컴플라이언스 목록

다음 주제에서는 상관관계 정책에 추가하기 전에 규정준수 허용리스트를 설정하는 방법을 설명합니다.

컴플라이언스 허용 목록 소개

줄여서 허용 목록이라고도 하는 컴플라이언스 허용 목록은 네트워크의 호스트에서 허용할 운영체제, 애플리케이션(웹 및 클라이언트)을 지정하는 기준 모음입니다. 호스트가 이 목록에 없으면 시스템은 이벤트(위반)를 생성합니다.

컴플라이언스 허용 목록은 다음과 같은 두 가지 주요 구성 요소로 이루어집니다.

- 대상은 컴플라이언스 평가를 위해 선택한 호스트입니다. 모니터링되는 전체 또는 일부 호스트를 서브넷, VLAN 및 호스트 속성으로 제한해 평가할 수 있습니다. 다중 도메인 구축의 경우에는 도메인과 도메인 내부 또는 사이에 있는 서브켓을 지정할 수 있습니다.
- 호스트 프로파일은 대상의 규정준수 기준을 지정합니다. 전역 호스트 프로파일은 운영체제의 구속을 받지 않습니다. 하나의 허용 목록에 국한되거나 여러 허용 목록이 공유하는 운영체제별 호스트 프로파일을 설정할 수도 있습니다.

Talos 인텔리전스 그룹은(는) 권장 설정을 적용한 기본 허용 목록을 제공합니다. 맞춤형 허용 목록을 만들 수도 있습니다. 단순 맞춤형 목록은 특정 운영체제를 실행하는 호스트만 허용할 수 있습니다. 더 복잡한 목록은 모든 운영체제를 허용할 수 있지만, 특정 포트에서 특정 애플리케이션 프로토콜을 실행하기 위해 호스트가 사용해야 하는 운영체제를 지정합니다.

참고 시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.이러한 제한은 컴플라이언스 허용 목록을 작성하는 방법에 영향을 미칠 수 있습니다.

컴플라이언스 허용 목록 구현

허용 목록을 구현하려면 해당 목록을 활성 상관관계 정책에 추가해야 합니다. 시스템은 대상을 평가하고 모든 호스트를 대응하는 속성에 할당합니다.

- 규정준수 - 호스트가 해당 목록을 위반하지 않습니다.
- 규정 미준수 - 호스트가 해당 목록을 위반합니다.
- 미평가 - 호스트가 해당 목록의 대상이 아니거나, 호스트가 현재 평가 중이거나, 정보가 부족해 시스템이 호스트의 규정준수 여부를 판단할 수 없습니다.

참고 호스트 속성을 삭제하려면 해당 허용 목록을 삭제해야 합니다. 상관관계 정책에서 허용 목록을 비활성화, 삭제 또는 제거하더라도 호스트 속성은 삭제되지 않으며, 각 호스트에 대한 속성의 값도 변경되지 않습니다.

최초 평가가 끝나면 시스템은 모니터링되는 호스트가 활성 허용 목록에 대한 규정준수에서 벗어날 때마다 허용 목록 이벤트를 생성하며, 허용 목록 위반을 기록합니다.

워크플로우, 대시보드, 네트워크 맵을 이용해 시스템 전반의 규정준수 활동을 모니터링하여 개별 호스트가 허용 목록을 언제 어떻게 위반하는지 확인할 수 있습니다. 그러한 위반에 대해 교정과 알림으로 자동 응답할 수도 있습니다.

예: **HTTP**를 웹 서버에 제한

보안 정책이 웹 서버만 HTTP를 실행하도록 규정합니다. 웹 팜을 제외한 전체 네트워크를 평가하는 허용 목록을 생성하여 어떤 호스트가 HTTP를 실행 중인지 확인합니다.

네트워크 맵과 대시보그를 사용하여, 네트워크 규정준수 상태를 한 눈에 확인할 수 있습니다. 조직 내의 어떤 호스트가 정책을 위반한 상태로 HTTP를 실행 중인지 단 몇 초 만에 정확히 확인하고, 적절한 조치를 취할 수 있습니다.

그런 다음 상관관계 기능을 사용하면 웹 팜에 없는 호스트가 HTTP 실행을 시작할 때마다 사용자에게 알림이 전송되도록 시스템을 구성할 수 있습니다.

관련 항목

상관관계 정책 설정

컴플라이언스 허용 목록 대상 네트워크

대상 네트워크는 규정준수에 대해 평가할 호스트를 지정합니다. 허용리스트는 하나 이상의 대상 네트워크를 가질 수 있으며, 대상 기준을 충족하는 호스트를 평가합니다.

