

Dell™ Remote Console Switch

시스템

사용 설명서



참고, 주의 및 경고



참고: 참고는 컴퓨터를 효과적으로 활용할 수 있는 중요 정보를 의미합니다.



주의: 주의는 지침을 따르지 않아 발생할 수 있는 하드웨어의 잠재적 손상 또는 데이터 손실을 나타냅니다.



경고: 경고는 재산상의 손해, 신체적 상해 또는 사망의 가능성을 나타냅니다.

이 문서의 내용은 사전 통지 없이 변경될 수 있습니다.

© 2012 Dell Inc. All rights reserved.

Dell Inc.의 서면 승인이 없는 한 본 자료에 대한 어떠한 방식의 복제도 엄격히 금지됩니다.

이 문서의 내용에 사용된 상표: *Dell*TM 및 *DELL* 로고는 Dell Inc.의 상표입니다.

이 문서에 사용된 다른 상표와 상표명은 해당 상표, 이름 또는 제품의 소유자를 나타냅니다. Dell Inc.는 자사 소유의 상표 및 상표명 이외에 대한 소유권을 주장하지 않습니다.

590-1021-512C

모델 1082DS/2162DS/4322DS Remote Console Switch

2012년 7월

목 차

제품 개요	1
기능 및 이점	1
감소 케이블 사용량	2
KVM 스위칭 기능	2
다중 플랫폼 지원	2
진정한 직렬 기능	3
로컬 및 원격 사용자 인터페이스	3
가상 미디어 및 스마트 카드 가능 스위치	3
온보드 웹 인터페이스	4
표준 TCP/IP 네트워크를 통한 스위치 액세스	4
암호화	4
비디오	4
플래시 업그레이드 가능	5
다층 구성 확장	5
Avocent 관리 Avocent 플러그인	5
모듈 연결	5
구성 예제	7
안전 주의사항	8
일반 사항	9
LAN 옵션	11
설치	13
RCS 빠른 설정	13
시작	15
네트워크 설정	16
랙 장착 RCS	16

랙 장착 안전 고려 사항	17
Dell ReadyRails™ 시스템 설치	17
RCS 설치	22
RCS 하드웨어 연결	26
SIP 연결	30
다층 구성 스위치 추가	32
리거시 스위치의 종속 연결 구성	34
PEM(옵션) 추가	36
Remote Console Switch 구성	38
내장 웹 서버 설정	38
방화벽을 통해 OBWI 방화벽	38
연결 확인	41
후면 패널 이더넷 연결 LED	41
후면 패널 전원 상태 LED	41
조정 마우스 설정 대상 장치	42
로컬 및 원격 구성	43
로컬 사용자 인터페이스(UI)	43
필터링	44
OBWI	45
사용자 인터페이스 사용	47
세션 실행	48
스캔 모드	49
시스템 정보 보기	50
RCS 도구	51
RCS 다시 부팅	51
RCS 펌웨어 업그레이드	51
RCS 구성 및 RCS 사용자 데이터베이스 저장 및 복구	52

네트워크 설정	54
DNS 설정	56
NTP 설정	56
SNMP 설정	56
이벤트 감사 설정	57
이벤트 대상 설정	58
포트 - SIP 구성	58
SIP 업그레이드	59
전원 장치 설정	60
연결된 대상 서버 및 전원 콘센트	61
전원 콘센트 그룹 만들기	63
기본 콘센트 이름	64
콘센트 이름 할당	65
로컬 포트의 로컬 세션 페이지	69
로컬 포트 UI 설정	70
모뎀 설정	71
설정 - 포트 보안 설정	72
세션	72
일반 세션 구성	72
KVM 세션 구성	73
로컬 가상 미디어 세션 구성	73
직렬 세션 구성	76
사용자 계정 설정	76
로컬 계정 매핑	76
액세스 수준	77
Avocent 관리 소프트웨어 장치 IP 주소	78

LDAP	78
Override 관리자	79
활성 세션	79
세션 닫기	79
Video Viewer 창	81
변경 도구 모음	83
세션 실행	84
세션 제한 시간	84
창 크기	85
보기 조정	85
이미지 새로 고침	87
비디오 설정	87
추가 비디오 조정	87
대상 비디오 설정	89
Automatic Video Adjustment	89
비디오 테스트 패턴	89
공급업체 전용 비디오 설정	90
색 설정	90
색 농도 조정	90
대비 및 밝기	90
노이즈 설정	91
한계치 탐지	91
마우스 설정	91
조정 마우스 옵션	91
커서 유형	91
마우스배율 조정	94
마우스 정렬 및 동기화	95

가상 미디어	95
요구 사항	95
공유 및 선점 고려 사항	96
Virtual Media 대화 상자	97
Virtual Media 세션 열기	97
가상 미디어 세션 닫기	101
스마트 카드	101
Keyboard Pass-through	102
매크로	103
보기 저장	103
세션 닫기	104
RCS의 LDAP 기능	105
Active Directory 구조	105
도메인 컨트롤러 컴퓨터	105
개체 클래스	106
속성	106
스키마 확장	107
표준 스키마 대 Dell 확장 스키마	108
표준 설치	109
관리자 무시 계정 구성	110
DNS 설정 구성	110
네트워크 시간 프로토콜(NTP) 설정 구성	111
LDAP 인증 매개변수 구성	112
LDAP 인증 활성화	112
인증 매개변수 입력 - 작동 모드	115
확장 옵션 입력 - Active Directory LDAP	116

인증 매개변수 입력 - 표준 LDAP	116
인증 매개변수 입력 - 사용자 정의 IP 포트 할당	116
LDAP 구성 완료	117
보조 LDAP 설정 - 표준 구성	118
표준 LDAP 쿼리 수행을 위한 RCS 설정	119
구성 설정 검색	120
쿼리 모드 선택 설정	121
그룹 구성 매개변수	122
보조 LDAP 설정 - Active Directory 구성	123
LDAP SSL 인증서	126
도메인 컨트롤러에서 SSL 활성화	126
로그인 제한 시간	131
CA 인증서 정보 표시	132
그룹 개체 구성	133
표준 스키마용 Active Directory 개체 개요	135
Dell Extended Schema Active Directory 개체 개요	136
사용자의 RCS에 액세스하기 위해 Dell 스키마 확장을 이용해	
Active Directory 구성	141
Active Directory 스키마 확장(옵션)	141
Active Directory 사용자 및 컴퓨터 스냅인에 Dell Extension 설	
치(옵션)	142
Active Directory 사용자 및 컴퓨터 스냅인 열기	143
Dell 스키마 확장을 통해 Active Directory에 사용자 및 권한 추가	144
SIP 개체 만들기	144
권한 개체 만들기	144
Dell 연결 개체 구문 사용	145
연결 개체 만들기	146
연결 개체에 개체 추가	146
콘솔 재지정 액세스 보안	147
Active Directory를 사용하여 RCS에 로그인	148
LDAP 구현을 위한 대상 장치 이름 지정 요구 사항	149

자주 묻는 질문	150
부록 A: 터미널 작동	153
콘솔 부팅 메뉴 옵션	153
콘솔 주 메뉴 옵션	154
부록 B: SIP 사용	155
ACS 콘솔 서버 포트 핀 배열	155
Cisco 포트 핀 배열	156
부록 C: MIB 및 SNMP 트랩	157
부록 D: 케이블 핀 배열 정보	163
모뎀 핀 배열	163
콘솔/설정 핀 배열	163
부록 E: UTP 케이블 연결	165
UTP 동축 케이블 연결	165
배선 표준	166
케이블 설치, 유지 보수 및 안전 정보	166
부록 F: Sun고급 키 에뮬레이션	169
부록 G: 기술 사양	171
부록 H: 기술 지원	175

제품 개요

IP 및 직렬 콘솔 스위치 상의 Dell 1082DS/2162DS/4322DS RCS 스위치 (RCS) 디지털 키보드, 비디오 및 마우스 (KVM)는 아날로그 및 디지털 기술을 결합하여 데이터 센터 서버의 유연하고 중앙 집중적인 제어를 제공하며, 숙련된 운영자가 없는 원격 지점의 운영, 활성화, 유지보수를 용이하게 합니다. IP 기반 RCS으로 유연한 대상 장치 관리 제어 및 언제 어디서나 RCS 소프트웨어나 온보드 웹 인터페이스 (OBWI)를 통한 안전한 원격 액세스를 제공합니다.

기능 및 이점

RCS에서 엔터프라이즈 고객에게 다음과 같은 기능 및 옵션을 제공합니다.

- 많은 양의 케이블 감소
- 가상 미디어 (VM) 기능, 아날로그 (로컬) 또는 디지털 (원격) 연결 구성 가능
- 스마트 카드/공통 액세스 카드 (CAC) 기능
- SSH 및 Telnet을 통한 진정한 직렬 기능
- 향상된 비디오 해상도 지원, 대상부터 원격까지 1600 x 1200 또는 1680 x 1050(와이드 스크린) 기본
- 중복을 위한 옵션 이중 전원 모델
- 지능형 전원 장치 관리를 위한 옵션 지원
- 이중 비종속 로컬 포트 비디오 경로 (ACI 전용)

- 동시 액세스를 위한 이중 스택 IPv4(DHCP) 및 IPv6(DHCPv6 및 스테이트리스 자동 구성)
- 10/100/1000BaseT LAN 포트에 대상 장치 액세스 가능
- 이더넷 연결이 불가능할 때 스위치에 액세스하기 위해 사용할 수 있는 V.34, V.90 또는 V.92 호환 모뎀을 지원하는 MODEM 포트
- FIPS 지원

감소 케이블 사용량

서버 밀도가 지속적으로 증가할 때 케이블 사용량은 네트워크 관리자의 주요 우려 사항입니다. RCS 제품은 혁신적인 SIP 모듈 및 하나의 업계 표준 UTP 케이블을 활용하여 랙의 KVM 케이블 사용량을 크게 줄입니다. 이를 통해 서버 밀도를 높이면서 공기 흐름과 냉각 성능을 향상시킬 수 있습니다.

KVM 스위칭 기능

RCS에서는 직접 대상 장치에서 전원을 제공 받는 SIP를 지원하며 스위치에 전원이 끊겼을 때 Keep Alive 기능을 제공합니다. CAT 5 설계의 SIP은 최적의 해상도 및 비디오 설정을 제공하면서 케이블 뭉치를 크게 줄입니다. SIP의 내장 메모리는 고유한 장치 이름 및 각 연결 장치에 대한 전자 ID(EID) 번호를 할당 및 보유하여 구성을 단순화합니다.

PS/2 및 USB SIP는 장치에 직접 KVM 연결을 허용하여 사용할 수 있습니다. USB2+CAC SIP도 사용 가능합니다. RCS는 SIP 연결을 위해 8, 16 또는 32 아날로그 랙 인터페이스(ARI)가 제공합니다. SIP를 활용하여, RCS 시스템을 확장하기 위해 추가적인 스위치를 연결할 수 있습니다. 이처럼 융통성이 좋기 때문에 데이터 센터가 커짐에 따라 용량을 추가할 수 있습니다.

다중 플랫폼 지원

Dell SIP은 PS/2, USB 및 USB2+CAC 장치 환경을 지원하기 위하여 RCS에 사용할 수 있습니다. 이 모듈과 OBWI를 연계하여 사용하면 여러 플랫폼에 쉽게 전환할 수 있습니다.

Avocent® IQ Module Intelligent Cabling과 상호 운용성은 장치를 RCS에 연결하기 위해서도 사용할 수 있습니다. PS/2, USB, Sun® 및 Serial 모듈 옵션이 제공됩니다. 자세한 내용은 제품에 대한 Avocent 설치/사용자 설명서를 참고하거나 avocent.com/manual에 방문하십시오.

진정한 직렬 기능

RCS에서는 Telnet을 통한 진정한 직렬 기능을 제공하는 SIP를 지원합니다. SIP를 사용하여 SSH 세션을 실행하거나 OBWI에서 Serial Viewer를 실행하여 RCS에 연결된 직렬 대상에 연결할 수 있습니다.

로컬 및 원격 사용자 인터페이스

직접 로컬 포트에 연결하여 RCS 관리를 수행할 경우 로컬 사용자 인터페이스(로컬 UI)를 사용할 수 있습니다. 원격 OBWI를 사용하여 스위치를 관리할 수도 있습니다. OBWI는 웹 브라우저 기반이며 직접 스위치에서 실행되고 스위치에 연결된 장치가 자동으로 감지됩니다.

가상 미디어 및 스마트 카드 가능 스위치

RCS에서 모든 대상 장치에 가상 미디어에 있는 데이터를 보고 이동하거나 복사할 수 있습니다. 운영 체제 설치, 운영 체제 복구, 하드 드라이브 복구 또는 복제, BIOS 업데이트, 대상 장치 백업 등을 통해 원격 시스템을 보다 효율적으로 관리할 수 있습니다.

RCS에서 스위치 시스템과 연계하여 스마트 카드를 사용할 수도 있습니다. 스마트 카드는 정보를 저장 및 처리하는 포켓 크기의 카드입니다. CAC와 같은 스마트 카드는 컴퓨터, 네트워크 및 안전한 방이나 건물에 액세스할 수 있는 식별 및 인증 정보를 저장하기 위해 사용할 수 있습니다.

가상 미디어 및 스마트 카드 판독기는 직접 스위치의 USB 포트에 연결할 수 있습니다. 또한 가상 미디어 및 스마트 카드 판독기는 원격 OBWI, Dell RCS 소프트웨어 또는 Avocent 관리 소프트웨어가 실행되는 원격 워크스테이션에 연결할 수 있으며 이더넷 연결을 사용하여 스위치에 연결됩니다.



참고: 대상 장치로 가상 미디어 또는 스마트 카드 세션을 열려면 먼저 SIP를 사용하여 대상 장치를 스위치에 연결해야 합니다.

온보드 웹 인터페이스

OBWI는 RCS 소프트웨어와 유사한 관리 기능을 제공하지만 소프트웨어 서버나 설치가 필요하지는 않습니다. OBWI는 직접 스위치에서 직접 실행되며 RCS에 연결된 서버는 자동으로 감지됩니다. OBWI를 사용하여 웹 브라우저에서 RCS를 구성할 수 있습니다. OBWI에서 Viewer를 실행하여 대상 장치에 대한 KVM 및 가상 미디어 세션을 설정합니다. 또한 OBWI는 LDAP 인증을 지원하여 단일 인터페이스를 통해 다양한 RCS를 관리할 수 있는 권한을 제공합니다.

표준 TCP/IP 네트워크를 통한 스위치 액세스

스위치는 에이전트 없는 원격 제어 및 액세스를 제공합니다. 연결된 서버나 클라이언트에는 특별한 소프트웨어나 드라이버가 필요하지 않습니다.



참고: 클라이언트는 인터넷 브라우저를 사용하여 스위치에 연결합니다.

클라이언트의 이더넷이나 V.34, V.90 또는 V.92 모뎀을 통해 스위치 및 모든 연결 시스템에 액세스할 수 있습니다. 클라이언트는 네트워크 연결이 되어 있는 곳이라면 어디든지 위치할 수 있습니다.

암호화

RCS는 128비트 SSL(ARCFOUR) 뿐 아니라 키보드/마우스, 비디오, 가상 미디어 세션의 AES, DES 및 3DES 암호화를 지원합니다.

비디오

RCS는 아날로그 VGA, SVGA 및 XGA 비디오에 대해 최적의 해상도를 제공합니다. 스위치와 서버를 분리하는 케이블 길이에 따라 최대 1600 x 1200 또는 1680 x 1050(와이드스크린)의 해상도를 구현할 수 있습니다.

플래시 업그레이드 가능

언제든지 RCS 및 SIP 모듈을 업그레이드하여 사용 가능한 가장 최신의 펌웨어 버전을 사용할 수 있습니다. 플래시 업그레이드는 OBWI 또는 직렬 콘솔을 통해 시작할 수 있습니다. SIP의 자동 펌웨어 업그레이드를 수행하도록 RCS를 구성할 수 있습니다. 자세한 내용은 51페이지의 "RCS 펌웨어 업그레이드"를 참조하십시오.

다층 구성 확장

RCS는 스위치의 각 ARI(Analog Rack Interface) 포트에서 추가로 Dell RCS를 다층 구성할 수 있는 기능을 지원합니다. 다층 구성 스위치는 다른 장치와 같은 방법으로 연결합니다. 이렇게 장비를 추가 층으로 연결하는 기능을 통해 시스템 한 대에 최대 1024대의 서버를 연결할 수 있습니다. 32페이지의 "다층 구성 스위치 추가"를 참조하십시오.

Avocent 관리 Avocent 플러그인

Avocent 관리 소프트웨어와 스위치를 함께 사용하면 IT 관리자는 단일 웹 기반 사용자 인터페이스를 통해 여러 플랫폼의 대상 장치를 원격으로 액세스, 모니터 및 제어할 수 있습니다. 자세한 내용은 Avocent 관리 소프트웨어의 기술 회보를 참조하십시오.

모듈 연결

RCS 스위치는 FIPS 140-2 수준 1 암호화 보안 요구사항을 지원합니다. OBWI 또는 로컬 포트를 통해 FIPS 운영 모드를 활성화 또는 비활성화하고 재부팅 후 실행할 수 있습니다. FIPS가 활성화될 때 스위치를 재부팅하면 FIPS 모드 무결성 확인을 완료하기 위해 약 2분이 더 소요됩니다. 또한 FIPS가 활성화되었을 때 키보드, 마우스 또는 비디오 암호화가 128비트 SSL(ARCFOUR) 또는 DES로 설정된 경우 암호화 수준은 자동으로 암호화 수준 AES로 변경됩니다.



참고: FIPS 작동 모드는 초기에 비활성화되므로, 작동하려면 활성화해야 합니다.



참고: 포트 설정의 출하 시 기본 설정은 자동으로 FIPS 모듈을 비활성화합니다.



참고: DSView 소프트웨어 플러그인을 통해 FIPS 모드를 변경할 수 있습니다.

RCS 스위치는 FIPS 140-2 구현 안내 섹션 G.5 지침에 따라 Linux PPC 플랫폼에서 실행하는 내장된 FIPS 140-2 검증 암호화 모듈(인증서 #1051)을 사용합니다.

OBWI, 로컬 포트 또는 DSView 플러그인을 통해 FIPS 모드를 활성화/비활성화할 수 있습니다. FIPS 모드를 활성화 또는 비활성화하려면 재부팅해야 합니다. 이 버전으로 펌웨어 업그레이드하거나 상태를 기본 상태(포트 설정 메뉴)로 설정하면 FIPS 모드가 비활성화됩니다.

FIPS 모드에서 암호화 암호는 AES 또는 3DES로 제한됩니다. FIPS가 활성화되었을 때 키보드/마우스 또는 비디오 암호화가 128비트 SSL 또는 DES로 설정된 경우 암호화 수준은 자동으로 AES로 변경됩니다. FIPS가 활성화되었을 때 이러한 파일은 FIPS 호환 가능 알고리즘, AES를 사용하여 저장(또는 복원)됩니다. FIPS가 비활성화될 때 외부 파일로 기기에서 저장되거나 기기로 복원된 복원된 저장되거나 기기로 복원된 외부 파일로 사용자 데이터베이스 및 기기 구성 파일은 DES를 사용하여 암호화(또는 암호 해독)됩니다.

이것은 사용자가 OBWI의 저장(또는 로드) 대화 상자에서 암호 매개변수를 채우지 않을 때도 마찬가지이며, 이 경우 암호화 또는 암호 해독을 위해 기본 OEM 암호가 사용됩니다.

FIPS 모듈을 활성화할 때 한 가지 결과는 이전에 저장된 사용자 데이터베이스 및 기기 구성 파일이 호환되지 않는 것으로 나타나는 것입니다. 이 경우 FIPS 모듈을 일시적으로 비활성화하고 기기를 재부팅하고 이전에 저장된 데이터베이스나 구성 파일을 복원하고 FIPS 모듈을 다시 활성화하고 재부팅한 다음, FIPS 모듈이 활성화된 상태에서 파일을 다시 외부로 저장할 수 있습니다. 새로 저장된 외부 파일은 기기가 FIPS 모드를 활성화하여 실행하는 동안에는 기기와 호환될 수 있습니다.

반대 상황에도 마찬가지입니다. FIPS 모듈이 활성화되었을 때 저장된 데이터베이스 및 구성 파일은 FIPS 모듈이 활성화되지 않은 기기나 FIPS 모드를 지원하지 않는 이전 펌웨어를 사용하는 기기로 복원하는데 호환되지 않습니다.

구성 예제

그림 1.1. RCS 구성 예제

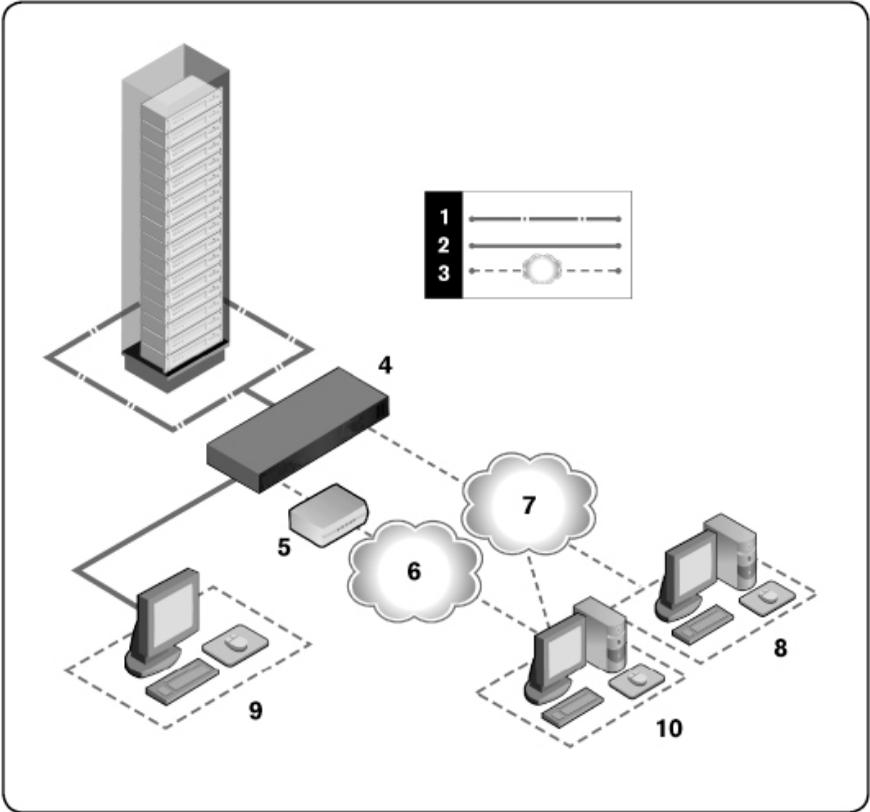


표 1.1: 그림 1.1 설명

번호	설명	번호	설명
1	UTP 연결	6	전화망
2	RCS에 대한 KVM 연결	7	이더넷
3	원격 IP 연결	8	Avocent 관리 소프트웨어 서버
4	RCS	9	아날로그 사용자(로컬 UI)
5	모뎀	10	디지털 사용자(원격 OBWI 또는 Dell RCS 소프트웨어를 위한 인터넷 브라우저가 있는 컴퓨터)

안전 주의 사항

다음 안전 지침을 준수하여 사용자 자신의 안전을 확보하고 시스템과 작업 환경이 손상되지 않도록 보호하십시오.

△ 주의: 시스템으로 공급되는 전원은 신체적 상해를 일으킬 수 있는 고압 전류와 유해한 에너지를 발생시킬 수 있습니다. 숙련된 서비스 전문가만 덮개를 분리하거나 시스템 내부의 구성부품을 취급할 수 있습니다. 이 경고는 **Dell™ Remote Console Switch**, **Dell™ PowerEdge™** 서버 및 **Dell PowerVault™** 스토리지 시스템에 적용됩니다.

이 문서의 내용은 Dell 1082DS/2162DS/4322DS Remote Console Switch에만 해당됩니다. 또한 추가 안전 사항을 잘 읽고 따라야 합니다.

- Dell Remote Console Switch 사용 설명서
- Dell 안전 지침
- Dell RTF 규제 기술 회보

일반 사항

- 다음과 같은 서비스 표시에 주의하고 이를 준수하십시오.
- 시스템 설명서에 설명된 경우가 아니면 제품을 수리하지 마십시오.
- 번개 모양의 삼각형 기호로 표시된 덮개를 열거나 분리하는 경우 감전의 위험에 노출될 수 있습니다.
- 이 격실 내부의 구성부품은 숙련된 서비스 전문가만 수리할 수 있습니다.
- 이 제품에는 사용자가 직접 수리할 수 있는 구성부품이 없습니다. 제품을 열지 마십시오.

다음과 같은 상황이 발생하면 제품을 전원 콘센트에서 분리하고 부품을 교체하거나 숙련된 서비스 기사에게 문의하십시오.

- 전원 케이블, 연장 케이블 또는 플러그가 손상된 경우
 - 물체가 제품으로 떨어진 경우
 - 제품이 물에 젖은 경우
 - 제품을 떨어뜨리거나 제품이 손상된 경우
 - 다음과 같은 사용 지침을 준수하지 않으면 제품이 올바르게 작동하지 않습니다.
- 시스템을 난방기나 열원에 가까이 하지 마십시오. 또한 냉각용 통풍구를 막지 않도록 주의하십시오.
 - 시스템 구성부품에 음식 또는 액체를 흘리거나 제품을 다습한 환경에서 작동하지 마십시오. 시스템이 물에 젖은 경우 문제 해결 정보의 해당 부분을 참조하거나 숙련된 서비스 기사에게 문의하십시오.
 - 이 제품과 다른 장비를 사용하려면 반드시 인증 여부를 확인하십시오.

- 덮개를 분리하거나 내부 구성부품을 만지기 전에 제품의 열을 식히십시오.
- 정격 전압 및 전류 레이블에 표시된 유형의 외부 전원으로만 제품을 작동시키십시오. 필요한 전원의 유형을 모를 경우 서비스 기사 또는 지역 전력 회사에 문의하십시오.



참고: 시스템 손상을 방지하려면 전원 공급 장치의 전압 선택 스위치(제공되는 경우)를 지역에 공급되는 AC 전원에 가장 근접한 전압으로 설정하십시오. 또한 모니터 및 기타 연결된 장치가 정격 범위에서 작동하는지 확인해야 합니다.

- 모니터 및 기타 연결된 장치가 해당 지역에 공급되는 전원으로 작동 가능한 정격 전압 및 전류 제품인지 확인하십시오.
- 제품과 함께 제공되는 전원 케이블만 사용하십시오.
- 감전 사고를 방지하려면 시스템과 주변기기의 전원 케이블을 적절하게 접지 처리된 전원 콘센트에 연결하십시오. 전원 케이블에는 적절하게 접지가 이루어질 수 있도록 3발 플러그가 장착되어 있습니다. 어댑터 플러그를 사용하거나 케이블에서 접지봉을 제거하지 마십시오.
- 연장 케이블과 멀티 탭의 정격 전압 및 전류를 준수하십시오. 멀티 탭에 연결된 모든 장치의 정격 전류 합계가 멀티 탭 정격 전류 한계치의 80%를 초과하지 않도록 주의하십시오.
- 전력이 급격히 상승하거나 하강하는 경우 시스템을 보호하려면 서지 방지기 (Surge Suppressor), 라인 컨디셔너 또는 무정전 전원 장치 (UPS)를 사용하십시오.
- 시스템 케이블과 전원 케이블을 주의해서 배치하십시오. 케이블이 밟히거나 걸리지 않도록 배선해야 합니다. 케이블 위에는 물건을 올려놓지 마십시오.
- 전원 케이블 또는 플러그를 변형하지 마십시오. 시설의 구조를 변경하려면 인증된 전기 기사 또는 전력 회사에 문의하십시오. 항상 지역/국가별 배선 규정을 준수하십시오.

LAN 옵션

- 번개 폭풍이 칠 때에는 연결하거나 사용하지 마십시오. 번개로 인한 전기 쇼크 위험이 있을 수 있습니다.
- 다습한 환경에서는 연결하거나 사용하지 마십시오.

설치

RCS는 이더넷이나 모뎀 연결을 사용하여 네트워크 상에 있는 스위치에 연결된 작업자와 대상 장치 간에 KVM 및 직렬 정보를 전송합니다. RCS는 이더넷을 통한 통신에 TCP/IP를 사용합니다. 최적의 시스템 성능을 위해 전용 스위치 방식의 100BaseT 또는 1000BaseT 네트워크를 사용합니다. 10BaseT 이더넷도 사용할 수 있습니다.

RCS는 V.34, V.90 또는 V.92 모뎀을 통한 통신에 Point-to-Point Protocol (PPP)을 사용합니다. OBWI 또는 Avocent 관리 소프트웨어를 사용하여 KVM 및 직렬 스위치 작업을 수행할 수 있습니다. Avocent 관리 소프트웨어의 자세한 내용은 <http://www.avocent.com>을 참조하십시오.

RCS 상자에는 RCS, RCS 소프트웨어 및 OBWI가 포함되어 있습니다. RCS 소프트웨어나 OBWI 사용을 선택하여 시스템을 관리할 수 있습니다. OBWI는 단일 RCS 및 해당 연결을 관리하는 반면 RCS 소프트웨어는 복수 스위치 및 해당 연결을 관리할 수 있습니다. OBWI만 사용할 계획이라면 RCS 소프트웨어를 설치할 필요가 없습니다.



참고: RCS 소프트웨어를 사용하여 일부 스위치를 관리할 수 있습니다. 자세한 내용은 해당 제품의 설치/사용자 설명서를 참조하십시오.



참고: 모든 RCS가 최신 버전의 펌웨어로 업그레이드되었는지 확인하십시오. OBWI를 통한 RCS 업그레이드에 대한 정보는 51페이지의 "RCS 도구"를 참조하십시오.

RCS 빠른 설정

다음은 빠른 설정 목록입니다. RCS를 하나의 랙에게 장착하여 시작하고 자세한 설치 설명을 보려면 15페이지의 "시작"을 참조하십시오.

1 각 서버의 마우스 가속도를 Slow 또는 None으로 조정합니다.

- 2 RCS 하드웨어를 설치하고 SIP(Server Interface Pod) 또는 Avocent® IQ 모듈을 각 서버 또는 다층 구성 스위치에 연결합니다. CAT 5 케이블로 각 SIP 또는 Avocent IQ 모듈을 RCS에 연결하고 키보드, 모니터 및 마우스 커넥터를 RCS의 아날로그 포트에 연결합니다
- 3 로컬 포트 주변 기기를 RCS 후면 패널의 해당 포트에 연결하고 네트워크 구성을 설정합니다. IP 주소는 여기서 또는 RCS 소프트웨어에서 설정할 수 있습니다. 고정 IP 주소를 사용하면 구성이 쉽기 때문에 Dell은 고정 IP를 권장합니다.
- 4 로컬 포트를 사용하여 OBWI 인터페이스를 사용하는 모든 서버 이름을 입력합니다.

RCS 소프트웨어를 설정하려면 (RCS 소프트웨어 사용 설명서 참조):

- 1 RCS 소프트웨어를 각 클라이언트 워크스테이션에 설치합니다.
- 2 클라이언트 워크스테이션에서 RCS 소프트웨어를 실행합니다.
- 3 **New RCS task** 버튼을 클릭하여 새 스위치를 RCS 소프트웨어 데이터베이스에 추가합니다. 위의 설명에 따라 IP 주소를 구성했으면 **Yes, the product already has an IP address**를 선택하고 그렇지 않은 경우에는 **No, the product does not have an IP address**를 선택합니다.

RCS 소프트웨어는 RCS 및 해당 RCS에 연결된 모든 SIP를 찾아 Explorer에 이름을 표시합니다.



참고: RCS 소프트웨어를 통한 Dell RCS 추가 및 관리 작업을 포함하여 일부 Avocent 스위치를 추가 및 관리할 수 있습니다.

- 4 Explorer를 통해 위치, 사이트 또는 폴더에 원하는 대로 등록 정보와 그룹 서버를 설정합니다.
- 5 OBWI를 통해 사용자 계정을 만듭니다. 자세한 내용은 76페이지의 "사용자 계정 설정"을 참조하십시오.
- 6 클라이언트 워크스테이션이 설치되면 **File - Database - Save**를 선택하여 모든 설정과 함께 데이터베이스 사본을 저장합니다.

- 7 두 번째 클라이언트 워크스테이션에서 **File - Database - Load**를 클릭하여 저장한 파일을 검색합니다. 파일을 선택하고 **Load**를 클릭합니다.
- 8 이 파일을 로드한 후에 로컬 사용자가 SIP를 추가, 삭제 또는 이름을 변경할 경우 **RCS**를 선택하고 **Resync**를 클릭하여 로컬 스위치를 재동기화할 수 있습니다. 연결된 서버를 제어하려면 Explorer에서 서버를 선택하고 **Connect Video** 작업 버튼을 클릭하여 Viewer에서 서버 세션을 실행합니다.
- 9 Viewer에서 서버 비디오의 해상도 (View - Scaling 선택) 및 품질 (View - Color 선택)을 조정합니다.

시작

다음은 Remote Console Switch와 함께 제공되는 품목입니다. RCS를 설치하기 전에 올바른 설치에 필요한 품목을 확인합니다.

- Remote Console Switch
- 점퍼 코드
- 0U 마운팅 브래킷
- 1U 마운팅 브래킷 하드웨어 키트 (RCS에 미리 장착된 2개의 추가 레일이 키트 부속품에 포함되어 있음)
- 설정 및 모뎀을 위한 케이블 및 어댑터
- Remote Console Switch 시스템 사용 설명서가 들어 있는 CD
- Dell 안전 지침
- Dell RTF 규제 기술 회보

필요한 추가 항목:

- 연결된 장치 하나당 Dell SIP 또는 Avocent IQ 모듈 1개
- 연결된 장치 하나당 CAT 5 패치 케이블 (최대 45미터) 1개

옵션 품목

- V.34, V.90 또는 V.92-호환 가능한 모뎀 및 케이블
- 전원 제어 장치
- 포트 확장 모듈 (PEM)



참고: 서버가 PEM을 통해 연결된 경우 가상 미디어 세션이나 CAC 세션을 열 수 없습니다.

네트워크 설정

스위치는 스위치와 대상 장치를 고유하게 식별하기 위해 IP 주소를 사용합니다. RCS에서는 DHCP(Dynamic Host Configuration Protocol) 및 정적 IP 주소 지정을 모두 지원합니다. 각 스위치에 대해 IP 주소가 예약되어 있으며 스위치가 네트워크에 연결되어 있는 동안 각 IP 주소가 정적으로 유지되도록 하십시오.

키보드

USB 키보드 및 마우스는 RCS의 아날로그 포트에 연결할 수 있습니다.



참고: 또한 RCS는 아날로그 포트에 여러 개의 키보드 및 마우스를 사용할 수 있도록 지원합니다. 그러나 둘 이상의 입력 장치를 동시에 사용할 경우 예측할 수 없는 결과가 발생할 수 있습니다.

랙 장착 RCS

RCS를 랙 선반에 배치하거나 스위치를 직접 19" 넓이의 EIA-310-E 호환 랙(4 포스트, 2 포스트 또는 나사산 방법)에 장착할 수 있습니다. Dell ReadyRails™ 시스템은 1U 전면 랙, 1U 후면 랙 및 2 포스트에 설치할 수 있습니다. ReadyRails 시스템에는 2개의 개별 포장된 레일 어셈블리와 RCS의 측면에 연결되어 배송된 2개의 레일이 있습니다. 또한 0U 구성을 위한 하나의 장착 브라킷이 제공되며 후면 랙 설치를 위한 하나의 블랭킹 패널이 제공됩니다.



경고: 이 표시는 간략한 참고 표시입니다. 시작하기 전에 안전, 환경 및 규제 정보 소책자의 안전 지침을 읽으십시오.



참고: 이 문서의 그림에는 특정 스위치가 표시되지 않습니다.

랙 장착 안전 고려 사항

- 랙 적재: 랙에 과부하가 걸리거나 기계적 부하가 일정하지 않으면 선반이나 랙이 고장나서 장비를 손상시키거나 인체에 부상을 입힐 수 있습니다. 따라서 장비를 장착하기 전에 랙의 위치를 정하고 안정하게 고정시켜야 합니다. 장비는 랙의 하단부터 위쪽으로 차례대로 장착해야 합니다. 랙의 적재 정량을 초과하지 않도록 합니다.
- 전원 고려 사항: 장치에 지정된 전원에만 연결하십시오. 하나의 랙에 여러 개의 전기 구성품을 설치할 때에는 전체 구성품 전원 정격이 회로의 용량을 초과하지 않도록 해야 합니다. 전원에 과부하가 걸리거나 연장 코드를 지나치게 많이 사용하면 화재나 감전의 위험이 있습니다.
- 주변 온도 상승: 밀폐된 랙어셈블리에 설치한 경우, 랙환경의 작동 온도가 실내 온도보다 높을 수 있습니다. 기기의 주위 온도가 최대 50°C를 초과하지 않도록 주의하십시오.
- 감소되는 공기 흐름: 장비의 안전한 작동에 필요한 공기 흐름을 막지 않도록 장비를 랙에 설치하십시오.
- 올바른 접지: 랙에 장착된 장비에 확실한 접지를 유지하십시오. 직접 연결 이외에 분기 회로에 전원을 연결할 때(예: 멀티 탭 사용)에는 특히 주의하십시오.
- 아래 방향을 향하는 후면 패널로 제품을 장착하지 마십시오.

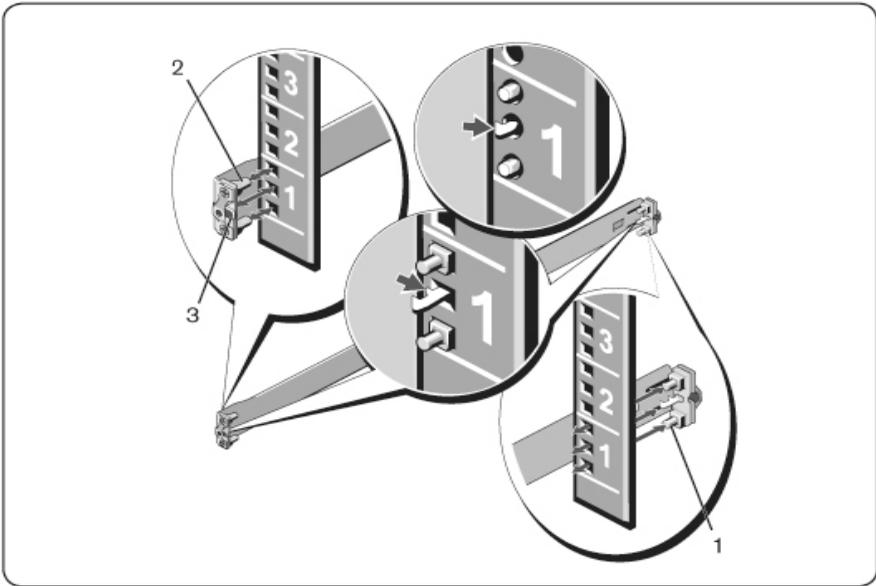
Dell ReadyRails™ 시스템 설치

ReadyRails 시스템은 RCS의 설치를 위해 랙을 쉽게 구성할 수 있도록 설계되었습니다. ReadyRails 시스템은 1U 도구 미사용 방법이나 3개의 가능한 1U 도구 사용 방법 중 하나(2 포스트 수평 장착, 2 포스트 중앙 장착 또는 4 포스트 나사산)를 사용하여 설치할 수 있습니다.

