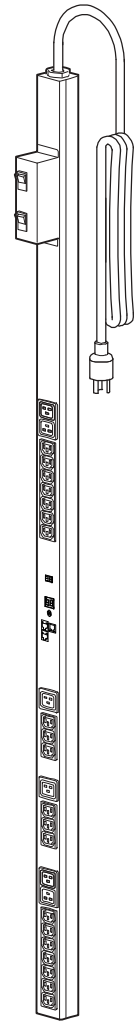
사용 설명서

관리 랙
전력 분배 장치(PDU)



목차

소개

제품 특징

Dell® 관리 랙 전력 분배 장치(PDU)는 네트워크로 관리할 수 있는 독립 실행형 전력 분배 장치입니다. 랙 PDU는 연결된 부하를 실시간으로 원격 모니터링합니다. 사용자 정의 경보가 잠재적 회로 과부하를 경고합니다. 랙 PDU는 원격 명령 및 사용자 인터페이스 설정을 통해 완벽한 출력 제어 기능을 제공합니다.

웹 인터페이스, 명령줄 인터페이스(CLI) 또는 SNMP (Simple Network Management Protocol)를 통해 랙 PDU를 관리할 수 있습니다.

- 웹 인터페이스에는 HTP (Hypertext Transfer Protocol)이나 SSL (Secure Sockets Layer)을 통한 보안 HTTP (HTTPS)를 사용하여 액세스합니다. 웹 인터페이스에 로그온을 참조하십시오.
- 직렬 연결, Telnet 또는 SSH (Secure Shell)를 통해 명령줄 인터페이스에 액세스합니다. 명령줄 인터페이스 정보을 참조하십시오.
- SNMP 브라우저와 Dell MIB (Management Information Base)를 사용하여 랙 PDU를 관리합니다.

랙 PDU에는 다음과 같은 추가 특징이 있습니다.

- 연결된 모든 부하에 대한 최고 부하 및 전력과 에너지 모니터링
- 위상 전압, 전류 및 전력 모니터링
- 각 출력의 전력 모니터링
- 회로 과부하 방지에 유용한 네트워크 및 시각적 알람을 제공하는 구성 가능한 알람 임계값
- 4가지 수준의 사용자 액세스 계정: 관리자, 장치 사용자, 읽기 전용 사용자 및 출력 사용자
- 독립적 출력 제어
- 구성 가능한 전력 지연

- 최대 24개의 독립 출력 사용자 계정.
- 이벤트 및 데이터 로깅. Telnet, SCP (Secure CoPy), FTP (File Transfer Protocol), 직렬 연결 또는 웹 브라우저(SSL를 통한 HTTPS 액세스 또는 HTTP 액세스 사용)를 통해 이벤트 로그에 액세스할 수 있습니다. 웹 브라우저, SCP 또는 FTP를 통해 데이터 로그에 액세스할 수 있습니다.
- 랙 PDU 및 시스템 이벤트에 대한 전자 메일 알림.
- 랙 PDU 및 시스템 이벤트의 심각도 수준 또는 카테고리에 기준한 SNMP 트랩, Syslog 메시지 및 전자 메일 알림
- 인증 및 암호화를 위한 보안 프로토콜

랙 PDU는 전력 서지 보호 기능을 제공하지 않습니다. 전력 장애 또는 서지로부터 장비를 확실히 보호하려면 랙 PDU를 무정전 전력 공급 장치(UPS)에 연결하십시오.

로그온 액세스 우선 순위

한 번에 한 명의 사용자만 랙 PDU에 로그온할 수 있습니다. 액세스 우선 순위는 다음과 같습니다(높은 순에서 낮은 순으로).

- 랙 PDU에 대한 직접 직렬로 연결된 컴퓨터에서 명령행 인터페이스로 로컬 액세스
- 원격 컴퓨터에서 명령줄 인터페이스로 Telnet 또는 SSH (Secure Shell) 액세스
- 웹 액세스

SNMP가 랙 PDU에 액세스를 제어하는 방식에 대한 자세한 내용은 SNMP를 참조하십시오.

사용자 계정 유형

랙 PDU에는 4가지 수준의 액세스(관리자, 장치 사용자, 읽기 전용 사용자 및 출력 사용자)가 있으며 사용자 이름과 암호로 보호됩니다.

- 관리자는 웹 인터페이스의 모든 메뉴와 명령줄 인터페이스의 모든 명령을 사용할 수 있습니다. 기본 사용자 이름과 암호는 모두 admin입니다.
- 장치 사용자는 다음에 대한 액세스 권한만 갖습니다.
  - 웹 인터페이스에서 Device Manager 탭과 Environment 탭의 메뉴와 Logs 탭의 왼쪽 탐색 메뉴에 있는 Events 및 Data 제목에서 액세스할 수 있는 이벤트 및 데이터 로그. 이벤트와 데이터 로그 화면에는 로그를 삭제하는 버튼이 없습니다.
  - 명령줄 인터페이스에서는 동일 기능과 옵션을 이용할 수 있습니다.

  기본 사용자 이름과 암호는 모두 device입니다.
- 읽기 전용 사용자의 액세스는 다음과 같이 제한되어 있습니다.
  - 웹 인터페이스를 통해서만 액세스할 수 있습니다.
  - 장치 사용자와 같은 탭과 메뉴에 액세스할 수 있지만, 구성 변경, 장치 제어, 데이터 삭제 및 파일 전송 관련 옵션에 대한 사용 권한은 없습니다. 구성 옵션과 연결된 링크는 볼 수만 있고 사용할 수는 없으며, 이벤트와 데이터 로그 화면에는 로그를 삭제하는 버튼이 없습니다.

  기본 사용자 이름과 암호는 모두 readonly입니다.

위 세 가지 계정 유형에 대한 User Name과 Password 값을 설정하려면 사용자 액세스 설정을 참조하십시오.

- 출력 사용자의 액세스는 다음과 같이 제한됩니다.
  - 웹 인터페이스 및 명령줄 인터페이스를 통해 액세스
  - 장치 사용자와 같은 메뉴에 액세스할 수 있지만, 구성 변경, 장치 제어, 데이터 삭제 및 파일 전송 관련 옵션에 대한 사용 권한에는 제한이 있습니다. 구성 옵션과 연결된 링크는 볼 수 있지만 사용할 수 없습니다. 출력 사용자는 관리자가 할당한 출력을 제어할 수 있는 Outlet Control 메뉴 옵션에 액세스할 수 있습니다. 출력 사용자는 이벤트나 데이터 로그를 삭제할 수 없습니다.

  사용자 이름과 암호는 새 출력 사용자를 추가하는 과정에서 관리자가 정의합니다.

시작하기

랙 PDU를 사용하려면:

1. 랙 PDU와 함께 제공된 *랙 전력 분배기 설치 안내서*를 참조하여 랙 PDU를 설치합니다.
2. 전력을 공급하고 네트워크에 연결합니다. *랙 전력 분배기 설치 안내서*의 지침을 따르십시오.
3. 네트워크 설정을 구성합니다. (네트워크 설정 지정를 참조하십시오.)
4. 다음 중 한 가지 방법으로 랙 PDU 사용을 시작합니다.
   - 웹 인터페이스
   - 명령줄 인터페이스
   - 랙 PDU 전면 패널

네트워크 설정 지정

네트워크에서 랙 PDU를 작동하려면 다음과 같은 TCP/IP 설정을 구성해야 합니다.

- 랙 PDU의 IP 주소
- 서브넷 마스크
- 기본 게이트웨이

기본 게이트웨이를 사용할 수 없는 경우에는 랙 PDU와 같은 서브넷에 있고 일반적으로 실행 중인 컴퓨터의 IP 주소를 사용하십시오. 랙 PDU는 트래픽이 매우 적을 때 기본 게이트웨이를 사용하여 네트워크를 테스트합니다.

루프백 주소(127.0.0.1)를 랙 PDU의 기본 게이트웨이 주소로 사용하지 마십시오. 루프백 주소를 기본 게이트웨이 주소로 사용할 경우 네트워크 관리 카드를 사용할 수 없게 되어 로컬 직렬 로그인을 사용하여 TCP/IP 설정을 기본값으로 초기화해야 합니다.

TCP/IP 구성 방식

다음 중 한 가지 방법을 사용하여 랙 PDU에 필요한 TCP/IP 설정을 정의합니다.

- BOOTP 및 DHCP 구성
- 명령줄 인터페이스

BOOTP 및 DHCP 구성

기본 TCP/IP 구성 설정인 DHCP는 적절히 구성된 DHCP 서버가 랙 PDU에 TCP/IP 설정을 제공할 수 있는 경우에 선택할 수 있습니다. BOOTP에 대한 설정을 구성할 수도 있습니다.

사용자 구성(INI) 파일은 BOOTP 또는 DHCP 부팅 파일의 기능으로 작동할 수 있습니다. 자세한 내용은 .ini 파일 사용을 참조하십시오.

BOOTP. 랙 PDU에서 BOOTP 서버를 사용하여 TCP/IP 설정을 구성하는 경우 적절히 구성된 RFC951- 규격 BOOTP 서버를 찾아야 합니다.

BOOTP 서버의 BOOTPTAB 파일에 랙 PDU의 MAC 주소, IP 주소, 서브넷 마스크 및 기본 게이트웨이, 그리고 선택적으로 부트업 파일 이름을 입력합니다. MAC 주소는 랙 PDU의 아래쪽 또는 패키지에 포함된 품질 보증서에 표시됩니다.

랙 PDU가 재부팅하면 BOOTP 서버가 TCP/IP 설정을 제공합니다.

- 부트업 파일 이름을 지정한 경우 랙 PDU가 TFTP 또는 FTP를 사용하여 BOOTP 서버에서 해당 파일을 전송합니다. 랙 PDU는 부트업 파일에 지정된 모든 설정을 기본적으로 사용합니다.
- 부트업 파일 이름을 지정하지 않은 경우, 웹 인터페이스 또는 명령줄 인터페이스를 통해 원격으로 랙 PDU의 기타 설정을 구성할 수 있습니다.

부트업 파일을 만드는 방법은 BOOTP 서버 설명서를 참조하십시오.

DHCP. RFC2131/RFC2132 호환 DHCP 서버를 사용하여 랙 PDU에 대한 TCP/IP 설정을 구성할 수 있습니다.

이 절에서는 DHCP 서버를 사용한 랙 PDU 통신을 요약합니다. DHCP 서버가 랙 PDU에 대한 네트워크 설정을 구성하는 방법에 대한 자세한 내용은 DHCP 응답 옵션을 참조하십시오.

1. 랙 PDU는 다음 정보를 사용하여 자신을 식별하는 DHCP 요청을 보냅니다.
   - 벤더 등급 ID
   - 클라이언트 ID(랙 PDU의 MAC 주소가 기본값임)
   - 사용자 등급 ID(기본적으로 랙 PDU의 애플리케이션 펌웨어의 ID임)
2. 적절히 구성된 DHCP 서버는 랙 PDU에 가 네트워크 통신을 위해 필요로 하는 모든 설정이 포함된 DHCP 제안으로 응답합니다. 또한 이 DHCP 제안에는 Vendor Specific Information 옵션(DHCP 옵션 43)도 포함되어 있습니다. 다음과 같은 16진 형식을 사용하여 DHCP 옵션 43의 벤더 쿠키를 캡슐화하지 않는 DHCP 제안을 무시하도록 랙 PDU를 구성할 수 있습니다. (기본적으로 랙 PDU에는 이 쿠키가 필요하지 않습니다.)

   ```
   Option 43 = 01 04 31 41 50 43
   ```

   여기서,
   - 첫 번째 바이트(01)는 코드입니다.
   - 두 번째 바이트(04)는 길이입니다.
   - 나머지 바이트(31 41 50 43)는 벤더 쿠키입니다.

Vendor Specific Information 옵션에 코드를 추가하는 방법은 DHCP 서버 설명서를 참조하십시오.

참고: 웹 인터페이스에서 **Require vendor specific cookie to accept DHCP Address** 확인란을 선택하여 DHCP 서버가 랙 PDU **Administration > Network > TCP/IP > ipv4 settings**에 정보를 제공하는 공급업체 쿠키를 제공하도록 할 수 있습니다.

명령줄 인터페이스

1. 명령줄 인터페이스에 로그온합니다. 명령줄 인터페이스에 로그온을 참조하십시오.
2. 네트워크 관리자에게 랙 PDU에 대한 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 문의합니다.
3. 다음 세 가지 명령을 사용하여 네트워크 설정을 구성합니다 (기울림꼴 문자는 변수임).

   a. `tcpip -i yourIPaddress`

   b. `tcpip -s yourSubnetMask`

   c. `tcpip -g yourDefaultGateway`

   각 변수에 *xxx.xxx.xxx.xxx* 형식의 숫자 값을 입력합니다.

   예를 들어 시스템 IP 주소가 156.205.14.141이면, 다음 명령어를 입력하고 ENTER를 누릅니다.

   `tcpip -i 156.205.14.141`
4. **exit**을 입력합니다. 랙 PDU를 다시 시작하여 변경 내용을 적용합니다.

분실 암호 복구

로컬 컴퓨터(직렬 포트를 통해 랙 PDU에 또는 다른 장치에 연결된 컴퓨터)를 사용하여 명령줄 인터페이스에 액세스할 수 있습니다.

1. 로컬 컴퓨터에서 직렬 포트를 선택하고 해당 포트를 사용하는 모든 서비스를 비활성화합니다.
2. 제공된 직렬 케이블을 컴퓨터에서 선택한 포트와 랙 PDU의 직렬 포트를 연결합니다.
3. 단말기 프로그램(예: HyperTerminal®)을 실행하고 2400 bps, 8 데이터 비트, 패리티 없음, 1 정지 비트 및 흐름 제어 없음으로 선택한 포트를 구성합니다.
4. User Name 프롬프트가 표시될 때까지 ENTER를 누릅니다. User User Name 프롬프트가 표시되지 않으면 다음 항목을 확인하십시오.
   - 다른 응용 프로그램이 직렬 포트를 사용하고 있지 않습니까?
   - 단말기 설정이 3단계에 지정한 내용과 같습니까?
   - 2단계에서 지정한 케이블을 사용하고 있습니까?
5. Reset 버튼을 누릅니다. 상태 LED가 orange과 녹색으로 번갈아 깜박입니다. LED가 깜박이는 동안 Reset 버튼을 바로 다시 눌러 사용자 이름과 암호를 일시적으로 기본값으로 초기화합니다.
6. 반복해서 필요한 경우, ENTER를 눌러 User Name 프롬프트를 다시 표시한 후 사용자 이름과 암호를 dell로 사용합니다. User Name 프롬프트가 다시 표시된 후 30초 동안 로그온하지 않으면 5단계를 반복하고 다시 로그온해야 합니다.
7. 명령줄 인터페이스에서 다음 명령을 사용하여 현재 모두 dell로 설정되어 있는 User Name과 Password 설정을 변경합니다.

   user -an *yourAdministratorName*

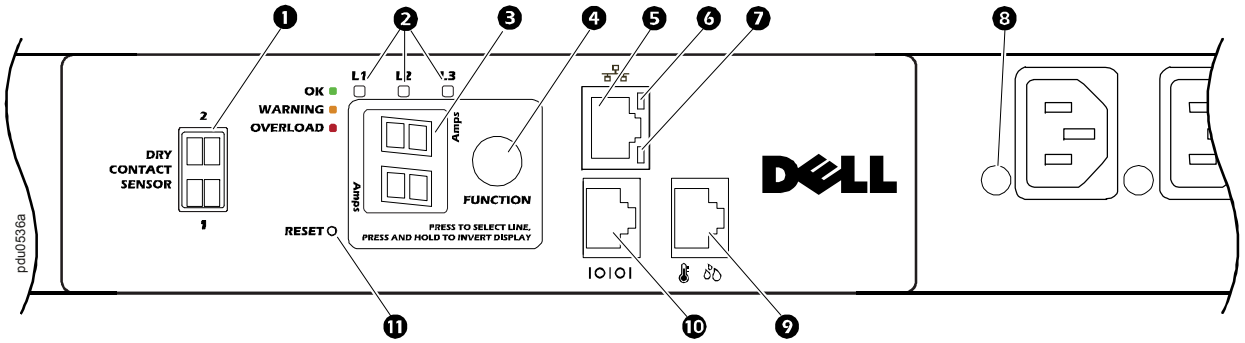
   user -ap *yourAdministratorPassword*

   예를 들어, 관리자 사용자 이름을 Don Admin으로 변경하려면 다음과 같이 입력합니다.

   user -an Don Adams

8. **quit** 또는 **exit**를 입력하여 로그오프한 후 분리한 직렬 케이블을 다시 연결하고 비활성화한 서비스를 다시 시작합니다.

랙 PDU 전면 패널



항목		기능
❶	드라이 접점 입력	드라이 접점 장치 2대용 커넥터
❷	위상 LED 참고: 단상 랙 PDU에는 LED가 한 개 뿐입니다.	알람이 발생하지 않을 때는 LED가 위상 전류를 표시하고 해당 위상에 대해 녹색 LED가 표시됩니다. 시스템이 자동으로 각 위상을 순환하며 3초 동안 위상 전류를 표시합니다. 한 위상에 대한 알람이 발생하면 해당 위상 LED가 켜져고 알람 조건이 종료될 때까지 꺼지지 않습니다. 알람이 Warning 수준이면 주황색으로, Critical 수준이면 빨간색으로 LED가 켜집니다. 여러 위상에 대해 알람이 발생하면 시스템은 자동으로 알람이 발생한 각 위상을 순환하면서 3초 동안 위상 LED를 켭니다.
❸	LED 디스플레이	현재 켜진 위상 LED에 대한 위상 전류를 표시합니다.

항목		기능
❹	Function 버튼	• 각 위상에 대한 전류를 수동으로 표시하려면 이 버튼을 반복해서 누릅니다. 30초 동안 또는 버튼을 다시 누를 때까지 전류가 표시됩니다. (단상 랙 PDU에서는 이 기능이 지원되지 않습니다.) • IP 주소를 표시하려면 IP가 나타날 때까지 5초간 누르고 있다가 놓습니다. LED 디스플레이에 주소가 한 번에 2자리씩 표시된 후 반복 순환됩니다. • 표시를 반전하려면 AA 패턴이 표시될 때까지 10초 동안 누르고 있습니다. AA가 원하는 방향이 될 때까지 누르고 있다가 놓습니다.
❺	10/100 base-T 커넥터	네트워크에 랙 PDU 연결용 포트
❻	10/100 LED	10/100 LED를 참조하십시오.
❼	네트워크 상태 LED	네트워크 상태 LED를 참조하십시오.
❽	출력 상태 LED	출력에 전력이 공급되면 녹색으로 켜집니다. (각 출력에 출력 LED가 있음)
❾	온도/습도 센서 포트	랙 PDU 온도 센서(G853N) 또는 랙 PDU 온도/습도 센서(H621N) 연결용 포트
❿	RJ-45 직렬 포트	명령줄 인터페이스에 로컬 액세스를 위한 단말기 에뮬레이터 프로그램에 랙 PDU 연결용 포트. 제공된 직렬 케이블을 사용하십시오.
⓫	Reset 버튼	콘센트에 영향을 주지 않고 랙 PDU의 인터페이스를 다시 시작하려면 RESET 버튼을 눌렀다가 놓습니다.

네트워크 상태 LED

상태	설명
꺼짐	다음 중 한 경우에 해당합니다. • 랙 PDU에 전원이 공급되고 있지 않습니다. • 랙 PDU가 제대로 작동하지 않습니다. 수리 또는 교체가 필요할 수 있습니다.
녹색으로 켜져 있음	랙 PDU의 TCP/IP 설정이 올바릅니다.
녹색으로 깜박임	랙 PDU에 유효한 TCP/IP 설정이 없습니다.
주황색으로 켜져 있음	랙 PDU에서 하드웨어 결함이 감지되었습니다.
주황색으로 깜박임	랙 PDU에서 BOOTP 요청을 발행합니다.
주황색과 녹색이 교대로 깜박임	LED가 천천히 깜박이는 경우는 랙 PDU가 DHCP를 요청하고 있는 상태입니다. LED가 빠르게 깜박이는 경우는 랙 PDU가 가동하고 있는 상태입니다.
1. BOOTP 또는 DHCP 서버를 사용하지 않는 경우, 네트워크 설정 지정을 참조하여 랙 PDU의 TCP/IP 설정을 구성하십시오. 2. DHCP 서버를 사용하려면 TCP/IP 및 통신 설정을 참조하십시오.	

10/100 LED

상태	설명
꺼짐	다음 중 하나 이상의 경우에 해당합니다. • 랙 PDU에 전원이 공급되고 있지 않습니다. • 랙 PDU와 네트워크를 연결하는 케이블이 분리되었거나 잘못 되었습니다. • 랙 PDU를 네트워크에 연결하는 장치가 꺼져 있습니다. • 랙 PDU가 제대로 작동하지 않습니다. 수리 또는 교체가 필요할 수 있습니다.
녹색으로 켜져 있음	랙 PDU가 초당 10메가비트(Mbps)로 작동하는 네트워크에 연결되었습니다.
주황색으로 켜져 있음	랙 PDU가 100 Mbps로 작동하는 네트워크에 연결되어 있습니다.
녹색이 깜박임	랙 PDU가 데이터 패킷을 10 Mbps로 수신 중이거나 전송 중입니다.
주황색이 깜박임	랙 PDU가 데이터 패킷을 100 Mbps로 수신 중이거나 전송 중입니다.

명령줄 인터페이스

명령줄 인터페이스 정보

명령줄 인터페이스를 사용하여 랙 PDU 상태를 확인하고 관리할 수 있습니다. 명령줄 인터페이스를 사용하여 또한 자동화 작업의 스크립트도 작성할 수 있습니다. 관리자는 명령줄 인터페이스에 완전히 액세스할 수 있고, 장치 사용자 및 출력 사용자는 제한적으로만 액세스할 수 있으며, 읽기 전용 사용자는 액세스가 완전히 제한됩니다. (자세한 내용은 사용자 계정 유형을 참조하십시오.)

CLI를 사용하여 INI 파일을 랙 PDU로 전송하여 랙 PDU의 모든 매개변수(특정 CLI 명령 이외의 명령에 대한 변수 포함)를 구성할 수 있습니다. CLI는 XMODEM을 사용하여 전송을 수행합니다. 하지만 XMODEM을 통해 현재 INI 파일을 읽을 수는 없습니다.

명령줄 인터페이스에 로그온

명령줄 인터페이스에 액세스하려면 랙 PDU와 동일한 네트워크에 있는 컴퓨터를 사용하여 로컬(직렬) 연결 또는 원격(Telnet 또는 SSH) 연결을 사용할 수 있습니다.

명령줄 인터페이스에 대한 원격 액세스

Telnet 또는 SSH를 통해 명령줄 인터페이스에 액세스할 수 있습니다. 기본값으로 사용되는 방법은 Telnet입니다. SSH를 사용하면 Telnet은 해제됩니다.

이러한 액세스 방법을 활성화하거나 비활성화하려면 웹 인터페이스를 사용하십시오. Administration 탭에서 상단 메뉴 표시줄의 Network, 왼쪽 탐색 메뉴의 Console 제목 아래에 있는 access 옵션을 선택합니다.

Telnet을 사용한 기본 액세스. Telnet은 사용자 이름과 암호로 기본적인 인증 보안을 제공하지만 암호화에 비해 보안 수준이 낮습니다.

Telnet을 사용하여 명령줄 인터페이스에 액세스하려면:

1. 랙 PDU와 동일한 네트워크에 있는 컴퓨터에서 랙 PDU의 **`telnet`** 및 IP 주소를 입력하고(예를 들어 랙 PDU가 기본 Telnet 포트 23을 사용할 때 **`telnet 139.225.6.133)`** ENTER를 누릅니다.
   랙 PDU가 기본값이 아닌 포트 번호(5000~32768)를 사용하는 경우는 Telnet 클라이언트에 따라 IP 주소(또는 DNS 이름)와 포트 번호 사이에 콜론 또는 공백을 포함시켜야 합니다. (이러한 명령은 일반적인 사용을 위한 명령입니다. 일부 클라이언트는 포트를 인수로 지정하는 것을 허용하지 않으며, 어떤 클라이언트는 추가 명령을 요구할 수도 있습니다.)
2. 사용자 이름과 암호(기본값은 관리자의 경우 admin와 admin, 장치 사용자의 경우 device와 device)를 입력합니다.

사용자 이름 또는 암호를 잊은 경우 분실 암호 복구을 참조하십시오.

SSH를 사용한 높은 수준의 보안 액세스. 웹 인터페이스에 보안 수준이 높은 SSL을 사용하는 경우는 SSH를 사용하여 명령줄 인터페이스에 액세스합니다. SSH는 사용자 이름, 암호 및 전송 데이터를 암호화합니다. SSH이나 Telnet을 통해 명령줄 인터페이스에 액세스하더라도 인터페이스, 사용자 계정 및 사용자 액세스 권한은 동일하지만, SSH를 사용하려면 먼저 컴퓨터에 SSH를 구성하고 SSH 클라이언트 프로그램을 설치해야 합니다.

명령줄 인터페이스로 로컬 액세스

로컬 액세스의 경우, 직렬 포트를 통해 랙 PDU에 연결된 컴퓨터를 사용하여 명령줄 인터페이스에 액세스할 수 있습니다.

1. 컴퓨터에서 직렬 포트를 선택하고 해당 포트를 사용하는 모든 서비스를 비활성화합니다.
2. 제공된 직렬 케이블을 컴퓨터에서 선택한 포트에서 랙 PDU의 직렬 포트로 연결합니다.
3. 단말기 프로그램(예: HyperTerminal)을 실행하고 9600 bps, 8 데이터 비트, 패리티 없음, 1 정지 비트 및 흐름 제어 없음으로 선택한 포트를 구성합니다.
4. ENTER를 누르고 프롬프트에서 사용자 이름과 암호를 입력합니다.

메인 화면 정보

다음은 랙 PDU의 명령줄 인터페이스에 로그온할 때 표시되는 메인 화면의 예입니다.

```
Dell Corporation                          Network Management Card AOS  vx.x.x
(c)Copyright 2009 All Rights Reserved  RPDUD                           vx.x.x
-------------------------------------------------------------------------------
Name     : Test Lab                                    Date : 10/30/2009
Contact  : Don Adams                                   Time : 5:58:30
Location : Building 3                                  User : Administrator
Up Time  : 0 Days, 21 Hours, 21 Minutes                Stat : P+ N+ A+

cli>
```

초기 화면 정보 필드:

- 두 필드는 운영 체제(AOS)와 응용 프로그램(APP) 펌웨어 버전을 나타냅니다. 응용 프로그램 펌웨어 이름은 네트워크에 연결하는 장치 유형을 식별합니다. 위 예에서는 랙 PDU의 응용 프로그램 펌웨어가 표시됩니다.

  ```
  Network Management Card AOS  vx.x.x

  RPDUD vx.x.x
  ```

- 세 필드는 시스템 이름, 담당자 및 랙 PDU의 위치를 나타냅니다. (제어 콘솔에서 System 메뉴를 사용하여 값을 설정합니다.)

  ```
  Name: Test Lab

  Contact: Don Adams

  Location: Building 3
  ```

- Up Time필드에는 랙 PDU를 마지막으로 켜거나 초기화한 이후 연속적으로 실행된 시간이 표시됩니다.

  ```
  Up Time: 0 Days, 21 Hours, 21 Minutes
  ```

- 두 필드에는 날짜와 시간으로 로그온한 시간이 표시됩니다.

  ```
  Date : 10/30/2009

  Time : 5:58:30
  ```

- User 필드에는 Administrator 또는 Device 사용자 계정으로 로그인했는지 여부가 표시됩니다. (**읽기 전용 사용자** 계정으로는 명령줄 인터페이스에 액세스할 수 없습니다.)

  ```
  User : Administrator
  ```

- Stat 필드에는 랙 PDU의 상태가 표시됩니다.

```
Stat : P+ N+ A+
```

P+	Dell 운영 체제가 제대로 작동하고 있습니다.

IPv4 전용	IPv6 전용	IPv4 및 IPv6*	설명
N+	**N+**	**N4+ N6+**	네트워크가 제대로 작동하고 있습니다.
N?	**N6?**	**N4? N6?**	BOOTP 요청 사이클이 진행되고 있습니다.
N-	**N6-**	**N4- N6-**	랙 PDU가 네트워크 연결에 실패했습니다.
N!	**N6!**	**N4! N6!**	다른 장치가 랙 PDU IP 주소를 사용하고 있습니다.
* N4 및 N6 값은 서로 다를 수 있습니다. 예를 들어, N4- N6+ 를 사용할 수 있습니다.			

A+	응용 프로그램이 제대로 작동하고 있습니다.
A-	응용 프로그램의 체크섬이 잘못되었습니다.
A?	응용 프로그램을 초기화하는 중입니다.
A!	응용 프로그램이 AOS와 호환되지 않습니다.

P+가 표시되지 않으면 Dell 지원 담당자에게 연락하십시오.

명령줄 인터페이스 사용

명령줄 인터페이스에서 명령을 사용하여 랙 PDU를 구성합니다. 명령을 사용하려면 해당 명령을 입력하고 ENTER를 누릅니다. 명령과 인수는 소문자, 대문자 또는 대/소문자를 혼합하여 사용할 수 있습니다. 옵션은 대소문자를 구분합니다.

명령줄 인터페이스를 사용하는 동안 다음과 같은 작업을 수행할 수 있습니다.

- **?**를 입력하고 ENTER를 누르면 계정 유형에 따라 사용 가능한 명령 목록을 확인할 수 있습니다.
- 지정된 명령의 용도 및 구문에 대한 정보를 보려면 명령과 공백, **?** 또는 **help** 단어를 입력합니다. 예를 들어, RADIUS 구성 옵션을 보려면 다음을 입력합니다.

  radius ?

  또는

  radius help

- 가장 최근에 세션에 입력된 명령을 보려면 UP 화살표 키를 누릅니다. UP 및 DOWN 화살표 키를 사용하여 최대 10개까지 이전에 사용한 명령 목록을 스크롤할 수 있습니다.
- 최소 하나의 명령어 문자를 입력하고 TAB 키를 누르면 명령줄에 입력한 텍스트와 일치하는 유효한 명령 목록이 나타납니다.
- 명령줄 인터페이스를 닫으려면 **exit** 또는 **quit**를 입력합니다.

명령 구문

항목	설명
-	옵션 앞에는 하이픈이 붙습니다.
< >	옵션 설명은 꺾쇠 괄호로 묶여 있습니다. 예: -dp <device password>
[ ]	하나의 명령으로 여러 개의 옵션을 사용할 수 있거나 하나의 옵션이 동시 적용이 불가한 인수를 허용하는 경우, 해당 값이 괄호로 묶여 있을 수 있습니다.
|	괄호 또는 꺾쇠 괄호로 묶여 있는 항목 사이의 세로선은 해당 항목이 상호 배타적임을 나타냅니다. 이 경우 하나의 항목만 사용해야 합니다.

여러 개의 옵션을 지원하는 명령의 예:

```
user [-an <admin name>] [-ap <admin password>]
```

이 예에서 user 명령은 관리자 사용자 이름을 정의하는 **-an** 옵션과 관리자 암호를 정의하는 **-ap** 옵션을 허용합니다. 관리자 사용자 이름과 암호를 XYZ로 변경하려면:

1. user 명령과 하나의 옵션, 인수 **XYZ**를 입력합니다.
   user -ap XYZ
2. 처음 명령이 성공한 후, user 명령과 두 번째 옵션, 인수 **XYZ**를 입력합니다.
   user -an XYZ

한 옵션에 대해 상호 배타적인 인수를 허용하는 명령의 예:

```
alarmcount -p [all | warning | critical]
```

이 예에서 -p 옵션은 all, warning 또는 critical입니다. 예를 들어, 활성 위험 알람의 수를 보려면 다음을 입력합니다.

alarmcount -p critical

지정되지 않은 인수를 입력하면 명령이 실패합니다.

명령 응답 코드

명령 응답 코드를 통해 오류 메시지 텍스트와 일치하는지 여부에 상관없이 스크립트된 연산으로 오류 조건을 안정적으로 검색할 수 있습니다.

CLI는 다음 형식으로 된 모든 명령 연산을 보고합니다.

E [0-9][0-9][0-9]: 오류 메시지

코드	메시지	코드	메시지
E000	Success	E105	명령 프리필
E001	성공적으로 발행됨	E106	데이터 사용 불가
E002	변경 내용을 적용하려면 재부팅 필요	E107	랙 PDU에 대한 직렬 통신이 끊김
E100	명령 실패		
E101	명령을 찾을 수 없음		
E102	매개변수 오류		
E103	명령줄 오류		
E104	사용자 수준 거부		

네트워크 관리 카드 명령 설명

?

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 계정 유형에 대해 사용 가능한 모든 CLI 명령 목록을 표시합니다. 특정 명령에 대한 도움말 텍스트를 보려면 명령 다음에 물음표를 입력합니다.

예: **alarmcount** 명령으로 허용되는 옵션 목록을 보려면 다음을 입력합니다.

```
alarmcount ?
```

about

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 하드웨어 및 펌웨어 정보를 표시합니다. 이 정보를 사용해 문제를 해결하고 펌웨어 업그레이드가 필요한지를 판별할 수 있습니다.

alarmcount

액세스: 관리자, 장치 사용자, 출력 사용자

설명:

옵션	인수	설명
-p	all	랙 PDU에서 보고된 활성 알람 수를 표시합니다. 알람에 대한 정보는 이벤트 로그에서 제공됩니다.
	warning	활성 경고 알람 수를 표시합니다.
	critical	활성 위험 알람 수를 표시합니다.

예: 모든 활성 경고 알람을 보려면 다음을 입력합니다.

```
alarmcount -p warning
```

boot

액세스: 관리자 전용

설명: IP 주소, 서브넷 마스크, 기본 게이트웨이를 포함하여 랙 PDU가 네트워크 설정을 가져오는 방법을 정의합니다. 그런 다음 BOOTP 또는 DHCP 서버 설정을 구성합니다.

옵션	인수	설명
-b <부팅 모드>	dhcp | bootp | manual	랙 PDU가 켜지거나 초기화 또는 다시 시작되었을 때 TCP/IP 설정이 구성되는 방법을 정의합니다. 각 부팅 모드 설정에 대한 자세한 내용은 TCP/IP 및 통신 설정을 참조하십시오.
-c	enable | disable	dhcp 및 dhcpBootp 부팅 모드만 해당됩니다. DHCP 서버가 벤더 쿠키를 제공하는 요구 사항을 활성화 또는 비활성화합니다.
일반적으로 이러한 세 가지 설정의 기본값은 변경할 필요가 없습니다. -v <벤더 클래스>: DELL -i <클라이언트 id>: 네트워크 상에서 고유하게 식별되는 랙 PDU의 MAC 주소입니다. -u <사용자 클래스>: 응용 프로그램 펌웨어 모듈 이름입니다.		

예: DHCP 서버를 사용하여 네트워크 설정을 가져오려면:

1. **boot -b dhcp**를 입력합니다.
2. DHCP 서버가 벤더 쿠키를 제공하는 요구 사항을 활성화합니다.

   boot -c enable

cd

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 랙 PDU의 디렉토리 구조 내에서 폴더를 탐색합니다.

예 1: **ssh** 폴더로 변경하고 SSH 보안 인증서가 랙 PDU에 업로드되었는지 확인하려면:

1. **cd ssh**를 입력하고 ENTER를 누릅니다.
2. **dir**을 입력하고 ENTER를 누르면 SSH 폴더에 저장된 파일 목록이 표시됩니다.

예 2: 메인 디렉토리 폴더로 돌아가려면 다음을 입력합니다.

```
cd ..
```

console

액세스: 관리자 전용

설명: 사용자가 기본적으로 설정되어 있는 Telnet 또는 사용자 이름, 암호 및 데이터를 암호화된 형식으로 전송하여 보호 기능을 제공하는 SSH(Secure Shell)를 사용하여 명령줄 인터페이스에 액세스할 수 있는지 여부를 정의합니다. 추가적인 보안을 위해 Telnet 또는 SSH 포트 설정을 변경할 수 있습니다. 또한 명령줄 인터페이스에 대한 네트워크 액세스를 비활성화할 수 있습니다.

옵션	인수	설명
-S	disable | telnet | ssh	명령줄 인터페이스에 대한 액세스를 구성하거나 disable 명령을 사용하여 액세스를 차단합니다. SSH를 활성화하면 SCP가 활성화되고 Telnet이 비활성화됩니다.
-pt	<텔넷 포트 번호>	랙 PDU와 통신하는 데 사용되는 Telnet 포트를 정의합니다(기본값: 23).
-ps	<SSH 포트 번호>	랙 PDU와 통신하는 데 사용되는 SSH 포트를 정의합니다(기본값: 22).
-b	2400 | 9600 | 19200 | 38400	직렬 포트 연결 속도를 구성합니다(기본값: 9600 bps).

예 1: 명령줄 인터페이스에 대한 SSH 액세스를 활성화하려면 다음을 입력합니다.

```
console -S ssh
```

예 2: Telnet 포트를 5000으로 변경하려면 다음을 입력합니다.

```
console -pt 5000
```

date

액세스: 관리자 전용

정의: 랙 PDU에서 사용되는 날짜를 구성합니다.

NTP 서버를 구성하여 랙 PDU에 사용되는 날짜와 시간을 정의하려면 날짜 및 시간 설정을 참조하십시오.

옵션	인수	설명
-d	<"날짜열">	현재 날짜를 구성합니다. `date -f` 명령에서 지정된 날짜 형식을 사용합니다.
-t	<00:00:00>	시간, 분, 초 단위로 현재 시간을 구성합니다. 24시간제 형식이 사용됩니다.
-f	mm/dd/yy | dd.mm.yyyy | mmm- dd- yy | dd- mmm-yy | yyyy- mm- dd	이 사용자 인터페이스에 모든 데이터를 표시하는 숫자 형식을 선택합니다. 각 문자 m(월), d(일), y(년)는 1자리수를 나타냅니다. 한 자리수 날짜와 달은 앞자리가 숫자 0으로 표시됩니다.
-z	<시간대 시차>	사용자 시간대를 지정하기 위해 GMT와의 시차를 설정합니다. 이렇게 하면 다른 시간대에 있는 사용자와 동기화할 수 있습니다.

예 1: yyyy-mm-dd 형식을 사용하여 날짜를 표시하려면 다음을 입력합니다.

```
date -f yyyy-mm-dd
```

예 2: 앞의 예에서 구성한 형식을 사용하여 날짜를 2009년 10월 30일로 정의하려면 다음을 입력합니다.

```
date -d "2009-10-30"
```

예 3: 시간을 5:21:03 p.m.으로 정의하려면 다음을 입력합니다.

```
date -t 17:21:03
```

delete

액세스: 관리자 전용

설명: 파일 시스템의 파일을 삭제합니다.

인수	설명
<파일 이름>	삭제할 파일 이름을 입력합니다.

dir

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 랙 PDU에 저장된 파일과 폴더를 표시합니다.

dns

액세스: 관리자 전용

정의: 수동 DNS (Domain Name Service) 설정을 구성합니다.