처음에는 대상 네트워크를 IP 주소 또는 범위로 제한합니다. 다중 도메인 구축의 경우, 최초 제한에는 도메인도 포함됩니다.

시스템이 제공하는 기본 허용리스트는 모니터링되는 모든 호스트, 즉 0.0.0.0/0과 ::/0을 지정합니다. 다중 도메인 구축의 경우, 기본 허용리스트는 전역 도메인으로 제한됩니다. 그리고 전역 도메인에서만 사용할 수 있습니다.

대상 네트워크나 호스트를 수정하여 호스트가 허용리스트의 유효한 대상이 되지 않게 하면 호스트는 해당 리스트로 평가되지 않으며 규정준수 또는 미준수로 간주되지 않습니다.

대상 네트워크 조사 및 개선

대상 네트워크를 허용리스트를 추가하는 경우, 시스템은 규정준수 호스트를 특성화할 수 있도록 네트워크 맵을 조사하라는 프롬프트를 표시합니다. 조사를 통해 조사 대상인 호스트를 나타내는 대상이 허용리스트에 추가됩니다.

서브넷 또는 개별 호스트를 조사할 수 있습니다. 다중 도메인 구축의 경우에는 전체 도메인을 조사하거나 여러 도메인에 걸쳐 조사를 진행할 수 있습니다. 상위 도메인을 조사하면 시스템은 해당 도메인의 하위 요소를 조사합니다.

추가한 대상 외에, 조사에서 탐지된 각 운영체제에 대해 하나의 호스트 프로파일과 허용리스트도 채웁니다. 이러한 호스트 프로파일은 해당 운영체제에서 탐지된 모든 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 허용합니다.

대상 네트워크 조사가 끝나면(또는 조사를 건너뛰면), 대상을 개선합니다. 호스트를 IP 주소를 기준으로 제외하거나, 대상 네트워크를 호스트 속성이나 VLAN을 기준으로 제한할 수 있습니다.

규정준수 허용리스트를 이용한 도메인 지정

다중 도메인 구축의 경우, 도메인과 대상 네트워크는 밀접하게 연결됩니다.

- 리프 도메인 관리자는 자신의 리프 도메인 내에서 호스트를 평가하는 허용리스트를 만들 수 있습니다.
- 상위 도메인 관리자가 도메인에 걸쳐 호스트를 평가하는 허용리스트를 생성할 수 있습니다. 동일한 허용 목록에서 다른 도메인에 있는 다른 서브넷을 대상으로 지정할 수 있습니다.

자신이 Global(전역) 도메인 관리자이며, 전체 구축의 웹 서버에 같은 규정준수 기준을 적용하는 상황을 고려해보십시오. 규정준수 기준을 정의하는 허용리스트를 전역 도메인에서 생성합니다. 그런 다음 각 리프 도메인에 있는 웹 서버의 IP 공간(또는 개별 IP 주소)을 지정하는 대상 네트워크를 이용하여 허용리스트를 제한합니다.

참고 리프 도메인의 IP 주소와 범위를 대상으로 지정할 수도 있지만, 상위 도메인을 이용해 대상 네트워크를 제한할 수도 있습니다. 상위 도메인에 있는 서브넷을 대상으로 지정하면 각 하위 리프 도메인의 같은 서브넷이 대상으로 지정됩니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

컴플라이언스 허용 목록 호스트 프로필

컴플라이언스 허용 목록에서 호스트 프로파일은 대상 호스트에서 실행할 수 있는 운영체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 지정합니다. 컴플라이언스 허용 목록에서는 3가지 유형의 호스트 프로파일을 사용할 수 있습니다. 각 유형은 규정준수 편집기에서 다르게 표시됩니다.

표 *1:* 컴플라이언스 허용 목록 호스트 프로파일 유형

호스트 프로파일 유형	모양	설명
전역글로벌	모든 운영체제	운영체제에 상관없이 대상 호스트에서 실행할 수 있는 요소를 지정
운영체제 한정	일반 텍스트로 나열됨	특정 운영체제의 대상 호스트에서 실행할 수 있는 요소를 지정
공유됨	기울임꼴로 나열	여러 허용 리스트에서 사용할 수 있는 운영체제 기준을 지정

운영 체제별 호스트 프로파일

규정준수 허용 목록에서 운영체제 한정 호스트 프로파일은 네트워크에서 실행할 수 있는 운영체제뿐만 아니라, 해당 운영체제에서 실행할 수 있는 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜을 나타냅니다.

