raritan 원격 클라이언트(RRC)는 KVM 콘솔에 대한 원격 액세스를 제어합니다. 이 애플리케이션은 LAN 수준부터 원격 전화접속 사용자에게 적합한 수준까지 조정할 수 있는 대역폭을 제공합니다.

그룹화 FAQ

질문	답변
그룹화	
특정 서버를 둘 이상의 그룹에 넣을 수 있습니까?	예. 한 사용자가 여러 그룹에 속할 수 있듯이 한 장치는 여러 그룹에 속할 수 있습니다. 예를 들어, NYC 내의 Sun 은 Group Sun 의 일부일 수 있습니다: "Ostype = Solaris" 및 Group New York: "location = NYC"

G: 자주 묻는 질문

질문	답변
<p>콘솔 포트의 활성화 사용을 통해 다른 사용이 차단된다면(예를 들어, 네트워크 인터페이스를 통해 관리를 허용하지 않는 일부 이기종 UNIX의 경우) 다른 사용에는 어떤 영향이 있습니까?</p>	<p>콘솔은 일반적으로 가장 안전하고 신뢰성 있는 액세스 경로로 간주됩니다. 일부 UNIX 시스템은 콘솔에서만 루트 로그인을 허용합니다. 보안상의 이유로, 다른 시스템은 다중 로그인을 금지하여 관리자가 콘솔에 로그인한 경우 다른 액세스를 거부합니다. 결국, 관리자는 콘솔에서 필요한 경우 네트워크 인터페이스를 비활성화하여 다른 모든 액세스를 차단할 수도 있습니다.</p> <p>콘솔에서 정상적인 명령 활동은 다른 인터페이스에서 실행하는 동등한 명령보다 더 큰 영향을 미치는 것은 아닙니다. 하지만 네트워크에 종속적이기 때문에 네트워크 로그인에 응답할 수 없을 정도로 과부하된 시스템도 여전히 콘솔 로그인을 지원할 수 있습니다. 따라서 콘솔 액세스의 또 다른 장점은 시스템 및 네트워크 문제를 진단하고 해결하는 것입니다.</p>
<p>논리 데이터베이스에 대한 변경 사항으로 물리적 수준에서 이동/교환된 CIM의 문제에 대해서는 어떤 해결 방법을 권장합니까? 예를 들어, 대상 서버가 있는 CIM을 하나의 포트에서 동일 장치 혹은 다른 장치의 다른 포트로 물리적 이동한다면 어떻게 됩니까? 포트 이름은 어떻게 됩니까? 노드는 어떻게 됩니까? 인터페이스는 어떻게 됩니까?</p>	<p>각 CIM에는 일련번호와 대상 시스템 이름이 포함됩니다. 시스템은 스위치 간에 연결을 이동할 때 CIM은 이름이 지정된 대상에 연결을 유지한다고 가정합니다. 이 이동은 CC-SG에서 포트 및 인터페이스에 자동으로 반영되고, 포트 이름 및 인터페이스 이름은 변경 사항을 반영하도록 업데이트됩니다. 인터페이스는 포트에 연결된 노드 아래에 표시됩니다. 그러나 노드 이름은 변경되지 않습니다. 수동으로 노드를 편집하여 노드 이름을 변경해야 합니다. 이 경우는 모든 관련 포트가 이미 구성되어 있다고 가정합니다. 대상 서버 및 CIM을 미구성 포트에 물리적으로 이동할 경우 CC-SG에서 포트를 구성할 수 있으며 노드는 자동으로 생성됩니다.</p>

상호 운용성 FAQ

질문	답변
상호 운용성	
CC-SG는 블레이드 새시 제품과 어떻게 통합됩니까?	CC-SG는 KVM 또는 직렬 인터페이스를 투명 통과 지점으로 사용하는 모든 장치를 지원할 수 있습니다.