매개변수	인수	설명
-OM	enable | disable	수동 DNS를 다시 정의합니다.
-p	<기본 DNS 서버>	기본 DNS 서버를 설정합니다.
-s	<보조 DNS 서버>	보조 DNS 서버를 설정합니다.
-d	<도메인 이름>	도메인 이름을 설정합니다.
-n	<도메인 이름 IPv6>	도메인 이름 IPv6을 설정합니다.
-h	<호스트 이름>	호스트 이름을 설정합니다.

eventlog

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 이벤트 로그, 랙 PDU 상태, 랙 PDU에 연결된 센서 상태를 확인한 날짜와 시간을 표시합니다. 가장 최근의 장치 이벤트와 해당 이벤트가 발생한 날짜와 시간이 표시됩니다. 이벤트 로그를 탐색하려면 다음 키를 사용합니다.

키	설명
ESC	이벤트 로그를 닫고 명령줄 인터페이스로 돌아갑니다.
ENTER	로그 표시를 업데이트합니다. 이 명령을 사용하면 마지막으로 검색하여 표시한 로그 이후에 기록된 이벤트를 볼 수 있습니다.
스페이스바	이벤트 로그의 다음 페이지를 표시합니다.
B	이벤트 로그의 이전 페이지를 표시합니다. 이 명령은 이벤트 로그 첫 페이지에서는 사용할 수 없습니다.
D	이벤트 로그를 지웁니다. 프롬프트를 따라 삭제를 확인하거나 거부합니다. 삭제된 이벤트는 복구할 수 없습니다.

exit

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 명령줄 인터페이스 세션을 종료합니다.

format

액세스: 관리자 전용

설명: 랙 PDU의 파일 시스템을 재포맷하고 모든 보안 인증서, 암호화 키, 구성 설정, 이벤트 및 데이터 로그를 삭제합니다.

랙 PDU를 기본 구성으로 초기화하려면 **resetToDef** 명령을 사용하십시오.

FTP

액세스: 관리자 전용

설명: FTP 서버에 대한 액세스를 활성화하거나 비활성화합니다. 또는 추가적인 보안을 위해 5001~32768 중에서 사용되지 않은 포트 번호로 포트 설정을 변경합니다.

옵션	인수	정의
-p	<포트 번호>	FTP 서버가 랙 PDU와 통신하는 데 사용하는 TCP/IP 포트를 정의합니다(기본값: 21). FTP 서버는 지정된 포트와 지정된 포트보다 한 자리가 낮은 포트 둘 다 사용합니다.
-S	enable | disable	FTP 서버에 대한 액세스를 구성합니다.

예: TCP/IP 포트를 5001로 변경하려면 다음을 입력합니다.

```
ftp -p 5001
```

help

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 계정 유형에 대해 사용 가능한 모든 CLI 명령 목록을 표시합니다. 특정 명령에 대한 도움말 텍스트를 보려면 명령 다음에 **help**를 입력합니다.

예 1: 장치 사용자에 대해 사용 가능한 명령 목록을 보려면 다음을 입력합니다.

```
help
```

예 2: **alarmcount** 명령으로 허용되는 옵션 목록을 보려면 다음을 입력합니다.

```
alarmcount help
```

netstat

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 네트워크 상태와 모든 활성 IPv4 및 IPv6 주소를 표시합니다.

ntp

액세스: Administrator

정의: 네트워크 시간 프로토콜 매개변수를 표시하고 구성합니다.

옵션	인수	정의
-OM	enable | disable	수동 설정을 다시 정의합니다.
-p	<기본 NTP 서버>	기본 서버를 지정합니다.
-s	<보조 NTP 서버>	보조 서버를 지정합니다.

예 1: 수동 설정 재정의를 활성화하려면 다음을 입력합니다.

```
ntp -OM enable
```

예 2: 기본 NTP 서버를 지정하려면 다음을 입력합니다.

```
ntp -p 150.250.6.10
```

ping

액세스: 관리자, 장치 사용자

설명. 지정한 IP 주소 또는 DNS 이름을 가진 장치가 네트워크에 연결되었는지 여부를 확인합니다. 4개의 질의가 이 주소로 전송됩니다.

인수	설명
<IP 주소 또는 DNS 이름>	*xxx.xxx.xxx.xxx* 형식의 IP 주소 또는 DNS 서버에 의해 구성된 DNS 이름을 입력합니다.

예: IP 주소 150.250.6.10을 갖는 장치가 네트워크에 연결되어 있는지 여부를 확인하려면 다음을 입력합니다.

```
ping 150.250.6.10
```

portSpeed

액세스: 관리자

설명:

옵션	인수	설명
-s	auto | 10H | 10F | 100H | 100F	이더넷 포트의 통신 속도를 정의합니다. `auto` 명령을 사용하면 이더넷 장치가 가능한 최고 속도의 전송 속도를 조절할 수 있습니다. 포트 속도 설정에 대한 자세한 내용은 포트 속도를 참조하십시오.

예: 반- 이중(한 번에 한 방향으로만 통신 가능) 통신을 지원하는 100 Mbps를 사용하여 통신할 수 있도록 TCP/IP 포트를 구성하려면 다음을 입력합니다.

```
portspeed -s 100H
```

prompt

액세스: 관리자, 장치 사용자

설명: 현재 로그인한 사용자의 계정 유형을 포함하거나 제외하도록 명령줄 인터페이스 프롬프트를 구성합니다. 모든 사용자가 이 설정을 변경할 수 있으며, 모든 사용자 계정이 새로운 설정을 사용하여 업데이트됩니다.

옵션	인수	설명
-s	long	프롬프트에 현재 로그인한 사용자의 계정 유형이 포함됩니다.
	short	기본 설정입니다. 프롬프트가 4자 길이로 구성됩니다: `cli>`

예: 명령 프롬프트에 현재 로그인한 사용자의 계정 유형을 포함시키려면 다음을 입력합니다.

```
prompt -s long
```

quit

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 명령줄 인터페이스 세션을 종료합니다(exit 명령과 동일).

radius

액세스: 관리자 전용

설명: 기존의 RADIUS 설정을 표시하고 RADIUS 인증을 활성화 또는 비활성화하거나 최대 2개의 RADIUS 서버에 대한 기본 인증 매개변수를 구성합니다.

RADIUS 서버 구성에 대한 요약과 지원되는 RADIUS 서버 목록은 RADIUS 서버 구성을 참조하십시오.

RADIUS 서버에 대한 추가 인증 매개변수는 랙 PDU의 웹 인터페이스에서 사용할 수 있습니다. 자세한 내용은 RADIUS를 참조하십시오.

RADIUS 서버 구성에 대한 자세한 내용은 부록 B: 보안 핸드북을 참조하십시오.

옵션	인수	설명
-a	local | radiusLocal | radius	RADIUS 인증을 구성합니다. **local**-RADIUS가 비활성화됩니다. 로컬 인증이 활성화됩니다. **radiusLocal**-RADIUS 이후, 로컬 인증. RADIUS와 로컬 인증이 활성화됩니다. 우선적으로 RADIUS 서버에서 인증을 요구합니다. RADIUS 서버가 응답하지 않으면 로컬 인증이 사용됩니다. **radiusl**-RADIUS가 활성화됩니다. 로컬 인증이 비활성화됩니다.
-p1 -p2	<서버 IP>	기본 또는 보조 RADIUS 서버의 서버 이름 또는 IP 주소입니다. **참고:** RADIUS 서버는 기본적으로 1812 포트를 사용하여 사용자를 인증합니다. 다른 포트를 사용하려면 RADIUS 서버명 또는 IP 주소 끝에 새로운 포트 번호를 입력하고 콜론(:)을 추가합니다.
-s1 -s2	<서버 보안>	기본 또는 보조 RADIUS 서버와 랙 PDU 간의 공유 보안입니다.
-t1 -t2	<서버 시간 제한>	기본 또는 보조 RADIUS 서버가 응답할 때까지 랙 PDU가 대기하는 시간(단위: 초)입니다.

예 1:

랙 PDU에 대한 기존의 RADIUS 설정을 보려면 **radius**를 입력하고 ENTER를 누릅니다.

예 2: RADIUS 및 로컬 인증을 활성화하려면 다음을 입력합니다.

```
radius -a radiusLocal
```

예 3: 보조 RADIUS 서버에 대한 10초 시간 제한을 구성하려면 다음을 입력합니다.

```
radius -t2 10
```

reboot

액세스: 관리자 전용

설명: 랙 PDU의 인터페이스를 다시 시작합니다.

resetToDef

액세스: 관리자 전용

설명:

옵션	인수	설명
-p	all | keepip	이벤트 작업, 장치 설정 또는 TCP/IP 구성 설정을 포함한 모든 구성 변경 내용을 재설정합니다.

예: 랙 PDU의 TCP/IP 설정을 제외한 모든 구성 변경 내용을 재설정하려면 다음을 입력합니다.

```
resetToDef -p keepip
```

snmp, snmpv3

액세스: 관리자 전용

설명: SNMP 1 또는 SNMP 3을 활성화하거나 비활성화합니다.

옵션	인수	설명
-S	enable | disable	SNMP, 1 또는 3을 각각 활성화하거나 표시합니다.

예: SNMP 버전 1을 활성화하려면 다음을 입력합니다.

```
snmp -S enable
```

system

액세스: 관리자 전용

설명: 시스템 이름, 접점, 위치를 보고 설정하거나 가동 시간을 비롯한 날짜 및 시간, 로그온한 사용자, 상위 수준 시스템 상태 P, N, A를 표시합니다(시스템 상태에 대한 자세한 내용은 메인 화면 정보 참조).

옵션	인수	설명
-n	<시스템 이름>	장치 이름, 해당 장치 담당자 이름, 장치의 실제 위치를 정의합니다. **참고:** 둘 이상의 단어로 값을 정의하는 경우, 해당 값을 따옴표로 묶어야 합니다.
-c	<시스템 접점>	
-l	<시스템 위치>	

예 1: 장치 위치를 **Test Lab**으로 구성하려면 다음을 입력합니다.

```
system -l "Test Lab"
```

예 2: 시스템 이름을 **Don Adams**로 구성하려면 다음을 입력합니다.

```
system -n "Don Adams"
```

tcpip

액세스: 관리자 전용

설명: 랙 PDU에 대한 네트워크 설정을 보고 수동으로 구성합니다.

옵션	인수	설명
-i	<IP 주소>	*xxx.xxx.xxx.xxx* 형식으로 랙 PDU의 IP 주소를 입력합니다.
-s	<서브넷 마스크>	랙 PDU의 서브넷 마스크를 입력합니다.
-g	<게이트웨이>	기본 게이트웨이의 IP 주소를 입력합니다. 기본 게이트웨이로 루프백 주소(127.0.0.1)를 **사용하지** 마십시오.
-d	<도메인 이름>	DNS 서버에 의해 구성된 DNS 이름을 입력합니다.
-h	<호스트 이름>	랙 PDU에서 사용할 호스트 이름을 입력합니다.

예 1: 랙 PDU에 대한 네트워크 설정을 보려면 **tcpip**를 입력하고 ENTER를 누릅니다.

예 2: 랙 PDU의 IP 주소 **150.250.6.10**을 수동으로 구성하려면 다음을 입력합니다.

```
tcpip -i 150.250.6.10
```

tcpip6

액세스: 관리자 전용

설명: IPv6을 활성화하고 랙 PDU에 대한 네트워크 설정을 보고 수동으로 구성합니다.

옵션	인수	설명
-S	enable | disable	IPv6를 활성화하거나 비활성화합니다.
-man	enable | disable	랙 PDU의 IPv6 주소에 대한 수동 주소 지정을 활성화합니다.
-auto	enable | disable	랙 PDU가 IPv6 주소를 자동으로 구성합니다.
-i	<IPv6 주소>	랙 PDU의 IPv6 주소를 설정합니다.
-g	<IPv6 게이트웨이>	기본 게이트웨이의 IPv6 주소를 설정합니다.
-d6	router | stateful | stateless | never	router controlled, statefull(주소 및 기타 정보에 대해 해당 상태 유지), stateless(주소 이외의 정보의 경우 상태가 유지되지 않음), never 매개변수를 사용하여 DHCPv6을 설정합니다.

예 1: 랙 PDU에 대한 네트워크 설정을 보려면 **tcpip6**을 입력하고 ENTER를 누릅니다.

예 2: 랙 PDU의 IPv6 주소 **2001:0:0:0:0:FFD3:0:57ab**를 수동으로 구성하려면 다음을 입력합니다.

```
tcpip -i 2001:0:0:0:0:FFD3:0:57ab
```

user

액세스: 관리자 전용

설명: 관리자, 장치 사용자 및 읽기 전용 사용자 계정 유형에 대한 사용자 이름, 암호 및 비활성 시간 제한를 구성합니다.

각 계정 유형에 부여된 권한에 대한 정보는 사용자 계정 유형을 참조하십시오.

옵션	인수	설명
-an -dn -rn	<관리자 이름> <장치 이름> <읽기 전용 이름>	각 계정 유형에 대해 대/소문자를 구분한 사용자 이름을 설정합니다. 최대 길이는 10자입니다.
-ap -dp -rp	<관리자 암호> <장치 암호> <읽기 전용 암호>	각 계정 유형에 대해 대/소문자를 구분한 암호를 설정합니다. 최대 길이는 32자입니다. 공백 암호(문자가 입력되지 않은 암호)는 허용되지 않습니다.
-t	<분>	비활성 사용자를 로그오프하기 전까지 시스템이 대기하는 시간을 구성합니다(기본값: 3분).

예 1: 관리자 사용자 이름을 XYZ로 변경하려면 다음을 입력합니다.

```
user -an XYZ
```

예 2: 로그오프 시간을 10분으로 변경하려면 다음을 입력합니다.

```
user -t 10
```

web

액세스: 관리자 전용

설명: HTTP 또는 HTTPS를 사용한 웹 인터페이스 액세스를 활성화합니다.

추가적인 보안을 위해 HTTP 및 HTTPS에 대한 포트 설정을 5000~32768 중에서 사용되지 않은 포트로 변경할 수 있습니다. 그런 다음 사용자는 브라우저 주소 필드에 콜론(:)을 사용하여 포트 번호를 지정해야 합니다. 예를 들어, 포트 번호가 5000이고 IP 주소가 152.214.12.114인 경우 다음을 입력합니다.

`http://152.214.12.114:5000`

옵션	인수	정의
-S	disable | http | https	웹 인터페이스에 대한 액세스를 구성합니다. HTTPS가 활성화되면 전송 중 데이터가 암호화되고 디지털 인증서에 의해 인증됩니다.
-ph	<http 포트 번호>	HTTP가 랙 PDU와 통신하는 데 사용하는 TCP/IP 포트를 지정합니다(기본값: 80).
-ps	<https 포트 번호>	HTTPS가 랙 PDU와 통신하는 데 사용하는 TCP/IP 포트를 지정합니다(기본값: 443).

예: 웹 인터페이스에 대한 모든 액세스를 차단하려면 다음을 입력합니다.

`web -S disable`

xferINI

액세스: 관리자 전용

설명: 직렬 연결을 통해 명령줄 인터페이스에 액세스하는 동안 XMODEM을 사용하여 INI 파일을 업로드합니다. 업로드가 완료된 후:

- 시스템 또는 네트워크가 변경된 경우 명령줄 인터페이스가 다시 시작되고, 사용자가 다시 로그인해야 합니다.
- 랙 PDU의 기본 전송 속도와 동일하지 않은 파일 전송 속도를 선택한 경우, 전송 속도를 기본값으로 초기화하여 랙 PDU와의 통신을 다시 설정해야 합니다.

xferStatus

액세스: 관리자 전용

설명: 마지막 파일 전송 결과를 표시합니다.

전송 결과 코드에 대한 설명은 업그레이드 및 업데이트 확인을 참조하십시오.

장치 명령어 설명

devLowLoad

액세스: 관리자, 장치 사용자

설명: 장치의 저부하 임계값을 kW 단위로 설정하거나 확인합니다.

예 1: 저부하 임계값을 확인하려면 다음을 입력합니다.

```
cli> devLowLoad
E000: Success
0.5 kW
```

예 2: 저부하 임계값을 1 kW로 설정하려면 다음을 입력합니다.

```
cli> devLowLoad 1.0
E000: Success
```

devNearOver

액세스: 관리자, 장치 사용자

설명: 장치의 과부하 예상 임계값을 kW 단위로 설정하거나 확인합니다.

예 1: 과부하 예상 임계값을 확인하려면 다음을 입력합니다.

```
cli> devNearOver
E000: Success
20.5 kW
```

예 2: 과부하 예상 임계값을 21.3 kW로 설정하려면 다음을 입력합니다.

```
cli> devNearOver 21.3
E000: Success
```

devOverLoad

액세스: 관리자, 장치 사용자

설명: 장치의 과부하 임계값을 kW 단위로 설정하거나 확인합니다.

예 1: 과부하 임계값을 확인하려면 다음을 입력합니다.

```
cli> devOverLoad
E000: Success
25.0 kW
```

예 2: 과부하 임계값을 25.5 kW로 설정하려면 다음을 입력합니다.

```
cli> devOverLoad 25.5
E000: Success
```

devReading

액세스: 관리자, 장치 사용자

설명: 장치의 총 전력(kW 단위) 또는 총 에너지(kW-hr 단위)를 확인합니다.

인수	정의
power	총 전력을 kW 단위로 표시
energy	총 에너지를 kW-hr 단위로 표시

예 1: 총 전력을 확인하려면 다음을 입력합니다.

```
cli> devReading power
E000: Success
5.2 kW
```

예 2: 총 에너지를 확인하려면 다음을 입력합니다.

```
cli> devReading energy
E000: Success
200.1 kWh
```

devStartDly

액세스: 관리자, 장치 사용자

설명: 랙 PDU에 전원이 인가된 후 각 출력의 Power On Delay에 추가할 초 단위 시간을 설정하거나 봅니다. 허용 값은 1~300 초 범위 또는 never (켜지 않음)입니다.

예 1: 콜드 스타트 지연을 보려면 다음을 입력합니다.

```
cli> devStartDly
E000: Success
5초
```

예 2: 콜드 스타트 지연을 6초로 설정하려면 다음을 입력합니다.

```
cli> devStartDly 6
E000: Success
```

humLow

액세스: 관리자, 장치 사용자

설명: 저습 임계값을 상대 습도의 백분율로 설정하거나 확인합니다.

예 1: 저습 임계값을 확인하려면 다음을 입력합니다.

```
cli> humLow
E000: Success
10 %RH
```

예 2: 저습 임계값을 설정하려면 다음을 입력합니다.

```
cli> humLow 12
E000: Success
```

humMin

액세스: 관리자, 장치 사용자

설명: 최저 습도 임계값을 상대 습도의 백분율로 설정하거나 확인합니다.

예 1: 최저 습도 한도를 확인하려면 다음을 입력합니다.

```
cli> humMin
E000: Success
6 %RH
```

예 2: 최저 습도 임계값을 설정하려면 다음을 입력합니다.

```
cli> humMin 8
E000: Success
```

humReading

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 센서에 감지된 습도값을 확인합니다.

예: 습도값을 확인하려면 다음을 입력합니다.

```
cli> humReading
E000: Success
25 %RH
```

inNormal

액세스: 관리자, 장치 사용자

설명: 각 드라이 접점 입력의 정상 상태를 확인합니다.

예: 각 드라이 접점 입력의 정상 상태를 확인하려면 다음을 입력합니다.

```
cli> inNormal
E000: Success
1: Open
2: Open
```

inReading

액세스: 관리자, 장치 사용자

설명: 각 드라이 접점 입력의 현재 상태를 확인합니다.

예: 각 드라이 접점 입력의 상태를 확인하려면 다음을 입력합니다.

```
cli> inReading
E000: Success
1: Open
2: Open
```

olAssignUsr

액세스: 관리자

설명: 출력 제어를 로컬 데이터베이스에 존재하는 출력 사용자에게 할당합니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록
<user>	로컬 데이터베이스에 존재하는 사용자 (userAdd를 참조하십시오.)

예 1: Bobby라는 이름의 사용자를 출력 3, 5~7 및 10에 할당하려면 다음을 입력합니다.

```
cli> olAssignUsr 3,5-7,10 bobby
E000: Success
```

예 2: Billy라는 이름의 사용자를 모든 출력에 할당하려면 다음을 입력합니다.

```
cli> olAssignUsr all billy
E000: Success
```

olCancelCmd

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 출력 또는 출력 그룹에 대해 보류 중인 모든 명령을 취소합니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록

예: 출력 3에 대한 모든 명령을 취소하려면 다음을 입력합니다.

```
cli> olCancelCmd 3
E000: Success
```

olDlyOff

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: Power Off Delay 이후 출력 또는 출력 그룹 해제(olOff 참조).

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록

예 1: 출력 3, 5~7 및 10을 해제하려면 다음을 입력합니다.

```
cli> olDlyOff 3,5-7,10
E000: Success
```

예 2: 모든 출력을 해제하려면 다음을 입력합니다.

```
cli> olDlyOff all
E000: Success
```

olDlyOn

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: Power On Delay 이후 출력 또는 출력 그룹 켜기(olOnDelay 참조).

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록

예 1: 출력 3, 5~7 및 10을 켜려면 다음을 입력합니다.

```
cli> olDlyOn 3,5-7,10
E000: Success
```

예 2: Outlet1의 구성 이름을 가진 출력을 켜려면 다음을 입력합니다.

```
cli> olDlyOn outlet1
E000: Success
```

olDlyReboot

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 출력 또는 출력 그룹에 공급되는 전원을 껐다 켭니다. 구성된 Power Off Delay에 따라 지정된 출력이 꺼집니다(olOffDelay 참조). 선택 출력 중 가장 긴 재부팅 기간(olRbootTime 참조)이 지난 후, 지정된 출력에 대해 설정된 Power On Delays 구성(olOnDelay 참조)에 따라 출력이 켜지기 시작합니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록

예 1: 출력 3, 5~7 및 10에 공급되는 전원을 껐다 켜려면 다음을 입력합니다.

```
cli> olDlyReboot 3,5-7,10
E000: Success
```

예 2: Outlet1의 구성 이름을 가진 출력에 공급되는 전원을 껐다 켜려면 다음을 입력합니다.

```
cli> olDlyReboot outlet1
E000: Success
```

olGroups

액세스: 관리자, 장치 사용자 및 출력 사용자

설명: 랙 PDU에 정의된 출력 동기화 그룹을 나열합니다. (자세한 내용은 출력 그룹 구성 및 제어을 참조하십시오.)

예: 출력 동기화 그룹을 나열하려면 다음을 입력합니다.

```
cli> olGroups
E000: Success
Outlet Group A:
159.215.6.141 -> Outlets: 2,4,5
159.215.6.143 -> Outlets: 2,8
Outlet Group B:
159.215.6.141 -> Outlets: 1
159.215.6.166 -> Outlets: 1
```

olLowLoad

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 출력 저부하 경고 임계값을 설정하거나 봅니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록
<전력>	새 출력 임계값(와트)

예 1: 모든 출력에 대해 저부하 임계값을 2 W로 설정하려면 다음을 입력합니다.

```
cli> olLowLoad all 2
E000: Success
```

예 2: 출력 3 및 5~7에 대한 저부하 임계값을 보려면 다음을 입력합니다.

```
cli> olLowLoad 3,5-7
E000: Success
3: BobbysServer: 2 W
5: BillysServer: 2 W
6: JoesServer: 2 W
7: JacksServer: 2 W
```

olName

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 출력에 대해 구성된 이름을 설정하거나 봅니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록
<newname>	특정 출력 이름. 문자 및 숫자만 사용하십시오.

예: 출력 3에 대한 이름을 BobbysServer로 구성하려면 다음을 입력합니다.

```
cli> olName 3 BobbysServer
E000: Success
3: BobbysServer
5: BillysServer
6: JoesServer
7: JacksServer
```

olNearOver

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 출력 과부하 예상 경고 임계값을 설정하거나 봅니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록
<전력>	새 출력 임계값(와트)

예 1: 출력 3 및 5~7에 대한 과부하 예상 임계값을 보려면 다음을 입력합니다.

```
cli> olNearOver 3,5-7
E000: Success
3: BobbysServer: 5 W
5: BillysServer: 6 W
6: JoesServer: 5 W
7: JacksServer: 4 W
```

예 2: 출력 3 및 5~7에 대한 과부하 예상 임계값을 6 W로 설정하려면 다음을 입력합니다.

```
cli> olNearOver 3,5-7 6
E000: Success
3: BobbysServer: 6 W
5: BillysServer: 6 W
6: JoesServer: 6 W
7: JacksServer: 6 W
```

olOff

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 지연 없이 출력 또는 출력 그룹을 해제합니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록

예 1: 출력 3 및 5~7을 해제하려면 다음을 입력합니다.

```
cli> olOff 3,5-7
E000: Success
```

olOffDelay

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: Off Delayed 명령(olDlyOff 참조) 및 Reboot Delayed 명령(olDlyReboot 참조)에 대한 시간 지연을 설정하거나 봅니다..

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록
<시간>	1~7200 초 범위 내의 지연 시간 (2시간).

예 1: 출력 3 및 5~7을 해제하기 위한 9초 지연을 설정하려면 다음을 입력합니다.

```
cli> olOffDelay 3,5-7 9
E000: Success
```

예 2: 출력 3 및 5~7에 대한 Off Delayed 명령의 지연을 보려면 다음을 입력합니다.

```
cli> olOffDelay 3,5-7
E000: Success
3: BobbysServer: 9 sec
5: BillysServer: 9 sec
6: JoesServer: 9 sec
7: JacksServer: 9 sec
```

olOn

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 지연 없이 출력 또는 출력 그룹을 켭니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록

예 1: 출력 3 및 5~7을 켜려면 다음을 입력합니다.

```
cli> olOn 3,5-7
E000: Success
```

olOnDelay

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: On Delayed 명령(olDlyOn 참조) 및 Reboot Delayed 명령(olDlyReboot 참조)에 대한 시간 지연을 설정하거나 봅니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록
<시간>	1~7200 초 범위 내의 지연 시간 (2시간).

예 1: 출력 3 및 5~7을 켜기 위한 6초 지연을 설정하려면 다음을 입력합니다.

```
cli> olOnDelay 3,5-7 6
E000: Success
```

예 2: 출력 3 및 5~7에 대한 On Delayed 명령의 지연을 보려면 다음을 입력합니다.

```
cli> olOnDelay 3,5-7
E000: Success
3: BobbysServer: 6 sec
5: BillysServer: 6 sec
6: JoesServer: 6 sec
7: JacksServer: 6 sec
```

olOverLoad

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 출력 과부하 경고 임계값을 설정하거나 봅니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록
<전력>	새 출력 임계값(와트)

예 1: 출력 3 및 5~7에 대한 과부하 임계값을 보려면 다음을 입력합니다.

```
cli> olOverLoad 3,5-7
E000: Success
3: BobbysServer: 7 W
5: BillysServer: 8 W
6: JoesServer: 7 W
7: JacksServer: 6 W
```

예 2: 출력 3 및 5~7에 대한 과부하 임계값을 7 W로 설정하려면 다음을 입력합니다.

```
cli> olOverLoad 3,5-7 7
E000: Success
3: BobbysServer: 7 W
5: BillysServer: 7 W
6: JoesServer: 7 W
7: JacksServer: 7 W
```

olRbootTime

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: Reboot Delayed 명령에 대해 출력이 꺼져 있는 시간을 설정하거나 봅니다 (olDlyReboot 참조).

예 1: 재부팅 중 출력 3 및 5~7이 꺼져 있도록 설정된 시간을 보려면 다음을 입력합니다.

```
cli> olRbootTime 3,5-7
E000: Success
3: BobbysServer: 4 sec
5: BillysServer: 5 sec
6: JoesServer: 7 sec
7: JacksServer: 2 sec
```

예 2: 재부팅 중 출력 3 및 5~7이 꺼져 있도록 할 시간을 설정하려면 다음을 입력합니다.

```
cli> olRebootTime 3,5-7 10
E000: Success
3: BobbysServer: 10 sec
5: BillysServer: 10 sec
6: JoesServer: 10 sec
7: JacksServer: 10 sec
```

olReading

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 출력 또는 출력 그룹에 대한 전류, 전력 또는 에너지를 봅니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록
current | power | energy	새 출력 임계값(와트)

예 1: 출력 3 및 5~7에 대한 전류를 보려면 다음을 입력합니다.

```
cli> olReading 3,5-7 current
E000: Success
3: BobbysServer: 4 A
5: BillysServer: 5 A
6: JoesServer: 7 A
7: JacksServer: 2 A
```

예 2: 출력 3에 대한 전력을 보려면 다음을 입력합니다.

```
cli> olReading 3 power
E000: Success
3: BobbysServer: 40 W
```

예 3: 출력 JoesServer에 대한 에너지를 보려면 다음을 입력합니다.

```
cli> olReading joesserver energy
E000: Success
6: JoesServer: 7.3 kWh
```

olReboot

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 지연 없이 출력 또는 출력 그룹에 공급되는 전원을 껐다 켭니다. 둘 이상의 출력이 지정된 경우, 이러한 출력이 함께 꺼졌다 켜집니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록

예: 출력 3 및 5~7을 재부팅하려면 다음을 입력합니다.

```
cli> olReboot 3,5-7
E000: Success
```

olStatus

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 지정된 출력의 상태를 봅니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록

예: 출력 3 및 5~7에 대한 상태를 보려면 다음을 입력합니다.

```
cli> olStatus 3,5-7
E000: Success
3: BobbysServer: On
5: BillysServer: Off
6: JoesServer: Off
7: JacksServer: On
```

olUnasgnUsr

액세스: 관리자

설명: 로컬 데이터베이스에 존재하는 출력 사용자로부터 출력 제어를 제거합니다.

인수	설명
all	모든 장치가 출력됩니다.
<출력 이름>	특정 출력에 대해 구성된 이름 (olName을 참조하십시오.)
<출력 번호>	단일 번호나 대시로 구분되는 번호 범위, 또는 콤마로 구분되는 단일 출력 번호와 번호 범위 목록
<user>	로컬 데이터베이스에 존재하는 사용자 (userList를 참조하십시오.)

예 1: Bobby라는 이름의 사용자를 출력 3, 5~7 및 10의 제어에서 제거하려면 다음을 입력합니다.

```
cli> olUnasgnUsr 3,5-7,10 bobby
E000: Success
```

예 2: Billy라는 이름의 사용자를 모든 출력의 제어에서 제거하려면 다음을 입력합니다.

```
cli> olUnasgnUsr all billy
E000: Success
```

phLowLoad

액세스: 관리자, 장치 사용자

설명: 위상 저부하 임계값을 kW 단위로 설정하거나 확인합니다. 위상을 지정하려면 다음 옵션을 선택합니다. 유형: **all**, 단상, 범위 또는 콤마로 구분된 위상 목록

예 1: 모든 위상에 대한 저부하 임계값을 1kW로 설정하려면 다음을 입력합니다

```
cli> phLowLoad all 1
E000: Success
```

예 2: 위상 1~3에 대한 저부하 임계값을 확인하려면 다음을 입력합니다.

```
cli> phLowLoad 1-3
E000: Success
1: 1 A
2: 1 A
3: 1 A
```

phNearOver

액세스: 관리자, 장치 사용자

설명: 위상 과부하 예상 임계값을 kW 단위로 설정하거나 확인합니다. 위상을 지정하려면 다음 옵션을 선택합니다. 유형: **all**, 단상, 범위 또는 콤마로 구분된 위상 목록

예 1: 모든 위상에 대한 과부하 예상 임계값을 10kW로 설정하려면 다음을 입력합니다

```
cli> phNearOver all 10
E000: Success
```

예 2: 위상 1~3에 대한 과부하 예상 임계값을 확인하려면 다음을 입력합니다.

```
cli> phNearOver 1-3
E000: Success
1: 10 A
2: 10 A
3: 10 A
```

phOverLoad

액세스: 관리자, 장치 사용자

설명: 위상 과부하 임계값을 kW 단위로 설정하거나 확인합니다. 위상을 지정하려면 다음 옵션을 선택합니다. 유형: **all**, 단상, 범위 또는 콤마로 구분된 위상 목록

예 1: 모든 위상에 대한 과부하 임계값을 13kW로 설정하려면 다음을 입력합니다

```
cli> phOverLoad all 13
E000: Success
```

예 2: 위상 1~3에 대한 과부하 임계값을 확인하려면 다음을 입력합니다.

```
cli> phOverLoad 1-3
E000: Success
1: 13 A
2: 13 A
3: 13 A
```

phReading

액세스: 관리자, 장치 사용자

설명: 위상에 대한 전류, 전압 또는 전력을 확인합니다. 위상 과부하 예상 임계값을 kW 단위로 설정하거나 확인합니다. 위상을 지정하려면 다음 옵션을 선택합니다. 유형: **all**, 단상, 범위 또는 콤마로 구분된 위상 목록

예 1: 위상 3에 대한 전류 측정값을 확인하려면 다음을 입력합니다.

```
cli> phReading 3 current
E000: Success
3: 4 A
```

예 2: 각 위상에 대한 전압을 확인하려면 다음을 입력합니다.

```
cli> phReading all voltage
E000: Success
1: 120 V
2: 120 V
3: 120 V
```

예 3: 위상 2에 대한 전력을 확인하려면 다음을 입력합니다.

```
cli> phReading 2 power
E000: Success
2: 40 W
```

phRestrictn

액세스: 관리자

설명: 과부하 경보 임계값이 위반되었을 때 출력이 켜지지 않게 하는 과부하 제한 기능을 설정하거나 봅니다. 허용 가능한 인수로는 **none**, **near** 및 **over**가 있습니다. 위상을 지정하려면 다음 옵션 중에서 선택합니다. 유형: **all**, 단상, 일정 범위 또는 쉼표로 구분된 위상 목록.

예 1: 위상 3에 대한 과부하 제한을 none으로 설정하려면 다음을 입력합니다.

```
cli> phRestrictn 3 none
E000: Success
```

예 2: 모든 위상의 과부하 제한을 보려면 다음을 입력합니다.

```
cli> phRestrictn all
E000: Success
1: over
2: near
3: none
```

prodInfo

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 랙 PDU에 대한 정보를 확인합니다.

예:

```
cli> prodInfo
E000: Success
AOS vX.X.X.X
관리 랙 PDU vX.X.X.X
Model:              DELL6xxx
Present Outlets:    12
Switched Outlets:   12
Metered Outlets:    0
Max Current:        20 A
Phases:             1
```

sensorName

액세스: 관리자, 장치 사용자

설명: 랙 PDU 온도/습도 센서 포트에 할당된 이름을 설정하거나 봅니다.

예 1: 포트 이름을 “Sensor1”로 설정하려면 다음을 입력합니다.

```
cli> sensorName Sensor1
E000: Success
```

예 2: 그런 다음 센서 포트에 대한 이름을 보려면 다음을 입력합니다.

```
cli> sensorName
E000: Success
Sensor1
```

tempHigh

액세스: 관리자, 장치 사용자

설명: 고온 임계값을 화씨(F) 또는 섭씨(C) 단위로 설정하거나 표시합니다.

예 1: 고온 임계값을 70ºF로 설정하려면 다음을 입력합니다.

```
cli> tempHigh F 70
E000: Success
```

예 2: 고온 임계값을 섭씨(C) 단위로 표시하려면 다음을 입력합니다.

```
cli> tempHigh C
E000: Success
21 C
```

예 3: 고온 임계값을 화씨(F) 단위로 표시하려면 다음을 입력합니다.

```
cli> tempHigh F
E000: Success
70 F
```

tempMax

액세스: 관리자, 장치 사용자

설명: 최대 온도 임계값을 화씨(F) 또는 섭씨(C) 단위로 설정하거나 표시합니다.

예 1: 최대 온도 임계값을 80ºF로 설정하려면 다음을 입력합니다.

```
cli> tempMax F 80
E000: Success
```

예 2: 최대 온도 임계값을 섭씨(C) 단위로 표시하려면 다음을 입력합니다.

```
cli> tempMax C
E000: Success
27 C
```

예 3: 최대 온도 임계값을 화씨(F) 단위로 표시하려면 다음을 입력합니다.

```
cli> tempMax F
E000: Success
80 F
```

tempReading

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 센서에 감지된 온도 값을 화씨(F) 또는 섭씨(C) 단위로 표시합니다.

예: 온도 값을 화씨(F) 단위로 표시하려면 다음을 입력합니다.

```
cli> tempReading F
E000: Success
51.1 F
```

userAdd

액세스: 관리자

설명: 로컬 사용자 데이터베이스에 출력 사용자를 추가합니다.

예: Bobby라는 이름의 사용자를 추가하려면 다음을 입력합니다.

```
cli> userAdd Bobby
E000: Success
```

userDelete

액세스: 관리자

설명: 로컬 사용자 데이터베이스에서 출력 사용자를 제거합니다.

예: Bobby라는 이름의 사용자를 제거하려면 다음을 입력합니다.

```
cli> userDelete Bobby
E000: Success
```

userList

액세스: 관리자, 장치 사용자 및 출력 사용자, 그러나 사용자에게 할당된 출력만 해당.

설명: 사용자 및 사용자에게 할당된 출력을 나열합니다.

예 1: 관리자로 로그인한 경우 다음을 입력합니다.

```
cli> userList
E000: Success
Local: admin: 1,2,3,4,5,6,7,8
Local: Bobby: 1,3
Local: Billy: 2,5
Local: Joe: 4,6
Local: Jack: 7,8
```

예 2: Billy로 로그인한 경우 다음을 입력합니다.

```
cli> userList
E000: Success
Local: Billy: 2,5
```

userPasswd

액세스: 관리자.

설명: 출력 사용자의 암호를 설정합니다.

예: Bobby의 암호를 "abc123"으로 설정하려면 다음을 입력합니다.

```
cli> userPasswd Bobby abc123 abc123
E000: Success
```

whoami

액세스: 관리자, 장치 사용자, 출력 사용자

설명: 활성 사용자의 사용자 이름을 표시합니다.

예:

```
cli> whoami
E000: Success
admin
```

웹 인터페이스

지원되는 웹 인터페이스

Microsoft® Internet Explorer®(IE) 7.x 이상(Windows® 운영 체제만 해당) 또는 Mozilla® Firefox® 3.0.6 이상(모든 운영 체제)을 사용하여 웹 인터페이스를 통해 랙 PDU에 액세스할 수 있습니다. 일반적으로 사용하는 다른 브라우저는 작동할 수는 있지만 완전한 테스트를 거치지는 않았습니다.

랙 PDU는 프록시 서버와 함께 사용할 수 없습니다. 랙 PDU의 웹 브라우저를 사용하여 웹 인터페이스에 액세스하기 전에 다음 중 하나를 수행해야 합니다.

- 웹 브라우저가 랙 PDU의 프록시 서버를 사용하지 못하도록 웹 브라우저를 구성합니다.
- 프록시 서버가 랙 PDU의 특정 IP 주소에 접근하지 못하도록 프록시 서버를 구성합니다.

웹 인터페이스에 로그온

개요

랙 PDU의 DNS 이름 또는 시스템 IP 주소를 웹 인터페이스의 URL 주소로 사용할 수 있습니다. 대소문자를 구분한 사용자 이름과 암호로 로그온합니다. 기본 사용자 이름 및 암호는 계정 유형에 따라 다릅니다.

- 관리자의 경우 admin/admin
- 장치 사용자의 경우 device/device
- 읽기 전용 사용자의 경우 readonly/readonly

출력 사용자 계정의 경우, 기본 사용자 이름 또는 암호가 없습니다. 관리자는 사용자 이름, 암호 및 출력 사용자의 다른 계정 특성을 지정해야 합니다. 출력 사용자 구성을 참조하십시오.

