비밀번호를 잊은 경우 AMP 커넥터 제거 절차

목차

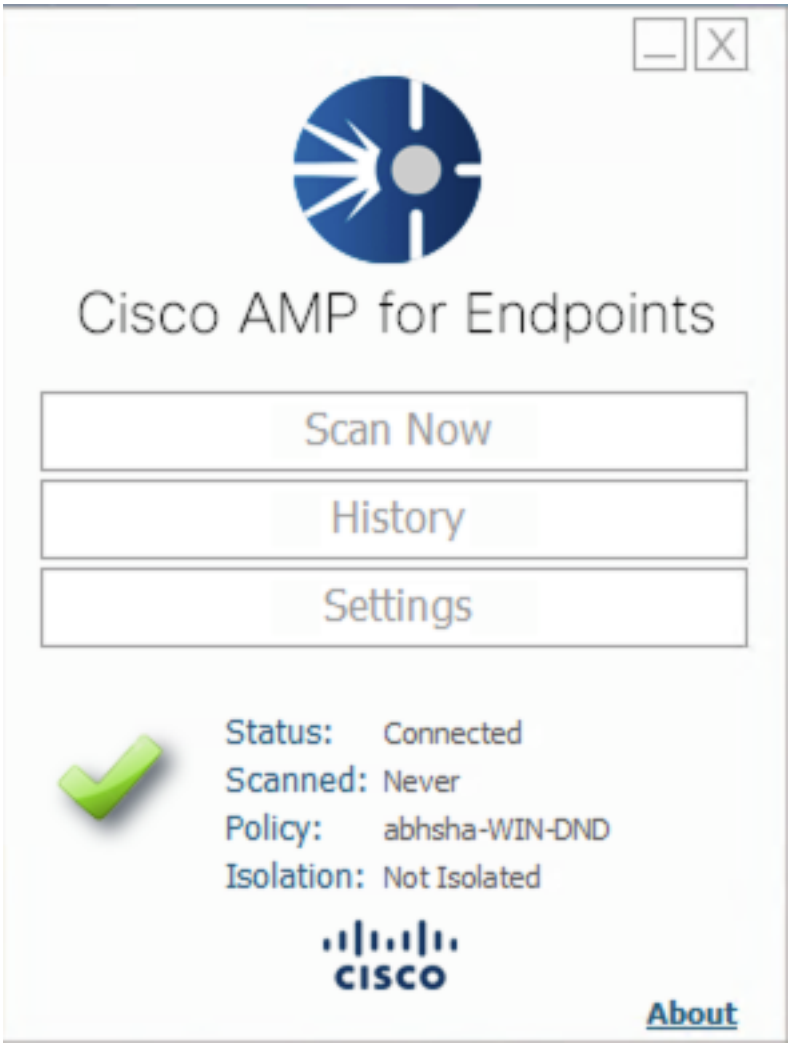
소개

이 문서에서는 비밀번호를 제공해야 하는 커넥터 보호 기능에 의해 제거가 차단되고 비밀번호가 잊혀질 경우 Cisco AMP(Advanced Malware Protection) 커넥터를 제거하기 위한 절차에 대해 설명합니다.이 경우에는 2가지 시나리오가 있으며, 커넥터에서 AMP 클라우드에 "Connected(연결됨)"를 표시하는지에 따라 달라집니다.커넥터 보호는 Windows OS에서만 사용할 수 있는 기능이므로 Windows OS에만 적용됩니다.

커넥터가 연결됨

1단계. 트레이 아이콘을 클릭하고 Cisco AMP for Endpoints Connector를 엽니다.

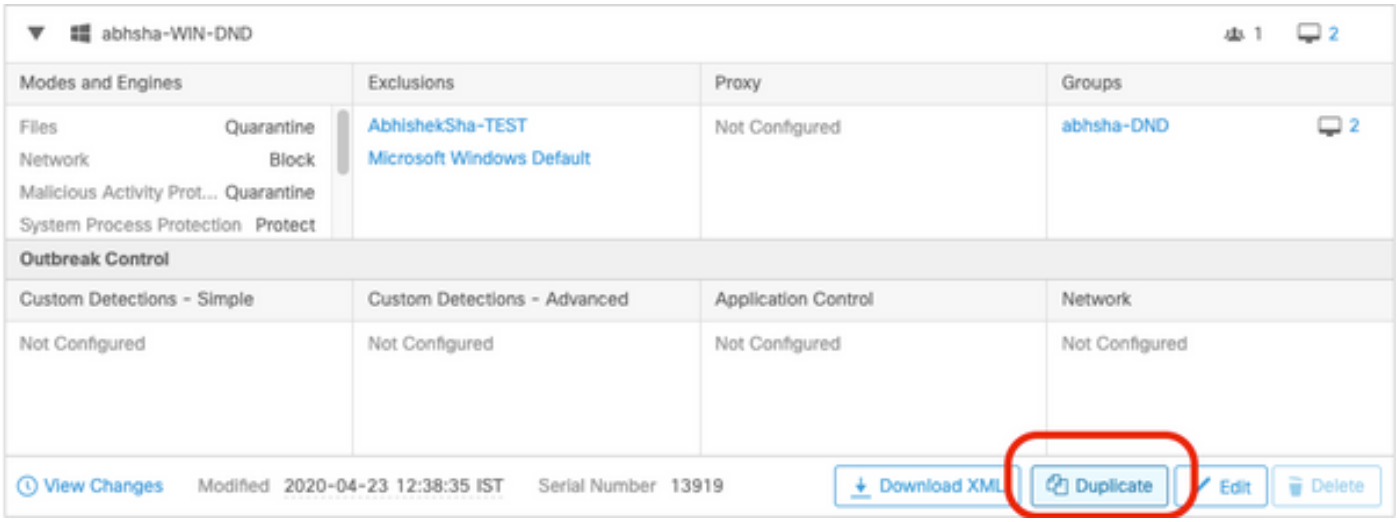
2단계. 커넥터가 연결된 것으로 표시되는지 확인합니다.