질문	답변
CC-SG 는 타사 KVM 도구와 어떤 수준으로 통합할 수 있습니까(타사 KVM 포트 수준으로 하향 또는 단순히 장치 수준으로)?	타사 KVM 공급업체가 타사 KVM 스위치용 통신 프로토콜을 공개하지 않을 때 타사 KVM 스위치 통합은 일반적으로 키보드 매크로를 통해 수행됩니다. 타사 KVM 스위치의 기능에 따라 통합의 긴밀성이 달라집니다.
IP-Reach 장치를 통한 4 개 동시 경로의 제한(잠재적 8 경로 장치의 로드맵 포함)을 어떻게 완화할 수 있습니까?	현재 가능한 한 최선의 구현은 IP-Reach 장치를 CC-SG 와 함께 집계하는 것입니다. 앞으로 Raritan 은 장치당 동시 액세스 경로를 증가시킬 계획입니다. 다른 프로젝트의 우선순위 때문에 이 계획은 아직 개발을 완료하지 못했지만 8 경로 솔루션의 시장 수요와 사용 사례에 대한 의견을 환영합니다.

인증 FAQ

질문	답변
권한	
RADIUS/TACACS/LDAP 를 통해 허가를 얻을 수 있습니까?	LDAP 및 TACACS 는 원격 인증에만 사용되며 허가에는 사용되지 않습니다.

사용자 경험 FAQ

질문	답변
사용자 경험	
네트워크 포트 또는 로컬 직렬 포트(예를 들어, COM2)를 통한 콘솔 관리의 경우 로깅은 어떻게 됩니까? 로깅은 어떻게 됩니까? CC-SG 에서 로컬 관리를 캡처합니까 아니면 사라집니까?	CC-SG 콘솔 자체를 통해 CC-SG 에 로그인하는 것은 CC-SG 가 실행 중일 때 운영 체제(Linux)의 루트 권한을 얻는 것과 같습니다. Syslog 는 이러한 이벤트를 기록하지만 CC-SG 콘솔 자체에서 사용자 유형은 소실됩니다.

G: 자주 묻는 질문

H

키보드 단축키

다음 키보드 단축키는 Java 기반 관리자 클라이언트에서 사용할 수 있습니다.

작업	키보드 단축키
새로 고침	F5
인쇄 패널	Ctrl + P
도움말	F1
연관체 표에 행 삽입	Ctrl + I

I

명명 규칙

이 부록은 CC-SG 에서 사용된 명명 규칙에 대한 정보를 포함하고 있습니다. 모든 CC-SG 구성 요소에 대해 이름을 지정할 때 최대 문자 수를 준수하십시오.

CC-SG 한도	
CC-SG 에서의 필드:	CC-SG 가 허용하는 문자 수
장치 이름	32
장치 그룹	40
포트 이름	32
사용자 이름	20
사용자 그룹 이름	64
암호(강력한 암호 아님)	16
암호(강력한 암호)	구성 가능성 최소: 8 최대: 64 기본 최소: 8 기본 최대: 16
범주 이름	64
요소 이름	32
노드 이름	64
노드 그룹 이름	40
규정 이름	56

색인

ㄱ

가상 노드 개요 - 76
가상 매체 지원 - 119
가상 분포도 보기 액세스 - xv, 84
가상 시스템 노드 삭제 - 82
가상 시스템이 있는 가상 호스트 추가 - 78, 80
가상 인프라 동기화 - 83
가상 인프라 삭제 - 82
가상 인프라 용어 - 75
가상 인프라의 일일 동기화 활성화 또는 비활성화 - 83
가상 호스트 노드의 재부팅 또는 강제 재부팅 - xv, 84
가상 호스트 및 가상 시스템이 있는 제어 시스템 추가 - 76, 80
가용성 보고서 - 153
감사 추적 보고서 - 151
강력한 암호 구성 및 적용 - xvi
개요 - 1
검색을 위한 와일드카드 - 31
고급 관리 - 108, 109, 132, 137, 174
고급 클러스터 설정 - 196
관리 다시 시작 - 48
관리된 전원 탭 - 27, 33, 35, 56, 57
관리된 전원 탭 연결을 위한 인터페이스 - 56, 57, 58, 60, 62, 87, 89
관리자 콘솔 - 233
관리자 콘솔 액세스 - xviii, 170, 234
관리자 콘솔 정보 - 231, 233
관리자 콘솔 탐색 - 234
규정 삭제 - 118
규정 추가 - 97, 115, 116, 119
규정 편집 - 117
그룹 생성 - 14, 17
그룹에 사용자 지정 - 109, 110
그룹에서 사용자 삭제 - 110, 111
그룹화 FAQ - 289
기본 검색 기본 설정 변경 - 31, 112
기본 사용자 그룹 - 104
기본 애플리케이션 구성 - 177
기본 애플리케이션 정보 - 177