HTTPS(SSL/TLS)를 액세스 프로토콜로 사용하는 경우 로그인 자격 증명이 서버 인증서의 정보와 비교됩니다. Security Wizard를 통해 인증서가 생성되고 IP 주소가 인증서에서 공통 이름으로 지정된 경우, 이 IP 주소를 사용하여 랙 PDU에 로그온해야 합니다. DNS 이름이 인증서에서 공통 이름으로 지정된 경우 DNS 이름을 사용하여 로그온해야 합니다.

웹 인터페이스에 로그온할 때 표시되는 웹 페이지에 대한 자세한 내용은 Home 탭 정보를 참조하십시오.

URL 주소 형식

웹 브라우저의 URL 주소 필드에 랙 PDU의 DNS 이름 또는 IP 주소를 입력하고 ENTER를 누릅니다. Internet Explorer에서 기본 이외의 웹 서버 포트를 지정할 경우 URL에 **http://** 또는 **https://**를 포함시켜야 합니다.

로그온 시 공통 브라우저 오류 메시지

오류 메시지	오류 원인	브라우저
“You are not authorized to view this page" 또는 "Someone is currently logged in..."	다른 사용자가 로그온되어 있습니다.	Internet Explorer, Firefox
"This page cannot be displayed."	웹 액세스가 거부되었거나 URL이 올바르지 않습니다.	Internet Explorer
"Unable to connect."		Firefox

URL 형식 예.

- Web1의 DNS 이름의 경우:
  - HTTP가 액세스 모드인 경우 **http://Web1**
  - HTTPS가 액세스 모드인 경우 **https://Web1**
- 시스템 IP 주소가 139.225.6.133이고 기본 웹 서버 포트(80)인 경우:
  - HTTP가 액세스 모드인 경우 **http://139.225.6.133**
  - HTTPS(SSL이 있는 HTTP)가 액세스 모드인 경우 **https://139.225.6.133**.
- 시스템 IP 주소가 139.225.6.133이고 기본이 아닌 웹 서버 포트(5000)인 경우:
  - HTTP가 액세스 모드인 경우 **http://139.225.6.133:5000**
  - HTTPS(SSL이 있는 HTTP)가 액세스 모드인 경우 **https://139.225.6.133:5000**.
- 시스템 IPv6 주소가 2001:db8:1::2c0:b7ff:fe00:1100이고 기본이 아닌 웹 서버 포트(5000)의 경우:
  - HTTP가 액세스 모드인 경우 **http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000**.

웹 인터페이스 기능

다음을 읽어 랙 PDU의 기본적인 웹 인터페이스 기능을 숙지하십시오.

탭

다음과 같은 탭을 사용할 수 있습니다.

- Home: 로그온할 때 나타납니다. 활성 알람, 랙 PDU의 부하 상태, 가장 최근 랙 PDU 이벤트를 표시합니다. 자세한 내용은 Home 탭 정보를 참조하십시오.
- Device Manager: 연결된 모든 장치, 위상 및 출력에 대한 부하 상태를 확인하고, 부하 임계값을 구성하고, 최고 부하 측정을 확인 및 관리합니다. 출력을 관리하고 제어합니다.자세한 내용은 Device Manager 탭 정보을 참조하십시오.
- Environment: 랙 PDU에 센서가 연결된 경우 온도와 습도 센서 데이터를 확인합니다.
- Logs: 이벤트, 데이터 및 시스템 로그를 표시합니다.
- Administration: 보안, 네트워크 연결, 알림 및 일반 설정을 구성합니다.

장치 상태 아이콘

하나 이상의 아이콘과 함께 표시된 텍스트는 랙 PDU의 현재 작동 상태를 나타냅니다.

	Critical: 위험 알람이며 바로 조치를 취해야 합니다.
	Warning: 주의가 필요한 알람으로, 원인을 해결하지 않을 경우 데이터 또는 장치가 손상될 수 있습니다.
	No Alarms: 발생된 알람이 없으며 랙 PDU가 정상적으로 작동합니다.

웹 인터페이스에서 매 페이지의 오른쪽 상단 모서리에는 랙 PDU 상태를 보고하기 위해 현재 Home 페이지에 표시된 것과 동일한 아이콘에 표시됩니다.

- 알람이 존재하지 않는 경우 No Alarms 아이콘이 나타납니다.
- 알람이 있는 경우 Critical 및 Warning 중 하나나 둘 다 나타나고, 각 아이콘 다음에 활성 알람의 심각도를 나타내는 번호가 표시됩니다.

활성 알람을 포함한 랙 PDU 상태 요약을 보기 위해 Home 페이지로 돌아가려면 인터페이스의 모든 페이지에서 빠른 상태 참조 아이콘을 클릭합니다.

빠른 링크

인터페이스의 왼쪽 하단에는 3개의 구성 가능한 링크가 있습니다. 기본 설정은 다음과 같습니다.

- Link 1: dell.com
- Link 2: dell.com/home
- Link 3: dell.com/business

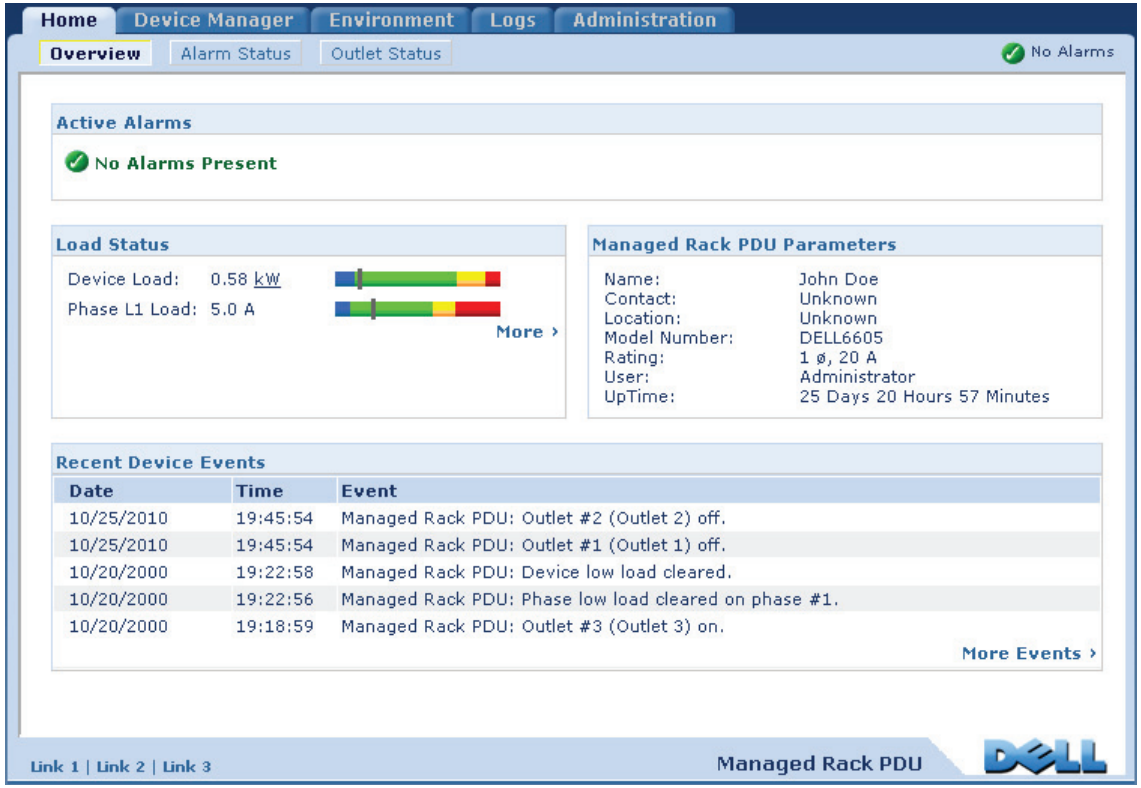
 링크를 재구성하려면 링크 구성을 참조하십시오.

기타 웹 인터페이스 기능

- 왼쪽 상단 모서리에 IP 주소가 나타납니다.
- 상황별 Help 링크와 Log off 링크가 오른쪽 상단 모서리에 있습니다.

Home 탭 정보

Home 탭에서는 활성 경보, 랙 PDU의 부하 상태 및 최근 랙 PDU 이벤트 정보를 확인합니다.

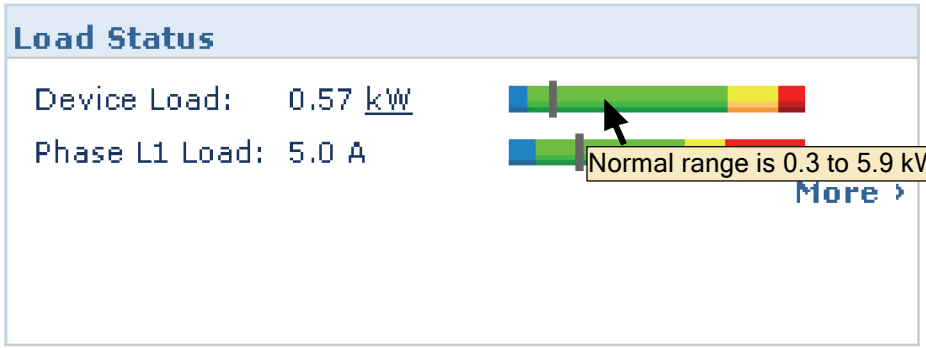


개요 보기

경로: Home > Overview

Overview의 맨 위에 알람 상태가 표시됩니다. 알람이 하나 이상 발생된 경우, 알람의 수와 유형이 Alarm Status 보기로 연결되는 링크와 함께 표시됩니다. 제공된 링크에서 각 알람에 대한 설명을 볼 수 있습니다. 발생된 알람이 없으면 Overview에 "No Alarms Present"가 표시됩니다.

Load Status 영역에 해당 상황에 따라 장치의 부하(kW 단위)와 위상의 부하(암페어 단위)가 표시됩니다. 녹색, 노란색 및 빨간색 계량기는 현재 부하 상태를 정상, 과부하 예상 또는 과부하 등 세 가지 상태로 보여줍니다. 저부하 임계값이 구성된 경우, 미터에는 녹색 왼쪽에 파란색 세그먼트도 포함됩니다. 색상 위로 마우스를 가져가면 구성된 부하 임계값이 표시됩니다.



임계값을 구성하고 최고 부하 정보를 확인하고 관리하려면 More를 클릭하여 Device Manager 탭으로 이동합니다.

장치 매개변수 영역에서는 랙 PDU에 액세스하는 사용자 계정의 이름, 연락처, 위치, 현재 등급, 유형, 그리고 전원 껐다 켜기 또는 관리 인터페이스 재부팅을 통해 마지막으로 재부팅한 후 랙 PDU 작동 시간 등의 정보를 확인합니다. (자세한 내용은 랙 PDU 재설정을 참조하십시오.)

Recent Device Events 영역에는 가장 최근에 발생한 순으로 이벤트와 해당 이벤트가 발생한 날짜와 시간이 표시됩니다. 한번에 최대 5가지 이벤트를 표시할 수 있습니다. 전체 이벤트 로그를 보려면 More Events를 클릭하여 Logs 탭으로 이동합니다.

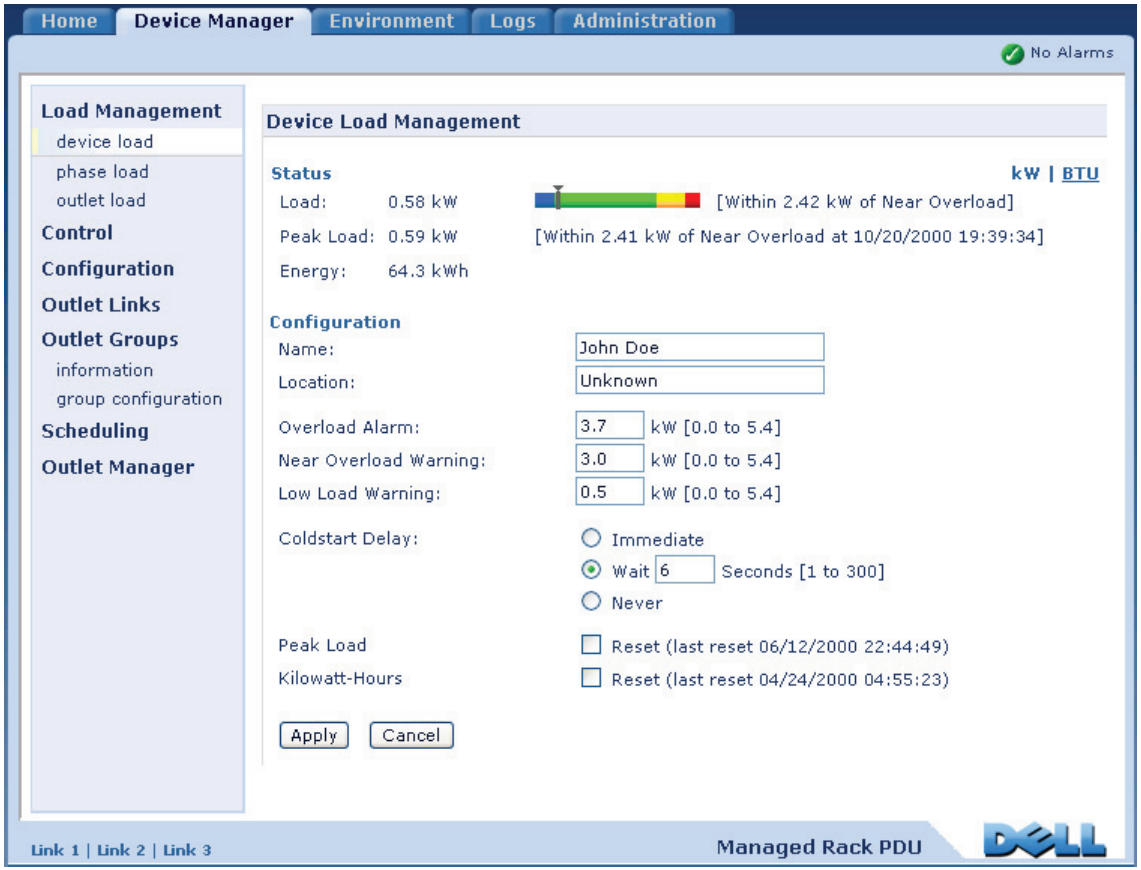
알람 상황 보기

경로: Home > Alarm Status

Alarm Status 보기는 존재하는 모든 알람에 대한 설명을 제공합니다.

온도 또는 습도 임계값 위반에 대한 자세한 내용을 보려면 Environment 탭을 클릭하십시오.

장치 관리


Home
Device Manager
Environment
Logs
Administration
No Alarms
Load Management
device load
phase load
outlet load
Control
Configuration
Outlet Links
Outlet Groups
information
group configuration
Scheduling
Outlet Manager
Device Load Management
Status
kW | BTU
Load: 0.58 kW
[Within 2.42 kW of Near Overload]
Peak Load: 0.59 kW
[Within 2.41 kW of Near Overload at 10/20/2000 19:39:34]
Energy: 64.3 kWh
Configuration
Name: John Doe
Location: Unknown
Overload Alarm: 3.7 kW [0.0 to 5.4]
Near Overload Warning: 3.0 kW [0.0 to 5.4]
Low Load Warning: 0.5 kW [0.0 to 5.4]
Coldstart Delay:
Immediate
Wait 6 Seconds [1 to 300]
Never
Peak Load
Reset (last reset 06/12/2000 22:44:49)
Kilowatt-Hours
Reset (last reset 04/24/2000 04:55:23)
Apply
Cancel
Link 1 | Link 2 | Link 3
Managed Rack PDU

Device Manager 탭 정보

경로: Device Manager

Device Manager 탭을 사용하여 다음 작업을 수행합니다.

- 랙 PDU의 부하 상태 보기
- 연결된 모든 장치 및 해당 위상에 대한 부하 한도 구성
- 출력 관리 및 제어
- 랙 PDU에 대한 이름과 위치 구성
- 최고 부하 측정값 확인 및 관리
- 사용자 구성 가능한 링크를 클릭하여 랙 PDU에 연결된 특정 장치에 대한 웹 페이지를 엽니다.

부하 상태 및 최고 부하 보기

경로: Device Manager > *Load Management 옵션*

녹색, 노란색 및 빨간색 미터의 표시기는 현재 부하 상태를 나타냅니다. 정상, 과부하 예상 또는 과부하 등 세 가지 상태로 보여줍니다. 저부하 임계값으로 구성했을 때는 계량기에서 녹색 왼쪽에 파란색 세그먼트가 나타납니다. Device Load 화면에서 미터 위의 삼각형은 최고 부하를 나타냅니다.

상단 오른쪽 모서리에 있는 kW | BTU를 클릭하여 킬로와트와 BTU (British Thermal Units) 사이에서 부하 값을 전환합니다.

부하 한도 구성

경로: Device Manager > *Load Management options*

부하 임계값을 구성하려면:

1. Device Manager 탭을 클릭합니다.
2. 장치 또는 위상에 대한 부하 한도를 구성하려면 Load Management 메뉴에서 항목을 선택합니다.
3. Overload Alarm, Near Overload Warning 및 Low Load Warning 한도를 설정합니다.
4. Apply를 클릭합니다.

랙 PDU의 이름과 위치 구성

경로: Device Manager > Load Management > Device Load

입력하는 이름과 위치가 Home 탭에 나타납니다.

Device Manager 탭 또는 Administration 탭을 통해 이름과 위치를 설정할 수 있습니다. 한 가지를 변경하면 나머지에도 영향을 줍니다.

1. Device Manager 탭을 클릭한 후 Load Management 메뉴에서 device load를 클릭합니다.
2. 이름과 위치를 입력합니다.
3. Apply를 누릅니다.

콜드 스타트 지연 설정

경로: Device Manager > Device Load

콜드 스타트 지연은 랙 PDU에 전원이 인가된 후 출력이 켜지기까지 각 출력의 Power On Dealy에 추가되는 초 단위 시간입니다. 허용 값은 1~300 초, Immediate 또는 Never(켜지 않음)입니다.

1. Device Manager 탭을 클릭한 후 Load Management 메뉴에서 device load를 클릭합니다.
2. Coldstart Delay에 대한 항목을 선택합니다.
3. Apply를 누릅니다.

최고 부하 및 kWh 초기화

경로: Device Manager > Device Load

1. Device Manager 탭을 클릭한 후 Load Management 메뉴에서 device load를 클릭합니다.
2. 필요에 따라 Peak Load 및 Kilowatt-Hours 확인란을 클릭합니다.
3. Apply를 누릅니다.

출력 그룹 구성 및 제어

출력 그룹 용어

*출력 그룹*은 동일한 랙 PDU에서 논리적으로 함께 연결된 출력으로 구성됩니다. 출력 그룹에 있는 출력은 동기화된 방식으로 켜지고, 꺼지고, 재부팅됩니다.

- *로컬 출력 그룹*은 랙 PDU에 있는 둘 이상의 출력으로 구성됩니다. 해당 그룹에 있는 출력만 동기화됩니다.
- *글로벌 출력 그룹*은 랙 PDU에 있는 하나 이상의 출력으로 구성됩니다. 하나의 출력은 출력 그룹을 최대 3개의 다른 랙 PDU에 있는 출력 그룹에 논리적으로 연결시키는 *글로벌 출력*으로 구성됩니다. 연결된 글로벌 출력 그룹의 모든 출력은 동기화됩니다.
  - 글로벌 출력 그룹의 경우, *시작 UPS 출력 그룹*은 조치를 내리는 그룹입니다.
  - 글로벌 출력 그룹의 경우, *종속 출력 그룹*은 시작 UPS 출력 그룹과 동기화되는 다른 모든 출력 그룹입니다.

출력 그룹의 구성원인 출력에 출력 제어 작업을 적용하면 출력이 다음과 같이 동기화됩니다.

- 글로벌 출력 그룹의 경우, 시작 UPS 출력 그룹의 글로벌 그룹에 대해 구성된 지연 기간 및 재부팅 기간을 사용합니다.
- 로컬 출력 그룹의 경우, 출력은 그룹에서 가장 낮은 번호를 가진 출력의 지연 기간과 재부팅 기간을 사용합니다.

출력 그룹의 목적과 이점

랙 PDU에서 동기화된 출력 그룹을 사용하면 출력을 동기화된 방식으로 켜고, 끄고, 재부팅할 수 있습니다. 출력 그룹을 통해 제어 그룹 작업을 동기화하면 다음과 같은 이점이 있습니다.

- 이중 코드 서버의 전원 공급장치에 대한 동기화된 방식의 셧다운과 시동을 통해 계획된 시스템 셧다운이나 재부팅 중에 전원 공급장치 장애가 잘못 보고되는 것을 방지합니다.
- 출력 그룹을 사용하여 출력을 동기화하면 개별 출력의 지연 기간에 의존하는 것보다 셧다운과 재시작 타이밍의 정확도가 향상됩니다.
- 글로벌 출력은 연결된 모든 랙 PDU의 사용자 인터페이스에 표시됩니다.

출력 그룹의 시스템 요구 사항

동기화된 출력 제어 그룹을 설정하고 사용하려면:

- 컴퓨터와 공유되지 않는 전원을 사용하는 이더넷 허브나 스위치 또는 동기화되는 기타 장치를 포함하여 10/100Base-T TCP/IP 네트워크가 필요합니다.
- 출력 그룹이 다수의 랙 PDU에 걸쳐 동기화되는 경우, 이러한 랙 PDU는 다음 요구 사항을 충족해야 합니다.
  - 동일 서브넷에 있어야 합니다.
  - 운영 체제(AOS) 모듈 및 응용 프로그램 모듈과 동일한 버전 번호를 가진 펌웨어를 사용해야 합니다.
- 웹 인터페이스, 랙 PDU의 명령줄 인터페이스 또는 SNMP를 통해 동기화된 제어 작업을 시작할 수 있는 컴퓨터가 필요합니다.
- 동기화하는 출력 그룹은 멀티캐스트 IP 주소가 동일해야 합니다. 랙 PDU를 연결하는 각 이더넷 스위치는 해당 멀티캐스트 IP 주소에 대한 멀티캐스트 네트워크 트래픽을 허용해야 합니다.

출력 그룹 구성을 위한 규칙

출력 그룹을 사용하는 시스템의 경우, 다음 규칙이 적용됩니다.

- 랙 PDU는 두 개 이상의 출력 그룹을 가질 수 있지만, 출력은 하나의 출력 그룹에만 속할 수 있습니다.
- 글로벌 출력이 없는 로컬 출력 그룹은 두 개 이상의 출력으로 구성되어야 합니다.
- 하나의 랙 PDU에 있는 글로벌 출력 그룹를 다른 3개의 랙 PDU 각각에 있는 글로벌 출력 그룹과 동기화시킬 수 있습니다.
  - 글로벌 출력 그룹에서 하나의 출력만 글로벌 출력으로 지정하여 동기화 목적으로 다른 랙 PDU의 출력 그룹에 연결할 수 있습니다. 해당 글로벌 출력은 그룹에서 유일한 출력이거나 그룹에 여러 개의 출력이 있을 수 있습니다.
  - 동기화를 위해 랙 PDU의 출력 그룹을 연결하려면 해당 랙 PDU가 동일한 장치 멀티캐스트 이름 및 장치 멀티캐스트 주소를 가져야 하며 동일 버전의 랙 PDU 펌웨어를 실행해야 합니다.
  - 한 출력 그룹의 글로벌 출력은 연결된 다른 출력 그룹의 글로벌 출력과 동일한 물리적 출력 수를 가져야 합니다.
- 출력 그룹을 만들고 구성하려면 웹 인터페이스를 사용하거나 구성된 랙 PDU에서 구성 파일(.ini 파일) 설정을 내보내야 합니다. 명령줄 인터페이스에서 출력이 출력 그룹의 구성원인지 여부를 표시하고 출력 그룹에 제어 작업을 적용할 수 있지만 명령줄 인터페이스에서 출력 그룹을 설정하거나 구성하지는 못합니다.

출력 그룹 활성화

Device Manager 탭을 클릭하고 Outlet Groups 왼쪽 탐색 메뉴에서 Group Information 을 선택합니다. 다음 매개변수를 구성하고 Apply를 클릭합니다.

출력 그룹의 생성 활성화.

매개변수	설명
Device Level Outlet Group	출력 그룹을 만들려면 이 매개변수를 활성화시켜야 합니다. 이 매개변수는 기본적으로 비활성화됩니다.

글로벌 출력 그룹(연결된 그룹)에 대한 지원을 활성화합니다.

매개변수	설명
Multicast Name	다수의 랙 PDU에 있는 출력 그룹을 연결하려면 해당 각 랙 PDU에서 동일한 멀티캐스트 이름 및 멀티캐스트 IP 주소를 정의해야 합니다. **참고:** 동일 멀티캐스트 이름 및 멀티캐스트 IP 주소로 최대 4개의 장치를 구성할 수 있습니다.
Multicast IP	

출력 그룹의 암호화 및 인증 활성화.

매개변수	설명
Authentication Phrase	장치가 다른 장치와 통신하고, 전송 과정에서 메시지가 변경되지 않으며, 메시지가 시기 적절하게 전달된다는 것을 확인시켜주는 15~32 ASCII 문자의 구문입니다. 인증 구문은 메시지가 지연되지 않았고, 복사되지 않았으며, 이후 적정하지 않은 시기에 다시 전송되지 않는다는 것을 나타냅니다.
Encryption Phrase	데이터의 기밀 유지를 보장하는 15~32 ASCII 문자의 구문입니다(암호화를 통한).

출력 그룹 포트 설정.

매개변수	설명
Outlet Group Port	장치가 다른 장치와 통신할 때 사용하는 포트 번호입니다.

다른 장치의 출력 그룹과 동기화하려는 장치는 모두 동일한 인증 문구, 암호화 문구 및 그룹 포트 번호를 가져야 합니다. 이 값은 사용자에게 숨겨집니다.

로컬 출력 그룹 만들기

1. Device Manager 탭의 Outlet Groups 왼쪽 탐색 메뉴에서 Information을 선택합니다.
2. 출력 그룹이 활성화되도록 합니다. (출력 그룹 활성화을 참조하십시오.)
3. Create Local Outlet Group을 클릭합니다.
4. Select Local Outlets 아래에서 그룹에 속할 각 출력을 선택하고 Outlet Group Name 필드에서 그룹 이름을 지정합니다. 최소 두 개의 출력을 선택해야 합니다.

여러 글로벌 출력 그룹 만들기

다른 랙 PDU의 출력 그룹과 연결되는 여러 글로벌 출력 그룹을 설정하려면:

1. Device Manager 탭의 Outlet Groups 왼쪽 탐색 메뉴에서 Information을 선택합니다.
2. 출력 그룹이 활성화되었고 연결시킬 모든 랙 PDU에 대해 멀티캐스트 매개변수(이름 및 IP 주소)가 동일한지 확인합니다. (출력 그룹 활성화을 참조하십시오.)
3. Create Global Outlet Groups을 클릭합니다.
4. 만드는 각 글로벌 출력 그룹에 대해 해당 확인란을 클릭하여 출력을 선택합니다. 그런 다음 Apply를 클릭합니다. 예를 들어, 5개의 출력을 선택하여 각각 하나의 글로벌 출력을 가진 5개의 출력 그룹을 만듭니다.
5. 만든 글로벌 출력 그룹에 출력을 추가하려면 출력 그룹 편집 또는 삭제를 참조하십시오.

출력 그룹 편집 또는 삭제

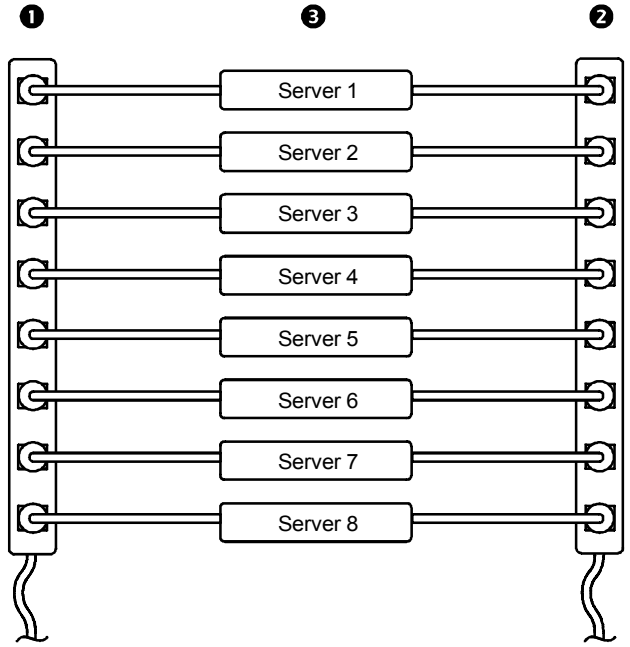
1. Device Manager 탭의 Outlet Groups 왼쪽 탐색 메뉴에서 Information을 선택합니다.
2. Configured Outlet Groups 아래에서 편집 또는 삭제할 출력 그룹의 번호나 이름을 클릭합니다.
3. 출력 그룹을 편집할 때 다음 작업을 수행할 수 있습니다.
   - 출력 그룹의 이름을 변경합니다.
   - 확인란을 클릭하여 체크를 표시 또는 제거하는 식으로 출력을 추가 또는 제거합니다.

   남은 출력이 글로벌 출력인 경우를 제외하고 두 개의 출력만 포함한 출력 그룹에서는 출력을 제거할 수 없습니다.

4. 출력 그룹을 삭제하려면 Delete Outlet Group을 클릭합니다.

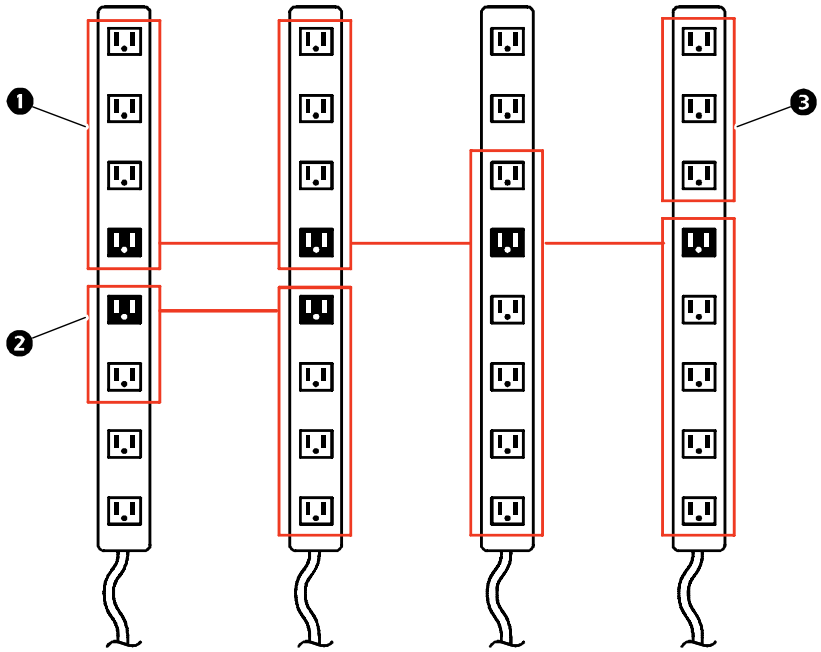
일반적인 출력 그룹 구성

다음 구성은 각각 8개의 출력 그룹을 가진 두 개의 랙 PDU를 나타냅니다. 각 출력 그룹에는 하나의 글로벌 출력이 있습니다. 첫 번째 랙 PDU에서 각 출력 그룹 ❶은 두 번째 랙 PDU에서 동일한 위치에 있는 출력 그룹 ❷에 연결됩니다. 이중 코드 서버 ❸의 한 전원 코드는 첫 번째 랙 PDU의 각 출력에 연결되고, 다른 코드는 두 번째 랙 PDU의 해당 출력에 연결되어 두 전원에서 서버로의 출력이 출력 제어 작업에 반응하여 동기화된 방식으로 켜지거나 꺼지게 됩니다.



다음 구성은 동기화된 3개의 출력 세트를 나타냅니다. 글로벌 출력은 검정색으로 표시됩니다. 출력 그룹은 빨간색 직사각형으로 표시됩니다.

❶	이러한 4개의 글로벌 출력 그룹은 총 19개의 출력을 동기화합니다.
❷	이러한 두 글로벌 출력 그룹은 한 그룹에서 2개와 다른 그룹에서 4개로 총 6개의 출력을 동기화합니다.
❸	이 로컬 출력 그룹은 동일한 랙 PDU에서 3개의 출력을 동기화합니다.



글로벌 출력 그룹에 대한 설정과 구성 확인

설정이 출력 그룹에 대한 모든 시스템 요구 사항을 충족하는지, 그리고 출력 그룹이 올바르게 구성됐는지 확인하려면 웹 인터페이스의 Outlet Groups 왼쪽 탐색 메뉴에서 Information을 선택하여 그룹 및 그룹의 연결 정보를 표시합니다.

- Configured Outlet Groups 섹션에 다음 정보가 표시됩니다.
  - 현재 랙 PDU에서 구성된 모든 출력 그룹.
  - 각 그룹의 출력 번호별 출력.
  - 글로벌 출력 그룹이 동기화되는 다른 랙 PDU의 출력 그룹. 각 랙 PDU는 IP 주소로 식별되고 각 글로벌 출력은 굵은 문자로 표시됩니다.
- Global Outlet Overview 섹션에 다음 정보가 표시됩니다.
  - 현재 랙 PDU의 IP 주소.
  - 다른 랙 PDU의 출력 그룹과 동기화에 사용 가능한 글로벌 출력을 포함한 랙 PDU의 IP 주소.
  - 현재 랙 PDU의 출력 그룹과 동기화되는지 여부와 관계 없이 랙 PDU에서 구성된 모든 글로벌 출력.

출력 및 출력 그룹에 대한 출력 설정

제어 작업 실행

출력 또는 출력 그룹에 출력 제어 작업을 적용하는 경우, 작업에 다음 지연이 사용됩니다.

- 개별 출력(출력 그룹이 아님)에 대해 작업은 해당 출력에 구성된 지연 기간과 재부팅 기간을 사용합니다.
- 글로벌 출력 그룹의 경우, 작업은 글로벌 출력에 구성된 지연 기간과 재부팅 기간을 사용합니다.
- 로컬 출력 그룹의 경우, 작업은 그룹에서 가장 낮은 번호를 가진 출력에 구성된 지연 기간을 사용합니다.

랙 PDU에서 출력을 제어하려면:

1. Device Manager 탭의 왼쪽 탐색 메뉴에서 Control을 선택합니다.
2. 제어할 각 개별 출력 또는 출력 그룹에 대한 확인란을 표시하거나 All Outlets 확인란을 선택합니다.
3. 목록에서 Control Action을 선택하고 Next >>를 클릭합니다. 작업을 설명하는 확인 페이지에서 작업을 적용 또는 취소합니다.

선택할 수 있는 제어 작업.

옵션	설명
No Action (웹 인터페이스 전용)	아무것도 행하지 않습니다.
On Immediate	선택한 출력에 전원을 공급합니다.
On Delayed	Power On Delay 값에 따라 각 선택한 출력에 전원을 공급합니다.†
Off Immediate	선택한 출력에서 전원을 제거합니다.
Off Delayed	Power Off Delay 값에 따라 각 선택한 출력에서 전원을 제거합니다.†
Reboot Immediate	각 선택한 출력에서 전원을 제거합니다. 그런 다음 Reboot Duration 값에 따라 각 출력에 전원을 공급합니다.†
Reboot Delayed	Power Off Delay 값에 따라 각 선택한 출력에서 전원을 제거합니다. 모든 출력이 꺼질 때까지 기다린 후 (Reboot Duration의 최대 값) Power On Delay 값에 따라 각 출력에 전원을 공급합니다.†
Cancel Pending Commands	선택한 출력에 대해 보류 중인 모든 명령을 취소하고 이를 현재 상태에서 유지시킵니다. **참고:** 글로벌 출력 그룹의 경우, 시작 UPS 출력 그룹의 인터페이스에서만 명령을 취소할 수 있습니다. 작업은 시작 UPS 출력 그룹 및 모든 종속 출력 그룹에 대한 명령을 취소합니다.

† 로컬 출력 그룹이 선택되면 그룹의 가장 낮은 번호의 출력 구성 지연 및 재부팅 기간만 사용됩니다. 글로벌 출력 그룹이 선택되면 글로벌 출력의 구성 지연 및 재부팅 기간만 사용됩니다.

출력 설정 및 출력 이름 구성

다음 설정을 사용할 수 있습니다.

설정	설명
Name	하나 이상의 출력에 대한 이름을 설정합니다. 이름은 상태 화면의 출력 번호 옆에 표시됩니다.
External Link	웹 사이트나 IP 주소에 대한 HTTP 또는 HTTPS 링크를 정의합니다. • http://www.dell.com은 출력을 Dell의 웹 사이트에 연결시킵니다. • http://*pdu_ip_address*, 여기서 *pdu_ip_address*는 랙 PDU의 IP 주소이고 이 IP 주소에서 랙 PDU의 웹 인터페이스에 출력을 연결시켜 권한이 있는 사용자가 로그인할 수 있게 합니다.
Power On Delay	명령이 내려지고 출력에서 전원이 인가되기까지 랙 PDU가 대기하는 초 단위 시간을 설정합니다. **참고:** 출력이 항상 꺼져 있도록 구성하려면 Power On Delay 옆에 있는 Never 확인란을 선택합니다.
Power Off Delay	명령이 내려지고 출력에서 전원을 제거하기까지 랙 PDU가 대기하는 초 단위 시간을 설정합니다. **참고:** 출력이 항상 켜져 있도록 구성하려면 Power Off Delay 옆에 있는 Never 확인란을 선택합니다.
Reboot Duration	재시작 전에 출력이 꺼져 있을 초 단위 시간을 설정합니다.

출력 설정 또는 출력 이름을 구성하려면 Device Manager 탭을 선택하고 왼쪽 탐색 메뉴에서 Configuration을 선택합니다. Outlet Configuration 섹션에서 Configure Multiple Outlets 버튼을 클릭하거나 출력 이름을 클릭합니다.

- 여러 출력에 대한 출력 설정 구성:
  - 수정할 출력의 번호 옆에 있는 확인란을 선택하거나 All Outlets 확인란을 선택합니다.
  - Name 및 Link 값을 입력하고 목록 바로 아래의 Apply 버튼을 클릭합니다.
  - Power On Delay, Power Off Delay 또는 Reboot Duration 값을 입력하고 목록 바로 아래의 Apply 버튼을 클릭합니다.
- 단일 출력에 대한 출력 설정 구성:
  - Name 및 Link 값을 입력하고 목록 바로 아래의 Apply 버튼을 클릭합니다.
  - Power On Delay, Power Off Delay 또는 Reboot Duration 값을 입력하고 목록 바로 아래의 Apply 버튼을 클릭합니다.

출력 작업 예약

예약할 수 있는 작업

각 출력의 Power On Delay, Power Off Delay 및 Reboot Duration에 대한 값을 구성하려면 출력 설정 및 출력 이름 구성을 참조하십시오. 웹 인터페이스를 사용하여 출력 작업을 예약해야 하지만 웹 또는 명령줄 인터페이스에서 이러한 값을 설정할 수 있습니다.

