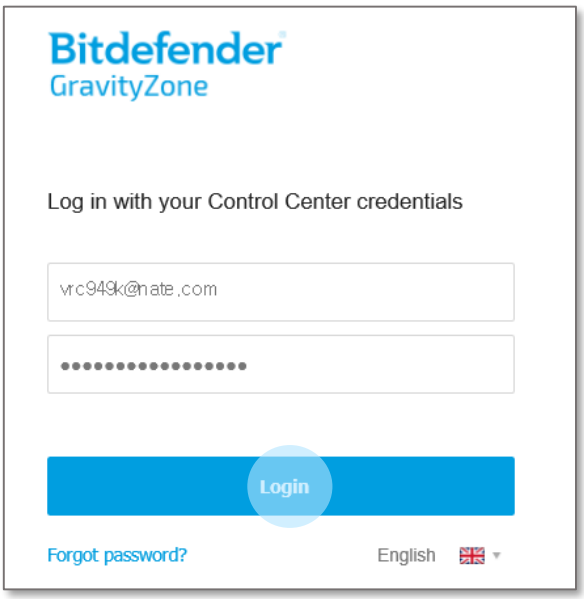
시작하기

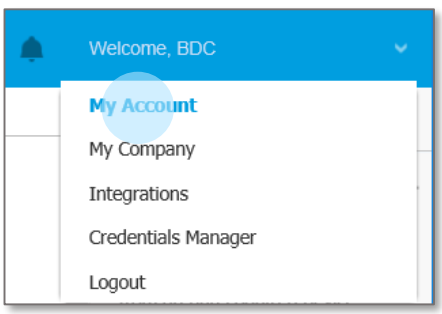
컨트롤 센터 로그인

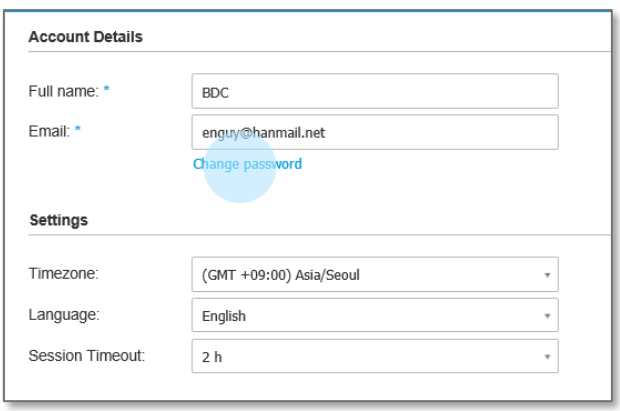
1. http://gravityzone.bitdefender.com 주소로 접속 합니다.
2. 발급 받은 계정 및 패스워드를 입력하여 로그인 합니다.



패스워드 및 설정 변경

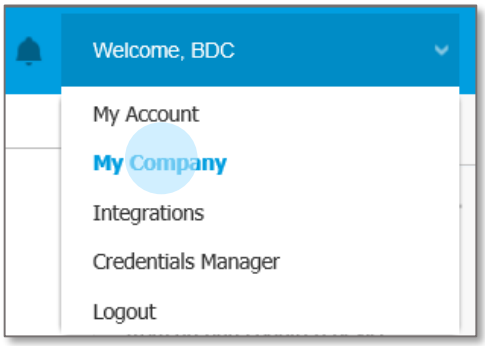
1. 로그인 후 우측 상단 서브메뉴 중 'My Account'를 선택합니다.
2. 'Change password' 를 클릭하여 패스워드를 변경합니다.
3. 'Timezone'을 클릭하여 표준시를 Asia/Seoul 로 변경합니다.
4. 'Session Timeout' 메뉴를 통해 세션 유지 시간을 변경할 수 있습니다.

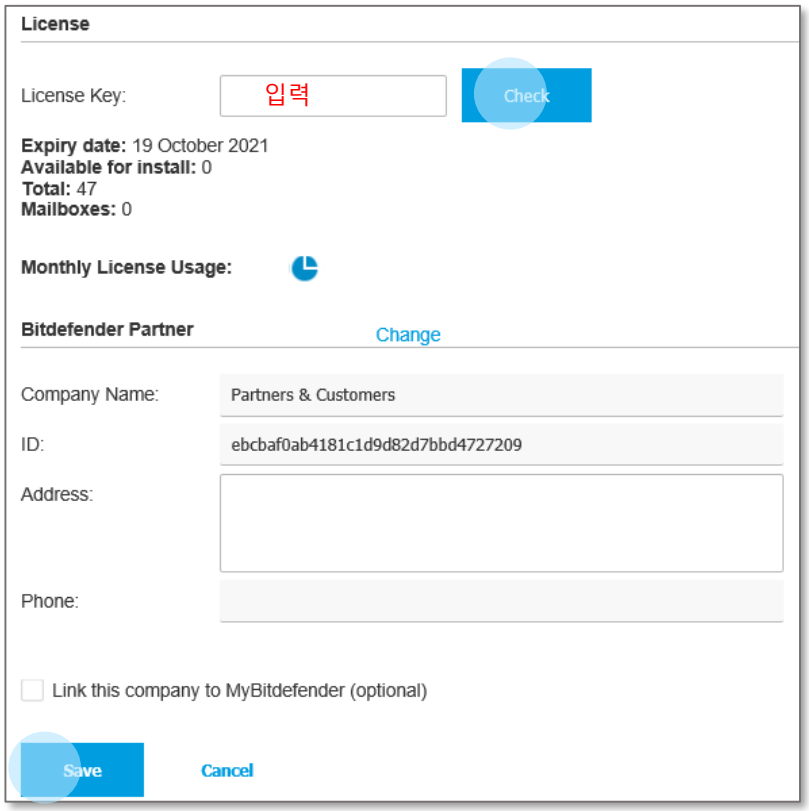




라이선스 등록

1. 우측 상단 서브메뉴 중 'My Company'를 선택합니다.
2. 'License' 항목에 발급 받은 라이선스 키를 입력 후 'Check' 버튼을 클릭합니다.
3. 등록이 완료되면 하단의 'Save' 버튼을 클릭하여 변경 내용을 저장합니다.

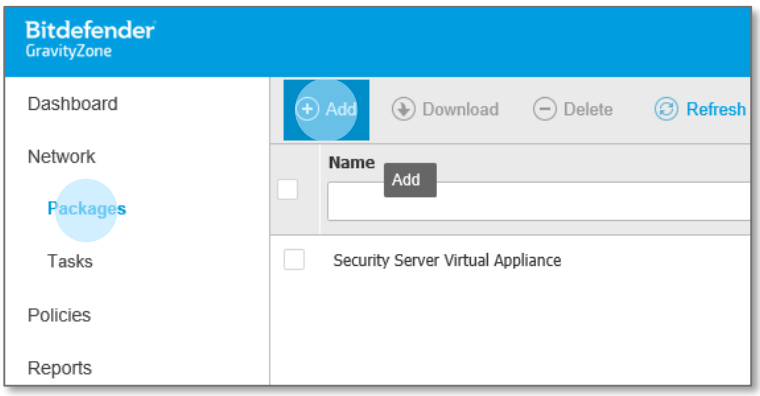




엔드포인트 설치본 제작하기

설치본 생성

1. 좌측 메인 메뉴 **‘Pakages’** 메뉴로 이동합니다.
2. 상단 **‘Add’** 항목을 클릭합니다.

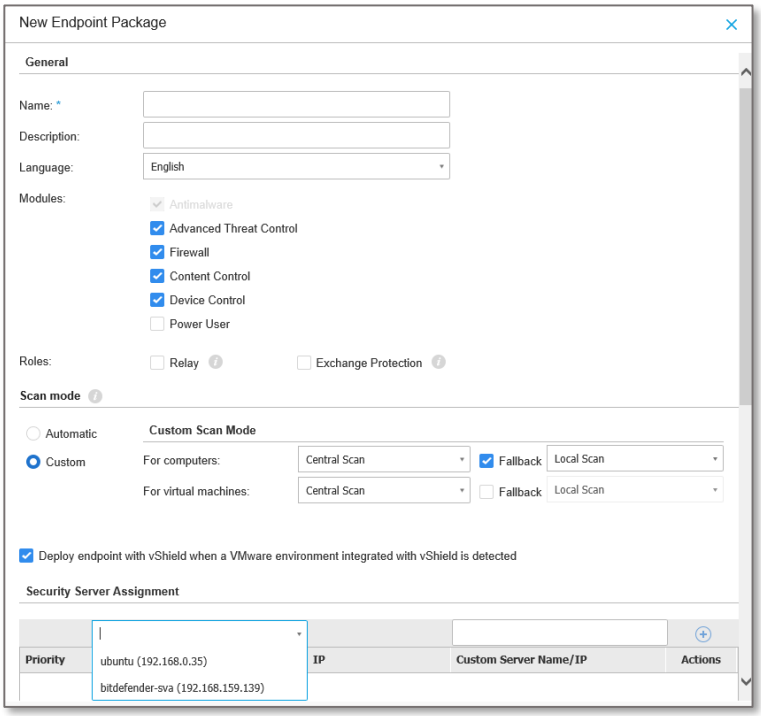


중요 : 비트디펜더 엔드포인트 설치본은 PC, 서버, 가상화 등 모든 운영 환경에 대응하는 통합 설치본으로 제공됩니다.