기본 애플리케이션 지정 보기 - 177
기본 CC-SG 노드 제거 - 195
기본 DN 지정 - 130
기본/백업 모드란 무엇입니까? - 179, 180

ㄴ

네트워크 설정 정보 - 3, 10, 179, 193, 236, 239
네트워크 설정을 제외한 모든 구성 데이터를 KX2, KSX2 또는 KX2-101 장치로 복원합니다. - 45
네트워크 인터페이스 구성 편집(네트워크 인터페이스) - 235
노드 그룹 개요 - 97
노드 그룹 데이터 보고서 - 159
노드 그룹 삭제 - 101
노드 그룹 전원 제어 - xix, 211
노드 그룹 추가 - 97, 115
노드 그룹 추가, 편집 및 삭제 - 97
노드 그룹 편집 - 101
노드 그룹별 필터 - 120
노드 그룹에 대한 전원 제어 및 전원 제어 작업 모니터링 - xix
노드 및 인터페이스 개요 - 65
노드 및 인터페이스 아이콘 - 68
노드 범주 및 요소 대량 복사 - 95
노드 보기 - 66
노드 사용자 정의 보기 - 121
노드 삭제 - 73, 82
노드 생성 보고서 - 159
노드 선택 - 98
노드 설명 - 99
노드 액세스를 위한 애플리케이션 구성 - 175
노드 액세스를 위한 애플리케이션 정보 - 175
노드 연결 - 85
노드 이름 - 65
노드 자산 보고서 - 95, 158
노드 정보 - 65
노드 추가 - 72
노드 추가, 편집 및 삭제 - 72
노드 탭 - 66

색인

노드 편집 - 73
노드 프로필 - 67
노드 프로필에 메모 추가 - xv, 67, 74
노드 프로필에 위치 및 연락처 추가 - xv, 67, 74
노드 핑 - 85
노드, 노드 그룹 및 인터페이스 - 27, 64
노드에 대한 RDP 액세스 - 270
노드에 대한 SSH 액세스 - 270
노드에 대한 VNC 액세스 - 270
노드에 직접 포트 액세스 구성 - 95
노드의 기본 사용자 정의 보기 할당 - 123
노드의 사용자 정의 보기 변경 - 122
노드의 사용자 정의 보기 삭제 - 123
노드의 사용자 정의 보기 적용 - 122
노드의 사용자 정의 보기 추가 - 121

ㄷ

다른 작업과 비슷한 작업 예약 - 216
대역내 연결을 위한 인터페이스 - xv, 86, 88
대역외 KVM, 대역외 직렬 연결을 위한 인터페이스 - 87, 88
두 요소 인증 - 147, 282
두 요소 인증 설정 요구사항 - 282
두 요소 인증을 위한 지원 환경 - 282
두 요소 인증의 알려진 문제 - 283
디스크 상태 표시 - 257

ㄹ

로그 활동 구성 - 185, 211
로그인 설정 - xvii, 198
로그인 설정 보기 - 198

ㄴ

명령 팁 - 221, 224
명명 규칙 - 14, 24, 26, 33, 35, 39, 40, 51, 65, 72, 73, 87, 91, 98, 105, 108, 116, 294
모든 구성 데이터를 KX2, KSX2 또는 KX2-101 장치로 복원 - 43, 46
모든 사용자 데이터 보고서 - 154
모든 사용자에게 대해 노드의 기본 사용자 정의 보기 할당 - xxii, 123
모든 사용자에게 대해 장치의 기본 사용자 정의 보기 할당 - 127

모든 사용자에게 강력한 암호가 필요함 - 198
모든 클라이언트 연결에 대해 직접 모드 구성 - 188
모든 클라이언트 연결에 대해 프록시 모드 구성 - 188
모든 AD 모듈 동기화 - 136, 137, 138, 139, 140
모든 AD 모듈의 일일 동기화 활성화 또는 비활성화 - 140
문제 해결 - 281