작업이 출력 그룹에 적용되려면 예약 작업을 시작할 때 활성화된 출력 그룹이 있어야 합니다. 예를 들어, Off Delayed가 오후 4:00에 예약된 경우, Power Off Delay가 오후 4:00에 시작됩니다. 그런 다음 어떤 출력도 꺼지도록 예약하기 전에 이 Power Off Delay 중 출력 그룹을 활성화하더라도 작업은 출력 그룹이 아니라 개별 출력에만 적용됩니다.

선택하는 모든 출력에 대해 다음 표에 나열된 작업이 매일; 1, 2, 4 또는 8주 간격; 또는 한 번만 수행되도록 예약할 수 있습니다.

옵션	설명
No Action	아무것도 행하지 않습니다.
On Immediate	선택한 출력에 전원을 공급합니다.
On Delayed	Power On Delay 값에 따라 각 선택한 출력에 전원을 공급합니다.†
Off Immediate	선택한 출력에서 전원을 제거합니다.
Off Delayed	Power Off Delay 값에 따라 각 선택한 출력에서 전원을 제거합니다.†
Reboot Immediate	각 선택한 출력에서 전원을 제거합니다. 그런 다음 Reboot Duration 값에 따라 각 출력에 전원을 공급합니다.†
Reboot Delayed	Power Off Delay 값에 따라 각 선택한 출력에서 전원을 제거합니다. 모든 출력이 꺼질 때까지 기다린 후 (Reboot Duration의 최대 값) Power On Delay 값에 따라 각 출력에 전원을 공급합니다.†

† 로컬 출력 그룹이 선택되면 그룹의 가장 낮은 번호의 출력 구성 지연 및 재부팅 기간만 사용됩니다. 글로벌 출력 그룹이 선택되면 글로벌 출력의 구성 지연 및 재부팅 기간만 사용됩니다.

출력 이벤트 예약

1. 웹 인터페이스에서 Device Manager 탭을 선택한 후 왼쪽 탐색 메뉴에서 Scheduling을 선택합니다.
2. Outlet Scheduling 페이지에서 이벤트가 발생할 빈도를 선택하고(One-Time, Daily 또는 Weekly), Next 버튼을 클릭합니다.

   Weekly를 선택하는 경우 이벤트 발생 주기를 매주 한 번 또는 2주, 4주 또는 8주에 한 번으로 선택할 수 있습니다.

3. Schedule a Daily Action 페이지의 Name of event 텍스트 상자에서 기본 이름인 **`Outlet Event`**를 새 이벤트 식별에 사용할 이름으로 대체합니다.
4. 드롭다운 목록을 사용하여 이벤트 유형과 발생 시기를 선택합니다.

   1회 이벤트에 대한 날짜 형식은 *mm*/*dd* 이고, 모든 이벤트에 대한 시간 형식은 *hh*/*mm* 이며 2자리 시간은 24시간으로 지정됩니다.

   - 매일 또는 Weekly 선택 항목에서 제공되는 주기 중 하나로 예약된 이벤트는 이벤트를 삭제하거나 비활성화할 때까지 예약 주기에 따라 계속해서 발생합니다.
   - 예약을 수행하는 날짜로부터 12개월 내의 한 날짜에만 발생하도록 1회 이벤트를 예약할 수 있습니다. 예를 들어, 2010년 12월 26일을 기준으로 하면 2011년 12월 26일을 넘지 않는 현재 날짜로부터의 어떤 날짜에 1회 이벤트를 예약할 수 있습니다.

5. 확인란을 사용하여 이 작업이 적용될 출력을 선택합니다. 하나 이상의 개별 출력 또는 All Outlets를 선택할 수 있습니다.
6. Apply를 클릭하여 이벤트 예약을 확정하거나 Cancel을 클릭하여 취소합니다.

이벤트를 확정하면 예약 이벤트 목록에 새 이벤트가 포함된 요약 페이지가 다시 표시됩니다.

예약된 출력 이벤트 편집, 비활성화, 활성화 또는 삭제

1. 웹 인터페이스에서 Device Manager 탭을 선택한 후 왼쪽 탐색 메뉴에서 Scheduling을 선택합니다.
2. Scheduling 페이지의 Scheduled Outlet Action 섹션에 있는 이벤트 목록에서 이벤트 이름을 클릭합니다.
3. Daily/Weekly scheduled action detail 페이지에서 다음을 수행할 수 있습니다.

- 이벤트 이름, 이벤트 발생이 예약된 시간 및 적용 출력 등의 이벤트 상세 정보를 변경합니다.
- 페이지 맨 위에 있는 Status of event에서 다음 작업을 수행할 수 있습니다.
  - 구성된 모든 상세 정보는 나중에 다시 활성화할 수 있도록 그대로 유지한 채로 이벤트를 비활성화합니다. 비활성화된 이벤트는 발생하지 않습니다. 기본적으로 이벤트는 생성될 때 활성화됩니다.
  - 이벤트가 이전에 Disable로 설정되었던 경우 이벤트를 활성화합니다.
  - 이벤트를 삭제하여 시스템에서 이벤트를 완전히 제거합니다. 삭제된 이벤트는 복구할 수 없습니다.

4. 이 페이지에서 변경을 완료하면 Apply를 클릭하여 변경 내용을 적용하거나 Cancel을 클릭합니다.

출력 관리자 메뉴

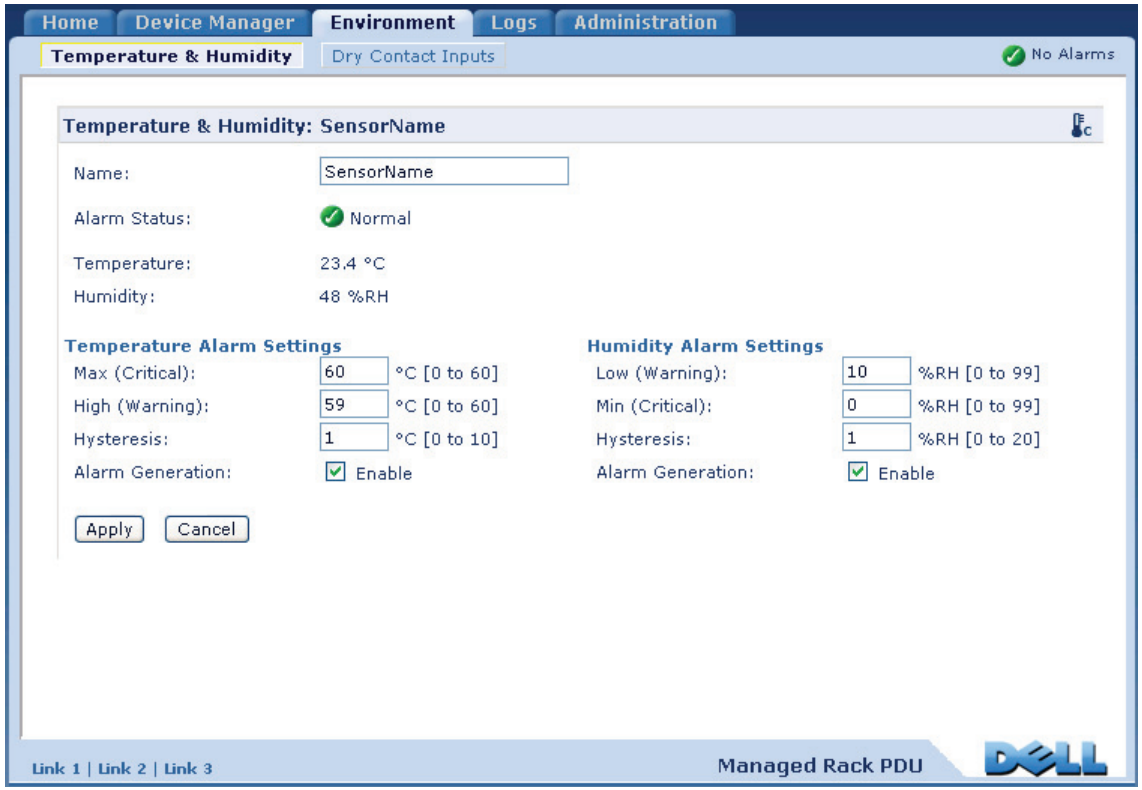
출력 사용자 계정을 만들고 구성합니다. 개별 출력에 출력 사용자 계정을 가진 한 명의 사용자를 할당할 수 있습니다. 출력 사용자 계정은 할당된 출력에 대해서만 제어를 허용합니다. 출력 구성은 관리자 권한을 가진 계정에만 허용됩니다. 장치 관리자는 제한적 출력 구성 권한을 갖습니다.

출력 사용자 구성

1. 웹 인터페이스에서 Device Manager 탭을 선택한 후 왼쪽 탐색 메뉴에서 Outlet Manager를 선택합니다.
2. Add New User 버튼을 클릭합니다.
3. 다음 옵션에 대한 정보를 입력하고 Apply를 클릭하여 변경 내용을 확인합니다.

옵션	설명
User Name	출력 사용자 이름을 설정합니다. "New User"는 내부 사용 전용이며 허용되지 않습니다. **참고:** 주황색으로 표시된 사용자 이름은 사용자 계정이 비활성화되었음을 나타냅니다.
Password	출력 사용자 암호를 설정합니다.
User Description	출력 사용자의 ID/설명을 설정합니다.
Account Status	출력 사용자의 계정을 활성화, 비활성화 또는 삭제합니다.
Device outlet access	사용자가 액세스할 수 있는 출력을 선택합니다.

환경


Home
Device Manager
Environment
Logs
Administration
Temperature & Humidity
Dry Contact Inputs
No Alarms
Temperature & Humidity: SensorName
Name:
SensorName
Alarm Status:
Normal
Temperature:
23.4 °C
Humidity:
48 %RH
Temperature Alarm Settings
Max (Critical):
60
°C [0 to 60]
High (Warning):
59
°C [0 to 60]
Hysteresis:
1
°C [0 to 10]
Alarm Generation:
Enable
Humidity Alarm Settings
Low (Warning):
10
%RH [0 to 99]
Min (Critical):
0
%RH [0 to 99]
Hysteresis:
1
%RH [0 to 20]
Alarm Generation:
Enable
Apply
Cancel
Link 1 | Link 2 | Link 3
Managed Rack PDU

온도 및 습도 센서 구성

경로: Environment > Temperature & Humidity

온도 또는 온도 및 습도 센서가 랙 PDU에 연결되어 있을 때, Temperature & Humidity 페이지를 통해 Warning 및 Critical 알람 생성에 대한 임계값을 설정할 수 있습니다(알람 유형별 자세한 설명은 장치 상태 아이콘 참조).

온도:

- 고온 임계값에 도달하면 시스템이 경고 알람을 생성합니다.
- 최대 온도 임계값에 도달하면 시스템이 위험 알람을 생성합니다.

습도:

- 저습 임계값에 도달하면 시스템이 경고 알람을 생성합니다.
- 최저 습도 임계값에 도달하면 시스템이 위험 알람을 생성합니다.

오른쪽 상단 모서리에 있는 온도계 기호를 클릭하여 화씨와 섭씨 사이에서 전환합니다.

온도 및 습도 센서를 구성하려면:

1. 최저, 최고, 높고 낮은 임계값을 입력합니다.
2. Hysteresis 값을 입력합니다. (자세한 내용은 이력 현상을 참조하십시오.)
3. 필요하면 알람 생성을 활성화합니다.
4. Apply를 클릭합니다.

이력 현상. 이 값은 온도 또는 습도에 대한 임계값 위반을 해결하기 위해 임계값을 기준으로 회복해야 하는 범위를 지정합니다.

- 최대 및 고온 임계값 위반의 경우, 해제 지점은 임계값에서 이력 현상을 뺀 값입니다.
- 최소 및 낮은 습도 위반의 경우, 해제 지점은 임계값에 이력 현상을 더한 값입니다.

온도 또는 습도로 인한 위반이 발생하고 위/아래로 값이 약간씩 변동할 때 다중 알람을 방지하려면 온도 이력 현상 또는 습도 이력 현상의 값을 늘립니다. 이력 현상 값이 너무 작으면 이러한 변동이 발생하므로 반복해서 임계값 위반을 해제합니다.

온도가 올라가고 변동할 경우의 예: 최대 온도 임계값이 29.4°C(85°F)이고 온도 이력 현상이 -16.1°C(3°F)인 경우, 온도가 29.4°C(85°F) 이상으로 올라가면 임계값 위반이 발생합니다. 그런 다음 반복해서 28.8°C(84°F)로 내려간 다음 30.0°C(86°F)로 올라가지만, 이벤트 해제나 새로운 위반이 발생하지 않습니다. 기존 위반을 해제하려면 온도가 27.7°C(82°F)로 내려가야 합니다(임계값에서 -16.1°C(3°F) 이하).

습도가 내려가고 변동할 경우의 예: 최저 습도 임계값이 18%이고 습도 이력 현상이 8%인 경우, 습도가 18% 이하로 내려가면 임계값 위반이 발생합니다. 그런 다음 반복해서 24%까지 올라간 다음 13%로 내려가지만, 이벤트 해제나 새로운 위반이 발생하지 않습니다. 기존 위반을 해제하려면 습도를 26% 이상으로 올려야 합니다(임계값에서 8% 감소).

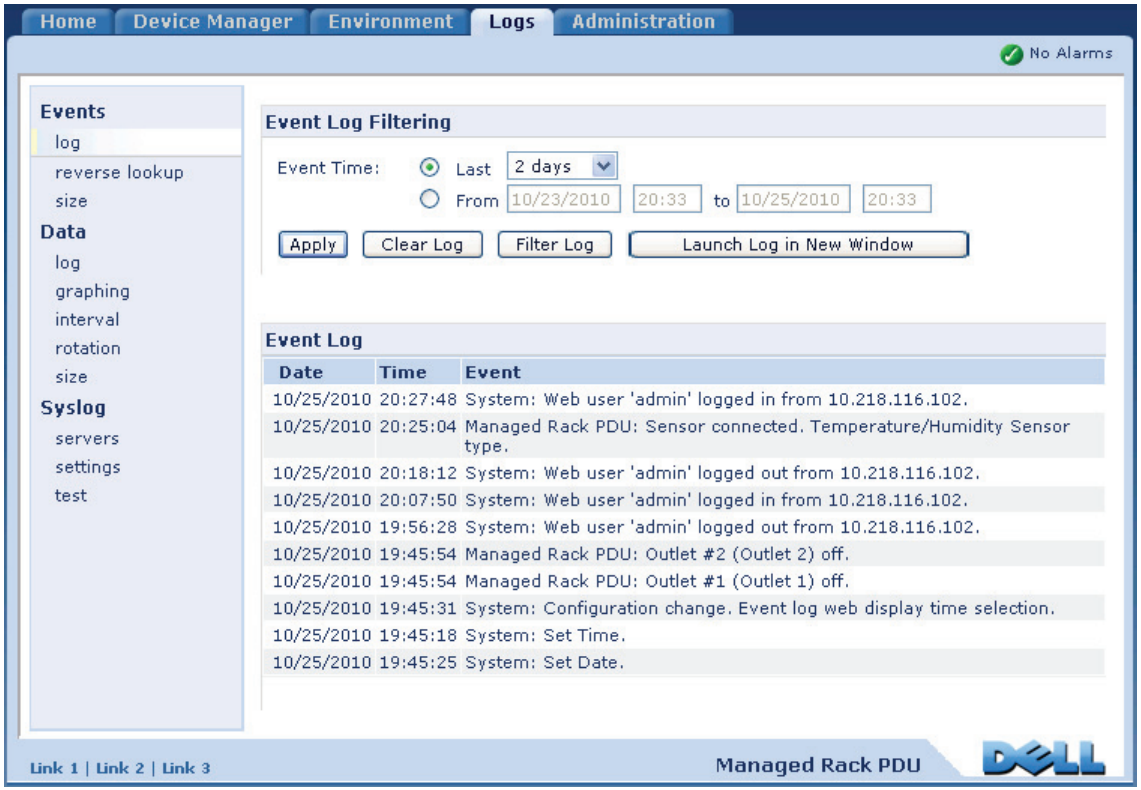
드라이 접점 입력 구성

경로: Environment > Dry Contact Inputs

Dry Contact Inputs 페이지를 통해 드라이 접점의 현재 상태를 확인하고 드라이 접점을 구성합니다.

매개변수	설명
Name	이 입력부의 이름입니다. *최대*: 20자
Alarm Status	이 입력부가 알람을 보고하지 않는 경우에는 Normal이 표시되거나 입력부가 알람을 보고할 경우 알람의 심각도가 표시됩니다.
State	이 입력부의 현재 상태입니다. Closed 또는 Open.
Alarm Generation	이 입력부를 활성화하거나 비활성화합니다. 비활성화하면 접점이 비정상적인 위치에 있어도 알람이 생성되지 않습니다.
Normal State	이 입력부의 정상(알람 없음) 상태입니다. Closed 또는 Open.

로그


Home
Device Manager
Environment
Logs
Administration
No Alarms
Events
log
reverse lookup
size
Data
log
graphing
interval
rotation
size
Syslog
servers
settings
test
Event Log Filtering
Event Time:
Last
2 days
From
10/23/2010
20:33
to
10/25/2010
20:33
Apply
Clear Log
Filter Log
Launch Log in New Window
Event Log
Date
Time
Event
10/25/2010 20:27:48 System: Web user 'admin' logged in from 10.218.116.102.
10/25/2010 20:25:04 Managed Rack PDU: Sensor connected. Temperature/Humidity Sensor type.
10/25/2010 20:18:12 System: Web user 'admin' logged out from 10.218.116.102.
10/25/2010 20:07:50 System: Web user 'admin' logged in from 10.218.116.102.
10/25/2010 19:56:28 System: Web user 'admin' logged out from 10.218.116.102.
10/25/2010 19:45:54 Managed Rack PDU: Outlet #2 (Outlet 2) off.
10/25/2010 19:45:54 Managed Rack PDU: Outlet #1 (Outlet 1) off.
10/25/2010 19:45:31 System: Configuration change. Event log web display time selection.
10/25/2010 19:45:18 System: Set Time.
10/25/2010 19:45:25 System: Set Date.
Link 1 | Link 2 | Link 3
Managed Rack PDU

이벤트 및 데이터 로그 사용

이벤트 로그

경로: Logs > Events > *options*

이벤트 로그를 확인, 필터링 또는 삭제할 수 있습니다. 기본적으로 로그에는 지난 2일 동안 기록된 모든 이벤트가 최근 발생한 시간 순으로 표시됩니다.

구성 가능한 모든 이벤트와 현재 구성 목록을 보려면 Administration 탭, 상단 메뉴 표시줄에서 Notification, 왼쪽 탐색 메뉴의 Event Actions 아래의 by event를 선택합니다.

이벤트별 구성을 참조하십시오.

이벤트 로그를 표시하려면(Logs > Events > log):

- 기본적으로 이벤트 로그는 웹 인터페이스의 페이지로 표시됩니다. 가장 최근의 이벤트가 1페이지에 기록됩니다. 로그 아래의 탐색 표시줄에서 다음의 기능을 사용할 수 있습니다.
  - 페이지 번호를 클릭하여 로그의 특정 페이지를 엽니다.
  - 현재 페이지에 나열된 이벤트 바로 이전 또는 이후에 기록된 이벤트를 보려면 Previous 또는 Next를 클릭합니다.
  - 첫 페이지로 돌아가려면 <<을 클릭하고, 로그 맨 마지막 페이지를 보려면 >>을 클릭합니다.
- 한 페이지에 나열된 이벤트를 보려면 이벤트 로그 페이지에서 Launch Log in Window를 클릭하여 로그의 전체 화면 보기를 표시합니다.

Laucch Log in New Window 버튼을 사용하려면 브라우저 옵션에 JavaScript®가 활성화되어 있어야 합니다.

또한 FTP나 SCP(Secure CoPy)를 사용해서도 이벤트 로그를 확인할 수 있습니다. FTP 또는 SCP를 사용하여 로그 파일을 불러오는 방법을 참조하십시오.

로그를 필터링하려면(Logs > Events > log):

- **날짜 또는 시간별로 로그 필터링:** 전체 이벤트 로그를 표시하거나 로그에 가장 최근에 발생한 이벤트가 표시되는 일 수 또는 주 수를 변경하려면 Last를 선택합니다. 드롭다운 메뉴에서 시간 범위를 선택한 후 Apply를 클릭합니다. 랙 PDU가 다시 시작할 때까지 필터 구성이 저장됩니다.
  특정 시간 범위 동안 기록된 이벤트를 표시하려면 From을 선택합니다. 이벤트를 표시할 시작 및 끝 시간(24시간제 형식 사용)과 날짜를 지정한 후 Apply를 클릭합니다. 랙 PDU가 다시 시작할 때까지 필터 구성이 저장됩니다.
- **이벤트별 로그 필터링:** 로그에 표시되는 이벤트를 지정하려면 Filter Log를 클릭합니다. 보기에서 이벤트를 제거하려면 이벤트 범주 또는 알람 심각성 수준에 대한 확인란 선택을 취소합니다. 이벤트 로그 페이지 상단 오른쪽 모서리에 있는 텍스트는 필터가 활성 상태임을 나타냅니다.
  관리자는 Save As Default를 클릭하여 이 필터를 모든 사용자에게 표시되는 기본 로그 보기로 저장할 수 있습니다. Save As Default를 클릭하지 않은 경우, 옵션 선택을 해제하거나 랙 PDU가 다시 시작되기 전까지 필터가 활성 상태로 유지됩니다.
  활성 필터를 제거하려면 Filter Log를 클릭한 후 Clear Filter (Show All)를 클릭합니다.

이벤트는 OR 논리를 사용하는 필터를 통해 처리됩니다.

- Filter By Severity 목록에서 선택하지 않은 이벤트는 해당 이벤트가 Filter by Category 목록에서 선택한 범주에서 발생한 경우라도 필터링된 이벤트 로그에 표시되지 않습니다.
- Filter By Severity 목록에서 선택하지 않은 이벤트는 해당 범주의 장치가 Filter by Severity 목록에서 선택한 알람 상태로 들어간 경우라도 필터링된 이벤트 로그에 표시되지 않습니다.

로그를 삭제하려면(Logs > Events > log):

로그에 기록된 모든 이벤트를 삭제하려면 로그가 표시된 웹 페이지에서 Clear Log를 클릭합니다. 삭제된 이벤트는 복구할 수 없습니다.

할당된 심각성 수준 또는 이벤트 범주에 따라 이벤트 기록을 해제하려면 이벤트별 구성을 참조하십시오.

역조회를 구성하려면(Logs > Events > revers lookup):

기본적으로 역조회는 해제되어 있습니다. 구성된 DNS 서버가 없거나 네트워크 트래픽이 과중하여 네트워크 성능이 떨어진 경우를 제외하고는 이 기능을 사용합니다.

역조회를 활성화한 경우, 네트워크 관련 이벤트가 발생하면 이벤트와 관련된 네트워크에 연결된 장치의 IP 주소와 도메인 이름이 모두 이벤트 로그에 기록됩니다. 장치에 도메인 이름이 없으면 IP 주소만 이벤트와 함께 기록됩니다. 일반적으로 도메인 이름은 IP 주소만큼 자주 변경되지 않기 때문에 역조회를 활성화하면 이벤트를 발생시키는 네트워크에 연결된 장치의 주소를 식별하는 기능이 향상될 수 있습니다.

이벤트 로그 크기를 조정하려면(Logs > Events > size):

기본적으로 이벤트 로그에는 400개의 이벤트가 저장됩니다. 로그에 저장되는 이벤트 수를 변경할 수 있습니다. 이벤트 로그의 크기를 조정할 경우 기존의 모든 로그 항목이 삭제됩니다. 로그 데이터 손실을 방지하려면 Event Log Size 필드에 새 값을 입력하기 전에 FTP 또는 SCP를 사용하여 로그를 불러오십시오.

FTP 또는 SCP를 사용하여 로그 파일을 불러오는 방법을 참조하십시오.

로그가 가득 차면 오래된 항목이 삭제됩니다.

데이터 로그

경로: Logs > Data > *options*

데이터 로그에는 장치 및 위상(3상 랙 PDU의 경우)의 전류 및 전력, 온도 및 습도, 드라이 접점 데이터가 지정한 시간 간격으로 기록됩니다. 각 항목은 데이터가 기록된 날짜와 시간을 기준으로 나열됩니다.

데이터 로그를 표시하려면(Logs > Data > log):

- 기본적으로 데이터 로그는 웹 인터페이스의 페이지로 표시됩니다. 가장 최근의 데이터 항목이 1페이지에 기록됩니다. 로그 아래의 탐색 표시줄에서 다음 기능을 사용할 수 있습니다.
  - 페이지 번호를 클릭하여 로그의 특정 페이지를 엽니다.
  - 현재 페이지에 나열된 데이터 바로 이전 또는 이후에 기록된 데이터를 보려면 Previous 또는 Next를 클릭합니다.
  - 로그의 첫 페이지로 돌아가려면 <<을 클릭하고, 로그 맨 마지막 페이지를 보려면 >>을 클릭합니다.
- 한 페이지에 나열된 데이터를 보려면 데이터 로그 페이지에서 Launch Log in New Window를 클릭하여 로그의 전체 화면 보기를 표시합니다.

Launch Log in New Window 버튼을 사용하려면 브라우저 옵션에 JavaScript가 활성화되어 있어야 합니다.

또는 FTP나 SCP를 사용해서도 데이터 로그를 확인할 수 있습니다. FTP 또는 SCP를 사용하여 로그 파일을 불러오는 방법을 참조하십시오.

날짜 또는 시간별로 로그를 필터링하려면(Logs > Data > log):

전체 데이터 로그를 표시하거나 로그에 가장 최근에 발생한 이벤트가 표시되는 일 수 또는 주 수를 변경하려면 Last를 선택합니다. 드롭다운 메뉴에서 시간 범위를 선택한 후 Apply를 클릭합니다. 장치가 다시 시작할 때까지 필터 구성이 저장됩니다.

특정 시간 범위 동안 기록된 데이터를 표시하려면 From을 선택합니다. 데이터를 표시할 시작 및 끝 시간(24시간제 형식 사용)과 날짜를 지정한 후 Apply를 클릭합니다. 장치가 다시 시작할 때까지 필터 구성이 저장됩니다.

데이터 로그를 삭제하려면:

로그에 기록된 모든 데이터를 삭제하려면 로그가 표시된 웹 페이지에서 Clear Data Log를 클릭합니다. 삭제된 데이터는 복구할 수 없습니다.

데이터 수집 간격을 설정하려면(Logs > Data > interval):

Log Interval 설정에서 데이터 표본이 추출되고 데이터 로그에 저장되는 주기를 정의한 다음, 선택한 간격을 기준으로 로그에 데이터를 저장할 수 있는 일 수 계산을 확인합니다. 로그가 가득 차면 오래된 항목이 삭제됩니다. 이전 데이터의 자동 삭제를 방지하려면 다음 단원에서 설명하는 데이터 로그 회전을 설정하여 구성하십시오.

데이터 로그 회전을 구성하려면(Logs > Data > rotation):

지정된 FTP 서버에 암호로 보호된 데이터 로그 리포지토리를 설정합니다. 회전 기능을 설정하면 데이터 로그 내용이 이름 및 위치별로 사용자가 지정한 파일에 추가됩니다. 이 파일의 업데이트는 지정한 업로드 간격에 따라 이루어집니다.

매개변수	설명
Data Log Rotation	데이터 로그 회전을 활성화 또는 비활성화(기본값)합니다.
FTP Server Address	데이터 리포지토리 파일이 저장되는 FTP 서버 위치입니다.
User Name	데이터를 리포지토리 파일로 전송하는 데 필요한 사용자 이름입니다. 또한 이 사용자가 데이터 리포지토리 파일과 데이터가 저장되는 디렉토리(폴더)에 대한 읽기/쓰기 권한을 갖도록 구성해야 합니다.
Password	데이터를 리포지토리 파일로 전송하는 데 필요한 암호입니다.
File Path	리포지토리 파일 경로입니다.
Filename	리포지토리 파일(ASCII 텍스트 파일) 이름입니다.
Delay *X* hours between uploads.	데이터가 파일에 업로드되는 간격(시간)입니다.
Upload every *X* minutes	업로드 실패 후 파일에 데이터 업로드를 시도하는 간격(분)입니다.
Up to *X* Gulim	초기 실패 후 업로드가 시도되는 최대 횟수입니다.
Until Upload Succeeds	전송이 완료될 때까지 파일 업로드가 시도됩니다.

데이터 로그 크기를 조정하려면(Logs > Data > size):

기본적으로 데이터 로그에는 1000개의 기록이 저장됩니다. 로그에 저장되는 기록 수를 변경할 수 있습니다. 데이터 로그의 크기를 조정할 경우 기존의 모든 로그 항목이 삭제됩니다. 기록 손실을 방지하려면, Data Log Size 필드에 새 값을 입력하기 전에 FTP 또는 SCP를 사용하여 로그를 불러오십시오.

 FTP 또는 SCP를 사용하여 로그 파일을 불러오는 방법를 참조하십시오.

로그가 가득 차면 오래된 항목이 삭제됩니다.

FTP 또는 SCP를 사용하여 로그 파일을 불러오는 방법

관리자 또는 장치 사용자는 FTP 또는 SCP를 사용하여 탭으로 구분된 이벤트 로그 파일(*event.txt*) 또는 데이터 로그 파일(*data.txt*)을 불러온 다음 스프레드시트로 가져올 수 있습니다.

- 최대 크기에 도달했기 때문에 로그가 마지막으로 삭제되거나 데이터 로그의 경우 잘린 이후 기록된 모든 이벤트 또는 데이터가 표시된 파일입니다.
- 이 파일에는 이벤트 로그 또는 데이터 로그에 표시되지 않은 정보가 있습니다.
  - 파일 형식 버전(첫 번째 필드)
  - 파일을 불러온 날짜 및 시간
  - 랙 PDU의 Name, Contact 및 Location 값 및 IP 주소
  - 기록된 각 이벤트의 고유 **이벤트 코드**(*event.txt* 파일만 해당)

랙 PDU의 로그 항목에는 4자리 연도를 사용합니다. 스프레드시트 응용 프로그램에서 4자리를 모두 표시하려면 4자리 날짜 형식을 선택해야 할 수 있습니다.

시스템에 암호화 기반 보안 프로토콜을 사용하는 경우에는 SCP를 사용하여 로그 파일을 불러와야 합니다.
시스템의 보안을 위해 암호화되지 않은 인증 방법을 사용하는 경우에는 FTP를 사용하여 로그 파일을 불러옵니다.

사용 가능한 프로토콜 및 원하는 보안 유형을 설정하는 방법에 대한 자세한 내용은 부록 B: 보안 핸드북을 참조하십시오.

SCP를 사용해서 파일을 불러오려면. SPC를 사용하여 *event.txt* 파일을 불러오려면 다음 명령을 사용합니다.

```
scp username@hostname_or_ip_address:event.txt ./event.txt
```

SCP를 사용하여 *data.txt* 파일을 불러오려면 다음 명령을 사용합니다.

```
scp username@hostname_or_ip_address:data.txt ./data.txt
```

FTP를 사용하여 파일을 불러오려면. FTP를 사용하여 *event.txt* 또는 *data.txt* 파일을 불러오려면:

1. 명령 프롬프트에서 **ftp** 및 랙 PDU의 IP 주소를 입력하고 ENTER를 누릅니다.

   Administration 탭의 Network 메뉴에서 FTP Server 옵션에 대한 Port 설정이 기본값(21)에서 다른 값으로 변경된 경우 FTP 명령에 기본값이 아닌 값을 사용해야 합니다. Windows FTP 클라이언트의 경우 공백을 포함하여 다음 명령을 사용합니다. (일부 FTP 클라이언트의 경우 IP 주소와 포트 번호 사이에 공백 대신 콜론(:)을 사용해야 합니다.)

   ftp>open ip_address port_number

   FTP 서버의 보안을 개선하기 위해 기본값이 아닌 포트 값을 설정하려면 FTP 서버를 참조하십시오. 5001~32768 범위의 포트를 지정할 수 있습니다.

2. 관리자 또는 장치 사용자가 로그온하려면 대/소문자를 구분하여 User Name과 Password를 입력합니다. 관리자의 경우 User Name과 Password의 기본값은 admin입니다. 장치 사용자의 경우 User Name과 Password의 기본값은 device입니다.
3. 로컬 드라이브로 로그 텍스트를 전송하려면 get 명령을 사용합니다.

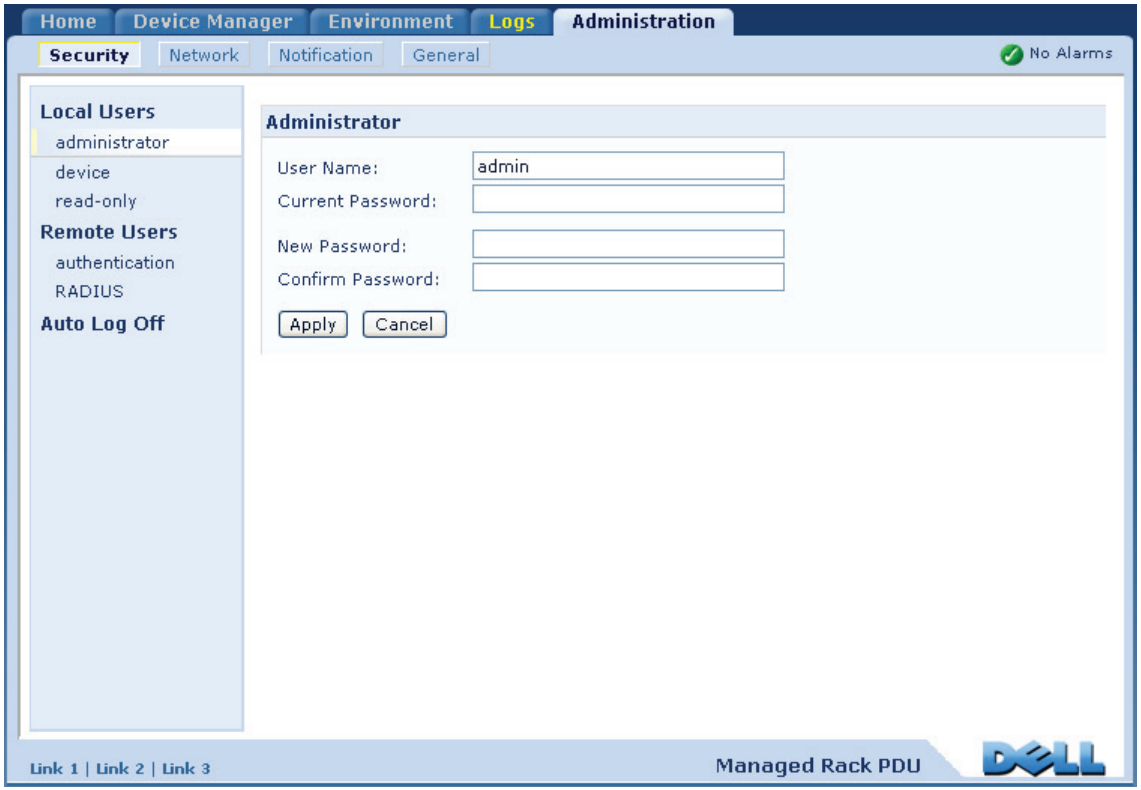
   ftp>get event.txt

   또는

   ftp>get data.txt

4. FTP를 종료하려면 **ftp>** 프롬프트에서 **quit**를 입력합니다.

관리: 보안


Home
Device Manager
Environment
Logs
Administration
Security
Network
Notification
General
No Alarms
Local Users
administrator
device
read-only
Remote Users
authentication
RADIUS
Auto Log Off
Administrator
User Name:
admin
Current Password:
New Password:
Confirm Password:
Apply
Cancel
Link 1 | Link 2 | Link 3
Managed Rack PDU

로컬 사용자

사용자 액세스 설정

경로: Administration > Security > Local Users > *options*

관리자 사용자 계정은 항상 랙 PDU에 액세스할 수 있습니다.

기본적으로 장치 사용자와 읽기 전용 사용자 계정이 설정되어 있습니다. 장치 사용자 또는 읽기 전용 사용자 계정을 비활성화하려면 왼쪽 탐색 메뉴에서 해당 사용자 계정을 선택한 후 Enable 확인란의 선택을 취소합니다.

동일한 방식으로 각 계정 유형에 대해 대/소문자를 구분한 사용자 이름과 암호를 설정합니다. 사용자 이름과 암호의 최대 길이는 모두 64자입니다. 공백 암호(문자가 입력되지 않은 암호)는 허용되지 않습니다.

각 계정 유형에 부여된 권한에 대한 정보는 사용자 계정 유형을 참조하십시오.

출력 사용자 계정의 경우, 기본 사용자 이름 또는 암호가 없습니다. 관리자는 사용자 이름, 암호 및 출력 사용자의 다른 계정 특성을 지정해야 합니다. 출력 사용자 구성을 참조하십시오.

계정 유형	기본 사용자 이름	기본 암호	허용된 액세스 권한
관리자	admin	admin	웹 인터페이스 및 명령줄 인터페이스
장치 사용자	device	device	
읽기 전용 사용자	readonly	readonly	웹 인터페이스 전용

원격 사용자

인증

경로: Administration > Security > Remote Users > Authentication Method

랙 PDU에 대한 원격 액세스를 관리하는 방식을 선택하려면 이 옵션을 사용합니다.

로컬 인증(RADIUS 서버의 중앙화된 인증을 사용하지 않음)에 대한 내용은 부록 B: 보안 핸드북을 참조하십시오.

랙 PDU는 RADIUS(Remote Authentication Dial-In User Service) 인증과 권한 부여 기능을 지원합니다.

- 사용자가 RADIUS가 활성화된 랙 PDU 또는 다른 네트워크 활성 장치에 액세스할 경우, 사용자의 권한 수준을 확인하기 위해 RADIUS 서버로 인증 요청이 전송됩니다.
- 랙 PDU에 사용되는 RADIUS 사용자 이름 길이는 32자로 제한됩니다.

다음 중 하나를 선택합니다.

- Local Authentication Only: RADIUS가 비활성화됩니다. 로컬 인증이 활성화됩니다.
- RADIUS, then Local Authentication: RADIUS와 로컬 인증이 활성화됩니다. 우선적으로 RADIUS 서버에서 인증을 요구합니다. RADIUS 서버가 응답하지 않으면 로컬 인증이 사용됩니다.
- RADIUS Only: RADIUS가 활성화됩니다. 로컬 인증이 비활성화됩니다.

RADIUS Only를 선택하고, RADUIS 서버가 사용 불능 상태이거나 제대로 확인 또는 구성되지 않은 경우 모든 사용자가 원격 액세스를 사용할 수 없습니다. 명령줄 인터페이스에 대한 직렬 연결을 사용하여 access 설정을 local 또는 radiusLocal로 변경하여 액세스 권한을 다시 받아야 합니다. 예를 들어, 액세스 설정을 local로 변경하는 명령은 다음과 같습니다.

```
radius -a local
```

RADIUS

경로: Administration > Security > Remote Users > RADIUS

이 옵션을 사용하여 다음 작업을 수행합니다.