예를 들어 규정준수 호스트가 특정 버전의 Microsoft Windows를 실행하도록 요구할 수 있습니다. 다른 예로, SSH가 포트 22의 Linux 호스트에서 실행되도록 허용하고 SSH 클라이언트의 벤더와 버전을 추가로 제한할 수 있습니다.

네트워크에서 허용하려는 각 운영체제에 대한 하나의 호스트 프로파일을 생성합니다. 네트워크에서 특정 운영체제를 허용하지 않으려면, 해당 운영체제에 대한 호스트 프로파일을 생성하지 마십시오. 예를 들어 네트워크의 모든 호스트가 Windows를 실행하게 하려면, 허용 목록에 해당 운영체제에 대한 호스트 프로파일만 포함되도록 구성하십시오.

참고 확인되지 않은 호스트는 확인될 때까지 모든 허용 목록을 준수하는 상태로 유지됩니다. 그러나 알 수 없는 호스트에 대한 허용 목록 호스트 프로파일을 생성할 수 있습니다. *Unidentified(*미확인*)* 호스트는 시스템이 해당 호스트의 운영체제를 식별하기 위한 충분한 정보를 아직 수집하지 못한 호스트입니다. *Unknown(*알 수 없는*)* 호스트는 운영체제가 알려진 핑거프린트와 일치하지 않는 호스트입니다.

공유 호스트 프로파일

규정준수 허용리스트에서 공유 호스트 프로파일은 특정 운영체제에 연결되지만, 각 공유 호스트 프로파일을 두 개 이상의 허용리스트에서 사용할 수 있습니다.

예를 들어, 전 세계에 지사가 있고 각 위치에 별도의 허용리스트를 적용하지만, Apple Mac OS X를 실행하는 모든 호스트에 동일한 프로파일을 사용하려면 해당 운영체제에 대한 공유 프로파일을 생성하고 이를 모든 허용리스트에 사용할 수 있습니다.

기본 허용리스트는 내장형 호스트 프로파일이라고 하는 특수 카테고리의 공유 호스트 프로파일을 사용합니다. 이러한 프로파일은 내장된 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜 및 클라이언트를 사용합니다. 규정준수 허용리스트 편집기에서 시스템은 이러한 프로파일에 내장 호스트 프로파일 아이콘을 표시합니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 공유 호스트 프로파일을 표시하며, 이러한 규칙은 편집할 수 있습니다. 상위 도메인의 공유 호스트 프로파일도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 공유 호스트 프로파일을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 공유 호스트 프로파일(내장된 프로파일 포함)을 수정하거나 내장된 애플리케이션 프로토콜, 프로토콜 또는 클라이언트를 수정하는 경우, 변경사항은 이를 사용하는 모든 허용리스트에 영향을 미칩니다. 의도하지 않은 변경사항을 적용하거나 내장된 요소를 삭제했다면, 공장 기본값으로 재설정할 수 있습니다.

허용 위반 트리거

호스트의 허용리스트 규정준수는 시스템이 다음 작업을 할 때 변경할 수 있습니다.

- 호스트 운영체제의 변경 사항을 탐지한 경우
- 호스트의 운영체제 또는 호스트에 있는 애플리케이션 프로토콜의 ID 충돌을 탐지한 경우
- 호스트에서 새 TCP 서버 포트(예: SMTP 또는 웹 서버에서 사용된 포트)가 활성화되었거나, 호스트에서 새 UDP 서버가 실행 중인 것을 탐지한 경우
- 호스트에서 실행 중인 것으로 검색된 TCP 또는 UDP 서버의 변경 사항을 탐지한 경우(예: 업그레이드로 인한 버전 변경)
- 호스트를 실행하는 새 클라이언트나 웹 애플리케이션을 탐지한 경우

- 비활성 상태인 클라이언트나 웹 애플리케이션을 데이터베이스에서 삭제하는 경우
- 새 네트워크 또는 전송 프로토콜과 통신하는 호스트를 탐지한 경우
- 새 탈옥 모바일 디바이스를 탐지한 경우
- 시스템에서 종료되거나 시간 초과된 TCP 또는 UDP 포트를 탐지한 경우

이와 더불어, 호스트 입력 기능 또는 호스트 프로파일을 사용하여 호스트의 규정준수 변경을 트리거할 수 있습니다.