ㄷ

방법

CC-SG 기본 기능 - xvi
백업 파일 삭제 - 165
백업 파일 저장 - 165
백업 파일 저장 및 삭제 - 164
범주 및 요소 생성 - 15
범주 삭제 - 25
범주 추가 - 24
범주 편집 - 25
범주별 보기 - 120
보고서 - 148, 211
보고서 내역 보기 - 149
보고서 데이터 정렬 - 148
보고서 사용 - 148
보고서 열 너비 크기 조정 - 148
보고서 인쇄 - 149
보고서 필터 숨기기 또는 표시 - 150
보고서를 파일로 저장 - 149
보안 관리자 - 196, 219
보안 FAQ - 287
보조 CC-SG 노드 제거 - 195
분포도 보기 - 30
브라우저 연결 프로토콜 구성
HTTP 또는 HTTPS/SSL - 198
브라우저 캐시 지우기 - xviii, 170, 171, 281
브라우저의 AES 암호화 확인 - 197
비활동 타이머 구성 - 201

ㄷ

사용자 경험 FAQ - 291
사용자 계정 - 129
사용자 관리 - 14, 20

사용자 그룹 권한 - 105, 155, 271
 사용자 그룹 및 사용자 추가 - 20
 사용자 그룹 삭제 - 107
 사용자 그룹 추가 - 105
 사용자 그룹 추가, 편집 및 삭제 - 71, 105
 사용자 그룹 편집 - 106
 사용자 그룹에 규정 지정 - 115, 119
 사용자 그룹에 대한 액세스 감사 구성 - xv, 68, 107
 사용자 대량 복사 - 114
 사용자 데이터 보고서 - 155
 사용자 로그아웃 - 113
 사용자 및 사용자 그룹 - 97, 102, 119, 129, 145, 146
 사용자 삭제 - 110
 사용자 연결 해제 - 50
 사용자 이름당 동시 로그인 허용 - 201
 사용자 정의 보기 유형 - 120
 사용자 정의 JRE 설정 구성 - xv, 6, 190
 사용자 추가 - 108, 155
 사용자 추가, 편집 및 삭제 - 108
 사용자 탭 - 103
 사용자 편집 - 109
 사용자 프로필 - 111
 상태 콘솔 - 233, 256
 상태 콘솔 액세스 - 233
 상태 콘솔 정보 - 231, 233
 상호 운용성 FAQ - 290
 서비스 계정 - xv, 69
 서비스 계정 개요 - 69
 서비스 계정 추가, 편집 및 삭제 - 70
 서비스 계정의 암호 변경 - 71
 설명 방법 대 선택 방법 - 54, 98
 설정 설명서를 사용하기 전에 - 14
 설정 안내서를 사용하여 CC-SG 구성 - 10, 14, 24, 115
 설정 안내서의 연관체 - 14, 15
 성능 FAQ - 289
 순차적 작업 예약 - 209
 시스템 관리자 그룹 - 104
 시스템 정비 - 162
 시작하기 - 10
 실패한 CC-SG 노드 복구 - 195

ㅅ

썬 클라이언트 사용 - 8
 썬 클라이언트 설치 - 6
 썬 클라이언트 액세스 - 6

ㅇ

암호 변경 - 111
 애플리케이션 버전 확인 및 업그레이드 - 12, 175
 애플리케이션 삭제 - 177
 애플리케이션 추가 - 12, 176
 액세스 보고서 - 152
 액세스 제어 규정 - 19, 51, 102, 105, 115
 액세스 제어 목록 - 206, 251
 여러 페이지 보고서 탐색 - 149
 연결 모드
 직접 및 프록시 - 116, 187, 270
 연결 모드 정보 - 187
 연관체-범주 및 요소 정의 - 23
 연관체 관리자 - 24
 연관체 생성 방법 - 24
 연관체 용어 - 22
 연관체 정보 - 22
 연관체, 범주 및 요소 - 22, 30, 34, 35, 60, 67, 72, 73, 97
 예약된 보고서 - 160, 161, 210
 예약된 작업 및 정비 모드 - 162
 예약된 작업 변경 - 215
 예제
 PX 노드에 웹 브라우저 인터페이스
 추가 - 91, 93
 오늘의 메시지 구성 - 174
 오류 로그 보고서 - 152
 와일드카드 예제 - 31
 외부 AA 서버의 순서 설정 - 131
 외부 SMTP 서버 구성 - 208
 요소 삭제 - 26
 요소 추가 - 25
 요소 편집 - 26
 용어/약어 - 2, 33, 35, 142, 145, 146, 181, 184, 208, 217, 224, 236
 원격 시스템 모니터링 구성 - xv, 255, 270
 원격 시스템 모니터링 포트 - 270
 원격 인증 - 102, 128, 196