- 랙 PDU에 사용 가능한 RADIUS 서버(최대 2개)와 각각에 대한 시간 제한 기간이 표시됩니다.
- 링크를 클릭하여 새 RADIUS 서버에 사용되는 인증 매개변수를 구성합니다.
- 나열된 RADIUS 서버를 클릭하여 해당 매개변수를 표시하고 수정합니다.

RADIUS 설정	정의
RADIUS Server	RADIUS 서버의 서버 이름 또는 IP 주소(IPv4 또는 IPv6)입니다. 링크를 클릭하여 서버를 구성합니다. **참고:** RADIUS 서버는 기본적으로 1812 포트를 사용하여 사용자를 인증합니다. 다른 포트를 사용하려면 RADIUS 서버명 또는 IP 주소 끝에 새로운 포트 번호를 입력하고 콜론(:)을 추가합니다.
Secret	RADIUS 서버와 랙 PDU 간의 공유 보안입니다.
Timeout	RADIUS 서버가 응답할 때까지 랙 PDU가 대기하는 시간(단위: 초)입니다.
Test Settings	관리자 사용자 이름과 암호를 입력하여 구성한 RADIUS 서버 경로를 테스트합니다.
Skip Test and Apply	RADIUS 서버 경로를 테스트하지 않습니다.

RADIUS 서버 구성

구성 절차 요약

랙 PDU와 함께 사용할 수 있도록 RADIUS 서버를 구성해야 합니다.

VAS(Vendor Specific Attributes)를 포함한 RADIUS 사용자 파일과 RADIUS 서버의 사전 파일에 있는 항목에 대한 예는 부록 B: 보안 핸드북을 참조하십시오.

1. RADIUS 서버 클라이언트 목록(파일)에 랙 PDU의 IP 주소를 추가합니다.
2. VAS (Vendor Specific Attributes)가 정의되지 않은 한 Service-Type 특성을 포함하여 사용자를 구성해야 합니다. Service-Type 특성이 구성되지 않은 경우 사용자에게 읽기 전용 권한(웹 인터페이스에 한해)만 부여됩니다.

   RADIUS 사용자 파일에 대한 자세한 내용은 RADIUS 서버 문서를 참조하고, 해당 예는 부록 B: 보안 핸드북을 참조하십시오.

3. RADIUS 서버에서 제공되는 Service-Type 특성 대신 VSA를 사용할 수 있습니다. VSA에는 사전 항목과 RADIUS 사용자 파일이 필요합니다. 사전 파일에서 숫자 값이 아닌 ATTRIBUTE 및 VALUE 키워드에 대한 이름을 정의합니다. 숫자 값을 변경하면 RADIUS 인증과 권한 부여가 실패합니다. VSA는 표준 RADIUS 특성에 우선합니다.

섀도우 암호를 사용하여 UNIX®에서 RADIUS 서버 구성

RADIUS 사전 파일에 UNIX 섀도우 암호 파일(/etc/passwd)이 사용된 경우 다음의 두 가지 방법을 사용하여 사용자를 인증할 수 있습니다.

- 모든 UNIX 사용자가 관리자 권한을 가진 경우 RADIUS "user" 파일에 다음을 추가합니다. 장치 사용자만 허용하려면 DELL-Service-Type을 **Device**로 변경합니다.

```
DEFAULT      Auth-Type = System
             DELL-Service-Type = Admin
```

- RADIUS "user" 파일에 사용자 이름과 특성을 추가하고 /etc/passwd에 대해 암호를 확인합니다. 다음은 **bconners** 및 **thawk** 사용자에 대한 예입니다.

```
bconners     Auth-Type = System
             DELL-Service-Type = Admin
thawk        Auth-Type = System
             DELL-Service-Type = Device
```

지원되는 RADIUS 서버

FreeRADIUS 및 Microsoft IAS 2003이 지원됩니다. 일반적으로 사용하는 다른 RADIUS 응용 프로그램은 작동할 수는 있지만 완전한 테스트를 거치지는 않았습니다.

비활성 시간 제한

경로: Administration > Security > Auto Log Off

비활성 사용자를 로그오프하기 전까지 시스템이 대기하는 시간을 구성하려면 이 옵션을 사용합니다(기본값: 3분). 이 값을 변경한 후, 변경 내용을 적용하려면 반드시 로그오프해야 합니다.

사용자가 오른쪽 상단에서 Log Off를 클릭하여 로그오프하지 않고 브라우저 창을 닫은 경우에는 이 타이머가 계속해서 실행됩니다. 이 사용자가 계속 로그온한 상태로 간주되기 때문에 Minutes of Inactivity에 지정된 시간이 만료되기 전까지 다른 사용자가 로그온할 수 없습니다. 예를 들어, Minutes of Inactivity 기본값을 사용할 때 사용자가 로그오프하지 않고 브라우저 창을 닫으면 3분 동안 다른 사용자가 로그온할 수 없습니다.

관리: 알림


Home
Device Manager
Environment
Logs
Administration
Security
Network
Notification
General
No Alarms
Event Actions
by event
by group
E-mail
server
recipients
test
SNMP Traps
trap receivers
test
Event Actions for Individual Events
To list all events in a main category by severity level, click the main category name. To list all events in a sub-category by severity level, click the sub-category name.
Device
Communications
Device
Phase Load
Outlet Load
Outlet Control
Sensor
System
Mass Configuration
Security
Link 1 | Link 2 | Link 3
Managed Rack PDU

이벤트 조치

경로: Administration > Notification > Event Actions > *options*

알림 유형

이벤트 또는 이벤트 그룹에 대해 수행할 이벤트 조치를 구성할 수 있습니다. 이러한 조치를 통해 다음과 같은 여러 가지 방식으로 사용자에게 해당 이벤트가 통보됩니다.

- 활성, 자동 알림. 지정된 사용자 또는 모니터링 장치에 직접 연결됩니다.
  - 전자 메일 알림
  - SNMP 트랩
  - Syslog 알림
- 간접 알림
  - 이벤트 로그. 직접 알림이 구성되지 않은 경우, 발생한 이벤트 종류를 파악하려면 사용자가 로그를 확인해야 합니다.

    또한 장치 모니터링에 사용할 시스템 성능 데이터를 기록할 수 있습니다. 이 데이터 로깅 옵션의 구성 및 사용 방법은 데이터 로그를 참조하십시오.
  - 쿼리(SNMP GET)

    자세한 내용은 SNMP를 참조하십시오. SNMP는 NMS를 활성화하여 정보용 쿼리를 수행합니다. 전송 전 데이터를 암호화하지 않는 SNMPv1의 경우, 가장 제한적인 SNMP 액세스 유형(읽기)을 구성하면 원격 구성 변경을 허용할 때의 위험 없이 정보용 쿼리를 활성화할 수 있습니다.

이벤트 조치 구성

알림 매개변수. 이벤트 해제와 연관된 이벤트의 경우, 다음에 나오는 두 단원에서 설명된 대로 개별 또는 그룹별로 이벤트를 구성할 때 다음 매개변수를 설정할 수 있습니다. 매개변수에 액세스하려면 수신기 또는 수신자 이름을 클릭합니다.

매개변수	설명
Delay *x* time before sending	지정된 시간 동안 이벤트가 지속되면 알림이 전송됩니다. 시간이 만료되기 전에 조건이 해제되면 알림이 전송되지 않습니다.
Repeat at an interval of *x* time	지정된 간격(예: 매 2분)으로 알림이 전송됩니다.
Up to *x* times	활성 이벤트 동안 이 횟수만큼 알림이 반복됩니다.
Until condition clears	조건이 제거되거나 해결될 때까지 알림이 반복해서 전송됩니다.

이벤트별 구성. 개별 이벤트에 대한 이벤트 조치를 정의하려면:

1. Administration 탭, 상단 메뉴 표시줄에서 Notification, 왼쪽 탐색 메뉴의 Event Actions 아래의 by event를 선택합니다.
2. 이벤트 목록에서 표시된 열을 검토하여 원하는 조치가 이미 구성되었는지 확인합니다. (기본적으로 모든 이벤트에 대해 로깅이 구성되어 있습니다.)
3. 전자 메일 또는 호출로 알림을 받을 수신자, SNMP 트랩에 의해 알림을 받을 네트워크 관리 시스템(NMS)과 같이 현재 구성을 보거나 변경하려면 이벤트 이름을 클릭합니다.

Syslog 서버가 구성되지 않은 경우 Syslog 구성과 관련된 항목이 표시되지 않습니다.

이벤트의 구성 세부 정보를 확인하는 경우, 구성을 변경하고 이벤트 로깅 또는 Syslog를 활성화/비활성화하거나 특정 전자- 메일 수신자 또는 트랩 수신기에 대한 알림을 해제할 수 있지만 수신자와 수신기를 추가하거나 제거할 수는 없습니다. 수신자 또는 수신기를 추가하거나 제거하려면 다음을 참조하십시오.

- Syslog 서버 확인
- 전자메일 수신자
- 트랩 수신기

그룹별 구성. 이벤트 그룹을 동시에 구성하려면:

1. Administration 탭, 상단 메뉴 표시줄에서 Notification, 왼쪽 탐색 메뉴의 Event Actions 아래의 by group을 선택합니다.
2. 구성할 이벤트의 그룹화 방법을 선택합니다.
   - Grouped by severity를 선택한 다음, 하나 이상의 심각성 수준에 대해 모든 이벤트를 선택합니다. 이벤트의 심각성을 변경할 수는 없습니다.
   - Grouped by category를 선택한 다음, 하나 이상의 사전 정의된 범주에서 모든 이벤트를 선택합니다.
3. Next>>를 클릭하여 페이지를 이동해서 다음을 수행합니다.
   a. 이벤트 그룹에 대한 이벤트 조치를 선택합니다.
   - Logging(기본값)을 제외한 조치를 선택하려면 먼저 최소 하나 이상의 관련 수신자 또는 수신기를 구성해야 합니다.
   - Logging을 선택하고 Syslog 서버가 구성되어 있으면, 다음 페이지에서 Event Log 또는 Syslog(또는 둘다)를 선택합니다.

   b. 이 이벤트 그룹에 대해 새로 구성된 이벤트 조치를 활성 상태로 유지할지, 조치를 해제할지를 선택합니다.

활성, 자동, 직접 알림

전자 메일 알림

설정 개요. SMTP (Simple Mail Transfer Protocol)를 사용하여 이벤트가 발생할 때 최대 4명의 수신자에게 전자 메일을 발송합니다.

전자메일 기능을 사용하려면 다음 설정을 지정해야 합니다.

- 기본 및 보조 DNS(Domain Name Service) 서버(옵션)의 IP 주소

   DNS을 참조하십시오.

- SMTP Server의 IP 주소 또는 DNS 이름과 From Address.

   SMTP을 참조하십시오.

- 최대 4명의 수신자의 전자 메일 주소

   전자메일 수신자을 참조하십시오.

recipients 옵션의 To Address 설정을 사용하여 텍스트 기반 호출기에 전자- 메일을 발송할 수 있습니다.

SMTP.

경로: Administration > Notification > E-mail > server

설정	설명
Local SMTP Server	로컬 SMTP 서버의 IPv4/ IPv6 주소 또는 DNS 이름입니다. **참고:** 이 설정은 SMTP Server가 Local로 설정된 경우에만 지정해야 합니다. 전자메일 수신자을 참조하십시오.
From Address	랙 PDU에서 전송되는 전자 메일 메시지의 From 필드 내용: • *사용자@ [IP_주소]* 형식(IP 주소가 **로컬 SMTP 서버**로 지정된 경우) • *사용자@도메인* 전자 메일 메시지 형식(DNS가 구성되고 DNS 이름이 **로컬 SMTP 서버**로 지정된 경우). **참고:** 로컬 SMTP 서버는 이 설정에 대한 서버의 유효한 사용자 계정을 사용할 수 있습니다. 서버 설명서를 참조하십시오.

전자메일 수신자.

경로: Administration > Notification > E- mail > recipients

최대 4명의 전자 메일 수신자를 확인합니다.

설정	설명
To Address	수신자의 사용자 이름과 도메인 이름입니다. 호출에 전자 메일을 사용하려면 수신자의 호출기 게이트웨이 계정의 전자- 메일 주소를 사용합니다(예: **myacct100@skytel.com**). 호출기 게이트웨이를 통해 호출이 생성됩니다. 메일 서버 IP 주소에 대해 DNS를 조회하지 않으려면 전자 메일 도메인 이름 대신 괄호 안에 있는 IP 주소를 사용하십시오(예: jsmith@company.com 대신 jsmith@[xxx.xxx.x.xxx] 사용). 이는 DNS 조회 기능이 제대로 작동하지 않을 때 유용합니다. **참고:** 수신자의 호출기에서 텍스트 기반 메시징을 사용할 수 있어야 합니다.
E-mail Generation	수신자에게 전자 메일 발송을 활성화하거나(기본값) 비활성화합니다.

설정	설명

SMTP 서버	다음 중 전자 메일 라우팅 방법을 선택할 수 있습니다.
	• Local: 랙 PDU의 SMTP 서버를 통하는 방법입니다. 이 설정(권장)은 랙 PDU의 20초 시간 제한을 초과하기 전에 전자- 메일을 발송하고 필요한 경우 여러 번 재시도합니다. 또한 다음 중 하나를 수행합니다.
	  • 랙 PDU의 SMTP 서버에서 전달 기능을 활성화하면 외부 SMTP 서버로 전자 메일을 라우팅할 수 있습니다. 일반적으로 SMTP 서버에는 전자 메일 전달 기능이 구성되어 있지 않습니다. 전달이 가능하도록 SMTP 서버 구성을 변경하기 전에 SMTP 서버 관리자에게 확인하십시오.
	  • 랙 PDU에서 전자- 메일을 외부 메일 계정에 전달할 수 있도록 특수 전자 메일 계정을 설정합니다.
	• Recipient: 수신자의 SMTP 서버에 직접 전달하는 방법입니다. 이 설정을 사용하면 랙 PDU가 전자 메일을 한 번만 전송합니다. 사용 중인 원격 SMTP 서버에서 시간 제한으로 인해 일부 전자 메일이 전송되지 않을 수 있습니다.
	수신자가 랙 PDU의 SMTP 서버를 사용할 경우 이 설정은 유효하지 않습니다.

Format	긴 형식에는 이름, 위치, 연락처, IP 주소, 장치의 일련 번호, 날짜 및 시간, 이벤트 코드 및 이벤트 설명이 포함됩니다. 짧은 형식은 이벤트 설명만 제공합니다.
User Name Password Confirm Password	메일 서버에서 인증이 필요한 경우 여기에 사용자 이름과 암호를 입력합니다. 이는 SSl가 아닌 단순 인증을 수행합니다.

전자메일 테스트.

경로: Administration > Notification > E- mail > test

구성된 수신자에게 테스트 메시지를 전송합니다.

SNMP 트랩

트랩 수신기.

경로: Administration > Notification > SNMP Traps > trap receivers

NMS IP/호스트 이름을 기준으로 트랩 수신기를 표시합니다. 최대 6개의 트랩 수신기를 구성할 수 있습니다.

- 새로운 트랩 수신기를 구성하려면 Add Trap Receiver를 클릭합니다.
- 트랩 수신기를 수정 또는 삭제하려면 먼저 IP 주소 또는 호스트 이름을 클릭하여 설정에 액세스합니다. (트랩 수신기를 삭제하면 삭제된 트랩 수신기의 이벤트 조치에 구성된 모든 알림 설정이 기본값으로 설정됩니다.)
- 트랩 수신기의 트랩 유형을 지정하려면 SNMPv1 또는 SNMPv3 라디오 버튼을 선택합니다. 두 가지 트랩 유형을 모두 수신하는 NMS의 경우 각 트랩 유형에 대해 하나씩 해당 NMS에 대한 두 개의 트랩 수신기를 구성해야 합니다.

항목	정의
Trap Generation	이 트랩 수신기에 대한 트랩 생성을 활성화(기본값) 또는 비활성화합니다.
NMS IP/Host Name	이 트랩 수신기의 IPv4/ IPv6 주소 또는 호스트 이름입니다. 기본값 0.0.0.0은 트랩 수신기를 정의하지 않은 상태로 그대로 둡니다.

SNMPv1 옵션.

항목	정의
Community Name	이 트랩 수신기에 SNMPv1 트랩이 전송될 때 식별자(ID)로 사용되는 이름(기본값: **public**)입니다.
Authenticate Traps	이 옵션을 설정(기본값)하면 NMS IP/호스트 이름 설정으로 식별된 NMS가 인증 트랩(이 장치에 대해 유효하지 않은 로그온 시도로 인해 생성된 트랩)을 수신합니다. 기능을 사용하지 않으려면 확인란 선택을 취소합니다.

SNMPv3 옵션. 이 트랩 수신기에 대한 사용자 프로필의 식별자(ID)를 선택합니다. (여기서 선택 가능한 사용자 이름으로 식별된 사용자 프로필 설정을 보려면 상단 메뉴 표시줄에서 **Network**를 선택하고 왼쪽 탐색 메뉴의 **SNMPv3**에서 **user profiles**를 선택합니다.)

사용자 프로필을 생성하고 인증 및 암호화 방법을 선택하는 방법에 대해서는 SNMPv3을 참조하십시오.

SNMP 트랩 테스트

경로: Administration > Notification > SNMP Traps > test

Last Test Result. 가장 최근의 SNMP 트랩 테스트 결과입니다. 성공적인 SNMP 트랩 테스트는 트랩이 전송되었는지 여부만 확인하며, 선택한 트랩 수신기에 트랩이 수신되었는지는 확인하지 않습니다. 다음 항목 모두가 참(True)이면 트랩 테스트가 성공합니다.

- 선택한 트랩 수신기에 대해 구성된 SNMP 버전(SNMPv1 또는 SNMPv3)이 이 장치에서 활성화된 경우
- 트랩 수신기가 활성화된 경우
- **To** 주소에서 호스트 이름을 선택한 경우 해당 호스트 이름을 유효한 IP 주소로 매핑할 수 있는 경우

To. 테스트 SNMP 트랩을 전송할 IP 주소 또는 호스트 이름을 선택합니다. 트랩 수신기가 구성되지 않은 경우 **Trap Receiver** 구성 페이지로 연결되는 링크가 표시됩니다.

Syslog

경로: Logs > Syslog > *options*

랙 PDU는 이벤트 발생 시 최대 4개의 Syslog 서버에 메시지를 전송할 수 있습니다. Syslog 서버는 네트워크 장치에서 발생한 이벤트를 이벤트에 대한 중앙 집중식 레코드를 제공하는 로그에 기록합니다.

이 사용 설명서에서는 Syslog 또는 Syslog 구성 값에 대해 자세히 설명하지 않습니다. Syslog에 대한 자세한 내용은 RFC3164를 참조하십시오.

Syslog 서버 확인.

경로: Logs > Syslog > servers

설정	정의
Syslog Server	IPv4/IPv6 주소 또는 호스트 이름을 사용하여 4개의 서버 중 랙 PDU에서 전송된 Syslog 메시지를 수신하는 서버를 식별합니다.
Port	랙 PDU가 Syslog 메시지를 발송하는 데 사용할 사용자 데이터그램 프로토콜(UDP) 포트입니다. 기본값은 Syslog에 할당된 UDP 포트의 번호인 514입니다.
Protocol	모든 Syslog 메시지에 사용할 언어를 선택합니다.

Syslog 설정.

경로: Logs > Syslog > settings

설정	정의
Message Generation	Syslog 기능을 활성화하거나(기본값) 비활성화합니다.
Facility Code	랙 PDU의 Syslog 메시지에 할당된 시설 코드를 선택합니다(기본값 User) **참고:** 랙 PDU에서 전송된 Syslog 메시지를 가장 잘 정의할 수 있는 옵션은 User입니다. 네트워크 또는 시스템 관리자가 요구하지 않는 한 이 선택 옵션을 변경하지 마십시오.
Severity Mapping	사용 가능한 Syslog 우선순위에 랙 PDU 또는 환경 이벤트에 대한 각각의 심각성 수준을 매핑합니다. 매핑을 변경할 필요는 없습니다. 다음 정의는 RFC3164에서 인용한 내용입니다. • Emergency: 시스템 사용 불가 • Alert: 즉시 조치해야 함 • Critical: 위험 조건 • Error: 오류 조건 • Warning: 경고 조건 • Notice: 정상이지만 중대한 상태 • Informational: 정보 메시지 • Debug: 디버그 단계 메시지 다음은 Local Priority 설정에 대한 기본 설정입니다. • Severe는 Critical에 매핑됩니다. • Warning은 Warning에 매핑됩니다. • Informational은 Info에 매핑됩니다. **참고:** Syslog 메시지를 해제하려면 이벤트 조치 구성을 참조하십시오.

Syslog 테스트 및 형식 예.

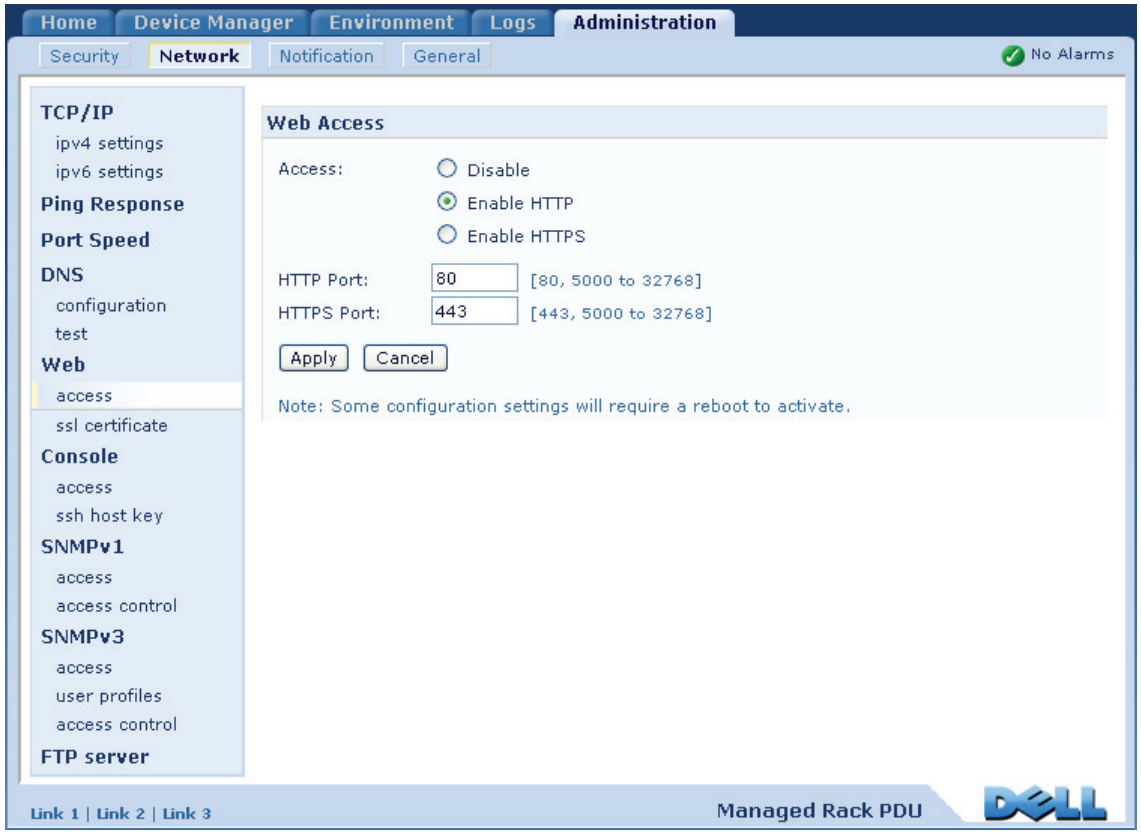
경로: Logs > Syslog > test

servers 옵션을 통해 구성된 Syslog 서버로 테스트 메시지를 전송합니다.

1. 심각성을 선택하여 테스트 메시지에 할당합니다.
2. 필수 메시지 필드에 따라 테스트 메시지를 정의합니다.
   - 우선순위(PRI): 메시지 이벤트에 할당된 Syslog 우선순위, 랙 PDU에서 전송된 메시지의 시설 코드.
   - 헤더: 타임 스탬프와 랙 PDU의 IP 주소.
   - 메시지(MSG) 부분:
     - TAG 필드 다음에 콜론과 공백으로 구성되며, 이벤트 유형을 식별합니다.
     - CONTENT 필드는 이벤트 텍스트이며 끝에서 한 칸 띄운 다음(옵션) 이벤트 코드를 표시합니다.

       예: **`Dell: Test Syslog`**가 유효합니다.

관리: 네트워크 기능


Home
Device Manager
Environment
Logs
Administration
Security
Network
Notification
General
No Alarms
TCP/IP
ipv4 settings
ipv6 settings
Ping Response
Port Speed
DNS
configuration
test
Web
access
ssl certificate
Console
access
ssh host key
SNMPv1
access
access control
SNMPv3
access
user profiles
access control
FTP server
Web Access
Access:
Disable
Enable HTTP
Enable HTTPS
HTTP Port:
80
[80, 5000 to 32768]
HTTPS Port:
443
[443, 5000 to 32768]
Apply
Cancel
Note: Some configuration settings will require a reboot to activate.
Link 1 | Link 2 | Link 3
Managed Rack PDU

TCP/IP 및 통신 설정

TCP/IP 설정

경로: Administration > Network > TCP/IP

상단 메뉴 표시줄에서 **네트워크** 선택 시 기본적으로 선택되어 있는 왼쪽 탐색 메뉴의 TCP/IP 옵션에는 랙 PDU의 현재 IPv4 주소, 서브넷 마스크, 기본 게이트웨이, MAC 주소 및 부팅 모드가 표시됩니다.

DHCP 및 DHCP 옵션에 대한 자세한 내용은 RFC2131 및 RFC2132를 참조하십시오.

설정	설명
Enable	이 확인란을 선택하면 IPv4가 활성화 또는 비활성화됩니다.
Manual	IP 주소, 서브넷 마스크 및 기본 게이트웨이를 입력하여 IPv4를 수동으로 구성합니다.
1. 일반적으로 구성 페이지에 있는 이러한 세 가지 설정의 기본값은 변경할 필요가 없습니다. •Vendor Class: DELL •Client ID: LAN에서 고유하게 식별되는 랙 PDU의 MAC 주소입니다. •User Class: 응용 프로그램 펌웨어 모듈 이름입니다.	

설정	설명
BOOTP	BOOTP 서버에서 TCP/IP 설정을 제공합니다. 32초 간격으로 랙 PDU가 모든 BOOTP 서버에서 네트워크 할당을 요청합니다. • 랙 PDU가 유효한 응답을 수신하면 네트워크 서비스가 시작됩니다. • 랙 PDU가 BOOTP 서버를 발견했지만 서버에 대한 요청이 실패 또는 타임아웃되면 랙 PDU는 다시 시작할 때까지 네트워크 설정 요청을 중지합니다. • 기본적으로 이전에 구성한 네트워크 설정이 존재하고 랙 PDU가 5번의 요청(처음 요청과 4번의 재시도)을 받지 못하면 액세스 가능한 상태를 유지할 수 있도록 이전에 구성된 설정이 사용됩니다. 재시도 횟수 또는 모든 재시도가 실패했을 때 취할 조치를 변경하려면 Next>>를 클릭하여 BOOTP 구성 페이지에 액세스합니다[1]. • Maximum retries: 유효한 응답이 수신되지 않을 때 발생하는 재시도 횟수를 입력하거나 재시도 횟수를 무제한으로 설정하려면 제로(0)를 입력합니다. • If retries fail: Use prior settings(기본값) 또는 Stop BOOTP request를 선택합니다.
DHCP	기본 설정입니다. 32초 간격으로 랙 PDU가 모든 DHCP 서버에서 네트워크 할당을 요청합니다. • 랙 PDU가 유효한 응답을 수신한 경우 네트워크 서비스를 임시 할당하여 시작하기 위해 DHCP 서버의 벤더 쿠키가 필요하지 않습니다. • 랙 PDU가 DHCP 서버를 발견했지만 서버에 대한 요청이 실패 또는 타임아웃되면 랙 PDU는 다시 시작할 때까지 네트워크 설정 요청을 중지합니다[1]. • Require vendor specific cookie to accept DHCP Address: 이 확인란을 선택하는 경우 랙 PDU에 정보를 제공하는 쿠키를 DHCP 서버가 제공하도록 설정해야 합니다.

1. 일반적으로 구성 페이지에 있는 이러한 세 가지 설정의 기본값은 변경할 필요가 없습니다.
   •Vendor Class: DELL
   •Client ID: LAN에서 고유하게 식별되는 랙 PDU의 MAC 주소입니다.
   •User Class: 응용 프로그램 펌웨어 모듈 이름입니다.

DHCP 응답 옵션

유효한 각 DHCP 응답에는 네트워크에서 랙 PDU를 작동하기 위해 필요한 TCP/IP 설정을 제공하는 옵션과 랙 PDU의 작동에 영향을 미치는 다른 정보가 있습니다.

Vendor Specific Information(옵션 43). 랙 PDU는 DHCP 응답 시 이 옵션을 사용하여 DHCP 응답의 유효성을 결정합니다. 이 옵션에는 공급업체 쿠키라고 하는 TAG/LEN/DATA 형식의 고유 옵션이 포함되어 있습니다. 이 항목은 기본적으로 비활성화됩니다.

- **Vendor Cookie. Tag 1, Len 4, Data "1APC"**
  옵션 43은 DHCP 서버가 Dell 랙 PDU를 관리하도록 구성되었음을 랙 PDU에 알립니다.
  다음은 벤더 쿠키가 포함된 Vendor Specific Information 옵션의 예(16진 형식)입니다.