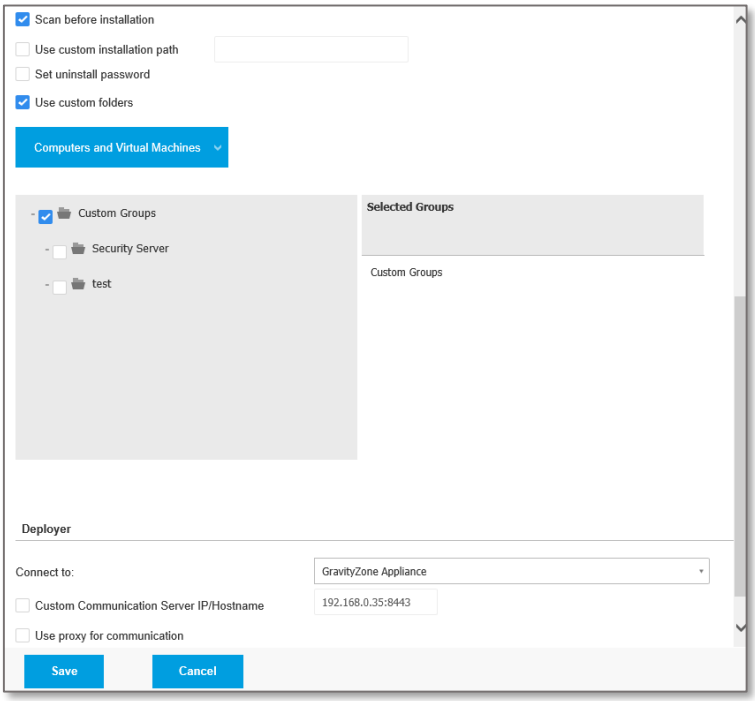
설치본 세부 설정

1. 사용하고자 하는 설치본 이름을 입력합니다.
2. ‘Modules’ 항목을 통해 설치본에 포함될 모듈을 선택합니다. (설치 후에도 변경 가능)
   - Antimalware : 악성코드 탐지 및 치료 (기본)
   - Advanced Thread Control: 행위기반탐지
   - Firewall: 네트워크 드라이버 기반 방화벽
   - Device Control: 매체제어 (USB 저장매체 통제)
   - Power User: 사용자 환경설정 권한 부여
3. 설치본 역할을 선택합니다.
   - Relay : 보조 서버 역할을 수행
   - Exchange Protection : MS 익스체인지 연동
4. 검사 방식을 선택합니다.
   - Automatic : 시스템 리소스 기준 자동 선택
   - Central Scan : 중앙 집중형 클라우드 검사
   - Hybrid Scan : 클라우드/로컬스캔 방식 혼용
   - Local Scan : 로컬에 패턴을 로딩하여 검사

‘Central Scan’ 기능은 Advanced Business 라이선스 사용시에만 선택할 수 있습니다.



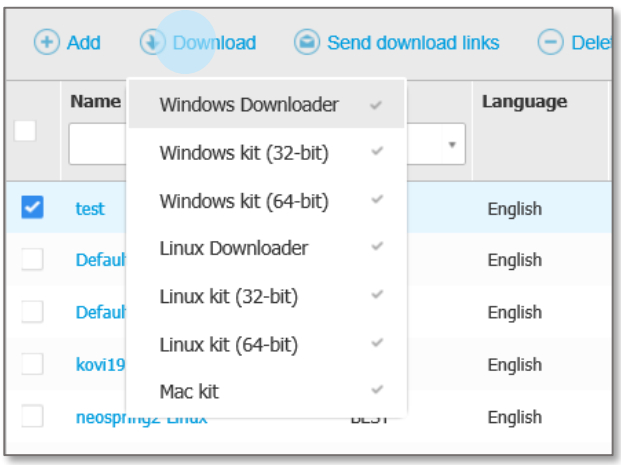
6. 설치 전 검사수행을 원하는 경우 ‘Scan before Installation’ 항목을 선택합니다.
7. 사용자 삭제 방지를 위해 패스워드 설정을 원하는 경우 ‘Set uninstall password’ 항목을 선택 후 패스워드를 입력합니다.
8. ‘User custom folders’ 항목을 선택하여 설치 시 등록될 관리 그룹을 지정할 수 있습니다.
9. 관리 노드 분배를 위한 로드 밸런싱 구성 시 ‘Custom Communication Server IP/Hostname’ 항목을 체크하고 서버 IP를 입력합니다.
10. ‘Save’ 버튼을 클릭하여 설정을 저장합니다.



중요 : 비트디펜더 엔드포인트 설치본은 PC, 서버, 가상화 등 모든 운영 환경에 대응하는 통합 설치본으로 제공됩니다.

엔드포인트 설치 (For Windows)

1. 좌측 메인 메뉴 **‘Pakages’** 메뉴로 이동합니다.
2. 생성된 설치본 항목을 체크 후 상단 메뉴 중 ‘Download’를 클릭합니다.
3. ‘Windows Downloader’ 항목을 선택 후 설치본을 다운로드 합니다.

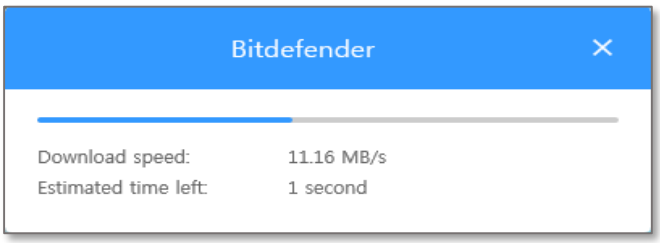


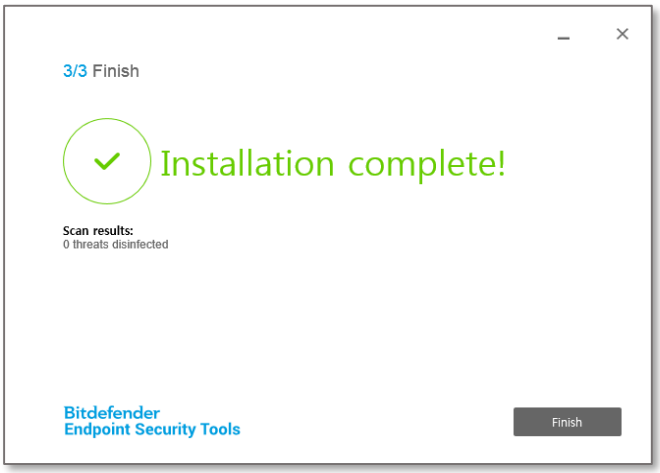
- Windows Downloader : 윈도우 다운로더 설치본 (3.3MB)
- Windows Kit (32-bit) : 윈도우 32비트용 풀 설치본 (400MB)
- Windows Kit (64-bit) : 윈도우 64비트용 풀 설치본 (400MB)
- Linux Downloader : 리눅스 다운로더 설치본 (8.2MB)
- Linux kit (32-bit) : 리눅스 32비트용 풀 설치본 (309MB)
- Linux kit (32-bit) : 리눅스 64비트용 풀 설치본 (309MB)
- Mac kit : 애플 MAC OS용 스크립트 설치본 (180MB)

4. 다운로드 받은 파일을 설치 대상 시스템으로 이동 및 복사하여 설치를 진행합니다.

주의 : ‘Windows Downloader’ 설치본의 경우 다운로드 받은 파일의 파일명을 사용자 임의로 변경하면 설치가 진행되지 않습니다. ‘Windows kit’ 설치본은 파일명 변경과 무관합니다.

5. 설치본 파일을 더블클릭 하면 다운로더가 실행되면서 관련 모듈을 서버로부터 다운로드 받습니다.
6. 설치가 정상적으로 완료되면 'Installation complete' 메시지가 나타나며 'Finish' 버튼을 클릭하여 설치를 종료합니다.
7. 최초 설치의 경우 재부팅은 필요하지 않습니다.