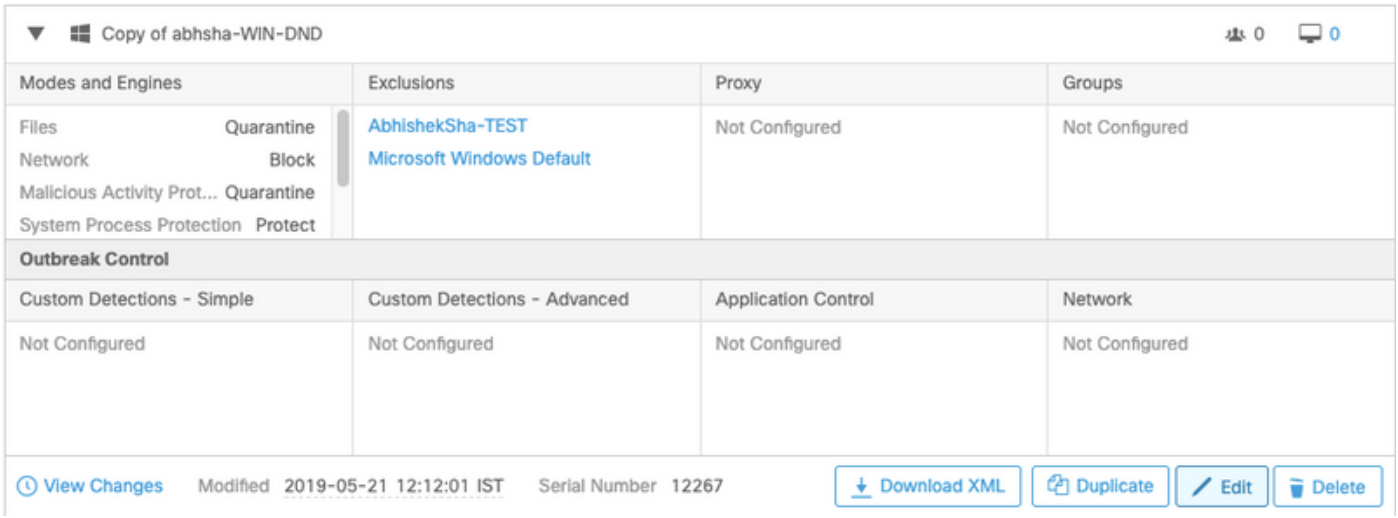
3단계. 정책이 해당 커넥터에 할당되었습니다.

4단계. AMP for Endpoints Console로 이동하여 이전에 기록된 정책을 검색합니다.

5단계. 정책을 확장하고 이미지에 표시된 대로 **Duplicate**를 클릭합니다.