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
```

TCP/IP 옵션. 유효한 DHCP 응답에 다음 옵션을 사용하여 랙 PDU의 TCP/IP 설정을 지정합니다. 첫 번째 옵션을 제외한 모든 옵션은 RFC2132에 설명되어 있습니다.

- **IP Address**(DHCP 응답의 **yiaddr** 필드에서, RFC2131에 설명되어 있음): DHCP 서버가 랙 PDU에 임시 할당하는 IP 주소입니다.
- **Subnet Mask**(옵션 1): 네트워크 상에서 랙 PDU가 작동해야 하는 서브넷 마스크 값입니다.
- **Router**, 즉 기본 게이트웨이(옵션 3): 네트워크 상에서 랙 PDU가 작동해야 하는 기본 게이트웨이 주소입니다.
- **IP Address Lease Time**(옵션 51): 랙 PDU에 IP 주소를 임시 할당하는 기간입니다.
- **Renewal Time, T1**(옵션 58): IP 주소가 임시 할당된 후 갱신을 요청하기까지 랙 PDU가 대기해야 하는 시간입니다.
- **Rebinding Time, T2**(옵션 59): IP 주소가 임시 할당된 후 리바인딩을 요청하기까지 랙 PDU가 대기해야 하는 시간입니다.

기타 옵션. 또한 랙 PDU는 유효한 DHCP 응답 내에서 이들 옵션을 사용합니다. 마지막 옵션을 제외한 모든 옵션은 RFC2132에 설명되어 있습니다.

- Network Time Protocal Servers(옵션 42): 랙 PDU가 사용할 수 있는 최대 2개의 NTP 서버를 나타냅니다(기본 및 보조).
- Time Offset(옵션 2): 세계 협정시(UTC)와 랙 PDU 서브넷의 시차(단위: 초)를 나타냅니다.
- Domain Name Server(옵션 6): 랙 PDU가 사용할 수 있는 최대 2개의 DNS(Domain Name System) 서버를 나타냅니다(기본 및 보조).
- Host Name(옵션 12): 랙 PDU에 사용되는 호스트 이름입니다(최대 32자).
- Domain Name(옵션 15): 랙 PDU가 사용하는 도메인 이름(최대 64자).
- Boot File Name(DHCP 응답의 file 필드에서, RFC2131에 설명되어 있음): 다운로드할 사용자 구성 파일(.ini 파일)에 대해 정규화된 디렉토리 경로입니다. DHCP 응답의 siaddr 필드는 랙 PDU가 .ini 파일을 다운로드할 서버의 IP 주소를 지정합니다. 다운로드 후, 랙 PDU 는 .ini 파일을 부팅 파일로 사용하여 설정을 재구성합니다.

경로: Administration > Network > TCP/IP > IPv6 settings

설정	설명
Enable	이 확인란을 선택하면 IPv6이 활성화 또는 비활성화됩니다.
Manual	IP 주소와 기본 게이트웨이를 입력하여 IPv6을 수동으로 구성합니다.
Auto Configuration	Auto Configuration 확인란을 선택하면 시스템이 라우터로부터 주소 지정 접두어를 가져옵니다(사용 가능한 경우). 이러한 접두어를 사용하여 IPv6 주소를 자동으로 구성합니다.

설정	설명
DHCPv6 Mode	Router Controlled: 이 옵션을 선택하면 DHCPv6이 IPv6 라우터 알림에 수신된 Managed(M) 및 Other(O) 플래그에 의해 제어됨을 의미합니다. 라우터 알림이 수신되면 NMC는 M 또는 O 플래그가 설정되었는지를 확인합니다. 다음의 경우 MNC가 M (관리 대상 주소 구성 플래그) 및 O (기타 유상태 구성 플래그) "비트"의 상태를 해석합니다. • *Neither is set*: 로컬 네트워크에 DHCPv6 인프라가 없음을 나타냅니다. NMC는 라우터 알림과 수동 구성을 사용하여 로컬 및 기타 설정과 연결되지 않은 주소를 가져옵니다. • *M, or M and O are set*: 이 경우에는 전체 DHCPv6 주소 구성이 이루어집니다. 주소와 기타 구성 설정을 가져오는 데 DHCPv6이 사용됩니다. 이를 DHCPv6 stateful이라 합니다. M 플래그가 수신된 후, 문제가 있는 인터페이스가 종료할 때까지 DHCPv6 주소 구성이 설정된 상태로 유지됩니다. M 플래그가 설정되지 않은 상황에서 후속 라우터 알림 패킷이 수신된 경우에도 마찬가지입니다. O 플래그가 먼저 수신되고 이후 M 플래그가 수신되면, NMC는 M 플래그 수신 시 전체 주소 구성을 수행합니다. • *Only O is set:* 이 경우 NMC가 DHCPv6 정보 요청 패킷을 전송합니다. "기타" 설정(예: DNS 서버 위치)을 구성하는 데 DHCPv6이 사용되지만, 주소를 제공하지는 않습니다. 이를 DHCPv6 stateless라 합니다. Address and Other Information: 이 라디오 버튼을 선택하면 주소 및 기타 구성 설정을 가져오는 데 DHCPv6이 사용됩니다. 이를 DHCPv6 stateful이라 합니다. Non-Address Information Only: 이 라디오 버튼을 선택하면 "기타" 설정(예: DNS 서버 위치)을 구성하는 데 DHCPv6이 사용되지만, 주소를 제공하지는 않습니다. 이를 DHCPv6 stateless라 합니다. Never: 이 옵션을 선택하면 DHCPv6이 비활성화됩니다.

Ping 응답

경로: Administration > Network > Ping Response

네트워크 관리 카드가 네트워크 핑에 응답할 수 있게 하려면 IPv4 Ping Response에서 사용 확인란을 선택합니다. 이 확인란 선택을 취소하면 NMC 응답이 비활성화됩니다. 이 항목은 IPv6에 적용되지 않습니다.

포트 속도

경로: Administration > Network > Port Speed

Port Speed 설정은 TCP/IP 포트의 통신 속도를 정의합니다.

- Auto-negotitaion(기본값)의 경우, 이더넷 장치가 가능한 최고 속도로 전송하도록 조절되지만, 지원되는 두 장치의 속도가 일치하지 않으면 둘 중 더 느린 속도가 사용됩니다.
- 또는 반- 이중(한 번에 한 방향으로만 통신)과 전-이중(동일 채널에서 동시에 양방향으로 통신) 옵션으로 구성된 10 Mbps 또는 100 Mbps를 선택할 수 있습니다.

DNS

경로: Administration > Network > DNS > *options*

DNS에 있는 옵션을 사용하여 DNS (Domain Name System)를 구성하고 테스트합니다.

- Primary DNS Server 또는 Secondary DNS Server를 선택하여 기본 및 보조 DNS 서버(옵션)의 IPv4 또는 IPv6 주소를 지정합니다. 랙 PDU에서 전자 메일을 전송하려면 최소한 기본 DNS 서버의 IP 주소를 정의해야 합니다.
  - 랙 PDU는 최대 15초까지 기본 DNS 서버 또는 보조 DNS 서버(보조 DNS 서버가 지정된 경우)의 응답을 기다립니다. 랙 PDU가 15초 이내에 응답을 수신하지 않으면 전자 메일을 보낼 수 없습니다. 그러므로 랙 PDU와 동일한 세그먼트 또는 인접 세그먼트(단, WAN(Wide-Area Network)의 서버는 제외)의 DNS 서버를 사용하십시오.
  - DNS 서버의 IP 주소를 지정한 후 동일한 네트워크에 있는 컴퓨터의 DNS 이름을 입력해서 컴퓨터의 IP 주소를 조회하는 방법을 사용하여 DNS가 제대로 작동하는지 확인하십시오.
- Host Name: 호스트 이름을 구성하고 Domain Name 필드에 도메인 이름을 구성하면 사용자는 도메인 이름을 허용하는 랙 PDU 인터페이스의 모든 필드(전자 메일 주소 제외)에 호스트 이름을 입력할 수 있습니다.
- Domain Name (IPv4): 여기서만 도메인 이름을 구성할 수 있습니다. 도메인 이름을 허용하는 랙 PDU 인터페이스의 다른 필드(전자 메일 주소 제외)에 호스트 이름만 입력한 경우 랙 PDU는 이 도메인 이름을 추가합니다.
  - 도메인 이름을 추가하여 모든 지정된 호스트 이름의 확장 인스턴스를 무시하려면 도메인 이름 필드를 기본값인 `somedomain.com` 또는 **`0.0.0.0`**으로 설정합니다.
  - 예를 들어, 트랩 수신기를 정의하는 경우와 같이 특정 호스트 이름 항목의 확장을 무시하려면 끝에 마침표를 추가합니다. 랙 PDU은 끝에 마침표가 있는 호스트 이름(예: *`mySnmpServer.`*)을 정식 도메인 이름으로 인식하므로 도메인 이름이 추가되지 않습니다.

- Domain Name (IPv6): 여기서 IPv6 도메인 이름을 지정합니다.
- DNS 서버의 설정을 테스트하는 DNS 쿼리를 전송하려면 test를 선택합니다.
  - Query Type으로 DNS 쿼리에 사용할 방법을 선택합니다.
    - by Host: 서버의 URL 이름
    - by FQDN: 정식 도메인 이름
    - by IP: 서버의 IP 주소
    - by MX: 서버에서 사용하는 메일 교환기(MX)
  - Query Qyestion으로 선택한 쿼리 유형에 사용할 값을 식별합니다.

선택한 쿼리 유형	사용할 쿼리 질문
by Host	URL
by FQDN	정식 도메인 이름(*my_server.my_domain*)
by IP	IP 주소
by MX	메일 교환기 주소

  - Last Query Response 필드에 테스트 DNS 요청 결과가 표시됩니다.

웹

경로: Administration > Network > Web > *options*

옵션	설명

access	이러한 선택 항목의 변경 내용을 적용하려면 랙 PDU에서 로그오프합니다.
	• Disable: 웹 인터페이스에 대한 액세스를 비활성화합니다. (액세스를 다시 활성화하려면 명령줄에 로그인한 다음 **`http -S enable`** 명령을 입력합니다. HTTPS 액세스의 경우 **`https -S enable`**을 입력합니다.)
	• Enable HTTP (기본값): HTTP (Hypertext Transfer Protocol)는 사용자 이름과 암호를 사용하여 웹에 액세스하지만 전송 중 사용자 이름, 암호 및 데이터를 암호화하지 않습니다.
	• Enable HTTPS: SSL(Secure Sockets Layter)의 HTTPS(Hypertext Transfer Protocol)을 활성화합니다. SSL는 전송 중 사용자 이름, 암호 및 데이터를 암호화하고 디지털 인증서를 통해 랙 PDU를 인증합니다. HTTPS가 활성화되면 브라우저에 작은 자물쇠 아이콘이 표시됩니다.
	부록 B: 보안 핸드북의 "디지털 인증서 만들기 및 설치"를 참조하여 디지털 인증서를 사용하는 몇 가지 방법 중에서 적합한 방법을 선택합니다.
	HTTP Port: HTTP가 랙 PDU와 통신하는 데 사용하는 TCP/IP 포트를 정의합니다 (기본값: 80).
	HTTPS Port: HTTPS가 랙 PDU와 통신하는 데 사용하는 TCP/IP 포트를 정의합니다(기본값: 443).
	이들 포트에 대해 추가 보안을 위해 5000~32768까지 사용하지 않는 포트로 포트 설정을 변경할 수 있습니다. 이 경우 사용자는 브라우저 주소 필드에 콜론(:)을 사용하여 포트 번호를 지정해야 합니다. 예를 들어, 포트 번호가 5000이고 IP 주소가 152.214.12.114인 경우:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

옵션	설명
ssl certificate	보안 인증서를 추가, 교체 또는 제거합니다. Status: • Not installed: 인증서가 설치되지 않았거나 FTP 또는 SCP에 의해 잘못된 위치에 설치되었습니다. Add or Replace Certifcate File을 사용하여 인증서를 랙 PDU의 **\ssl**의 올바른 위치에 설치합니다. • Generating: 유효한 인증서가 발견되지 않기 때문에 랙 PDU에서 인증서를 생성하는 중입니다. • Loading: 랙 PDU에서 인증서를 활성화하고 있습니다. • Valid certificate: 유효한 인증서가 랙 PDU에 설치되어 있거나 랙 PDU에서 생성되었습니다. 인증서 내용을 보려면 이 링크를 클릭합니다. **유효하지 않은 인증서를 설치하거나 SSL 사용 시 로드된 인증서가 없는 경우** 랙 PDU**는 기본 인증서를 생성하고, 이로 인해 인터페이스에 대한 액세스가 최대 1분 정도 지연될 수 있습니다.** 기본 암호화 기반 보안에 대해 기본 인증서를 사용할 수 있지만, 로그온할 때마다 보안 경보 메시지가 표시됩니다. Add or Replace Certificate File: Security Wizard를 통해 생성된 인증서 파일을 입력하거나 검색합니다. 부록 B: 보안 핸드북의 “디지털 인증서 만들기 및 설치”를 참조하여 보안 마법사 또는 랙 PDU에서 생성하는 디지털 인증서의 사용 방법을 선택합니다. Remove: 현재 인증서를 삭제합니다.

콘솔

경로: Administration > Network > Console > *options*

옵션	설명

access	Telnet 또는 SSH (Secure Shell) 액세스에 대해 다음 중 하나를 선택합니다.
	• Disable: 명령줄 인터페이스에 대한 모든 액세스를 비활성화합니다.
	• Enable Telnet(기본값): 암호화 없이 Telnet이 사용자 이름, 암호 및 데이터를 전송합니다.
	• Enable SSH: SSH가 암호화된 형식으로 사용자 이름, 암호 및 데이터를 전송하며, 데이터 전송 중 데이터를 가로채거나 날조 또는 변경하려는 시도에 대한 보호 기능을 제공합니다.
	이러한 프로토콜에서 사용되는 포트 구성:
	• Telnet Port: 랙 PDU와 통신하는 데 사용되는 Telnet 포트입니다(기본값: 23). 추가 보안을 위해 5000~32768까지 사용하지 않는 포트로 포트 설정을 변경할 수 있습니다. 그런 다음 사용자가 Telnet 클라이언트 프로그램의 요청에 따라 콜론(:) 또는 공백을 사용하여 기본값이 아닌 포트를 지정해야 합니다. 예를 들어, 포트 5000과 IP 주소 152.214.12.114의 경우 Telnet 클라이언트에서 다음과 같은 명령 중 하나를 요청합니다.
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• SSH Port: 랙 PDU와 통신하는 데 사용되는 SSH 포트입니다(기본값: 22). 추가 보안을 위해 5000~32768까지 사용하지 않는 포트로 포트 설정을 변경할 수 있습니다. 기본 포트가 아닌 포트를 지정하려면 명령줄 형식에 대한 SSH 클라이언트 설명서를 참조하십시오.

옵션	설명
ssh host key	Status는 호스트 키(개인 키)의 상태를 나타냅니다. • SSH Disabled: No host key in use: 이 옵션이 비활성화되면 SSH가 호스트 키를 사용할 수 없습니다. • Generating: 유효한 호스트 키가 발견되지 않았기 때문에 랙 PDU가 호스트 키를 생성하는 중입니다. • Loading: 랙 PDU에서 호스트 키를 활성화하고 있습니다. • Valid: 다음의 유효한 호스트 키 중 하나가 /ssh 디렉토리에 있습니다(랙 PDU에서 필요한 위치). •Security Wizard에 의해 생성된 1024비트 또는 2048비트 호스트 키 •랙 PDU에 의해 생성된 2048비트 RSA 호스트 키 Add or Replace: Security Wizard에 의해 생성된 호스트 키 파일을 찾아 업로드합니다. 보안 마법사를 사용하려면 부록 B: 보안 핸드북을 참조하십시오. **참고:** SSH를 활성화하는 데 필요한 시간을 줄이려면 미리 호스트 키를 생성하여 업로드하십시오. **호스트 키를 업로드하지 않고 SSH를 활성화하면** 랙 PDU**가 호스트 키를 생성하는 데 최대 1분 정도 걸리며, 이 시간 동안 SSH 서버에 액세스할 수 없습니다.** Remove: 현재 호스트 키를 제거합니다.

SSH를 사용하려면 SSH 클라이언트가 설치되어 있어야 합니다. 대부분의 Linux 및 다른 UNIX 플랫폼에는 SSH 클라이언트가 포함되어 있지만, Microsoft Windows 운영 체제에는 포함되어 있지 않습니다. 클라이언트는 여러 공급업체로부터 구매할 수 있습니다.

SNMP

SNMP의 모든 사용자 이름, 암호 및 커뮤니티 이름은 네트워크에서 일반 텍스트로 전송됩니다. 네트워크에 높은 암호화 보안이 필요한 경우 SNMP 액세스를 비활성화하거나 각 커뮤니티의 액세스를 읽기 권한으로 설정하십시오. (읽기 권한을 가진 커뮤니티는 상태 정보를 수신하고 SNMP 트랩을 사용할 수 있습니다.)

사용자 시스템 보안 강화 및 관리에 대한 자세한 내용은 부록 B: 보안 핸드북을 참조하십시오.

SNMPv1

경로: Administration > Network > SNMPv1 > *options*

옵션	설명
access	Enable SNMPv1 Access: 이 장치와의 통신 방법으로 SNMP 버전 1을 활성화합니다.
access control	최대 4개의 액세스 제어 항목을 구성하여 네트워크 관리 시스템(NMS)이 이 장치에 대해 갖는 액세스 권한을 지정할 수 있습니다. 기본적으로 액세스 제어 첫 페이지에는 사용 가능한 4개의 SNMPv1 커뮤니티 각각에 대해 하나의 항목이 할당되어 있지만, 커뮤니티에 둘 이상의 항목을 적용하여 여러 개의 구체적인 IPv4 및 IPv6 주소, 호스트 이름 또는 IP 주소 마스크에 따라 액세스 권한을 부여하도록 이러한 설정을 편집할 수 있습니다. 커뮤니티에 대한 액세스 제어 설정을 편집하려면 커뮤니티 이름을 클릭합니다. • 커뮤니티에 대해 기본 액세스 제어 항목을 변경하지 않은 상태로 두면 해당 커뮤니티는 네트워크 상의 어떤 위치에서 이 장치에 액세스할 수 있습니다. • 한 커뮤니티 이름에 대해 여러 개의 액세스 제어 항목을 구성할 경우, 4개의 항목에 대해 나머지 하나 이상의 커뮤니티에 액세스 제어 항목이 없어야 한다는 제한이 적용됩니다. 커뮤니티에 액세스 제어 항목이 표시되지 않으면 해당 커뮤니티는 이 장치에 대한 액세스 권한이 없는 것입니다. Community Name: 커뮤니티에 액세스할 때 NMS가 사용해야 하는 이름입니다. 최대 길이는 15자의 ASCII 문자이며, 4개의 커뮤니티에 대한 기본 커뮤니티 이름은 **public**, **private**, **public2** 및 **private2**입니다. NMS IP/Host Name: NMS에 의해 액세스가 제어되는 IPv4 또는 IPv6 주소, IP 주소 마스크 또는 호스트 이름입니다. 호스트 이름과 149.225.12.1과 같은 특정 IP 주소만 사용하여 해당 위치에서 NMS에 액세스할 수 있습니다. 255 제한 액세스를 포함하는 IP 주소는 다음과 같습니다. • 149.225.12.225: 149.225.12 세그먼트에서만 NMS에 액세스합니다. • 149.225.225.255: 149.225 세그먼트에서만 NMS에 액세스합니다. • 149.225.255.255: 149 세그먼트에서만 NMS에 액세스합니다. • 255.255.255.255로도 표시할 수 있는 0.0.0.0 (기본 설정): 어떤 세그먼트에서도 NMS에 액세스합니다. Access Type: 커뮤니티를 통해 NMS가 수행할 수 있는 작업입니다. • Read: GETS만, 항상. • Write: 항상 GETS, 웹 인터페이스 또는 명령줄 인터페이스에 로그온한 사용자가 없을 경우 SETS. • Write+: 항상 GETS 및 SETS. • Disable: 항상 GETS 또는 SETS 없음.

SNMPv3

경로: Administration > Network > SNMPv3 > *options*

SNMP GET, SET 및 트랩 수신기의 경우 SNMPv3은 사용자 프로파일 시스템을 사용하여 사용자를 식별합니다. SNMPv3 사용자가 GET 및 SET를 수행하고 MIB를 찾아 트랩을 수신하기 위해서는 MIB 소프트웨어 프로그램에 사용자 프로파일이 할당되어 있어야 합니다.

SNMPv3을 사용하려면 SNMPv3을 지원하는 MIB 프로그램이 있어야 합니다.

랙 PDU는 SHA 또는 MD5 인증과 AES 또는 DES 암호화를 지원합니다.

옵션	설명
access	SNMPv3 Access: 이 장치와의 통신 방법으로 SNMPv3을 활성화합니다.

옵션	설명
user profiles	기본적으로 dell snmp profile1에서 dell snmp profile4까지의 사용자 이름과 인증 없음, 프라이버시 없음(암호화 없음)으로 구성된 4개의 사용자 프로필 설정이 표시됩니다. 사용자 프로필에 대해 다음 설정을 편집하려면 목록에서 사용자 이름을 클릭합니다. User Name: 사용자 프로필 식별자입니다. SNMP 버전 3은 프로필의 사용자 이름과 전송할 데이터 패킷의 사용자 이름을 일치시켜 GET, SET 및 트랩을 매핑합니다. 사용자 이름에는 최대 32자의 ASCII 문자를 사용할 수 있습니다. Authentication Passphrase: SNMPv3을 통해 이 장치와 통신 중인 NMS가 클레임 대상 NMS인지, 전송 중 메시지가 변경되지 않았는지, 지연 없이 적시에 메시지가 전송되고 나중에 부적절한 시간에 메시지가 복사 또는 재전송되지 않았는지를 확인하는 15~32자의 ASCII 문자로 구성된 구문(기본값: **dell auth passphrase**)입니다. Privacy Passphrase: NMS가 이 장치로 전송하거나 SNMPv3을 통해 이 장치로부터 수신하는 데이터의 프라이버시를 보장(암호화를 통해)하는 15~32자의 ASCII 문자로 구성된 구문(기본값: **dell crypt passphrase**)입니다. Authentication Protocol: Dell이 구현한 SNMPv3은 SHA와 MD5 인증을 지원합니다. 인증 프로토콜을 선택하지 않은 한 인증은 발생하지 않습니다. Privacy Protocol: Dell이 구현한 SNMPv3은 데이터 암호화 및 암호화 해독을 위한 프로토콜로 AES와 DES를 지원합니다. 전송된 데이터의 프라이버시를 보장하기 위해서는 프라이버시 프로토콜을 선택해야 하며, NMS의 요청 시 프라이버시 구문을 입력해야 합니다. 프라이버시 프로토콜이 사용되었지만 NMS가 프라이버시 암호 구문을 제공하지 않으면 SNMP 요청이 암호화되지 않습니다. 참고: 인증 프로토콜이 선택되지 않은 경우 프라이버시 프로토콜을 선택할 수 없습니다.

옵션	설명
access control	최대 4개의 액세스 제어 항목을 구성하여 NMS가 이 장치에 대해 갖는 액세스 권한을 지정할 수 있습니다. 기본적으로 액세스 제어 첫 페이지에는 4개의 사용자 프로필 각각에 대해 하나의 항목이 할당되어 있지만, 사용자 프로필에 둘 이상의 항목을 적용하여 여러 개의 구체적인 IP 주소, 호스트 이름 또는 IP 주소 마스크에 따라 액세스 권한을 부여하도록 이러한 설정을 편집할 수 있습니다. • 사용자 프로필에 대해 기본 액세스 제어 항목을 변경하지 않은 상태로 두면, 해당 프로필을 사용하는 모든 NMS가 이 장치에 액세스할 수 있습니다. • 한 사용자 프로필에 대해 여러 개의 액세스 항목을 구성할 경우, 4개의 항목에 대해 나머지 하나 이상의 사용자 프로필에 액세스 제어 항목이 없어야 한다는 제한이 적용됩니다. 사용자 프로필에 액세스 제어 항목이 표시되지 않으면 해당 프로필을 사용하는 NMS는 이 장치에 대한 액세스 권한이 없는 것입니다. 사용자 프로필에 대한 액세스 제어 설정을 편집하려면 사용자 이름을 클릭합니다. Access: 이 액세스 제어 항목의 매개변수로 지정된 액세스 제어를 활성화하려면 Enable 확인란을 선택합니다. User Name: 드롭다운 목록에서 이 액세스 제어 항목을 적용할 사용자 프로필을 선택합니다. 사용 가능한 선택 옵션은 왼쪽 탐색 메뉴의 user profiles를 통해 구성한 4개의 사용자 이름입니다. NMS IP/Host Name: NMS에 의해 액세스가 제어되는 IP 주소, IP 주소 마스크 또는 호스트 이름입니다. 호스트 이름과 149.225.12.1과 같은 특정 IP 주소만 사용하여 해당 위치에서 NMS에 액세스할 수 있습니다. 255 제한 액세스를 포함하는 IP 주소는 다음과 같습니다. • 149.225.12.225: 149.225.12 세그먼트에서만 NMS에 액세스합니다. • 149.225.225.255: 149.225 세그먼트에서만 NMS에 액세스합니다. • 149.225.255.255: 149 세그먼트에서만 NMS에 액세스합니다. • 255.255.255.255로도 표시할 수 있는 0.0.0.0 (기본 설정): 어떤 세그먼트에서도 NMS에 액세스합니다.

FTP 서버

경로: Administration > Network > FTP Server

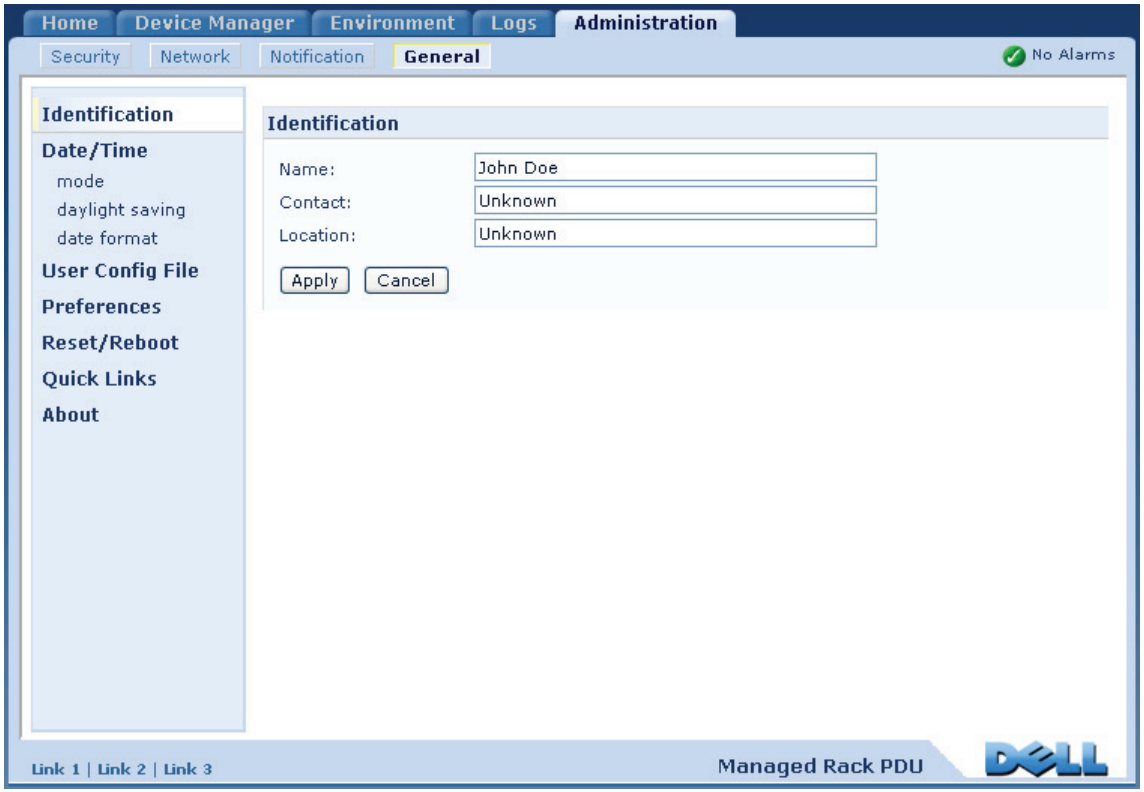
FTP Server 설정은 FTP 서버에 대한 액세스를 활성화(기본값) 또는 비활성화하며 FTP 서버가 랙 PDU와 통신하는 데 사용하는 TCP/IP 포트(기본값: 21)를 지정합니다. FTP 서버는 지정된 포트와 지정된 포트보다 한 자리가 낮은 포트 둘 다 사용합니다.

추가적인 보안을 위해 5001~32768 중에서 사용되지 않은 포트 번호로 Port 설정을 변경합니다. 사용자는 기본값이 아닌 포트 번호를 지정하려면 콜론(:)을 사용해야 합니다. 예를 들어, 포트 5001과 IP 주소 152.214.12.114의 경우 명령은 **`ftp 152.214.12.114:5001`**입니다.

FTP에서는 파일을 암호화하지 않고 전송합니다. 보안을 강화하려면 FTP 서버를 비활성화하고 SCP를 사용하여 파일을 전송합니다. SSH (Secure Shell)를 선택하고 구성하면 SCP가 자동으로 활성화됩니다.

사용자 시스템 보안 강화 및 관리에 대한 자세한 내용은 부록 B: 보안 핸드북을 참조하십시오.

관리: 일반 옵션


Home
Device Manager
Environment
Logs
Administration
Security
Network
Notification
General
No Alarms
Identification
Date/Time
mode
daylight saving
date format
User Config File
Preferences
Reset/Reboot
Quick Links
About
Identification
Name:
John Doe
Contact:
Unknown
Location:
Unknown
Apply
Cancel
Link 1 | Link 2 | Link 3
Managed Rack PDU

ID

경로: Administration > General > Identification

랙 PDU의 SNMP 에이전트에서 사용되는 Name(장치 이름), Location(실제 위치) 및 Contact(장치 담당자)를 정의합니다. 이 설정은 MIB-II sysName, sysContact 및 sysLocation OID(Object Identification)에서 사용하는 값입니다.

MIB-II OID에 대한 자세한 정보는 Dell MIB (Management Information Base)를 참조하십시오.

날짜 및 시간 설정

방법

경로: Administration > General > Date & Time > mode

랙 PDU에서 사용되는 시간과 날짜를 설정합니다. 현재 설정을 수동으로 변경하거나 NTP(Network Time Protocol) 서버를 통해 변경할 수 있습니다.

- Manual Mode: 다음 중 하나를 수행합니다.
  - 랙 PDU의 날짜와 시간을 입력합니다.
  - 사용 중인 컴퓨터의 날짜 및 시간 설정과 일치시키려면 Apply Local Computer Time 확인란을 선택합니다.
- Synchronize with NTP Server: NTP 서버가 랙 PDU의 날짜와 시간을 정의합니다.

설정	정의
Primary NTP Server	기본 NTP 서버의 IP 주소 또는 도메인 이름을 입력합니다.
Secondary NTP Server	보조 서버를 사용할 수 있는 경우 보조 NTP 서버의 IP 주소 또는 도메인 이름을 입력합니다.
Time Zone	시간대를 선택합니다. 목록에서 각 시간대 앞에 있는 시간 값은 이전에 그리니치 천문대 시간(GMT)이었던 세계 협정시(UTC)의 시차를 나타냅니다.
Update Interval	랙 PDU를 업데이트하기 위해 NTP 서버에 액세스하는 빈도(시간 단위)를 지정합니다. *최소*: 1; *최대*: 8760(1년).
Update Using NTP Now	NTP 서버를 사용하여 날짜와 시간을 즉시 업데이트합니다.

섬머타임

경로: Administration > General > Date & Time > daylight saving

기존의 US 섬머타임(DST)를 사용하거나 현지에서 섬머타임이 적용되는 방식과 일치시킨 사용자 정의 섬머타임을 사용하여 구성합니다. DST는 기본적으로 해제됩니다.

섬머타임(DST)을 사용자 정의하는 경우:

- 현지 DST가 항상 매달 지정된 넷째주(예: 넷째주 일요일)에 시작하거나 끝나는 경우, Fourth/Last를 선택합니다. 다음 연도의 해당 월에 다섯 번째 일요일이 있으면 네 번째 일요일에서 시간 설정이 변경됩니다.
- 현지 DST가 네 번째 또는 다섯 번째 요일의 존재 여부에 상관 없이 항상 매달 지정된 마지막 주에 시작하거나 끝나는 경우, Fifth/Last를 선택합니다.

형식

경로: Administration > General > Date & Time > date format

이 사용자 인터페이스에 모든 데이터를 표시하는 숫자 형식을 선택합니다. 선택 옵션에서 각 문자 m(월), d(일), y(년)는 1자릿수를 나타냅니다. 한 자리수 날짜와 달은 앞자리가 숫자 0으로 표시됩니다.

.ini 파일 사용

경로: Administration > General > User Config File

한 랙 PDU의 설정을 사용하여 다른 랙 PDU의 설정을 구성합니다. 구성된 랙 PDU에서 config.ini 파일을 검색하고 해당 파일을 사용자 정의한 다음(예: IP 주소 변경), 사용자 정의한 파일을 새 랙 PDU로 업로드합니다. 파일 이름에는 최대 64자를 사용할 수 있으며, 반드시 .ini로 끝나야 합니다.

Status	업로드 진행률을 보여줍니다. 파일에 오류가 있는 경우에도 업로드에 성공하나, 시스템 이벤트가 이벤트 로그에 오류를 보고합니다.
Upload	사용자 정의된 파일을 검색한 후 업로드합니다. 그러면 현재 랙 PDU가 이 파일을 사용하여 자체 구성을 설정할 수 있습니다.

구성된랙 PDU의 파일을 검색하고 사용자 정의하려면 구성 설정 내보내기 방법을 참조하십시오.

파일을 하나의 랙 PDU로 업그레이드하는 대신 FTP 또는 SCP 스크립트를 사용하여 여러 랙 PDU로 내보낼 수 있습니다.

이벤트 로그 및 온도 단위

경로: Administration > General > Preferences

이벤트 로그 텍스트 색상 코딩

이 항목은 기본적으로 비활성화됩니다. 이벤트 로그에 기록된 알람 텍스트의 색상 코딩을 사용하려면 Event Log Color Coding 확인란을 선택합니다. 시스템 이벤트 항목과 구성 변경 항목은 색상이 변경되지 않습니다.

텍스트 색상	알람 심각성
적색	Critical: 위험 알람이며 바로 조치를 취해야 합니다.
주황색	Warning: 주의가 필요한 알람으로, 원인을 해결하지 않을 경우 데이터 또는 장치가 손상될 수 있습니다.
녹색	Alarm Cleared: 알람이 진행될 수 있는 조건을 나타냅니다.
검정색	Normal: 알람이 존재하지 않습니다. 랙 PDU와 연결된 모든 장치가 정상적으로 작동하고 있습니다.

기본 온도 눈금 변경

이 사용자 인터페이스에 모든 온도 측정값을 표시할 온도 눈금(화씨 또는 섭씨)을 선택합니다.

랙 PDU 재설정

경로: Administration > General > Reset/Reboot

작업	정의
Reboot Management Interface	랙 PDU의 인터페이스를 다시 시작합니다.
Reset All[1]	모든 구성 값을 재설정하려면 Exclude TCP/IP 확인란의 선택을 취소하고, TCP/IP를 제외한 모든 값을 재설정하려면 Exclude TCP/IP 확인란을 선택합니다.
Reset Only[1]	TCP/IP settings: TCP/IP 구성을 기본 설정인 DHCP & BOOTP로 설정합니다. 이 경우 랙 PDU가 DHCP 또는 BOOTP 서버에서 TCP/IP 설정을 수신해야 합니다. TCP/IP 및 통신 설정을 참조하십시오.
	Event configuration: 이벤트 및 그룹에 따라 이벤트 구성에 대한 모든 변경 내용을 기본 설정으로 재설정합니다.
	RPDU to Defaults: 네트워크 설정은 제외하고 랙 PDU 설정만을 기본값으로 재설정합니다.
1. 재설정이 완료되기까지 최대 1분 정도 걸릴 수 있습니다.	

링크 구성

경로: Administration > General > Quick Links

각 인터페이스 페이지 왼쪽 하단에 표시되는 URL 링크를 보거나 변경하려면 상단 메뉴 표시줄에서 Administration 탭, General을 선택하고 왼쪽 탐색 메뉴에서 Quick Lingks를 선택합니다.

기본적으로 이들 링크는 다음 웹 페이지에 액세스합니다.

- Link 1: dell.com
- Link 2: dell.com/home
- Link 3: dell.com/business

다음 항목을 재구성하려면 Display 열에서 링크 이름을 클릭합니다.

- Display: 각 인터페이스 페이지에 표시되는 간략한 링크 이름
- Name: 링크 대상 또는 용도를 완전히 보여주는 이름
- Address: URL(예: 다른 장치 또는 서버의 URL)

랙 PDU 정보

경로: Administration > General > About

하드웨어 정보는 랙 PDU에 발생한 문제를 해결하는 데 유용합니다. 일련 번호 및 MAC 주소 또한 랙 PDU 자체에서 확인할 수 있습니다.

응용 프로그램 모듈, Dell OS(AOS) 및 부트 모니터의 펌웨어 정보는 이름, 펌웨어 버전, 각 펌웨어 모듈이 생성된 날짜와 시간을 나타냅니다. 이러한 정보는 문제 해결에도 유용합니다.

Management Uptime은 인터페이스가 연속해서 실행된 시간 길이를 나타냅니다.

구성 설정 내보내기 방법

.ini 파일 검색 및 내보내기

절차 요약

관리자가 랙 PDU의 .ini 파일을 복구하여 또 다른 랙 PDU나 여러 랙 PDU로 내보낼 수 있습니다.

1. 내보낼 설정으로 랙 PDU를 구성합니다.
2. 랙 PDU에서 .ini 파일을 불러옵니다.
3. 최소한 TCP/IP 설정을 변경하여 파일을 사용자 지정합니다.
4. 랙 PDU가 지원하는 파일 전송 프로토콜을 사용하여 사본을 1대 이상의 랙 PDU로 전송합니다. 여러 랙 PDU로 전송하려면 FTP 또는 SCP 스크립트를 사용합니다.

각각의 수신 랙 PDU는 이 파일을 사용하여 자체 설정을 재구성한 후 파일을 삭제합니다.

.ini 파일 내용

랙 PDU에서 불러오는 config.ini 파일에는 다음 내용이 있습니다.

- *섹션 제목* 및 *키워드*(파일을 불러온 장치에서 지원되는 경우만): 섹션 제목은 대괄호([ ])로 묶은 범주 이름을 나타냅니다. 각 섹션 제목 아래의 키워드는 특정 랙 PDU 설정을 설명하는 레이블입니다. 각 키워드 다음에는 등호와 값(기본값 또는 구성된 값)이 옵니다.
- **Override** 키워드: 이 키워드의 기본값을 사용할 경우 하나 이상의 키워드와 장치별 값의 내보내기가 차단됩니다. 예를 들어 **[NetworkTCP/IP]** 섹션에서 **Override** (랙 PDU의 MAC 주소) 블록에 기본값을 지정하면 **SystemIP**, **SubnetMask**, **DefaultGateway** 및 **BootMode** 값을 내보냅니다.

자세한 절차

불러오기. 내보낼 .ini 파일을 설정하고 불러오려면:

1. 가능하면 랙 PDU 인터페이스를 사용하여 파일을 설정하고 내보냅니다. .ini 파일을 직접 편집하면 오류가 발생할 위험이 있습니다.
2. FTP를 사용하여 구성된 랙 PDU에서 config.ini를 불러오려면:
   a. 랙 PDU의 IP 주소를 사용하여 랙 PDU에 연결합니다.

      ftp> open *ip_address*

   b. 관리자 사용자 이름과 암호를 사용하여 로그온합니다.
   c. 랙 PDU의 설정이 있는 config.ini 파일을 불러옵니다.

      ftp> get *config.ini*

   FTP를 실행한 폴더에 파일이 기록됩니다.

사용자 지정. 파일을 내보내기 전에 사용자 지정해야 합니다.

1. 텍스트 편집기를 사용하여 파일을 사용자 지정합니다.
   - 섹션 제목, 키워드 및 미리 정의된 값은 대/소문자를 구분하지 않지만 사용자가 정의하는 문자열 값은 대/소문자를 구분합니다.
   - 같이 없음을 나타내려면 따옴표를 이어 사용합니다. 예를 들어 **LinkURL1=""** 는 URL을 의도적으로 정의하지 않았음을 의미합니다.
   - 앞이나 뒤에 공백을 포함한 값 또는 이미 따옴표로 묶여 있는 값을 물음표로 묶습니다.
   - 예약된 이벤트를 내보내려면 .ini 파일에 직접 값을 구성합니다.
   - 최대한의 정확도로 시스템 시간을 내보내려면, 수신 랙 PDU가 네트워크 시간 프로토콜 서버에 액세스할 수 있는 경우 **NTPEnable**을 **enabled**로 구성합니다.

     NTPEnable=enabled

     또는 **[SystemDate/Time]**을 별도의 .ini 파일로 내보내면 전송 시간을 줄일 수 있습니다.
   - 설명을 추가하려면 각 설명 행을 세미콜론(;)으로 시작합니다.
2. 사용자 정의된 파일을 같은 폴더의 다른 파일 이름으로 복사합니다.
   - 파일 이름에는 최대 64자를 사용할 수 있으며, 반드시 .ini 확장자로 끝나야 합니다.
   - 사용자 지정된 원본 파일은 나중에 사용할 수 있도록 보존합니다. **보존하는 파일은 사용자 설명이 기록되어 있는 유일한 파일입니다.**

하나의 랙 PDU로 파일 전송. .ini 파일을 다른 랙 PDU로 전송하려면 다음을 수행합니다.

- 수신 랙 PDU의 웹 인터페이스에서 상단 메뉴 표시줄의 Administration 탭, General을 선택하고 왼쪽 탐색 메뉴에서 User Config File을 선택합니다. 파일의 전체 경로를 입력하거나 **찾아보기**를 사용합니다.
- 랙 PDU에서 지원되는 파일 전송 프로토콜(예: FTP, FTP 클라이언트, SCP 또는 TFTP)을 사용합니다. 다음 예는 FTP를 사용합니다.
  a. 사용자 지정 .ini 파일의 복사본이 있는 폴더에서 FTP를 사용하여 .ini 파일을 내보내려는 랙 PDU에 로그인합니다.

     ```
     ftp> open ip_address
     ```

  b. 사용자 지정한 .ini 파일의 사본을 수신 랙 PDU의 루트 디렉토리로 내보냅니다.

     ```
     ftp> put filename.ini
     ```

여러 랙 PDU로 파일 내보내기. .ini 파일을 여러 랙 PDU로 내보내려면 FTP 또는 SCP를 사용합니다. 하지만 랙 PDU 1대로 파일을 내보내는 절차를 통합하여 반복하는 스크립트를 작성합니다.

업로드 이벤트 및 오류 메시지

이벤트 및 관련 오류 메시지

수신 랙 PDU가 .ini 파일을 사용하여 설정을 업데이트하는 과정을 완료하면 다음의 이벤트가 발생합니다.

`Configuration file upload complete, with` *`number`* `valid values`

키워드, 섹션 이름 또는 값이 유효하지 않고 수신 랙 PDU의 업로드가 성공한 경우 추가 이벤트 텍스트에 오류가 나타납니다.

이벤트 텍스트	설명
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	잘못된 키워드 또는 값이 있는 행은 무시됩니다.
Configuration file warning: Invalid section on line *number*.	섹션 이름이 잘못된 경우 해당 섹션의 모든 키워드/값 쌍은 무시됩니다.
Configuration file warning: Keyword found outside of a section on line *number*.	파일의 시작 부분(섹션 제목 이전)에 입력된 키워드는 무시됩니다.
Configuration file warning: Configuration file exceeds maximum size.	파일이 너무 크면 업로드가 완료되지 않습니다. 파일의 크기를 줄이거나 두 파일로 나눈 다음 다시 업로드하십시오.

config.ini의 메시지

config.ini 파일을 다운로드하는 랙 PDU가 구성에 포함되려면 성공적으로 검출되어야 합니다. 랙 PDU가 없거나 검출되지 않으면 config.ini 파일은 키워드와 값 대신 적절한 섹션 이름 아래에 메시지를 포함합니다. 예:

```
Rack PDU not discovered
```

ini 파일을 가져올 때 랙 PDU의 구성을 내보내지 않은 경우 이 메시지를 무시하십시오.

무시된 값에 의해 발생하는 오류

Override 키워드와 해당 값은 값 내보내기를 차단하면 이벤트 로그에 오류 메시지를 기록합니다.

무시되는 값에 대한 자세한 내용은 .ini 파일 내용을 참조하십시오.

무시되는 값은 장치 고유 값이며 다른 랙 PDU로 내보내기에 적절하지 않기 때문에 이러한 오류 메시지를 무시합니다. **Override** 키워드가 있는 행과 무시된 값이 있는 행을 삭제하면 이 오류 메시지가 발생하지 않도록 할 수 있습니다. 섹션 제목이 있는 행은 삭제하거나 변경하지 마십시오.

파일 전송

펌웨어 업그레이드 방법

펌웨어 업그레이드의 장점

랙 PDU의 펌웨어를 업그레이드하는 경우:

- 최신 버그 수정이 적용되고 성능이 향상됩니다.
- 새 기능을 즉시 사용할 수 있습니다.

네트워크에서 펌웨어 버전을 일관되게 유지하면 모든 랙 PDU가 동일한 방법으로 같은 기능을 지원하게 됩니다.

펌웨어 파일

펌웨어 버전은 운영 체제(AOS) 모듈, 애플리케이션 모듈, 부트 모니터(bootmon) 모듈 등 세 가지 모듈로 구성됩니다. 각 모듈에는 전송 중 데이터 손상을 방지할 수 있도록 하나 이상의 CRC(Cyclical Redundancy Check: 주기적 리던던시 확인)가 포함되어 있습니다.

랙 PDU에 사용되는 운영 체제(AOS), 응용 프로그램 및 부트 모니터 모듈 파일은 동일한 기본 형식을 공유합니다.

dell_*hardware-version*_*type*_*firmware-version*.bin

- **dell**: 이 파일이 Dell 파일임을 나타냅니다.
- ***hardware-version***: **hw0***x*: 이 이진 파일을 사용할 하드웨어 버전을 나타냅니다.
- ***type***: 파일이 랙 PDU의 운영 체제(AOS) 모듈, 응용 프로그램 모듈 또는 부트 모니터 모듈인지를 확인합니다.
- ***version***: 파일의 버전 번호입니다.
- **bin**: 이 파일이 이진 파일임을 나타냅니다.

랙 PDU 정보를 참조하여 랙 PDU에 있는 각 펌웨어 모듈의 버전 번호를 확인하십시오.

펌웨어 파일 전송 방법

랙 PDU의 펌웨어를 업그레이드하려면 다음 방법 중 하나를 사용합니다.

- 지원되는 운영 체제의 네트워크에 연결된 컴퓨터에서 FTP 또는 SCP를 사용하여 개별 AOS 및 응용 프로그램 펌웨어 모듈을 전송할 수 있습니다.
- 네트워크에 있지 않은 랙 PDU의 경우 직렬 연결을 통해 XMODEM을 사용하여 컴퓨터의 개별 펌웨어 모듈을 랙 PDU로 전송할 수 있습니다.

개별 펌웨어 모듈을 전송할 경우 응용 프로그램 모듈을 전송하기 전에 랙 PDU에 운영 체제(AOS) 모듈을 **전송해야 합니다**.

FTP 또는 SCP를 사용한 하나의 랙 PDU 업그레이드

FTP. FTP를 사용하여 네트워크를 통해 하나의 랙 PDU를 업그레이드하려면:

- 랙 PDU를 네트워크에 연결하고 관리 카드의 시스템 IP, 서브넷 마스크 및 기본 게이트웨이를 구성해야 합니다.
- 랙 PDU에서 FTP 서버가 설정되어 있어야 합니다.
- 펌웨어 파일이 Dell.com에서 다운로드되었습니다.

파일을 전송하려면:

1. 네트워크 상의 컴퓨터에서 명령 프롬프트 창을 엽니다. 펌웨어 파일이 있는 디렉토리로 이동하고 파일 목록을 표시합니다.

   ```
   C:\>cd\dell
   C:\dell>dir
   ```

   나열된 파일에서 *xxx*는 펌웨어 버전 번호를 나타냅니다.

   - **dell_hw05_aos_*xxx*.bin**
   - **dell_hw05_application_*xxx*.bin**

2. FTP 클라이언트 세션을 엽니다.
   C:\dell>ftp
3. **open**과 IP 주소를 입력하고 랙 PDUEnterENTER를 누릅니다. FTP 서버에 대한 포트 설정을 기본값인 21에서 다른 값으로 변경한 경우 FTP 명령에 변경된 값을 사용해야 합니다.
   - Windows FTP 클라이언트의 경우 공백으로 IP 주소에서 변경된 포트 번호를 분리합니다. 예:
     ftp> open 150.250.6.10 21000
   - 일부 FTP 클라이언트에는 포트 번호 이전에 콜론이 필요합니다.
4. 관리자로 로그온합니다. 기본 사용자 이름과 암호는 모두 admin입니다.
5. AOS를 업그레이드합니다. (예에서 *xxx*는 펌웨어 버전 번호입니다.)
   ftp> bin
   ftp> put dell_hw05_aos_*xxx*.bin
6. FTP에서 전송을 확인할 때 quit를 입력하여 세션을 종료합니다.
7. 20초 후에 2~5 단계를 반복합니다. 5단계에서 응용 프로그램 모듈 파일 이름을 사용합니다.

SCP. SCP(Secure CoPy)를 사용하여 랙 PDU 펌웨어를 업그레이드하려면:

1. 앞의 FTP 지침에서 설명한 펌웨어 모듈을 확인하고 준비합니다.
2. SCP 명령줄을 사용하여 AOS 펌웨어 모듈을 랙 PDU로 전송합니다. 다음 예에서는 *xxx*를 사용하며, 이는 AOS 모듈의 버전 번호를 나타냅니다.
   scp dell_hw05_aos_xxx.bin
   dell@158.205.6.185:dell_hw05_aos_xxx.bin
3. 응용 프로그램 모듈의 이름을 지정한 유사한 SCP 명령줄을 사용하여 응용 프로그램 펌웨어 모듈을 랙 PDU에 전송합니다.

여러 랙 PDU를 업그레이드하는 방법

FTP 또는 SCP를 사용하여 다수의랙 PDU 업그레이드하기. FTP 클라이언트 또는 SCP를 사용하여 여러 랙 PDU를 업그레이드하려면 이 절차를 자동으로 수행하는 스크립트를 작성합니다.

XMODEM을 사용하여 하나의 랙 PDU 업그레이드

XMODEM을 사용하여 네트워크에 없는 랙 PDU 1대를 업그레이드하려면 먼저 Dell.com에서 펌웨어를 다운로드해야 합니다.

파일을 전송하려면:

1. 로컬 컴퓨터에서 직렬 포트를 선택하고 해당 포트를 사용하는 모든 서비스를 비활성화합니다.
2. 제공된 직렬 구성 케이블을 선택한 포트와 랙 PDU의 직렬 포트에 연결합니다.
3. 단말기 프로그램(예: HyperTerminal)을 실행하고 57600 bps, 8 데이터 비트, 패리티 없음, 1 정지 비트 및 흐름 제어 없음으로 선택한 포트를 구성합니다.
4. 랙 PDU에서 RESET 버튼을 누른 후, 즉시 ENTER 키를 두 번 누르거나 부트 모니터 프롬프트가 표시될 때까지 누릅니다. **BM>**
5. **XMODEM**을 입력하고 ENTER를 누릅니다.
6. 단말기 프로그램 메뉴에서 XMODEM을 선택한 후 이진 AOS 펌웨어 파일을 선택해서 XMODEM으로 파일을 전송합니다. XMODEM 전송이 완료되면 부트 모니터 프롬프트로 되돌아옵니다.
7. 응용 프로그램 모듈을 설치하려면 5단계와 6단계를 반복하십시오. 6단계에서는 응용 프로그램 모듈 파일 이름을 사용합니다.
8. **reset**을 입력하거나 Reset 버튼을 눌러 랙 PDU를 다시 시작합니다.

펌웨어 모듈에 사용되는 형식에 대한 자세한 내용은 펌웨어 파일을 참조하십시오.

업그레이드 및 업데이트 확인

전송 성공 또는 실패 확인

펌웨어 업그레이드의 성공 여부를 확인하려면 명령줄 인터페이스에서 **xferStatus** 명령을 사용하여 마지막 전송 결과를 확인하거나 mfiletransferStatusLastTransferResult OID에 대해 SNMP GET을 사용합니다.

최종 전송 결과 코드

코드	설명
Successful	파일이 성공적으로 전송되었습니다.
Result not available	기록된 파일 전송 결과가 없습니다.
Failure unknown	마지막 파일 전송이 알 수 없는 이유로 실패했습니다.
Server inaccessible	네트워크에서 TFTP 또는 FTP 서버를 찾지 못했습니다.
Server access denied	TFTP 또는 FTP 서버에서 액세스가 거부되었습니다.
File not found	TFTP 또는 FTP 서버에서 요청한 파일을 찾지 못했습니다.
File type unknown	파일을 다운로드했지만 내용을 인식할 수 없습니다.
File corrupt	파일이 다운로드되었지만 최소 하나 이상의 CRC(Cyclical Redundancy Check)가 실패했습니다.

설치된 펌웨어의 버전 번호 확인

웹 인터페이스를 사용하여 상단 메뉴 표시줄에서 Administration 탭, General을 선택하고 왼쪽 탐색 메뉴에서 About를 선택하여 업그레이드된 펌웨어 모듈 버전을 확인하거나 MIB II sysDescr OID에 대해 SNMP GET을 사용합니다. 명령줄 인터페이스에서는 **about** 명령을 사용합니다.

문제 해결

랙 PDU 액세스 문제

문제	해결 방법
랙 PDU를 핑(ping)할 수 없는 경우	랙 PDU의 상태 LED가 녹색으로 켜지면 랙 PDU와 동일한 네트워크 세그먼트에서 다른 노드로 ping을 시도해 보십시오. 그래도 실패하면 랙 PDU에 문제가 있는 것이 아닙니다. 상태 LED가 녹색이 아니거나 ping 테스크가 성공하면 다음을 점검해 보십시오. • 모든 네트워크 연결을 확인하십시오. • 랙 PDU와 NMS의 IP 주소를 확인하십시오. • NMS가 랙 PDU와 다른 실제 네트워크(또는 서브넷)에 있다면 기본 게이트웨이(또는 라우터)의 IP 주소를 확인하십시오. • 랙 PDU의 서브넷 마스크에 지정된 서브넷 비트 수를 확인하십시오.
단말기 프로그램을 통해 통신 포트를 할당할 수 없는 경우	단말기 프로그램을 사용하여 랙 PDU를 구성하기 전에 통신 포트를 사용하고 있는 응용 프로그램, 서비스 또는 프로그램을 종료해야 합니다.
직렬 연결을 통해 명령줄 인터페이스에 액세스할 수 없는 경우	전송 속도를 변경하지 않았는지 확인하십시오. 전송 속도를 2,400, 9,600, 19,200 또는 38,400으로 변경해 보십시오.
명령줄 인터페이스에 원격으로 액세스할 수 없는 경우	• 정확한 액세스 방법(Telnet 또는 SSH (Secure Shell))을 사용하고 있는지 확인하십시오. 관리자가 이러한 액세스 방법을 활성화할 수 있습니다. 기본값으로 사용되는 방법은 Telnet입니다. SSH가 활성화되면 Telnet은 자동으로 비활성화됩니다. • SSH의 경우 랙 PDU에서 호스트 키를 만드는 중일 수 있습니다. 랙 PDU가 이 호스트 키를 만드는 데 최대 1분이 소요될 수 있으며 이 동안은 SSH에 액세스할 수 없습니다.

문제	해결 방법
웹 인터페이스에 액세스할 수 없는 경우	• HTTP 또는 HTTPS 액세스가 활성화되어 있는지 확인하십시오. • 올바른 URL을 지정했는지 확인하십시오. 랙 PDU에서 사용되는 보안 시스템과 일관된 URL이어야 합니다. SSL의 경우 URL 시작 부분에 http가 아닌 https를 사용해야 합니다. • 랙 PDU를 핑(ping)할수 있는지 확인하십시오. • 랙 PDU에서 지원되는 웹 브라우저를 사용하고 있는지 확인하십시오. 지원되는 웹 인터페이스을 참조하십시오. • 랙 PDU가 다시 시작되어 SSL 보안을 설정 중인 경우 랙 PDU가 서버 인증서를 생성하는 중일 수 있습니다. 랙 PDU가 이 인증서를 만드는 데 최대 1분이 소요될 수 있으며 이 시간에는 SSL 서버에 액세스할 수 없습니다.

부록 A: 지원되는 명령어 목록

네트워크 관리 카드 명령어 설명

```
?
about
alarmcount
   [-p [all | warning | critical]]
boot
   [-b <dhcpBootp | dhcp | bootp | manual>]
   [-a <remainDhcpBootp | gotoDhcpOrBootp>]
   [-o <정지 | prevSettings>]
   [-f <재시도 후 장애 횟수>]
   [-c <dhcp 쿠키> [활성화 | 해제]]
   [-s <재시도 후 정지 횟수>]
   [-v <벤더 클래스>]
   [-i <클라이언트 id>]
   [-u <사용자 클래스>]
cd
console
   [-S<disable | telnet | ssh>]
   [-pt <Telnet 포트 번호>]
   [-ps <SSH 포트 번호>]
   [-b <2400 | 9600 | 19200 | 38400>]
date
   [-d <"datestring">]
   [-t <00:00:00>]
   [-f [mm/dd/yy | dd.mm.yyyy | mmm- dd- yy | dd- mmm-yy | yyyy- mm- dd]]
delete
dir
dns
   [-OM <enable | disable>]
   [-p <기본 DNS 서버>]
   [-s <보조 DNS 서버>]
   [-d <도메인 이름>]
   [-n <도메인 이름 IPv6>]
   [-h <호스트 이름>]
eventlog
exit
format
```

ftp
[-p <포트 번호>]
[-S <enable | disable>]
help
netstat
ntp
[-OM <활성화 | 해제>]
[-p <기본 NTP 서버>]
[-s <보조 NTP 서버>]
ping
[<IP 주소 또는 DNS 이름>]
portspeed
[-s [auto | 10H | 10F | 100H | 100F]]
prompt
[-s [long | short]]
quit
radius
[-a <액세스> [local | radiusLocal | radius]]
[-p# <서버 IP>]
[-s# <서버 보안>]
[-t# <서버 시간 제한>]
reboot
resetToDef
[-p <all | keepip>]
snmp, snmpv3
[-S <활성화 | 해제>]
system
[-n <시스템 이름>]
[-c <시스템 담당자>]
[-l <시스템 위치>]
tcpip
[-i <IP 주소>]
[-s <서브넷 마스크>]
[-g <게이트웨이>]
[-d <도메인 이름>]
[-h <호스트 이름>]
tcpip6
[-S <활성화 | 해제>]
[-man <활성화 | 해제>]
[-auto <활성화 | 해제>]
[-i <IPv6 주소>]
[-g <IPv6 게이트웨이>]
[-d6 <router | stateful | stateless | never>]

user
[-an <관리자 이름>]
[-dn <장치 사용자 이름>]
[-rn <읽기 전용 사용자 이름>]
[-ap <관리자 암호>]
[-dp <장치 사용자 암호>]
[-rp <읽기 전용 사용자 암호>]
[-t <비활성 시간 제한(분 단위)>]
web
[-S <disable | http | https>]
[-ph <http 포트 번호>]
[-ps <https 포트 번호>]
xferINI
xferStatus

장치 명령어 설명

devLowLoad
[<전력>]
devNearOver
[<전력>]
devOverLoad
[<전력>]
devReading
[<"전력" | "에너지">]
devStartDly
humLow
[<습도>]
humMin
[<습도>]
humReading
inNormal
inReading
olAssignUsr
[<“all” | 출력 이름 | 출력 번호 > <사용자>]
olCancelCmd
[<"all" | 출력 이름 | 출력 번호>]
olDlyOff
[<"all" | 출력 이름 | 출력 번호>]
olDlyOn
[<"all" | 출력 이름 | 출력 번호>]
olDlyReboot
[<"all" | 출력 이름 | 출력 번호>]
olGroups

olLowLoad
[<“all” | 출력 이름 | 출력 번호 > <전원>]
olName
[<“all” | 출력 번호 > <새 이름>]
olNearOver
[<“all” | 출력 이름 | 출력 번호 > <전원>]
olOff
[<"all" | 출력 이름 | 출력 번호>]
olOffDelay
[<“all” | 출력 이름 | 출력 번호 > <시간>]
olOn
[<"all" | 출력 이름 | 출력 번호>]
olOnDelay
[<“all” | 출력 이름 | 출력 번호 > <시간>]
olOverLoad
[<“all” | 출력 이름 | 출력 번호 > <전원>]
olRbootTime
[<“all” | 출력 이름 | 출력 번호 > <시간>]
olReading
[<“all” | 출력 이름 | 출력 번호 > <전류 | 전원 | 에너지>]
olReboot
[<"all" | 출력 이름 | 출력 번호>]
olStatus
[<"all" | 출력 이름 | 출력 번호>]
olUnasgnUsr
[<“all” | 출력 이름 | 출력 번호 > <사용자>]
phLowLoad
[<"all" | 위상 번호> <전류>]
phNearOver
[<"all" | 위상 번호> <전류>]
phOverLoad
[<"all" | 위상 번호> <전류>]
phReading
[<"all" | 위상 번호> <"전류" | "전압" | "전원">]
phRestrictn
[<“all” | 위상 번호> <none | near | over>]
prodInfo
tempHigh
[<"F"| "C"> <온도>]
tempMax
[<"F"| "C"> <온도>]
tempReading
[<“F” | “C”>]

userAdd
[<새 사용자>]
userDelete
[<사용자>]
userList
userPasswd
[<사용자> <새 암호> <새 암호>]
whoami

부록 B: 보안 핸드북

부록의 내용 및 용도

이 부록에는 네트워크 상에서 원격으로 랙 PDU를 작동시키는 데 사용되는 Dell® 랙 PDU용 펌웨어 버전 5.*x.x*의 보안 기능이 수록되어 있습니다.

다음과 같은 프로토콜과 기능, 사용자 상황에 적합한 프로토콜 및 기능 선택 방법, 전체 보안 시스템 내에서 프로토콜 및 기능을 설정하고 사용하는 방법에 대해서 설명합니다.

- Telnet 및 SSH (Secure SHell)
- SSL (Secure Sockets Layer)
- RADIUS
- SNMPv1 및 SNMPv3

또한, Rack PDU Security Wizard를 사용하여 SSL 및 SSH를 통해 사용 가능한 높은 보안 수준에 필요한 구성 요소를 생성하는 방법도 설명합니다.

보안 기능

암호 및 암호 구문 보안 기능

랙 PDU에서는 암호 또는 암호 문구가 일반 텍스트로 저장되지 않습니다.

- 암호는 단방향 해시 알고리즘을 사용하여 해싱합니다.
- 인증 및 암호화에 사용되는 암호 문구는 랙 PDU에 저장하기 전에 암호화합니다.

액세스 방법 요약

명령줄 인터페이스에 직렬 액세스.

보안 액세스	설명
사용자 이름과 비밀번호를 통한 액세스	항상 사용

명령줄 인터페이스에 원격 액세스.

보안 액세스	설명
사용 가능한 방법: • 사용자 이름과 암호 • 선택 가능한 서버 포트 • 사용 또는 사용 불가능으로 설정할 수 있는 액세스 프로토콜 • SSH (Secure Shell)	강화된 보안을 원하면 SSH를 사용하십시오. • Telnet을 이용할 경우 사용자 이름과 암호가 일반 텍스트로 전송됩니다. • SSH를 선택하면 Telnet을 사용할 수 없으며 명령줄 인터페이스에 암호화된 방법으로 액세스하기 때문에 전송 중 데이터를 가로채거나 날조 또는 변경하려는 시도에 대해 보안이 강화되었습니다.

SNMPv1 및 SNMPv3.

보안 액세스	설명
사용 가능한 방법(SNMPv1): • 커뮤니티 이름 • 호스트 이름 • NMS IP 필터 • 사용 또는 사용 불가능으로 설정할 수 있는 에이전트 • 읽기/쓰기/해제 기능을 포함한 4개의 액세스 커뮤니티	SNMPv1과 SNMPv3 모두 호스트 이름이 해당 위치에서만 네트워크 관리 시스템(NMS)에 액세스하도록 제한하고, NMS IP 필터는 다음 예에 나온 IP 주소 형식 중 하나로 지정된 NMS에만 액세스를 허용합니다. • 159.215.12.1: IP 주소 159.215.12.1의 NMS로 제한 • 159.215.12.255: 159.215.12 세그먼트의 모든 NMS • 159.215.255.255: 159.215 세그먼트의 모든 NMS • 159.255.255.255: 159 세그먼트의 모든 NMS • 0.0.0.0 또는 255.255.255.255: 모든 NMS SNMPv3에는 다음을 포함하는 추가적인 보안 기능이 있습니다. • 랙 PDU에 액세스를 시도하는 NMS가 클레임 대상 NMS임을 확인하는 인증 암호 문구. • 암호화 및 암호 해독에 필요한 프라이버시 암호 문구를 사용하여 전송 중에 데이터 암호화
사용 가능한 방법(SNMPv3): • 네 가지 사용자 프로필 • 인증 암호 문구를 통한 인증 • 프라이버시 암호 문구를 통한 암호화 • SHA 또는 MD5 인증 • AES 또는 DES 암호화 알고리즘 • NMS IP 필터	

파일 전송 프로토콜.

보안 액세스	설명
사용 가능한 방법: • 사용자 이름과 암호 • 선택 가능한 서버 포트 • 사용 또는 사용 불가능으로 설정할 수 있는 FTP 서버 및 액세스 프로토콜 • SCP (Secure CoPy)	FTP를 사용할 경우 사용자 이름과 암호는 일반 텍스트로 전송되며 파일은 암호화되지 않고 전송됩니다. SCP를 사용하면 사용자 이름과 암호 및 펌웨어 업데이트, 구성 파일, 로그 파일, SSL (Secure Sockets Layer) 인증서, SSH (Secure Shell) 호스트 키와 같은 파일을 암호화하여 전송합니다. 파일 전송 프로토콜로 SCP를 선택하면 SSH를 사용할 수 있으며 FTP는 사용할 수 없습니다.

웹 서버.

보안 액세스	설명
사용 가능한 방법: • 사용자 이름과 암호 • 선택 가능한 서버 포트 • 사용 또는 사용 불가능으로 설정할 수 있는 웹 인터페이스 액세스 • SSL (Secure Sockets Layer)	기본 HTTP 인증 모드에서는 사용자 이름과 암호가 암호화 없이 base-64 인코딩된 상태로 전송됩니다. SSL은 관리 카드 또는 네트워크 활성 장치 및 대부분의 웹 서버와 함께 사용되도록 지원하는 웹 브라우저에서 사용할 수 있습니다. SSL상의 HTTP(HTTPS) 웹 프로토콜에서는 웹 서버에 요청하는 페이지 및 웹 서버가 사용자에게 되돌려주는 페이지를 암호화하고 해독합니다.

RADIUS.

보안 액세스	설명
사용 가능한 방법: • 액세스 권한의 중앙 집중식 인증 • RADIUS 서버와 랙 PDU 또는 장치 간에 공유된 서버 보안	RADIUS (Remote Authentication Dial-In User Service)는 각 랙 PDU에 대한 원격 액세스를 중앙에서 관리하는 데 사용되는 인증, 권한 및 계정 서비스입니다. (랙 PDU는 인증 및 권한 기능을 지원합니다.)

액세스 우선 순위

액세스 우선 순위는 다음과 같습니다(높은 순에서 낮은 순으로).

- 랙 PDU에 대한 직접 직렬로 연결된 컴퓨터에서 명령줄 인터페이스로 로컬 액세스
- 원격 컴퓨터에서 명령줄 인터페이스로 Telnet 또는 SSH (Secure Shell) 액세스
- 웹 액세스

기본 사용자 이름과 암호 즉시 변경하기

랙 PDU의 설치 및 초기 구성을 완료한 후, 기본적 보안을 유지하기 위해 기본 사용자 이름과 암호를 고유한 사용자 이름과 암호로 즉시 변경하십시오.

포트 할당

Telnet, FTP server, SSH/SCP 또는 웹 서버가 비표준 포트를 사용하는 경우, 사용자는 랙 PDU 액세스에 사용되는 명령줄 또는 웹 주소에서 포트를 지정해야 합니다. 비표준 포트 번호가 보안 수준을 강화합니다. 포트는 처음에 프로토콜에 대해 표준의 "잘 알려진 포트"로 설정됩니다. 보안을 강화하려면 FTP 서버에 대해서는 5001~32768 범위, 나머지 프로토콜 및 서버에 대해서는 5000~32768 범위의 사용하지 않는 포트 번호들로 포트를 재설정합니다. (FTP 서버는 지정된 포트와 지정된 포트보다 한 자리가 낮은 포트 둘 다 사용합니다.)

SNMPv1에서 사용자 이름, 암호 및 커뮤니티 이름

SNMPv1의 모든 사용자 이름, 암호 및 커뮤니티 이름은 네트워크에서 일반 텍스트로 전송됩니다. 네트워크 트래픽을 모니터할 수 있는 사용자는 랙 PDU의 명령줄 인터페이스 또는 웹 인터페이스 계정에 로그인하는 데 필요한 사용자 이름과 암호를 결정할 수 있습니다. 명령줄 인터페이스 및 웹 인터페이스에 사용할 수 있는 암호화 기반 옵션의 네트워크 보안 수준을 강화해야 하는 경우, SNMPv1 액세스를 해제하거나 Read로 액세스를 설정해야 합니다. (Read 액세스는 상태 정보 수신과 SNMPv1 트랩 사용을 허용합니다.)

SNMPv1 액세스를 해제하려면 Administration 탭의 상단 메뉴 표시줄에서 Network를 선택하고 왼쪽 탐색 메뉴의 SNMPv1 아래에서 access를 선택합니다. Enable SNMPv1 access 확인란 선택을 취소하고 Apply를 클릭합니다.

SNMPv1 액세스를 Read로 설정하려면 Administration 탭의 상단 메뉴 표시줄에서 Network를 선택하고 왼쪽 탐색 메뉴의 SNMPv1 아래에서 access control을 선택합니다. 그런 다음, 구성된 각 네트워크 관리 시스템(NMS)의 커뮤니티 이름을 클릭하고 액세스 유형을 Read로 설정합니다.

인증

암호화를 사용하지 않고 사용자 이름, 암호 및 IP 주소를 사용한 기본적 인증으로 액세스를 제어하는 랙 PDU의 보안 기능을 선택할 수 있습니다. 민감한 데이터가 전송되지 않는 대부분의 환경에는 이 정도의 기본적 보안 기능으로 충분합니다.

SNMP GETS, SETS 및 트랩

SNMP를 사용하여 랙 PDU를 모니터하고 구성할 때 인증을 강화하려면 SNMPv3을 선택합니다. SNMPv3 사용자 프로파일과 함께 사용되는 인증 암호는 랙 PDU와 통신하려고 하는 네트워크 관리 시스템(NMS)이 실제로 NMS이고, 전송 중 메시지가 변경되지 않았으며, 메시지가 지연되지 않았고, 이후 부적합한 시기에 다시 전송되지 않는다는 것을 보장합니다. SNMPv3은 기본적으로 해제됩니다.

Dell에서 구현한 SNMPv3은 SHA-1 또는 MD5 프로토콜을 사용한 인증을 지원합니다.

웹 인터페이스 및 명령줄 인터페이스

명령줄 인터페이스 및 웹 인터페이스와 같은 클라이언트 인터페이스와 랙 PDU 간의 데이터 통신을 가로챌 수 없도록 하려면 다음과 같은 암호화 기반 방법 중 하나 이상을 사용하여 보안 수준을 강화할 수 있습니다.

- 웹 인터페이스의 경우 SSL (Secure Sockets Layer) 프로토콜을 사용합니다.
- 명령줄 인터페이스 액세스의 사용자 이름과 암호를 암호화하려면 SSH (Secure Shell) 프로토콜을 사용합니다.
- 보안 파일 전송을 위해 사용자 이름, 비밀번호 및 데이터를 암호화하려면 SCP 프로토콜을 사용합니다.

암호화 기반 보안에 대한 자세한 내용은 암호화를 참조하십시오.

암호화

SNMP GETS, SETS 및 트랩

SNMP를 사용하여 랙 PDU를 모니터하고 구성할 때 통신을 암호화하려면 SNMPv3을 선택합니다. SNMPv3 사용자 프로필에 사용되는 프라이버시 암호 문구를 통해 NMS가 랙 PDU와 보내고 받는 데이터의 프라이버시를 보장합니다(AES 또는 DES 암호화 알고리즘을 사용한 암호화를 통해).

명령줄 인터페이스에 대한 SSH (Secure Shell) 및 SCP (Secure CoPy)

SSH (Secure Shell) 프로토콜. SSH는 컴퓨터 콘솔 또는 *셸*에 원격으로 액세스하는 보안 방법을 제공합니다. 이 프로토콜에서는 서버(이 경우 랙 PDU)를 인증하고 SSH 클라이언트와 서버 간의 모든 전송 내용을 암호화합니다.

- SSH는 Telnet의 대안이 되는 수준 높은 보안입니다. Telnet에는 암호화 기능이 없습니다.
- SSH에서는 네트워크 트래픽을 가로챌 수 있는 타인이 인증 자격 증명으로 사용되는 사용자 이름과 암호를 사용할 수 없도록 보호합니다.
- SSH 서버(랙 PDU)를 SSH 클라이언트에 인증하기 위해 SSH는 SSH 서버에 고유한 호스트 키를 사용합니다. 호스트 키는 위조가 불가능한 ID이므로 이 키를 사용하면 네트워크상의 잘못된 서버가 유효한 서버로 위장하여 사용자 이름과 암호를 알아낼 수 없습니다.

지원되는 SSH 클라이언트 응용 프로그램에 대한 자세한 내용은 Telnet 및 SSH (Secure SHell)를 참조하십시오. 호스트 키를 만드는 방법은 SSH 호스트 키 만들기를 참조하십시오.

- 랙 PDU는 전송 중 데이터 가로채기, 날조 또는 변경 시도를 차단하는 기능을 제공하는 SSH 버전 2를 지원합니다.
- SSH를 사용하면 Telnet은 자동으로 해제됩니다.
- 인터페이스, 사용자 계정 및 사용자 액세스 권한은 SSH 또는 Telnet을 사용하여 명령줄 인터페이스에 액세스하는 경우에도 동일합니다.

Secure CoPy. SCP는 FTP 대신 사용할 수 있는 보안 파일 전송 응용 프로그램입니다. SCP에서는 사용자 이름, 암호 및 파일을 암호화하기 위한 기본 전송 프로토콜로 SSH 프로토콜을 사용합니다.

- SSH를 사용 및 구성하면 SCP도 자동으로 사용 및 구성됩니다. 그러므로 SCP를 추가로 구성할 필요가 없습니다.
- FTP는 명시적으로 해제해야 합니다. FTP는 SSH를 사용해도 해제되지 않습니다. FTP를 해제하려면 Administration 탭의 상단 메뉴 표시줄에서 Network를 선택하고 왼쪽 탐색 메뉴에서 FTP Server를 선택합니다. Enable 확인란 선택을 취소하고 Apply를 클릭합니다.

웹 인터페이스에 대한 SSL (Secure Sockets Layer)

웹 통신 보안을 원할 경우 랙 PDU의 웹 인터페이스에 액세스하기 위한 프로토콜 모드로 HTTPS를 선택하여 SSL (Secure Sockets Layer)을 설정합니다. HTTPS는 사용자가 요청하는 페이지와 웹 서버에서 사용자에게 반환하는 페이지를 암호화 및 해독하는 웹 프로토콜입니다.

랙 PDU는 SSL 버전 3.0 및 연관 TLS (Transport Layer Security) 버전 1.0을 지원합니다. 대부분의 브라우저에서 사용할 SSL 버전을 선택할 수 있습니다.

SSL이 활성화되면 브라우저에 작은 자물쇠 아이콘이 표시됩니다. 

SSL은 디지털 인증서를 사용하여 브라우저에서 서버(이 경우 랙 PDU)를 인증할 수 있도록 합니다. 브라우저는 다음 항목을 확인합니다.

- 서버 인증서 형식의 정확성
- 서버 인증서의 만료 날짜 및 시간 초과 여부
- 사용자가 로그인할 때 지정한 DNS 이름 또는 IP 주소가 서버 인증서의 공통 이름과 일치하는지 여부
- 신뢰할 수 있는 인증 기관에서 서버 인증서에 서명했는지 여부

각 주요 브라우저 제조업체는 서버 인증서의 서명을 CA 루트 인증서의 서명과 비교할 수 있도록 브라우저의 인증서 저장소(캐시)에 상용 인증 기관의 CA 루트 인증서를 배포합니다.

Rack PDU Security Wizard를 사용하여 외부 인증 기관에 보낼 인증서 서명 요청을 만들 수 있습니다. 또는 기존 인증 기관을 사용하지 않으려면 Dell 루트 인증서를 만들어 브라우저의 인증서 저장소(캐시)에 업로드합니다. 또한 이 마법사를 사용하여 서버 인증서를 만들어 랙 PDU에 업로드할 수 있습니다.

이 인증서를 사용하는 방법은 디지털 인증서 만들기 및 설치를 참조하십시오. 인증서 및 인증서 요청을 만드는 방법은 루트 인증서 및 서버 인증서 만들기 및 서버 인증서 및 서명 요청 만들기를 참조하십시오.

또한 SSL은 다양한 알고리즘과 암호화 방법을 사용하여 서버 인증과 데이터 암호화를 수행하고 데이터 무결성을 보장합니다. 즉, 다른 서버에서 데이터를 가로채거나 전송하지 못하도록 합니다.

최근에 액세스한 웹 페이지는 사용자 이름과 암호를 다시 입력하지 않고 액세스한 웹 페이지에 돌아올 수 있도록 웹 브라우저의 캐시에 저장됩니다. 그러므로 컴퓨터를 켜 두고 자리를 비울 때는 항상 브라우저를 닫으십시오.

디지털 인증서 만들기 및 설치

목적

랙 PDU의 웹 인터페이스에서는 암호 암호화보다 더 높은 수준의 보안이 요구되는 네트워크 통신을 위해 디지털 인증서를 SSL 프로토콜과 함께 사용할 수 있도록 지원합니다. 디지털 인증서를 통해랙 PDU(서버)를 웹 브라우저(SSL 클라이언트)에 인증할 수 있습니다.

복잡한 암호화 및 더 높은 수준의 보안을 제공하는 1024비트 키를 생성하거나 2048- 비트 키를 생성할 수 있습니다.

다음에는 사용자 시스템에 가장 적합한 방법을 결정하는 데 활용할 수 있도록 디지털 인증서 만들기, 구현 및 사용 방법을 간단히 설명합니다.

- 방법 1: 랙 PDU에 의해 자동으로 생성된 기본 인증서 사용.
- 방법 2: Rack PDU Security Wizard를 사용하여 CA 인증서와 서버 인증서 생성.
- 방법 3: Rack PDU Security Wiard를 사용하여 외부 인증 기관의 루트 인증서를 통해 서명을 요구하는 인증서 서명 요청을 만들고 서버 인증서를 만듭니다.

자체 인증 기관을 운영하는 회사나 기관의 경우 방법 3을 사용할 수도 있습니다. Rack PDU Security Wizard는 동일한 방법으로 사용할 수 있지만 상용 인증 기관 대신 자체 인증 기관을 사용하십시오.

시스템에 적절한 방법 선택

SSL 프로토콜을 사용하는 경우 다음과 같은 방법으로 디지털 인증서를 사용할 수 있습니다.

방법 1: 랙 PDU에 의해 자동으로 생성된 기본 인증서 사용. SSL을 활성화하는 경우 랙 PDU를 재부팅해야 합니다. 재부팅 중 서버 인증서가 존재하지 않는 경우, 랙 PDU가 자체- 서명되었지만 사용자가 구성할 수 없는 기본 서버 인증서를 생성합니다.

방법 1의 장점과 단점은 다음과 같습니다.

- **장점**
  - 랙 PDU의 사용자 이름, 암호 및 모든 데이터는 전송 전에 암호화됩니다.
  - 나머지 두 디지털 인증서 옵션 중 하나를 설정할 때 이 기본 서버 인증서를 사용하여 암호화 기반 보안을 적용하거나, SSL 암호화의 장점을 위해 이 방법을 계속 사용할 수 있습니다.
- **단점:**
  - 랙 PDU가 이 인증서를 만드는 데 최대 1분이 소요될 수 있으며 이 동안은 웹 인터페이스를 사용할 수 없습니다. 이 지연은 SSL을 설정한 후 처음 로그인할 때만 발생합니다.
  - 이 방법은 방법 2 및 3과 같이 CA 인증서가 제공하는 인증(인증 기관이 서명한 인증서)을 포함하지 않습니다. 즉, 브라우저에 CA 인증서가 캐싱되지 않습니다. 그러므로 랙 PDU에 로그인하면 신뢰할 수 있는 기관이 서명한 인증서가 없음을 알려주고 계속할지 여부를 묻는 브라우저 보안 경고 메시지가 표시됩니다. 이 메시지가 나타나지 않게 하려면 랙 PDU에 액세스해야 하는 각 사용자 브라우저의 인증서 보관소(캐시)에 기본 서버 인증서를 설치해야 하며, 각 사용자는 랙 PDU에 로그온할 때 항상 서버의 정규화된 도메임 이름을 사용해야 합니다.
  - 기본 서버 인증서는 유효한 *공통 이름*(랙 PDU의 DNS 이름 또는 IP 주소) 대신 랙 PDU의 일련 번호를 갖습니다. 그러므로 랙 PDU에서 사용자 이름, 암호 및 계정 유형(Administrator, Device Manager 또는 Read Only User)을 통해 웹 인터페이스에 대한 액세스를 제어할 수 있지만, 브라우저는 데이터를 송신 또는 수신하는 랙 PDU를 인증할 수 없습니다.

- SSL 세션을 설정할 때 암호화를 위해 사용되는 *공개 키*(RSA 키)의 길이는 기본적으로 2048비트밖에 안 됩니다.

방법 2: Rack PDU Security Wizard를 사용하여 CA 인증서와 서버 인증서 생성.

Rack PDU Security Wizard를 사용하여 다음 두 가지 디지털 인증서를 만듭니다.

- *CA 루트 인증서*(인증 기관 루트 인증서): Rack PDU Security Wizard가 이 인증서를 사용하여 모든 서버 인증서에 서명하면 랙 PDU에 액세스가 필요한 각 사용자의 브라우저의 인증서 저장소(캐시)에 설치합니다.
- 랙 PDU에 업로드하는 *서버 인증서*. Rack PDU Security Wizard에서 서버 인증서를 만들 때 CA 루트 인증서를 사용하여 서버 인증서에 서명합니다.

웹 브라우저는 데이터를 송신 또는 요청하는 랙 PDU를 인증합니다.

- 브라우저는 인증서가 생성될 때 서버 인증서의 *고유 이름*에 지정된 *공통 이름*(랙 PDU의 IP 주소 또는 DNS 이름)을 사용하여 랙 PDU를 식별합니다.
- 브라우저는 서버 인증서의 서명을 브라우저 캐시에 저장된 루트 인증서의 서명과 비교하여 '신뢰할 수 있는' 인증 기관이 서명한 서버 인증서인지 확인합니다. 또한 만료 날짜를 확인하여 서버 인증서가 만료되지 않았는지 확인합니다.

방법 2의 장점과 단점은 다음과 같습니다.

- **장점**
  - 사용자 이름, 암호 및 모든 데이터는 전송되기 전에 랙 PDU에서 암호화됩니다.
  - SSL 세션을 설정할 때 암호화에 사용되는 *공개 키*(RSA 키)의 길이를 선택합니다(기본 설정인 1024비트 또는 복잡한 암호화 및 강화된 보안 수준을 제공하는 2048비트 사용).
  - 랙 PDU으로 업로드된 서버 인증서는 SSL을 사용하여 올바른 랙 PDU에서 수신된 데이터와 랙으로 전송된 데이터를 인증합니다. 이 방식은 사용자 이름, 암호 및 전송된 데이터를 암호화보다 더 높은 수준의 보안을 제공합니다.
  - 브라우저에 루트 인증서를 설치하면 브라우저는 랙 PDU의 서버 인증서를 인증할 수 있기 때문에 무단 액세스에 대한 보안이 강화됩니다.

- **단점**
  인증서에 상용 인증 기관의 디지털 서명이 없기 때문에 각 사용자의 브라우저의 인증서 저장소(캐시)에 개별적으로 루트 인증서를 로드해야 합니다. 방법 3에서 설명한 대로 브라우저의 인증서 저장소에는 브라우저 제조업체에서 제공한 상용 인증 기관의 루트 인증서가 있을 것입니다.

방법 3: Rack PDU Security Wiard를 사용하여 외부 인증 기관의 루트 인증서를 통해 서명을 요구하는 인증서 서명 요청을 만들고 서버 인증서를 만듭니다. Rack PDU Security Wizard를 사용하여 인증 기관에 보낼 요청(.csr 파일)을 만듭니다. 인증 기관은 요청에 제출된 정보를 기반으로 서명된 인증서(.crt 파일)를 반환합니다. 이 때 Rack PDU Security Wizard를 사용하여 인증 기관이 반환한 루트 인증서의 서명이 포함된 서버 인증서(.p15 파일)를 만들 수 있습니다. 서버 인증서를 랙 PDU에 업로드합니다.

자체 인증 기관을 운영하는 회사나 기관의 경우 방법 3을 사용할 수도 있습니다. Rack PDU Security Wizard는 동일한 방법으로 사용할 수 있지만 상용 인증 기관 대신 자체 인증 기관을 사용하십시오.

방법 3의 장점과 단점은 다음과 같습니다.

- **장점**
  - 사용자 이름, 암호 및 모든 데이터는 전송되기 전에 랙 PDU에서 암호화됩니다.
  - 브라우저의 인증서 캐시에 서명된 루트 인증서가 이미 있는 인증 기관을 통해 인증할 수 있다는 장점이 있습니다. 상용 인증 기관의 CA 인증서는 브라우저 소프트웨어의 일부로 배포되며, 회사나 비영리기관 자체의 인증 기관에서 각 사용자의 브라우저에 대한 인증서 저장소에 로드한 CA 인증서가 이미 있을 것입니다. 따라서 랙 PDU에 액세스해야 하는 각 사용자의 브라우저에 루트 인증서를 업로드할 필요가 없습니다.
  - SSL 세션 설정에 사용되는 *공개 키*(RSA 키)의 길이를 선택합니다(기본 설정인 1024비트 또는 복잡한 암호화 및 강화된 보안 수준을 제공하는 2048비트 사용).
  - 랙 PDU으로 업로드된 서버 인증서는 SSL을 사용하여 올바른 랙 PDU에서 수신된 데이터와 랙으로 전송된 데이터를 인증합니다. 이 방식은 사용자 이름, 암호 및 전송된 데이터를 암호화보다 더 높은 수준의 보안을 제공합니다.

- 브라우저는 랙 PDUd에 업로드된 서버 인증서의 디지털 서명과 브라우저의 인증서 캐시에 이미 존재하는 CA 루트 인증서의 서명과 대조하므로 무단 액세스에 대한 보안이 강화됩니다.

- **단점:**
  - 설치 시 인증 기관에서 서명한 루트 인증서를 요청하는 추가 단계가 필요합니다.
  - 외부 인증 기관은 서명된 인증서에 대해 요금을 부과할 수 있습니다.

방화벽

일부 인증 방법은 다른 방법보다 강화된 보안을 제공하지만 보안 위반을 완벽하게 방지한다는 것은 거의 불가능합니다. 전체 보안 방법을 위해 효과적으로 구성된- 방화벽이 반드시 필요합니다.

Rack PDU Security Wizard 사용

Rack PDU Security Wizard는 보안 소켓 레이어(SSL)와 관련 프로토콜 및 암호화 루틴을 사용하는 경우 네트워크상의 랙 PDU에 대한 보안을 강화하기 위해 필요한 구성 요소를 만듭니다.

인증서 및 호스트 키를 사용한 인증

*인증*은 사용자 또는 랙 PDU와 같은 네트워크 장치의 ID를 확인하는 과정입니다. 일반적으로 암호를 통해 컴퓨터 사용자를 확인합니다. 그러나 랙 PDU는 더 엄격한 인터넷 보안이 요구되는 트랜잭션 또는 통신을 위해 더 안전한 인증 방법을 지원합니다.

- 보안 웹 액세스를 위해 사용되는 SSL에서는 디지털 인증서를 사용하여 인증합니다. 디지털 *CA 루트* 인증서는 공개 키 인프라의 일부로 인증 기관에서 발급하며, 이 인증서의 디지털 서명은 랙 PDU의 서버 인증서에 있는 디지털 서명과 일치해야 합니다.
- 랙 PDU의 명령줄 인터페이스에 원격 단말기로 액세스하기 위해 사용되는 SSH (Secure Shell)는 공용 *호스트 키*를 인증에 사용합니다.

인증서 사용 방법. 랙 PDU에서 지원하는 모든 브라우저를 포함한 대부분의 웹 브라우저에는 모든 상용 인증 기관이 발급한 CA 루트 인증서가 포함되어 있습니다.

브라우저는 서버로 연결할 때마다 서버(이 경우 랙 PDU)를 인증합니다. 브라우저는 알려진 인증 기관에서 서명한 서버 인증서인지 확인합니다.

인증을 위해 다음 조건이 전제되어야 합니다.

- SSL이 설정된 각 서버(랙 PDU) 자체에 서버 인증서가 있어야 합니다.
- 랙 PDU의 웹 인터페이스에 액세스할 때 사용하는 모든 브라우저에 서버 인증서를 서명한 CA 루트 인증서가 있어야 합니다.

인증에 실패하면 서버를 인증할 수 없지만 계속할지 묻는 브라우저 메시지가 표시됩니다.

네트워크에 디지털 인증서의 인증이 필요하지 않은 경우 랙 PDU가 자동으로 생성하는 기본 인증서를 사용할 수 있습니다. 기본 인증서의 디지털 서명은 브라우저에서 인식되지 않지만 기본 인증서를 사용하면 사용자 이름, 암호 및 데이터를 전송할 때 SSL을 사용하여 암호화할 수 있습니다. 기본 인증서를 사용하면랙 PDU의 웹 인터페이스에 로그인하기 전에 인증되지 않은 액세스에 동의하는지 묻는 대화 상자가 표시됩니다.

SSH 호스트 키 사용. SSH *호스트 키*는 SSH 클라이언트가 해당 서버에 접속할 때마다 서버(랙 PDU)의 ID를 인증합니다. SSH가 설정된 각 서버 자체에 SSH 호스트 키가 있어야 합니다.

SSL과 SSH 보안에 사용할 파일 만들기

Rack PDU Security Wizard를 사용하여 이러한 SSL 및 SSH 보안 시스템 구성 요소를 만듭니다.

- 랙 PDU 서버 인증서. 인증서를 사용한 인증에 따른 장점을 원하는 경우에 해당하며, 다음과 같은 유형의 서버 인증서를 만들 수 있습니다.
  - Rack PDU Security Wizard로 만들고 사용자 정의 CA 루트 인증서가 서명한 서버 인증서. 회사나 기관 자체의 인증 기관이 없지만 외부 인증 기관을 사용하여 서버 인증서를 서명하지 않으려면 이 방법을 사용합니다.
  - 외부 인증 기관에서 서명한 서버 인증서. 외부 인증 기관이란 회사 또는 기관 자체에서 관리하는 인증 기관 또는 CA 루트 인증서를 브라우저 소프트웨어에 포함하여 배포하는 상용 인증 기관을 말합니다.
- 디지털 서명을 제외한 서버 인증서에 필요한 모든 정보가 들어 있는 인증서 서명 요청. 외부 인증 기관을 사용하는 경우 이 요청이 필요합니다.
- CA 루트 인증서
- 명령줄 인터페이스에 로그인할 때 SSH 클라이언트 프로그램이 랙 PDU를 인증하기 위해 사용하는 SSH 호스트 키

Rack PDU Security Wizard로 생성하는 SSH용 호스트 키와 SSL 인증서용 공개 키가 1024비트 RSA 키(기본 설정)인지 또는 복잡한 암호화 및 강화된 보안 수준을 제공하는 2048비트 RSA 키인지 여부를 정의합니다.

Rack PDU Security Wizard로 SSL 서버 인증서 및 SSH 호스트 키를 만들어 사용하지 않는 경우 랙 PDU에서 2048비트 RSA 키를 생성합니다.

랙 PDU 보안 마법사가 생성하는 서버 인증서, 호스트 키 및 CA 루트 인증서를 사용할 수 있는 제품은 Dell 랙 PDU 제품이 유일합니다. OpenSSL® 및 Microsoft® IIS와 같은 제품에는 이러한 파일을 사용할 수 없습니다.

루트 인증서 및 서버 인증서 만들기

요약

회사나 기관 자체의 인증 기관이 없지만 상용 인증 기관을 사용하여 서버 인증서를 서명하지 않으려면 이 방법을 사용합니다.

Rack PDU Security Wizard로 생성하는 인증서의 일부인 공개 RSA 키의 크기를 정의합니다. 1024비트 키를 생성하거나 복잡한 암호화 및 강화된 보안 수준을 제공하는 2048비트 키를 생성할 수 있습니다. (마법사를 사용하지 않는 경우 랙 PDU에서 생성하는 기본 키는 2048비트입니다.)

- 랙 PDU에 사용할 모든 서버 인증서에 서명하는 CA 루트 인증서를 만듭니다. 이 작업으로 두 파일이 생성됩니다.
  - 확장자가 .p15인 파일은 인증 기관의 개인 키 및 공개 루트 인증서가 들어 있는 암호화된 파일입니다. 이 파일을 통해 서버 인증서에 서명합니다.
  - 확장자가 .crt인 파일에는 인증 기관의 공개 루트 인증서만 들어 있습니다. 브라우저가 랙 PDU의 서버 인증서를 확인할 수 있도록 랙 PDU에 액세스할 때 사용하는 각 웹 브라우저로 이 파일을 로드합니다.
- 확장자가 .p15인 파일에 저장되는 서버 인증서를 만듭니다. 이 작업을 수행하는 동안 서버 인증서에 서명하는 CA 루트 인증서를 지정하는 대화 상자가 표시됩니다.
- 서버 인증서를 랙 PDU로 로드합니다.
- 서버 인증서가 필요한 각 랙 PDU에 대해 서버 인증서 만들기와 로드 작업을 반복합니다.

절차

CA 루트 인증서 만들기.

1. Rack PDU Security Wizard가 컴퓨터에 설치되어 있지 않으면 설치 프로그램(Rack PDU Security Wizard.exe)을 실행합니다.
2. Windows의 **시작** 메뉴에서 **프로그램**, **Rack PDU Security Wizard**를 선택합니다.
3. **1단계** 화면에서, 만들 파일 유형으로 **CA Root Certificate**를 선택한 다음 생성할 키 길이를 선택합니다(기본 설정인 1024비트를 사용하거나 2048비트를 사용하여 복잡한 암호와 높은 수준의 보안 제공).
4. 인증 기관의 공개 루트 인증서와 개인 키를 포함할 파일의 이름을 입력합니다. 파일 확장자는 **.p15**여야 하며, 기본적으로 설치 폴더인 **C:\Program Files\Dell\Rack PDU Security Wizard**에 파일이 생성됩니다.
5. **Step 2** 화면에서 CA 루트 인증서를 구성할 정보를 제공합니다. **Country** 및 **Common Name** 필드는 반드시 입력해야 합니다. **Common Name** 필드에 회사 또는 기관을 식별하는 이름을 입력합니다. 공백없이 영숫자만 사용합니다.

   CA 루트 인증서는 기본적으로 현재 날짜 및 시간으로부터 10년 동안 유효하지만 **Validity Period Start** 및 **Validity Period End** 필드를 편집할 수 있습니다.

6. 다음 화면에서 인증서에 대한 요약 정보를 검토합니다. 아래로 스크롤하여 인증서 고유의 일련 번호와 기초 정보를 확인합니다. 제공한 정보를 변경하려면 **Back**을 클릭합니다. 정보를 변경합니다.

   인증서의 제목과 발급자 정보는 동일해야 합니다.

7. 마지막 화면에서 인증서가 생성되었는지 보여주고 다음 작업에 필요한 정보를 표시합니다.
   - 서버 인증서를 서명하는 데 사용할 .p15 파일의 위치와 이름
   - 랙 PDU에 액세스해야 하는 각 사용자의 브라우저로 로드하는 CA 루트 인증서인 .crt 파일의 위치와 이름

브라우저에 CA 루트 인증서 로드. .crt 파일을 랙 PDU에 액세스가 필요한 각 사용자의 브라우저에 로드합니다.

.crt 파일을 브라우저의 인증서 저장소(캐시)에 로드하는 방법은 브라우저의 도움말을 참조하십시오. 다음은 Microsoft Internet Explorer용 절차를 요약한 내용입니다.

1. **도구**를 선택하고 메뉴 모음에서 **인터넷 옵션**을 선택합니다.
2. 대화 상자의 Content 탭에서 Certificates와 Import를 차례로 클릭합니다.
3. Certificate Import Wizard가 나머지 절차를 안내합니다. X.509 파일 형식을 선택해야 하며 CA 공개 루트 인증서는 루트 인증서 및 서버 인증서 만들기 절차에서 만든 .crt 파일을 선택해야 합니다.

SSL 서버 사용자 인증서 만들기.

1. Windows의 **시작** 메뉴에서 **프로그램**, Rack PDU Security Wizard를 선택합니다.
2. Step 1 화면에서 파일 유형으로 SSL Server Certificate를 선택한 후 생성할 키의 길이를 선택합니다(기본 설정인 1024비트 사용 또는 복잡한 암호화 및 강화된 보안 수준을 제공하는 2048비트 사용).
3. 서버 인증서와 개인 키를 포함할 파일의 이름을 입력합니다. 파일 확장자는 .p15여야 하며, 기본적으로 **C:\Program Files\Dell\Rack PDU Security Wizard** 폴더에 파일이 생성됩니다.
4. Browse 를 클릭하고 루트 인증서 및 서버 인증서 만들기 절차에서 만든 CA 루트 인증서를 선택합니다. CA 루트 인증서는 만들어진 서버 사용자 인증서를 서명할 때 사용합니다.

5. Step 2 화면에서 서버 인증서를 구성할 정보를 제공합니다. Country 및 Common Name 필드는 반드시 입력해야 합니다. Common Name 필드에 서버(랙 PDU)의 IP 주소 또는 DNS 이름을 입력합니다. 서버 인증서는 기본적으로 10년 동안 유효하지만 Validity Period Start 및 Validity Period End 필드를 편집할 수 있습니다.

   구성 정보는 서명의 일부이기 때문에 모든 인증서의 구성 정보가 고유해야 합니다. 서버 인증서의 구성은 CA 루트 인증서의 구성과 동일할 수 없습니다. (만료 날짜는 고유한 구성으로 간주되지 않으며, 일부 다른 구성 정보도 달라야 합니다.)

6. 다음 화면에서 인증서에 대한 요약 정보를 검토합니다. 아래로 스크롤하여 인증서 고유의 일련 번호와 기초 정보를 확인합니다. 제공한 정보를 변경하려면 Back을 클릭합니다. 정보를 변경합니다.
7. 마지막 화면은 인증서가 만들어졌는지 보여주고 랙 PDU에 서버 인증서를 로드하는 작업을 안내합니다. 파일 확장자가 .p15이고 랙 PDU 개인 키와 공개 루트 인증서가 포함되어 있는 서버 인증서의 위치와 이름이 표시됩니다.

랙 PDU로 서버 인증서 로드.

1. Administration 탭에서 상단 메뉴 표시줄의 Network, 왼쪽 탐색 메뉴의 Web 제목 아래에 있는 ssl certificate를 선택합니다.
2. Add or Replace Certificate File을 선택하고 루트 인증서 및 서버 인증서 만들기 절차에서 만든 서버 인증서 .p15 파일을 찾습니다. (기본 위치는 **C:\Program Files\Dell\Rack PDU Security Wizard**입니다.)

   서버 인증서를 전송하는 대신 FTP 또는 SCP (Secure CoPy)를 사용할 수 있습니다. SCP의 경우, cert.p15 이름의 인증서를 IP 주소가 156.205.6.185인 랙 PDU로 전송하는 명령은 다음과 같습니다.

   ```
   scp cert.p15 dell@156.205.6.185
   ```

서버 인증서 및 서명 요청 만들기

요약

회사나 기관 자체의 인증 기관이 있거나 상용 인증 기관을 사용하여 서버 인증서를 서명하려는 경우 이 절차를 사용합니다.

- 인증서 서명 요청(CSR) 만들기 CSR에는 디지털 서명을 제외한 서버 인증서의 모든 정보가 있습니다. 이 프로세스로 두 개의 출력 파일이 생성됩니다.
  - 확장자가 .p15인 파일에 랙 PDU의 개인 키가 들어 있습니다.
  - 확장자가 .csr 인 파일에는 외부 인증 기관에 보내는 인증서 서명 요청이 들어 있습니다.
- 인증 기관에서 서명한 인증서를 받는 경우 이 인증서를 가져오기합니다. 인증서를 가져오면 개인 키가 들어 있는 파일이 외부 인증 기관에서 서명한 인증서가 들어 있는 .p15 파일과 결합됩니다. 출력 파일은 확장자가 .p15 이고 새로운 암호화된 서버 인증서 파일입니다.
- 서버 인증서를 랙 PDU로 로드합니다.
- 서버 인증서가 필요한 각 랙 PDU에 대해 서버 인증서 만들기와 로드 작업을 반복합니다.

절차

인증서 서명 요청(CSR) 만들기.

1. Rack PDU Security Wizard가 컴퓨터에 설치되어 있지 않으면 설치 프로그램(Rack PDU Security Wizard.exe)을 실행합니다.
2. Windows의 **시작** 메뉴에서 **프로그램**, **Rack PDU Security Wizard**를 선택합니다.
3. **Step 1** 화면에서 생성할 파일 유형으로 **Certificate Request**를 선택한 후 생성할 키의 길이를 선택합니다(기본 설정인 1024비트 사용 또는 복잡한 암호화 및 강화된 보안 수준을 제공하는 2048비트 사용).

4. 랙 PDU의 개인 키를 포함할 이 파일의 이름을 입력합니다. 파일 확장자는 .p15 여야 하며, 기본적으로 설치 폴더인 **C:\Program Files\Dell\Rack PDU Security Wizard**에 파일이 생성됩니다.
5. Step 2 화면에서 서명된 서버 인증서에 저장할 정보와 같은 인증서 서명 요청(CSR)의 구성 정보를 입력합니다. Country 및 Common Name 필드는 반드시 입력해야 합니다. 나머지 필드는 생략할 수 있습니다. Common Name 필드에 랙 PDU의 IP 주소 또는 DNS 이름을 입력합니다.

서버 인증서는 기본적으로 현재 날짜 및 시간으로부터 10년 동안 유효하지만 Validity Period Start 및 Validity Period End 필드를 편집할 수 있습니다.

6. 다음 화면에서 인증서에 대한 요약 정보를 검토합니다. 아래로 스크롤하여 인증서 고유의 일련 번호와 기초 정보를 확인합니다. 제공한 정보를 변경하려면 Back을 클릭합니다. 정보를 변경합니다.

인증서의 제목과 발급자 정보는 동일해야 합니다.

7. 마지막 화면은 인증서 서명 요청이 만들어졌는지 보여주고 확장자가 .csr 인 파일의 위치와 이름을 표시합니다.
8. 인증서 서명 요청을 외부 인증 기관, 즉 상용 인증 기관 또는 해당하는 경우 회사나 기관 자체에서 관리하는 인증 기관으로 보냅니다.

인증 기관이 제공한 서버 인증서의 서명과 발급에 관한 지침을 참조하십시오.

서명된 인증서 가져오기. 외부 인증 기관에서 서명된 인증서를 반환하면 인증서를 가져옵니다. 이 절차에서 서명된 인증서와 개인 키가 SSL 서버 인증서에 결합된 후 SSL 서버 인증서를 랙 PDU에 업로드합니다.

1. Windows의 **시작** 메뉴에서 **프로그램**, Rack PDU Security Wizard를 선택합니다.
2. Step 1 화면에서 Import Signed Certificate를 선택합니다.
3. 외부 인증 기관에서 받은 서명된 서버 인증서를 찾아 선택합니다. 이 파일의 확장자는 .cer 또는 .crt입니다.
4. 인증서 서명 요청(CSR) 만들기작업의 step 4에서 만든 파일을 찾아 선택합니다. 파일 확장자는 .p15이고, 랙 PDU의 개인 키가 파일에 포함되며, 파일은 기본적으로 설치 폴더인 **C:\Program Files\Dell\Rack PDU Security Wizard**에 있습니다.
5. 랙 PDU에 업로드할 서명된 서버 인증서인 출력 파일의 이름을 지정합니다. 파일 확장자는 .p15여야 합니다.
6. Next를 클릭하여 서버 인증서를 생성합니다. 요약 화면의 Issuer Information에서 외부 인증 기관이 인증서에 서명했는지 확인할 수 있습니다.
7. 마지막 화면은 인증서가 만들어졌는지 보여주고 랙 PDU에 서버 인증서를 로드하는 작업을 안내합니다. 파일 확장자가 .p15이며 랙 PDU의 개인 키와 .cer 또는 .crt 파일로부터 가져온 공개 키가 포함된 서버 인증서의 위치와 이름이 표시됩니다.

랙 PDU로 서버 인증서 로드.

1. Administration 탭에서 상단 메뉴 표시줄의 Network, 왼쪽 탐색 메뉴의 Web 제목 아래에 있는 ssl certificate를 선택합니다.
2. Add or Replace Certificate File을 선택하고 루트 인증서 및 서버 인증서 만들기 절차에서 만든 서버 인증서 .p15 파일을 찾습니다. (기본 위치는 **C:\Program Files\Dell\Rack PDU Security Wizard**입니다.)

FTP 또는 SCP (Secure CoPy)를 사용하여 서버 인증서를 랙 PDU로 전송하는 방법도 있습니다. SCP의 경우, cert.p15 이름의 인증서를 156.205.6.185의 IP 주소를 가진 랙 PDU로 전송하기 위한 명령은 다음과 같습니다.