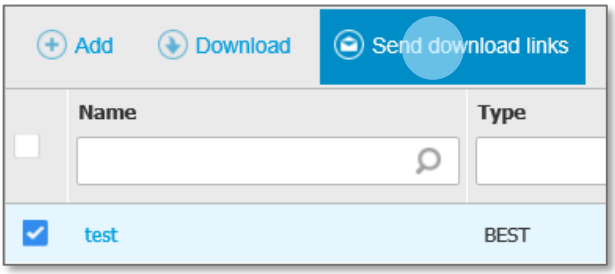


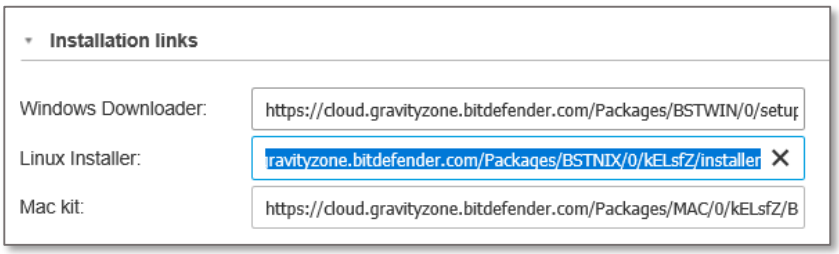


주의 : 기존에 설치된 비트디펜더 제품을 삭제하고 재설치를 진행 하는 경우에는 시스템 재부팅이 필요합니다.

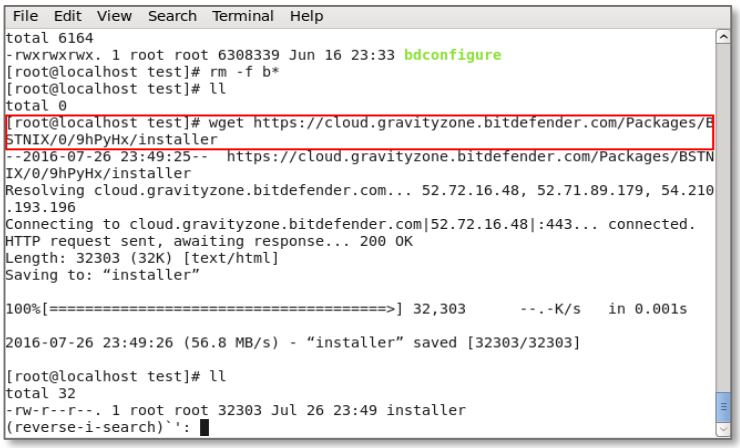
엔드포인트 설치 (For Linux)

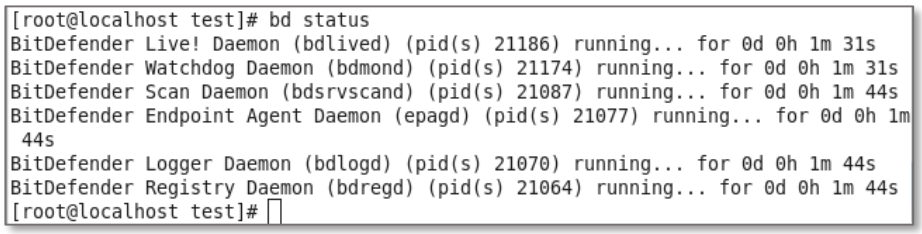
1. 좌측 메인 메뉴 **'Pakages'** 메뉴로 이동합니다.
2. 생성된 설치본 항목을 체크 후 상단 메뉴 중 'Send download links'를 클릭합니다.
3. 'Installations links' 활성화 후 'Linux Installer' 경로를 복사합니다.





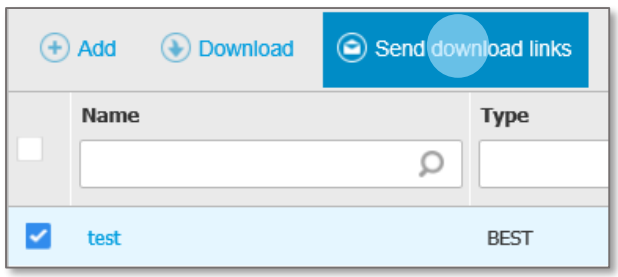
4. 설치 대상 시스템 Root 계정으로 로그인 합니다.
5. Wget 명령을 통해 설치 패키지를 다운로드 합니다.
   (복사한 Linux Installer 경로 입력)
   ex) wget https://cloud.gravityzone.bitdefender.com/...
6. #chmod +x installer 명령으로 퍼미션을 변경합니다.
7. #./installer 명령으로 설치를 진행합니다.
8. 정상적으로 설치가 완료되면 #bd status 명령으로 서비스 상태를 확인합니다.

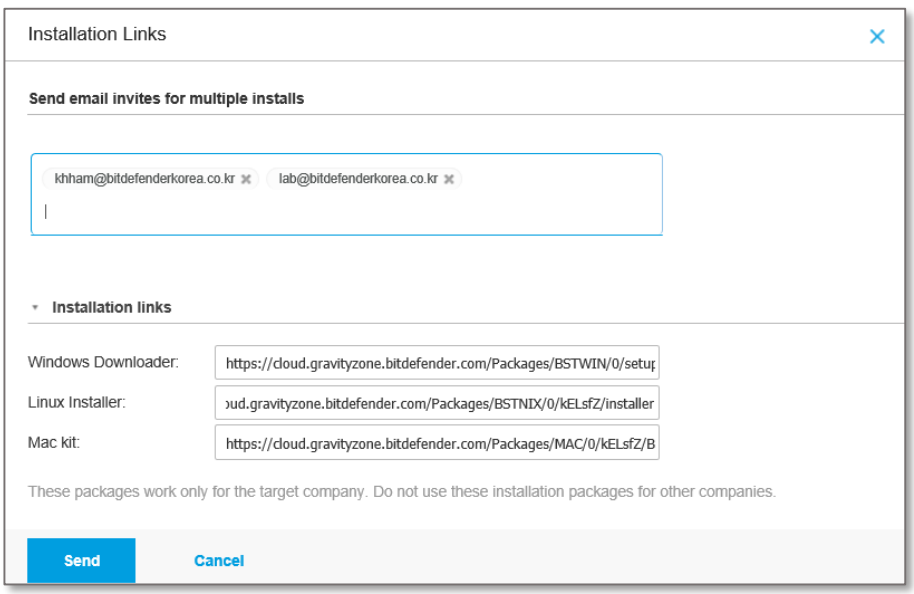




설치본 배포 (다운로드 링크 메일 전송)

1. 좌측 메인 메뉴 **‘Pakages’** 메뉴로 이동합니다.
2. 생성된 설치본 항목을 체크 후 상단 메뉴 중 ‘Send download links’를 클릭합니다.
3. ‘Send email invites for multiple installs’ 항목에 배포 대상 사용자 이메일을 등록합니다.
4. ‘Send’ 버튼을 클릭합니다.



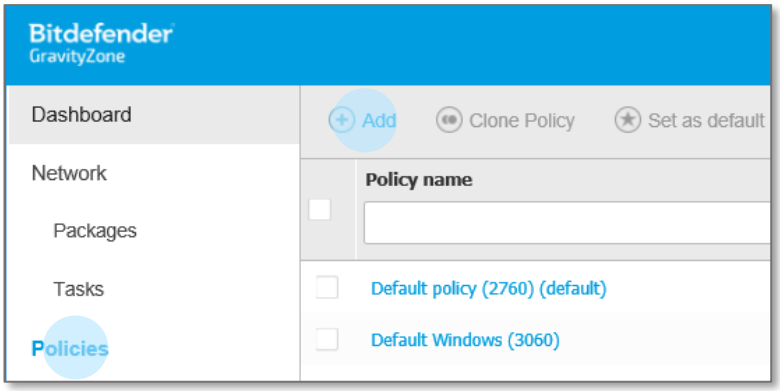


Security Policies

정책 설정하기

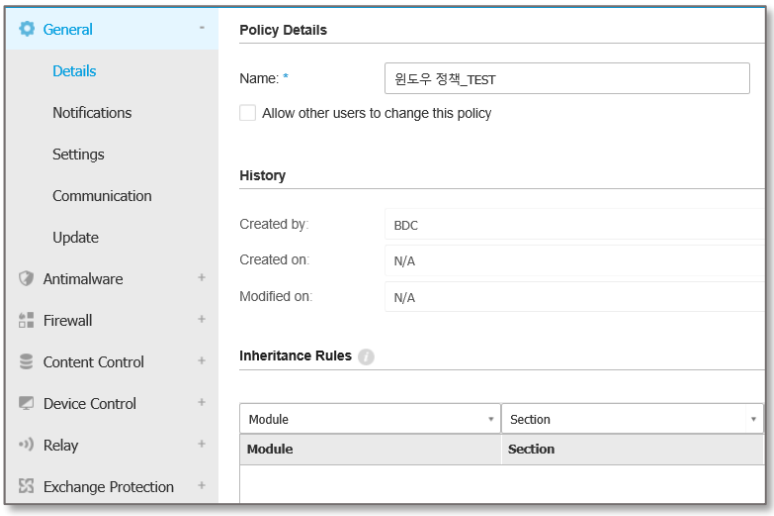
정책 생성

1. 좌측 메인 메뉴 **'Policies'** 메뉴로 이동합니다.
2. 상단 **'Add'** 항목을 클릭합니다.
3. 모든 설정이 완료되면 하단 'Save' 버튼을 클릭하여 정책을 저장합니다.
4. 'Set as default' 항목을 클릭하여 선택한 정책을 디폴트 정책으로 변경할 수 있습니다.
5. 디폴트 정책은 관리 노드 최상위 그룹에 자동으로 적용되며 그룹별 정책 부여는 'Assign policy' 를 통해 적용할 수 있습니다.