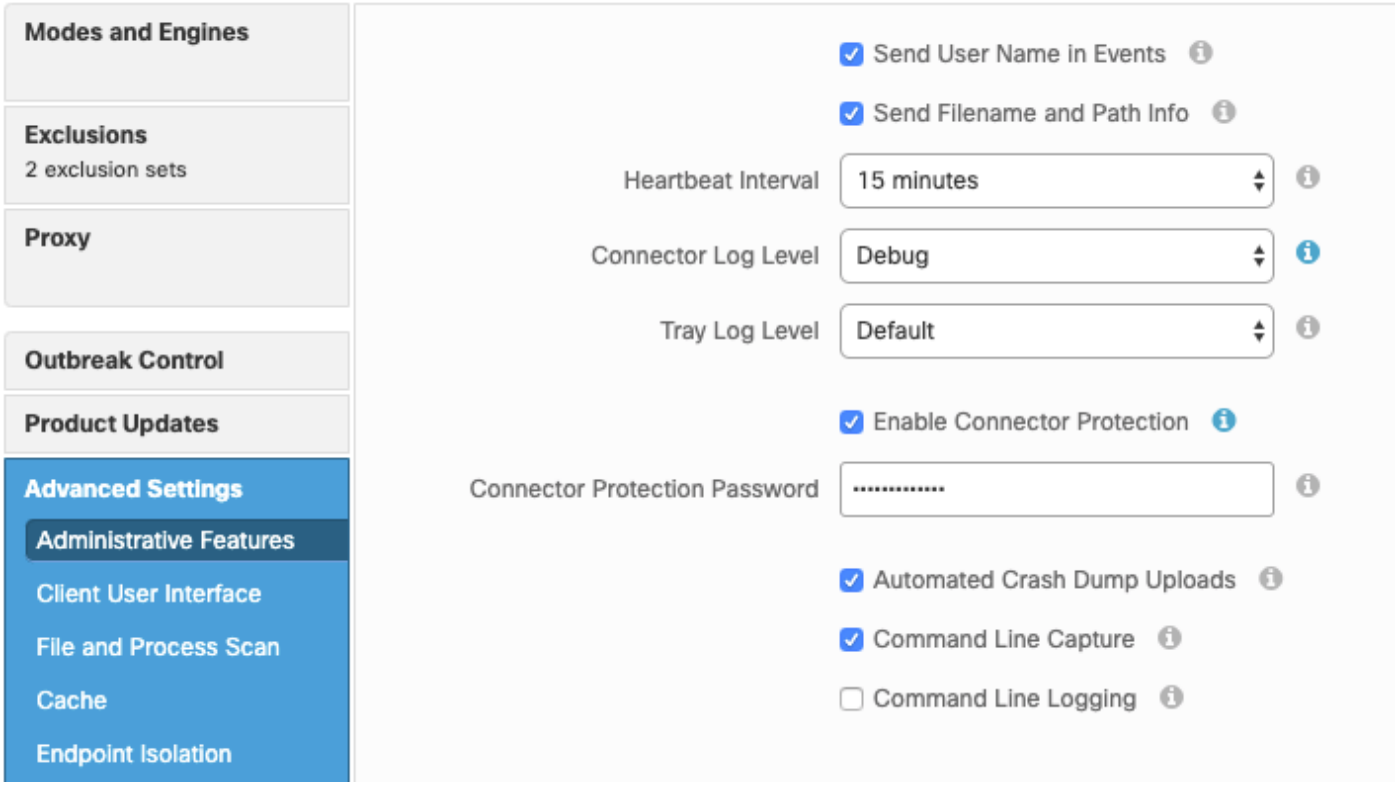


6단계. "Copy of.."라는 새로운 정책 생성됩니다.이미지에 표시된 대로 이 정책을 수정하려면 **Edit**를 클릭합니다.



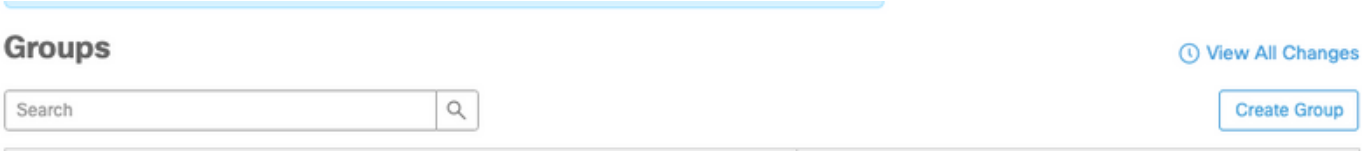
7단계. Edit Policy(**정책 수정**) 페이지에서 Advanced Settings(고급 설정) **> Administrative Features(관리 기능)로 이동합니다.**

8단계. **Connector Password Protection**(커넥터 비밀번호 보호) 필드에서 비밀번호를 이미지에 표시된 대로 회수할 수 있는 새 비밀번호로 교체합니다.