색인

웹 브라우저 인터페이스 - 87, 91
웹 브라우저 인터페이스 추가를 위한 팁 - 92
이력 데이터 추세 구성 - xv, 256
이메일 주소 변경 - 112
인증 및 허가(AA) 개요 - 128
인증 및 허가에 대한 모듈 지정 - 130
인증 흐름 - 128
인증 FAQ - 286, 291
인증서 - 203
인증서 작업 - 203
인터페이스 또는 포트 유형에 대한 기본 애플리케이션을 선택합니다. - 178
인터페이스 삭제 - xv, 81, 94
인터페이스 정보 - 65
인터페이스 책갈피 설정 - 94, 95, 158
인터페이스 추가 - 72, 86, 93
인터페이스 추가 결과 - 93
인터페이스 추가, 편집 및 삭제 - 71, 86
인터페이스 편집 - 93
인터페이스에 서비스 계정 지정 - 71
인프라 서비스 액세스 - 266
일반 FAQ - 284
일일 AD 동기화 시간 변경 - 141

ㅈ

자주 묻는 질문 - 284
작업 관리자 - 9, 10, 160, 162, 186, 208, 209
작업 삭제 - 216
작업 예약 - 211, 215
작업 유형 - 209
작업 재예약 - 215, 216
작업 찾기 및 보기 - 210
작업에 대한 이메일 통지 - 209
잠금 설정 - 154, 200
잠긴 사용자 보고서 - 154
장치 검색 - 31, 32, 33
장치 검색 및 추가 - 16
장치 구성 백업 - 43, 211
장치 구성 복사 - 47, 211
장치 구성 복원 - 44, 211
장치 구성 복원(KX, KSX, KX101, SX, IP-Reach) - 44
장치 그룹 관리자 - 51
장치 그룹 데이터 보고서 - 156

장치 그룹 및 노드 그룹 추가 - 17
장치 그룹 삭제 - 55
장치 그룹 추가 - 51, 55, 115
장치 그룹 편집 - 54
장치 그룹별 필터 - 120
장치 다시 시작 - 47, 211
장치 및 노드의 사용자 정의 보기 - xxiii, 66, 120
장치 및 포트 아이콘 - 28
장치 백업 파일의 저장, 업로드 및 삭제 - 46
장치 범주 및 요소 대량 복사 - 42
장치 보기 - 28
장치 사용자 정의 보기 - 124
장치 삭제 - 30, 38
장치 설정 - xv, 14, 15, 189
장치 설정 또는 사용자 및 사용자 그룹 데이터만 KX2, KSX2 또는 KX2-101 장치로 복원 - 45
장치 업그레이드 - 34, 42, 178
장치 자산 보고서 - 156
장치 전원 관리자 - 49
장치 추가 - 33
장치 탭 - 28
장치 탭에서 옵션을 마우스 오른쪽 버튼으로 클릭합니다. - 31
장치 펌웨어 관리 - 178
장치 펌웨어 업그레이드 보고서 - xxii, 161, 215
장치 펌웨어 업그레이드 예약 - 211, 213, 215
장치 편집 - 36
장치 프로필 화면 - 30
장치 프로필에 메모 추가 - xv, 30, 37
장치 프로필에 위치 및 연락처 추가 - xv, 30, 37
장치 핑 - 48
장치, 장치 그룹 및 포트 - 27
장치에 대한 CC-SG의 관리 일시 중지 - 48
장치의 관리 페이지 실행 - 49
장치의 기본 사용자 정의 보기 지정 - 126
장치의 사용자 정의 보기 변경 - 125
장치의 사용자 정의 보기 삭제 - 126
장치의 사용자 정의 보기 적용 - 125
장치의 사용자 정의 보기 추가 - 124
전원 상태 메시지 - xx