- 호스트에 클라이언트, 프로토콜 또는 서버 추가
- 호스트에서 클라이언트, 프로토콜 또는 서버 삭제
- 호스트의 운영체제 정의 설정
- 해당 호스트가 더 이상 유효 대상이 되지 않도록 호스트의 호스트 속성 변경

참고 이벤트 과잉을 방지하기 위해, 시스템은 최초 평가 시에는 규정 미준수 호스트에 대한 허용리스트 이벤트를 생성하지 않으며, 활성 허용리스트 또는 공유 호스트 프로파일을 수정해도 호스트는 규정 미준수가 되지 않습니다. 그러나 위반 사항은 계속 기록됩니다. 모든 규정 미준수 대상에 대한 허용리스트 이벤트를 생성하려면 검색 데이터를 비웁니다. 네트워크 자산을 재검색하면 허용리스트 이벤트가 트리거될 수도 있습니다.

운영체제 규정준수

네트워크에서 Microsoft Windows 호스트만 허용하도록 허용리스트를 지정할 경우, 시스템에서는 Mac OS X를 실행하는 호스트를 탐지하며 허용리스트 이벤트를 생성합니다. 또한 허용리스트와 연결된 호스트 속성은 해당 호스트에 대해 Compliant(규정준수)에서 Non-Compliant(규정 미준수)로 변경됩니다.

이 예시에 나온 호스트의 상태가 규정준수로 돌아가려면 다음 중 하나를 수행해야 합니다.

- Mac OS X 운영체제를 허용하도록 허용리스트 편집
- 호스트의 운영체제 정의를 Microsoft Windows로 수동으로 변경
- 운영체제가 Microsoft Windows로 다시 변경된 사실을 시스템에서 탐지함

네트워크 맵에서 규정 미준수 자산 삭제

허용리스트에서 FTP 사용이 허용되지 않고 사용자가 애플리케이션 프로토콜 네트워크 맵 또는 이벤트 보기에서 FTP를 삭제할 경우, FTP를 실행하는 호스트는 규정준수를 상태가 됩니다. 그러나 애플리케이션 프로토콜이 다시 탐지될 경우, 시스템에서는 허용리스트 이벤트를 생성하며 호스트는 규정준수 위반 상태가 됩니다.

완전한 정보에서만 트리거

허용리스트가 포트 21의 TCP FTP 트래픽만 허용하며 시스템이 포트 21/TCP에서의 불확정 활동을 탐지하면 허용리스트는 트리거하지 않습니다. 허용리스트는 시스템이 트래픽을 FTP가 아닌 다른 무언가로 식별하거나, 사용자가 호스트 입력 기능을 이용하여 트래픽을 비 FTP 트래픽으로 지정하는 경우에만 트리거합니다. 시스템은 부분적인 정보만 있는 위반은 기록하지 않습니다.

컴플라이언스 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모두

사용자 역할

- 관리자

컴플라이언스 허용 목록 생성

규정준수 허용 목록을 생성하는 경우, 시스템은 최초 대상을 생성하고 규정준수 호스트 속성을 설명할 수 있도록 네트워크를 조사하라는 프롬프트를 표시합니다.

프로시저

단계 **1** 허용 목록을 선택하고 **Policies(**정책**)** > **Correlation(**상관관계**)**를 클릭합니다.

단계 **2** 새로 만들기허용 목록를 클릭합니다.

단계 **3** 선택적으로, 최초 대상 네트워크의 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**를 입력합니다. 다중 도메인 구축인 경우에는 대상 네트워크가 상주하는 **Domain(**도메인**)**을 선택합니다.

팁 전체 모니터링된 네트워크를 조사하려면, 기본값 0.0.0.0/0 및 ::/0을 사용합니다.

참고 대상 네트워크의 도메인은 선택이 끝나면 변경할 수 없습니다. 상위 도메인에 있는 서브넷을 대상으로 지정하면 각 하위 리프 도메인의 같은 서브넷이 대상으로 지정됩니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **4** 대상 네트워크 추가:

- Add(추가) - 조사하지 않고 대상 네트워크를 추가하려면 **Add(**추가**)**를 클릭합니다.
- Add and Survey Network(추가 및 네트워크 조사) - 대상 네트워크를 추가하고 조사하려면 **Add and Survey Network(**네트워크 추가 및 조사**)**를 클릭합니다.
- Skip(건너뛰기) - 네트워크를 조사하지 않고 허용 목록을 생성하려면 **Skip(**건너뛰기**)**을 클릭합니다.

단계 **5** 선택적으로, 허용 목록의 새 **Name(**이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **6** 선택적으로, 네트워크에서 탈옥 모바일 디바이스를 허용합니다. 이 옵션을 비활성화하면 탈옥한 디바이스가 허용 목록 위반을 생성할 수 있습니다.