1U 도구 미사용 구성 (4개의 포스트 사각 구멍 또는 나사산 없는 원형 구멍)

- 1 ReadyRails 플랜지 귀가 밖으로 향한 상태에서 좌우 세로 포스트 사이에 하나의 레일을 배치하십시오. 후면 플랜지 레일 못을 후면 세로 포스트 플랜지에 정렬하여 배치합니다. 그림 2.1은 사각 및 나사산 없는 원형 구멍에 끼워진 항목 1과 해당 돌출부를 나타냅니다.

그림 2.1. 1U 도구 미사용 구성



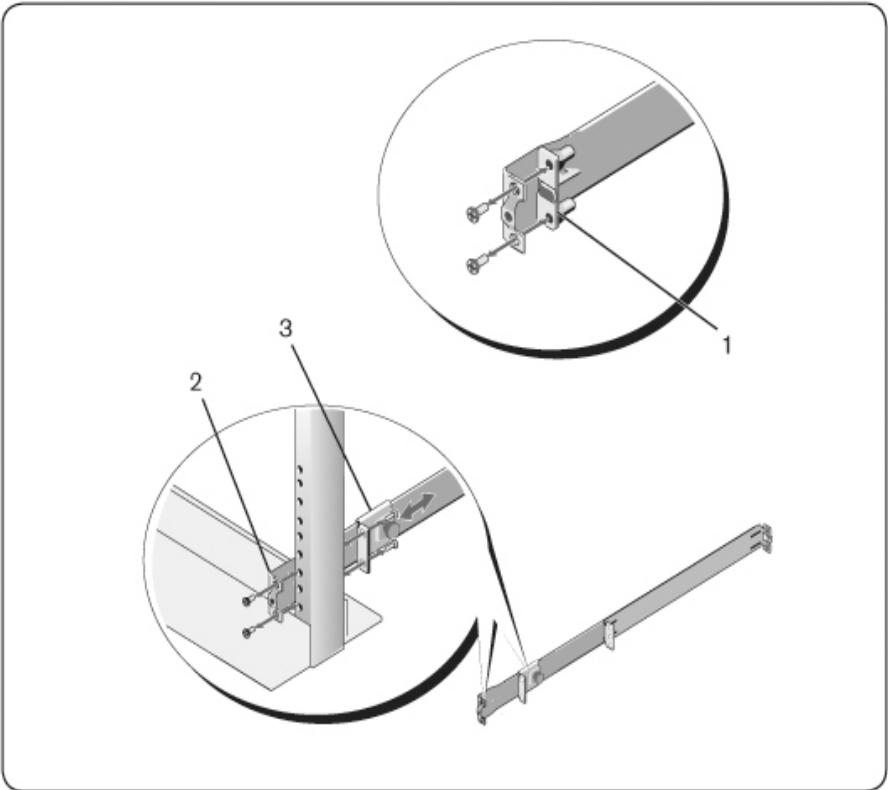
- 2 전면 플랜지 못을 세로 포스트의 전면 에 있는 구멍에 맞춰 끼웁니다 (항목 2).
- 3 두 번째 레일에 이 절차를 반복합니다.

4 각 레일을 제거하려면 각 플랜지 귀(항목 3)의 래치 해제 버튼을 당겨 각 레일을 제거합니다.

2 포스트 수평 장착 구성

1 이 구성의 경우 캐스팅은 각 ReadyRails 어셈블리의 전면에서 제거해야 합니다(그림 2.2, 항목 1). Torx™ 드라이버를 사용하여 레일의 장치 쪽에 있는 각 전면 플랜지 귀에서 2개의 나사를 제거하고 각 캐스팅을 제거합니다. 향후 랙 요구를 위해 캐스팅을 보관합니다. 후면 플랜지 캐스팅을 제거할 필요는 없습니다.

그림 2.2. 2 포스트 수평 장착 구성

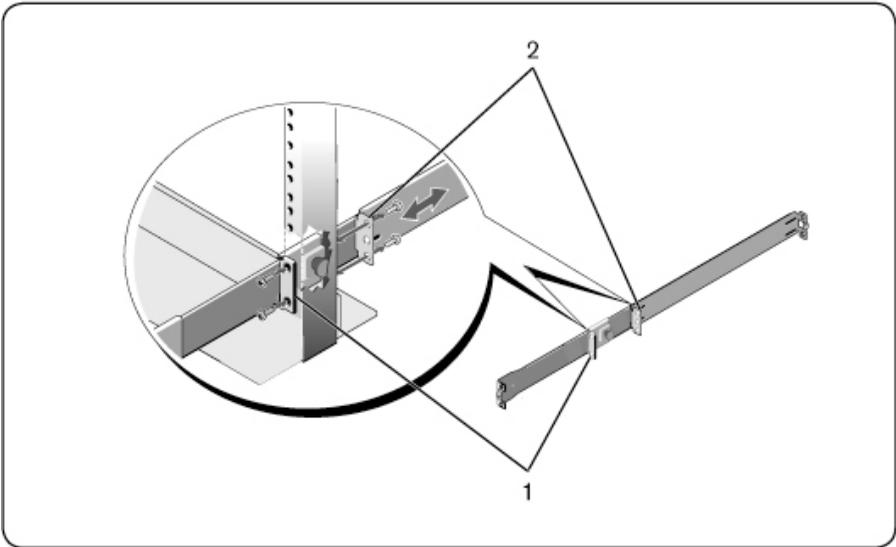


- 2 2개의 제공된 나사를 사용하여 하나의 레일을 전면 포스트 플랜지에 연결합니다(항목 2).
- 3 세로 포스트 쪽으로 플런저 브래킷을 밀고 플런저 브래킷을 2개의 사용자가 준비한 나사를 사용하여 포스트 플랜지에 고정합니다(항목 3).
- 4 두 번째 레일에 이 절차를 반복합니다.

2 포스트 중앙 장착 구성

- 1 플런저 브래킷이 제 위치에 찰칵하고 걸릴 때까지 뒤로 밀고 2개의 사용자가 준비한 나사를 사용하여 전면 포스트 플랜지에 브래킷을 고정합니다(그림 2.3, 항목 1).

그림 2.3. 2 포스트 중앙 장착 구성



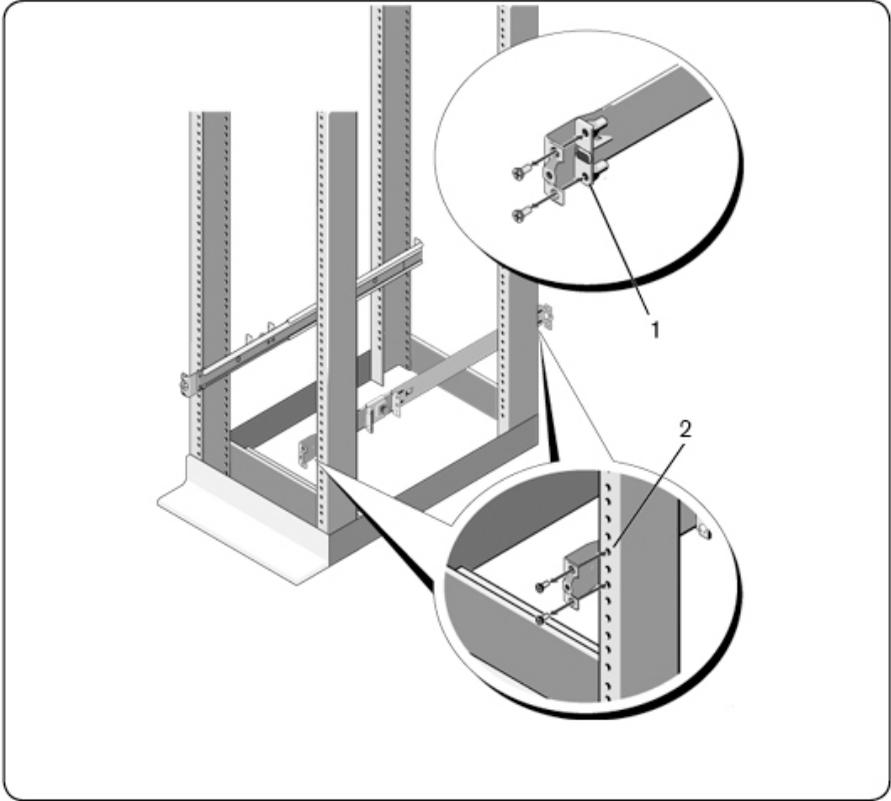
- 2 뒤 브래킷을 포스트 쪽으로 밀고 2개의 사용자가 준비한 나사를 사용하여 포스트 플랜지에 고정합니다(항목 2).

3 두 번째 레일에 이 절차를 반복합니다.

4 포스트 나사산 구성

- 1 이 구성의 경우 플랜지 귀 캐스팅을 각 ReadyRails 어셈블리의 끝에서 제거해야 합니다. Torx™ 드라이버를 사용하여 각 플랜지 귀에서 2개의 나사를 제거하고 각 캐스팅을 제거합니다(그림 2.4, 항목 1). 향후 랙 요구를 위해 캐스팅을 보관합니다.
- 2 각 레일에 대해, 전면 및 후면 플랜지를 2개의 사용자가 준비한 나사를 사용하여 각각의 끝에서 포스트 플랜지에 연결합니다(항목 2).

그림 2.4.4 포스트 나사산 구성



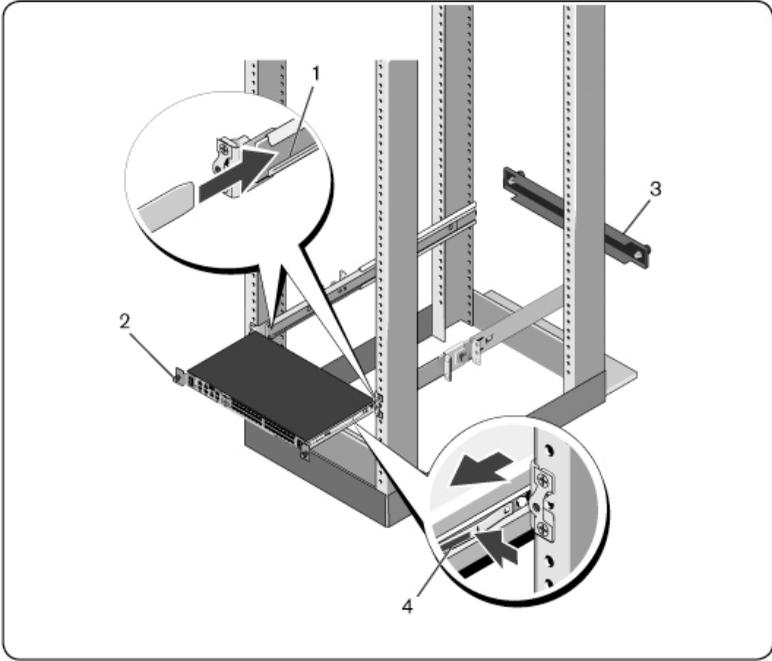
RCS 설치

스위치는 1U 후면 랙, 1U 전면 랙, 1U 2 포스트(수평 및 중앙) 및 0U 구성으로 장착할 수 있습니다. 다음은 1U 후면 랙, 1U 전면 랙 및 0U 구성의 예입니다. 1U 2 포스트(수평 및 중앙) 구성의 경우, 4 포스트 구성과 동일한 방법으로 스위치를 레일에 밀어 넣을 수 있습니다.

1U 후면 랙 설치

1 스위치에 연결된 레일의 끝을 ReadyRails 어셈블리에 끼우고 스위치를 랙으로 밀어 넣습니다(그림 2.5, 항목 1).

그림 2.5. 1U 후면 랙 설치



2 엄지 나사로 각 스위치 레일을 고정합니다(항목 2).

3 블랭킹 패널을 랙 전면의 레일에 조립하고 엄지 나사로 조입니다(항목 3)(옵션).

랙에서 스위치를 제거하려면:

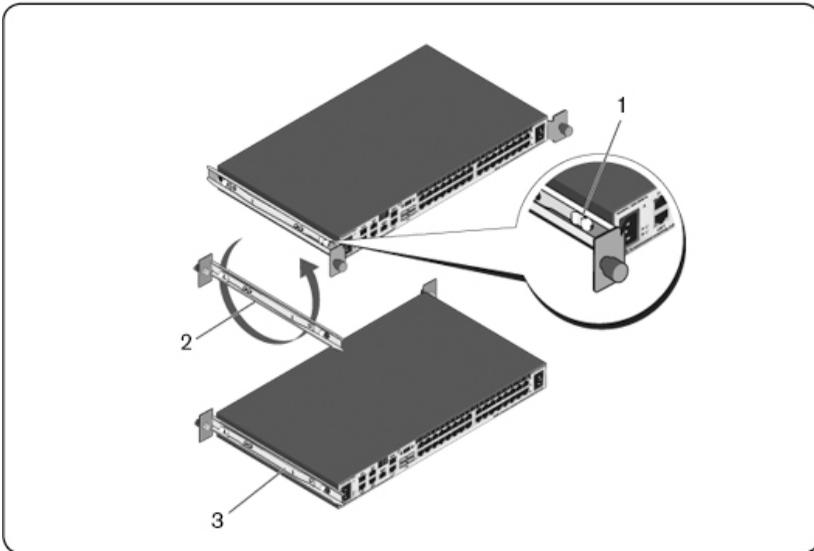
- 1 엄지 나사를 풀고 스위치 어셈블리를 이동 정지 위치에 도달할 때까지 랙에서 잡아 당깁니다. 이동 정지 위치는 레일 그룹을 재배치할 수 있도록 하기 위한 것이며 수리를 위한 것은 아닙니다.
- 2 스위치 레일 측면에서 파란색 탭을 찾으십시오(항목 4).
- 3 탭을 안 쪽으로 밀고 스위치 레일이 ReadyRails 어셈블리에서 제거될 때까지 어셈블리를 잡아 당깁니다.

10 전면 랙 설치

설치 전에 스위치에 연결된 레일을 재구성해야 합니다.

- 1 각 스위치 레일에서 전면 격리 애자 아래의 탭을 들어 올리고 레일을 스위치에서 들어 올리면서 레일을 앞 쪽으로 밀니다(그림 2.6, 항목 1).

그림 2.6. 스위치 레일 회전



- 2 각 레일을 180°(항목 2) 회전한 다음 각 레일을 스위치에 재조립합니다(항목 3).
- 3 1U 후면 랙 설명을 참조하여 스위치 어셈블리를 ReadyRails 시스템에 삽입 및 제거합니다.

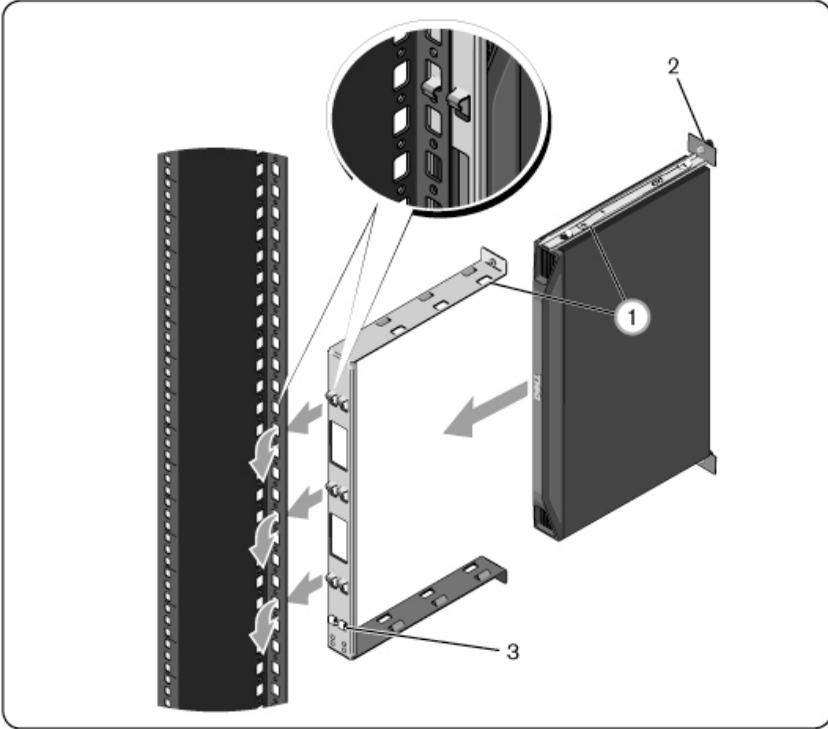


참고: 이 구성에는 블랭킹 패널이 필요없습니다.

0U RCS 설치

- 1 0U 장착 브래킷을 스위치 레일에 맞춰 조립합니다(그림 2.7, 항목 1). 엄지 나사를 조입니다(항목 2).
- 2 장착 브래킷 고리를 랙 구멍에 끼우고 파란색 버튼이 튀어 나오고 브래킷이 제 자리에 고정될 때까지 누릅니다.

그림 2.7. 0U 설치



스위치 어셈블리를 제거하려면 파란색 버튼(항목 3)을 눌러 브래킷을 풀고 어셈블리를 포스트에서 들어 올립니다.

RCS 하드웨어 연결

다음 그림은 DSR 하드웨어의 가능한 구성 방법 중 하나를 나타낸 것입니다.

그림 2.8. 기본적인 RCS 구성

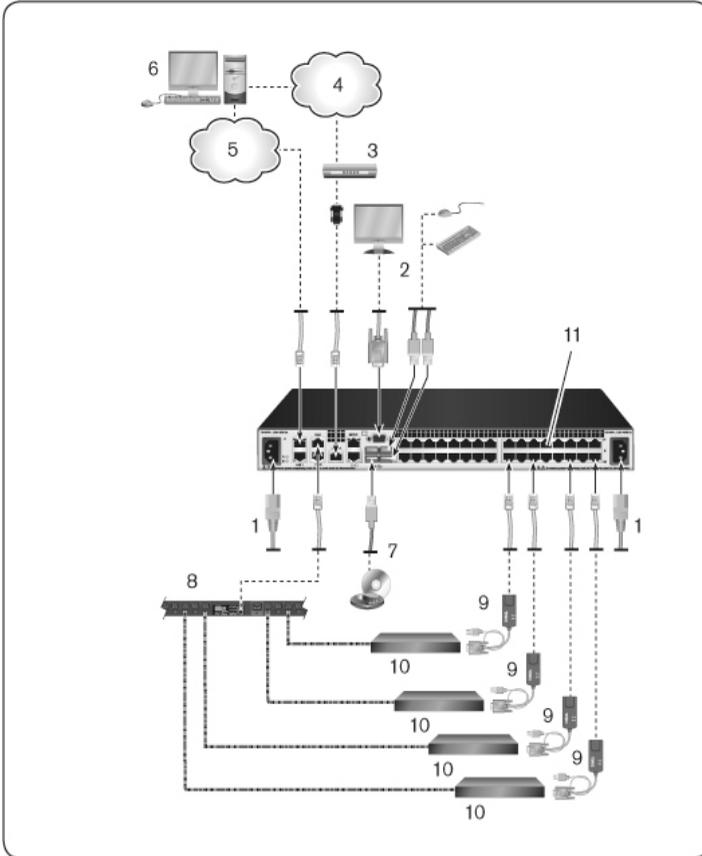


표 2.1: 기본적인 RCS 구성 설명

번호	설명	번호	설명
1	점퍼 코드	7	외부 가상 매체

번호	설명	번호	설명
2	아날로그 사용자	8	전원 제어 장치
3	모뎀	9	SIP
4	전화망	10	대상 장치
5	Network	11	RCS(표시된 32 포트 모델)
6	디지털 사용자		

연결 후 스위치를 켜려면:

 **주의:** 감전이나 장비 손상 위험을 줄이려면 점퍼 코드 접지 플러그를 사용하십시오. 접지 플러그는 중요한 안전 기능입니다. 점퍼 코드를 언제든지 쉽게 접근할 수 있는 접지된 콘센트에 꽂으십시오. 장비 전원을 차단하려면 전기 콘센트나 장치에서 점퍼 코드를 뽑으십시오.

 **참고:** 건물에서 3상 AV 전원을 사용하는 경우 서버와 모니터에서 같은 상을 사용하도록 하여 상과 관련된 잠재적인 비디오나 키보드 관련 문제를 방지하십시오.

 **참고:** 스위치에서 연결 장치까지의 최대 지원 케이블 길이는 30미터입니다.

- 전원 접지 플러그를 비활성화하지 마십시오. 접지 플러그는 중요한 안전 기능입니다.
- 점퍼 코드를 언제든지 쉽게 접근할 수 있는 접지된 콘센트에 연결하십시오.
- 제품의 전원을 차단하려면 전원이나 제품에서 점퍼 코드를 분리하십시오.
- 이 제품의 전원을 차단하려면 기본적으로 AC 코드의 연결을 끊습니다. AC 코드가 두 개 이상인 제품의 경우 전원을 완전히 차단하려면 모든 AC 선 코드를 뽑아야 합니다.
- 이 제품의 제품 엔클로저 내부에는 사용자가 수리할 수 있는 부품이 없습니다. 제품 덮개를 열거나 제거하지 마십시오.

- 1 VGA 모니터와 USB 키보드 및 마우스 케이블을 레이블이 표시된 해당 포트에 연결하십시오.
- 2 UTP 케이블(4쌍, 최대 150ft/45m)의 한쪽 끝을 숫자가 부여된 사용 가능한 포트에 꽂습니다. 다른 쪽 끝을 SIP의 RJ 45 커넥터에 연결합니다.
- 3 SIP을 대상 장치의 후면에 있는 해당 포트에 연결합니다. 연결할 모든 대상 장치에 대해 2와 3단계를 반복합니다.



참고: Sun Microsystems 대상 장치를 연결할 때에는 로컬 포트의 다중 동기 모니터를 사용하여 Sun 컴퓨터를 VGA와 sync-on-green 또는 합성 동기가 모두 지원되도록 하십시오.

- 4 사용자의 UTP 케이블을 이더넷 네트워크에서 RCS 후면의 LAN 포트에 연결합니다. 네트워크 사용자는 이 포트를 통해 RCS에 액세스합니다. 중복 LAN 포트를 별도의 이더넷 스위치에 꽂으면 하나의 이더넷 스위치에 장애가 일어날 경우 추가적인 중복성을 제공합니다.
- 5 스위치는 ITU V.92, V.90 또는 V.24 호환 모뎀을 사용하여 액세스할 수도 있습니다(옵션). RJ-45 케이블의 한쪽 끝을 스위치 후면의 MODEM 포트에 꽂습니다. 반대쪽 끝을 제공된 RJ-45 대 DB-9(수) 어댑터에 꽂은 다음, 모뎀 후면의 해당 포트에 연결합니다.



참고: LAN 연결 대신 모뎀 연결을 사용하면 스위치의 성능이 제한됩니다.

- 6 CAT 5 케이블의 한쪽 끝을 스위치의 PDU1 포트에 연결하여 지원되는 PDU를 RCS에 연결합니다(옵션). 다른 쪽 끝을 PDU에 연결합니다. 대상 장치의 전원 코드를 PDU에 꽂습니다. PDU를 전원에 연결합니다. 필요한 경우 PDU2 포트에 대해 이 절차를 반복하여 두 번째 PDU에 연결합니다.
- 7 각 대상 장치를 켜려면 스위치와 함께 공급된 점퍼 코드를 찾으십시오. 전원 코드의 한쪽 끝을 스위치 후면의 전원 소켓에 연결합니다. 반대쪽 끝을 적절한 전원에 연결합니다. 이 중 전원이 장착된 RCS를 사용하는 경우 두 번째 점퍼 코드를 사용하여 RCS 후면의 두 번째 전원 소켓에 연결하고 반대쪽 끝을 다른 전원에 꽂습니다.

 **참고:** 중복 전원 공급 장치를 별도의 분기 회로에 꽂아 외부 AC 전원이 공급되지 않을 경우 추가적인 중복성을 제공합니다.

8 가상 매체 장치 또는 스마트 카드 판독기를 스위치에 있는 USB 포트 중 하나에 연결합니다(옵션).

 **참고:** 모든 가상 미디어 세션에 대해 USB2 또는 USB2+CAC SIP를 사용해야 합니다.

SIP 연결

SIP를 각 서버에 연결하는 방법:

- 1 해당 RCS에 대한 SIP를 찾습니다.
- 2 PS/2 SIP 연결을 사용하는 경우 SIP의 색상이 표시된 끝을 이 Remote Console Switch에 연결되는 첫 번째 서버의 적절한 키보드, 모니터 및 마우스 포트에 연결합니다. USB 연결을 사용하는 경우 SIP 플러그를 이 Remote Console Switch 장치에 연결되는 첫 번째 서버의 USB 포트에 연결합니다.
- 3 SIP의 RJ-45 커넥터의 경우에는 SIP에서 실행될 CAT 5 케이블의 한쪽 끝을 Remote Console Switch 장치에 연결합니다. 그림 2.9을 참조하십시오.
- 4 CAT 5 케이블의 반대쪽 끝을 RCS 후면의 원하는 ARI(Avocent Rack Interface) 포트에 연결합니다.
- 5 연결하려는 모든 서버에 대해 2~ 4단계를 반복합니다.

 **참고:** 서비스를 시작하기 전에 RCS 전원을 끕니다. 점퍼 코드는 항상 전원에서 분리합니다.

 **참고:** Dell SIP 이외에도 RCS를 Sun 및 Serial IQ 모듈을 포함하여 Avocent IQ 모듈을 사용하는 장치에 연결할 수 있습니다.

그림 2.9. SIP 연결

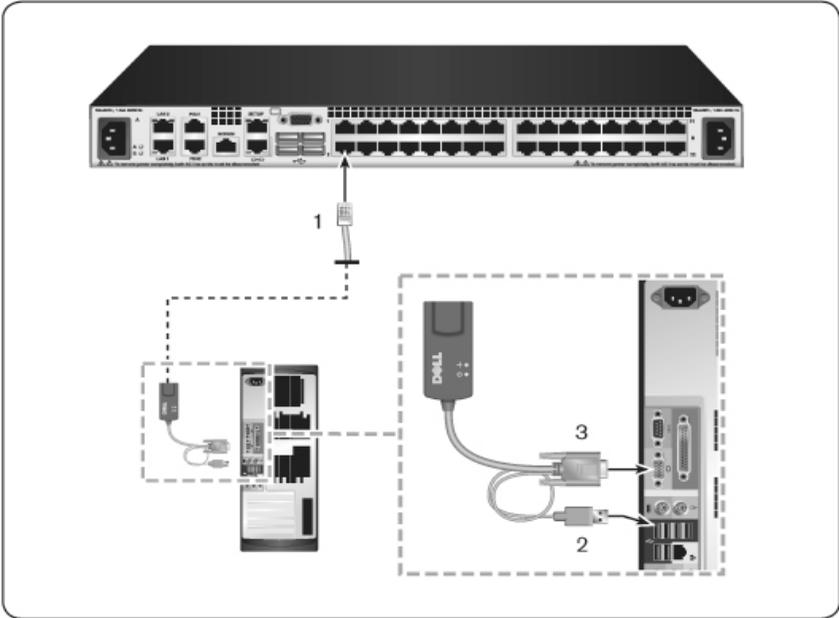


표 2.2: 그림 2.9 설명

번호	설명
1	CAT 5
2	USB 연결
3	VGA 연결

UTP 커넥터를 사용하여 SIP를 직렬 장치에 연결하려면:

- 1 SIP RJ-45 커넥터를 직렬 장치에 연결합니다.

-또는-

SIP을 RJ-45 대 9핀 암컷 어댑터에 연결합니다. 어댑터를 직렬 장치의 직렬 포트에 연결합니다.

- 2 UTP 케이블 (4쌍, 최대 150 ft/45 m)의 한 쪽 끝을 스위치 후면의 가용한 번호 포트에 연결합니다. 다른 쪽 끝을 SIP의 RJ-45 커넥터에 연결합니다.
- 3 USB 대 배럴 전원 코드를 SIP의 전원 커넥터에 연결합니다. USB 대 배럴 전원 코드의 USB 커넥터를 직렬 대상 장치의 가용한 USB 포트에 연결합니다.

다층 구성 스위치 추가



참고: RCS는 EL80-DT를 지원하지 않습니다.



참고: M1000e Modular Enclosure는 계층식 구성에서 지원됩니다. CAT 5 케이블의 한 쪽 끝을 RCS 스위치의 대상 포트에 연결합니다. ACI(Analog Console Interface) 호환 가능 RJ45 포트의 다른 쪽 끝을 M1000e 새시의 뒷면에 있는 iKVM 모듈에 연결합니다. M1000e Modular Enclosure의 구성요소로 평웨어 업그레이드는 이 계층식 구성을 통해 가능하지 않습니다.

최대 2층의 스위치를 구성하여 사용자가 최대 1024 서버에 연결할 수 있도록 할 수 있습니다. 다층 구성 시스템에서 주 스위치의 각 대상 포트는 각 다층 구성 스위치의 ACI 포트에 연결됩니다. 그런 다음 각 다층 구성 스위치는 SIP 또는 Avocent IQ 모듈을 통해 장치로 연결할 수 있습니다.

여러 스위치를 다층 구성하려면:

- 1 UTP 케이블의 한쪽 끝을 스위치의 대상 포트에 연결합니다.
- 2 UTP 케이블의 반대쪽 끝을 다층 구성 스위치 후면의 ACI 포트에 연결합니다.
- 3 장치를 다층 구성 스위치에 연결합니다.
- 4 시스템에 연결할 모든 다층 구성 스위치에 대해 이 단계를 반복합니다.



참고: 시스템에서 두 스위치를 자동으로 "병합"합니다. 다층 구성 스위치에 연결된 모든 스위치는 로컬 UI의 주 스위치 목록에 표시됩니다.

참고: 스위치는 주 스위치의 대상 포트 당 하나의 다층 구성 스위치를 지원 합니다. 하나의 스위치를 다층 구성 스위치에 연결할 수 없습니다.

참고: RCS에 종속 연결할 경우 기본 장치가 다층 구성되어 있기 때문에 8포트나 16포트 아날로그 콘솔 스위치는 지원되지 않습니다. RCS는 기본 장치여야 합니다.

그림 2.10. RCS를 UTP 아날로그 스위치와 다층 구성

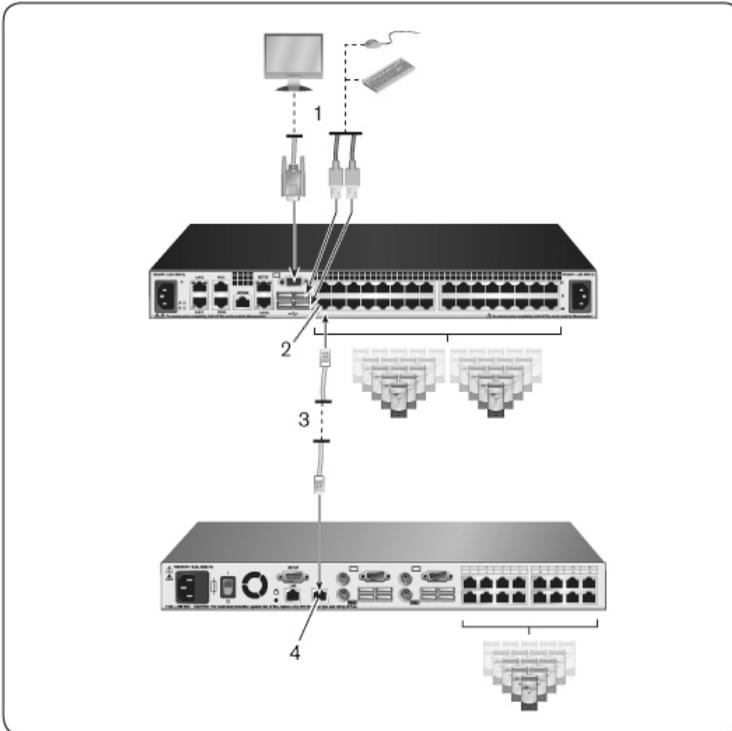


표 2.3: 그림 2.10 설명

번호	설명
1	로컬 사용자
2	ARI 연결
3	UTP 연결
4	ACI 연결

리거시 스위치의 종속 연결 구성

리거시 스위치(옵션)를 추가하려면:

- 1 랙에 스위치를 장착합니다. UTP 케이블을 찾아 RCS를 리거시 스위치에 연결합니다.
- 2 UTP 케이블의 한쪽 끝을 콘솔 스위치의 ARI 포트에 연결합니다.
- 3 UTP 케이블의 반대쪽 끝을 PS/2 SIP에 연결합니다.
- 4 스위치 제조업체의 권장 사항에 따라 SIP를 리거시 스위치에 연결합니다.
- 5 스위치에 연결하려는 모든 리거시 스위치에 대해 1-4 단계를 반복합니다.



참고: RCS는 ARI 포트 당 하나의 스위치만 지원합니다. 이 첫 번째의 스위치에 다른 스위치를 종속 연결할 수 없습니다.



참고: RCS에 종속 연결할 경우 기본 장치이기 때문에 8포트나 16포트 아날로그 콘솔 스위치는 지원되지 않습니다. RCS는 기본 장치여야 합니다.

그림 2.11. 리거시 스위치 종속 연결

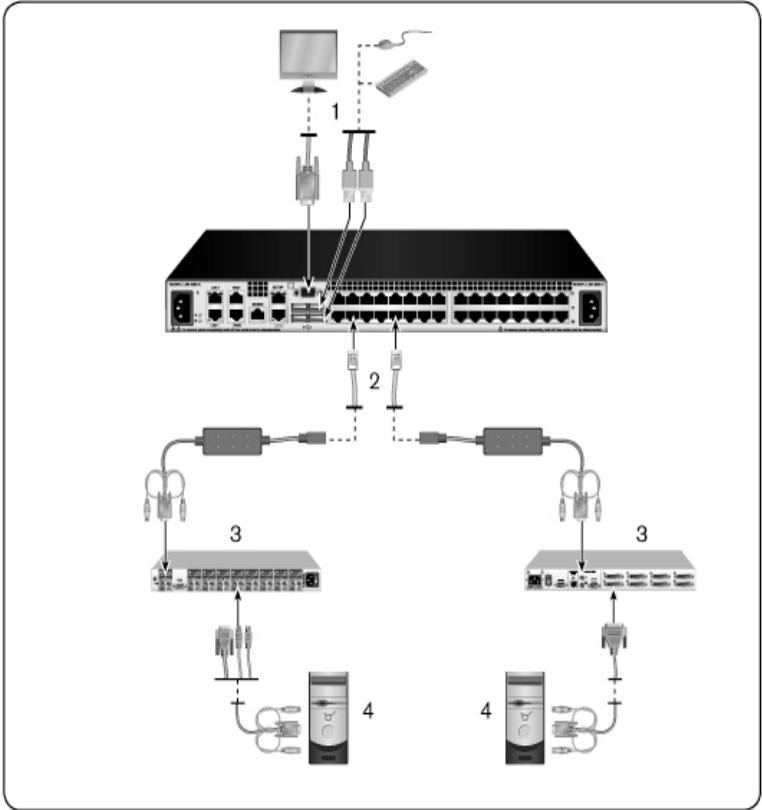


표 2.4: 그림 2.11 설명

번호	설명
1	로컬 사용자
2	ARI 연결

번호	설명
3	PS2 연결
4	연결 대상

PEM(옵션) 추가

PEM(Port Expansion Module)을 사용하면 각 ARI 포트를 확장하여 1대가 아니라 최대 8대의 장치를 연결할 수 있습니다. 다음 그림과 그림 설명표를 참조하십시오.

 **참고:** PEM은 수동으로 작동합니다. 따라서 사용자가 일단 PEM에 연결된 장치에 접속하면 그 다음 사용자가 PEM에 연결된 어떤 장치에 액세스를 시도하더라도 차단됩니다.

 **참고:** PEM 뒤에서 VM 또는 CAC SIP 사용은 지원되지 않습니다.

 **참고:** True Serial SIP가 PEM 뒤에서 작동하지 않습니다.

PEM(옵션)을 추가하려면:

- 1 랙에 PEM을 장착합니다. 최대 9개의 UTP 케이블을 사용하여 하나는 RCS와 PEM을 연결하고 다른 8개는 PEM을 각 장치에 연결된 SIP에 연결합니다.
- 2 PEM과 RCS 사이에 설치할 UTP 케이블의 한쪽 끝을 PEM의 다른 커넥터와 약간 떨어져 있는 RJ-45 커넥터에 연결합니다. UTP 케이블의 나머지 끝을 DSR 기기 후면의 원하는 ARI 포트에 연결합니다.
- 3 PEM 후면에 있는 8개 RJ45 커넥터 중 하나에 PEM과 각 장치의 SIP 사이에 설치할 UTP 케이블을 연결합니다.
- 4 UTP 케이블의 반대쪽 끝을 첫 번째 SIP에 연결합니다.
- 5 연결하려는 모든 장치에 대해 3~ 4단계를 반복합니다.

그림 2.12. PEM을 사용한 RCS 구성

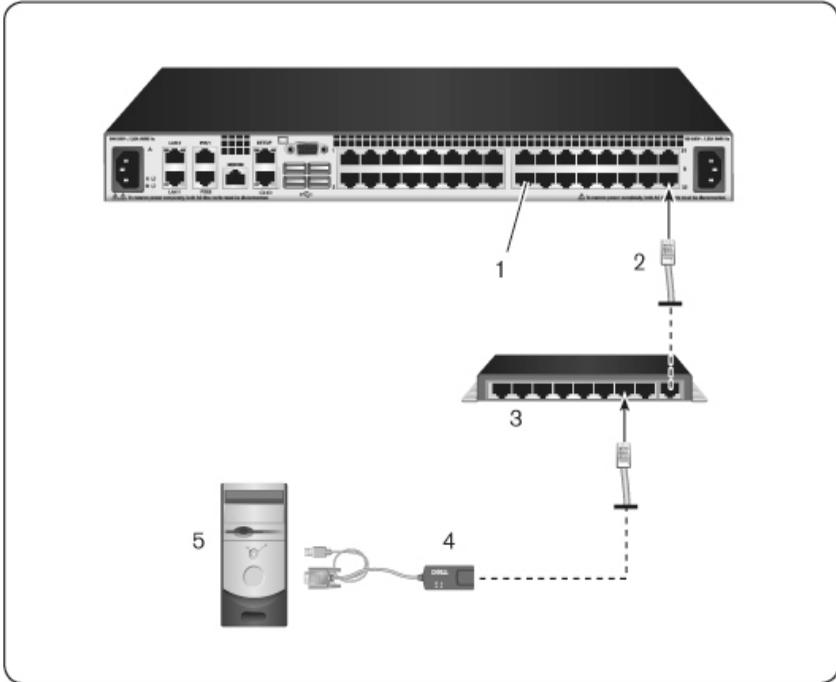


표 2.5: 그림 2.12 설명

번호	설명
1	ARI 포트
2	UTP
3	PEM
4	SIP 또는 Avocent IQ 모듈
5	서버

Remote Console Switch 구성

모든 물리적 연결이 이루어지면 전체 스위치 시스템에서 사용할 수 있도록 스위치를 구성해야 합니다. 이 작업은 두 가지 방법으로 수행할 수 있습니다.

Avocent 관리 소프트웨어를 사용하여 스위치를 구성하려면 해당 Avocent 설치/사용 설명서의 자세한 설명을 참조하십시오.