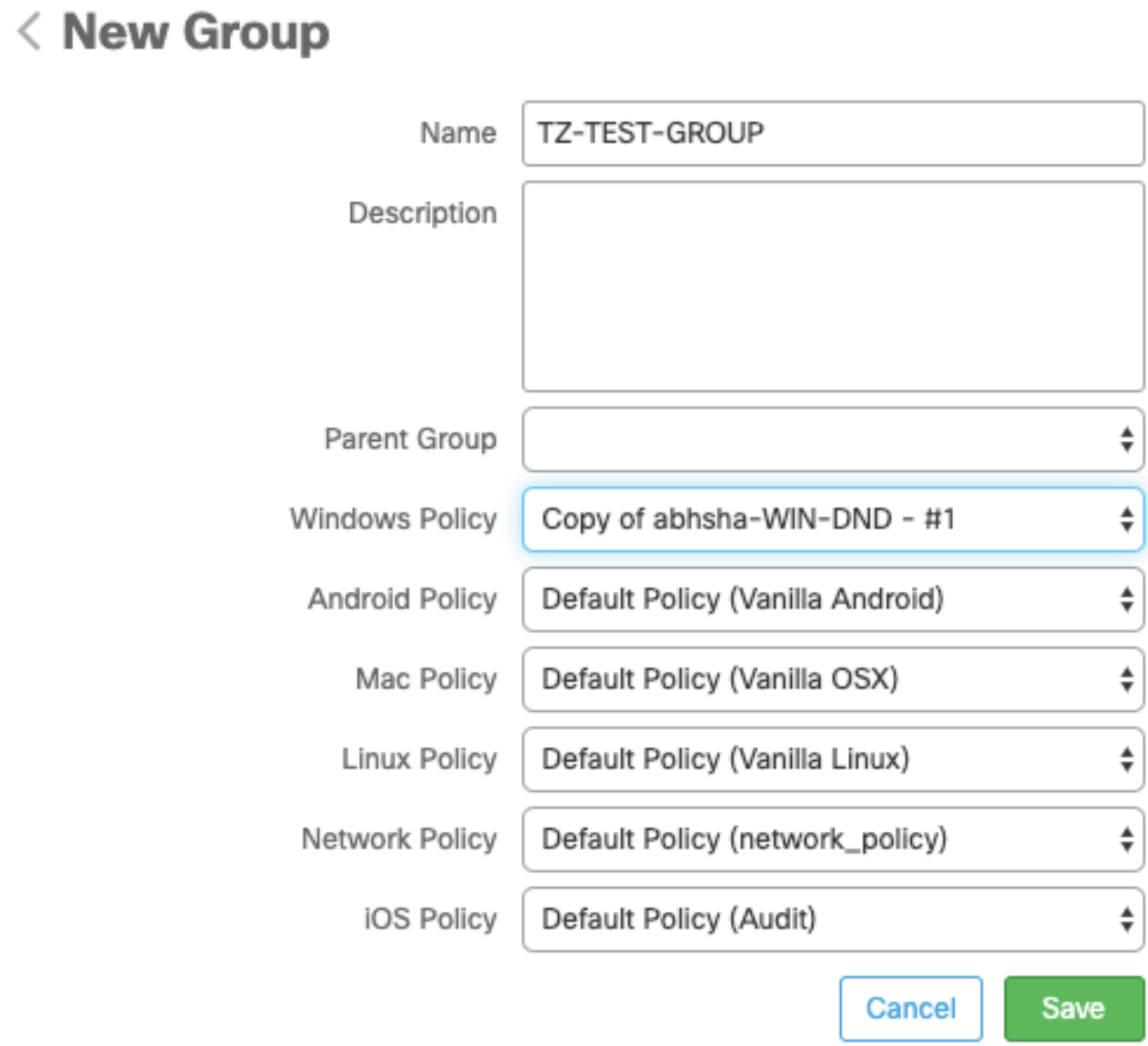


9단계. 이 정책을 저장하려면 **Save**(저장) 버튼을 클릭합니다.

10단계. **관리 > 그룹**으로 이동하고 새 그룹을 생성합니다.

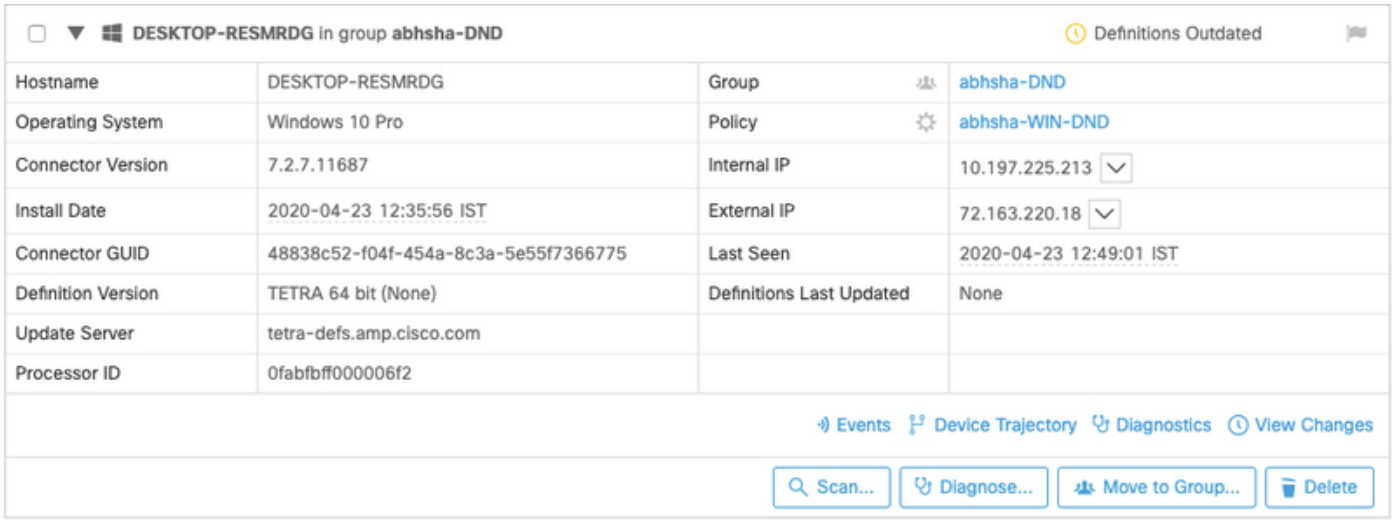


11단계. 그룹 이름을 입력하고 **Windows 정책을** 이전에 편집한 정책으로 선택합니다.이미지에 표시된 대로 **저장** 단추를 클릭합니다.



12단계. **Management(관리)** > Computers(컴퓨터)로 이동하여 AMP 커넥터를 제거하려고 하는 컴퓨터를 검색합니다.

13단계. 컴퓨터를 확장하고 **그룹으로 이동**을 클릭합니다.나타나는 대화 상자에서 이전에 만든 그룹을 선택합니다.