일반 > 세부 항목 설정

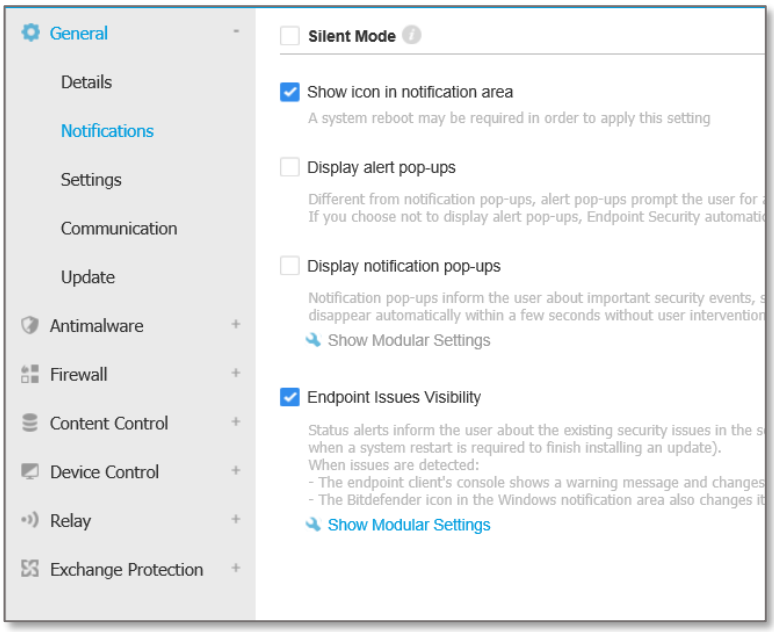
1. 'Name' 항목에 사용할 정책명을 입력합니다.
2. 다른 계정 사용자가 해당 정책을 변경하도록 허용할 경우 'Allow other users to change this policy' 항목을 체크합니다.



일반 > 알림 항목 설정

1. Silent Mode: 엔드포인트 동작이 백그라운드 상태에서 실행됩니다.

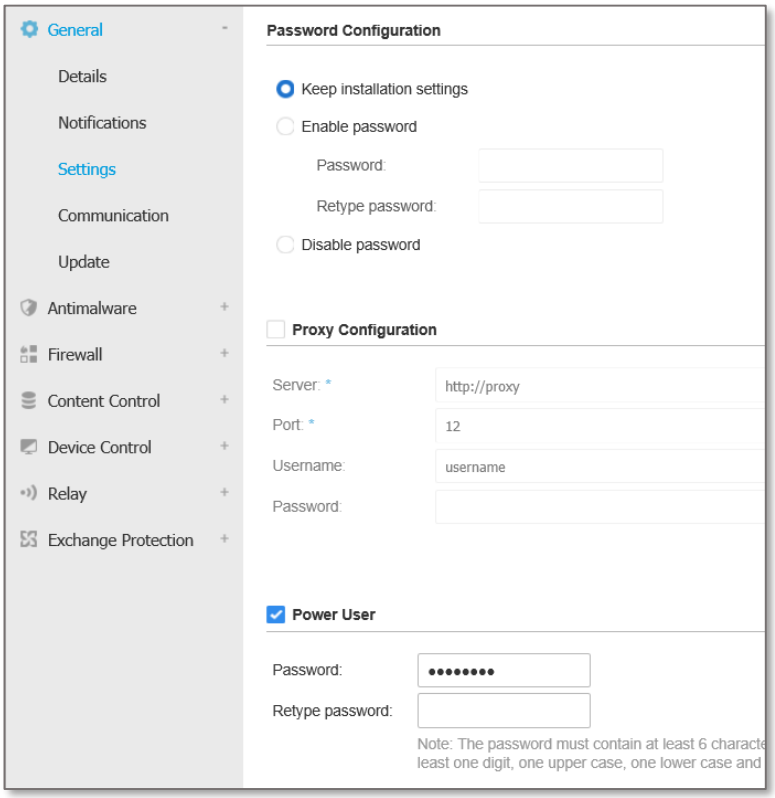
   - Show icon in notification area : 엔드포인트에 이벤트 로그를 생성합니다.
   - Display alert pop-ups : 사용자 화면에 팝업 메시지를 발생시켜 행위를 결정하도록 합니다.
   - Display notification pop-ups : 일반적인 알림 내용을 사용자 화면에 팝업 시킵니다. 항목 선택 시 'Show Modular Settings' 을 클릭하여 세부 항목을 변경할 수 있습니다.
   - Endpoint Issues Visibility : 엔드포인트 UI 상단에 표시되는 시스템 보호 수준 알림을 설정합니다. 보호 수준은 안전, 경고, 위험 3단계로 표기되며 'Show Modular Settings' 을 클릭하여 세부 항목을 변경할 수 있습니다.



일반 > 기타 설정

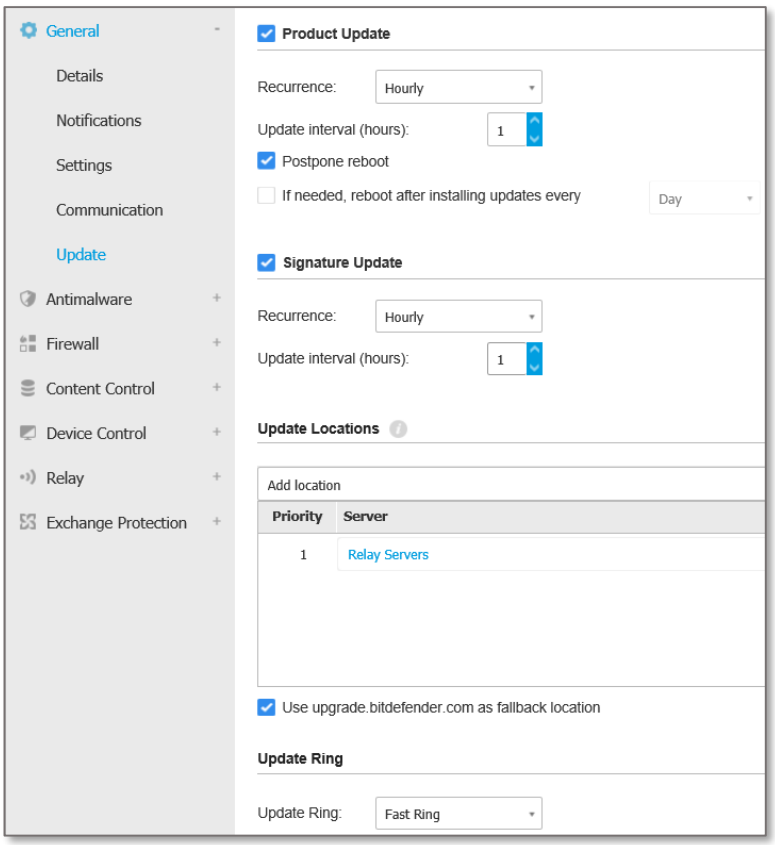
1. Password Configuration : 엔드포인트 삭제 시 패스워드 입력이 필요하도록 설정합니다.
   - Enable password : 패스워드 활성화
   - Keep installation settings : 설치본 제작 시 설정된 패스워드 유지
   - Disable password : 패스워드 사용하지 않음

2. Power User : 설치본 세부 설정에 'Power User' 모듈이 포함되어 있는 경우 'Power User' 항목을 선택 후 사용하고자 하는 패스워드를 설정합니다. 패스워드를 설정하지 않은 경우 엔드포인트의 파워유저 모드가 활성화되지 않습니다.