로컬 UI를 사용하여 스위치를 구성하려면:

54페이지의 "네트워크 설정"에서 로컬 UI를 통한 초기 네트워크 설정 구성에 대한 자세한 설명을 참조하십시오.

내장 웹 서버 설정

대부분의 일상적인 스위치 작업을 처리하는 내장 웹 서버를 사용하여 스위치에 액세스할 수 있습니다. 웹 서버를 사용하여 스위치에 액세스하기 전에 먼저 스위치 뒷면의 SETUP 포트나 로컬 UI를 통해 IP 주소를 지정하십시오. 스위치 사용자 인터페이스 사용에 대한 자세한 설명은 3장을 참조하십시오.

방화벽을 통해 OBWI 방화벽

액세스를 위해 OBWI를 사용하는 스위치 설치의 경우 외부 액세스를 허용하려면 다음 포트가 방화벽에서 열려 있어야 합니다.

표 2.6: 방화벽이 있는 OBWI 포트

포트 번호	기능
TCP 22	SIP에 대한 직렬 세션을 위해 SSH에 사용
TCP 23	Telnet에 사용(Telnet이 사용으로 설정된 경우)

포트 번호	기능
TCP 80	Video Viewer의 최초 다운로드에 사용됩니다. RCS 관리자는 이 값을 바꿀 수 있습니다.
TCP 443	스위치를 관리하고 KVM 세션을 실행하기 위해 웹 브라우저 인터페이스에서 사용됩니다. RCS 관리자는 이 값을 바꿀 수 있습니다.
TCP 2068	KVM 세션 데이터 전송(마우스 및 키보드) 또는 스위치에 대한 비디오 전송
TCP/UDP 3211	탐색
TCP 389	(선택 사항) LDAP 디렉토리 서비스에서 사용됨. 표준 액세스 포트
TCP 636	(선택 사항) LDAP 디렉토리 서비스에서 사용됨. 보안/SSL 포트
TCP 3268	(선택 사항) Microsoft Active Directory 서비스에 사용됨. 표준 액세스 포트
TCP 3269	(선택 사항) Microsoft Active Directory 서비스에 사용됨. 보안/SSL 액세스 포트

다음 그림과 표는 사용자 컴퓨터가 방화벽 외부에 있고 스위치가 방화벽 내부에 있는 일반적인 구성을 나타냅니다.

그림 2.13. 일반적인 RCS 방화벽 구성

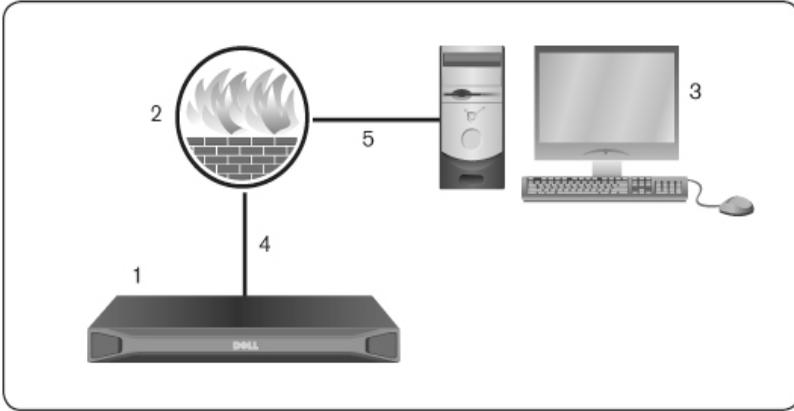


표 2.7: 그림 2.13 설명

번호	설명
1	RCS
2	방화벽
3	사용자 컴퓨터
4	방화벽은 HTTP 요청 및 KVM 트래픽을 스위치로 전달합니다.
5	사용자는 방화벽의 외부 IP 주소를 탐색합니다.

방화벽을 구성하려면:

방화벽 외부에서 스위치에 액세스하려면 방화벽 내부 인터페이스를 통해 포트 22, 23(telnet이 사용 설정된 경우), 80, 443, 2068 및 3211을 해당 외부 인터페이스에서 KVM 스위치로 전달하도록 방화벽을 구성합니다. 특정 포트 전달에 설명은 방화벽 설명서를 참조하십시오.

 **참고:** 포트 80과 443은 관리자가 구성할 수 있습니다.

OBWI 실행에 대한 내용은 45페이지의 "OBWI"를 참조하십시오.

연결 확인

후면 패널 이더넷 연결 LED

RCS의 후면 패널에는 이더넷 LAN1 연결 상태를 나타내는 두 개의 LED와 이더넷 LAN2 연결 상태를 나타내는 두 개의 LED가 있습니다.

- 녹색 LED는 네트워크에 올바른 연결이 이루어졌을 때 불이 들어오고 포트에서 전송이 이루어질 때 깜빡입니다.
- 두 색상의 LED는 녹색이나 호박색 불이 들어옵니다.
 - 통신 속도가 1000M일 경우 녹색 불이 들어옵니다.
 - 통신 속도가 100M일 경우 호박색 불이 들어옵니다.
 - 통신 속도가 10M일 경우 불이 들어오지 않습니다.

후면 패널 전원 상태 LED

각 RCS의 후면 패널에는 각 전원 공급 장치에 대한 하나의 LED 있습니다. 이 중 전원 모델(16 포트 및 32 포트)의 경우 두 개의 전원 LED 있으며 8 포트 모델의 경우 하나의 LED만 있습니다. LED는 스위치가 켜져서 정상 작동 중일 때 녹색 불이 들어옵니다.

- LED는 전원 공급 장치에 전원이 들어오지 않거나 고장 났을 때 꺼집니다.
- LED는 장치가 준비되었을 때 불이 들어옵니다.
- LED는 스위치가 부팅 중이거나 업그레이드가 진행 중일 때 깜박입니다.
- LED는 전원 공급 장치 고장, 주변 온도 상승 또는 팬 오류와 같은 장애가 발생할 경우 "SOS"를 깜박입니다. LED는 장애가 지속되면 "SOS"를 계속 깜박입니다.

스위치는 모듈의 전원이 차단된 경우 연결된 장치의 전원이 연속으로 차단되지 않도록 합니다. 그러나 사용자가 직렬 세션 뷰어에서

Serial Break를 눌러 연결 장치의 연속 차단이 발생하도록 할 수 있습니다.

조정 마우스 설정 대상 장치

원격 사용자 제어에 사용할 수 있는 스위치에 컴퓨터를 연결하기 전에 대상 마우스 속도를 설정하고 가속을 꺼야 합니다. Microsoft® Windows®(Windows NT®, 2000, XP, Server 2003)이 실행되는 시스템에서 기본 PS/2 마우스 드라이버를 사용하십시오.

로컬 마우스 움직임과 원격 커서 표시를 계속 동기화하려면 KVM 스위치를 통해 원격 시스템에 액세스하는 모든 사용자 계정에 대해 마우스 가속을 "없음"으로 설정해야 합니다. 또한 마우스 가속은 모든 원격 시스템에서 "없음"으로 설정해야 합니다. 특수 커서를 사용해서는 안 되며 포인터 꼬리, *Ctrl* 키 커서 위치 애니메이션, 커서 그림자 및 커서 숨기기와 같은 커서 표시 옵션도 꺼야 합니다.



참고: Windows 운영 체제에서 마우스 가속을 비활성화할 수 없거나 모든 대상 장치의 설정을 조정하고 싶지 않을 경우 Video Viewr 창에 있는 *Tools - Single Cursor Mode* 명령을 사용할 수 있습니다. 이 명령은 Video Viewer 창을 "마우스 숨기기" 모드로 변경하여 보고 있는 대상 시스템에 대한 마우스 포인터와 클라이언트 컴퓨터의 마우스 포인터 간에 제어를 수동으로 전환할 수 있습니다.

로컬 및 원격 구성

RCS는 다음 두 개의 "포인트 앤 클릭" 인터페이스를 제공합니다: 로컬 사용자 인터페이스(로컬 UI) 및 원격 OBWI. 이러한 인터페이스가 제공하는 구성 옵션을 사용하여 스위치를 특정 용도에 맞게 사용자 정의하고, 연결 장치를 제어하고, 모든 기본 KVM 또는 직렬 스위치 요구사항을 처리할 수 있습니다.



참고: 로컬 UI 및 원격 OBWI는 거의 동일합니다. 지정하지 않을 경우 이 장의 모든 정보는 두 인터페이스에 모두 적용됩니다.

두 인터페이스에서 두 가지 종류의 세션을 실행할 수 있습니다.

- Video Viewer 창에서 스위치에 연결된 개별 대상 장치의 키보드, 모니터 및 마우스 기능을 실시간으로 제어할 수 있습니다. 또한 사전 정의된 전역 매크로를 사용하여 Video Viewer 창에서 작업을 수행할 수 있습니다. Video Viewer 사용 방법에 대한 지침은 4장을 참조하십시오.
- Serial Viewer 창에서 명령어나 스크립트를 사용하여 개별 직렬 대상 장치를 관리할 수 있습니다.

로컬 사용자 인터페이스(UI)

스위치 후면에는 로컬 포트가 있습니다. 이 포트를 통해 키보드, 모니터 및 마우스를 직접 스위치에 연결하여 로컬 UI를 사용할 수 있습니다.

다음 키 조합 중 하나를 선택하여 로컬 UI를 열거나 로컬 UI와 활성 세션 간에 전환할 수 있도록 구성할 수 있습니다: <Print Screen>, <Ctrl

+ Ctrl>, <Shift + Shift> 및 <Alt + Alt>. 기본값은 <PrintScreen> 및 <Ctrl-Ctrl>입니다.

로컬 UI를 실행하려면:

- 1 모니터, 키보드 및 마우스 케이블을 스위치에 연결합니다. 자세한 내용은 26페이지의 "RCS 하드웨어 연결"을 참조하십시오.
- 2 로컬 UI를 실행하려면 활성화된 키 입력 중 하나를 누르십시오.
- 3 로컬 UI 인증이 활성화된 경우 사용자 이름 및 비밀번호를 입력합니다.



참고: Avocent 관리 소프트웨어 서버에 스위치를 추가한 경우 사용자를 인증하기 위해 Avocent 관리 소프트웨어 서버를 액세스합니다. Avocent 관리 소프트웨어 서버에 연결할 수 없는 경우 사용자를 인증하기 위해 스위치 로컬 사용자 데이터베이스에 액세스합니다. 기본 로컬 사용자 이름은 Admin이며 비밀번호는 없습니다. 로컬 사용자 데이터베이스의 사용자 이름은 대소문자를 구분합니다.

로컬 포트 사용자 인터페이스의 연결된 대상 장치는 왼쪽 탐색 도구 모음에서 선택된 두 개의 개별 화면에서 보고 관리할 수 있습니다. 대상이 20개 미만인 경우 탐색할 경우에는 Target List-Basic 화면이 권장됩니다. 연결된 대상 장치가 20개 이상인 경우에는 Target List-Full 화면이 추가 탐색 도구를 제공합니다. Target List-Full 화면에서 페이지 번호를 입력하거나, 페이지 탐색 버튼을 사용하거나 필터를 사용하여 탐색할 수 있습니다. Basic 또는 Full 화면을 대상 장치를 선택하기 위한 기본 화면으로 설정할 수 있습니다.

필터링

일치하는 항목을 검색하기 위해 사용될 텍스트 문자열을 입력하여 목록 정보를 필터링할 수 있습니다. 필터링을 통해 더 짧고 더 정확한 항목 목록을 제공할 수 있습니다. 필터링이 시작되면 이름 열에서 지정된 문자열을 검색합니다. 검색은 대소문자를 구분하지 않습니다. 필터링할 때 텍스트 문자열 앞 또는 뒤에 별표(*)를 와일드카드로 사용할 수 있습니다. 예를 들어, **emailserver***를 입력하고 **필터**를 클릭하

면 emailserver로 시작하는 항목을 표시합니다(emailserver, emailserverbackup 등).

OBWI

스위치 OBWI는 원격 웹 브라우저 기반 사용자 인터페이스입니다. 시스템 설정에 대한 자세한 내용은 26페이지의 "RCS 하드웨어 연결"을 참조하십시오. 다음 표에는 OBWI가 지원하는 운영 체제 및 브라우저가 나열되어 있습니다. 최신 버전의 웹 브라우저를 사용하고 있는지 확인하십시오.

표 3.1: OBWI가 지원하는 운영 체제

운영 체제	브라우저	
	Microsoft® Internet Explorer 버전 6.0 SP1 이상	Firefox 버전 2.0 이상
Microsoft Windows 2000 Workstation 또는 Server 서비스 팩 2	예	예
Microsoft Windows Server® 2003 Standard, Enterprise 또는 Web Edition	예	예
Microsoft Windows Server® 2008 Standard, Enterprise 또는 Web Edition	예	예
Windows XP Professional 서비스 팩 3	예	예
Windows Vista® Business 서비스 팩 1	예	예
Red Hat Enterprise Linux® 4 및 5 Standard, Enterprise 또는 Web Edition(스마트 카드는 운영 체제에서 지원하지 않을 수 있음)	아니오	예

운영 체제	브라우저	
	Microsoft® Internet Explorer 버전 6.0 SP1 이상	Firefox 버전 2.0 이상
Sun Solaris® 9 및 10(스마트 카드는 운영 체제에서 지원하지 않을 수 있음)	아니오	예
Novell SUSE Linux Enterprise 10 및 11(스마트 카드는 운영 체제에서 지원하지 않을 수 있음)	아니오	예
Ubuntu 8 Workstation(스마트 카드는 운영 체제에서 지원하지 않을 수 있음)	아니오	예

스위치 OBWI에 로그인하려면:

- 1 웹 브라우저를 실행합니다.
- 2 브라우저의 주소 필드를 액세스할 스위치에 할당된 IP 주소 또는 호스트 이름을 입력합니다. `https://xxx.xx.xx.xx` 또는 `https://hostname` 형식을 사용합니다.

 **참고:** IPv6 모드를 사용하는 경우 대괄호 안에 IP 주소를 사용해야 합니다. `https://[<ipaddress-]>` 형식을 사용합니다.

- 3 브라우저로 스위치에 연결할 때 사용자 이름 및 비밀번호를 입력하고 *Login*을 클릭합니다. 스위치 OBWI가 표시됩니다.

 **참고:** 기본 사용자 이름은 비밀번호가 없는 Admin입니다.

방화벽 외부에서 스위치 OBWI에 로그인하려면 위 절차를 반복하며 대신에 방화벽 외부 IP 주소를 입력합니다.

 **참고:** RCS에서 JavaPC에 이미 설치되었는지 감지합니다. Java가 아직 설치되어 있지 않으면 On-board Web Interface를 사용하기 위해 Java를 설치해야 합니다. 또한 JNLP 파일을 Java WebStart와 연결해야 합니다.

 **참고:** 온보드 웹 인터페이스를 사용하려면 JRE(Java Runtime Environment) 버전 1.6.0_11 이상을 사용해야 합니다.



참고: 일단 온보드 웹 인터페이스에 로그인하면 로그아웃하거나 해당 세션이 관리자가 지정한 활동부재 시간 제한을 초과하지 않는 한, 다시 로그인할 필요가 없습니다.

사용자 인터페이스 사용

인증 후 사용자 인터페이스가 나타납니다. 스위치를 보고, 액세스하고, 관리할 수 있을 뿐 아니라 시스템 설정을 지정하고 프로파일 설정을 변경할 수 있습니다. 다음 그림은 사용자 인터페이스 창 영역을 보여줍니다. 다음 표에는 화면 설명이 나와 있습니다.

그림 3.1. 사용자 인터페이스 창

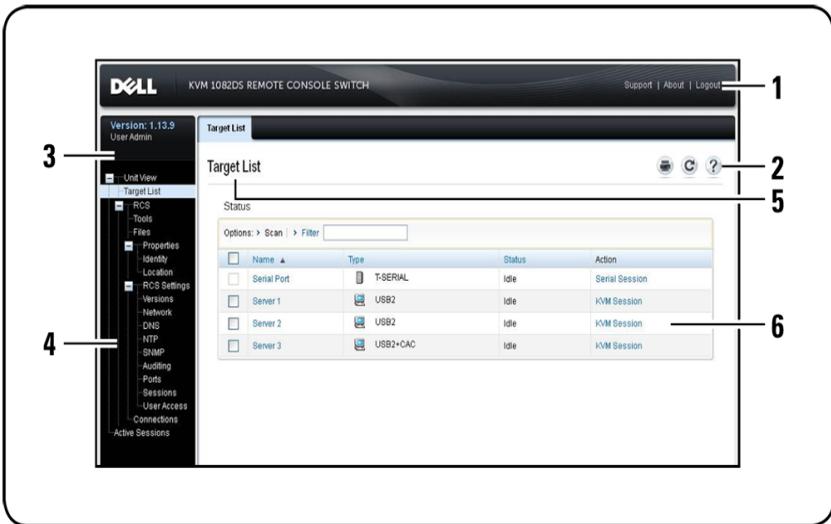


표 3.2: 사용자 인터페이스 설명

번호	설명
1	맨 위 옵션 모음: 맨 위 옵션 모음을 사용하여 기술 지원 센터에 문의하고 소프트웨어 일반 정보를 확인하거나 OBWI 세션에서 로그아웃합니다.
2	두 번째 옵션 모음: 이 모음을 사용하여 웹 페이지를 인쇄하고 현재 웹 페이지를 새로 고치거나 도움말 도구에 액세스합니다.
3	버전 블록: 제품의 펌웨어 버전 및 현재 로그인된 사용자의 사용자 이름이 맨 위 옵션 모음의 왼쪽에 나타납니다.
4	측면 탐색 모음: 측면 탐색 모음을 사용하여 표시할 정보를 선택합니다. 측면 탐색 모음을 사용하여 설정을 지정하거나 작업을 수행할 수 있는 창을 표시할 수 있습니다.
5	Navigation 탭: 선택된 탭에는 콘텐츠 영역의 시스템 정보가 표시됩니다. 일부 탭에는 클릭하여 표시한 후 범주 내의 세부 정보를 수정할 수 있는 하위 탭이 있습니다.
6	콘텐츠 영역: 콘텐츠 영역을 사용하여 스위치 OBWI 시스템을 표시하거나 변경할 수 있습니다.

세션 실행

 **참고:** 세션을 실행하려면 **Java 1.6.0_11** 이상이 필요합니다.

세션을 실행하려면:

- 1 측면 탐색 모음에서 **Target List**를 선택합니다. 가용한 장치 목록이 표시됩니다.
- 2 해당 작업, **KVM 세션** 또는 **직렬 세션**이 **Action** 열에 표시되며 세션을 실행하기 위해 선택한 대상 장치에 따라 다릅니다. 특정 대상 장치에 둘 이상의 작업이 가능한 경우 드롭다운 화살표를 클릭하고 목록에서 해당 작업을 선택합니다.

대상 장치가 현재 사용 중인 경우, 선점 수준이 현재 사용자 수준 이상이면 장치에 강제로 연결하여 액세스할 수 있습니다.

또한 RCS는 외부 Telnet이나 PuTTY와 같은 SSH 응용 프로그램을 통해 Serial SIP에 직렬 세션을 연결할 수 있습니다. Telnet 및 SSH 세션은 Serial SIP에만 연결하는 데 사용하며 RCS나 KVM 대상 장치에 액세스 하거나 관리하는 데는 사용할 수 없습니다.

Telnet 또는 SSH 응용 프로그램에서 직렬 세션을 실행하려면:

- 1 Serial SIP가 연결된 RCS 호스트 IP 주소를 입력합니다.
- 2 <RCS-username>:<Serial-SIP-name>을 입력합니다 (예: jsmith:router).
- 3 RCS 사용자의 비밀번호를 입력합니다.

 **참고:** Telnet 기능 기본값은 비활성화됩니다. Telnet 지원을 활성화하려면 76 페이지의 "직렬 세션 구성"을 참조하십시오.

로컬 UI에서 활성 세션으로 전환하려면 (로컬 사용자 전용):

- 1 측면 탐색 모음에서 **Local Session**을 선택합니다.
- 2 **Resume Active Session** 확인란을 선택합니다. Video Viewer 창이 열립니다.

스캔 모드

검색 모드에서 스위치가 여러 대상 장치를 스캔합니다. 검색 순서는 목록의 장치 위치에 의해 결정됩니다. 순서에 따라 하나의 장치 검색 후 다음 대상 장치를 검색하기 전 대기 시간을 구성할 수도 있습니다.

 **참고:** 모뎀으로 연결한 경우 Scan 버튼은 비활성화됩니다.

Scan 목록에 대상 장치를 추가하려면:

- 1 측면 탐색 모음에서 **Unit View - Target List**를 선택하여 Target Devices 화면을 엽니다.
- 2 검색할 대상 장치 이름 옆의 확인란을 선택합니다.
- 3 Scan을 클릭합니다.

검색 시간을 구성하려면:

- 1 측면 탐색 모음에서 **Ports - Local Port UI**를 선택하여 Local Port UI Settings 화면을 엽니다.
- 2 Scan Mode 머리글 아래에서 Scan Time 필드에 시간(초)을 입력합니다(3-255).
- 3 **Save**를 클릭합니다.

시스템 정보 보기

사용자 인터페이스의 다음 화면에서 스위치 및 대상 장치 정보를 볼 수 있습니다.

표 3.3: 시스템 정보

범주	선택 메뉴:	표시 내용:
RCS	<i>Unit View - RCS - Tools</i>	RCS 이름 및 유형, RCS 도구(Maintenance, Diagnostics, Certificates 및 Trap MIB)
	<i>Unit View - RCS - Files</i>	RCS 구성, 사용자 데이터베이스 및 대상 장치
	<i>Unit View - RCS - Properties - Identity</i>	포트 번호, 일련번호 및 EID
	<i>Unit View - RCS - Properties - Location</i>	사이트, 부서 및 위치
	<i>Unit View - RCS Settings - Versions</i>	현재 응용 프로그램 및 부트 버전

범주	선택 메뉴:	표시 내용:
대상 장치	<i>Unit View - Target List</i>	각 장치의 이름, 유형, 상태 및 기능을 비롯한 연결된 대상 장치 목록 다음 추가 정보를 보려면 대상 장치를 클릭하십시오. 이름, 유형, EID, 사용 가능한 세션 옵션 및 연결 경로

RCS 도구

Tools - Maintenance - Overview 화면에서 기기 이름 및 유형을 볼 수 있습니다. 기본적인 기기 작업도 수행할 수 있습니다.

RCS 다시 부팅

RCS를 다시 부팅하려면:

- 1 측면 탐색 모음에서 **Unit View - RCS - Tools - Maintenance - Overview** 탭을 선택하여 Unit Overview 화면을 엽니다.
- 2 *Reboot*를 클릭합니다.
- 3 모든 활성 세션이 연결 해제된다고 경고하는 대화 상자가 표시됩니다. *OK*를 클릭합니다.



참고: 로컬 UI를 사용하는 경우 스위치가 다시 부팅되는 동안 화면은 공백이 됩니다. 원격 OBWI를 사용하는 경우 기기가 완전히 다시 부팅되는 동안 인터페이스가 기다리고 있다고 알려 주는 메시지가 표시됩니다.

RCS 펌웨어 업그레이드

최신 펌웨어로 RCS를 업데이트할 수 있습니다.

플래시 메모리를 업그레이드하여 다시 프로그래밍한 후에는 스위치는 모든 SIP 세션을 종료하는 소프트 다시 설정을 수행합니다. SIP 펌웨어 업데이트를 거치는 대상 장치는 연결 해제된 상태로 표시될 수도 있고 표시되지 않을 수도 있습니다. 대상 장치는 플래시 업그레이드가 완료되면 정상으로 나타납니다.

주의: 펌웨어 업데이트 또는 전원 켜고 끄기 중에 SIP 연결을 해제하면 모듈이 작동하지 않게 되어 SIP를 출하시 기본값으로 복구해야 합니다.

스위치 펌웨어를 업그레이드하려면:

- 1 측면 탐색 모음에서 *Unit View - RCS - Tools - Maintenance - Upgrade* 탭을 선택하여 Upgrade RCS Firmware 창을 엽니다.
- 2 *Upgrade*를 클릭하여 Upgrade Appliance Firmware를 엽니다.
- 3 펌웨어 파일을 로드하려면 다음 방법 중 하나를 선택합니다. *Filesystem, TFTP, FTP* 또는 *HTTP*.

 **참고:** Filesystem 옵션은 원격 OBWI에 대해서만 사용 가능합니다.

- 4 Filesystem을 선택할 경우 *Browse*를 선택하여 펌웨어 업그레이드 파일의 위치를 지정합니다.

-또는-

TFTP를 선택한 경우 로드할 서버 IP 주소 및 펌웨어 파일을 입력합니다.

-또는-

FTP 또는 HTTP를 선택한 경우 로드할 서버 IP 주소 및 펌웨어 뿐 아니라 사용자 이름 및 비밀번호를 입력합니다.

- 5 *Upgrade*를 클릭합니다.

RCS 구성 및 RCS 사용자 데이터베이스 저장 및 복구

스위치 구성을 파일에 저장할 수 있습니다. 구성 파일에는 다음을 포함하여 관리 대상 기기에 대한 정보가 포함됩니다. 스위치의 로컬 사용자 데이터베이스를 저장할 수도 있습니다. 파일을 저장한 후 이전에 저장된 구성 파일이나 로컬 사용자 데이터베이스 파일을 스위치에 복원할 수 있습니다.

관리 기기 구성이나 관리 기기의 사용자 데이터베이스를 저장하려면:

- 1 측면 탐색 모음에서 *Unit View - RCS - Files* 탭을 클릭합니다.

- 2 *RCS Configuration* 탭 또는 *User Database* 탭을 클릭한 다음 *Save* 탭을 클릭합니다.
- 3 파일 저장 방법 선택: **Filesystem, TFTP, FTP** 또는 **HTTP PUT**
- 4 TFTP를 선택한 경우 로드할 서버 IP 주소 및 펌웨어 파일 이름을 입력합니다.
- 또는-
- FTP 또는 HTTP를 선택한 경우 로드할 서버 IP 주소, 사용자 이름, 사용자 비밀번호 및 펌웨어 파일 이름을 입력합니다.
- 5 다운로드하기 전에 데이터를 암호화하려면 암호화 비밀번호를 입력합니다.
- 6 *Download*를 클릭합니다. *Save As* 저장 대화 상자가 나타납니다.
- 7 원하는 위치로 이동하고 파일 이름을 입력합니다. **Save**를 클릭합니다.

관리 기기 구성 또는 관리 기기의 사용자 데이터베이스를 복구하려면:

- 1 측면 탐색 모음에서 *Unit View - RCS - Files* 탭을 클릭합니다.
- 2 *RCS Configuration* 탭 또는 *User Database* 탭을 클릭한 다음 *Restore* 탭을 클릭합니다.
- 3 파일 저장 방법 선택: **Filesystem, TFTP, FTP** 또는 **HTTP**.
- 4 Filesystem을 선택할 경우 *Browse*를 선택하여 펌웨어 업그레이드 파일의 위치를 지정합니다.
- 또는-
- TFTP를 선택한 경우 로드할 서버 IP 주소 및 펌웨어 파일 이름을 입력합니다.
- 또는-
- FTP 또는 HTTP를 선택한 경우 로드할 서버 IP 주소, 사용자 이름, 사용자 비밀번호 및 펌웨어 파일 이름을 입력합니다.

- 5 **Browse**를 클릭합니다. 원하는 위치로 이동하여 파일 이름을 선택합니다. **Upload**를 클릭합니다.
- 6 원본 파일이 암호화된 경우 비밀번호 해제 비밀번호를 입력합니다.
- 7 성공 화면이 표시된 후 관리 기기를 다시 부팅하여 복구된 구성을 활성화합니다. 51페이지의 "RCS 다시 부팅"을 참조하십시오.

플래시 업데이트 실패에서 복구하려면:

플래시 절차 후에 RCS가 새 펌웨어 버전으로 부팅하지 않을 경우 다음 단계를 사용하여 이전 펌웨어 버전으로 복구할 수 있습니다.

- 1 직렬 케이블을 RCS 후면 패널의 SETUP 포트에 연결합니다.
- 2 Setup 포트에 연결된 PC의 터미널 프로그램을 실행합니다. 직렬 포트 설정은 다음과 같아야 합니다. 9600 baud, 8 data bits, 1 stop bit, no parity 및 no flow control
- 3 RCS를 켭니다.
- 4 터미널 프로그램에서 "Hit any key to stop autoboot" 프롬프트가 나타날 때 아무 키나 누릅니다. 메뉴가 표시됩니다.
- 5 <1> (Boot Alternate)을 입력하고 <Enter> 키를 누릅니다. 자동으로 RCS가 이전 펌웨어 버전으로 다시 부팅됩니다.
- 6 RCS가 다시 부팅된 후에 플래시 업그레이드를 시도할 수 있습니다.

네트워크 설정

 **참고:** 스위치 관리자만 네트워크 대화 상자 설정을 변경할 수 있습니다. 다른 사용자는 보기 액세스만 가능합니다.

측면 탐색 모음에서 **Network**를 클릭하여 General, IPv4 및 IPv6 탭을 표시합니다.

일반 네트워크 설정을 구성하려면:

- 1 *Network* 탭을 클릭한 다음 **General** 탭을 클릭하여 RCS General Network Settings 화면을 표시합니다.
- 2 LAN Speed 드롭 다운 메뉴에서 다음 옵션 중 하나를 선택합니다. *Auto-Detect, 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex, 100 Mbps Full Duplex, 또는 1 Gbps Full Duplex*



참고: 이더넷 모드를 변경할 경우 다시 부팅해야 합니다.

- 3 ICMP Ping Reply 드롭 다운 메뉴에서 *Enabled* 또는 *Disabled*를 선택합니다.
- 4 HTTP 또는 HTTPS 포트를 확인 또는 수정합니다. 설정이 기본값인 HTTP 80 및 HTTPS 443으로 설정됩니다.
- 5 *Save*를 클릭합니다.

IPv4 네트워크 설정을 구성하려면:

- 1 **IPv4** 탭을 클릭하여 IPv4 Settings 화면을 표시합니다.
- 2 **Enable IPv4** 확인란을 클릭하여 선택하거나 선택 취소합니다.
- 3 Address, Subnet 및 Gateway 필드에 원하는 정보를 입력합니다. IPv4 주소는 xxx.xxx.xxx.xxx 점 표기법으로 입력합니다.
- 4 DHCP 드롭 다운 메뉴에서 *Enabled* 또는 *Disabled*를 선택합니다.



참고: DHCP를 사용할 경우 Address, Subnet 및 Gateway 필드에 입력한 모든 정보는 무시됩니다.

- 5 *Save*를 클릭합니다.

IPv6 네트워크 설정을 구성하려면:

- 1 **IPv6** 탭을 클릭하여 IPv6 Settings 화면을 표시합니다.
- 2 **Enable IPv6** 확인란을 클릭하여 선택하거나 선택 취소합니다.
- 3 Address, Subnet 및 Prefix Length 필드에 원하는 정보를 입력합니다. 600IPv4 주소는 FD00:172:12:0:0:0:33 또는 축약형 FD00:172:12::33 16진법으로 입력합니다.

4 DHCP 드롭 다운 메뉴에서 *Enabled* 또는 *Disabled*를 선택합니다.



참고: DHCPv6를 사용할 경우 *Address*, *Subnet*, *Gateway* 및 *Prefix length* 필드에 입력한 모든 정보는 무시됩니다.

5 *Save*를 클릭합니다.

DNS 설정

수동으로 DNS 서버를 할당할 것인지 DHCP 또는 DHCPv6를 사용해 얻은 주소를 사용할 것인지 선택할 수 있습니다.

DNS 설정을 수동으로 구성하려면:

- 1 측면 탐색 모음에서 *DNS*를 클릭하여 RCS DNS Settings 화면을 엽니다.
- 2 *Manual*, *DHCP* (IPv4를 사용하는 경우) 또는 *DHCPv6* (IPv6을 사용하는 경우)을 선택합니다.
- 3 *Manual*을 선택한 경우 *Primary*, *Secondary* 및 *Tertiary* 필드에 DNS 서버 번호를 입력합니다.
- 4 *Save*를 클릭합니다.

NTP 설정

인증서가 만료되지 않았는지 확인하려면 스위치가 현재 시간에 액세스할 수 있어야 합니다. 스위치가 NTP로부터 시간 업데이트를 요청하도록 구성할 수 있습니다. 5장의 네트워크 시간 프로토콜(NTP) 설정 구성을 참조하십시오.

SNMP 설정

SNMP는 네트워크 관리 응용 프로그램과 스위치 사이의 관리 정보를 주고 받는 데 사용하는 프로토콜입니다. 다른 SNMP 관리자는 MIB-II

를 액세스하여 스위치와 통신할 수 있습니다. SNMP 화면을 열 때 OBWI는 장치에서 SNMP 매개변수를 검색합니다.

SNMP 화면에서 시스템 정보와 커뮤니티 문자열을 입력할 수 있습니다. 스위치를 관리하고 스위치에서 SNMP 트랩을 수신할 수 있는 스테이션을 지정할 수도 있습니다. **Enable SNMP**를 선택한 경우 장치는 UDP 포트 161을 통해 SNMP 요청에 응답합니다.

일반 SNMP 설정을 구성하려면:

- 1 **SNMP**을 클릭하여 SNMP 화면을 엽니다.
- 2 UDP 포트 161을 통해 SNMP 요청에 스위치가 응답하도록 **Enable SNMP** 확인란을 클릭합니다.
- 3 Name 필드에 시스템의 정식 도메인 이름을 입력하고 Contact 필드에 노드 담당자를 입력합니다.
- 4 Read, Write, Trap 커뮤니티 이름을 입력합니다. 이러한 일련의 작업들로 SNMP 동작에 사용하는 커뮤니티 문자열을 지정합니다. Read 및 Write 문자열은 UDP 포트 161을 통해서만 SNMP에 적용되기 때문에 스위치 접근을 차단하는 비밀번호 역할을 합니다. 값은 64문자 길이까지 지정할 수 있습니다. 이러한 필드는 비워둘 수 없습니다.
- 5 Allowable Managers 필드에 이 스위치를 관리할 수 있는 최대 4대의 워크스테이션 주소를 입력합니다. 또는 이러한 필드를 비워 모든 스테이션에서 RCS를 관리할 수 있도록 할 수 있습니다.
- 6 **Save**를 클릭합니다.

이벤트 감사 설정

이벤트는 스위치가 관리 스테이션에 추가적인 주의가 필요한 일이 발생했음을 나타내는 알림입니다.

개별 이벤트를 활성화하려면:

- 1 **Auditing**을 클릭하여 Events 화면을 엽니다.

- 2 목록에서 적절한 확인란을 클릭하여 알림을 생성하는 이벤트를 지정합니다.

-또는-

Event Name 옆의 확인란을 선택하거나 선택 취소하여 전체 목록을 선택하거나 선택 취소합니다.

- 3 Save를 클릭합니다.

이벤트 대상 설정

SNMP 트랩 대상과 Syslog 서버로 전송할 감사 이벤트를 구성할 수 있습니다. Events 화면에서 활성화된 이벤트는 Event Destination 화면에 나열된 모든 서버로 전송됩니다.

- 1 Auditing 및 Destinations 탭을 클릭하여 Event Destinations 화면을 엽니다.
- 2 SNMP Trap Destination 필드에 이 스위치에서 이벤트를 전송할 최대 4대의 관리 워크스테이션 주소와 최대 4대의 Syslog 서버 주소를 입력합니다.
- 3 Save를 클릭합니다.

포트 - SIP 구성

스위치에서 연결된 SIP 뿐 아니라 각 SIP에 대한 다음 정보를 확인할 수 있습니다: EID(전자 ID), 포트, 상태, 애플리케이션, 인터페이스 유형 및 USB 속도 SIP 중 하나를 클릭하여 스위치 유형, 부트 버전, 응용 프로그램 버전, 하드웨어 버전, FPGA 버전, 가용한 버전 및 업그레이드 상태.

다음 작업도 수행할 수 있습니다: 오프라인 SIP 삭제, SIP 펌웨어 업그레이드, USB 속도 설정 또는 케이블 해제.

오프라인 SIP를 삭제하려면:

- 1 측면 탐색 모음에서 Ports - SIPs를 클릭하여 SIP 화면을 엽니다.

2 *Delete Offline*을 클릭합니다.

SIP 업그레이드

SIP FLASH 업그레이드 기능을 사용하여 RCS 관리자는 SIP를 최신 펌웨어로 업데이트할 수 있습니다. 이 업데이트는 스위치 사용자 인터페이스 또는 Avocent 관리 소프트웨어를 사용하여 수행할 수 있습니다.

플래시 메모리를 업그레이드하여 다시 프로그래밍한 후에는 스위치는 모든 SIP 세션을 종료하는 소프트 다시 설정을 수행합니다. SIP 펌웨어 업데이트 작업을 수행한 대상 장치는 연결 해제된 상태로 표시되거나 표시되지 않을 수 있습니다. 대상 장치는 플래시 업그레이드가 완료되면 정상으로 나타납니다.

RCS를 Auto-Upgrade SIP로 구성하면 SIP는 스위치 업데이트 시 자동으로 업데이트됩니다. 스위치 펌웨어를 업데이트하려면 51페이지의 "RCS 도구" 또는 Avocent 관리 소프트웨어 온라인 도움말을 참조하십시오. 정상적인 업그레이드 과정에서 문제가 발생할 경우 SIP는 필요에 따라 강제로 업그레이드할 수도 있습니다.

 **참고:** 펌웨어 업그레이드 파일은 <http://www.dell.com>에서 확인하십시오.

SIP Auto-Upgrade 기능을 변경하려면:

- 1 측면 탐색 모음에서 *Ports - SIPs*를 클릭하여 SIP 화면을 엽니다.
- 2 업그레이드할 SIP 옆의 확인란을 선택하고 *Enable Auto-Upgrade*를 클릭합니다.

주의: 펌웨어 업데이트 또는 전원 켜고 끄기 중에 SIP 연결을 해제하면 모듈이 작동하지 않게 되어 SIP를 출하시 기본값으로 복구해야 합니다.

SIP 펌웨어를 업그레이드하려면:

- 1 측면 탐색 모음에서 *Ports - SIPs*를 클릭하여 SIP 화면을 엽니다.
- 2 수정할 SIP 옆의 확인란을 선택합니다.
- 3 *Choose an operation*을 선택한 다음 *Upgrade*를 선택합니다.
- 4 설정이 올바른 경우 *Upgrade*를 클릭합니다.

USB 속도를 설정하려면:

 **참고:** 이 섹션은 USB2 SIP에만 적용됩니다.

- 1 측면 탐색 모음에서 *Ports - SIPs*를 클릭하여 SIP 화면을 엽니다.
- 2 수정할 SIP 옆의 확인란을 선택합니다.
- 3 *Choose an operation*을 선택한 다음 *Set USB 1.1 Speed* 또는 *Set USB 2.0 Speed*를 선택합니다.

전원 장치 설정

 **참고:** 전원 제어 장치 설정을 변경하려면 관리자 권한을 가지고 있어야 합니다.

 **참고:** 지원되는 PDU 목록은 www.dellkvm.com을 참조하십시오.

RCS Power Devices 화면에서 연결된 장치 목록 뿐 아니라 각 전원 장치에 대한 다음 정보를 볼 수 있습니다: 이름, 포트, 상태, 버전, 모델, 버저, 알람 및 온도. 전원 장치를 선택한 다음 **Settings**를 선택하여 해당 전원 장치에 대한 다음 세부 정보를 볼 수도 있습니다: 이름, 설명, 상태, 버전, 소켓, 공급업체 이름, 모델 및 입력 피드.