전원 탭 장치 또는 Dominion PX 장치 편집 - xv, 36
 전원 탭 장치 추가 - 32, 33, 35
 전원 탭의 장치 또는 포트 연관체 변경(SX 3.0, KSX) - 59, 60
 전원 탭의 콘센트 구성 - 57, 58, 60, 62
 전제조건 - 1
 정비 모드 - 117, 162
 정비 모드 시작 - xvii, 12, 162, 170, 176
 정비 모드 종료 - xviii, 163, 171
 정적 루트 편집 - 184, 238, 239
 제어 시스템 및 가상 호스트 삭제 - 82
 제어 시스템, 가상 호스트 및 가상 시스템 편집 - 80, 82
 제한 시간 내에 여러 장치 업그레이드 - xx
 종료 후 CC-SG 다시 시작 - 172
 직렬 가능 장치에 SSH 연결 생성 - 225
 직렬 관리 포트 - 227
 직렬 포트 구성 - 38
 직접 모드 또는 프록시 모드의 조합 구성 - 188
 진단 콘솔 - 5, 172, 231
 진단 콘솔 계정 구성 - 253
 진단 콘솔 구성 편집 - 235
 진단 콘솔 암호 설정 - 234, 248, 251
 진단 콘솔 액세스 - 231
 진단 콘솔로 상단 부분 표시 보기 - 257
 진단 콘솔로 CC 슈퍼 사용자 암호 재설정 - 248
 진단 콘솔로 CC-SG 다시 시작 - 245
 진단 콘솔로 CC-SG 재부팅 - 246
 진단 콘솔에서 로그 파일 보기 - 241
 진단 콘솔에서 CC-SG 시스템 전원 끄기 - 247
 질의 포트 보고서 - 156

ㅊ

채팅 사용 - 96
 초기 화면 - 202

ㅋ

클라이언트 브라우저 요구사항 - 4
 클라이언트와 CC-SG 사이에 AES 암호화가 필요합니다. - 197
 클러스터 생성 - 194

키보드 단축키 - 293

ㅌ

터미널 애플리케이션 프로그램 정보 - 228
 통지 관리자 - 208, 209

ㅍ

펌웨어 삭제 - 179
 펌웨어 업로드 - 178
 포트 구성 - 38, 61
 포트 구성에 의해 생성된 노드 - 38, 40, 73
 포트 삭제 - 41
 포트 정렬 옵션 - 29
 포트 편집 - 40

ㅎ

호환성 매트릭스 확인 - 12
 활성 노드 보고서 - 159
 활성 사용자 보고서 - 154
 활성/활성 모드란 무엇입니까? - 179, 183
 회계 FAQ - 288

A

AD 고급 설정 - 133, 136
 AD 그룹 설정 - 134, 136, 137
 AD 모듈 편집 - 136
 AD 및 CC-SG 개요 - 131
 AD 사용자 그룹 가져오기 - 137
 AD 사용자 그룹 보고서 - 160
 AD 일반 설정 - 132, 136
 AD Trust(트러스트) 설정 - 135, 136
 AD 와 모든 사용자 그룹 동기화 - 136, 137, 138, 139
 AD 와 CC-SG 동기화 - 138
 AD 의 사용자 이름 지정 - 130
 AD 의 DN 지정 - 129
 Admin 클라이언트에서 사용자 정의 보기 사용 - 121
 AES 암호화 - 197