일반 > 업데이트 설정

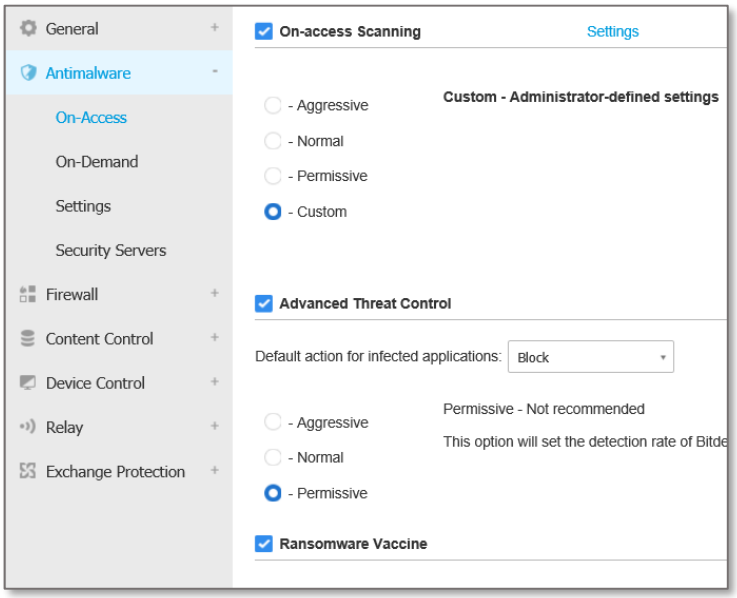
1. Product Update : 모듈 업데이트 설정
   - Recurrence : 시간, 일간, 주간 선택
   - Update interval : 업데이트 주기 설정
   - Postpone reboot : 자동 재부팅 연기
   - If needed, reboot after installing updates every : 업데이트 후 재부팅 필요시 수행 시간 설정
2. Signature Update : 패턴 및 엔진 업데이트 설정
3. Update Locations : 업데이트 서버 주소 지정
   - add location : 사용할 업데이트 서버 주소 입력
   - Use upgrade.bitdefender.com as fallback location : 업데이트 실패 시 upgrade.bitdefender.com 으로 failover 수행
4. Update Ring : 업데이트 서비스 레벨 설정
   - Fast Ring : 베타버전 서비스를 정식 업데이트 이전에 서비스 받을 수 있습니다. 오탐 확률이 높아지나 빠른 악성코드 대응이 가능합니다.
   - Slow Ring : 정식으로 업데이트된 모듈 및 패턴을 서비스 받습니다.



Security Policies

안티 멀웨어 > 실시간 감시 설정

1. 실시간 감시 레벨을 설정합니다.
   > Aggressive : 아주 높음
   > Normal : 보통
   > Permissive : 낮음
   > Custom : 사용자 설정
2. 'Settings' 를 클릭하여 사용자 임의로 감시 레벨을 설정할 수 있습니다.
3. Advanced Threat Control : 행위기반 감시 레벨 및 위협 탐지 시 수행할 행위를 설정합니다.
   > Take no action : 아무런 행위도 하지 않음
   > Block : 위협 파일 차단
   > Delete: 위협 파일 삭제
4. Ransomware Vaccine: 알려진 랜섬웨어 유형인 경우 파일 암호화 시도를 차단합니다.

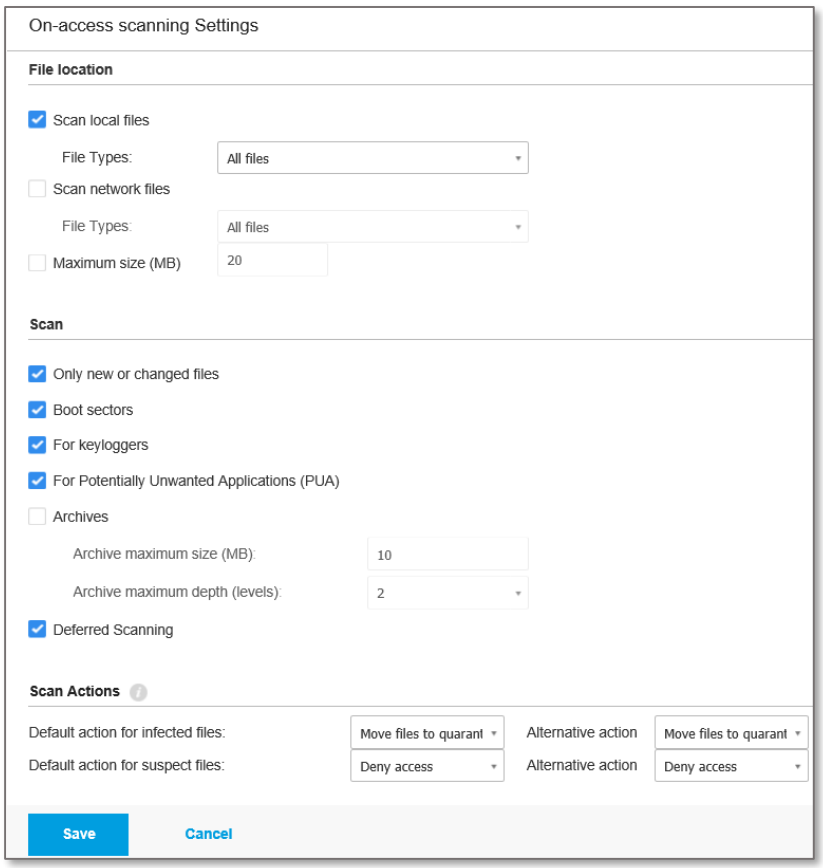


실시간 감시 레벨 사용자 설정

1. File location : 감시대상 파일 유형 설정
   > Scan local files : 로컬 드라이브
   > Scan network files : 네트워크 드라이브
   > File Types : 모든파일, 실행파일, 사용자 정의 확장자 파일 중 선택
   > Maximum size : 검사대상 파일크기 제한

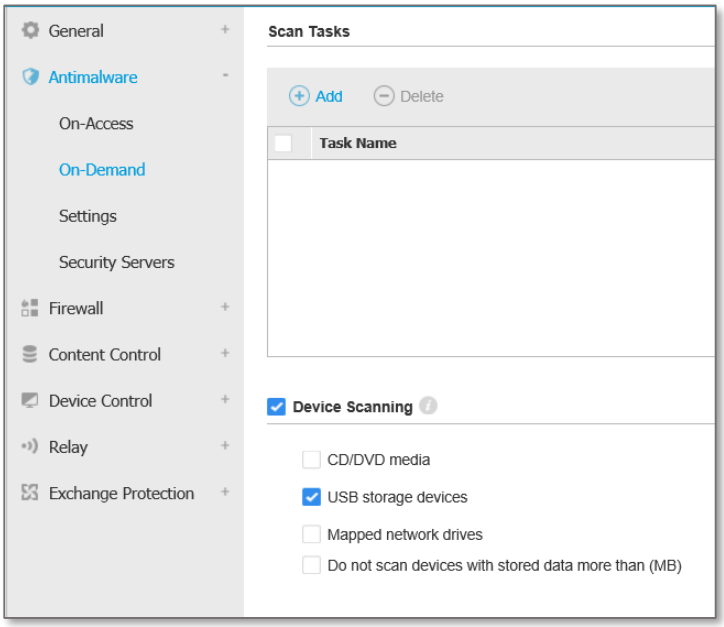
2. Scan : 감시대상 카테고리 설정
   > Only new or changed files : 새로운 파일 또는 변경된 파일만 감시
   > Boot sectors : 부트섹터 감시
   > For keyloggers : 키로거 파일 감시
   > For Potentially Unwanted Applications : 잠재적으로 위험한 어플리케이션 감시
   > Archives : 압축파일 감시
   > Deferred Scanning : 지연 검사

3. Scan Actions : 치료 행위 설정
   > Deny Access : 파일 차단
   > Disinfected : 치료
   > Delete : 삭제
   > Move to quarantine : 검역소로 이동
   > Take no action : 아무런 행위도 하지 않음



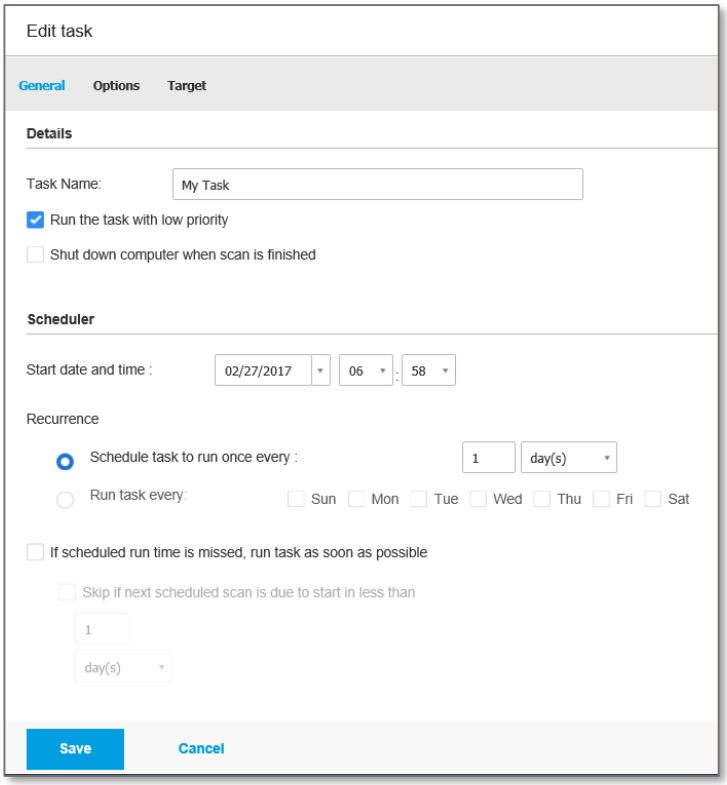
안티 멀웨어 > 예약검사 설정

1. ‘Add’ 버튼을 클릭하여 예약 검사를 등록합니다.
   > Quick Scan : 주요 파일만 검사
   > Full Scan : 모든 드라이브 검사
   > Custom Scan : 사용자 정의 검사
2. 검사대상 지정 및 옵션 변경은 ‘Custom Scan’ 선택 시 가능합니다.
3. Device Scanning : 외부저장장치 검사를 설정합니다.
   > USB Storage devices : USB 저장 장치가 인식되면 자동으로 검사를 수행합니다.
   > Mapped network drives : 네트워크 드라이브 매핑 시 자동으로 검사를 수행합니다.
   > Do not scan devices with stored data more than : 사용자가 정의한 크기 이상의 저장 장치에 대해서는 검사를 수행하지 않습니다.