14단계. 엔드포인트에서 정책이 업데이트될 때까지 기다립니다.보통 30분에서 1시간 정도 소요되며 구성된 간격에 따라 달라집니다.

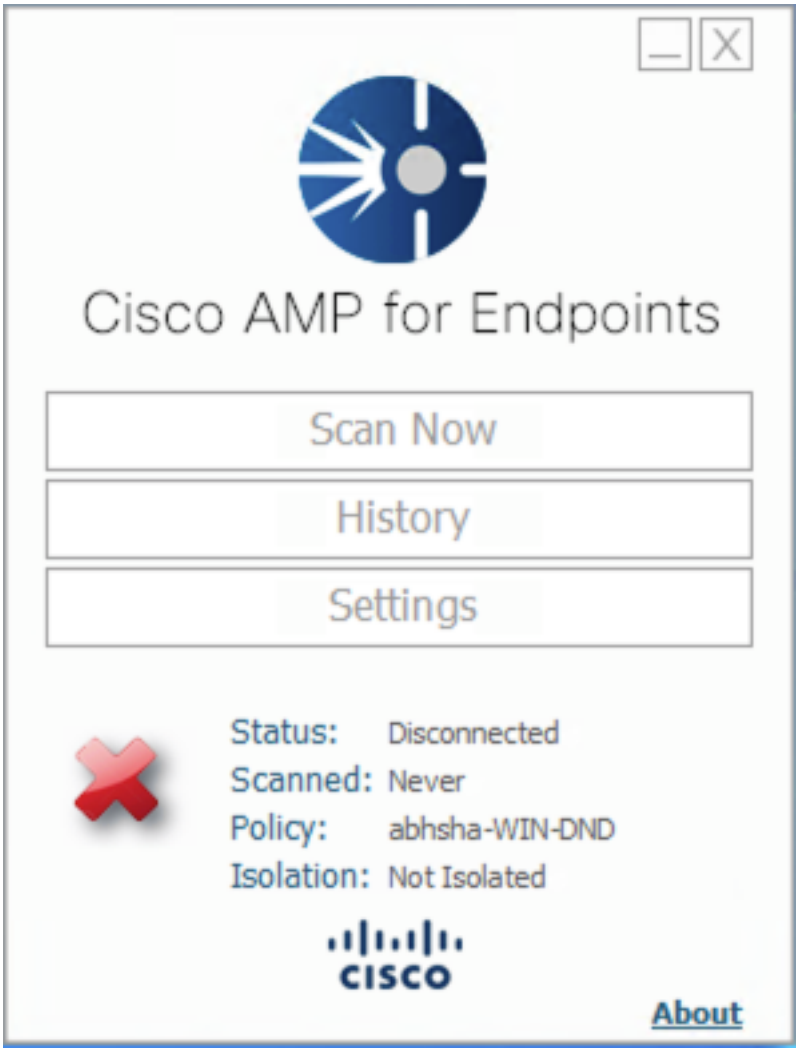
15단계. 엔드포인트에서 정책이 업데이트되면 새로 구성한 비밀번호를 사용하여 커넥터를 제거할 수 있습니다.

커넥터의 연결이 끊어졌습니다.

커넥터가 AMP 클라우드에서 분리되어 있으면 안전 모드에서 컴퓨터를 부팅할 수 있어야 합니다.

1단계. 트레이 아이콘을 클릭하고 Cisco AMP for Endpoints Connector를 엽니다.

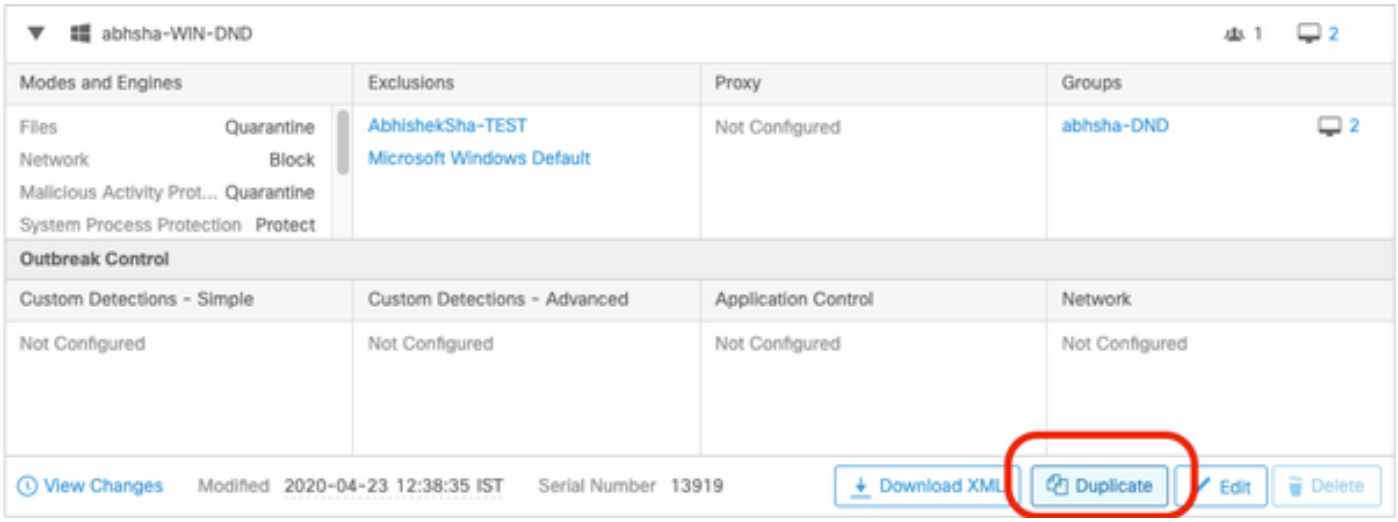
2단계. 커넥터가 연결 해제된 것으로 표시되는지 확인합니다.



