



## IPSec 정책 관리

---

- [IPsec 정책 개요, 1 페이지](#)
- [IPsec 정책 구성, 2 페이지](#)
- [IPsec 인증서 확인, 2 페이지](#)
- [IPsec 정책 관리, 3 페이지](#)

### IPsec 정책 개요

IPsec은 암호화 보안 서비스를 사용하여 IP 네트워크를 통해 개인 보안 통신을 보장하는 프레임워크입니다. IPsec 정책은 IPsec 보안 서비스를 구성하는 데 사용됩니다. 정책은 네트워크에서 대부분의 트래픽 유형을 위해 다양한 수준의 보호를 제공합니다. 컴퓨터, OU(조직 단위), 도메인, 사이트 또는 글로벌 엔터프라이즈의 보안 요구 사항을 충족하도록 IPsec 정책을 구성할 수 있습니다.

## IPSec 정책 구성



참고

- 시스템 업그레이드 중 IPSec 정책에 적용되는 변경 사항은 손실되므로 업그레이드하는 동안 IPSec 정책을 수정 또는 생성하지 마십시오.
- IPSec은 양방향 프로비저닝 또는 각 호스트(또는 게이트웨이)에 대해 하나의 피어가 필요합니다.
- 한 IPSec 정책 프로토콜이 “ANY”로 설정되고 다른 IPSec 정책 프로토콜이 “UDP” 또는 “TCP”로 설정된 두 Unified Communications Manager 노드에서 IPSec 정책을 프로비저닝할 때 “ANY” 프로토콜을 사용하는 노드에서 실행할 경우 유효성 검사 결과는 거짓 부정이 될 수 있습니다.
- 특히 암호화를 사용하면 IPSec은 시스템 성능에 영향을 미칩니다.
- IPSec 정책이 현재 또는 업그레이드된 버전에 구성되어 있지만 기본 버전에 구성되어 있지 않은 경우 이 버전을 기본 버전으로 전환할 때 IPSec 정책을 삭제하거나 비활성화해야 합니다. 이는 IPSec 정책이 노드 중 하나에서만 구성되고 다른 노드에서는 이 두 버전을 모두 전환할 때까지 IPSec 정책이 구성되지 않기 때문입니다. 그렇지 않으면 연결 문제가 발생할 수 있습니다.
- Unified CM 노드를 재부팅한 후 IPSec 연결이 작동하지 않으면 명령 **utils ipsec restart**를 사용하여 IPSec 서비스를 다시 시작하여 IPSec 연결을 성공적으로 설정해야 합니다. 이 해결 방법은 네트워크 연결을 설정하기 전에 IPSec 서비스 다시 시작과 관련된 문제를 완화하는 것입니다.

프로시저

- 단계 1 Cisco Unified OS 관리에서 보안 > **IPSec** 구성을 선택합니다.
- 단계 2 새로 추가를 클릭합니다.
- 단계 3 **IPSec** 정책 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
- 단계 4 저장을 클릭합니다.
- 단계 5 (선택 사항) IPSec를 확인하려면 서비스 > **Ping**을 선택하고 **IPSec** 확인 확인란을 선택한 다음 **Ping**을 클릭합니다.

## IPSec 인증서 확인

다음 절차에 따라 IPSec 인증서를 확인합니다.

## 프로시저

단계 1 Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 2 검색 기준을 지정하고 찾기를 클릭합니다.

단계 3 IPsec 인증서를 검색합니다(게시자 및 가입자 노드에 개별적으로 로그인).

참고 일반적으로 게시자 노드에서는 가입자 노드 IPsec 인증서를 볼 수 없습니다. 그러나 게시자 노드 IPsec 인증서는 IM&P 노드의 가입자 노드에서 볼 수 있습니다.

IPsec 연결을 활성화하려면 한 노드의 CA 서명 IPsec 인증서를 다른 노드에서 IPsec-신뢰 인증서로 사용해야 합니다.

새 인증서를 IPsec-신뢰로 업로드하기 전에 IPsec-신뢰에서 동일한 일반 이름을 가진 이전 인증서를 제거해야 합니다.

## IPsec 정책 관리

시스템 업그레이드 중 IPsec 정책에 적용되는 변경 사항은 손실되므로 업그레이드하는 동안 IPsec 정책을 수정 또는 생성하지 마십시오.



주의 인증서 이름, 도메인 또는 IP 주소 변경으로 인해 기존 IPsec 인증서가 변경되면 IPsec 정책을 삭제하고 다시 생성해야 합니다. 인증서 이름이 변경되지 않은 경우 원격 노드의 재생성된 인증서를 가져온 후 IPsec 정책을 비활성화하고 활성화해야 합니다.

## 프로시저

단계 1 Cisco Unified OS 관리에서 보안 > IPSEC 구성을 선택합니다.

단계 2 정책을 표시, 활성화 또는 비활성화하려면 다음 단계를 수행합니다.

- a) 정책 이름을 클릭합니다.
- b) 정책을 활성화 또는 비활성화하려면 정책 활성화 확인란을 선택하거나 선택 취소합니다.
- c) 저장을 클릭합니다.
- d) 정책을 비활성화하는 경우에는 **utils ipsec restart** 명령을 실행하여 변경 비활성화를 적용해야 합니다.

단계 3 하나 이상의 정책을 삭제하려면 다음 단계를 수행합니다.

- a) 삭제할 각 정책 옆의 확인란을 선택합니다.

모든 정책을 선택하려면 모두 선택을 클릭하고, 모든 확인란을 지우려면 모두 지우기를 클릭하면 됩니다.

b) 선택한 항목 삭제를 클릭합니다.

---

## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.