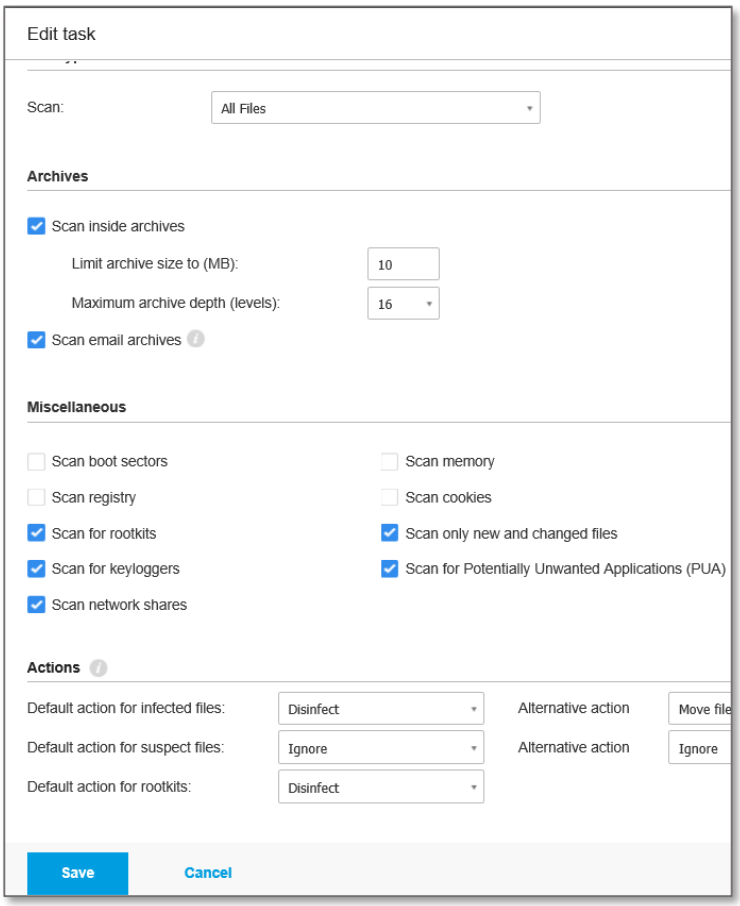
예약검사 사용자 정의 설정 - 일반

1. Task Name : 사용할 이름을 입력합니다.
   > Run the task with low priority : 낮은 CPU 우선순위로 검사를 수행합니다.
   > Shut down computer when scan is finished : 검사 완료 후 시스템을 종료합니다.
2. Scheduler : 검사 시간을 설정합니다.
   > Start date and time : 검사 시작 시간 설정
   > Recurrence : 반복 수행 설정
   > If scheduled run time is missed, run task as soon as possible : 예약 검사가 수행되지 않은 경우 가능한 가장 빠른 시간에 재검사 수행



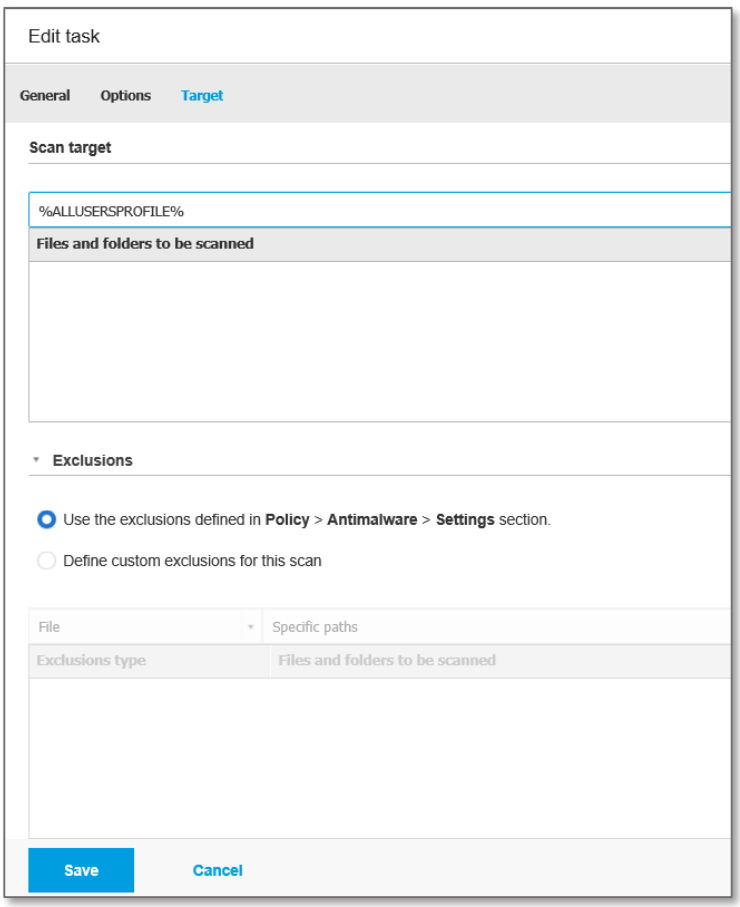
예약검사 사용자 정의 설정 – 검사 옵션

1. Scan : 검사대상 파일 유형을 선택합니다.
2. Archives : 압축파일 및 이메일 아카이브 파일 검사 여부를 선택합니다.
3. Miscellaneous : 검사대상 카테고리를 선택합니다.
4. Actions : 악성코드 처리 옵션을 설정합니다.
5. 오탐으로 인한 중요 파일 삭제 위험을 방지하기 위해 'Move to quarantine' 설정을 권고합니다.



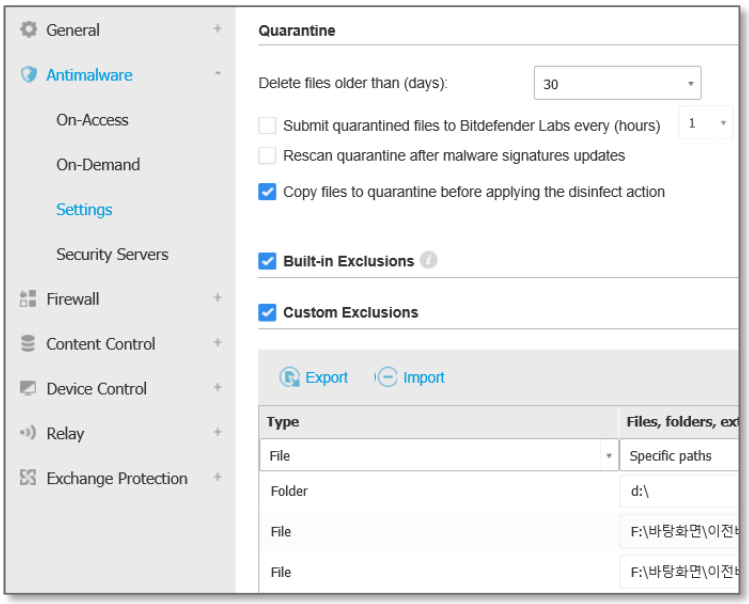
예약검사 사용자 정의 설정 – 검사 대상

1. Scan target : 검사 대상을 입력합니다. 상대경로 또는 절대경로 형식으로 입력할 수 있습니다.
2. Exclusions : 검사예외 대상을 선택합니다. 기본적으로 기존에 설정된 예외처리 목록을 불러오며, 'Define custom exclusions for this scan' 선택 시 일회성 예외처리 항목을 추가할 수 있습니다.
3. 모든 설정 완료 후 'Save' 버튼을 클릭하여 예약검사 목록을 등록할 수 있습니다.