C

CC 사용자 그룹 - 104
 CC 슈퍼 사용자 그룹 - 104
 CC-NOC 동기화 보고서 - 161, 217

- CC-NOC 삭제 - 218
 - CC-NOC 실행 - 218
 - CC-NOC 추가 - 161, 216
 - CC-NOC 편집 - 218
 - CC-SG 관리자 설명서의 새로운 내용 - xv
 - CC-SG 기본 글꼴 크기 변경 - 112
 - CC-SG 내부 포트 - 269
 - CC-SG 네트워크 구성 - 131, 179
 - CC-SG 네트워크를 위한 필수 개방 포트 요약 - 263
 - CC-SG 다시 시작 - 169, 182, 245
 - CC-SG 및 네트워크 구성 - 263
 - CC-SG 및 CC-NOC - 268
 - CC-SG 및 IPMI, iLO/RILOE, DRAC, RSA 용 클라이언트 - 268
 - CC-SG 및 Raritan 장치 - 264
 - CC-SG 및 SNMP - 268
 - CC-SG 백업 - xviii, 163, 168, 171, 190, 211
 - CC-SG 복원 - 164, 165
 - CC-SG 서버 시간 및 날짜 구성 - 186
 - CC-SG 서버 시간 설정 - 10
 - CC-SG 세션 종료 - 173
 - CC-SG 슈퍼 사용자의 사용자 이름 변경 - 113
 - CC-SG 암호 정보 - 199
 - CC-SG 액세스 - 5
 - CC-SG 업그레이드 - xv, 169
 - CC-SG 일련 번호 찾기 - 228
 - CC-SG 재설정 - xv, 166
 - CC-SG 전원 끄기 - 172
 - CC-SG 종료 - 172, 173
 - CC-SG 출고 시 구성(Admin) 재설정 - 249
 - CC-SG 클러스터 구성 - 193
 - CC-SG 클러스터 및 CC-NOC 정보 - 193
 - CC-SG 클러스터란 무엇입니까? - 193
 - CC-SG 클러스터링 - 265
 - CC-SG 클러스터의 요구 사항 - 193
 - CC-SG 통신 채널 - xv, 264
 - CC-SG Admin 클라이언트 - 8
 - CC-SG Admin 클라이언트를 통한 브라우저 기반 액세스 - 5
 - CC-SG LAN 포트 정보 - 179, 180, 183
 - CC-SG 를 새 펌웨어 버전으로 업그레이드 - xvii
 - CC-SG 에 대한 권장 DHCP 구성 - 179, 181, 184, 185
 - CC-SG 에 대한 SSH 액세스 - 198, 219
 - CC-SG 에 AD 모듈 추가 - 131
 - CC-SG 에 LDAP(Netscape) 모듈 추가 - 141
 - CC-SG 에 SSH 액세스를 위한 포트 번호 설정 - 198
 - CC-SG 에서 가상 인프라 구성 - xv, 75, 86
 - CC-SG 에서 다른 장치가 관리하는 전원 탭 구성 - xv, 56, 57
 - CC-SG 에서 로그아웃 - 173
 - CC-SG 에서 보고서 데이터 제거 - 150, 151, 152, 186
 - CC-SG 와 가상 인프라 동기화 - xv, 83
 - CC-SG 의 내부 로그 제거 - 186
 - CommandCenter NOC - 216
- ## D
- Dominion PX 장치 추가 - xv, 32, 33, 35
 - DRAC, RSA 및 ILO 프로세서 전원 제어 연결을 위한 인터페이스 - 87, 89
- ## E
- E1 모델 - 261
 - E1 일반 사양 - 261
 - E1 환경 요구사항 - 261
- ## I
- IP 주소 핑 - 237
 - IP 주소 확인 - 10
 - IPMI 전원 제어 연결을 위한 인터페이스 - 87, 90
 - IP-Reach 및 UST-IP 관리 - 51
- ## J
- Java 캐시 지우기 - xviii, 170, 171, 281
 - JRE 비호환성 - xv, 5, 6
- ## K
- KVM 또는 직렬 장치 추가 - 32, 33, 59, 61
 - KVM 포트 구성 - 39
 - KX, KX2, KX2-101, KSX2 또는 P2SC 장치에 연결된 전원 탭 장치 삭제 - 58, 59
 - KX, KX2, KX2-101, KSX2 또는 P2SC 장치에 연결된 전원 탭 장치 추가 - 58