대상 장치가 전원 제어 장치 콘센트에 연결된 경우 대상 장치를 켜거나 끄거나 껐다 켤 수 있습니다.

대상 장치의 전원을 켜기, 끄기 및 껐다 켜기하려면:

- 1 측면 탐색 모음에서 *Ports - Power Devices*를 클릭하여 Power Devices 화면을 엽니다.
- 2 구성할 장치 이름을 클릭하고 *Outlet List*를 선택합니다.
- 3 구성할 콘센트의 왼쪽에 있는 확인란을 선택합니다.
- 4 필요에 따라 *On*, *Off*, 또는 *Cycle*을 클릭합니다.

오프라인 전원 장치를 삭제하려면:

- 1 측면 탐색 모음에서 *Ports - Power Devices*를 클릭하여 Power Devices 화면을 엽니다.
- 2 *Delete Offline*을 클릭합니다.

최소 켜기 시간, 끄기 시간 또는 가동 상태를 변경하려면:

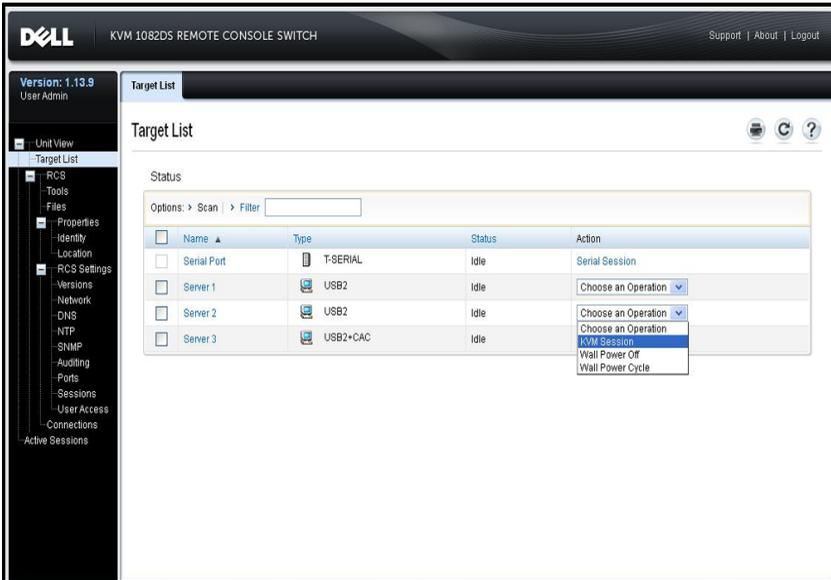
- 1 측면 탐색 모음에서 *Ports - Power Devices*를 클릭하여 *Power Devices* 화면을 엽니다.
- 2 구성할 장치 이름을 클릭하고 *Outlets*를 선택합니다.
- 3 수정할 콘센트 이름을 클릭합니다.
- 4 드롭다운 창을 사용하여 원하는 설정을 변경하고 *Save*를 클릭합니다.

연결된 대상 서버 및 전원 콘센트

OBWI 대상 장치 페이지에서 연결된 콘센트가 있는 대상에 대한 전원 제어 작업을 선택할 수 있습니다. *Ports - Power Devices* 탭을 선택한 다음 장치 이름을 클릭하면 *Device Settings*, *Device Firmware Upgrade* 및 *Outlet List* 탭이 표시됩니다. *Outlet List* 탭을 클릭하여 대상 장치와 연결된 콘센트를 표시합니다.

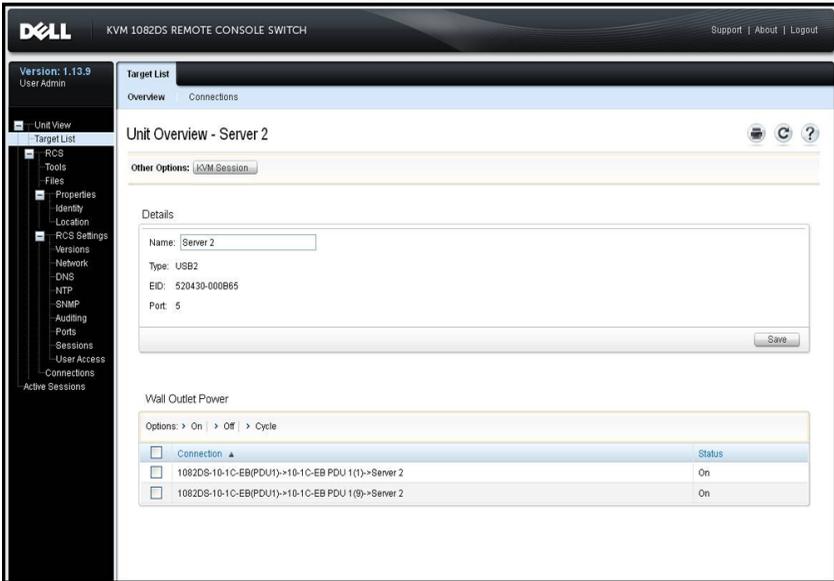
다음 그림에서 *Server2*라는 대상 장치가 전원 콘센트와 연결되어 있습니다. *Action* 열에서 드롭다운 메뉴 화살표를 클릭하면 추가로 사용할 수 있는 전원 작업이 표시됩니다.

그림 3.2. 대상 목록



다음 그림에서 Server2에 대한 대상 장치 개요 페이지에는 PDU 1의 outlet 1과 outlet 9Server2에 연결된 벽 콘센트 전원이 표시되어 있습니다.

그림 3.3. 대상 개요 서버 2



전원 콘센트 그룹 만들기

보다 편리한 제어를 위해 콘센트를 대상 서버에 연결하거나 결합할 수 있습니다. 콘센트(또는 서버에 대한 콘센트)를 그룹화하려면, 이름을 지정할 첫 번째 장치에서 **Manual Name** 필드를 사용해야 합니다. 두 번째 및 이후 장치는 **Link to Target Device** 메뉴를 사용하여 드롭다운 목록에서 첫 번째 장치의 대상 이름을 선택해야 합니다.

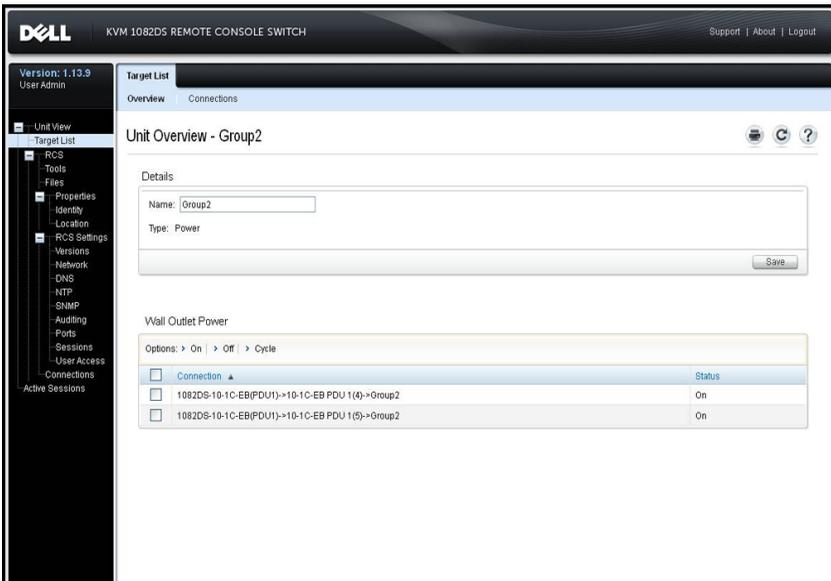
대상 목록 페이지에서 수행한 전원 작업은 모든 적용 가능한 콘센트에 적용됩니다. 대상의 특정 전원 콘센트에 대한 전원 제어 작업은 **Unit Overview** 페이지에서 수행할 수 있습니다. 다음 그림에서 **Group2**이라는 이름의 대상은 PDU1의 전원 콘센트 4와 5로 구성됩니다.

소켓 4 및 5를 그룹화하려면:

- 1 콘센트 4를 선택하여 *Power Devices Outlet Settings* 페이지를 엽니다.
- 2 *Manual*을 선택한 다음 **Group2**를 입력합니다.

- 3 Save를 클릭합니다.
- 4 콘센트 5를 선택하여 *Power Devices Outlet Settings* 페이지를 엽니다.
- 5 *Link to Target Device*를 선택한 다음 드롭다운 메뉴에서 *Group2*를 선택합니다.
- 6 Save를 클릭합니다. 콘센트 목록으로 돌아오면 콘센트 4와 5가 동일한 이름을 갖습니다.

그림 3.4. Group2의 대상 개요

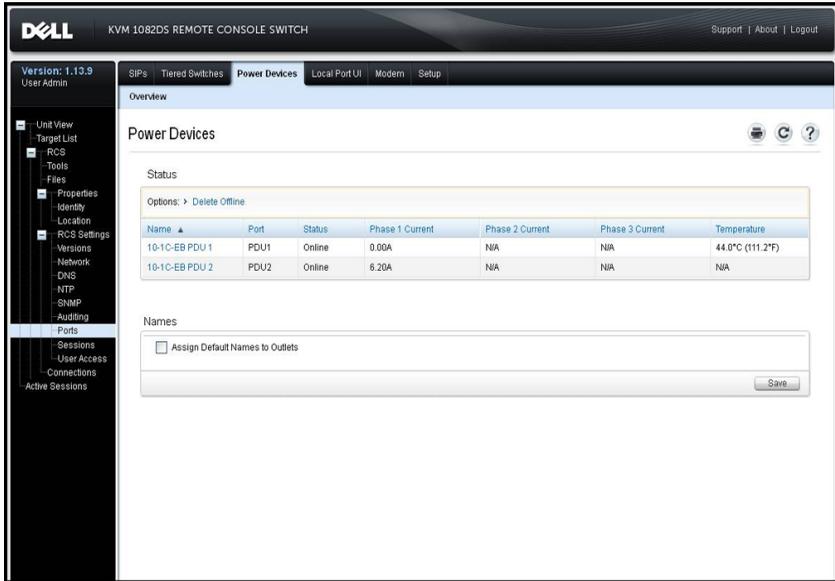


기본 콘센트 이름

Power Devices 페이지의 "Assign Default Names to Outlets" 확인란은 다음 그림과 같이 전원 콘센트에 전원 장치의 기본 이름을 지정할지 여부를 결정합니다. 이름이 있는 전원 콘센트만 Target 페이지에 나열됩니다. 지정된 기본 전원 콘센트 이름은 "Assign Default Names to Outlets" 확인란을 선택 취소하고 저장하면 제거할 수 있습니다. 이름이 없는 전

원 콘센트는 "Assign Default Names to Outlets"를 선택하고 저장하면 기본 이름이 할당됩니다.

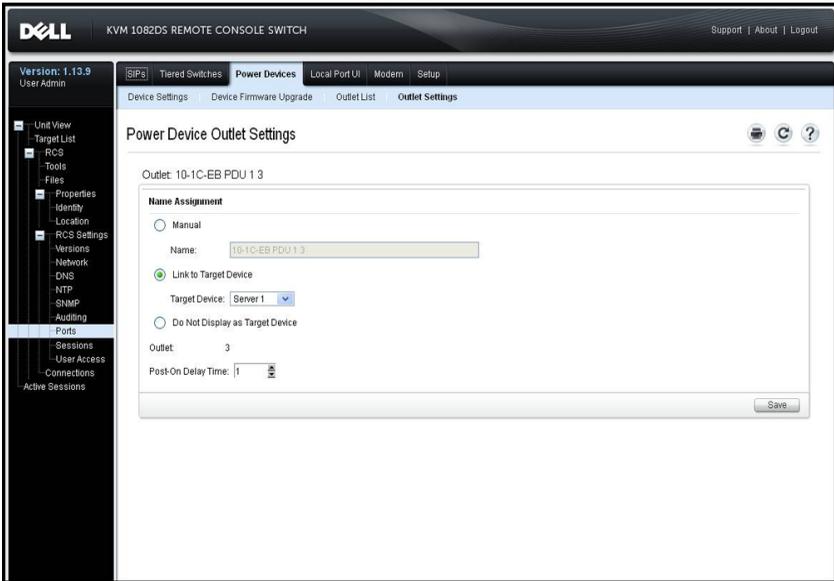
그림 3.5. RCS Power Devices 페이지



콘센트 이름 할당

Power Device Outlet Settings 페이지에서 다음 그림과 같이 콘센트 이름을 할당하기 위한 3개의 옵션을 사용할 수 있습니다. 옵션은 Manual Name assignment, Link to Target Device 및 Do Not Display as Target Device입니다.

그림 3.6. 전원 장치 콘센트 설정 페이지



- Manual Name 할당은 콘센트에 고유한 이름을 지정합니다. 이름은 모든 SIP 및 전원 콘센트 이름에 대해 고유해야 합니다. 고유하지 않은 수동 이름을 지정하면 오류가 발생하여 이름이 저장되지 않습니다.
- Link to Target List 할당은 이름 지정된 대상의 전원 제어를 위해 콘센트를 또 다른 대상 이름(콘센트 또는 SIP)에 연결합니다. 콘센트가 SIP 대상 이름에 연결된 경우 일반적으로 콘센트는 SIP에 연결된 서버에 실제 전원을 제공합니다.
- Do Not Display as Target Device 옵션은 콘센트에 빈 이름을 지정하여 Target List 페이지에 표시되지 않도록 합니다. 이 옵션은 빈 콘센트를 Target List 페이지에서 제거하는 데 사용할 수 있습니다.

장치 제어 상속

전원 콘센트 이름을 대상에 연결하여 변경할 경우 콘센트는 해당 대상 이름에 이미 구성된 액세스 제어를 상속합니다. SIP를 추가할 때

SIP에서 검색한 이름이 기존 대상의 이름과 일치할 경우, 새 SIP는 해당 대상의 액세스 제어를 상속합니다. 대상 장치의 이름을 변경할 경우 모든 SIP 및 해당 대상의 콘센트에 대한 이름이 변경되고 이전 대상 이름에 구성된 액세스 제어를 상속합니다.

대상 장치의 이름 변경

Target List - Overview 페이지에서 해당 대상의 이름은 고유한 대상 이름으로 변경할 수 있습니다. 이름은 SIP 및 전원 콘센트를 포함하여 모든 대상 집합에 대해 고유해야 합니다. 대상의 이름을 변경하면 해당 대상에 연결된 모든 콘센트도 새로운 대상 이름이 부여됩니다.

대상 장치의 우선 순위 상태

Target List 페이지에서 연결된 전원 콘센트가 있는 대상이 여러 장치를 제어합니다. 하나의 대상에 대해 표시된 상태 값은 모든 장치 상태 값의 최우선 순위로서 선택됩니다. 다음 표에는 가능한 상태 값이 우선 순위 순서(높은 순위에서 낮은 순위로)로 나열되어 있으며 해당 대상 장치 유형이 표시되어 있습니다.

표 3.4: 대상 상태 값

상태 값	적용 대상:		상태 설명
	SIP	전원 콘센트	
In Use	x	없음	세션이 활성화되어 있음
Path Blocked	x	없음	Path to Target을 다른 세션에서 사용 중
Upgrading	x	없음	SIP 업그레이드 중
Turning On	없음	x	하나 이상의 콘센트를 켜는 중
Turning Off	없음	x	하나 이상의 콘센트를 끄는 중

상태 값	적용 대상:		상태 설명
	SIP	전원 콘센트	
No Power	x	없음	SIP의 전원이 감지되지 않음
부분 전력	없음	x	대상에 켜진 상태와 꺼진 상태의 콘센트가 모두 있음
Locked-Off	없음	x	하나 이상의 콘센트가 잠김
Turned Off	없음	x	하나 이상의 콘센트가 꺼짐
Locked-On	없음	x	하나 이상의 콘센트 잠금이 해제됨
Idle	x	없음	활성화된 세션 없음, SIP에 전원이 공급됨
Turned On	없음	x	콘센트가 켜짐

대상 장치에 이름으로 연결된 여러 전원 콘센트가 있고 이러한 전원 콘센트에 공통 전원 상태가 없는 경우, RCS는 Locked-Off 콘센트 상태를 꺼짐으로 간주하고 Locked-On 콘센트 상태를 켜짐으로 간주합니다. 다음 표에는 두 콘센트 상태 값의 조합에 대한 최종 상태 값이 나열되어 있습니다.

표 3.5: 여러 콘센트 상태 값 및 표시된 상태

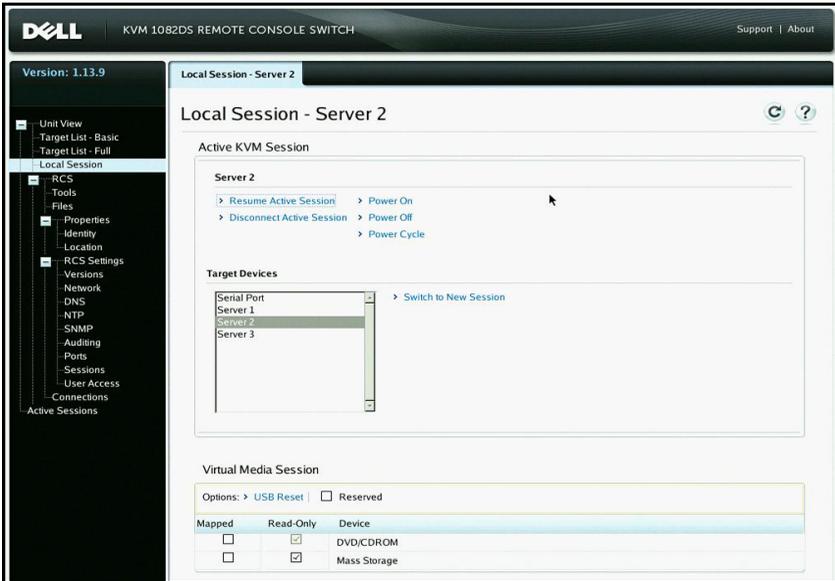
콘센트 1 상태	콘센트 2 상태	최종 상태
꺼짐	꺼짐	꺼짐
꺼짐	켜짐	부분 전력
켜짐	켜짐	전원 켜짐
Locked-On	켜짐	전원 켜짐

콘센트 1 상태	콘센트 2 상태	최종 상태
Locked-On	Locked-On	Locked-On
Locked-On	꺼짐	부분 전력
Locked-Off	켜짐	부분 전력
Locked-Off	Locked-Off	Locked-Off
Locked-Off	꺼짐	전원 꺼짐
Locked-On	Locked-Off	부분 전력

로컬 포트의 로컬 세션 페이지

로컬 포트의 Local Session 페이지에서, 활성 세션의 대상에 전원 콘센트가 연결된 경우 3개의 전원 제어가 Active 세션 아래의 페이지에 표시됩니다. 다음 그림은 대상 이름 Server2의 활성화된 로컬 포트 세션에 대해 표시된 전원 제어를 도식적으로 설명합니다.

그림 3.7. 전원 제어가 가능한 Local Session 페이지



로컬 포트 UI 설정

로컬 UI를 호출하는 방법을 변경하려면:

- 1 측면 탐색 모음에서 *Ports - Local Port UI*를 선택하여 Local Port UI Settings 화면을 엽니다.
- 2 Invoke Local Port UI 머리글 아래에서 나열된 방법 옆에 있는 확인란을 하나 이상 선택합니다.
- 3 *Save*를 클릭합니다.

로컬 포트 사용자 인터페이스 인증을 켜거나 끄고 사용자 액세스 수준을 선택할 수 있습니다. 로컬 포트 사용자 인터페이스 인증을 켜면 인터페이스를 사용하기 위해 로그인해야 합니다.

또한 로컬 포트의 키보드 언어, 스캔 모드 시간, 로컬 포트 비밀번호 사용/사용 안 함을 선택하고 사용자 선점 수준을 선택할 수 있습니다. 사용자의 선점 수준은 대상 장치에 대한 다른 사용자의 직렬 또는 KVM 세션 연결을 해제할 수 있는지를 결정합니다. 선점 수준은 1-4이며 4가 가장 높은 수준입니다. 예를 들어 선점 수준 4를 가진 사용자는 1, 2, 3 수준이 설정된 사용자 뿐 아니라 수준 4의 다른 사용자를 선점할 수 있습니다.

로컬 포트 사용자 인증을 변경하려면(관리자 전용):

- 1 측면 탐색 모음에서 **Ports - Local Port UI**를 선택하여 Local Port UI Settings 화면을 엽니다.
- 2 **Disable Local Port User Authentication** 확인란을 선택합니다.
- 3 **Disable Local Port User Authentication**을 선택한 경우 User Access Level 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다:**사용자, 사용자 관리자, 또는 RCS 관리자.**
- 4 **Save**를 클릭합니다.

모뎀 설정

RCS Modem Settings 화면에서 여러 모뎀 설정을 구성할 수 있을 뿐 아니라, 로컬 주소, 원격 주소, 서브넷 마스크 및 게이트웨이와 같은 모뎀 설정도 볼 수 있습니다.

스위치를 모뎀에 연결하기 위한 정보는 26페이지의 "RCS 하드웨어 연결"을 참조하십시오.

모뎀 설정을 구성하려면:

- 1 측면 탐색 모음에서 **Ports - Modem**을 선택하여 Modem Settings 화면을 엽니다.
- 2 **Modem sessions can preempt digital sessions** 확인란을 활성화 또는 비활성화합니다.
- 3 인증 제한 시간을 30에서 300초로 선택하고 비활동 제한 시간은 1분에서 60분으로 선택합니다.

4 **Save**를 선택합니다.

설정 - 포트 보안 설정

사용자는 직렬 설정 포트에서 기기 네트워크 구성을 변경하고, 디버그 정보를 활성화하고, 기기를 초기화할 수 있습니다.

비밀번호를 사용하여 직렬 설정 포트에 대한 액세스를 제한하려면:

- 1 측면 탐색 모음에서 *RCS Settings - Ports - Setup*을 선택하여 Setup Port Settings 페이지를 엽니다.
- 2 *Enable Setup Port Security* 상자를 클릭하여 활성화합니다.
- 3 비밀번호를 입력하고 확인합니다.
- 4 **Save**를 클릭합니다.

세션

활성 세션 화면에서 활성 세션 목록 및 각 세션에 대한 다음 정보를 볼 수 있습니다. 대상 장치, 소유자, 원격 호스트, 기간 및 유형.

일반 세션 구성

일반 세션 설정을 구성하려면:

- 1 측면 탐색 모음에서 *Sessions - General*을 선택합니다. General Session Settings 화면이 나타납니다.
- 2 *Enable Inactivity Timeout* 확인란을 선택하거나 선택 취소합니다.
- 3 Inactivity Timeout 필드에 세션이 닫히는 활동 부재 시간을 입력합니다 (1분 ~ 90분).
- 4 Login Timeout 필드에 다시 로그인해야 하는 활동 부재 시간을 입력합니다 (21초 ~ 120초).
- 5 *Enable Preemption Timeout* 확인란을 선택하거나 선택 취소합니다.

- 6 Preemption Timeout 필드에 세션이 선정될 것이라고 알려주는 프롬프트가 표시되는 시간을 입력합니다(1초 ~ 120초).
- 7 옵션을 공유하는 적용 가능한 세션을 선택합니다(Enabled, Automatic, Exclusive 또는 Stealth).
- 8 1 ~ 50 범위의 입력 제어 제한 시간을 선택합니다. 여기서 1은 1/10 초를 나타냅니다.
- 9 **Save**를 클릭합니다.

KVM 세션 구성

KVM 세션 설정을 구성하려면:

- 1 측면 탐색 모음에서 Sessions - KVM을 선택합니다. KVM 세션 설정 화면이 나타납니다.
- 2 키보드 및 마우스 신호(128-bit SSL(**ARCFOUR**), DES, DES, 또는 AES) 및 비디오 신호(128-bit SSL(**ARCFOUR**), DES, 3DES, **AES**, 또는 None)에 대한 암호화 수준 선택합니다.
- 3 키보드 드롭다운 메뉴에서 언어를 선택합니다.
- 4 하드웨어에 USB2+CAC SIP가 있는 경우, 비디오 해상도를 선택합니다.
- 5 **Save**를 클릭합니다.

로컬 가상 미디어 세션 구성

가상 미디어 옵션을 설정하려면:

- 1 측면 탐색 모음에서 Sessions - **Virtual Media**를 선택하여 Virtual Media Session Settings 화면을 엽니다.
- 2 *Virtual Media locked to KVM Sessions* 확인란을 활성화 또는 비활성화합니다.
- 3 **Allow Reserved Sessions** 확인란을 활성화 또는 비활성화합니다.
- 4 드롭다운 메뉴의 Virtual Media Access Mode에서 다음 옵션 중 하나를 선택합니다: *Read-Only* 또는 *Read-Write*.

- 5 지원할 암호화 수준 중 하나를 선택합니다.
- 6 *Save*를 클릭합니다.
- 7 가상 미디어를 활성화할 각 SIP 옆의 확인란을 선택하고 *Enable VM*을 클릭합니다.

-또는-

가상 미디어를 비활성화할 각 SIP 옆의 확인란을 선택하고 *Disable VM*을 클릭합니다.

가상 미디어 옵션

Virtual Media Session Settings 화면에 제공된 옵션을 사용하여 가상 미디어 세션 동안의 스위치 동작을 결정할 수 있습니다. 표 3.4는 가상 미디어 세션에 설정할 수 있는 옵션을 간략히 보여줍니다.

KVM 세션에서 가상 미디어 사용에 대한 자세한 내용은 95페이지의 "가상 미디어"를 참조하십시오.

표 3.6: Virtual Media 세션 설정

설정	설명
Session Settings: Virtual Media locked to KVM Session	잠금 옵션은 가상 미디어 세션을 대상 장치의 KVM 세션에 대해 잠글지 여부를 지정합니다. 잠금이 설정되고(기본 설정) KVM 세션이 닫힌 경우 가상 미디어 세션도 닫힙니다. 잠금을 사용 안하고 KVM 세션이 닫힌 경우 가상 미디어 세션은 활성 상태를 유지합니다.
Session Settings: Allow Reserved Sessions	사용자 이름만 사용하여 가상 미디어 연결에 액세스할 수 있고 다른 사용자가 KVM을 대상 장치에 연결할 수 없도록 합니다. 연결된 KVM 세션이 끊어지면 Virtual Media 대화 상자의 Locked 설정에 따라 가상 미디어 세션의 연결이 끊어질 수 있습니다.

설정	설명
Drive Mappings: Virtual Media Access Mode	<p>매핑된 드라이브에 대한 액세스 모드를 읽기 전용 또는 읽기쓰기로 설정할 수 있습니다. 액세스 모드가 읽기 전용일 경우 사용자는 데이터를 클라이언트 서버의 매핑된 드라이브에 쓸 수 없습니다. 액세스 모드가 읽기쓰기일 경우 사용자는 매핑된 드라이브로부터/드라이브에 데이터를 읽기 및 쓰기 할 수 있습니다. 매핑된 드라이브가 읽기 전용 드라이브인 경우(예: CD-ROM, DVD-ROM 드라이브 또는 ISO 이미지), 구성된 읽기-쓰기 액세스 모드는 무시됩니다. 읽기 전용 모드를 설정하면 대용량 저장 장치나 USB 이동식 미디어 같은 읽기쓰기 드라이브가 매핑되고 사용자가 데이터를 쓰지 못하도록 막고자 할 경우 유용할 수 있습니다.</p> <p>하나의 DVD 드라이브와 대용량 저장 장치를 동시에 매핑할 수 있습니다. CD 드라이브, DVD 드라이브 또는 ISO 디스크 이미지 파일은 가상 CD 드라이브로 매핑됩니다.</p>
Encryption Level	가상 미디어 세션의 암호화 수준을 구성할 수 있습니다. 선택 옵션은 None (기본값), 128-bit SSL (ARCFOUR) , DES , 3DES 및 AES 입니다.
SIP 당 Virtual Media Access: VM 활성화/VM 비활성화	Virtual Media Access per the SIP 섹션에는 모든 가상 미디어 SIP 가 나열됩니다. 이 목록에는 각 케이블에 대해 가상 미디어를 활성화 또는 비활성화 하는 옵션을 포함하여 각 케이블에 대한 세부 정보가 포함되어 있습니다.

로컬 사용자

또한 로컬 사용자는 **Local Session** 화면에서 가상 미디어의 동작을 결정할 수 있습니다. 가상 미디어 세션을 연결 및 연결 해제하는 것 이외에도 다음 표의 설정을 구성할 수 있습니다.

표 3.7: 로컬 가상 미디어 세션 설정

설정	설명
CD ROM/ DVD ROM	첫 번째 감지된 CD-ROM 또는 DVD-ROM(읽기 전용) 드라이브에 가상 미디어 세션을 허용합니다. 이 확인란을 활성화하면 가상 미디어 CD-ROM 또는 DVD-ROM 연결을 대상 장치에 연결할 수 있습니다. 이 확인란을 비활성화하면 대상 장치에 대한 CD-ROM 또는 DVD-ROM 연결을 종료합니다.
Mass Storage	처음에 감지된 대용량 스토리지 드라이브의 가상 미디어 세션을 허용합니다. 이 확인란을 활성화하면 가상 미디어 대용량 스토리지를 대상 장치에 연결할 수 있습니다. 이 확인란을 비활성화하면 대상 장치에 대한 가상 미디어 대용량 스토리지 연결을 종료합니다.
Reserved	사용자 이름만 사용하여 가상 미디어 연결에 액세스할 수 있고 다른 사용자가 KVM을 대상 장치에 연결할 수 없도록 합니다.

직렬 세션 구성

직렬 세션 설정을 구성하려면:

- 1 측면 탐색 모음에서 *Sessions - Serial*을 클릭하여 Serial Session Settings 화면을 엽니다.
- 2 *Telnet Access Enabled* 확인란은 선택하거나 선택하지 않습니다.
- 3 **Save**를 클릭합니다.

사용자 계정 설정

로컬 계정 매핑

스위치 OBWI는 관리자 정의 사용자 계정을 통해 로컬 및 로그인 보안을 제공합니다. 측면 탐색 모음에서 *User Accounts* 를 선택하여 관리자는 사용자를 추가 및 삭제하고, 사용자 선점 및 액세스 수준을 정의하며 비밀번호를 변경할 수 있습니다.

액세스 수준

사용자 계정이 추가되면 사용자는 다음 액세스 수준 중 하나가 할당될 수 있습니다: RCS 관리자, 사용자 관리자 및 사용자.

표 3.8: 액세스 수준별 허용된 작업

작업	RCS 관리자	사용자 관리자	사용자
인터페이스 시스템 수준 설정 구성	예	아니오	아니오
액세스 권한 구성	예	예	아니오
사용자 계정 추가, 변경 및 삭제	예, 모든 액세스 수준에 대해	예, 사용자 및 사용자 관리자 전용	아니오
자신의 비밀번호 변경	예	예	예
대상 장치 액세스	예, 모든 대상 장치	예, 모든 대상 장치	예, 허용되는 경우

새 사용자 계정을 추가하려면 (사용자 관리자 또는 RCS 관리자 전용):

- 1 측면 탐색 모음에서 *User Accounts - Local User Accounts*를 선택하여 Local User Accounts 화면을 엽니다.
- 2 *Add* 버튼을 클릭합니다.
- 3 빈 곳에 새 사용자의 이름 및 비밀번호를 입력합니다.
- 4 새 사용자의 액세스 수준을 선택합니다.
- 5 사용자 계정에 할당할 가용 대상 장치를 선택하고 **Add**를 클릭합니다.



참고: 사용자 관리자 및 RCS 관리자는 모든 대상 장치에 액세스할 수 있습니다.

- 6 *Save*를 클릭합니다.

사용자 계정을 삭제하려면(사용자 관리자 또는 RCS 관리자 전용):

- 1 측면 탐색 모음에서 *User Accounts - Local Accounts*를 선택하여 Local User Accounts 화면을 엽니다.
- 2 삭제할 각 계정의 왼쪽에 확인란을 클릭한 다음 *Delete*를 클릭합니다.

사용자 계정을 편집하려면(관리자 또는 활성 사용자 전용):

- 1 측면 탐색 모음에서 *User Accounts - Local Accounts*를 클릭합니다. Local User Accounts 화면이 표시됩니다.
- 2 편집할 사용자 이름을 클릭합니다. 사용자 프로필이 나타납니다.
- 3 화면에서 사용자 정보를 입력한 다음 *Save*를 클릭합니다.

Avocent 관리 소프트웨어 장치 IP 주소

관리 소프트웨어 서버의 IP 주소를 지정하여 Avocent 관리 소프트웨어 서버로 관리되지 않는 스위치를 연결 및 등록할 수 있습니다.

서버 IP 주소를 구성하려면:

- 1 측면 탐색 모음에서 *User Accounts - Avocent*를 선택합니다. Avocent Management Software Settings 화면이 표시됩니다.
- 2 연결할 서버 IP 주소를 입력합니다. 최대 네 개의 주소가 허용됩니다.
- 3 스크롤 막대를 사용하여 원하는 재시도 간격을 선택합니다.
- 4 서버에 등록된 RCS를 연결 해제하려면 **Disassociate** 버튼을 클릭합니다.
- 5 *Save*를 클릭합니다.

LDAP

Dell 1082DS/2162DS/4322D RCS는 로컬 데이터베이스를 통해 또는 Dell RCS 소프트웨어나 LDAP(Lightweight Directory Assistance Protocol) 지원하는 OBWI를 사용하는 외부 확장 가능 분산 디렉토리 서비스를 통해

사용자를 인증 및 승인할 수 있습니다. RCS에서 LDAP 구성 및 사용에 대한 자세한 내용은 LDAP 절을 참조하십시오.

Override 관리자

네트워크 오류가 발생하면 LDAP 서버에 대한 장치의 인증 권한과 관계 없이 사용할 수 있는 계정이 제공됩니다. 5장에서 Override 관리자 계정 구성을 참조하십시오.

활성 세션

활성 세션 화면에서 활성 세션 목록 및 각 세션에 대한 다음 정보를 볼 수 있습니다. 대상 장치, 소유자, 원격 호스트, 기간 및 유형.

세션 닫기

세션을 닫으려면:

- 1 측면 탐색 모음에서 *Active Sessions*를 클릭하여 RCS 활성 세션 화면을 표시합니다.
- 2 원하는 대상 장치 옆에 있는 확인란을 클릭합니다.
- 3 *Disconnect*를 클릭합니다.

 **참고:** 연결된 잠겨진 가상 미디어 세션이 있는 경우 연결 해제됩니다.

세션을 닫으려면 (로컬 사용자 전용):

- 1 측면 탐색 모음에서 *Local Session*을 선택합니다.
- 2 *Disconnect Active Session* 확인란을 선택합니다.

Video Viewer 창

Video Viewer는 OBWI를 사용하여 하나의 스위치에 연결된 대상 장치로 KVM 세션을 실행하는 데 사용됩니다. Video Viewer를 사용해 장치에 연결할 경우 대상 장치 바탕 화면이 로컬 및 대상 장치 커서를 모두 포함하고 있는 별도의 창에 표시됩니다.

스위치 OBWI 소프트웨어는 Java 기반 프로그램을 사용하여 Video Viewer 창을 표시합니다. 스위치 OBWI는 처음 열 때 Video Viewer를 자동으로 다운로드하여 설치합니다.



참고: 세션을 실행하려면 Java 1.6.0_11 이상이 필요합니다.



참고: 스위치 OBWI는 JRE(Java Resource Engine)를 설치하지 않습니다. JRE는 <http://www.sun.com>에서 무료로 다운로드할 수 있습니다.



참고: 스위치 OBWI는 Video Viewer 창의 이미지를 저장하고 표시하기 위해 시스템 메모리를 사용합니다. 각 열려진 Video Viewer 창은 추가 시스템 메모리가 필요합니다. 클라이언트 서버의 8비트 색상 설정은 Video Viewer 창마다 1.4 MB의 메모리가 필요하며 16비트 색상 설정은 2.4 MB 그리고 32비트 색상 설정은 6.8 MB 메모리가 필요합니다. 시스템 메모리가 허용하는 수(보통 4)보다 더 많은 Video Viewer 창을 열려고 시도할 경우 메모리 부족 오류가 발생하며 요청된 Video Viewer 창은 열리지 않습니다.

액세스하려는 장치를 현재 다른 사용자가 보고 있는 경우 선점 수준이 다른 사용자의 선점 수준과 같거나 높을 경우 다른 사용자를 선점할 것인지 묻는 프롬프트가 표시됩니다. RCS 관리자는 Active Session 페이지를 통해 활성 사용자의 연결을 해제할 수도 있습니다. 자세한 내용은 RCS79페이지의 "활성 세션"을 참조하십시오.

그림 4.1. Video Viewer 창(표준 창 모드)

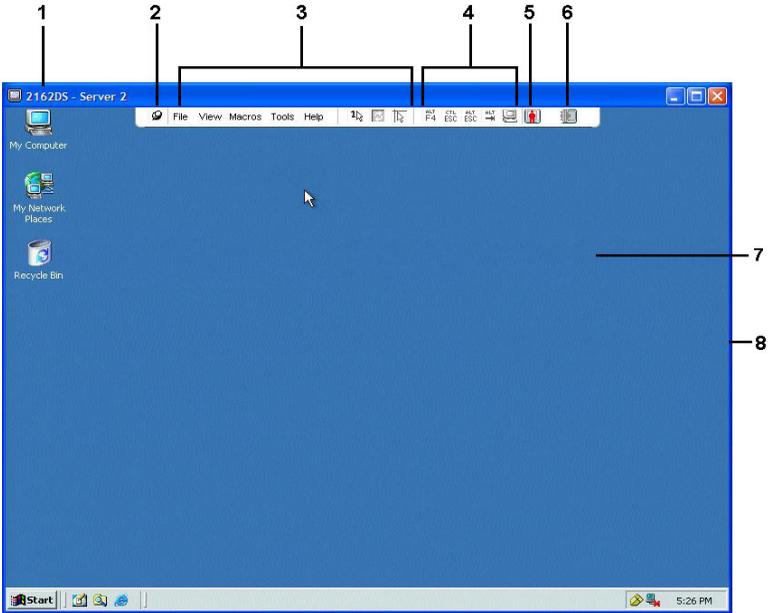


표 4.1: Video Viewer 설명

번	설명
1	제목 표시줄: 보고 있는 대상 장치의 이름을 표시합니다. 전체 화면 모드일 경우 제목 표시줄이 사라지고 대상 장치 이름이 메뉴와 도구 모음 사이에 표시됩니다.
2	압핀 아이콘: 메뉴 및 도구 모음의 표시를 고정시키기 때문에 항상 볼 수 있습니다.