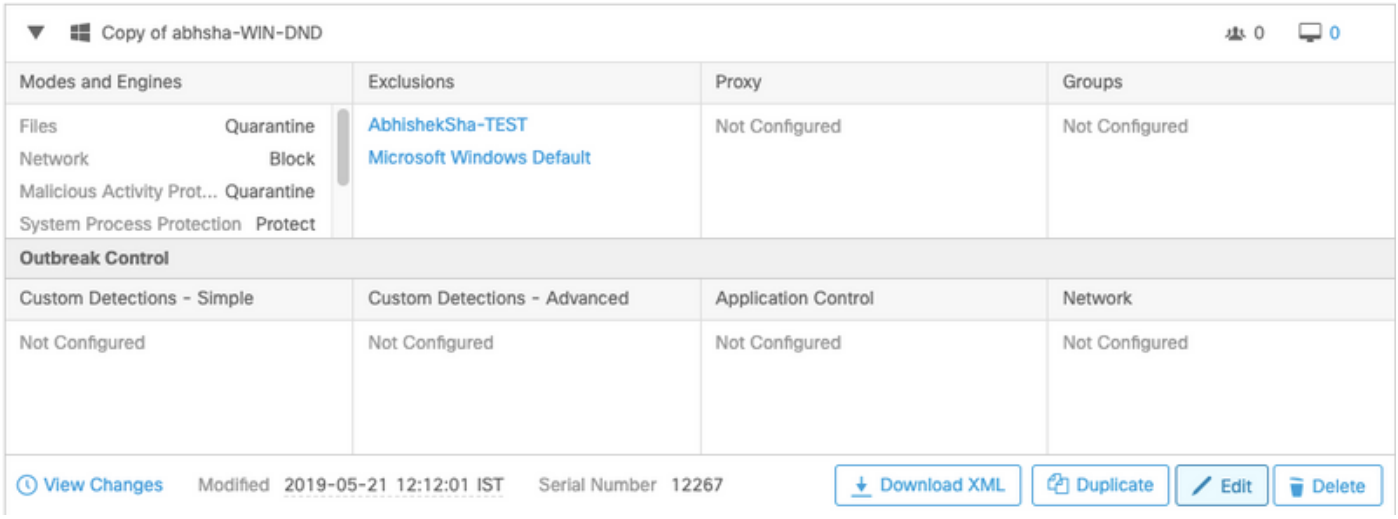
3단계. 해당 커넥터에 할당된 정책을 확인합니다.

4단계. AMP for Endpoints Console로 이동하여 이전에 기록된 정책을 검색합니다.

5단계. 정책을 확장하고 이미지에 표시된 대로 **Duplicate**를 클릭합니다.