KX, KX2, KX2-101, KSX2 또는 P2SC 의 전원 탭을 다른 포트로 이동 - 58

KX, KX2, KX2-101, KSX2 및 P2SC 에 연결된 전원 탭 구성 - 57, 58

L

LDAP 고급 설정 - 142

LDAP 및 AD 의 DN(구분 이름) - 129

LDAP 및 CC-SG 정보 - 141

LDAP 일반 설정 - 141

LDAP 의 DN 지정 - 130

M

MIB 파일 - 192

N

NAT 사용 방화벽을 통한 CC-SG 액세스 - 270

NTP 상태 표시 - 258

O

OpenLDAP(eDirectory) 구성 설정 - 144

P

P2-SC(Paragon II System Controller) - 50

Paragon II 시스템 장치로의 특별 액세스 - 50

PC 클라이언트 및 노트 - 267

PC 클라이언트 및 CC-SG - 266

R

RADIUS 모듈 추가 - 146

RADIUS 및 CC-SG 정보 - 146

RADIUS 일반 설정 - 146

RADIUS 를 이용한 Two-Factor 인증 - 147

S

SNMP 구성 - xv, 191

SNMP 트랩 - 192, 279

SSH 명령 및 매개변수 - 221

SSH 명령에 대한 도움말 얻기 - 220

SSH 연결 종료 - 224, 227

SSH 를 사용하여 대역외 직렬 인터페이스를 통해 노트에 연결 - 226

SSH 를 통한 진단 콘솔 액세스 - 231

Sun One LDAP(iPlanet) 구성 설정 - 144

SX 3.0 또는 KSX 장치에 연결된 전원 탭 삭제 - 59, 60

SX 3.0 또는 KSX 장치에 연결된 전원 탭 추가 - 59

SX 3.0 및 KSX 에 연결된 전원 탭 구성 - 57, 59

SX 3.1 장치에 연결된 전원 탭 삭제 - 61, 62

SX 3.1 장치에 연결된 전원 탭 추가 - 61, 62

SX 3.1 에 연결된 전원 탭 구성 - 57, 61

SX 3.1 의 전원 탭을 다른 포트로 이동 - 61, 62

T

TACACS+ 모듈 추가 - 145

TACACS+ 및 CC-SG 정보 - 145

TACACS+ 일반 설정 - 145

Traceroute 사용 - 238

V

V1 모델 - 260

V1 및 E1 사양 - 260

V1 일반 사양 - 260

V1 환경 요구사항 - 260

VGA/키보드/마우스 포트를 통한 진단 콘솔 액세스 - 231

W

Web Services API - 228

▶ 미국/캐나다/라틴 아메리카

월요일 - 금요일
8 a.m. - 8 p.m. ET
전화: 800-724-8090 또는 732-764-8886
CommandCenter NOC: 6번 입력 후 1번 입력
CommandCenter Secure Gateway: 6번 입력 후 2번 입력
팩스: 732-764-8887
CommandCenter NOC에 관한 이메일: tech-ccnoc@raritan.com
기타 모든 제품에 관한 이메일: tech@raritan.com

▶ 중국

북경

월요일 - 금요일
9 a.m. - 6 p.m. 현지 시간
전화: +86-10-88091890

상하이

월요일 - 금요일
9 a.m. - 6 p.m. 현지 시간
전화: +86-21-5425-2499

광저우

월요일 - 금요일
9 a.m. - 6 p.m. 현지 시간
전화: +86-20-8755-5561

▶ 인도

월요일 - 금요일
9 a.m. - 6 p.m. 현지 시간
전화: +91-124-410-7881

▶ 일본

월요일 - 금요일
9:30 a.m. - 5:30 p.m. 현지 시간
전화: +81-3-3523-5994
이메일: support.japan@raritan.com

▶ 유럽

유럽

월요일 - 금요일
8:30 a.m. - 5 p.m. GMT+1 CET
전화: +31-10-2844040
이메일: tech.europe@raritan.com

영국

월요일 - 금요일
8:30 a.m. - 5 p.m. GMT+1 CET
전화: +44-20-7614-77-00
프랑스
월요일 - 금요일
8:30 a.m. - 5 p.m. GMT+1 CET
전화: +33-1-47-56-20-39

독일

월요일 - 금요일
8:30 a.m. - 5 p.m. GMT+1 CET
전화: +49-20-17-47-98-0

▶ 한국

월요일 - 금요일
9 a.m. - 6 p.m. 현지 시간
전화: +82-2-5578730

▶ 호주 멜버른

월요일 - 금요일
9:00 a.m. - 6 p.m. 현지 시간
전화: +61-3-9866-6887

▶ 대만

월요일 - 금요일
9 a.m. - 6 p.m. GMT -5 표준 -4 일광 절약 시간제
전화: +886-2-8919-1333
이메일: tech.rap@raritan.com