예 단 설명

- 3 메뉴 및 도구 모음: **Video Viewer** 창에서 대부분의 기능에 액세스할 수 있습니다. 메뉴 및 도구 모음은 압핀을 사용하지 않을 경우 표시/숨기기 상태에 있게 됩니다. 메뉴 및 도구 모음을 표시하려면 커서를 도구 모음 위로 이동합니다. 최대 **10개**의 명령 및/또는 매크로 그룹 버튼이 도구 모음에 표시될 수 있습니다. 기본으로 단일 커서 모드, 새로 고침, 자동 비디오 조정 및 로컬 커서 정렬 버튼이 도구 모음에 표시됩니다. 자세한 내용은 **83**페이지의 "변경 도구 모음" 및 **103**페이지의 "매크로"를 참조하십시오.
-
- 4 매크로 버튼: 대상 장치로 전송할 수 있는 자주 사용하는 키보드 순서
-
- 5 연결 상태 표시기: 이 서버의 **RCS**에 연결된 사용자 상태를 나타냅니다. 모드에는 독점, 기본 활성화 연결, 주 활성화 공유, 보조 활성화 공유, 수동 공유, 스텔스 및 검색이 있습니다.
-
- 6 스마트 카드 상태 표시기: 스마트 카드가 스마트 카드 판독기에 있는지 여부를 나타냅니다. **Video Viewer** 화면 스마트 카드 아이콘은 회색이고 스마트 카드 옵션을 사용할 수 없거나 비활성화되었음을 나타냅니다. 스마트 카드가 매핑되면 아이콘은 녹색이 됩니다.
-
- 7 표시 영역: 서버 바탕 화면에 액세스합니다.
-
- 8 프레임: 프레임을 클릭하고 누른 상태로 **Video Viewer** 창의 크기를 조절합니다.
-

변경 도구 모음

도구 모음이 표시/숨기기 상태(즉, 압핀에 의해 자리에 고정되지 않은 상태)에 있을 경우 **Video Viewer** 창에서 도구 모음이 숨겨지기 전의 지연 시간을 선택할 수 있습니다.

도구 모음 숨기기 시간을 지정하려면:

- 1 **Video Viewer** 창에서 **Tools - Session Options**를 선택합니다.
-또는-
Session Options 버튼을 클릭합니다.

Session Options 대화 상자가 표시됩니다.

- 2 **Toolbar** 탭을 클릭합니다.
- 3 도구 모음을 숨기기 전의 지연 시간(초)을 지정하려면 화살표 키를 사용합니다.
- 4 OK를 클릭하여 변경 사항을 저장하고 대화 상자를 닫습니다.

세션 실행



참고: 비프록시된 연결을 사용할 경우 느린 네트워크 연결로 인해 비디오 성능이 떨어질 수 있습니다. 특정 색상 설정(회색조와 같은)은 다른 설정(최적 색상)보다 네트워크 대역폭을 덜 사용하기 때문에 색상 설정을 변경하면 비디오 성능을 높일 수 있습니다. 느린 네트워크 연결의 최적의 비디오 성능을 위해 **Grayscale/Best Compression** 또는 **Low Color/High Compression**을 사용하십시오. 자세한 내용은 85페이지의 "보기 조정"을 참조하십시오.



참고: 사용자가 로컬 컴퓨터보다 높은 해상도의 대상 장치에 연결할 경우 **Video Viewer** 창은 대상 장치 화면의 일부분만 표시되고 나머지 화면을 볼 수 있도록 스크롤 막대가 표시됩니다. 사용자는 대상 장치, 로컬 컴퓨터 또는 둘 모두의 해상도를 조정하여 전체 화면으로 볼 수 있습니다.

Explorer 전환 창에서 KVM 세션을 실행하려면:

- 1 **Target List** 화면에 나열된 장치를 클릭하여 **unit overview** 창을 엽니다.
- 2 **KVM Session** 링크를 클릭하여 새 **Video Viewer** 창을 엽니다.

세션 제한 시간

원격 세션은 지정된 시간 동안 세션 창에서 아무런 작업을 하지 않을 경우 제한 시간이 발생할 수 있습니다. 세션 시간 제한 값은 **RCS KVM Session Settings** 창에서 구성할 수 있습니다. 지정된 시간 제한 값은 다음에 **OBWI**에 액세스할 때 사용됩니다.

세션 시간 제한을 활성화, 비활성화 또는 구성하려면:

- 1 측면 메뉴에서 **Unit View - RCS - RCS Settings - Sessions - General**을 선택합니다.
- 2 **Enable Activity Timeout** 상자에서 원하는 설정을 선택합니다.

- 3 필요한 경우 비활동 시간 제한의 시간 제한 값을 선택합니다.
- 4 *Save*를 클릭합니다.

창 크기



참고: *View - Scaling* 명령은 **Video Viewer** 창이 전체 화면 모드에 있거나 공유 세션의 주 사용자가 아닐 경우 사용할 수 없습니다.

스위치 OBWI를 처음 사용할 경우 열려 있는 **Video Viewer** 창은 사용자가 값을 바꿀 때까지 1024 x 768 해상도로 표시됩니다. 각 **Video Viewer** 창은 다른 해상도로 설정할 수 있습니다.

스위치 OBWI는 자동 배율이 활성화된 경우 세션 동안 창 크기를 변경하면 화면을 자동으로 조정합니다. 세션 동안 언제든지 대상 장치 해상도를 변경할 수 있으며 이 때 화면은 자동으로 조정됩니다.

Video Viewer 창 해상도를 변경하려면:

- 1 *View - Scaling* 명령을 선택합니다.
- 2 원하는 해상도를 선택합니다.

보기 조정

Video Viewer 창의 메뉴 또는 작업 버튼을 사용하여 다음을 수행할 수 있습니다.

- 마우스 커서를 정렬합니다.
- 화면을 새로 고칩니다.
- 전체 화면 모드를 활성화 또는 비활성화합니다. 전체 화면 모드가 활성화되면 이미지는 최대 1600 x 1200 또는 1680 x 1050(와이드스 크린) 크기의 바탕 화면에 맞게 조정됩니다. 바탕 화면이 고해상도일 경우 다음과 같은 사항이 발생합니다.
 - 전체 화면 이미지가 바탕 화면의 가운데로 정렬되고 **Video Viewer** 창 주위의 영역은 검은색이 됩니다.
 - 메뉴 및 도구 모음이 잠기고 항상 표시됩니다.

- 세션 이미지의 자동, 전체 또는 수동 배율 조정을 활성화합니다.
 - 전체 배율 조정을 사용하면 바탕 화면 창은 고정되고 장치 이미지는 창에 맞게 조정됩니다.
 - 자동 배율 조정일 경우, 바탕 화면 창은 보고 있는 대상 장치의 해상도에 맞게 크기가 조정됩니다.
 - 수동 배율 조정을 사용하면 지원되는 이미지 배율 조정 해상도의 드롭다운 메뉴가 표시됩니다.
- 세션 이미지의 색 농도를 변경합니다.

마우스 커서를 정렬하려면:

Video Viewer 창 도구 모음에서 *Align Local Cursor* 버튼을 클릭합니다. 로컬 커서가 원격 장치의 커서와 정렬되어야 합니다.



참고: 커서가 정렬되지 않을 경우 연결된 장치에서 마우스 가속을 끕니다.

화면을 새로 고치려면 Video View 창에서 *Refresh Image* 버튼을 클릭하거나 Video Viewer 창 메뉴에서 *View - Refresh*를 선택합니다. 디지털 비디오 이미지가 완벽하게 생성됩니다.

전체 화면 모드를 사용으로 설정하려면 *Maximize* 버튼을 클릭하거나 Video Viewer 창 메뉴에서 *View - Full Screen*을 선택합니다. 바탕 화면 창이 사라지고 액세스된 대상 장치의 바탕 화면만 표시됩니다. 화면은 최대 1600 x 1200 또는 1680 x 1050(와이드스크린) 크기로 조정됩니다. 바탕 화면에 더 높은 해상도가 있으면 검정색 배경이 전체 화면 이미지를 둘러쌉니다. 이동식 도구 모음이 표시됩니다.

전체 화면 모드를 사용 안 함으로 설정하려면 이동식 도구 모음의 *Full Screen Mode* 버튼을 클릭하여 바탕 화면 창으로 돌아갑니다.

전체 배율 조정을 사용으로 설정하려면 Video Viewer 창 메뉴에서 *View - Scaling*을 선택하고 **Full Scale**을 선택합니다. 장치 이미지는 보고 있는 대상 장치의 해상도로 자동 배율 조정됩니다.

수동 배율 조정을 사용으로 설정하려면 Video Viewer 창 메뉴에서 *View - Scaling*을 선택합니다. 창을 배율 조정할 크기를 선택합니다. 가용한 수동 배율 조정 크기는 시스템에 따라 다릅니다.

이미지 새로 고침

Manual Video Adjust 대화 상자에서 *Refresh Image* 버튼을 클릭하면 디지털화된 비디오 이미지를 완벽하게 재생합니다.



참고: 또한 Video Viewer 메뉴에서 *View - Refresh*를 선택하여 이미지를 새로 고칠 수 있습니다.

비디오 설정

추가 비디오 조정

일반적으로 Video Viewer 창 자동 조정 기능은 비디오를 가장 적합한 보기로 최적화합니다. 그러나 사용자는 Dell 기술 지원 센터의 도움을 받아 Video Viewer 창 메뉴에서 *Tools - Manual Video Adjust* 명령을 선택하거나 *Manual Video Adjust* 버튼을 클릭하여 비디오를 미세 조정할 수 있습니다. Manual Video Adjust 대화 상자가 나타납니다. 대상 설정마다 비디오 조정이 이루어집니다.

사용자는 대화 상자의 왼쪽 아래 모서리에 있는 패킷 전송 속도를 보고 정적 화면을 지원하는 데 필요한 초당 패킷 수준을 확인할 수 있습니다.

창의 비디오 품질을 수동으로 조정하려면:



참고: 다음 비디오 조정은 Dell 기술 지원 센터의 도움을 받아 수행해야 합니다.

- 1 Video Viewer 창 메뉴에서 *Tools - Manual Video Adjust*를 선택합니다.

-또는-

Manual Video Adjust 버튼을 클릭합니다.

Manual Video Adjust 대화 상자가 나타납니다.

그림 4.2. Manual Video Adjust 대화 상자

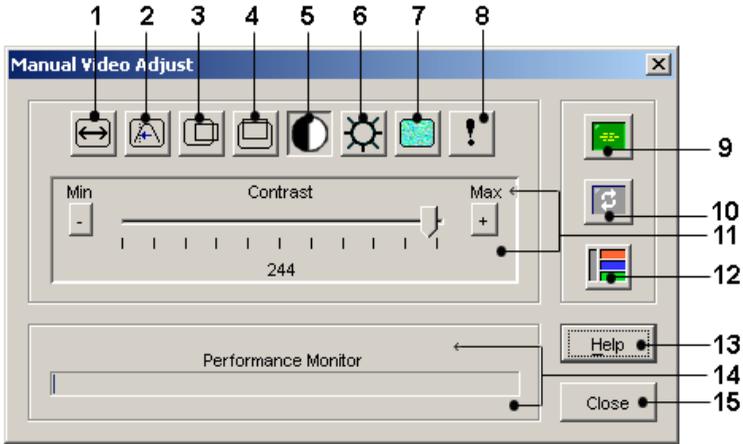


표 4.2: 그림 4.2 설명

번호	설명	번호	설명
1	이미지 캡처 폭	9	Automatic Video Adjustment
2	픽셀 샘플링/미세 조정	10	이미지 새로 고침
3	이미지 캡처 수평 위치	11	조정 막대
4	이미지 캡처 수직 위치	12	비디오 테스트 패턴
5	대비	13	도움말
6	밝기	14	성능 모니터
7	노이즈 임계값	15	닫기 버튼
8	우선 순위 임계값		

2 조정할 기능에 해당하는 아이콘을 클릭하십시오.

- 3 대비 슬라이더 막대를 이동하거나 **최소(-)** 또는 **최대(+)** 버튼을 클릭하여 눌러진 각 아이콘의 매개변수를 조정합니다. 조정사항은 Video Viewer 창에 바로 표시됩니다.
- 4 완료되었으면 *Close* 를 클릭하여 Manual Video Adjust 대화 상자를 닫으십시오.

대상 비디오 설정

이미지 캡처 폭, 픽셀 샘플링/미세 조정, 이미지 캡처 수평 위치 및 이미지 캡처 수직 위치 조정은 대상 비디오가 캡처되고 디지털화되는 방법에 영향을 미칩니다. 거의 변경되지 않습니다.

이미지 캡처 매개변수는 자동 조정 기능에 의해 자동으로 변경됩니다. 독립적으로 정확한 조정을 하려면 대상에 특수한 이미지가 요구됩니다.

Automatic Video Adjustment

대부분의 경우 비디오 설정의 기본값을 변경할 필요가 없습니다. 시스템이 자동으로 조정하며 최적의 비디오 매개변수를 사용합니다. 스위치 OBWI는 비디오 패킷이 정적 화면에 대해 전송되지 않는 (0) 상태로 비디오 매개변수가 설정될 때 최적의 작업을 수행합니다.

Manual Video Adjust 대화 상자에서 *Auto Adjust Video* 버튼을 클릭하여 비디오 매개변수를 이상적인 설정으로 쉽게 조정할 수 있습니다.



참고: 또한 Video Viewer 창 메뉴에서 *Tools - Automatic Video Adjust*를 선택하거나 *Automatic Video Adjust* 도구 모음 아이콘을 클릭하여 자동으로 비디오를 조정할 수 있습니다.

비디오 테스트 패턴

Manual Video Adjust 대화 상자에서 *Video Test Pattern* 버튼을 클릭하면 비디오 테스트 패턴이 전환됩니다. *비디오 테스트 패턴* 버튼을 다시 클릭하여 정상 비디오 이미지로 전환합니다.

공급업체 전용 비디오 설정

비디오 설정은 제조업체에 따라 크게 다릅니다. Dell은 특히 Sun 전용 비디오 카드와 같이 여러 비디오 카드에 대해 최적화된 비디오 설정의 온라인 데이터베이스를 관리하고 있습니다. 이 정보는 Dell 온라인 기술 자료나 Dell 기술 지원 센터에 연락하여 얻을 수 있습니다.

색 설정

색 농도 조정

Dambrackas Video Compression®(DVC) 알고리즘을 사용하여 사용자는 원격 세션 창의 다양한 표시 가능 색을 조정할 수 있습니다. 최상의 화질을 얻으려면 더 많은 색을 표시하고 네트워크에서 전송되는 데이터 양을 줄으려면 더 적은 색을 표시하도록 선택합니다.

Video Viewer 창은 Best Color Available(느린 업데이트), Best Compression(가장 빠른 업데이트), Best Color와 Best Compression의 조합 또는 그레이스케일로 볼 수 있습니다.

각 포트 및 채널의 색 농도는 원격 세션 창에서 *View Color* 명령을 선택하여 지정할 수 있습니다. 이러한 설정은 채널마다 개별적으로 저장됩니다.

대비 및 밝기

Video Viewer 창의 이미지가 너무 어둡거나 밝은 경우 *Tools - Automatic Video Adjust*를 선택하거나 *Automatic Video Adjust* 버튼을 선택합니다. 이 명령은 비디오 조정 대화 상자에도 있습니다. 대부분의 경우, 이렇게 하면 비디오 문제가 해결됩니다.

*Auto Adjust*를 여러 번 클릭해도 대비 및 밝기가 원하는 대로 설정되지 않는 경우에는 수동으로 대비 및 밝기를 조정하는 것이 도움이 될 수 있습니다. 밝기를 증가시킵니다. 대비를 움직이기 전에 10 단위 이상 높이지 않습니다. 일반적으로 대비는 아주 적게 움직여야 합니다.

노이즈 설정

한계치 탐지

일부의 경우 비디오 전송의 노이즈는 패킷/초 카운트를 증가시켜 커서가 이동하는 커서 영역의 작은 점 변경으로 표시됩니다. 임계값을 변경하면 화면이 "더 깨끗해 지고" 커서 추적이 향상됩니다.

표준 비디오 압축을 사용하는 경우 노이즈 임계값 및 우선 순위 임계값을 수정할 수 있습니다. *Auto Adjust Video*를 클릭하여 기본 임계값을 복원할 수 있습니다.



참고: 노이즈 임계값을 0으로 두면 지속적인 비디오 새로 고침, 네트워크 사용량 증가 및 비디오 깜박임 현상이 발생합니다. 효과적인 시스템 성능을 얻으면서 마우스 커서가 움직이는 영역의 픽셀 색상을 복구할 수 있는 최고 수준으로 노이즈 임계값을 설정하는 것이 좋습니다.



참고: 노이즈 임계값을 조정할 때 넓은 범위의 조정은 슬라이더 막대를 사용하고 미세한 조정은 슬라이더 막대 끝에 있는 더하기 (+) 및 빼기 (-) 버튼을 사용합니다.

색 농도 변경에 대한 정보는 85페이지의 "보기 조정"을 참조하십시오.

마우스 설정

조정 마우스 옵션

Video Viewer 창 마우스 옵션은 커서 유형, 커서 모드, 배율 조정, 정렬 및 재설정에 영향을 줍니다. 마우스 설정은 장치별로 적용됩니다. 즉, 각 장치에 대해 다르게 설정할 수 있습니다.



참고: 장치가 마우스를 뺐다가 다시 꽂는 기능을 지원하지 않으면(거의 모든 신형 PC는 지원함) 마우스를 사용할 수 없게 되어 장치를 재부팅해야 합니다.

커서 유형

Video Viewer 창은 로컬 마우스 커서에 대한 5가지 표시 옵션을 제공합니다. 커서를 선택하지 않거나 기본 커서를 선택할 수도 있습니다.

단일 커서 모드에서는 Video Viewer 창의 로컬(보조) 커서 표시가 꺼지고 대상 장치 마우스 포인터만 볼 수 있습니다. 표시되는 유일한 마우스 움직임은 대상 장치 원격 커서의 움직임입니다. 단일 커서 모드는 로컬 커서가 필요하지 않을 경우에 사용됩니다.

그림 4.3. 로컬 및 원격 커서가 표시된 Video Viewer 창

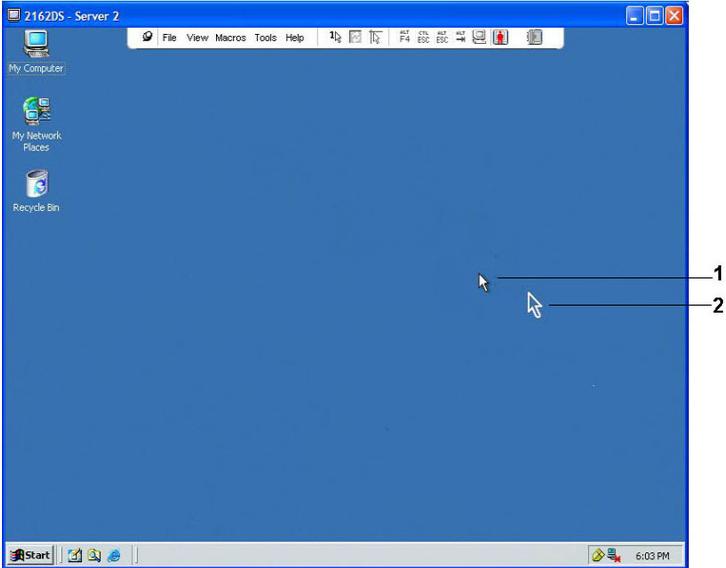


표 4.3: 그림 4.3 설명

번호	설명
1	원격 커서
2	로컬 커서

Video Viewer 창의 커서 모드 상태는 단일 커서 모드를 종료하는 키 입력과 함께 제목 표시줄에 표시됩니다. Session Options 대화 상자에서 단일 커서 모드를 종료하는 키 입력을 정의할 수 있습니다.



참고: 클라이언트 서버에 도달하기 전에 키 입력을 캡처하는 장치를 사용할 경우 마우스 포인터를 복원하기 위해 이 키를 사용하지 않아야 합니다.

단일 커서 모드에 들어가려면 Video Viewer 창 메뉴에서 *Tools - Single Cursor Mode*를 선택하거나 *Single Cursor Mode* 버튼을 클릭합니다. 로컬 커서는 표시되지 않고 모든 움직임은 대상 장치와 연관됩니다.

기존 단일 커서 모드에 대한 키를 선택하려면:

- 1 Video Viewer 창에서 *Tools - Session Options*를 선택합니다.
-또는-
Session Options 버튼을 클릭합니다.
Session Options 대화 상자가 표시됩니다.
- 2 *Mouse* 탭을 클릭합니다.
- 3 단일 커서 모드 영역의 드롭다운 메뉴에서 종료 키 입력을 선택합니다.
- 4 *Save*를 클릭하여 설정을 저장합니다.

단일 커서 모드를 활성화할 경우 지정된 키를 눌러 일반 바탕화면 모드로 복귀할 수 있습니다.

단일 커서 모드를 종료하려면 제목 표시줄에 있는 키보드의 키를 누릅니다.

마우스 커서 설정을 변경하려면:

- 1 Video Viewer 창에서 *Tools - Session Options*를 선택합니다.
-또는-
Session Options 버튼을 클릭합니다.
Session Options 대화 상자가 표시됩니다.
- 2 *Mouse* 탭을 클릭합니다.
- 3 Local Cursor 패널에서 마우스 커서 유형을 선택합니다.
- 4 *OK*를 클릭하여 설정을 저장합니다.

마우스배율 조정

일부 이전 버전의 Linux는 조정 가능한 마우스 가속을 지원하지 않습니다. 이러한 이전 버전을 지원해야 하는 설치의 경우, 3개의 사전 구성된 마우스 배율 옵션 중에서 선택하거나 사용자 정의 배율을 설정할 수 있습니다. 미리 구성된 설정은 Default(1:1), High(2:1) 또는 Low(1:2)입니다.

- 1:1 배율에서는, 바탕 화면 창에서의 마우스 움직임을 동일한 마우스 이동으로 대상 장치에 전송합니다.
- 2:1 배율에서는 같은 마우스 움직임이 2배로 확대되어 전송됩니다.
- 1:2 배율에서는 값이 1/2배로 줄어듭니다.

마우스 스케일링을 설정하려면:

1 Video Viewer 창에서 *Tools - Session Options*를 선택합니다.

-또는-

Session Options 버튼을 클릭합니다.

Session Options 대화 상자가 표시됩니다.

2 *Mouse* 탭을 클릭합니다.

3 사전 구성된 설정 중 하나를 사용하려면 원하는 라디오 버튼을 선택합니다.

-또는-

사용자 정의 배율을 설정하려면:

- a. *Custom* 라디오 버튼을 클릭하여 X 및 Y 필드를 활성화합니다.
- b. X 및 Y 필드에 배율 값을 입력합니다. 마우스 입력 때마다, 마우스 움직임이 각각의 X 및 Y 배율 계수에 의해 증가됩니다. 유효한 입력 범위는 0.25-3.00입니다.

마우스 정렬 및 동기화

스위치 OBWI는 마우스로부터 지속적인 피드백을 받을 수 없기 때문에 스위치의 마우스가 호스트 시스템의 마우스와 서로 동기화되지 않을 수 있습니다. 마우스나 키보드가 더 이상 올바르게 응답하지 않을 경우 마우스를 정렬하여 적절한 트래킹을 재설정하십시오.

정렬은 로컬 커서와 원격 대상 장치의 커서를 정렬합니다. 재설정하면 마우스 및 키보드를 연결 해제했다가 다시 연결할 때 처럼 마우스와 키보드의 재연결을 시연합니다.

마우스를 다시 정렬하려면 Video Viewer 창 도구 모음에서 *Align Local Cursor* 버튼을 클릭하십시오.

가상 미디어

가상 미디어 기능을 사용하면 클라이언트 서버의 사용자가 해당 시스템의 물리적 드라이브를 대상 장치의 가상 드라이브로 매핑할 수 있습니다. 또한 클라이언트 서버는 ISO 또는 플로피 이미지 파일을 대상 장치의 가상 드라이브로서 추가하고 매핑할 수 있습니다. 하나의 CD 드라이브 및 매핑된 하나의 대용량 저장 장치를 동시에 가질 수 있습니다.

- CD/DVD 드라이브, 디스크 이미지 파일(예: ISO 또는 플로피 이미지 파일)이 가상 CD/DVD-ROM 드라이브로 매핑됩니다.
- 플로피 드라이브, USB 메모리 장치나 기타 미디어 유형은 가상 대용량 저장 장치로 매핑됩니다.

OBWI를 사용하여 가상 미디어 설정을 구성하는 방법에 대한 자세한 내용은 73페이지의 "로컬 가상 미디어 세션 구성"을 참조하십시오.

요구 사항

대상 장치는 가상 미디어를 지원하고 USB2 또는 USB2+CAC SIP을 사용하여 KVM 스위치에 연결해야 합니다.

대상 장치는 가상으로 매핑하는 USB2 호환 미디어 유형을 본질적으로 사용할 수 있어야 합니다. 즉, 대상 장치가 이동식 USB 메모리 장치를 지원하지 않으면 클라이언트 서버에서 대상 장치에 가상 미디어 드라이브로 매핑할 수 없습니다.

사용자(또는 사용자가 속한 사용자 그룹)는 가상 미디어 세션 및/또는 예약된 가상 미디어 세션을 대상 장치에 설정할 수 있는 권한을 가지고 있어야 합니다. 76페이지의 "사용자 계정 설정"을 참조하십시오.

한 번에 하나의 가상 미디어 세션만 대상 장치에 활성화될 수 있습니다.

공유 및 선점 고려 사항

KVM 및 가상 미디어 세션은 별개이므로 세션의 공유, 예약 또는 선점을 위한 여러가지 옵션이 있습니다. Avocent 관리 소프트웨어는 시스템 요구를 수용할 수 있는 유연성을 제공합니다.

예를 들어, KVM 및 가상 미디어 세션은 함께 잠길 수 있습니다. 이 모드에서 KVM 세션이 연결 해제된 경우 연관된 가상 미디어 세션도 연결 해제됩니다. 세션이 함께 잠기지 않을 경우 KVM 세션은 닫을 수 있지만 가상 미디어 세션은 활성 상태를 유지합니다. 만일 사용자가 가상 미디어 세션을 사용하여 운영 체제 로드와 같은 시간 집중적인 작업을 수행하고 있고 운영 체제 로드 진행 중에 다른 기능을 수행하기 위해 다른 대상 장치를 사용하여 KVM 세션을 설정하려는 경우 바람직한 방법이 될 수 있습니다.

대상 장치가 연관된 활성 KVM 세션이 없는 활성 가상 미디어 세션을 가지고 있을 경우 두 가지 상황이 발생할 수 있습니다. 즉, 원래 사용자(사용자 A)가 재연결하거나 다른 사용자(사용자 B)가 해당 채널에 연결할 수 있습니다. Virtual Media 대화 상자에서 사용자 A만 KVM 세션을 가진 해당 채널에 액세스할 수 있도록 하는 옵션(예약됨)을 설정할 수 있습니다.

사용자 B가 해당 세션을 액세스할 수 있는 경우(예약된 옵션을 사용할 수 없음), 사용자 B는 가상 미디어 세션에서 사용 중인 미디어를 제어할 수 있습니다. 계층 환경에서 예약된 옵션을 사용하여 사용자 A

만 사용자 A에게 예약된 상위 스위치 및 하위 스위치 사이에서 하위 스위치 및 KVM 채널을 액세스할 수 있습니다.

Virtual Media 대화 상자

Virtual Media 대화 상자를 사용하여 가상 미디어의 매핑 및 매핑 해제를 관리할 수 있습니다. 이 대화 상자에는 가상 미디어로 매핑할 수 있는 클라이언트 서버의 모든 실제 드라이브가 표시됩니다. ISO 및 플로피 이미지 파일도 추가하고 Virtual Media 대화 상자를 사용하여 매핑할 수 있습니다.

장치가 매핑된 후 Virtual Media 대화 상자 상세 보기는 장치가 매핑된 이후 전송된 데이터 양 및 경과 시간을 표시합니다.

가상 미디어 세션이 예약되도록 지정할 수 있습니다. 세션이 예약되고 연결된 KVM 세션이 닫힐 경우 다른 사용자는 해당 대상 장치에 KVM 세션을 시작할 수 없습니다. 세션이 예약되지 않은 경우 다른 KVM 세션을 시작할 수 있습니다.

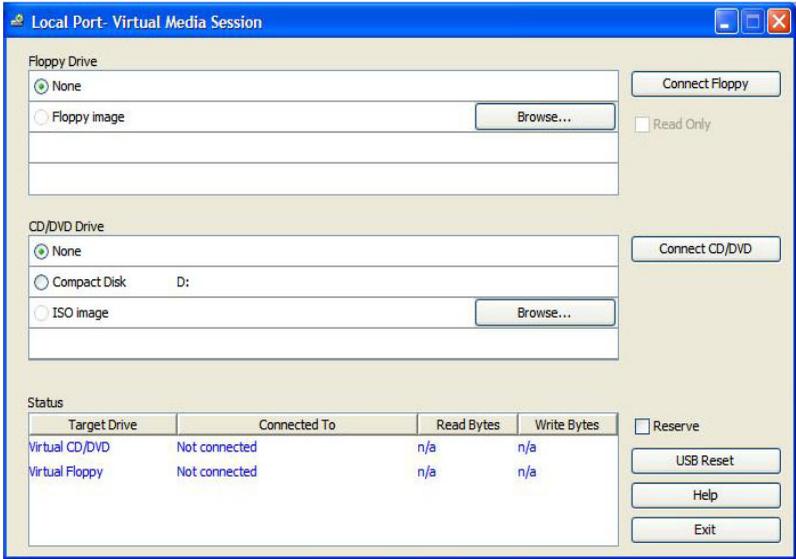
Virtual Media 대화 상자에서 SIP를 재설정할 수도 있습니다. 이 작업을 수행하면 대상 장치의 USB 미디어의 모든 형식이 재설정됩니다. 대상 장치가 응답하지 않을 경우에만 주의해서 사용합니다.

Virtual Media 세션 열기

가상 미디어 세션을 시작하려면:

Video Viewer 메뉴에서 *Tools - Virtual Media*를 선택합니다. Virtual Media 대화 상자가 나타납니다. 이 예약 세션을 만들려면 *Details*를 선택하고 *Reserved* 확인란을 선택합니다.

그림 4.4. Video Viewer Virtual Media 대화 상자



가상 미디어 드라이브를 매핑하려면 :

- 1 Tools - Virtual Media를 선택하여 Video Viewer 메뉴에서 가상 미디어 세션을 엽니다.
- 2 물리적 드라이브를 가상 미디어 드라이브로 매핑하려면 :
 - a. Virtual Media 대화 상자에서 매핑하려는 드라이브 옆의 *Mapped* 확인란을 클릭합니다.
 - b. 매핑된 드라이브를 읽기 전용 액세스로 제한하려는 경우 드라이브 옆의 *Read Only* 확인란을 클릭합니다. 가상 미디어 세션 설정이 이전에 구성되어 있어 모든 매핑된 드라이브가 읽기 전용이 되어야 할 경우 이 확인란은 이미 사용으로 설정되고 변경할 수 없습니다.

세션 설정은 읽기 및 쓰기 액세스를 사용으로 설정되어 있지만 특정한 드라이브 액세스를 읽기 전용으로

제한하려는 경우 *Read Only* 확인란을 사용으로 설정할 수 있습니다.

- 3 ISO 또는 플로피 이미지를 가상 미디어 드라이브로 추가하고 매핑하려면:
 - a. Virtual Media 대화 상자에서 *Add Image*를 클릭합니다.
 - b. 공통 파일 대화 상자가 표시되며 디스크 이미지 파일(즉, *.iso* 또는 *.img*로 끝나는 파일)을 포함하고 있는 디렉토리가 표시됩니다. 원하는 ISO 또는 플로피 이미지 파일을 선택하고 *Open*을 클릭합니다.

-또는-

클라이언트 서버의 운영 체제가 끌어다 놓기를 지원할 경우 공통 파일 대화 상자에서 원하는 ISO 또는 플로피 이미지 파일을 선택하고 Virtual Media 대화 상자에 끌어다 놓습니다.

- c. 파일이 올바른지 확인하기 위해 파일의 헤더를 확인합니다. 올바른 파일일 경우 공통 파일 대화 상자가 닫히고 선택된 이미지 파일은 Virtual Media 대화 상자에 표시되고 여기서 *Mapped* 확인란을 클릭하여 매핑할 수 있습니다.
- d. ISO 또는 플로피 이미지를 추가하고자 할 경우 a ~ c 단계를 반복합니다. 임의 수의 이미지 파일을 추가할 수 있지만(최대 메모리 한계까지), 하나의 가상 CD, DVD 또는 가상 대용량 저장 장치만 동시에 매핑할 수 있습니다.

너무 많은 드라이브(하나의 CD 또는 DVD 및 하나의 대용량 저장 장치) 또는 너무 많은 특정 유형의 드라이브(둘 이상의 CD, DVD 또는 대용량 저장 장치)를 매핑하려고 시도할 경우 메시지가 표시됩니다. 새 드라이브를 매핑하려는 경우 먼저 기존 매핑된 드라이브를 매핑 해제한 다음 새 드라이브를 매핑합니다.

물리적 드라이브나 이미지가 매핑된 후 대상 장치에서 사용될 수 있습니다.

가상 미디어 드라이브의 매핑을 해제하려면:

- 1 Virtual Media 대화 상자에서 매핑 해제하려는 드라이브 옆의 *Mapped* 확인란을 선택 해제합니다.
- 2 확인하기 위한 프롬프트가 표시됩니다. 매핑 해제를 확인하거나 취소합니다.
- 3 추가적인 가상 미디어 드라이브를 매핑 해제하려면 반복합니다.

가상 미디어 드라이브 상세 정보를 표시하려면:

Virtual Media 대화 상자에서 *Details*를 클릭합니다 대화 상자가 *Details* 표를 표시하기 위해 확장됩니다. 각 행은 다음 사항을 나타냅니다.

- Target Drive - Virtual CD 1 또는 Virtual CD 2와 같이 매핑된 드라이브를 위해 사용된 이름
- Mapped to - 클라이언트 보기 드라이브 열에 표시되는 드라이브 정보와 동일
- Read Bytes and Write Bytes - 매핑 이후 전송된 데이터 양
- Duration - 드라이브가 매핑된 후 경과 시간

Details 창을 닫으려면 *Details*를 다시 클릭합니다.

대상 장치에서 모든 USB 장치를 재설정하려면:



참고: USB 재설정 기능은 마우스와 키보드를 포함하여 대상 장치의 모든 USB 장치를 재설정합니다. 대상 장치가 응답하지 않을 때만 사용해야 합니다.

- 1 Virtual Media 대화 상자에서 *Details*를 클릭합니다
- 2 *Details View*가 나타납니다. *USB Reset*을 클릭합니다.
- 3 재설정의 영향을 나타내는 경고 메시지가 표시됩니다. 재설정을 확인하거나 취소합니다.
- 4 *Details* 창을 닫으려면 *Details*를 다시 클릭합니다.

가상 미디어 세션 닫기

Virtual Media 대화 상자를 닫으려면:

- 1 *Exit*를 클릭합니다.
- 2 매핑된 드라이브가 있는 경우 드라이브가 매핑 해제된다는 메시지가 표시됩니다. 작업을 확인하거나 취소합니다.

사용자가 가상 미디어 세션이나 잠겨진 가상 미디어 세션과 연결된 활성 KVM 세션을 연결 해제하려고 할 경우 가상 미디어 매핑이 해제된다는 확인 메시지가 표시됩니다.

스마트 카드

스마트 카드 판독기를 클라이언트 서버의 가용한 USB 포트에 연결하고 스위치 시스템의 연결된 대상 장치에 액세스할 수 있습니다. 그런 후 KVM 세션을 실행하여 Video Viewer를 열고 스마트 카드를 매핑할 수 있습니다.

 **참고:** 모든 스마트 카드 판독기의 경우 Dell USB2+CAC SIP 또는 Avocent VMC IQ 모듈을 사용해야 합니다.

비디오 뷰어 도구 모음의 오른쪽 모서리에 있는 스마트 카드 아이콘에 스마트 카드 상태가 표시됩니다. 다음 표는 스마트 카드 상태 아이콘을 설명합니다.

표 4.4: 스마트 카드 아이콘

아이콘	설명
	스마트 카드가 스마트 카드 판독기에 있지 않거나, 스마트 카드 판독기가 연결되어 있지 않습니다.
	스마트 카드가 스마트 카드 판독기에 있지만 매핑되지 않았습니다.
	스마트 카드가 매핑되었습니다(녹색 아이콘).

스마트 카드를 매핑하려면:

- 1 KVM 세션을 열어 Video Viewer 창 메뉴를 표시합니다.
- 2 클라이언트 서버에 연결된 스마트 카드 판독기에 스마트 카드를 넣습니다.
- 3 Video Viewer 창 메뉴에서 *Tools - Map Smart Card*를 클릭합니다.
- 4 대상 장치에 매핑된 스마트 카드가 없으면 매핑된 카드 없음 옵션 옆에 점이 표시됩니다. 이 옵션 아래 나열된 스마트 카드를 선택하여 스마트 카드를 매핑합니다.

스마트 카드 매핑을 해제하려면 Video Viewer 창 메뉴에서 X를 클릭하고 *Tools - No Card Mapped*를 선택하고 스마트 카드 판독기에서 스마트 카드를 제거하거나 클라이언트 서버에서 스마트 카드 판독기를 연결 해제하여 KVM 세션을 닫습니다.

Keyboard Pass-through

Video Viewer 창을 사용할 때 사용자가 입력하는 키 입력은 Video Viewer 창의 화면 모드에 따라 두 가지 방법으로 해석할 수 있습니다.

- 비디오 뷰어 창이 전체 화면 모드일 경우 *Ctrl-Alt-Del*을 제외하고 모든 키 입력 및 키보드 조합이 보고 있는 원격 대상 장치로 전송됩니다.
- Video Viewer 창이 정상 바탕화면 모드일 경우 keyboard pass through 모드를 사용하여 원격 대상 장치 또는 로컬 컴퓨터가 특정 키 입력 또는 키 입력 조합을 인식하도록 제어할 수 있습니다.

Keyboard pass-through는 Session Options 대화 상자를 사용하여 지정해야 합니다. 사용으로 설정한 경우 keyboard pass-through는 *Ctrl-Alt-Del*을 제외하고 모든 키 입력 및 키 입력 조합을 Video Viewer 창이 활성화되었을 때 보고 있는 원격 대상 장치로 전송합니다. 로컬 바탕화면이 활성화된 경우 사용자가 입력한 키 입력 및 키 입력 조합이 로컬 컴퓨터에 영향을 미칩니다.



참고: Ctrl-Alt-Del 키보드 조합은 매크로를 사용하여 원격 대상 장치만으로 전송할 수 있습니다.



참고: 일본어 키보드 ALT-Han/Zen 키 입력 조합은 화면 모드나 keyboard pass through 설정에 상관 없이 항상 대상 장치로 전송됩니다.

keyboard pass through를 지정하려면:

- 1 Video Viewer 창에서 *Tools - Session Options*를 선택합니다.
-또는-
Session Options 버튼을 클릭합니다.
Session Options 대화 상자가 표시됩니다.
- 2 *General* 탭을 클릭합니다.
- 3 *Pass-through all keystrokes in regular window mode*를 선택합니다
- 4 *OK*를 클릭하여 설정을 저장합니다.

매크로

스위치 OBWI는 Windows, Linux 및 Sun 플랫폼용 매크로로 사전에 구성되어 제공됩니다.

매크로를 전송하려면 Video Viewer 창 메뉴에서 *Macros - <desired macro>*를 선택하거나 Video Viewer 메뉴에 있는 버튼에서 원하는 매크로를 선택합니다.

보기 저장

Video Viewer의 화면을 파일이나 클립보드로 저장하여 워드 프로세서나 다른 프로그램에 붙여넣기 할 수 있습니다.