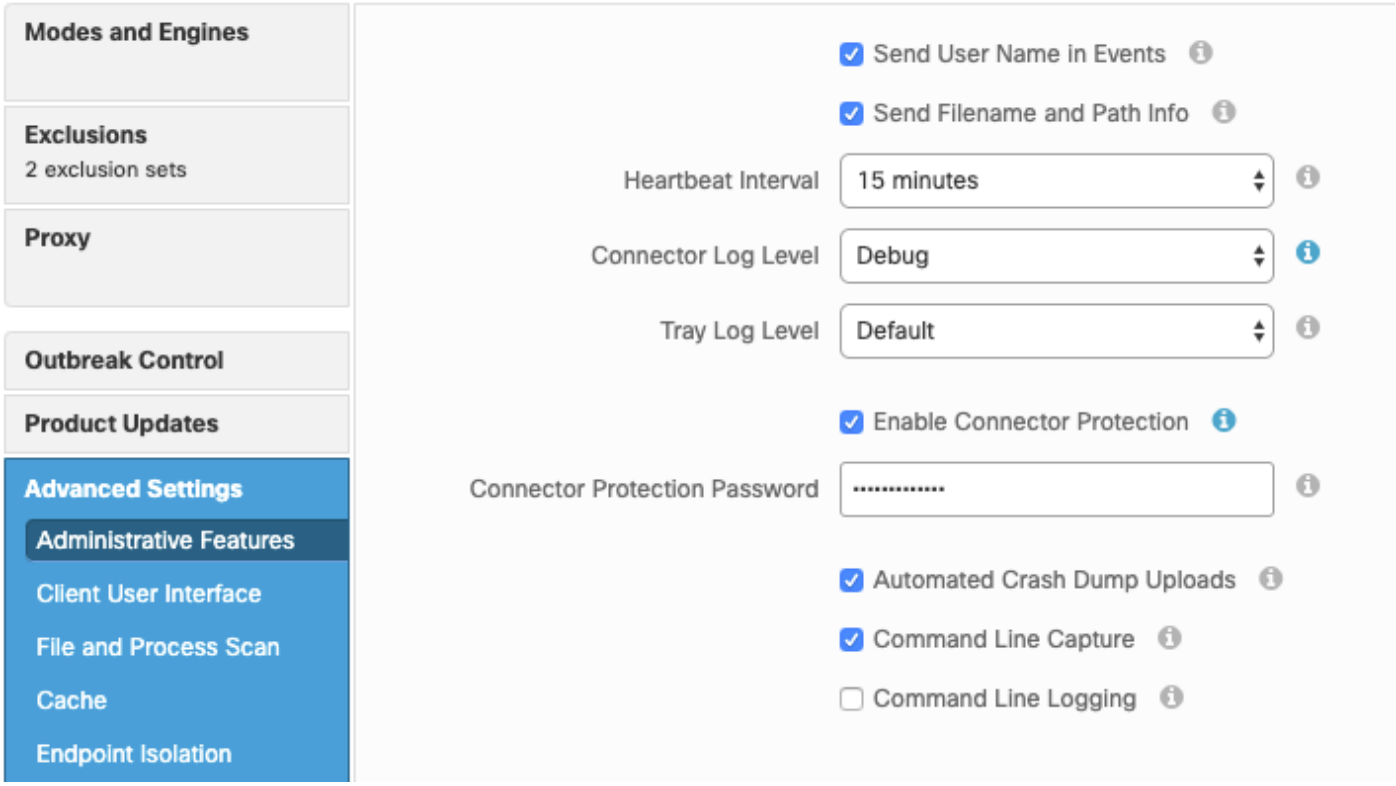


6단계. "Copy of.."라는 새로운 정책 생성됩니다.이 정책을 수정하려면 **Edit**를 클릭합니다.



7단계. Edit Policy(정책 수정) 페이지에서 **Advanced Settings(고급 설정) > Administrative Features(관리 기능)로 이동합니다**.

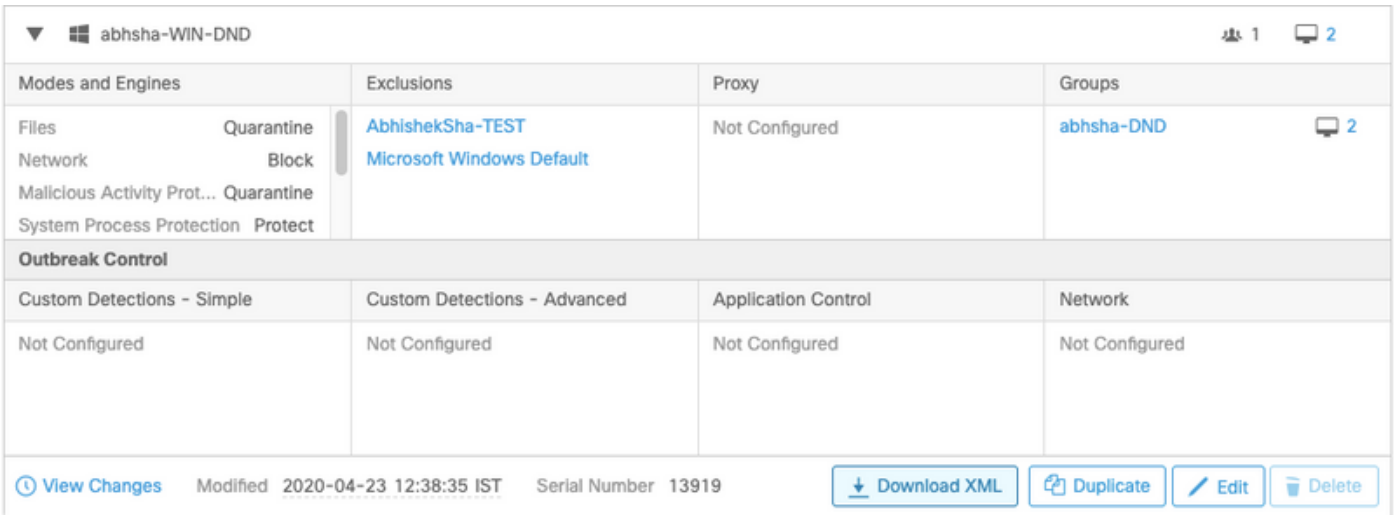
8단계. Connector **Password Protection(커넥터 비밀번호 보호)** 필드에서 비밀번호를 회수할 수 있는 새 비밀번호로 교체합니다.



9단계. 이 정책을 저장하려면 **Save**(저장) 버튼을 클릭합니다.

10단계. **Management(관리) > Policies(정책)**로 이동하고 새로 복제된 정책을 검색합니다.