단계 **7** 규정준수 허용 목록에 대한 대상 네트워크 설정, 9 페이지에 설명된 대로 하나 이상의 **Target Network(**대상 네트워크**)**를 허용 목록에 추가합니다.

단계 **8** **Allowed Host Profiles(**허용되는 호스트 프로파일**)**을 이용해 규정준수 호스트의 특성 설명:

- Global Host Profile(전역 호스트 프로파일) - 허용 목록의 전역 호스트 프로파일을 편집하려면 **Any Operating System(**모든 운영체제**)**을 클릭하고 허용 리스트 호스트 프로필 빌드, 10 페이지에 설명된 대로 진행합니다.
- Edit Surveyed Profiles(조사한 프로파일 편집) - 네트워크 조사로 생성한 기존 운영체제 한정 호스트 프로파일을 편집하려면, 해당 프로파일의 이름을 클릭하고 허용 리스트 호스트 프로필 빌드, 10 페이지에 설명된 대로 진행합니다.
- Create New Profiles(새 프로파일 생성) - 이 허용 목록에 대한 새로운 운영체제 한정 호스트 프로파일을 생성하려면, **Allowed Host Profiles(**허용되는 호스트 프로파일**)** 옆에 있는 **Add(**추가**)** (+)을 클릭하고 허용 리스트 호스트 프로필 빌드, 10 페이지에 설명된 대로 진행합니다.
- Add Shared Host Profile(공유 호스트 프로파일 추가) - 기존 공유 호스트 프로파일을 허용 목록에 추가하려면, **Add Shared Host Profile(**공유 호스트 프로파일 추가**)**을 클릭하고 추가할 공유 호스트 프로파일을 선택한 다음 **OK(**확인**)**를 클릭합니다. 공유 호스트 프로파일은 기울임꼴로 표시됩니다.

단계 **9** **Save(**저장**)**허용 목록를 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 설정에 설명된 대로 활성 상관관계 정책에 허용 목록을 추가합니다. 시스템은 허용 목록 평가와 위반 생성을 즉시 시작합니다.

관련 항목

컴플라이언스 허용 목록 대상 네트워크, 3 페이지
선택한 호스트를 기반으로 규정준수 허용리스트 생성
Firepower System IP 주소 규칙

규정준수 허용 목록에 대한 대상 네트워크 설정

대상 네트워크를 추가할 때 해당 네트워크를 조사해 규정준수 호스트의 특성을 설명할 수 있습니다. 조사에서 탐지된 각 운영체제에 대해 하나의 호스트 프로파일과 허용 목록을 채웁니다. 이러한 호스트 프로파일은 해당 운영 체제에서 탐지된 모든 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 허용합니다.

프로시저

단계 **1** 규정준수 허용 목록 편집기에서 **Add Target Network(**대상 네트워크 추가**)**를 클릭합니다.

단계 **2** 대상 네트워크의 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**를 입력합니다.

단계 **3** 다중 도메인 구축인 경우에는 대상 네트워크가 상주하는 **Domain(**도메인**)**을 선택합니다.

참고 대상 네트워크의 도메인은 선택이 끝나면 변경할 수 없습니다. 상위 도메인에 있는 서브넷을 대상으로 지정하면 각 하위 리프 도메인의 같은 서브넷이 대상으로 지정됩니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **4** 대상 네트워크 추가:

- Add(추가) - 조사하지 않고 대상 네트워크를 추가하려면 **Add(**추가**)**를 클릭합니다.
- Add and Survey Network(추가 및 네트워크 조사) - 대상 네트워크를 추가하고 조사하려면 **Add and Survey Network(**네트워크 추가 및 조사**)**를 클릭합니다.

단계 **5** 선택적으로, 추가 설정할 새 대상을 클릭합니다.

- Name(이름) - 새 **Name(**이름**)**을 입력합니다.
- Add Networks(네트워크 추가) - 추가 호스트를 대상으로 지정하려면, **Add(**추가**)** (+)을 클릭하고 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**를 입력합니다. 네트워크를 허용 목록 규정준수에서 제외하려면, **Exclude(**제외**)**를 선택합니다.
- Add Host Attributes(호스트 속성 추가) - 호스트를 특정 호스트 속성과 함께 대상으로 지정하려면, **Add(**추가**)** (+)을 클릭하고 **Attribute(**속성**)**와 그 **Value(**값**)**를 지정합니다.
- Add VLANs(VLAN 추가) - VLAN을 대상으로 지정하려면 **Add(**추가**)** (+)을 클릭하고 (802.1q VLAN에 대한) VLAN 번호를 입력합니다.
- Delete(삭제) — 대상 제한을 제거하려면 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **6** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

관련 항목

컴플라이언스 허용 목록 대상 네트워크, 3 페이지

Firepower System IP 주소 규칙

허용 리스트 호스트 프로필 빌드

호스트 프로파일은 허용 리스트의 규정준수 기준, 즉 대상 호스트에서 실행할 수 있는 운영체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 지정합니다.