Video Viewer 창을 파일로 캡처하려면:

- 1 Video Viewer 창 메뉴에서 *File - Capture to File*을 선택합니다.
-또는-
Capture to File 버튼을 클릭합니다.
Save As 저장 대화 상자가 표시됩니다.

2 파일 이름을 입력하고 파일을 저장할 위치를 선택합니다.

3 *Save*를 클릭하여 화면을 파일로 저장합니다.

Video Viewer 창을 클립보드로 캡처하려면 Video Viewer 창 메뉴에서 *File - Capture to Clipboard*를 선택하거나 *Capture to Clipboard* 버튼을 클릭합니다. 이미지 데이터가 클립보드로 저장됩니다.

세션 닫기

Video Viewer 창 세션을 닫으려면:

Video Viewer 창에서 *File - Exit*를 선택합니다.

RCS의 LDAP 기능

LDAP는 TCP/IP를 사용하여 디렉토리를 액세스 및 업데이트하는 데 사용되는 표준 프로토콜입니다. Dell RCS 소프트웨어 및 OBWI는 표준 스키마 및 Dell 확장 스키마를 모두 지원하며 인증, 개인 정보 보호 및 무결성을 포함한 강력한 보안 기능을 제공합니다.



참고: Windows 2008 Server는 IPv6 모드에서 LDAP을 사용해야 합니다.



참고: Active Directory를 사용한 RCS 사용자 인식은 Microsoft Windows® 2000 및 Windows Server 2003 운영 체제에서 지원됩니다.

Active Directory 구조

AD(Active Directory) 배포는 개체의 계층 구조가 포함된 분산형 데이터베이스로 구성됩니다. 각 개체는 해당 개체에 저장할 수 있는 데이터 종류를 결정하는 개체 클래스와 연결됩니다. 계층 구조는 보통 AD 도메인을 나타내는 개체로 시작되며 DNS 이름 공간의 일반적인 서술 방식과 동일한 방식의 3개 도표로 나타낼 수 있는 도메인 이름 계층을 형성하도록 배포됩니다. Dell RCS는 얕거나 깊은 계층 이름 구조로 배포되는 단일 도메인 트리를 지원하도록 설계되어 있습니다.

도메인 컨트롤러 컴퓨터

도메인 계층은 ADLDAP 서비스를 제공하는 도메인 컨트롤러 컴퓨터의 상응하는 계층과 연결되어 있습니다. 각 도메인에는 여러 개의 피어 도메인 컨트롤러가 있을 수 있으며 이들 역시 지리적으로 분산되어 있을 수 있습니다. Dell RCS 제품군은 AD의 이러한 측면을 모두 지원하도록 설계되어 있습니다. DNS는 각 도메인 컨트롤러의 네트워크 위치를 파악해 네트워크에서 도메인 컨트롤러 일부를 사용할 수 없

을 때 Dell RCS가 상황을 적절히 해결할 수 있도록 해 줍니다. DNS SRV 레코드는 이러한 목적으로 사용되므로 Dell RCS는 SRV 레코드에 구성되어 있는 관리 설정에 따라 항상 먼저 가장 가까운 지점의 대체 도메인 컨트롤러에 접속을 시도합니다.

개체 클래스

각 도메인에는 다양한 항목 및 항목 그룹화에 대한 정보를 저장하도록 설계된 개체의 또 다른 계층이 있습니다. 이들 항목은 AD에서 개체 그룹화 구성을 돕는 "컨테이너"를 정의하는 데 사용되는 개체 클래스에 의해 나타납니다. 다른 개체 클래스들은 네트워크 사용자, 컴퓨터, 프린터 또는 네트워크 서비스와 같은 항목들을 나타냅니다. 두 종류의 컨테이너 개체 클래스인 그룹 및 구성 단위(OU)는 특별한 역할을 합니다. 이 두 가지 개체 클래스는 AD 관리자가 액세스 제어 및 기타 관리 상의 정책 적용을 단순화하기 위한 목적으로 개체의 그룹화를 정의할 수 있게 합니다. 예를 들어, '하드웨어', '소프트웨어', '지원' 등 기능에 따라 이름을 정한 여러 그룹 개체가 포함된 'Engineering'이라는 OU 컨테이너를 포함하도록 도메인을 구성할 수 있으며, 각 그룹은 사용자 개체 및 컴퓨터 개체 구성원 목록으로 구성됩니다. 하지만 중첩 그룹에 의해 또 다른 계층 수준을 구성할 수 있습니다. 중첩은 그룹 개체 이름을 다른 그룹 개체의 구성원에 포함함으로써 형성됩니다. 이 때 각 AD 그룹 개체에는 해당 그룹이 다른 그룹과 갖도록 허용된 중첩 관계 유형을 구성하는 데 사용되는 연결된 범위가 있습니다. 예를 들어 범위가 유니버설로 설정되면 이 그룹은 도메인 경계를 넘는 중첩에 참가할 수 있지만 범위가 로컬로 설정되면 이러한 중첩에는 참가할 수 없습니다. 중첩 규칙은 Microsoft에서 구할 수 있는 AD 제품 설명서에 나와 있습니다. Dell RCSs 제품군은 AD에 대해 정의된 중첩 규칙을 모두 지원하도록 설계되어 있습니다.

속성

AD에 사용되는 계층은 한 개가 더 있습니다. 나타낼 항목에 관한 구체적인 정보를 저장하는 데 사용되는 "속성" 집합이 각 개체 클래스와 연결되어 있습니다. 예를 들어, 사용자 개체 클래스에는 SAM ACCOUNT NAME이라는 속성 유형과 FIRST NAME, SURNAME,

PASSWORD 등과 같은 기타 속성이 연결되어 있습니다. Dell Remote Console Switches 세트는 SAM ACCOUNT NAME 및 PASSWORD 속성을 사용하여 사용자를 인증합니다(이러한 두 속성의 공식 AD 이름은 각각 sAMAccountName과 unicodePWD입니다).

스키마 확장

AD에는 컴퓨터 및 사용자 개체용 기본 컨테이너뿐 아니라 OU 컨테이너용 클래스 및 컴퓨터 및 사용자 항목을 나타내는 클래스를 비롯한 많은 개체 클래스가 포함되어 있습니다. Dell이 액세스 컨트롤 관리를 간단하게 만들기 위해 제공하는 것과 같은 새로운 개체 클래스를 포함하도록 AD를 확장할 수 있으며, 이러한 확장을 일반적으로 "스키마 확장"이라 하며 본 설명서에서 설명하는 Dell 확장 스키마 기능의 핵심이라고 할 수 있습니다. 이 스키마 확장은 특정 액세스 제어 정보를 Dell RCSs 및 사용자의 특정 인스턴스와 연결하는 데 사용된 Dell RCSs, 액세스 제어 정보 및 컨테이너 유형을 나타내는 사용자 정의된 개체 클래스를 제공합니다. AD에서 사용된 각 속성 유형 및 개체 클래스에는 개체 식별자(OID)로 알려져 있는 글로벌 고유 식별자가 있어야 합니다. 이 고유 식별자는 국제 공인 기관에서 최종 관리하며, AD의 경우 OID 공간은 Microsoft에서 2차적으로 관리합니다. Dell은 Dell 확장 스키마 기능에서 사용된 사용자 정의 개체 클래스 및 속성 유형을 위한 OID를 확보했습니다. 아래에 Dell이 확보한 OID가 요약되어 있습니다.

Dell 확장: dell

Dell 베이스 OID: 1.2.840.113556.1.8000.1280

RCS LinkID 범위: 12070 ~ 12079

Dell RCSs 제품군도 AD 패키지 클래스에 있는 개체 클래스만 사용해서 작동하도록 설계되어 있으며, 이 옵션은 표준 스키마라고 합니다. 이 옵션에서 컴퓨터 개체 클래스는 Dell RCSs를 나타내는 데 사용되며 표준 그룹 개체는 특정 액세스 제어 정보를 Dell RCSs 및 사용자의 특정 인스턴스와 연결하는 데 사용됩니다. 이 경우 액세스 제어 정보는 그룹 개체의 특정 속성 유형에 저장됩니다.

AD에 있는 계층 구조는 디렉토리 개체에 저장된 정보에 대한 사용자의 액세스를 복잡하게 만들 수 있습니다. 계층에 대한 탐색과 관련된 지연 가능성을 없애기 위해 Dell Remote Console Switch 제품군은 GC (Global Catalog)라는 AD의 한 측면을 사용하도록 설계되어 있습니다. GC는 전체 AD 데이터베이스에 저장되어 있는 데이터 하위 집합에 대한 액세스를 제공하고 모든 계층 및 지리적 분포를 비교적 평평한 단일 구조로 "축소"시켜 "빠른 조회서비스"를 제공합니다. GC는 전체 AD 데이터베이스에서 작동하는 동일한 LDAP 디렉토리 쿼리를 사용하여 조회합니다. AD 제품이 GC 서비스를 제공하도록 구성하려면 기업 내에 하나 이상의 도메인 컨트롤러가 필요하며 AD의 실제 배포 시 일부 또는 전체 도메인 컨트롤러가 GC 서비스를 제공하도록 구성할 수 있습니다. Dell RCSs 제품군은 DNS를 사용해 각 GC 서버의 네트워크 위치를 파악하여 네트워크에서 GC 서버 일부를 사용할 수 없을 때 상황을 적절히 해결할 수 있게 해 줍니다. DNS SRV 레코드는 이러한 목적으로 사용되므로 Dell RCSs는 SRV 레코드에 구성되어 있는 관리 설정에 따라 항상 먼저 "가장 가까운" 지점의 대체 GC 서버에 접속을 시도합니다.

표준 스키마 대 Dell 확장 스키마

다수의 고객 환경에 최대한의 유연성을 제공하기 위해 Dell은 원하는 결과를 기준으로 사용자가 구성할 수 있는 개체 그룹을 제공합니다. Dell은 연결, 장치 및 권한 개체가 포함되도록 스키마를 확장했습니다. 연결 개체는 특정 권한 집합을 보유한 사용자 또는 그룹을 한 개 이상의 SIP에 연결하는 데 사용됩니다. 장치 개체는 Active Directory 구조 내 개별 RCS 스위치를 정의하고 권한 개체는 사용 권한을 할당하기 위해 연결 개체를 통해 장치 개체에 연결됩니다.

이 모델은 복잡성을 심화시키지 않으면서 사용자, 권한 및 Remote Console Switch의 SIP를 다양하게 조합할 수 있어 관리자에게 최대한의 유연성을 제공합니다.

Dell 스키마 확장을 설치하기 전에 관리자는 이 장의 설명 및 지침을 꼼꼼히 읽어 특정 설치에 어떤 스키마가 적합한지 파악해야 합니다. 스키마 개체를 변경하면 Active Directory 전체에 영향이 미치기 때문

에 생성된 후에는 삭제할 수 없으며, 비활성화만 가능합니다. 따라서 스키마를 변경하기 전에 변경에 따른 이점을 신중히 고려해야 합니다.

Dell 스키마 확장을 설치하여 얻을 수 있는 주요 이점은 혼란을 없애 준다는 것입니다. 표준 Active Directory 스키마를 사용할 경우 Remote Console Switch는 대개 컴퓨터 장치 개체에 가장 비슷하게 대응하며 하나로 구성됩니다. 하지만 RCS 스위치는 컴퓨터가 아니므로 일부 스키마 기능은 적용되지 않습니다. 이러한 방법으로 지정된 RCS 스위치를 올바르게 구성하려면 신중을 기해야 합니다.

아울러 Dell 스키마 확장을 이용하면 보다 쉽게 스위치 장치를 검색하고 식별할 수 있습니다. 컴퓨터 장치 개체를 사용하여 구성된 스위치는 Active Directory 구조 내 모든 컴퓨터 장치에서 검색됩니다.

RCS는 어느 한쪽의 스키마를 사용해 동등하게 인증할 수 있으며 어떤 방법을 사용하든 기능은 전혀 유실되지 않습니다. 관리자는 특정 설치에 어떤 방법이 적합한지 선택할 수 있습니다. Dell 스키마 확장 여부에 따른 설치에 대한 지침이 제공되었습니다. 하나의 스키마 집합에만 속하는 절 및 지침은 이와 같이 표시되며 사용되지 않는 설치에서는 무시될 수 있습니다.

표준 설치

Dell RCS에서 인증을 위해 Active Directory를 사용하려면 다음을 수행합니다.

- 1 관리자 무시 계정 구성
- 2 DNS 설정 구성
- 3 네트워크 시간 프로토콜 설정
- 4 인증 매개변수 구성
- 5 그룹 개체 구성
- 6 CA 루트 인증서 작성 및 다운로드
- 7 로그인 제한 시간 설정

관리자 무시 계정 구성

네트워크 오류가 발생하면 LDAP 서버에 대한 장치의 인증 권한과 관계 없이 사용할 수 있는 계정이 제공됩니다. 다른 설정을 구성하기 전에 이 계정을 구성해야 합니다. 온보드 웹 인터페이스에서 Override 관리자 계정을 구성하려면:

- 1 *User Accounts*를 클릭한 다음 *Override Admin*을 클릭합니다.
- 2 사용자에게 할당할 사용자 이름과 비밀번호를 입력한 후 Verify Password 필드에 비밀번호를 다시 입력하여 확인합니다.
- 3 *Save*를 클릭합니다.

 **참고:** 이 옵션의 경우 관리자로 로그인되어야 합니다.

DNS 설정 구성

LDAP 클라이언트가 이름을 확인하기 전에 하나 이상의 DNS 서버를 지정해야 합니다.

그러면 Network 하위 범주에 RCS의 이름이 표시되고 IP 주소, 서브넷 마스크, 게이트웨이, LAN 속도 및 DHCP/BootP 설정을 포함한 네트워크 설정을 변경할 수 있습니다. RCS용으로 표시된 이름은 SNMP 범주의 System Name 필드에서 지정된 이름과 동일합니다.

Network 하위 범주에는 최대 3개의 DNS 서버까지 입력 및 관리할 수 있습니다. 이 DNS 서버는 LDAP 인증 패널에서 제공된 DNS 이름을 확인하는 데 사용됩니다.

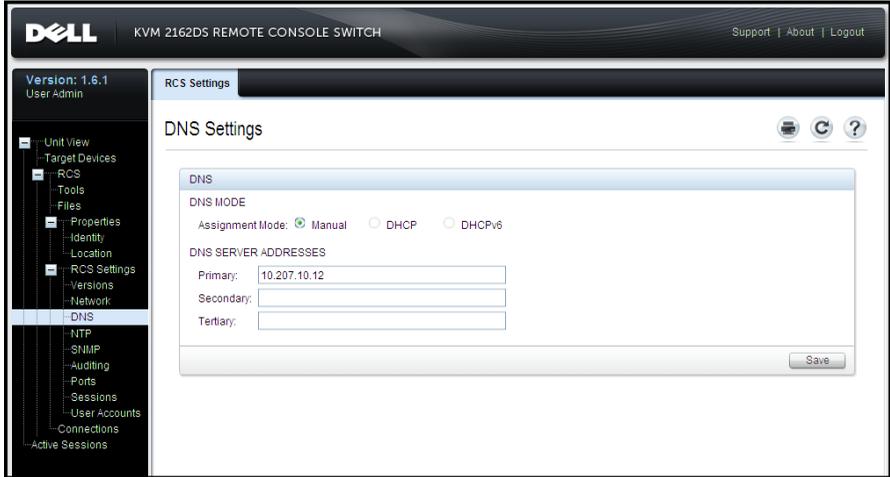
 **참고:** LDAP 기능이 작동하려면 하나 이상의 DNS 서버를 구성해야 합니다. 기본 서버가 사용할 수 없을 때마다 RCS 소프트웨어는 자동으로 여기에 식별된 대로, 백업 DNS 서버로 장애복구합니다.

 **참고:** RCS의 연속적인 관리 인터페이스를 사용하여 DNS 서버 주소를 설정할 수도 있습니다. 연속적인 관리 인터페이스 사용에 대한 자세한 내용은 RCS 설명서를 참조하십시오.

온보드 웹 인터페이스에서 DNS 설정을 구성하려면:

- 1 DNS를 클릭하여 DNS Settings 화면을 엽니다.
- 2 DNS 모드를 지정하고 서버 주소를 입력한 다음 Save를 클릭합니다.

그림 5.1. OBWI - DNS 설정



네트워크 시간 프로토콜(NTP) 설정 구성

인증서가 만료되지 않았는지 확인하려면 스위치가 현재 시간에 액세스할 수 있어야 합니다. 스위치가 NTP로부터 시간 업데이트를 요청하도록 구성할 수 있습니다. 온보드 웹 인터페이스에서 NTP 설정을 구성하려면:

- 1 NTP를 클릭하여 NTP 화면을 엽니다.
- 2 **Enable NTP** 상자를 클릭합니다.
- 3 제공된 입력란에 네트워크 시간 소스 이름을 입력합니다. 시간 업데이트 요청 빈도를 지정하기 위한 시간 간격을 설정할 수도 있습니다. 간격을 0으로 설정하면 RCS 시작 또는 Global - NTP 메뉴 변경 시에만 요청이 수용됩니다.
- 4 **Save**를 클릭합니다.

LDAP 인증 매개변수 구성

RCS 관리자는 인증 패널을 사용하여 LDAP 디렉토리 서비스에 액세스하는 데 필요한 매개변수를 구성할 수 있습니다. 사용자로부터 액세스 요청을 수신할 때 RCS는 LDAP 프로토콜을 사용하여 사용자 이름, 암호 및 기타 정보를 디렉토리 서비스로 보내어 사용자가 가지는 인증 권한을 결정합니다.



참고: LDAP 구성을 설정하기 위한 용어는 KVM 사용자, KVM 사용자 관리자 및 KVM 기기 관리자이며, 이들은 각각 사용자, 사용자 관리자 및 RCS 관리자 와 동등합니다. 액세스 수준은 변경되지 않고, 지시에 따라 새 용어를 사용합니다.

LDAP 인증 활성화

LDAP Configuration Options 화면의 Operational Modes 세션을 사용하여 사용자 인증에 사용할 적절한 유형의 LDAP 서비스를 선택할 수 있습니다. 다음과 같은 모드를 사용할 수 있습니다.

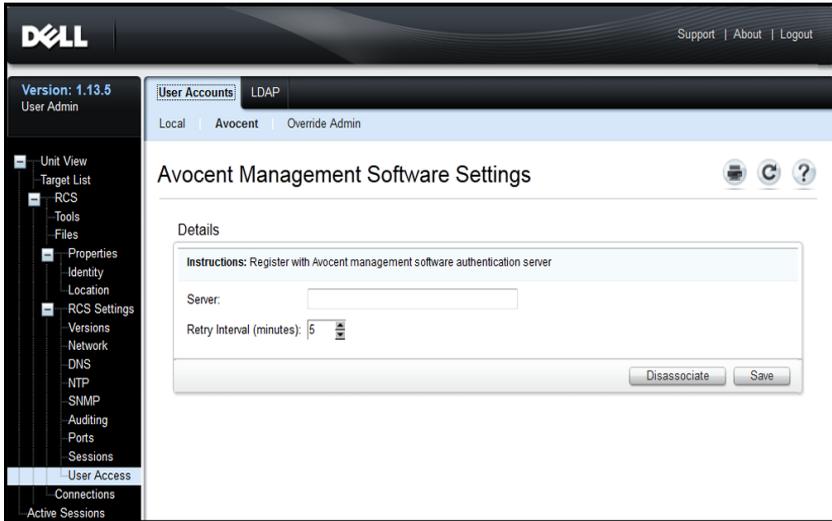
- 표준 LDAP 디렉토리 서비스(비 Microsoft)
- Microsoft Active Directory 서비스
- LDAP 인증 비활성화

대체(비 LDAP) 인증 방법이 이미 사용하도록 선택되었으면 LDAP 인증이 자동으로 비활성화됩니다. LDAP 디렉토리 서비스를 사용하려면 이 방법을 선택 취소해야 합니다.

LDAP 인증을 사용하는 기능을 복원하려면:

- User Access 아래에서 *Avocent* 탭을 선택합니다. 그림 5.2을 참조하십시오.
- Disassociate*를 클릭하여 Avocent 관리 인증 서버 사용을 선택 취소합니다.
- Save*를 클릭합니다.

그림 5.2. Avocent 인증 화면

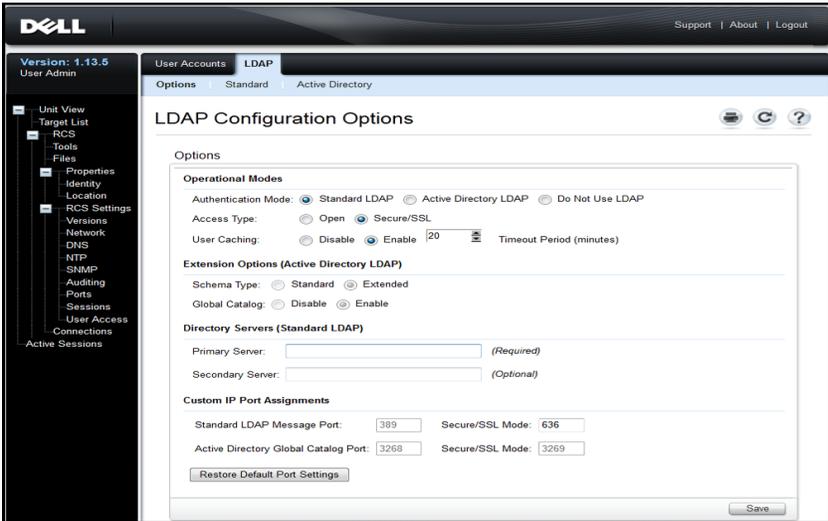


참고: 이러한 단계를 수행하지 않고도 Avocent 인증 연결을 외부적으로 차단할 수 있습니다. 그렇지만, 사용자 인증을 위해 Avocent 서버 연결이 생성되었다면 명시적으로 이 절차를 통해 이 연결을 제거해야 LDAP 인증 구성을 계속 허가할 수 있습니다.

LDAP 인증 활성화:

- 1 User Access 아래에서 LDAP 탭을 선택합니다. 그림 5.3를 참조하십시오.

그림 5.3. LDAP Configuration Options 화면



- 2 Operational Modes 섹션에서 사용 가능한 LDAP 인증 모드 중 하나를 선택합니다.
- 3 구성 옵션은 전체적으로 사용 대상으로 LDAP 인증을 활성화하도록 설정되어야 합니다. 각 옵션에 대해서 이 장에서 자세히 설명합니다.
- 4 Save를 클릭합니다.

LDAP 인증을 비활성화하려면 *Do Not Use LDAP* 옵션을 선택하고 Save를 클릭하십시오. 화면의 다른 모든 옵션은 비활성화되고, 이러한 다른 필드 편집은 허용되지 않습니다. 뿐만 아니라, Standard 및 Active Directory 탭 아래 추가 구성 화면도 비활성화됩니다.

LDAP 인증이 비활성화될 때 User Access는 로컬로 정의된 사용자 액세스 목록이나 Avocent 관리 소프트웨어로 조정됩니다 (User Access 섹션 참조).

LDAP 인증이 활성화될 때 로컬로 정의된 사용자 액세스 목록이 LDAP Directory Servers에 대한 요청보다 높은 우선순위를 가집니다. 사

용자 액세스는 먼저 RCS 정의 사용자를 확인하여 요청합니다. 일치 사항을 찾을 수 없으면 요청은 구성된 대로, LDAP Directory Server로 전송됩니다.

인증 매개변수 입력 - 작동 모드

액세스 유형

LDAP Directory Server를 Open 또는 Secure 모드에서 작동하도록 설정할 수 있습니다(SSL - Secure Socket Layer 암호화 사용). 선택한 모드는 호스트 디렉토리 서버의 모드와 일치해야 합니다. Secure/SSL 모드를 선택할 때 암호화된 작업 요구사항을 충족하기 위한 안내로 LDAP SSL 인증서 섹션도 참조하십시오.

사용자 캐싱

LDAP를 통해 성공적인 사용자 인증이 완료될 때마다 RCS는 선택한 시간 동안 LDAP Directory Server에서 얻은 결과를 보존할 수 있습니다. 그 시간 창에 있는 동안, 일반적으로 Directory Server의 반복 요청을 생성하는 다른 액세스 요청이 생성될 경우 이러한 요청은 RCS에서 즉시 처리됩니다. 이것은 거의 즉각적인 응답으로, 사용자가 지연이 최소화된 여건에서 작업을 계속할 수 있습니다.

이 구성 옵션에 대한 세 가지 설정은 disable(비활성화), enable(활성화) 및 timeout period(시간 초과 기간)입니다.

Disable - 사용자 캐싱을 허용하지 않고, 필요할 때마다 항상 모든 사용자에 대한 인증 상태에 대한 안내를 LDAP Directory Server에 요청합니다. 기본적으로 사용자 캐싱은 비활성입니다.

Enable - LDAP Directory Server의 결정에 따라 최근 사용자 인증 요청의 결과를 유지합니다. 사전 결정된 시간 내에 동일한 인증 요청을 수신할 때 이러한 이전 결과를 사용하여 새 요청을 서비스합니다.

Timeout Period - 시간 창의 지속 기간을 설정합니다. 값은 분으로 기록됩니다. 상자에 숫자만 입력하거나, 화살표 컨트롤을 사용하십시오.

- 기본 시간 초과 값: 15분

- 최소 제한 시간: 1분
- 최대 제한 시간: 1,000분



참고: 모든 구성 업데이트에서처럼, 변경 사항을 저장하려면 **Save**를 클릭해야 합니다. 일반적으로 LDAP 구성 변경 사항은 재부팅할 필요 없이, 즉시 RCS에 사용될 수 있습니다.

확장 옵션 입력 - Active Directory LDAP

Active Directory 모드가 선택될 때 관리자는 표준 또는 확장 스키마를 사용할 지를 결정해야 합니다. 뿐만 아니라, 관리자는 Microsoft Global Catalog 옵션의 사용 여부를 선언해야 합니다.

인증 매개변수 입력 - 표준 LDAP

Microsoft Active Directory LDAP가 아닌 표준 LDAP를 사용할 때는 하나 이상의 관련 디렉토리 서버 주소를 직접 입력해야 합니다. Primary Server 및 Secondary Server 필드에 주소를 입력합니다. 기본 서버 항목은 필수입니다.

다음 중 하나의 방식으로 서버 주소를 입력합니다.

- DNS 주소 (예: myldapserver.com)
- IPv4 주소 (예: 10.20.255.255)
- IPv6 주소 (예: fe80::200:f8af:fe20:76ce)

인증 매개변수 입력 - 사용자 정의 IP 포트 할당

이 섹션에서는 일반적으로 LDAP에 사용되는 업계 표준 IP 포트 번호의 변경을 허용합니다. 대부분의 경우 이 값들을 변경할 필요가 없습니다. 그러나, 사용 중인 LDAP Directory Server 관리자가 다른 포트 할당을 요구하면 그 요구하는 포트를 여기에 입력할 수 있습니다.

정확한 구성에 따라, LDAP는 최대 4개의 IP 포트를, 한 번에 두 개씩 이용할 수 있습니다. 이러한 네 개 포트 각각에 대한 슬롯은 LDAP Configuration Options 화면에 나타납니다. 동일한 화면의 다른 설정은 변경될 수 있는 포트를 식별하는 데 사용됩니다. 다음 차트는 사

용 가능한 포트 슬롯이 활성화되고 편집이 허용되는 조건을 정의합니다.

표 5.1: IP 포트 할당 편집

활성화되고 사용자 정의할 수 있는 포트 슬롯 목록	열기 모드	보안/SSL 모드
Global Catalog 사용 안 함	Standard LDAP 메시지 포트	Standard LDAP 메시지 포트 - Secure/SSL 모드
Global Catalog 사용	Standard LDAP 메시지 포트 및 Active Directory Global Catalog 포트	Standard LDAP 메시지 포트 - Secure/SSL 모드 및 Active Directory Global Catalog 포트 - Secure/SSL 모드

언제든지 원래 산업 표준 IP 포트 지정을 복원해야 할 경우에는 'Restore Default Port Settings' 버튼을 클릭하십시오. 네 개의 포트 값이 모두 다음의 원래 값으로 반환됩니다.

Standard LDAP 메시지 포트 - 389

SSL을 통한 Standard LDAP 메시지 포트 - 636

Global Catalog 서버를 통한 Active Directory - 3268

Global Catalog 서버/SSL을 통한 Active Directory - 3269

IP 포트 번호는 1~65535 범위에서 허용됩니다. 포트 번호가 LDAP Directory Server가 사용하는 포트 번호와 일치하지 않으면 해당 서버와의 통신이 설정되지 않습니다.

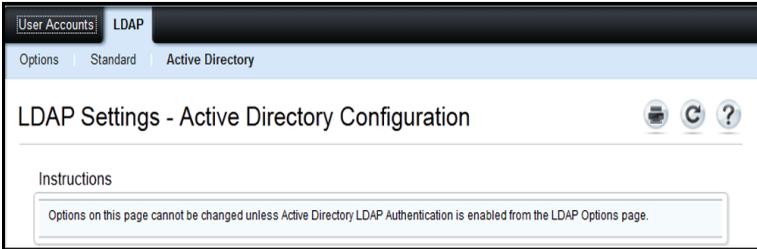
LDAP 구성 완료

표준 및 Active Directory LDAP 모드 모두, LDAP Directory Server에 적절하게 연결되기 위한 추가 매개변수가 필요합니다. 각 매개변수는 다

음 절에 설명되어 있습니다. 그러나, OBWI 페이지에는 해당 페이지에서 매개변수 업데이트를 수행하도록 하여 관리자를 지원하는 'interlocks'가 설정되어 있음을 알아두십시오.

예를 들어, Active Directory LDAP 탭을 선택할 경우 화면에 다음 디스플레이가 표시될 수 있습니다. 그림 5.4을 참조하십시오.

그림 5.4. 알림 메시지 - LDAP 모드 활성화 안 됨 (LDAP Mode Not Enabled)



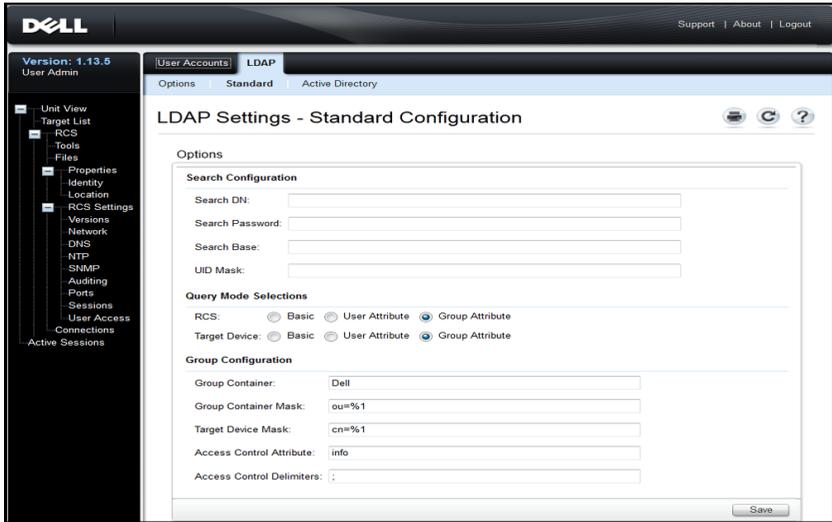
이 화면이 표시될 때 이것은 Active Directory 모드가 활성화되지 않았거나 활성화되었지만 저장되지 않았다는 표시입니다. LDAP Options 화면으로 돌아가서, *Active Directory LDAP*를 선택하고, 해당 페이지에서 이 모드에 대한 보조 매개변수를 기록한 다음 *Save*를 클릭한 후 이 화면으로 돌아가십시오.

표준 LDAP 모드의 경우에도 해당 모드가 활성화되지 않으면 항상 동일한 화면이 나타납니다.

보조 LDAP 설정 - 표준 구성

LDAP Active Directory 구성에서와 마찬가지로, 표준 LDAP 인증, 검색 및 쿼리 매개변수는 원격 OBWI를 통해 구성됩니다. 이 섹션에서 설정은 그림 5.5에 나타난 OBWI 창을 통해 User Access / LDAP / Standard 탭에서 액세스할 수 있습니다.

그림 5.5. 보조 LDAP 설정 - 표준 구성



참고: 이 섹션에서는 표준 LDAP Directory Server에 설정하는 연결에 대한 설정 매개변수를 설명하지만, Active Directory 서비스의 일반 버전엔 연결을 설정할 때도 이 섹션을 사용할 수 있습니다.

표준 LDAP쿼리 수행을 위한 RCS 설정

참고: Active Directory에 대한 쿼리 모드를 사용하기 전에 먼저 선택한 쿼리 모드가 사용자에 대한 올바른 인증 단계를 지정할 수 있도록 Active Directory를 변경해야 합니다

그룹 쿼리를 설정하려면:

- 1 관리자 권한으로 LDAP Directory Server 소프트웨어에 로그인합니다.
- 2 그룹 컨테이너로 사용할 OU(Organizational Unit)를 생성하십시오.
- 3 기기 쿼리를 위해 스위칭 시스템 이름과 동일한 컴퓨터 개체를 생성하거나 대상 장치를 쿼리하기 위해 연결된 대상 장치와 동일한 이름으로 컴퓨터 개체를 생성합니다. 이름은 대소문자를 포함하여 정확히 일치해야 합니다.

- 4 그룹 쿼리에 사용되는 기기 이름과 대상 장치 이름은 기기에 저장됩니다. 원격 OBWI 대상 장치 이름의 Appliance Overview 화면에 지정된 기기 이름은 영문자 대소문자와 숫자 및 하이픈의 조합으로 구성되어야 하고, LDAP 서버의 개체 이름과 일치해야 합니다.
- 5 그룹 컨테이너 OU(organizational unit) 아래에 하나 이상의 그룹을 작성하십시오.
- 6 사용자 이름과 대상 장치 및 기기 개체를 4단계에서 작성한 그룹에 추가하십시오.
- 7 액세스 제어 특성을 구현하는데 사용되는 특성의 값을 지정하십시오.

구성 설정 검색

LDAP 연결이 성공하려면 네 가지 설정이 필요합니다. 검색 DN(Search DN), 검색 암호(Search Password), 검색 기본(Search Base) 및 UID 마스크(UID Mask)입니다.

DN 검색

Search DN은 대상 장치가 디렉토리 서비스에 로그인하는 데 사용하는 관리자 수준 사용자를 정의합니다. 일단 기기가 인증되면 디렉토리 서비스에서는 LDAP 쿼리 페이지에 지정된 사용자 인증 쿼리를 수행하기 위해 디렉토리에 대한 액세스를 기기에 부여합니다. 각각의 검색 값은 쉼표(,)로 구분해야 합니다. 일반적인 항목 형식은 다음과 같습니다.

```
cn=Administrator,cn=Users,dc=MyDomainName,dc=com
```

검색 암호

검색 암호는 검색 옵션에 암호가 필요한 경우 사용됩니다. 이것은 Search DN 필드에 지정된 관리자 또는 사용자를 인증합니다. 인쇄 가능한 모든 ASCII 문자가 허용됩니다.

검색 기준

Search Base는 LDAP 검색이 시작되는 시작점을 정의합니다. 기본값은 dc=yourDomainName 및 dc=com입니다. 각각의 검색 구성 요소는 쉼표

(,)로 구분해야 합니다. 예를 들어, test.com에 대해 검색 기준을 정의하려면 값은 dc=test, dc=com입니다.

UID 마스크

UID Mask에서는 LDAP 대상 장치의 사용자 ID 검색을 위한 검색 기준을 지정합니다. 형식은 <name>=<%1>입니다. 기본값은 sAMAccountName=%1이며 Microsoft Active Directory 서비스 기본값에 대응합니다.

쿼리 모드 선택 설정

기기 및 대상 장치에 대한 쿼리 모드 매개변수를 구성합니다. 기기는 콘솔 스위치에 액세스하려는 사용자와 관리자를 인증하는 데 사용됩니다. 대상 장치는 연결된 대상 장치에 액세스하려는 사용자를 인증하는 데 사용됩니다.

세 가지 쿼리 모드를 사용할 수 있으며, 기본, 사용자 속성 및 그룹 속성입니다.

기본 작동

사용자에 대한 사용자 이름 및 암호가 디렉토리 서비스로 전송됩니다. 사용자가 유효한 사용자로 인증되었으면 기기와 연결된 대상 장치에 액세스할 수 있습니다.

사용자 속성

사용자에 대한 사용자 이름, 암호 및 Access Control Attribute 쿼리가 디렉토리 서비스로 전송됩니다. Access Control Attribute는 Active Directory에 있는 사용자 개체에서 읽습니다. 값을 찾을 수 없으면 사용자는 기기 또는 대상 장치에 액세스할 수 없습니다.

그룹 속성

사용자 이름, 암호 및 그룹 쿼리가 Query Mode(기기) 사용 시에는 기기 및 연결된 대상 장치의 디렉토리 서비스로, Query Mode(대상 장치) 사용 시에는 선택한 대상 장치의 디렉토리 서비스로 전송됩니다. 사용자 이름과 기기 이름을 포함하고 있는 그룹이 발견되면 Query Mode (Appliance)를 사용할 경우 사용자에게 기기 또는 및 연결된 대상 장치

에 대한 액세스 권한이 지정됩니다. 사용자 및 대상 장치 ID를 포함하고 있는 그룹이 발견되면 **Query Mode**(대상 장치)를 사용할 경우 사용자에게 선택한 대상 장치에 대한 액세스 권한이 지정됩니다.



참고: 선택한 쿼리 모드에 따라 이 화면의 여러 구성 항목을 적용성에 따라 활성화 또는 비활성화할 수 있습니다.

그룹 구성 매개변수

상업용으로 이용할 수 있는 몇 가지 그룹 구성 매개변수가 있습니다.

Group Container

Group Container는 관리자가 Active Directory에 그룹 개체의 위치로 만드는 OU(Organizational Unit)를 지정합니다. 그룹 개체는 사용자, 컴퓨터, 연락처 및 기타 그룹을 각각에 특정 액세스 수준을 할당하여 포함할 수 있습니다.

Group Container 마스크

그룹 컨테이너 마스크는 일반적으로 OU라고 하는 그룹 컨테이너의 개체 유형을 정의합니다. 기본값은 `ou=%1`입니다.

대상 장치 마스크

대상 장치 마스크에서는 대상 장치용 검색 필터를 정의합니다. 기본값은 `cn=%1`입니다.

액세스 제어 속성

액세스 제어 속성은 쿼리 모드가 User Attribute 또는 Group Attribute로 설정된 경우에 사용되는 특성의 이름을 지정합니다. 기본값은 **"info"**입니다.

액세스 제어 구분 기호

LDAP 표준은 명명된 단일 속성 내에 여러 특성을 세미콜론(;)을 사용하여 구분함을 지정합니다. 정상적인 상황에서는 이것을 변경할 필요가 없습니다. 예를 들어, LDAP Directory에 건식 지움(dry-erase-board) 마커 개체가 있고, 이 마커가 가질 수 있는 색상을 식별하는 데 "Color" 속성을 사용한다고 가정합니다.

Color: red;blue;green;black;purple

"Color"는 속성의 이름이고 나머지는 속성의 값(이 경우에는 복합 값)을 나타냅니다. 복합 값을 사용할 경우, 세미콜론이 한 구성요소의 끝과 다음 구성요소의 시작을 표시하는 데 사용된 구분 기호입니다.