```
scp cert.p15 dell@156.205.6.185
```

SSH 호스트 키 만들기

요약

이 절차는 생략할 수 있습니다. SSH 암호화를 선택했지만 호스트 키를 만들지 않은 경우 랙 PDU가 재부팅할 때 2048비트 RSA 키를 생성합니다. Rack PDU Security Wizard로 생성하는 SSH용 호스트 키가 1024비트 또는 2048비트 RSA 키인지 정의합니다.

1024비트 키를 생성하거나 복잡한 암호화 및 강화된 보안을 지원하는 2048비트 키를 생성할 수 있습니다.

- Rack PDU Security Wizard를 사용하여 확장자가 .p15 인 파일에 암호화되어 저장되는 호스트 키를 만듭니다.
- 호스트 키를 랙 PDU로 로드합니다.

절차

호스트 키 만들기.

1. Rack PDU Security Wizard가 컴퓨터에 설치되어 있지 않으면 설치 프로그램(Rack PDU Security Wizard.exe)을 실행합니다.
2. Windows의 **시작** 메뉴에서 **프로그램**, Rack PDU Security Wizard를 선택합니다.
3. Step 1 화면에서 생성할 파일 유형으로 SSH Server Host Key를 선택하고, 생성할 키의 길이를 선택합니다(기본 설정인 1024비트 사용 또는 복잡한 암호화 및 강화된 보안 수준을 제공하는 2048비트 사용).
4. 호스트 키가 포함될 이 파일의 이름을 입력합니다. 파일 확장자는 .p15여야 합니다. 이 파일은 기본적으로 설치 폴더 **C:\Program Files\Dell\Rack PDU Security Wizard**에 만들어집니다.
5. Next를 클릭하여 호스트 키를 생성합니다.
6. 요약 화면에 SSH 버전 2 기초 정보가 표시됩니다. 이 정보는 각 호스트 키에 대해 고유하며 호스트 키를 식별하는 정보입니다. 호스트 키를 랙 PDU에 로드한 후 여기에 표시된 지문이 SSH 클라이언트 프로그램에 표시된 랙 PDU의 SSH 지문과 일치하는지 확인하여 정확한 호스트 키가 업로드되었는지 확인할 수 있습니다.
7. 마지막 화면은 호스트 키가 만들어졌는지 보여주고 호스트 키를 랙 PDU에 로드하는 작업을 안내하며, 파일 확장자가 .p15인 호스트 키의 위치와 이름을 표시합니다.

랙 PDU에 호스트 키 로드.

1. Administration 탭에서 상단 메뉴 표시줄의 Network, 왼쪽 탐색 메뉴의 Console 제목 아래에 있는 ssh host key를 선택합니다.
2. Add or Replace Host Key를 선택하고 호스트 키 만들기 절차에서 만든 서버 인증서 .p15 파일을 찾습니다. (기본 위치는 **C:\Program Files\Dell\Rack PDU Security Wizard**입니다.)
3. User Host Key 페이지 하단에서 SSH 지문을 확인합니다. SSH 클라이언트 프로그램으로 랙 PDU에 로그인하고 이 지문이 클라이언트 프로그램에서 표시된 지문이 일치하는지 확인하여 정확한 호스트 키가 업로드되었는지 확인합니다.

또는, FTP 또는 SCP를 사용하여 호스트 키 파일을 랙 PDU로 전송할 수 있습니다. SCP의 경우, hostkey.p15 이름의 호스트 키를 IP 주소가 156.205.6.185인 랙 PDU로 전송하는 명령은 다음과 같습니다.

```
scp hostkey.p15 dell@156.205.6.185
```

명령줄 인터페이스 액세스 및 보안

관리자 또는 장치 사용자 계정을 가진 사용자는 Telnet 또는 SSH (Secure Shell) 중 활성화된 방식을 통해 명령줄 인터페이스에 액세스할 수 있습니다. (관리자는 Administration 탭을 선택한 다음 상단 메뉴 표시줄의 Network 및 왼쪽 탐색 메뉴의 Console 제목 아래에 있는 access를 선택하여 이러한 액세스 방법을 설정할 수 있습니다.) 기본값으로 사용되는 방법은 Telnet입니다. SSH가 활성화되면 Telnet은 자동으로 비활성화됩니다.

Telnet을 사용한 기본 액세스. Telnet은 사용자 이름과 암호로 기본적인 인증 보안을 제공하지만 암호화에 비해 보안 수준이 낮습니다.

SSH를 사용한 높은 수준의 보안 액세스. 웹 인터페이스에 보안 수준이 높은 SSL을 사용하는 경우는 SSH (Secure Shell)를 사용하여 명령줄 인터페이스에 액세스합니다. SSH는 사용자 이름, 암호 및 전송 데이터를 암호화합니다.

SSH이나 Telnet을 통해 명령줄 인터페이스에 액세스하더라도 인터페이스, 사용자 계정 및 사용자 액세스 권한은 동일하지만, SSH를 사용하려면 먼저 컴퓨터에 SSH를 구성하고 SSH 클라이언트 프로그램을 설치해야 합니다.

Telnet 및 SSH (Secure SHell)

SSH가 설정되어 있으면 Telnet을 사용하여 명령줄 인터페이스에 액세스할 수 없습니다. SSH를 사용하면 SCP가 자동으로 사용됩니다.

SSH를 사용하며 해당 포트를 구성한 경우 SCP (Secure CoPy)를 사용하기 위해 필요한 추가 구성은 없습니다. SCP는 SSH에 동일한 구성을 사용됩니다.

SSH를 사용하려면 SSH 클라이언트가 설치되어 있어야 합니다. 대부분의 Linux 및 다른 UNIX® 플랫폼에는 SSH 클라이언트가 포함되어 있지만, Microsoft Windows 운영 체제에는 포함되어 있지 않습니다. SSH 클라이언트 제품은 여러 공급업체로부터 구매할 수 있습니다.

Telnet 및 SSH (Secure Shell)에 대한 옵션을 구성하려면:

1. 웹 인터페이스의 Administration 탭에서 상단 메뉴 표시줄의 Network, 왼쪽 탐색 메뉴의 Console 제목 아래에 있는 access를 선택합니다.
2. Telnet 및 SSH에 사용할 포트 설정 구성

   비표준 포트를 사용한 추가 보안에 대한 자세한 내용은 포트 할당을 참조하십시오.

3. 왼쪽 탐색 메뉴의 Console 아래에서 ssh host key를 선택하고 이전에 Rack PDU Security Wizard로 생성한 호스트 키 파일을 지정한 다음, 키 파일을 랙 PDU에 로드합니다.

   여기서 호스트 키 파일을 지정하지 않는 경우, 유효하지 않은 호스트 키를 설치하는 경우 또는 호스트 키를 설치하고 않고 SSH를 사용하는 경우 랙 PDU에서 2048 비트 RSA 호스트 키를 생성합니다. 랙 PDU가 호스트 키를 생성하도록 하려면 재부팅해야 합니다. 랙 PDU**가 이 호스트 키를 만드는 데 최대 1분이 소요될 수 있으며 이 동안은 SSH에 액세스할 수 없습니다.**

   대신에 Windows 운영 체제의 명령 프롬프트와 같은 명령 행 인터페이스에서 FTP 또는 SCP를 사용하여 호스트 키 파일을 전송할 수 있습니다.

4. SSH 버전 2에 대한 SSH 호스트 키의 *지문* 표시. 대부분의 SSH 클라이언트는 세션이 시작될 때 지문을 표시합니다. 클라이언트가 표시한 지문을 랙 PDU의 웹 인터페이스 또는 명령줄 인터페이스에서 기록한 지문과 비교합니다.

웹 인터페이스 액세스 및 보안: HTTP 및 HTTPS (SSL 사용)

HTTP(Hypertext Transfer Protocol)는 사용자 이름과 암호를 사용하여 액세스를 제공하지만 전송 중 사용자 이름, 암호 및 데이터를 암호화하지 않습니다. SSL 상의 HTTPS는 전송 중에 사용자 이름, 암호 및 데이터를 암호화하고 디지털 인증서를 통해 랙 PDU 인증을 제공합니다.

여러 가지 디지털 인증서 사용 방법 중에서 선택하려면 디지털 인증서 만들기 및 설치를 참조하십시오.

HTTP 및 HTTPS를 구성하려면:

1. Administration 탭에서 상단 메뉴 표시줄의 Network, 왼쪽 탐색 메뉴의 Web 제목 아래에 있는 access를 선택합니다.
2. HTTP 또는 HTTPS를 설정하고 각각의 두 프로토콜이 사용할 포트를 구성합니다. 다시 로그온할 때 변경 내용이 적용됩니다. SSL이 활성화되면 브라우저에 작은 자물쇠 아이콘이 표시됩니다.

비표준 포트를 사용한 추가 보안에 대한 자세한 내용은 포트 할당을 참조하십시오.

3. 왼쪽 탐색 메뉴의 Web 아래에서 ssl certificate를 선택하여 랙 PDU에 서버 인증서를 설치할 지 여부를 결정합니다. 인증서를 Rack PDU Security Wizard로 생성한 후 설치하지 않은 경우:
   - 웹 인터페이스에서 인증서 파일을 찾아 랙 PDU에 업로드합니다.
   - 또는 SCP (Secure CoPy) 프로토콜이나 FTP를 사용하여 인증서 파일을 랙 PDU에 업로드합니다.

서버 인증서를 만들어 미리 업로드하면 HTTPS를 활성화하는 데 필요한 시간이 감소합니다. 서버 인증서를 로드하지 않고 HTTPS를 설정하면 재부팅될 때 랙 PDU가 인증서를 만듭니다. 랙 PDU가 인증서를 만드는 데 최대 1분이 소요될 수 있으며 이 시간에는 SSL 서버에 액세스할 수 없습니다.

랙 PDU가 생성하는 인증서에는 몇 가지 제한이 있습니다. 방법 1: 랙 PDU에 의해 자동으로 생성된 기본 인증서 사용을 참조하십시오.

4. 유효한 디지털 서버 인증서를 로드하면 Status 필드에 링크가 표시됩니다. Valid certificate 링크를 클릭하면 인증서의 매개변수가 표시됩니다.

매개변수	설명
Issued To:	Common Name (CN): 랙 PDU의 IP 주소 또는 DNS 이름. 이 필드는 웹 인터페이스에 로그인해야 하는 방법을 제어합니다. • 인증서가 만들어질 때 이 필드에 IP 주소가 지정된 경우 해당 IP 주소를 사용하여 로그온합니다. • 인증서가 만들어질 때 이 필드에 DNS 이름이 지정된 경우에는 해당 DNS 이름을 사용하여 로그온합니다. 해당 인증서에 지정한 IP 주소 또는 DNS 이름을 사용하지 않으면 인증이 실패하며 계속할지 묻는 오류 메시지가 나타납니다. 랙 PDU에서 생성된 기본 서버 인증서의 경우 랙 PDU의 일련 번호 대신에 이 필드가 표시됩니다. Organization (O), Organizational Unit (OU) 및 Locality, Country: 서버 인증서를 사용하고 있는 조직의 이름, 조직 단위, 위치. 랙 PDU에서 기본적으로 생성된 서버 인증서의 경우, Organizational Unit (OU) 필드에 “Internally Generated Certificate"가 표시됩니다. Serial Number: 서버 인증서의 일련 번호.
Issued By:	Common Name (CN): CA 루트 인증서에 지정된 공통 이름. 랙 PDU에서 생성된 기본 서버 인증서의 경우 랙 PDU의 일련 번호 대신에 이 필드가 표시됩니다. Organization (O) 및 Organizational Unit (OU): 서버 인증서를 발생한 조직의 이름과 조직 단위. 서버 인증서가 랙 PDU에서 기본적으로 생성된 경우 이 필드에 “Internally Generated Certificate”가 표시됩니다.
Validity:	Issued on: 인증서가 발급된 날짜 및 시간 Expires on: 인증서가 만료된 날짜 및 시간

매개변수	설명
Fingerprints	두 지문은 각각 콜론으로 구분된 긴 영숫자 문자열입니다. 지문은 서버를 추가 인증하기 위한 고유한 ID입니다. 기록한 지문은 브라우저에 표시되는 인증서에 포함된 지문과 비교합니다. SHA1 Fingerprint: SHA-1 (Secure Hash Algorithm)로 생성된 지문 MD5 Fingerprint: MD5 (Message Digest 5) 알고리즘으로 생성된 지문

지원되는 RADIUS 기능 및 서버

지원되는 기능

지원되는 인증 및 권한 부여 기능: RADIUS (Remote Authentication Dial-In User Service). RADIUS를 사용하여 각 랙 PDU에 대한 원격 액세스를 중앙에서 관리합니다. 사용자가 랙 PDU에 액세스할 때 사용자의 권한 수준을 확인하기 위한 인증 요청이 RADIUS 서버로 전송됩니다.

권한 수준에 대한 자세한 내용은 사용자 계정 유형을 참조하십시오.

지원되는 RADIUS 서버

지원되는 RADIUS 서버: FreeRADIUS 및 Microsoft IAS 2003. 일반적으로 사용되는 다른 RADIUS 응용 프로그램도 작동할 수는 있지만 완전한 테스트는 거치지는 않았습니다.

랙 PDU 구성

인증

랙 PDU에 사용되는 RADIUS 사용자 이름의 길이는 32자로 제한됩니다.

Administration 탭의 상단 메뉴 표시줄에서 Security를 선택합니다. 계속해서 왼쪽 탐색 메뉴의 Remote Users 아래에서 authentication을 선택하여 인증 방법을 정의합니다.

- Local Authentication Only: RADIUS가 비활성화됩니다. 로컬 인증이 활성화됩니다.
- RADIUS, then Local Authentication: RADIUS와 로컬 인증 모두 활성화됩니다. 우선 RADIUS 서버에서 인증을 요청합니다. 로컬 인증은 RADIUS 서버가 응답하지 않는 경우에만 사용됩니다.
- RADIUS Only: RADIUS가 활성화됩니다. 로컬 인증이 비활성화됩니다.

RADIUS Only를 선택하고, RADUIS 서버가 사용 불능 상태이거나 제대로 확인 또는 구성되지 않은 경우 모든 사용자가 원격 액세스를 사용할 수 없습니다. 명령줄 인터페이스에 대한 직렬 연결을 사용하여 RADIUS 액세스 설정을 **local** 또는 **radiusLocal**로 변경하여 액세스 권한을 다시 받아야 합니다. 예를 들어, 액세스 설정을 **local**로 변경하는 명령은 다음과 같습니다.

```
radius -a local
```

RADIUS

RADIUS를 구성하려면 Administration 탭의 상단 메뉴 표시줄에서 Security를 선택합니다. 계속해서 왼쪽 탐색 메뉴의 Remote Users 아래에서 RADIUS를 선택합니다.

설정	정의
RADIUS Server	서버 이름 또는 RADIUS 서버의 IP 주소입니다. **참고:** RADIUS 서버는 기본적으로 1812 포트를 사용하여 사용자를 인증합니다. 다른 포트를 사용하려면 RADIUS 서버명 또는 IP 주소 끝에 새로운 포트 번호를 입력하고 콜론(:)을 추가합니다.
Secret	RADIUS 서버와 랙 PDU 간의 공유 보안입니다.
Reply Timeout	RADIUS 서버가 응답할 때까지 랙 PDU가 대기하는 시간(단위: 초)입니다.
Test Settings	관리자 사용자 이름과 암호를 입력하여 구성한 RADIUS 서버 경로를 테스트합니다.
Skip Test and Apply	RADIUS 서버 경로를 테스트하지 않습니다.

구성된 서버 2대가 나열되고 RADIUS, then Local Authentication 또는 RADIUS Only가 인증 방법으로 설정되어 있는 경우, Switch Server Priority 버튼을 클릭하여 사용자를 인증할 RADIUS 서버를 변경할 수 있습니다.

RADIUS 서버 구성

랙 PDU와 함께 사용할 수 있도록 RADIUS 서버를 구성해야 합니다. 여기에 제시되는 예는 지정한 RADIUS 서버에 필수적인 내용 및 형식과 약간 다를 수도 있습니다. 예에서 콘센트에 대한 내용은 콘센트 사용자를 지원하는 랙 PDU 장치에만 적용됩니다.

1. RADIUS 서버 클라이언트 목록(파일)에 랙 PDU의 IP 주소를 추가합니다.
2. VAS(Vendor Specific Attributes)가 정의되지 않은 한 대신에 Service-Type 특성을 포함하여 사용자를 구성해야 합니다. Service-Type 특성이 구성되지 않은 경우 사용자에게 읽기 전용 권한만 부여됩니다(웹 인터페이스에 한해). Service-Type에 허용되는 두 가지 값은 사용자에게 관리자 권한을 부여하는 Administrative-User (6)와 장치 권한을 부여하는 Login-User (1)입니다.

RADIUS 사용자 파일에 대한 자세한 내용은 RADIUS 서버 설명서를 참조하십시오.

Service-Type Attributes 사용 예

다음 RADIUS 사용자 파일 예에서:

- **RPDUAdmin**은 **Service-Type: Administrative-User, (6)**에 해당
- **RPDUDevice**는 **Service-Type: Login-User, (1)**에 해당
- **RPDUReadOnly**는 **Service-Type: null**에 해당

```
RPDUAdmin       Auth-Type = Local, Password = "admin"
   Service-Type = Administrative-User

RPDUDevice      Auth-Type = Local, Password = "device"
   Service-Type = Login-User

RPDUReadOnly    Auth-Type = Local, Password = "readonly"
```

Vendor Specific Attributes 사용 예

RADIUS 서버에서 제공되는 Service-Type 특성 대신 VSA(Vendor Specific Attributes)를 사용할 수 있습니다. 이 방법은 사전 항목과 RADIUS 사용자 파일이 필요합니다. 사전 파일에서 숫자 값이 아닌 ATTRIBUTE 및 VALUE 키워드에 대한 이름을 정의할 수 있습니다. 숫자 값을 변경하면 RADIUS 인증과 권한 부여가 제대로 작동하지 않습니다. VSA는 표준 RADIUS 특성에 우선합니다.

Dictionary file. RADIUS 사전 파일(dictionary.dell)의 예:

```
#
# dictionary.dell
#
#
VENDOR   DELL 318
#
# Attributes
#
ATTRIBUTE DELL-Service-Type 1 integer DELL
ATTRIBUTE DELL-Outlets      2 string DELL

VALUE DELL-Service-Type Admin    1
VALUE DELL-Service-Type Device   2
VALUE DELL-Service-Type ReadOnly 3
#
# For devices with outlet users only
#
VALUE DELL-Service-Type Outlet   4
```

RADIUS Users file with VSAs. VSA를 사용하는 RADIUS 사용자 파일의 예:

```
VSAAdmin     Auth-Type = Local, Password = "admin"
             DELL-Service-Type = Admin

VSADevice    Auth-Type = Local, Password = "device"
             DELL-Service-Type = Device

VSAReadOnly  Auth-Type = Local, Password = "readonly"
             DELL-Service-Type = ReadOnly

# Give user access to device outlets 1, 2 and 3.
VSAOutlet    Auth-Type = Local, Password = "outlet"
             DELL-Service-Type = Outlet,
             DELL-Outlets = "1,2,3"
```

다음의 관련 항목을 참조하십시오.

- 세 가지 기본적 사용자 권한 수준(관리자, 장치 사용자 및 읽기 전용 사용자)에 대한 정보를 보려면 사용자 계정 유형.
- 테스트 및 지원되는 RADIUS 서버에 대한 정보를 보려면 지원되는 RADIUS 서버.

UNIX 섀도우 암호 사용의 예. RADIUS 사전 파일에 UNIX 섀도우 암호 파일(/etc/passwd)이 사용된 경우, 다음 두 가지 방법으로 사용자를 인증할 수 있습니다.

- 모든 UNIX 사용자가 관리자 권한을 가진 경우 RADIUS "user" 파일에 다음을 추가합니다. 장치 사용자만 허용하려면 Dell-Service-Type을 **Device**로 변경합니다.

```
DEFAULT    Auth-Type = System
           DELL-Service-Type = Admin
```

- RADIUS "user" 파일에 사용자 이름과 특성을 추가하고 /etc/passwd에 대해 암호를 확인합니다. 다음은 **bconners** 및 **thawk** 사용자에 대한 예입니다.

```
bconners          Auth-Type = System
                  DELL-Service-Type = Admin
thawk             Auth-Type = System
                  DELL-Service-Type = Outlet
                  DELL-Outlets = "1,2,3"
```

색인

N

O

P

R

S

T

U

X

Z

11/2010 부품 번호 990-3926-019

www.dell.com | support.dell.com