Security Policies

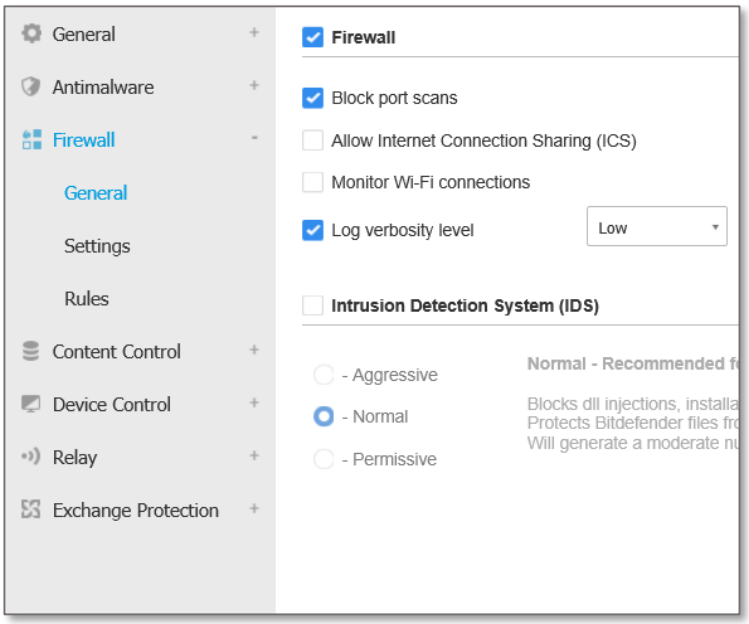
안티 멀웨어 > 일반 설정



1. Quarantine : 검역소 관련 옵션을 설정합니다.
   - Delete files older than : 설정한 값을 초과 시 검역소에 보관된 파일을 삭제합니다.
   - Copy files to quarantine before applying the disinfect action : 치료 수행 전 파일을 검역소로 복사합니다.
2. Built-in Exclusions : 기본 예외 항목을 사용합니다.
3. Custom Exclusions : 사용자 정의 예외처리 항목을 추가합니다.
   - Type: 파일, 폴더, 확장자, 프로세스 중 선택
   - Specific paths : 경로 입력
   - Modules : 실시간, 수동, 행위기반 모듈 중 선택
4. Export 메뉴를 사용하여 저장된 예외처리항목을 CSV 파일로 내보내거나 Import 메뉴를 사용하여 불러오기가 가능합니다.

중요 : 잠재적 위협으로 탐지된 파일에 대한 예외처리는 Type 항목을 'Process' , Modules 항목을 'ATC/IDS' 로 선택해야 합니다.

방화벽 > 일반 설정

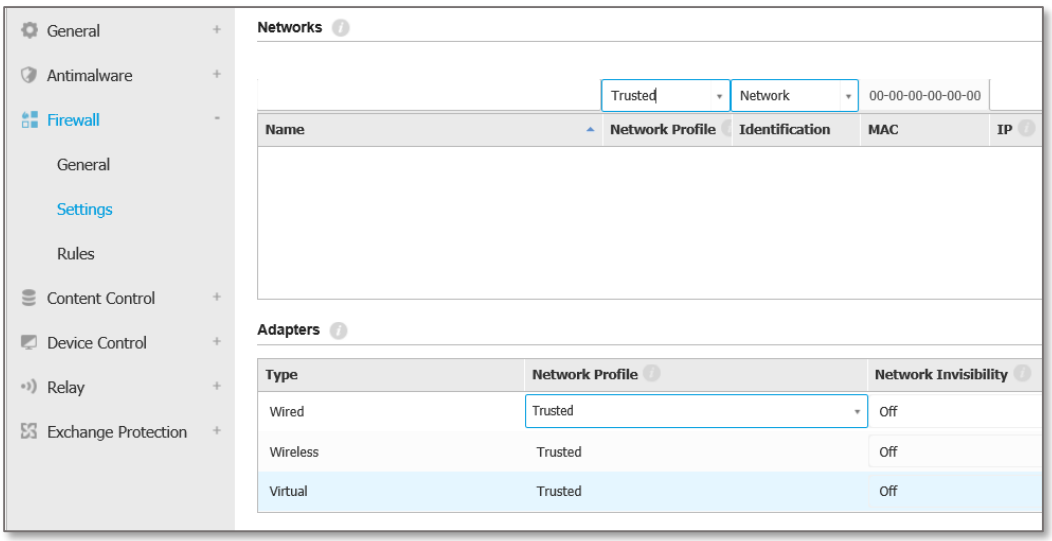


1. Firewall : 방화벽 기능을 On/Off 합니다.
   - Block port scans : 포트 스캔 차단
   - Allow Internet Connection Sharing (ICS) : 인터넷 공유 허용
   - Monitor Wi-Fi connections : Wi-Fi 연결을 감시
   - Log verbosity level : 로그 발생 레벨 설정

2. Intrusion Detection System (IDS) : 침입차단 시스템 사용을 활성화 합니다.
   - Aggressive : 인젝션, 루트킷, 키로깅 차단, 오탐 확률 높음
   - Normal : : dll 인젝션, 루트킷 차단, 오탐 확률 중간
   - Permissive : 루트킷 차단, 오탐 확률 낮음

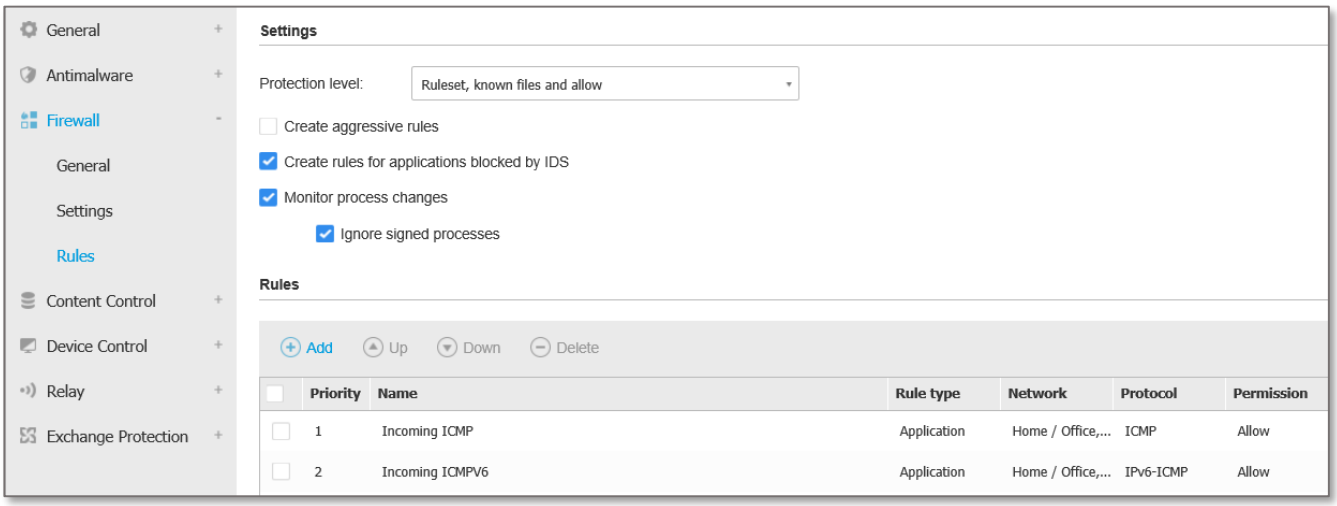
방화벽 > 기타 설정

1. Networks : 신뢰할 수 있는 네트워크 영역을 Gateway, DNS, IP 범위별로 등록할 수 있습니다.
2. Adapters : 유선, 무선, 가상화 회선별로 네트워크 프로필을 설정할 수 있습니다.
   'Network Profile' 항목은 'Trusted' , 'Network Invisibility' 항목은 'Off' 설정을 권고합니다.



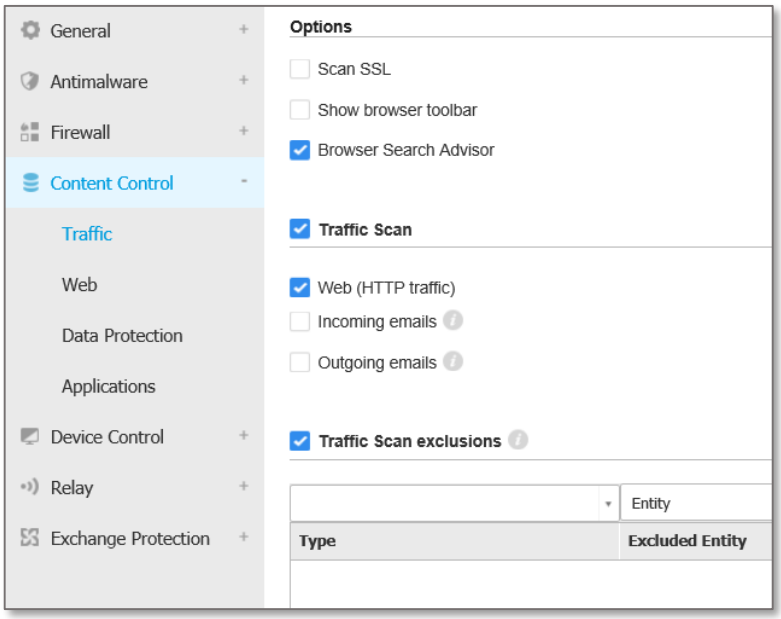
방화벽 > 규칙 설정

1. Setting : 기타 기능을 설정합니다.
   - Protection level : 차단 레벨 설정
   - Create aggressive rules : 강력한 규칙 생성
   - Create rules for applications blocked by IDS : 침입차단 시스템으로부터 차단된 어플리케이션 목록 규칙 생성
   - Monitor process changes : 프로세스 변경 감시
   - Ignore signed processes : 전자 서명된 프로세스는 프로세스 변경 감시에서 예외처리
2. Rules : 방화벽 규칙을 등록합니다. 'Add' 버튼을 클릭하여 'Application' 또는 'Connection' 별로 규칙을 등록할 수 있습니다.