드문 경우이지만, LDAP 관리자가 세미콜론을 값 자체의 부분으로 해야 할 수 있습니다. 이러한 경우 구분 기호 문자는 다른 것으로 변경되어야 합니다. 그럴 경우, 이 필드를 사용하여 액세스 제어 속성을 나누는 방식을 식별할 모든 문자를 지정하십시오(하나 이상의 문자가 필요하며, 더 많이 수락할 수 있음). 예를 들어, 구분 기호 필드가 #\$\$;(세 개의 문자)로 설정됩니다.

Color: red#blue\$green;black#purple

이러한 구분 기호는 위의 첫 번째 예와 동일한 다섯 개 값 구성요소를 찾습니다. LDAP 관리자는 정의된 액세스 제어 구분 기호 문자가 구분 기호의 목적이 아닌 다른 목적으로 다른 곳에 있는 속성에 대한 값으로 나타나지 않음을 확인해야 합니다.

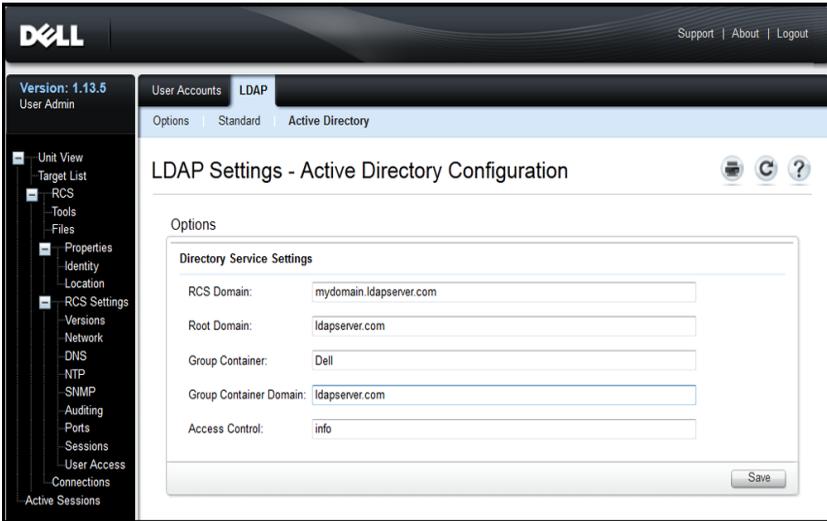
위에서 처럼, 액세스 제어 속성(ACA)은 이름과 값의 조합으로 구성됩니다. 기본적으로 사용자 및 대상 장치와 일치하는 LDAP 디렉토리 항목을 검색하여, 'info'라는 속성을 찾습니다. 이러한 속성을 찾았을 때 이들 속성의 값은 해당 장치에 대한 사용자의 인증 수준을 알려줍니다. LDAP 서비스 관리자가 info가 아닌 다른 속성을 사용하려고 할 경우에는 위에 표시된 필드를 사용하여 속성을 사용자 정의할 수 있습니다.

사용자는 여러 그룹의 구성원일 수 있고 각 그룹은 장치마다 다른 인증 수준을 가질 수 있으므로, 실행 기록이 결과로 유지됩니다. LDAP 표준에 의거하여 보고된 최종 인증 수준은 정밀 조사에서 특정 사용자 및 장치에 대해 발견된 모든 긍정적 결과 중에서 가장 높은(가장 많이 허용되는) 수준입니다.

보조 LDAP 설정 - Active Directory 구성

이 섹션에서 설정은 그림 5.6에 나타난 OBWI 창을 통해 User Access / LDAP / Active Directory 탭에서 액세스할 수 있습니다.

그림 5.6. 보조 LDAP 설정 - Active Directory 구성



Dell 확장 스키마를 설치하려면 사용할 RCS 및 루트 도메인만 입력합니다.

Dell 확장 스키마를 사용하지 않을 경우에는 설치 시 RCS 및 액세스 제어된 SIP가 Active Directory 내에 컴퓨터 개체로 구성됩니다. 이렇게 하려면 먼저 액세스 제어된 RCS 및 연결된 SIP에 사용자를 연관시키는 그룹 개체를 저장할 조직 구성 단위를 구성해야 합니다. 이전에 생성된 OU 또는 해당 목적으로 새로 만든 OU를 사용할 수 있으며, 이때 Group Container 도메인의 모든 OU 개체에 대해 고유해야 합니다.

다음으로 임의의 액세스 제어 정보를 포함하는 데 사용될 LDAP 디렉토리 내 속성을 선택합니다. 이 속성은 문자열 값을 저장할 수 있는 이전에 사용되지 않은 속성이어야 합니다 (기본값은 그룹 개체의 "info" 속성임).

마지막으로, OBWI 창의 공백에 Group Container, Group Container Domain 및 Access Control Attribute 위치를 입력해야 합니다.

그림 5.6에 나와있는 필드에 대한 자세한 설명은 표 5.2를 참조하십시오.

표 5.2: Active Directory 구성 필드 설명

필드	설명
RCS Domain	RCS Domain 필드에는 RCS 및 SIP를 나타내는 모든 개체를 저장하기 위해 선택된 Active Directory 도메인 이름이 포함됩니다.
Root Domain	Active Directory 포리스트 내 최상위 도메인입니다.
Group Container (표준 스키마 집합 전용)	<p>이 필드는 표준 스키마를 선택한 경우에 사용할 수 있으며 Active Directory의 조직 구성 단위 (OU) 개체의 고유 이름 일부를 포함합니다. OU는 사용자를 액세스 제어된 Remote Console Switch 및 스위치에 연결된 SIP에 연관시키는 그룹 개체를 저장하는 데 사용됩니다.</p> <p>예를 들어 선택한 OU의 고유 이름이 ou=KVM-AccessControls, dc=MyCom,dc=com이라고 가정하면 Group Container 필드는 "KVM-AccessControls"로 구성되어야 합니다. Group Container 필드에 입력된 이름은 Group Container 도메인의 모든 OU 개체에서 고유해야 합니다. Group Container용으로 전에 생성된 OU를 사용하도록 선택하거나 이 용도로 사용할 OU를 새로 만들 수 있습니다.</p> <p>기본 Group Container는 KVM입니다.</p>
Group Container Domain (표준 스키마 집합 전용)	이 필드는 표준 스키마를 선택한 경우에 사용할 수 있으며 Group Container가 상주하는 Active Directory 도메인의 DNS 이름입니다.

필드	설명
Access Control Attribute (표준 스키마 집합 전용)	<p>이 필드의 값은 임의의 액세스 제어 정보를 포함하기 위해 LDAP 디렉토리의 어떤 속성을 사용할 것인지 지정하며 표준 스키마를 선택한 경우에만 활성화됩니다.</p> <p>Access Control Attribute는 구성원에 사용자, RCS 및 사용자가 액세스를 시도 중인 연결된 컴퓨터를 포함하고 있는 그룹을 나타내는 LDAP 디렉토리 개체의 속성들 중에서 선택됩니다.</p> <p>표준 스키마를 사용할 경우 Group Container의 그룹 개체가 해당 그룹과 관련된 권한 수준을 포함하도록 선택된 속성을 갖도록 해야 합니다. Access Control Attribute 필드는 표준 스키마를 선택한 경우에 사용할 수 있으며 선택한 속성의 이름이 포함됩니다. 선택된 속성은 문자열 값을 저장할 수 있어야 합니다. 예를 들어 기본 속성은 "info"로서 Active Directory 사용자 및 컴퓨터 (ADUC) 스냅인을 통해 액세스할 수 있는 속성입니다. "info" 속성 값은 그룹 개체의 "Notes" 속성에 액세스하여 설정되며 이 때 ADUC를 사용합니다.</p>

LDAP SSL 인증서

(RCS와 Active Directory 서버 간) 모든 LDAP 프로토콜 교환은 SSL에 의해 보호됩니다. LDAP 프로토콜이 SSL에 의해 보호될 경우 LDAPS (Lightweight Directory Access Protocol over SSL)라고 합니다. 각 LDAPS 연결은 관련 Active Directory 서버에서 RCS로 보안 인증서 전송을 지시하는 프로토콜 핸드셰이크를 통해 시작됩니다. 수신된 후에는 RCS가 인증서를 확인합니다. 인증서를 확인하려면 RCS에 루트 인증 기관 (CA) 인증서 사본이 구성되어 있어야 합니다. 이를 수행하려면 먼저 인증서를 작성해야 합니다.

도메인 컨트롤러에서 SSL 활성화

Microsoft 엔터프라이즈 루트 CA를 사용하여 사용자의 모든 도메인 컨트롤러에 SSL 인증서를 자동으로 할당하려면 이전에 SSL을 활성화하

지 않은 경우 다음 단계에 따라 각 도메인 컨트롤러에서 SSL을 활성화해야 합니다.

- 1 도메인 컨트롤러에서 Microsoft Enterprise Root CA를 설치합니다.
 - a. 시작 - 제어판 - 프로그램 추가/제거를 선택합니다.
 - b. Windows 구성 요소 추가/제거를 선택합니다.
 - c. Windows 구성 요소 마법사에서 인증서 서비스 확인란을 선택합니다.
 - d. CA 종류로 엔터프라이즈 루트 CA를 선택한 후 다음을 클릭합니다.
 - e. 이 CA의 일반 이름을 입력하고 다음을 클릭한 후 마침을 클릭합니다.
- 2 각 컨트롤러용 SSL 인증서를 설치하여 각 도메인 컨트롤러에서 SSL을 활성화합니다.
 - a. 시작 - 관리 도구 - 도메인 보안 정책을 클릭합니다.
 - b. 공개 키 정책 폴더를 확장한 뒤 자동 인증서 요청 설정을 마우스 오른쪽 단추로 클릭한 후 자동 인증서 요청을 클릭합니다.
 - c. 자동 인증서 요청 설치 마법사에서 다음을 클릭하고 도메인 컨트롤러를 선택합니다.
- 3 다음을 클릭한 후 마침을 클릭합니다.

인증서/개인 키 파일은 Linux를 사용하는 openssl을 사용해서 생성할 수 있습니다. Openssl은 openssl.org에서 다운로드할 수 있습니다. 아래 <> 안의 텍스트에 있는 지침은 사용자가 해당 줄의 끝에 있는 기준에 따라 값을 설정하는데 필요한 내용입니다.

 **참고:** 아래 <anglebrackets> 안의 텍스트에 있는 지침은 사용자가 해당 줄의 끝에 있는 기준에 따라 값을 설정하는데 필요한 내용입니다.

가져오기할 인증서를 생성하려면:

- 1 Linux 명령 프롬프트에 openssl을 입력하고 <Enter> 키를 누릅니다. 사용자에게 OpenSSL 프롬프트가 표시됩니다.

```
OpenSSL> genrsa -out privatekey.pem <512>
```

RSA 개인키, 512 비트 길이 로그 계수 생성

```
.....+++++
```

```
.....+++++
```

e는 65537(0x10001)입니다.

```
OpenSSL req -new -key privatekey.pem -x509 -out certificate.pem-batch  
-days <365>
```

- 2 고유 이름 (DN: Distinguished Name)으로 인증서 요청에 포함될 정보를 입력합니다. 일부 필드는 기본값이 있을 수 있습니다. 원하는 경우 '!'을 입력하여 필드를 공백으로 둘 수 있습니다.

Country Name(2 문자 코드) [GB]:<US>

State 또는 Province Name(전체 이름) [Berkshire]:<Texas>

Locality Name(예, 도시) [Newbury]:<Austin>

Organization Name(예, 회사) [My Company Ltd]:<Dell, Inc.>

Organizational Unit Name(예, 부분) []:<Round Rock>

Common Name(예, 사용자 이름 또는 서버 호스트 이름)
[]:<RCS

DNS Name 또는 IP>

Email Address []:<support@dell.com>

```
OpenSSL> quit
```

- 3 Linux 명령 프롬프트에 `cat certificate.pem privatekey.pem > webserver.pem`을 입력한 다음, `unix2dos webserver.pem`을 입력하여 파일을 UNIX 줄바꿈에서 DOS 캐리지 리턴/줄바꿈으로 변환합니다.

CA 인증서를 내보내려면:

- 1 Windows 운영 체제에서 Certificate Authority 관리 도구를 열려면 시작 - 모든 프로그램 - 관리 도구 - 인증서 기관을 클릭합니다.

- 2 트리 보기에서 인증 기관을 마우스 오른쪽 단추로 클릭한 뒤 속성을 선택하면 인증 기관의 속성을 볼 수 있습니다. CA 속성 대화 상자가 열립니다.
- 3 일반 탭을 클릭한 뒤 인증서 보기 버튼을 클릭하여 인증서 대화 상자를 엽니다.
- 4 자세히 탭을 클릭한 뒤 파일에 복사 버튼을 클릭합니다. 인증서 내보내기 마법사가 열립니다.
- 5 다음을 클릭하여 마법사를 시작합니다.
- 6 파일 내보내기 형식 화면에서 base 64로 인코딩된 X.509(.CER) 라디오 버튼을 선택한 뒤 다음 버튼을 누릅니다.
- 7 내보낼 파일 화면에서 내보낸 인증서의 파일 이름 및 경로를 입력하거나 찾습니다. 다음 버튼을 누릅니다.
- 8 마침 버튼을 누릅니다.

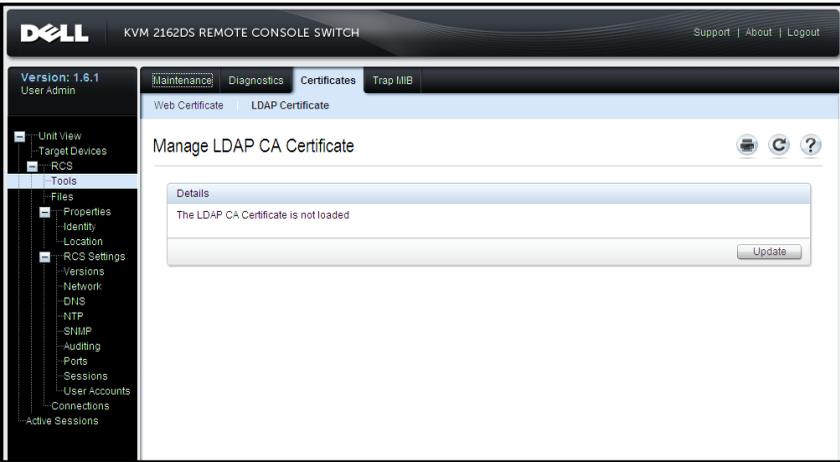
내보낸 인증서 파일의 형식이 올바르게 지정되고 OpenSSL에서 읽을 수 있습니다.

일반적으로 CA 인증서는 한 번만 업로드하면 되지만, 인증이 취소된 경우나 인증서 사용 기한이 만료되어 해지된 경우 또는 직렬 콘솔 메뉴에서 "Restore Factory Defaults"를 선택한 경우에는 다시 업로드해야 합니다.

 **참고:** 위의 지침은 Microsoft CA 인증서용으로 작성되었습니다. 다른 CA의 경우에는 CA 공급업체에 확인하십시오.

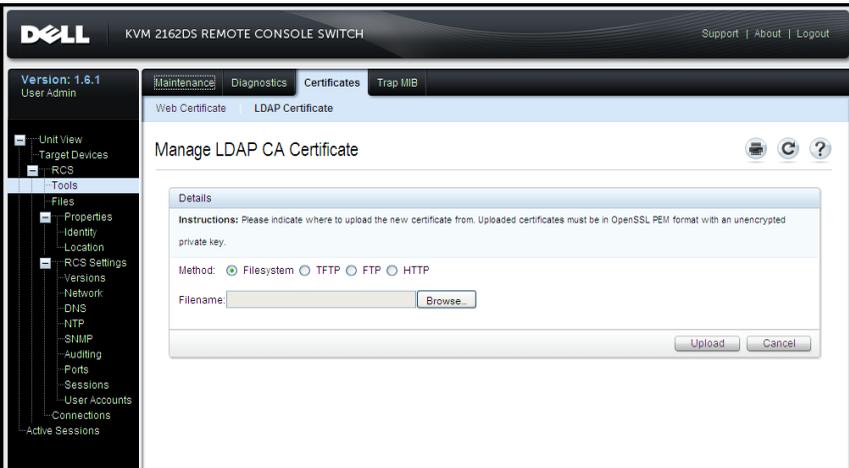
 **참고:** LDAPS가 작동하려면 네트워크 시간 프로토콜(NTP)을 활성화해야 합니다.

그림 5.7. OBWI - LDAP 인증서



업데이트를 클릭하면 다음 창이 표시됩니다.

그림 5.8. OBWI - LDAP 인증서 업데이트



인증서를 찾아서 열 수 있습니다. 인증서가 열리고 내용이 표시되면 사용자는 인증서를 RCS로 전송할 수 있습니다.

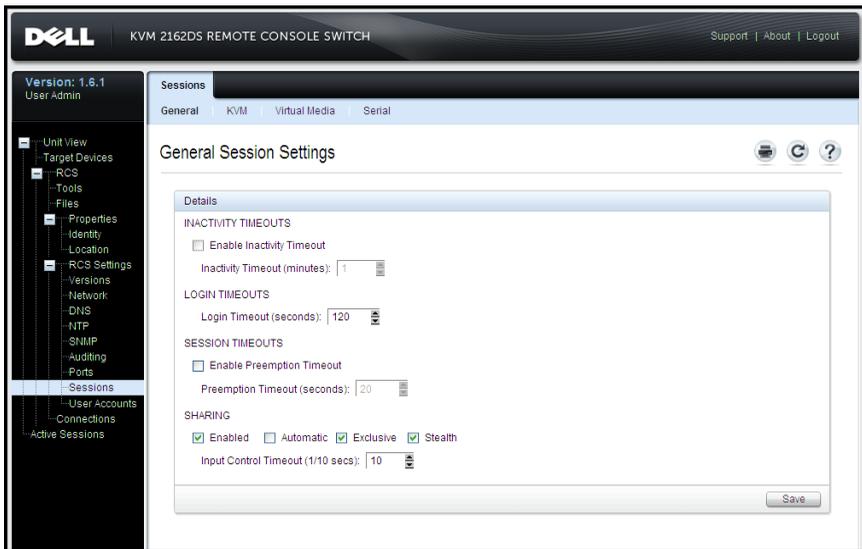
로그인 제한 시간

많은 양의 디렉토리 트리로 인해 LDAP 인증이 느리게 수행될 경우 세션 창에 기본 제한 시간 30초의 로그인 제한 시간 기능이 포함됩니다. 로그인 제한 시간은 사용자가 Login 대화 상자에서 **OK** 버튼을 누른 이후부터 장치의 응답이 없을 때까지의 시간입니다. RCS에서도 이 값을 사용해 LDAP 인증 요청 제한 시간을 결정합니다.

온보드 웹 인터페이스에서 로그인 제한 시간을 지정하려면:

- 1 Sessions를 클릭하여 General Session Settings 화면을 엽니다.
- 2 Login Timeout 메뉴에서 시간(초 단위)을 지정합니다.
- 3 Save를 클릭합니다.

그림 5.9. OBWI - 로그인 제한 시간



참고: Login Timeout(로그인 시간 초과)은 User Login Caching(사용자 로그인 캐싱)기능과 다릅니다. 후자는 일정 기간 동안의 인증 결과를 캐시하여 로그인이 완료된 후 작동하여, 반복된 LDAP 통신 요청을 제거합니다.

CA 인증서 정보 표시

공개 키 길이가 2048 비트보다 작거나 같으면 RCS는 해당 창에 전체 CA 인증서 정보를 표시할 수 있습니다. 키가 2048 비트보다 크면 해당 창에서 제목, 발행인 및 유효 기간 데이터가 표시되지 않습니다.¹

다음은 CA 인증서 정보가 표시되는 예입니다.

- 1 클라이언트에서 CA 인증서를 RCS로 다운로드합니다.
- 2 직렬 콘솔 주 메뉴에서 **옵션 8**을 입력하여 LDAP CA 인증서를 표시합니다.

RCS에 다음과 같은 정보 유형이 표시됩니다.

```
Begin CA certificate information display
subject = /DC=msft/DC=ldaptest/CN=MyCertificate
issuer = /DC=msft/DC=ldaptest/CN=MyCertificate
notBefore=Dec 7 20:09:56 2005 GMT
notAfter=Dec 7 20:18:34 2010 GMT
serial=7BA146C0221A08B447B989292074329F
MD5 Fingerprint =
CB:6D:70:30:31:E5:1B:C0:90:BB:DB:32:B2:C9:D1:5A
End CA certificate information display
```

RCS 소프트웨어를 Microsoft Windows Server 2003 플랫폼에 설치하려면 다음 단계를 수행하십시오.

- 1 시작 메뉴를 선택합니다.
- 2 내 컴퓨터를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
- 3 고급 탭을 선택합니다.
- 4 성능 설정 버튼을 클릭합니다.
- 5 데이터 실행 방지 (DEP) 탭을 선택합니다.

- 6 데이터 실행 방지 (DEP)를 필수적인 Windows 프로그램 및 서비스에만 사용 라디오 버튼을 선택합니다.
- 7 OK를 클릭합니다.
- 8 시스템 속성 대화 상자에서 **확인**을 다시 클릭합니다.

그룹 개체 구성

사용자를 Group Container의 그룹 구성원에 포함시킴으로써 특정 Active Directory 사용자 계정에 대해 액세스 제어가 적용됩니다. 이 때 그룹 구성원이 사용자의 액세스가 허용된 RCS 및 SIP를 나타내는 개체도 포함하고 있어야 합니다. 허용된 액세스 수준은 그룹 개체(표준 스키마) 또는 연결 개체(확장 스키마)의 특정 속성 값에 의해 결정되며, 세 가지의 사용 권한 수준이 있습니다. 액세스 수준은 오름차순으로 KVM User, KVM User Admin 그리고 가장 높은 수준인 KVM Appliance Admin입니다.

 **참고:** 두 관리자 권한은 모두 기본적으로 모든 SIP에 액세스할 수 있으므로 KVM User 액세스 수준을 사용하지만 않는다면 SIP 개체를 따로 구성할 필요가 없습니다.

표 5.3: 액세스 수준별 허용된 작업

작업	KVM Appliance Admin	KVM User Admin	KVM User
선점	다른 KVM Appliance Admin 또는 KVM User Admin에 우선합니다. 디렉토리의 적절한 그룹 개체에 TD를 포함시켜 대상 장치별로 사용 권한을 구성해야 합니다.	다른 User Admin에 우선합니다. 디렉토리의 적절한 그룹 개체에 대상 장치별 권한을 구성해야 합니다.	아니오

작업	KVM Appliance Admin	KVM User Admin	KVM User
네트워크 매개변수 및 글로벌 설정 구성	예 - 디렉토리의 적절한 그룹 개체에 RCS를 포함시켜 RCS별로 사용 권한을 구성해야 합니다.	아니오	아니오
다시 시작	예 - 디렉토리의 적절한 그룹 개체에 RCS를 포함시켜 RCS별로 사용 권한을 구성해야 합니다.	아니오	아니오
FLASH 업그레이드	예 - 디렉토리의 적절한 그룹 개체에 RCS를 포함시켜 RCS별로 사용 권한을 구성해야 합니다.	아니오	아니오
Administrator 사용자 계정	예 - 디렉토리의 적절한 그룹 개체에 RCS를 포함시켜 RCS별로 사용 권한을 구성해야 합니다.	예 - 디렉토리의 적절한 그룹 개체에 RCS를 포함시켜 RCS별로 사용 권한을 구성해야 합니다.	아니오
포트 설정 구성	예 - 디렉토리의 적절한 그룹 개체에 RCS를 포함시켜 RCS별로 사용 권한을 구성해야 합니다.	아니오	아니오

작업	KVM Appliance Admin	KVM User Admin	KVM User
대상 장치 액세스	예 - 디렉토리의 적절한 그룹 개체에 RCS를 포함시켜 RCS별로 사용 권한을 구성해야 합니다.	예 - 디렉토리의 적절한 그룹 개체에 RCS를 포함시켜 RCS별로 사용 권한을 구성해야 합니다.	예(관리자가 구현한 경우) 디렉토리의 적절한 그룹 개체에 TD를 포함시켜 대상 장치별로 사용 권한을 구성해야 합니다.

해당 계정의 Authentication Panel 필드의 수정이 허용되기 전에 RCS 관리자 (KVM Appliance Admin) 사용 권한을 받으려면 AD 사용자 계정을 구성해야 합니다. 특히 인증 설정은 RCS 관리자만 수정할 수 있습니다.

표준 스키마용 Active Directory 개체 개요

인증 및 승인을 위해 Active Directory와 통합하려는 네트워크의 실제 RCS의 경우 스위치별로 이를 나타낼 컴퓨터 개체를 하나 이상 만들어야 합니다. 또한 KVM User 권한 수준을 이용해 제어할 RCS에 연결된 각각의 SIP에 대해 컴퓨터 개체도 만들어야 합니다. SIP를 나타내는 컴퓨터 개체는 관리자 수준 그룹에는 필요하지 않습니다. KVM User 그룹의 사용자는 KVM User 그룹에 있는 SIP에만 액세스할 수 있습니다. 관리자 권한을 갖고 있는 사용자는 기본적으로 모든 SIP에 액세스할 수 있습니다.

RCS에 대한 그룹 개체를 설정하려면:

- 1 아직 만들지 않았다면 스위치 설치와 관련된 그룹 개체가 포함된 조직 구성 단위를 만듭니다.
- 2 이 조직 구성 단위에서 사용자 권한 수준을 나타내는 그룹 개체 3개를 만듭니다. KVM Appliance Administrators, KVM User Administrators 그리고 KVM Users용 개체를 한 개씩 만듭니다.
- 3 MSADUC 도구를 사용해 KVM Appliance Administrator 그룹 개체를 열어 Notes 속성을 선택합니다. Notes 필드에 해당 그룹의 액세스

수준 ("KVM Appliance Admin")을 입력한 뒤 저장합니다. 다른 2개의 그룹 개체에 대해서도 해당 이름을 사용하여 이 절차를 반복합니다.



참고: 모든 액세스 제어 속성 값을 위한 단일 구문은 다음과 같습니다.

```
"[<arbitrary text string> <delimiter>] < privilege level>
[<delimiter> <arbitrary text string>]"
```

여기에서: <privilege level> := "KVM User" 또는 "KVM User Admin" 또는 "KVM Appliance Admin"

<구분 기호> ::= 다음 중 한 가지 이상: <newline> 또는 <c/r> 또는 <comma> 또는 <semicolon> 또는 <tab>

<arbitrary text string>은 영숫자 문자열로서 널(비어 있음) 문자열일 수 있습니다.

대괄호는 옵션 항목을 나타냅니다. 예를 들어 다음 서식은 옵션 문자열 및 구분 기호 뒤에 필수 권한 수준이 따라 옵니다: "[<arbitrary text string> <delimiter>] < privilege level>"

- 4 RCS를 나타내는 컴퓨터 개체를 만듭니다.
- 5 KVM User 권한 수준에서 액세스가 제한될 서버에 연결된 각각의 SIP에 대해 컴퓨터 개체를 만듭니다.
- 6 적절한 그룹 개체에 스위치를 나타내는 컴퓨터 개체를 추가합니다.
- 7 액세스 수준에 맞는 적절한 그룹 개체에 사용자 개체를 추가합니다.
- 8 액세스 제어된 SIP용 컴퓨터 개체를 KVM User 그룹에 추가합니다.

Dell Extended Schema Active Directory 개체 개요

인증 및 승인을 위해 Active Directory와 통합하려는 네트워크 상의 실제 RCS의 경우 스위치별로 이를 나타낼 최소 한 개의 RCS 장치 개체, 한 개의 연결 개체를 만들어야 합니다. 연결 개체는 특정 권한 집합을 보유한 사용자 또는 그룹을 한 개 이상의 SIP에 연결하는 데 사용됩니다. 이 모델은 복잡성을 심화시키지 않으면서 사용자, RCS 권한 및

Remote Console Switch의 SIP를 다양하게 조합할 수 있어 관리자에게 최대한의 유연성을 제공합니다.

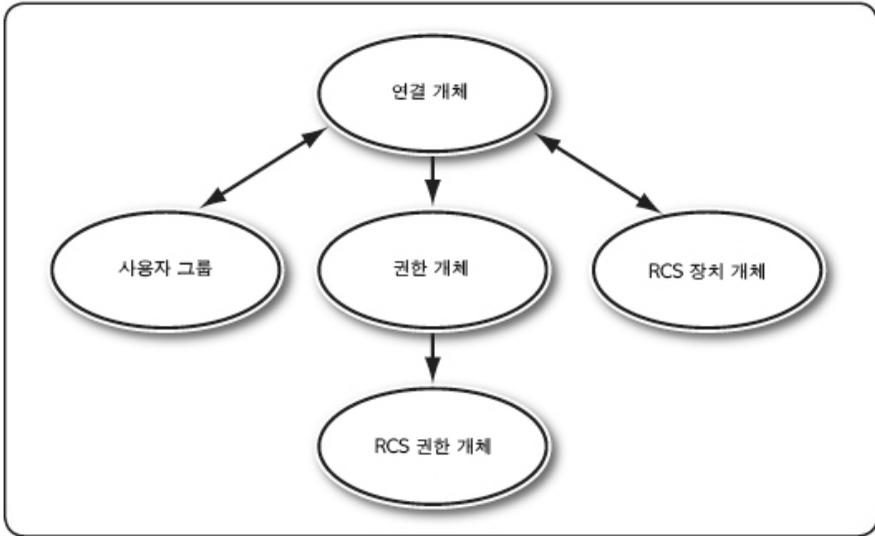
RCS 장치 개체는 Active Directory에 인증 및 승인을 쿼리하기 위한 RCS 링크입니다. 네트워크에 RCS 추가되면 사용자가 Active Directory에서 인증 및 승인을 수행할 수 있도록 관리자가 Active Directory 이름으로 RCS 및 RCS의 장치 개체를 구성해야 합니다. 또한 사용자가 인증을 받으려면 관리자는 하나 이상의 연결 개체에 Remote Console Switch를 추가해야 합니다.

사용자는 원하는 만큼 연결 개체를 만들 수 있으며 각 연결 개체는 필요한 만큼의 사용자, 사용자 그룹 또는 RCS 장치 개체에 연결될 수 있습니다. 사용자 및 RCS 장치 개체는 기업의 도메인 구성원일 수 있습니다.

하지만 각각의 연결 개체는 단 한 개의 권한 개체에만 연결될 수 있습니다 (또는 사용자, 사용자 그룹 또는 RCS 장치 개체를 연결). 권한 개체를 통해 관리자는 특정 SIP에서 어떤 사용자가 어떤 종류의 권한을 갖는지 제어할 수 있습니다.

다음 그림은 연결 개체가 모든 인증 및 승인을 위해 필요한 연결을 제공함을 보여 줍니다.

그림 5.10. Active Directory 개체의 일반적인 설정

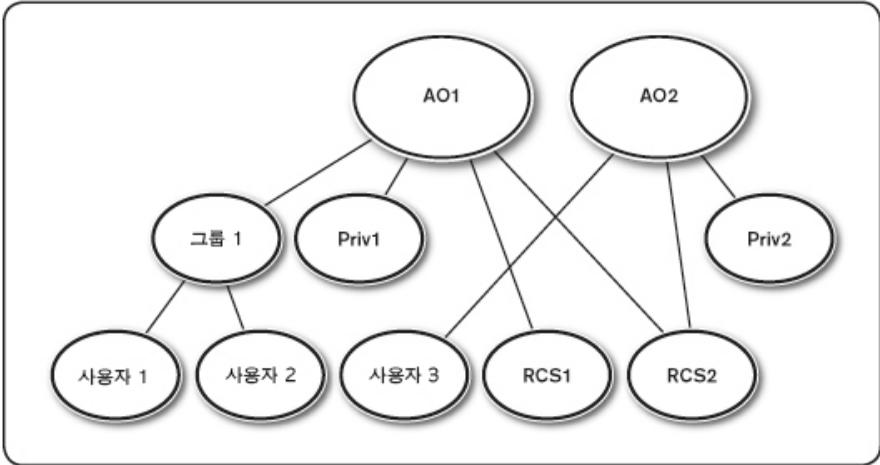


사용자는 자신이 원하거나 필요로 하는 만큼의 연결 개체를 만들 수 있습니다. 하지만 하나 이상의 연결 개체를 만들어야 하며 RCS 인증 및 승인을 위해 Active Directory와 통합하려는 네트워크의 각 RCS에 대해 하나의 RCS 장치 개체를 가지고 있어야 합니다. 연결 개체를 통해 RCS 장치 개체뿐 아니라 사용자 및/또는 그룹을 원하는 만큼 만들 수 있지만 연결 개체는 연결 개체 당 단 하나의 권한 개체만 갖습니다. 연결 개체는 RCS에 대한 "권한"을 갖는 "사용자"를 연결합니다.

또한 사용자는 Active Directory 개체를 단일 도메인 또는 복수 도메인에 설치할 수 있습니다. 예를 들어, 2개의 RCS(RCS1 및 RCS2) 및 3개의 기존 Active Directory 사용자(사용자1, 사용자2 및 사용자3)를 갖고 있다고 가정해 보면, 사용자1 및 사용자2에게는 2개의 RCS 모두에 대한 관리자 권한을 주고, 사용자3에게는 RCS2에 대한 로그인 권한을 주고자 합니다.

다음 그림은 이 시나리오에서 Active Directory 개체를 설치하는 방법을 설명합니다.

그림 5.11. 단일 도메인에 Active Directory 개체 설정



단일 도메인 시나리오를 위해 개체를 설정하려면 다음 작업을 수행하십시오.

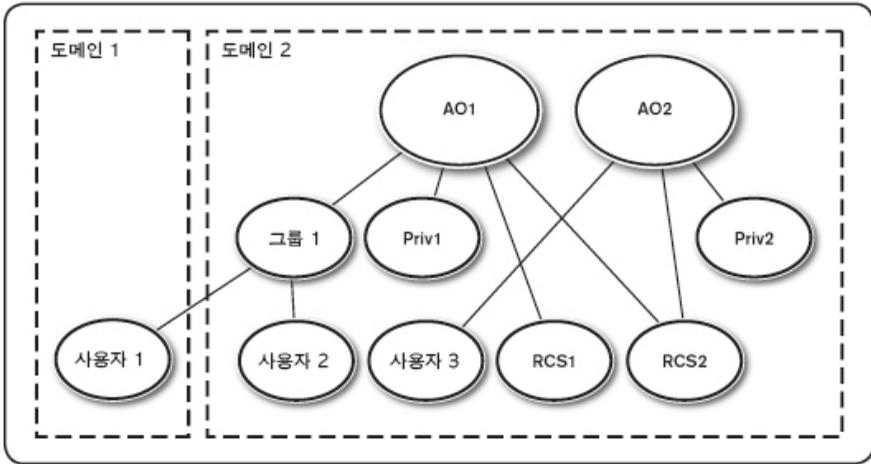
- 1 2개의 연결 개체를 만듭니다.
- 2 2개의 RCS 장치 개체인 RCS1 및 RCS2를 생성합니다.
- 3 권한1은 모든 권한(관리자)을 갖고 권한2는 로그인 권한을 갖도록 2개의 권한 개체 권한1과 권한2를 만듭니다.
- 4 User1 및 User2를 Group1로 묶습니다.
- 5 그룹1을 연결 개체 1(AO1)의 구성원으로, 권한1을 AO1의 권한 개체로 그리고 RCS1 및 RCS2를 AO1의 RCS 장치로 추가합니다.
- 6 사용자3을 연결 개체 2(AO2)의 구성원으로, 권한2를 AO2의 권한 개체로 그리고 RCS2를 AO2의 RCS 장치로 추가합니다.

자세한 내용은 "Dell 스키마 확장을 통해 Active Directory에 RCS 사용자 및 권한 추가"를 참조하십시오.

다음 그림은 다중 도메인의 Active Directory 개체 설정 방법을 나타냅니다. 이 시나리오에서는 2개의 RCS(RCS1 및 RCS2) 및 3개의 기존 Active Directory 사용자(사용자1, 사용자2 및 사용자3)를 갖고 있습니다.

사용자1은 도메인1에 그리고 사용자2와 사용자3은 도메인2에 있습니다. 사용자1 및 사용자2에게는 2개의 RCS 모두에 대한 관리자 권한을 주고, 사용자3에게는 RCS2에 대한 로그인 권한을 주고자 합니다.

그림 5.12. 복수 도메인에 Active Directory 개체 설정



복수 도메인 시나리오에 대해 개체를 설정하려면 다음 작업을 수행하십시오.

- 1 도메인 포리스트 기능이 기본 모드 또는 Windows 2003 모드인지 확인합니다.
- 2 임의의 도메인에 두 개의 연결 개체 즉, AO1(유니버설 범위) 및 AO2를 만듭니다. 그림에서 개체는 도메인2에 있습니다.
- 3 2개의 RCS 장치 개체인 RCS1 및 RCS2를 생성합니다.

- 4 권한1은 모든 권한(관리자)을 갖고 권한2는 로그인 권한을 갖도록 2개의 권한 개체 권한1과 권한2를 만듭니다.
- 5 User1 및 User2를 Group1로 묶습니다. 그룹1의 그룹 범위는 유니버설이어야 합니다.
- 6 그룹1을 연결 개체 1(AO1)의 구성원으로, 권한1을 AO1의 권한 개체로 그리고 RCS1 및 RCS2를 AO1의 RCS 장치로 추가합니다.
- 7 사용자3을 연결 개체 2(AO2)의 구성원으로, 권한2를 AO2의 권한 개체로 그리고 RCS2를 AO2의 RCS 장치로 추가합니다.

사용자의 RCS에 액세스하기 위해 Dell 스키마 확장을 이용해 Active Directory 구성

Active Directory를 사용해 사용자의 RCS에 액세스하려면 먼저 다음 단계를 순서대로 수행하여 Active Directory 소프트웨어와 Remote Console Switch를 구성해야 합니다.

- 1 Active Directory 스키마를 확장합니다.
- 2 Active Directory 사용자 및 컴퓨터 스냅인을 확장합니다.
- 3 RCS 사용자 및 해당 권한을 Active Directory에 추가합니다.

Active Directory 스키마 확장(옵션)

Active Directory 스키마를 확장하면 Dell 조직 구성 단위, 스키마 클래스 및 속성 그리고 예제 권한 및 연결 개체가 Active Directory 스키마에 추가됩니다.

 **참고:** 스키마를 확장하기 전에 도메인 포리스트의 스키마 마스터 FSMO (Flexible Single Master Operation) 역할 소유자에 대한 스키마 관리 권한을 가져야 합니다.

두 가지 서로 다른 방법으로 사용자의 스키마를 확장할 수 있습니다. Dell Schema Extender 유틸리티 또는 LDIF 스크립트 파일을 사용할 수 있습니다.



참고: LDIF 스크립트 파일을 사용하면 Dell 조직 구성 단위는 추가되지 않습니다.

LDIF 파일 및 Dell Schema Extender는 dell.com/support에서 얻을 수 있습니다.

LDIF 파일을 사용하려면 LDIF 파일 디렉토리에 있는 readme의 지침을 참조하십시오. Dell Schema Extender를 사용하여 Active Directory 스키마를 확장하려면 "Dell Schema Extender 사용"에서 해당 단계를 수행하십시오.

Schema Extender 또는 LDIF 파일은 어떤 위치에서든 복사해 실행할 수 있습니다.