모든 허용 리스트에는 운영체제에 구속되지 않는 전역 호스트 프로파일이 있습니다. 예를 들어 여러 개의 Microsoft Windows 및 Linux 호스트 프로파일을 수정하는 대신 Mozilla Firefox를 허용하려면, Firefox가 탐지되는 운영체제에 상관없이 Firefox를 허용하도록 전역 호스트 프로파일을 구성할 수 있습니다.

개별 허용 리스트에 국한되거나 여러 허용 리스트가 공유하는 운영체제 한정 호스트 프로파일을 설정할 수도 있습니다.

참고 공유 호스트 프로파일(내장된 프로파일 포함)을 수정하거나 내장된 애플리케이션 프로토콜, 프로토콜 또는 클라이언트를 수정하는 경우, 변경사항은 이를 사용하는 모든 허용리스트에 영향을 미칩니다. 의도하지 않은 변경사항을 적용하거나 내장된 요소를 삭제했다면, 공장 기본값으로 재설정할 수 있습니다.

시작하기 전에

- 컴플라이언스 허용 목록 편집, 14 페이지에 설명된 대로 허용내에서 호스트 프로파일을 생성 또는 편집하거나, 공유 호스트 프로파일 관리, 16 페이지에 설명된 대로 공유 호스트 프로파일을 생성 또는 편집합니다.

프로시저

단계 **1** 규정준수 허용 리스트 호스트 프로파일 편집기에서 호스트 프로파일을 설정합니다.

- Name(이름) - **Name(**이름**)**을 입력합니다.
- Operating System(운영체제) - 호스트 프로파일을 특정 운영체제에 제한하려면, **OS Vendor(**운영체제 벤더**)**, **OS Name(**운영체제 이름**)**, **Version(**버전**)** 드롭다운 목록을 이용합니다. 운영체제 종류에 상관없이 운영체제를 실행하는 모든 호스트에 적용하는 것이 목표이므로, 전역 호스트 프로파일을 제한할 수는 없습니다.
- Application Protocol(애플리케이션 프로토콜) - 애플리케이션 프로토콜을 허용하려면 **Add(**추가**)** (+) 을 클릭하고 컴플라이언스 허용 목록에 애플리케이션 프로토콜 추가, 11 페이지에 설명된 대로 진행합니다.
- Client(클라이언트) - 클라이언트를 허용하려면 **Add(**추가**)** (+) 을 클릭하고 컴플라이언스 허용 목록에 클라이언트 추가, 12 페이지에 설명된 대로 진행합니다.

- Web Application(웹 애플리케이션) - 웹 애플리케이션을 허용하려면 **Add(**추가**)** (+) 을 클릭하고 컴플라이언스 허용 목록에 웹 애플리케이션 추가, 12 페이지에 설명된 대로 진행합니다.
- Protocol(프로토콜) - 프로토콜을 허용하려면 **Add(**추가**)** (+) 을 클릭하고 컴플라이언스 허용 목록에 프로토콜 추가, 13 페이지에 설명된 대로 진행합니다.
- Delete(삭제) - 이전에 허용한 항목을 허용하지 않으려면 아이콘**(Delete(**삭제**)** ( ))을 클릭합니다.
- Edit Properties(속성 편집) - 허용되는 애플리케이션 프로토콜, 클라이언트 또는 프로토콜의 속성을 편집하려면 해당 요소의 이름을 클릭합니다. 변경사항은 해당 요소를 사용하는 모든 호스트 프로파일에 반영됩니다.

팁 적절한 **Allow all...(**모두 허용**...)** 확인란을 선택해 이 프로파일과 일치하는 호스트에 대한 모든 애플리케이션 프로토콜, 클라이언트 또는 웹 애플리케이션을 허용합니다.

단계 **2** 마지막으로 저장한 이후 적용된 모든 변경사항을 즉시 구현하려면 **Save(**저장**)**허용 목록(공유 호스트 프로파일을 편집하는 경우에는 **Save All Profiles(**모든 프로파일 저장**))**를 클릭합니다.