11단계. 정책을 확장하고 **XML 다운로드**를 클릭합니다. **policy.xml**이라는 파일이 시스템에 저장됩니다.

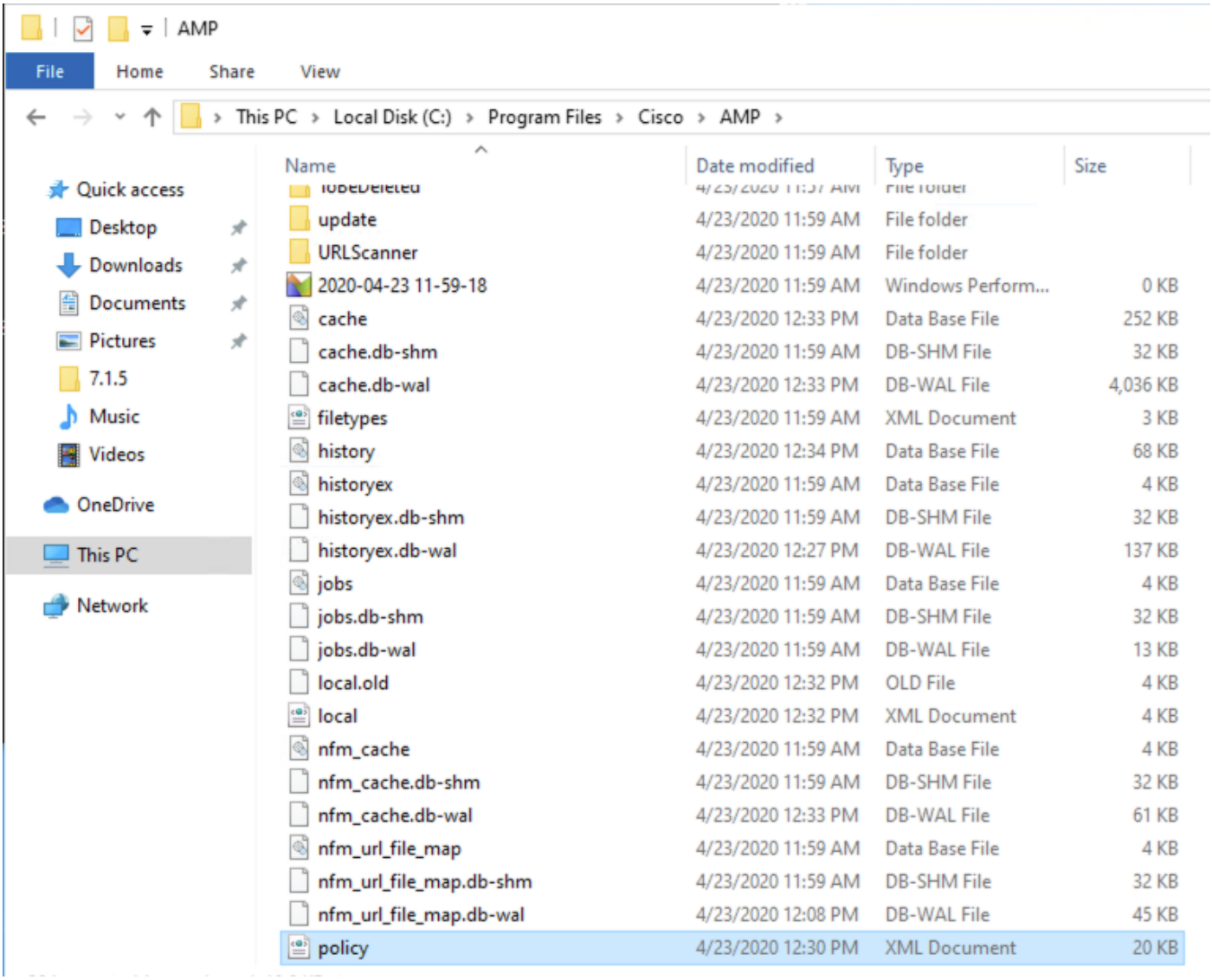


12단계. 이 **policy.xml을** 영향받는 엔드포인트에 복사합니다.

13단계. **안전 모드**에서 영향을 받는 엔드포인트를 **재부팅합니다**.

14단계. 영향을 받는 엔드포인트가 **안전 모드**에 **있으면 C:\Program Files\Cisco\AMP**으로 **이동합니다**.

15단계. 이 폴더에서 **policy.xml**이라는 파일을 검색하고 이 이름을 policy_**old.xml로 바꿉니다**.



16단계. 이제 이전에 복사한 **policy.xml을** 이 폴더에 붙여넣습니다.

17단계. 파일을 복사한 후 제거를 정상적으로 수행할 수 있으며 비밀번호 프롬프트에 새로 구성된 비밀번호를 입력해야 합니다.

18단계. 이 단계는 선택 사항입니다.컴퓨터의 연결이 끊어질 때 커넥터가 제거되었으므로 컴퓨터 항목이 콘솔에 남아 있습니다.따라서 **Management(관리) > Computers(컴퓨터)로 이동하여** 영향을 받는 엔드포인트를 확장할 수 있습니다.엔드포인트**를** 삭제하려면 Delete를 클릭합니다.