Dell Schema Extender 사용



참고: Dell Schema Extender는 SchemaExtenderOem.ini 파일을 사용합니다. Dell Schema Extender 유틸리티가 제대로 작동하도록 하려면 이 파일의 이름을 수정하지 마십시오.

- 1 Welcome 화면에서 **Next**를 클릭합니다.
- 2 경고 내용을 읽은 뒤 다시 **Next**를 클릭합니다.
- 3 Use Current Log In Credentials를 선택하거나 스키마 관리자 권한이 있는 사용자 이름 및 비밀번호를 입력합니다.
- 4 **Next**를 클릭해 Dell Schema Extender를 실행합니다.
- 5 **Finish**를 클릭합니다.

Active Directory 사용자 및 컴퓨터 스냅인에 Dell Extension 설치(옵션)

Active Directory에서 스키마를 확장하려면 관리자가 RCS 장치, 사용자 및 사용자 그룹, RCS 연결 및 SIP 권한을 관리할 수 있도록 Active Directory 사용자 및 컴퓨터 스냅인도 확장해야 합니다. Active Directory 사용자 및 컴퓨터 스냅인에 대한 Dell Extension은 Dell 시스템 관리 콘솔 CD를 사용해 시스템 관리 소프트웨어를 설치할 때 설치할 수 있는 옵션 사항입니다. 시스템 관리 소프트웨어 설치에 대한 추가 지침

은 Dell OpenManage 소프트웨어 빠른 설치 설명서 (Dell OpenManage Software Quick Installation Guide)를 참조하십시오.



참고: Active Directory RCS 개체를 관리하는 각 시스템에 관리자 팩을 설치해야 합니다. 설치 방법은 다음 절인 "Active Directory 사용자 및 컴퓨터 스냅인 열기"에서 설명합니다. 관리자 팩을 설치하지 않으면 컨테이너의 Dell SIP 개체를 볼 수 없습니다.



참고: Active Directory 사용자 및 컴퓨터 스냅인에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

Active Directory 사용자 및 컴퓨터 스냅인 열기

Active Directory 사용자 및 컴퓨터 스냅인을 열려면 다음 단계를 수행하십시오.

도메인 컨트롤러에 있다면 **시작 -관리 도구 - Active Directory 사용자 및 컴퓨터**를 클릭합니다.

-또는-

도메인 컨트롤러에 있지 않다면 적절한 Microsoft 관리자 팩을 로컬 시스템에 설치해야 합니다. 이 관리자 팩을 설치하려면 **시작 - 실행**을 클릭한 다음 MMC를 입력한 후 Enter 키를 누릅니다. 그러면 MMC (Microsoft Management Console)가 열립니다.

- 1 콘솔 1 창에서 **파일** (또는 Windows 2000 시스템의 콘솔)을 클릭합니다.
- 2 **스냅인 추가/제거**를 클릭합니다.
- 3 **Active Directory 사용자 및 컴퓨터 스냅인**을 선택하고 **추가**를 클릭합니다.
- 4 **닫기**를 클릭한 후 **확인**을 클릭합니다.

Dell 스키마 확장을 통해 Active Directory에 사용자 및 권한 추가

Dell 확장 Active Directory 사용자 및 컴퓨터 스냅인을 통해 SIP, 연결 및 권한 개체를 만들어 RCS 사용자 및 권한을 추가할 수 있습니다. 각각의 개체 유형을 추가하려면 각 하위 절의 단계를 수행하십시오.

SIP 개체 만들기

- 1 MMC 콘솔 루트 창에서 컨테이너를 마우스 오른쪽 단추로 클릭합니다.
- 2 **New - Dell SIP Object**를 선택합니다. New Object 창이 열립니다.
- 3 새 개체의 이름을 입력합니다. 이 이름은 38페이지의 "Remote Console Switch 구성"의 4단계에서 입력할 RCS 이름과 일치해야 합니다.
- 4 **SIP Device Object**를 선택합니다.
- 5 **OK**를 클릭합니다.

권한 개체 만들기

권한 개체는 권한 개체가 연결되는 연결 개체와 동일한 도메인에 만들어야 합니다.

- 1 콘솔 루트(MMC) 창에서 컨테이너를 마우스 오른쪽 단추로 클릭합니다.
- 2 **New - Dell SIP Object**를 선택하여 New Object 창을 엽니다.
- 3 새 개체의 이름을 입력합니다.
- 4 **Privilege Object**를 선택합니다.
- 5 **OK**를 클릭합니다.
- 6 생성된 권한 개체를 마우스 오른쪽 버튼으로 클릭하고 **Properties**를 선택합니다.

7 RCS 권한 탭을 클릭한 다음 사용자에게 부여할 RCS 권한을 선택합니다.

Dell 연결 개체 구문 사용

Dell 연결 개체 구문을 사용하면 개체 유형이 Dell LDAP 스키마에서 사용자 및 그룹으로 기본 설정됩니다. Dell은 Dell 확장 스키마에서 네 개의 새로운 개체 클래스에 대해 고유한 개체 ID를 추가했습니다.

- KVM RCS 개체
- KVM SIP 개체
- 권한 개체
- 연결 개체

이러한 새로운 개체 클래스는 기본 Active Directory 클래스의 다양한 결합(계층)과 Dell의 고유한 속성 유형의 관점에서 정의되었습니다. Dell의 고유한 각 속성 유형은 기본 Active Directory 속성 구문의 관점에서 정의되었습니다.

사용된 기본 Microsoft Active Directory 개체 클래스에는 사용자 및 그룹이 포함됩니다. 사용자 클래스는 주로 단일 항목에 대한 정보를 포함하는 Active Directory 개체를 표시합니다. 그룹 클래스는 중첩에 사용되며 개체 수집에 대한 정보를 포함하는 컨테이너를 표시합니다.

각 KVM RCS 개체는 Active Directory 내의 개별 Remote Console Switch를 나타냅니다. 이들은 단일 개체이기 때문에 LDAP 기본 언어에서 그룹 개체가 아닌 사용자 개체입니다.

각 권한 개체는 개별적으로 결합된 권한 집합을 정의합니다. 각 집합은 분리된 개체로 인식되므로 그룹 개체가 아닌 사용자 개체입니다.

연결 개체는 특정 RCS 및/또는 특정 SIP와 관련하여 특정 사용자 계정에 부여된 권한에 대한 정보 수집을 포함합니다. RCS 개체의 사용자 계정은 다음 계정의 임의 결합으로 지정되었을 수 있습니다.

- 개별 계정
- 사용자 계정의 Active Directory 보안 그룹

- 사용자 계정의 여러 Active Directory 보안 그룹

유사하게, RCS 및/또는 SIP에 대하여 연결 개체가 동일한 방법으로 보안 그룹을 사용하는 기능이 있으므로 그룹 개체로 정의됩니다.

연결 개체 만들기

연결 개체는 그룹에서 파생되며 그룹 유형을 포함해야 합니다. 연결 범위는 연결 개체의 보안 그룹 유형을 지정합니다. 연결 개체 생성 시 추가하고자 하는 개체 유형에 적용되는 연결 범위를 선택해야 합니다. 예를 들어, Universal 선택은 Active Directory 도메인이 기본 모드 (Native Mode) 이상에서 기능할 때만 연결 개체를 사용할 수 있음을 의미합니다.

연결 개체를 만들려면:

- 1 콘솔 루트(MMC) 창에서 컨테이너를 마우스 오른쪽 단추로 클릭합니다.
- 2 **New - Dell SIP Object**를 선택하여 New Object 창을 엽니다.
- 3 새 개체의 이름을 입력합니다.
- 4 **Association Object**를 선택합니다.
- 5 연결 개체 범위를 선택합니다.
- 6 **OK**를 클릭합니다.

연결 개체에 개체 추가

Association Object Properties 창에서 사용자, 사용자 그룹, 권한 개체, SIP 장치 또는 SIP 장치 그룹을 연결할 수 있습니다.

 **참고:** Windows 2000 모드 이상을 이용할 경우 사용자 또는 SIP 개체를 통해 도메인을 확장하려면 유니버설 그룹을 사용해야 합니다.

사용자 및 SIP 장치 그룹을 추가할 수 있습니다. Dell 관련 그룹을 만드는 것은 다른 그룹을 만드는 것과 동일한 방식으로 수행됩니다.

사용자 또는 사용자 그룹을 추가하려면:

- 1 연결 개체를 마우스 오른쪽 버튼으로 클릭하고 **Properties**를 선택합니다.
- 2 **Users** 탭을 선택한 다음 **Add**를 클릭합니다.
- 3 사용자 또는 사용자 그룹 이름을 입력한 뒤 **OK**를 클릭합니다.

Privilege Object 탭을 클릭하여 SIP 장치에 대한 인증을 받을 때 사용자 또는 사용자 그룹의 권한을 정의하는 연결에 관한 개체를 추가합니다.

 **참고:** 연결 개체에는 하나의 권한 개체만 추가할 수 있습니다.

권한을 추가하려면:

- 1 **Privileges Object** 탭을 선택한 다음 **Add**를 클릭합니다.
- 2 권한 개체 이름을 입력한 뒤 **OK**를 클릭합니다.

Products 탭을 클릭하여 하나 이상의 SIP 장치를 연결에 추가합니다. 연결된 장치는 정의된 사용자 또는 사용자 그룹에 대해 사용할 수 있는 네트워크에 SIP 장치를 연결하도록 지정합니다.

 **참고:** 연결 개체에 여러 개의 SIP 장치를 추가할 수 있습니다.

SIP 장치 또는 SIP 장치 그룹을 추가하려면:

- 1 **Products** 탭을 선택한 다음 **Add**를 클릭합니다.
- 2 SIP 장치 또는 SIP 장치 그룹 이름을 입력한 뒤 **OK**를 클릭합니다.
- 3 Properties 창에서 **Apply**를 클릭한 뒤 **OK**를 클릭합니다.

콘솔 재지정 액세스 보안

RCS 설치 시, 사용자 권한이 있는 모든 사용자가 On-board Web Interface를 시작할 수 있습니다. 해당 사용자에 대한 On-board Web Interface 기능은 RCS에 설정된 사용자 권한 수준에 따라 제한됩니다. Dell 확장 스키마를 가진 LDAP는 관리자가 사용자의 On-board Web Interface 액세스를 제한할 수 있도록 하여 RCS 관리에 대한 추가 보안 수준을 추가합니다.

On-board Web Interface 사용 승인은 사용자 권한 수준이 Dell Privilege Object(DPO)의 KVM RCS Privileges 탭에 구성되어 있는지 여부에 따라 정의됩니다. DPO의 KVM SIP Privileges 탭에 있는 Console Redirection Access 확인란은 On-board Web Interface를 확인할 수 없는 사용자가 RSC 클라이언트를 통해 SIP 하위 집합에 대해 Video Viewer 세션을 실행할 수 있는 방법을 제공합니다. 승인은 Dell 연결 개체(DAO)에 포함되어 있는 DPO 및 SIP 개체의 구성 매개변수 집합의 조합에 의해 제어됩니다.

사용자의 On-board Web Interface 액세스는 허용하지 않고, RSC 클라이언트로부터 Viewer 세션만 실행할 수 있도록 설정하려면 다음 단계를 수행합니다.

- 1 사용자 액세스가 허용된 각 SIP에 대해 Dell SIP 개체를 만듭니다.
- 2 제어할 각 사용자에게 대해 Active Directory 사용자 계정을 만듭니다.
- 3 DPO를 만듭니다. KVM RCS Privileges 탭에 있는 3개의 확인란을 모두 선택 해제합니다. KVM SIP Privileges 탭의 Console Redirection Access 확인란을 선택합니다.



참고: KVM RCS Privileges 확인란에서 하나 이상의 항목을 선택하고 Console Redirection Access 확인란을 선택한 경우, KVM RCS Privileges 확인란에서 선택한 권한 수준과 연결된 일반 사용자 권한이 Console Redirection Access 확인란보다 우선권을 가지며 사용자는 AMP를 계속 확인할 수 있습니다.

- 4 DAO를 만듭니다.
- 5 4단계에서 생성된 DAO에 대한 Properties 대화 상자를 엽니다.
 - a. 2단계에서 생성된 모든 사용자 계정을 추가합니다.
 - b. 3단계에서 생성된 DPO를 추가합니다.
 - c. 1단계에서 생성된 SIP 개체를 추가합니다.

Active Directory를 사용하여 RCS에 로그인

Active Directory를 사용하여 RCS 소프트웨어나 OBWI를 통해 RCS에 로그인할 수 있습니다.

로그인 구문은 세 가지 방법 모두 동일합니다

<username@domain> 또는 <domain>\<username> 또는 <domain>/<username>(사용자 이름이 1-256 바이트의 ASCII 문자열일 경우). 공백과 특수 문자(예:\, / 또는 @)는 사용자 이름이나 도메인 이름에 사용할 수 없습니다.

 **참고:** Americas와 같은 NetBIOS 도메인 이름은 식별할 수 없으므로 지정할 수 없습니다.

 **참고:** 도메인 이름이 포함되지 않으면 사용자를 인증하는 데 Remote Console Switch의 로컬 데이터베이스가 사용됩니다.

LDAP 구현을 위한 대상 장치 이름 지정 요 구 사항

다음 오류 메시지가 나타날 경우:

Login Failure. Reason: Access cannot be granted due to Authentication Server errors

SIP 개체가 Active Directory에 만들어졌으며 개체 이름이 콘솔 스위치의 OBWI를 통해 해당 SIP에 지정된 이름과 정확하게 일치하는지 확인합니다.

Dell 표준 스키마 및 Dell 확장 스키마는 Microsoft Windows Active Directory에서 특정 개체를 사용해 SIP를 표현합니다. 이러한 개체 클래스에 대한 Microsoft의 표준 이름 지정 규칙에서는 특수 문자나 공백의 사용을 금지합니다. 현재 SIP의 대상 장치 이름에 공백이나 특수 문자가 포함되어 있는 배포 환경에서 LDAP를 사용하려면, 대상 장치 이름을 공백이나 특수 문자가 없는 이름으로 변경해야 합니다.

SIP의 대상 장치 이름 변경은 콘솔 스위치의 OBWI에서 이루어져야 하며 RSC 소프트웨어를 통해 다시 동기화되어야 합니다. OBWI에서는 SIP에 지정된 이름에 공백을 삽입할 수 있지만 Active Directory에서는 불가능하다는 점을 주의하십시오. Microsoft Active Directory 규정에 따라 SIP 개체의 이름을 지정해야 합니다.

자주 묻는 질문

다음 표에는 자주 묻는 질문과 대답이 나열되어 있습니다.

표 5.4: 자주 묻는 질문

<p>여러 개의 포리스트에 걸쳐 있는 Active Directory를 사용하여 Remote Console Switch에 로그인할 수 있습니까?</p>	<p>RCS Active Directory 쿼리 알고리즘은 단일 포리스트의 단일 트리만 지원합니다.</p>
<p>Active Directory를 사용한 Remote Console Switch 로그인이 혼합 모드(즉, 포리스트의 도메인 컨트롤러가 Microsoft Windows NT® 4.0, Windows 2000 또는 Windows Server 2003과 같은 서로 다른 운영 체제를 실행)로 작동합니까?</p>	<p>예. 혼합 모드에서 사용자, SIP 장치 개체, 연결 개체 중에서 RCS 쿼리 프로세스에서 사용되는 모든 개체는 동일한 도메인에 있어야 합니다. Dell 확장 Active Directory 사용자 및 컴퓨터 스냅인은 모드를 확인하여 혼합 모드일 경우 도메인 간에 개체를 만들기 위해 사용자를 제한합니다.</p>
<p>Active Directory와의 RCS 사용이 복수 도메인 환경을 지원합니까?</p>	<p>예. 도메인 포리스트 기능 수준은 기본 모드 또는 Windows 2003 모드이어야 합니다. 또한 연결 개체, Remote Console Switch 사용자 개체 그리고 SIP 장치 개체들(연결 개체 포함) 사이의 그룹은 유니버설 그룹이어야 합니다.</p>
<p>이들 Dell 확장 개체(Dell 연결 개체, Dell Remote Console Switch 장치, Dell 권한 개체)가 서로 다른 도메인에 있을 수 있습니까?</p>	<p>연결 개체 및 권한 개체는 동일한 도메인에 있어야 합니다. Dell 확장 Active Directory 사용자 및 컴퓨터 스냅인은 사용자가 이들 두 개체를 동일한 도메인에 만들도록 합니다. 다른 개체는 다른 도메인에 있을 수 있습니다.</p>

도메인 컨트롤러 **SSL** 구성에 대한 제한이 있습니까?

예. **RCS**는 신뢰할 수 있는 **CA SSL** 인증서 하나에 대해서만 업로드를 허용하므로 포리스트에서 모든 **Active Directory** 서버의 **SSL** 인증서는 동일한 루트 **CA**에 의해 서명되어야 합니다.

다음과 같이 문제를 해결하십시오.

- 도메인 이름을 지정하지 않으면 로컬 데이터베이스가 사용됩니다. **AD** 인증이 작동하지 않을 때 로그인하려면 기본 로컬 관리 계정을 사용하십시오.

- **RCS Active Directory** 구성 창에서 **Enable Active Directory** 확인란 (**RCS Software**) 또는 **Use LDAP Authentication** 확인란(온보드(on-board) 웹 인터페이스)을 선택했는지 확인하십시오.

- **RCS Networking** 구성 페이지에서 **DNS** 설정이 올바른지 확인하십시오.

- **NTP** 패널에서 지정된 서버 중 하나 이상의 서버에서 네트워크 시간 프로토콜이 활성화되어 있는지 확인하십시오.

Active Directory 루트 **CA**의 **Active Directory** 인증서를 **RCS**로 업로드했는지 확인하십시오.

- 도메인 컨트롤러 **SSL** 인증서의 사용 기한이 만료되지 않았는지 확인하십시오.

- 사용자의 "**Remote Console Switch** 이름", "루트 도메인 이름", "**RCS** 도메인 이름"이 **Active Directory** 환경 구성과 일치하는지 확인하십시오.

- 로그인 시 정확한 사용자 도메인 이름을 사용하고 있으며 **NetBIOS** 이름을 사용하지 않는지 확인하십시오.

Active Directory 인증을 사용하여 RCS에 로그인할 수 없다면 어떻게 해야 합니까?

부록 A: 터미널 작동

각 RCS는 SETUP 포트를 통해 액세스하는 Console 메뉴 인터페이스에서 스위치 레벨에 구성할 수 있습니다. 모든 터미널 명령어는 터미널 또는 터미널 에뮬레이션 소프트웨어가 실행되고 있는 PC를 통해 액세스합니다.

 **참고:** 선호하는 방법은 모든 구성 설정을 로컬 UI에 만드는 것입니다.

터미널을 스위치에 연결하려면:

- 1 제공되는 RJ-45 DB-9(암) 어댑터 및 플랫 RJ-45 케이블을 사용하여 터미널 및 터미널 에뮬레이션 소프트웨어 (HyperTerminal 등)가 실행되는 PC를 스위치 후면 패널의 SETUP 포트에 연결합니다. 터미널 설정은 9600bps(초당 비트 수), 8비트, 1 stop bit(정지 비트), no parity(패리티 없음), no flow control(흐름 제어 안함)입니다.
- 2 각 대상 장치의 전원을 다음 스위치의 전원을 켭니다. 스위치가 초기화를 완료하면 Console 메뉴에 다음 메시지가 표시됩니다. **Press any key to continue.**라는 메시지를 보냅니다.

콘솔 부팅 메뉴 옵션

스위치가 켜지는 동안 키를 눌러 부팅 메뉴를 볼 수 있습니다. 이 메뉴에서 4개의 옵션 중 하나를 선택할 수 있습니다.

- Boot Normal
- Boot Alternate Firmware
- Reset Factory Defaults
- Full-Factory Reset

콘솔 주 메뉴 옵션

전원을 켜면 주 메뉴에 제품 이름 및 버전이 표시됩니다. 이 메뉴에서 4개의 옵션 중 하나를 선택할 수 있습니다.

- **Network configuration:** 이 메뉴 옵션을 사용하여 RCS의 네트워크 설정을 구성할 수 있습니다.
- **Debug Messages:** 이 메뉴 옵션은 콘솔 상태 메시지를 캡니다. 이 옵션은 성능을 상당히 저하시킬 수 있으므로 Dell™ 기술 지원 센터에 요청하는 경우에만 디버그 메시지를 활성화하십시오. 메시지 확인이 끝나면 아무 키나 눌러 이 모드를 종료하십시오.
- **RCS 재설정:** 이 메뉴 옵션으로 스위치의 소프트 초기화를 실행할 수 있습니다.
- **종료:** 이 메뉴를 선택하면 대기 중인 프롬프트로 돌아갑니다. Console 메뉴 인터페이스 비밀번호가 활성화된 경우 Console 주 메뉴를 종료해야 다음 사용자에게 사용자 이름 및 비밀번호를 입력하는 로그인 화면이 표시됩니다.

부록 B: SIP 사용

관리자는 로컬 사용자 인터페이스나 원격 OBWI를 통해 각 Serial SIP 포트에 대해 Avocent ACS 콘솔 서버와 Cisco 핀 배열 중에 하나를 선택해야 합니다. ACS 기본입니다.

Cisco 모드로 핀 배열을 변경하려면:

- 1 *Unit View - RCS - RCS Settings - Ports - SIPs*를 선택합니다.
- 2 원하는 SIP를 클릭합니다.
- 3 *Settings - Pinout*을 선택합니다.



참고: DB-9 어댑터를 사용할 경우 ACS 콘솔 서버 핀 배열을 선택합니다.

ACS 콘솔 서버 포트 핀 배열

다음 표에는 SIP에 대한 ACS 콘솔 서버 직렬 포트 핀 배열이 나열되어 있습니다.

표 B.1: ACS 콘솔 서버 직렬 포트 핀 배열

핀 번호	신호 이름	입력/출력
1	RTS - Request to Send	출력
2	DTR - Data Terminal Ready	출력
3	TXD - Transmit Data	출력
4	GND - Signal Ground	없음
5	CTS - Clear to Send	입력

핀 번호	신호 이름	입력/출력
6	RXD - Receive Data	입력
7	DCD/DSR - Data Set Ready	입력
8	N/C - Not Connected	없음

Cisco 포트 핀 배열

다음 표에는 SIP에 대한 Cisco 직렬 포트 핀 배열이 나열되어 있습니다.

표 B.2: Cisco 직렬 포트 핀 배열

핀 번호	신호 이름	입력/출력
1	CTS - Clear to Send	입력
2	DCD/DSR - Data Set Ready	입력
3	RXD - Receive Data	입력
4	GND - Signal Ground	없음
5	N/C - Not Connected	없음
6	TXD - Transmit Data	출력
7	DTR - Data Terminal Ready	출력
8	RTS - Request to Send	출력

부록 C: MIB 및 SNMP 트랩

Dell RCS는 SNMP 관리자에게 감사 이벤트를 전송할 수 있습니다. SNMP 트랩은 SNMP 트랩 MIB에 정의됩니다.

트랩 MIB 파일은 트랩 MIB 저장 기능을 사용하여 RCS로부터 업로드할 수 있습니다. 업로드된 트랩 MIB 파일은 SNMP Trap Receiver 응용 프로그램으로 로드할 수 있습니다.

감사 이벤트도 "syslog" 대상으로 전달할 수 있습니다. 각 syslog 메시지 형식은 트랩 MIB 파일에 정의된 각 트랩의 해당 "--#SUMMARY" 메모에 제공됩니다.

이 부록은 RCS에서 생성할 수 있는 트랩 이벤트를 설명합니다. 이 부록의 정보를 최신으로 유지하기 위해 노력했지만 트랩 MIB 파일에는 가장 정확한 트랩 정보가 포함되어 있습니다.

SNMP 관리자는 IPv4 또는 IPv6 프로토콜을 사용하여 RCS의 MIB-II 개체에 액세스할 수 있습니다.

설계에 따라 RCS 내의 특정 MIB 개체는 SNMP를 사용하여 액세스할 수 없습니다.

RCS 트랩 정의는 다음 RFC에 기술된 구조를 사용합니다.

- RFC-1155-SMI
TCP/IP 기반 인터넷 사용을 위한 관리 정보 규정에 대한 일반적인 구조 및 식별 체계를 설명합니다.
- RFC-1212
간결하고 서술적인 MIB 모듈을 만들기 위한 형식을 설명합니다.
- RFC-1213-MIB

TCP/IP 기반 상호 네트워크에서 네트워크 관리 프로토콜과 함께 사용하기 위한 인터넷 표준 MIB-II를 설명합니다.

- RFC-1215

SNMP 표준 트랩을 설명하고 전사적 트랩을 정의하기 위한 수단을 제공합니다. 각 트랩이 보고한 특정 개체는 RCS에서 업로드된 트랩 MIB 파일에 정의됩니다. 다음 표는 생성된 트랩 이벤트의 목록입니다.

표 C.1: 생성된 트랩 이벤트

트랩 이벤트	트랩 번호
Reboot Started	1
User Login	2
User Logout	3
Target Session Started	4
Target Session Stopped	5
Target Session Terminated	6
traps 7 through 9 are deprecated	7-9
Image File Upgrade Started	10
Image File Upgrade Results	11
User Added	12
User Deleted	13
User Modified	14
User Locked	15

트랩 이벤트	트랩 번호
User Unlocked	16
User Authentication Failure	17
SIP Added	18
SIP Removed	19
SIP Moved	20
Target Device Name Changed	21
Tiered Switch Added	22
Tiered Switch Removed	23
Tiered Switch Name Changed	24
Configuration File Loaded	25
User Database File Loaded	26
Ca Certificate Loaded	27
SIP Image Upgrade Started	28
SIP Image Upgrade Result	29
SIP Restarted	30
Virtual Media Session Started	31
Virtual Media Session Stopped	32
Virtual Media Session Terminated	33
Virtual Media Session Reserved	34

트랩 이벤트	트랩 번호
Virtual Media Session Unreserved	35
Virtual Media Drive Mapped	36
Virtual Media Drive Unmapped	37
traps 38 through 44 are deprecated	38-44
Screen Resolution Changed	45
Aggregated Target Device Status Changed	46
Factory Defaults Set	47
Power Supply Failure	48
Power Supply Restored	49
Pdu Device Online	50
Pdu Device Offline	51
Pdu Socket On Command	52
Pdu Socket Off Command	53
Pdu Socket Reboot Command	54
Pdu Socket On Sense Fail	55
Pdu Socket Off Sense Fail	56
Pdu Status Socket On	57
Pdu Status Socket Off	58
Pdu Port Name Changed	59

트랩 이벤트	트랩 번호
Pdu Socket Name Changed	60
Pdu Input Feed Total Load High	61
Pdu Input Feed Total Load Low	62
Pdu Device Name Changed	63
Pdu Input Feed Name Changed	64
Pdu Socket Lock Command	65
Pdu Socket Unlock Command	66
Pdu Status Socket Lock	67
Pdu Status Socket Unlock	68
Pdu Image File Upgrade Started	69
Pdu Image File Upgrade Result	70
Pdu Circuit Name Changed	71
Pdu Device Total Load High	72
Pdu Circuit Total Load High	73
Pdu Socket Total Load High	74
Fan Failure	75
Temperature Range	76
Smart Card Inserted	77
Smart Card Removed	78

부록 D: 케이블 핀 배열 정보



참고: 모든 스위치는 모뎀 및 콘솔/설정 포트를 위한 8 핀 모듈형 잭이 있습니다.

모뎀 핀 배열

다음 그림 및 표에 모뎀 포트 핀 배열 및 설명이 나와 있습니다.

그림 D.1. 모뎀 핀 배열

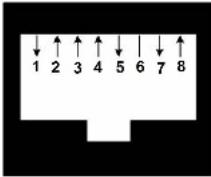


표 D.1: 모뎀 핀 배열 설명

핀 번호	설명	핀 번호	설명
1	RTS(Request to Send)	5	TXD(Transmit Data)
2	DSR(Data Set Ready)	6	GS(Signal Ground)
3	DCD(Data Carrier Detect)	7	DTR(Data Terminal Ready)
4	RXD(Receive Data)	8	CTS(Clear to Send)

콘솔/설정 핀 배열

다음 그림과 표에 콘솔/설정 포트 핀 배열 및 설명이 나와 있습니다.

그림 D.2. 콘솔/설정 핀 배열

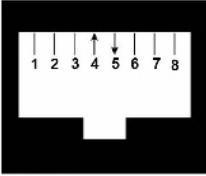


표 D.2: 콘솔/설정 핀 배열 설명

핀 번호	설명	핀 번호	설명
1	연결 없음	5	TXD(Transmit Data)
2	연결 없음	6	GS(Signal Ground)
3	연결 없음	7	연결 없음
4	RXD(Receive Data)	8	연결 없음

부록 E: UTP 케이블 연결

이 부록은 연결 미디어의 여러 가지 기능을 설명합니다. RCS 시스템은 UTP 케이블 연결을 사용합니다. 고품질 연결은 스위치 시스템의 성능에 매우 중요합니다. 케이블 연결의 품질이 나쁘거나 잘못 설치 또는 유지 관리되면 스위치 시스템 성능이 저하될 수 있습니다.



참고: 이 부록은 참고용으로만 제공됩니다. 설치하기 전에 지역 코드 관계자나 케이블링 컨설턴트의 자문을 구하십시오.

UTP 동축 케이블 연결

다음은 RCS이/가 지원하는 3가지 유형의 UTP 케이블 연결에 대한 기본적인 정의입니다.

- CAT 5(4쌍) 고성능 케이블은 데이터 전송을 위해 주로 사용되는 트위스트 페어 선으로 구성됩니다. 선 쌍을 이 방식으로 꼬면 바람직스럽지 못한 간섭의 침투에 대해 어느 정도 면역성이 생깁니다. CAT 5 케이블은 대개 10 또는 100 Mbps 속도로 실행되는 네트워크에 사용됩니다.
- CAT 5E(확장) 케이블은 CAT 5와 같은 특성을 지니고 있지만 좀더 엄격한 표준에 따라 제조됩니다.
- CAT 6 케이블은 CAT 5E 케이블보다 더 엄격한 요구 사항에 따라 제조됩니다. CAT 6은 동일한 주파수에서 CAT 5E보다 더 높은 측정 주파수 범위와 훨씬 더 우수한 성능 요구 사항을 가지고 있습니다.

배선 표준

컨덕터 8개 (4쌍) RJ-45 터미네이션 UTP 케이블에 대해 지원되는 두 가지 배선 표준, 즉 EIA/TIA 568A 및 B. 이 표준은 UTP 케이블 사양을 사용하는 설치에 적용됩니다. RCS 시스템은 이 배선 표준 중 하나를 지원합니다. 다음 표에서 각 핀의 표준을 설명합니다.

표 E.1: UTP 배선 표준

핀	EIA/TIA 568A	EIA/TIA 568B
1	흰색/녹색	흰색/주황색
2	녹색	주황색
3	흰색/주황색	흰색/녹색
4	파란색	파란색
5	흰색/파란색	흰색/파란색
6	주황색	녹색
7	흰색/갈색	흰색/갈색
8	갈색	갈색

케이블 설치, 유지 보수 및 안전 정보

다음은 케이블을 설치 또는 유지보수하기 전에 검토해야 하는 중요한 안전 주의사항입니다.

- 모든 UTP의 길이를 각각 최대 30 피트를 초과하지 않도록 하십시오.

- 선 쌍을 끝 지점까지 고르게 꼬아야 합니다. 꼬지 않은 부분의 길이가 1.2cm를 넘지 않도록 하십시오. 끝까지 끈 후에 재킷을 2.5cm 이상 벗기지 마십시오.
- 케이블을 구부려야 할 경우 반경 1인치 이상 급격히 굽는 부분이 없도록 하십시오. 케이블이 너무 심하게 굽거나 비틀어지면 케이블의 내부가 회복 불가능하게 손상될 수 있습니다.
- 케이블들을 케이블 타이로 가볍게 가지런히 묶으십시오. 너무 세게 묶지 마십시오.
- 케이블을 교차시켜 이어야 할 경우 정격 펀치 블록, 패치 패널 및 구성 요소를 사용하십시오. 어떤 지점에서든 케이블을 쪼개거나 중간을 잘라내어 연결하지 마십시오.
- UTP 케이블은 전기 케이블, 변압기, 전등 설비 등 EMI가 발생할 수 있는 곳에서 가능한 멀리 설치하십시오. 케이블을 전선에 묶거나 전기 설비에 올려 놓지 마십시오.
- 모든 설치된 세그먼트는 항상 케이블 테스터로 검사하십시오. 자체적으로 조율하는 것은 유효한 검사 방법이 아닙니다.
- 잭은 언제나 접점에 먼지나 다른 오염 물질이 끼지 않도록 설치하십시오. 잭의 접점은 평면 장착판에서는 위로 향하고 표면 장착상자에서는 왼쪽/오른쪽/아래로 향해야 합니다.
- 언제나 케이블을 약간 느슨하게 하고 천장이나 잘 보이지 않는 위치에 깔끔하게 감아 두십시오. 작업 출구 쪽에 최소 1.5미터, 패치 패널 쪽에 최소 4.5m의 여유를 두십시오.
- 시작하기 전에 568A 또는 568B 배선 표준을 선택하십시오. 모든 잭과 패치 패널을 동일한 배선 방법으로 배선하십시오. 동일한 설치 환경에 568A 및 568B 배선을 혼용하지 마십시오.
- 언제나 모든 지역 및 국가 화재/건물 안전 법규를 준수하십시오. 방화벽을 관통하는 모든 케이블에 대한 방화 대책을 수립하십시오. 필요한 경우 플레늄급 케이블을 사용하십시오.

F

부록 F: Sun고급 키 에뮬레이션

표준 유형 5(US) Sun 키보드의 특정 키는 로컬 포트 USB 키보드의 키 누름 시퀀스로 에뮬레이트할 수 있습니다. Sun 고급 키 에뮬레이션 모드를 활성화하고 이 키를 사용하려면 <Ctrl+Shift+Alt> 키를 누른 상태에서 <Scroll Lock> 키를 누르십시오. Scroll Lock LED가 깜박입니다. Sun 키보드의 고급 키를 사용하듯이 다음 표의 표시된 키를 사용하십시오. 예: <Stop+A>의 경우 <Ctrl+Shift+Alt>를 누른 채 <Scroll Lock>, <F1+A를 >차례로 누릅니다.

이러한 키 조합은 Dell USB, USB2 및 USB2+CAC SIP 그리고 Avocent USB, USB2 및 VMC IQ 모듈에서 작동됩니다. <F12> 키를 제외하고는 이러한 키 조합은 Microsoft Windows에서는 인식되지 않습니다. <F12> 키를 사용하면 Windows 키 기능을 수행합니다. 작업이 완료되면 <Ctrl+Shift+Alt> 키를 누른 상태에서 <Scroll Lock> 키를 눌러 Sun 고급 키 에뮬레이션 모드를 끄십시오.

표 F.1: Sun 키 에뮬레이션

구성	Application ¹
구성	키패드 *
전원	F11
열기	F7
도움말	Num Lock
특성	F3
앞	F5

중지	F1
재실행	F2
실행 취소	F4
잘라내기	F10
복사	F6
붙여넣기	F8
찾기	F9
음소거	키패드 /
Vol.+	키패드 +
소리 작게	키패드 -
Command(왼쪽) ²	F12
Command(왼쪽) ²	Win(GUI) 왼쪽 ¹
Command(오른쪽) ²	Win(GUI) 오른쪽 ¹

주석:

(1) Windows 95 104 키 키보드.

(2) 명령 키는 Sun 메타(다이아몬드) 키입니다.

부록 G: 기술 사양

표 G.1: RCS 기술 사양

	1082DS: 8
포트 수	2162DS: 16 4322DS: 32
유형	Dell PS/2, USB, USB2, USB2+CAC 및 Serial SIP. Avocent PS/2, PS2M, USB, Sun, USB2, VMC 및 Serial 모듈
커넥터	8핀 모듈형 (RJ45)
동기화 유형	개별 수평 및 수직 동기
	표준
	640 x 480 @ 60 Hz
	600 x 600 @ 75 Hz
	960 x 700 @ 75 Hz
	1024 x 768 @ 75 Hz
입력 비	1280 x 1024 @ 75 Hz
디오 해	1600 x 1200 @ 60 Hz
상도	와이드스크린
	800 x 500 @ 60 Hz
	1024 x 640 @ 60 Hz
	1280 x 800 @ 60 Hz
	1440 x 900 @ 60 Hz
	1680 x 1050 @ 60 Hz

지원되는 케이블	4쌍 UTP, 최대 길이 45 미터
크기	
폼 팩터	1U 또는 0U 랙 장착
크기	1.72 x 17.00 x 9.20(높이 x 너비 x 깊이)
중량(케이블 제외)	1082DS: 6.6 lb(3.0kg) 2162DS: 7.0 lb(3.2kg) 4322DS: 7.6 lb(3.4kg)
SETUP 포트	
번호	1
프로토콜	RS-232 직렬
커넥터	8핀 모듈형 (RJ45)
로컬 포트	
수/유형	1 VGA/4 USB
네트워크 연결	
번호	2
프로토콜	10/100/1000 이더넷
커넥터	8핀 모듈형 (RJ45)
USB 장치 포트	

번호	4
프로토콜	USB 2.0
MODEM 포트	
번호	1
프로토콜	RS-232 직렬
커넥터	8핀 모듈형 (RJ45)
PDU 포트	
번호	2
프로토콜	RS-232 직렬
커넥터	8핀 모듈형 (RJ45)
전원 사양	
	1082DS: 1 IEC C14
커넥터	2162DS: 2 IEC C14
	4322DS: 2 IEC C14
유형	내부
전원	18W
발열량	47 BTU/hr
AC 입력 범위	100 - 240 VAC

AC 주파수	50/60 Hz 자동 감지
AC 정격 입력 전류	1.25A
AC 입력 전원(최대)	40W
대기 조건 등급	
온도	작동 시 32 ~ 122 °F (0 ~ 50 °C), 정지 시 -4 ~ 158 °F (-20 ~ 70 °C)
습도	작동: 20% ~ 80 % 상대습도(비응결 정지 시: 5% ~ 95% 상대 습도, 38.7 °C 최대 습식 전구 온도)
안전성 및 EMC 표준 승인 및 표시	<p>UL / cUL, CE - EU, N (Nemko), GOST, C-Tick, NOM / NYCE, MIC (KCC), SASO, TUV-GS, IRAM, FCC, ICES, VCCI, SoNCAP, SABS, Bellis, FIS/ Kvalitet, Koncar, INSM, Ukrtest, STZ, KUCAS</p> <p>본 제품에 대한 안전 인증 및 EMC 인증은 다음에 명시되어 있습니다. CMN(인증 모델 번호), MPN(제조업체 부품 번호) 또는 영업 레벨 번호 EMC 및/또는 안전 보고서와 인증서에서 언급하는 내용은 본 제품의 레이블에 인쇄되어 있습니다</p>

부록 H: 기술 지원

기술 지원 센터 직원이 Dell 제품 설치 및 운영 시 발생하는 문제에 대해 도와 드리고 있습니다. 문제가 발생하면 아래 절차에 따라 가장 신속한 서비스를 받으십시오.

문제를 해결하는 방법:

- 1 이 설명서의 해당 부분을 찾아보고 제시된 절차에 따라 문제 해결을 시도해 봅니다.
- 2 Dell 웹 사이트 (dell.com/support)에서 기술 자료를 검색하거나 온라인 서비스를 요청하십시오.
- 3 해당 지역 Dell 기술 지원 센터에 전화로 문의합니다.