컴플라이언스 허용 목록에 애플리케이션 프로토콜 추가

허용 리스트 호스트 프로파일을 사용하면 애플리케이션 프로토콜을 전역적으로, 또는 특정 운영체제에서만 허용할 수 있습니다. 선택적으로, 애플리케이션 프로토콜을 포트, 벤더 또는 버전으로 제한할 수도 있습니다. 예를 들어 OpenSSH 특정 버전이 포트 22/TCP의 Linux 호스트에서 실행되도록 허용할 수 있습니다.

프로시저

단계 **1** 컴플라이언스 허용 리스트 호스트 프로파일을 생성하거나 수정할 경우, **Allowed Application Protocols(**허용되는 애플리케이션 프로토콜**)**(전역 호스트 프로파일을 수정할 경우에는 **Globally Allowed Application Protocols(**전역적으로 허용되는 애플리케이션 프로토콜**))** 옆에 있는 **Add(**추가**)** (+)를 클릭합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 허용할 애플리케이션 프로토콜이 목록에 있다면 해당 프로토콜을 선택합니다. 웹 인터페이스는 허용 목록이 허용해 왔거나 현재 허용하는 애플리케이션 프로토콜을 나열합니다.
- 목록에 없는 애플리케이션 프로토콜을 허용하려면, **<New Application Protocol>**을 선택하고 **OK(**확인**)**를 클릭하여 애플리케이션 프로토콜 편집기를 표시합니다. 허용할 애플리케이션 프로토콜 **Type(**유형**)**과 **Protocol(**프로토콜**)**을 선택합니다. 선택적으로, 애플리케이션 프로토콜을 포트, **Vendor(**벤더**)**, **Version(**버전**)**으로 제한합니다.

  참고 애플리케이션의 테이블 보기에 표시되는 벤더와 버전을 정확하게 입력해야 합니다. 벤더 또는 버전을 지정하지 않을 경우, 허용 목록에서는 유형 및 프로토콜이 매칭될 때까지 모든 벤더와 버전을 허용합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

컴플라이언스 허용 목록에 클라이언트 추가

허용 목록 호스트 프로파일을 사용하면 클라이언트를 전역적으로 또는 특정 운영체제에서만 허용할 수 있습니다. 선택적으로, 클라이어트가 특정 버전이길 요청할 수 있습니다. 예를 들어 Microsoft Internet Explorer 10에서만 Microsoft Windows 호스트를 실행하도록 허용할 수 있습니다.

프로시저

단계 **1** 컴플라이언스 허용 리스트 호스트 프로파일을 생성하거나 수정할 경우 **Allowed Clients(**허용되는 클라이언트**)**(전역 호스트 프로파일을 수정할 경우에는 **Globally Allowed Clients(**전역적으로 허용되는 클라이언트**)**) 옆에 있는 **Add(**추가**)** (+)를 클릭합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 허용할 클라이언트가 목록에 있다면 해당 클라이언트를 선택합니다. 웹 인터페이스는 허용이 허용해 왔거나 현재 허용하는 클라이언트를 나열합니다.
- 목록에 없는 클라이언트를 허용하려면 **<New Client>**를 선택하고 **OK(**확인**)**를 클릭해 클라이언트 편집기를 표시합니다. 드롭다운 목록에서 허용할 **Client(**클라이언트**)**를 선택하고, 원한다면 클라이언트를 허용되는 **Version(**버전**)**에 제한합니다.

  참고 클라이언트의 테이블 보기에 표시되는 버전을 정확하게 입력해야 합니다. 버전을 지정하지 않으면 모든 버전이 허용됩니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

컴플라이언스 허용 목록에 웹 애플리케이션 추가

허용리스트 호스트 프로파일을 사용하면 웹 애플리케이션을 전역적으로, 또는 특정 운영체제만 허용할 수 있습니다.

프로시저

단계 **1** 규정준수 허용리스트 호스트 프로파일을 생성하거나 수정할 경우, **Allowed Web Applications(**허용되는 웹 애플리케이션**)**(전역 호스트 프로파일을수정할경우에는**Globally Allowed Web Applications(**전역적으로 허용되는 웹 애플리케이션**)**) 옆에 있는 **Add(**추가**)** (+)를 클릭합니다.

단계 **2** 허용할 웹 애플리케이션을 선택합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

컴플라이언스 허용 목록에 프로토콜 추가

허용리스트 호스트 프로파일을 사용하면 프로토콜을 전역적으로, 또는 특정 운영체제에서만 허용할 수 있습니다. ARP, IP, TCP, UDP는 항상 모든 호스트에서 허용되며 해당 프로토콜은 허용하지 않을 수 없습니다.