컨텐츠 컨트롤 > 트래픽 설정

1. Options : 옵션 설정
   - Scan SSL : SSL 트래픽 감시
   - Show browser toolbar : 브라우저 툴바 활성화
   - Browser Search Advisor : 웹 페이지 감시
2. Traffic Scan : 트래픽 감시 설정
   - Web (HTTP traffic) : HTTP 트래픽 감시
   - Incoming emails : 수신 메일 감시
   - Outgoing emails : 발신 메일 감시
3. Traffic Scan exclusions : 트래픽 감시 예외처리
   - IP : IP를 기준으로 예외처리
   - URL : URL 기준으로 예외처리
   - Application : 어플리케이션 기준으로 예외처리

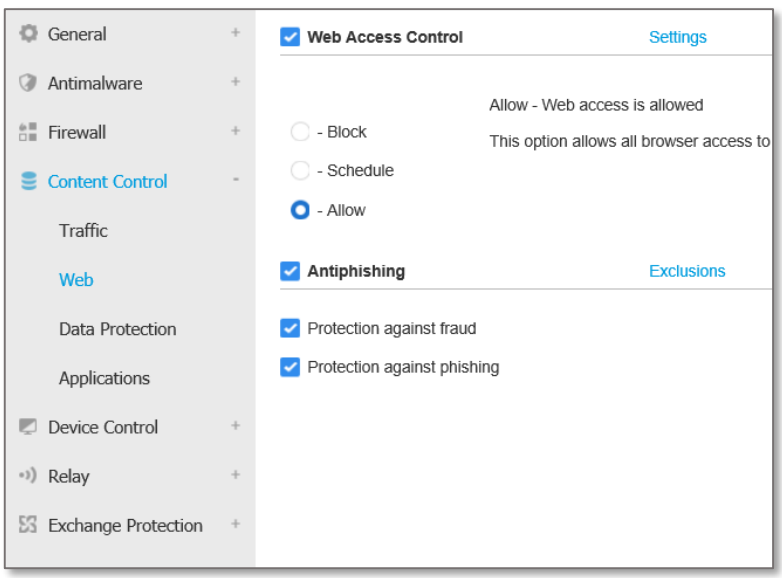


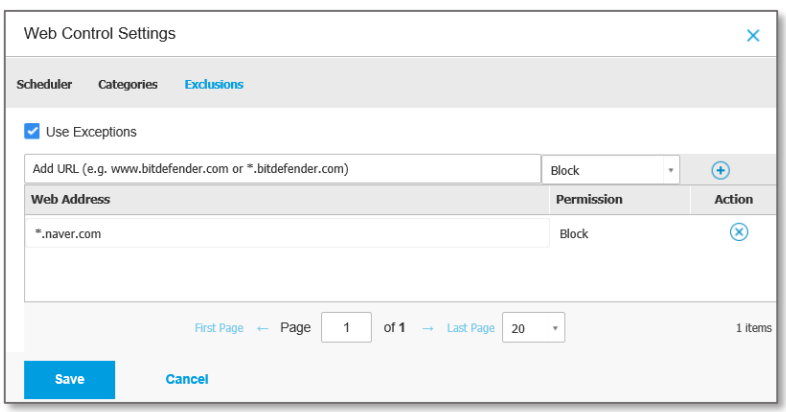
컨텐츠 컨트롤 > 웹 설정

1. Web Access Control : 차단하고자 하는 웹 사이트 URL 기반으로 등록할 수 있습니다.

2. ‘Settings’ 을 클릭하여 상세 설정을 등록합니다.
   - Scheduler : 시간별 차단 설정
   - Categories : 카테고리 목록별 차단 설정
   - Exclusions : 차단 사이트 등록 및 예외처리

3. Antiphishing : 위협을 발생시킬 수 있는 웹 사이트를 차단합니다.
   - Protection against fraud : 사기 사이트 차단
   - Protection against phishing : 피싱 사이트 차단



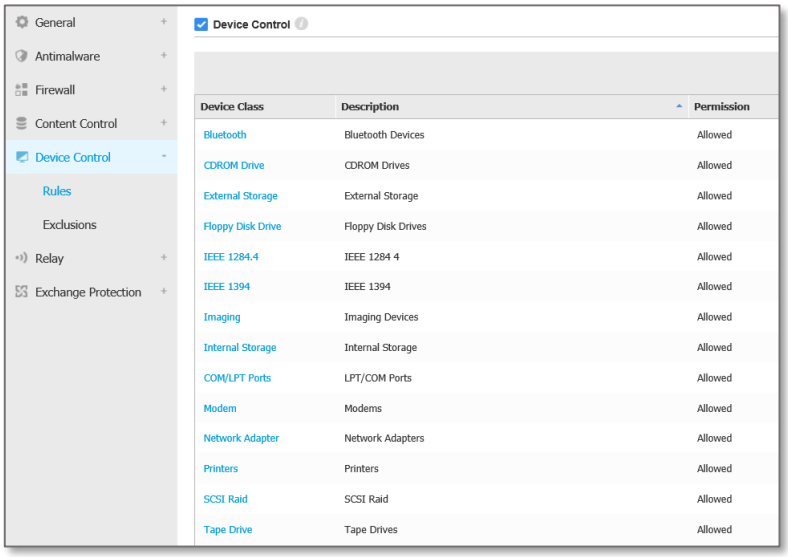


매체 제어 설정

1. Device Control : 매체 제어 기능을 On/Off 합니다.

2. ‘External Storage’ 를 클릭하여 외부 저장 장치인 USB 메모리, 외장 HDD 등의 장치를 입출력 포트로 구분하여 차단 설정이 가능합니다.

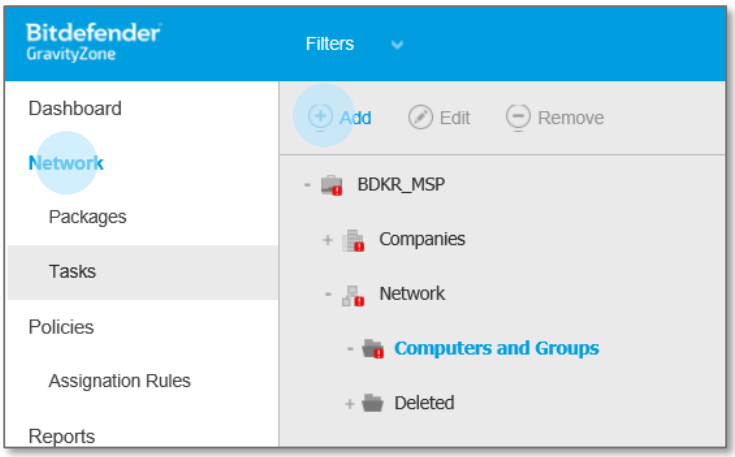
3. ‘Network Adapter’ 를 클릭하여 스마트폰 USB 테더링 기능을 통한 인터넷 접근을 차단할 수 있습니다.

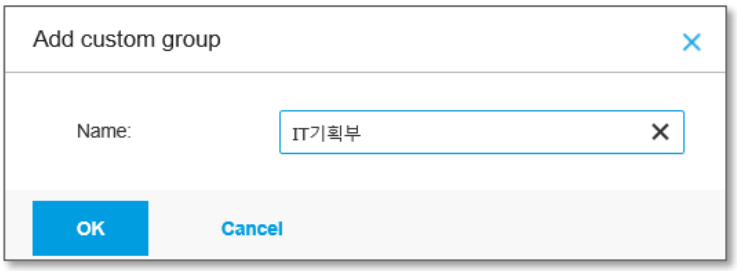


네트워크 노드 관리하기

그룹 추가 및 생성

1. 좌측 메인 메뉴 **'Network'** 메뉴로 이동합니다.
2. 상단 **'Add'** 항목을 클릭합니다.
3. 그룹명을 입력하여 그룹을 생성 및 추가합니다.





관리 노드 이동

1. 좌측 메인 메뉴 **'Network'** 메뉴로 이동합니다.
2. 이동을 원하는 노드를 선택 후 마우스 드래그 앤 드롭으로 좌측 그룹 폴더로 이동시킬 수 있습니다.
3. 다수의 노드를 선택하면 한번에 원하는 그룹으로 이동시킬 수 있습니다.