프로시저

단계 **1** 허용리스트 호스트 프로파일을 생성하거나 수정할 경우, **Allowed Protocols(**허용되는 프로토콜**)**(전역 호스트 프로파일을 수정할 경우에는 **Globally Allowed Protocols(**전역적으로 허용되는 프로토콜**))** 옆에 있는 **Add(**추가**)** (+)를 클릭합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 허용할 프로토콜이 목록에 있다면 해당 프로토콜을 선택합니다. 웹 인터페이스는 허용되어 왔거나 허용리스트가 현재 허용하는 프로토콜을 나열합니다.
- 목록에 없는 프로토콜을 허용하려면, **<New Protocol>**을 선택하고 **OK(**확인**)**를 클릭하여 프로토콜 편집기를 표시합니다. **Type(**유형**)** 드롭다운 목록에서 프로토콜 유형**(Network(**네트워크**)** 또는 **Transport(**전송**))**을 선택하고, 드롭다운 목록에서 **Protocol(**프로토콜**)**을 선택합니다.

  팁 **Other (manual entry)(**기타**(**수동 입력**)**를 선택하여 목록에 없는 프로토콜을 지정합니다. 네트워크 프로토콜의 경우, http://www.iana.org/assignments/ethernet-numbers/에 나열된 적합한 번호를 입력합니다. 전송 프로토콜의 경우, http://www.iana.org/assignments/protocol-numbers/에 나열된 적합한 번호를 입력합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

컴플라이언스 허용 목록 관리

허용List(화이트리스트) 페이지를 이용하여 규정준수 허용리스트와 공유 호스트 프로파일을 관리할 수 있습니다. 기본 허용리스트는 권장 설정을 표시하며 내장형 호스트 프로파일이라고 하는 특수 범주의 공유 호스트 프로파일을 사용합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 규정준수 허용리스트를 표시하며, 이러한 리스트는 수정할 수 있습니다. 상위 도메인의 선택된 허용리스트도 표시되지만, 이는 편집할 수 없습니다. 하위 도메인에서 생성된 허용리스트를 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 상위 도메인의 컨피그레이션이 이름, 매니지드 디바이스 등 관련이 없는 도메인에 대한 정보를 표시하는 경우 상위 도메인의 컨피그레이션은 표시되지 않습니다. 기본 허용리스트는 전역 도메인에서만 사용할 수 있습니다.

프로시저

단계 **1** 허용 목록을 선택하고 **Policies(**정책**)** > **Correlation(**상관관계**)**를 클릭합니다.

단계 **2** 다음과 같이 규정준수 허용리스트를 관리합니다.

- Create(생성) - 새 허용리스트를 생성하려면 **New(**신규**)**허용 목록를 클릭하고 컴플라이언스 허용 목록 생성, 7 페이지에 설명된 대로 진행합니다.
- Delete(삭제) - 사용하지 않는 허용리스트를 삭제하려면 **Delete(**삭제**)** ( )를 클릭하고 허용리스트 삭제 여부를 확인합니다. 허용리스트를 삭제하면 관련된 호스트 속성이 네트워크의 모든 호스트에서 제거됩니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- Edit(편집) - 기존 허용리스트를 수정하려면 **Edit(**수정**)** ( )을 클릭하고 컴플라이언스 허용 목록 편집, 14 페이지에 설명된 대로 진행합니다. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- Shared Host Profiles(공유 호스트 프로파일) - 허용리스트의 공유 호스트 프로파일을 관리하려면 **Edit Shared Profiles(**공유 프로파일 편집**)**를 클릭하고 공유 호스트 프로파일 관리, 16 페이지에 설명된 대로 진행합니다.

컴플라이언스 허용 목록 편집

활성 상관관계 정책에 포함된 규정준수 허용 목록을 수정하고 저장하는 경우, 시스템은 허용 목록의 대상 네트워크에 있는 호스트의 규정준수 여부를 즉시 다시 평가합니다. 이러한 재평가로 인해 일부 호스트의 상태가 규정준수 또는 규정 미준수로 바뀔 수 있으나, 시스템은 어떤 허용 목록 이벤트도 생성하지 않습니다.

프로시저

단계 **1** 허용 목록을 선택하고 **Policies(**정책**)** > **Correlation(**상관관계**)**를 클릭합니다.

단계 **2** 수정할 허용 목록 옆의 **Edit(**수정**)** ( )를 클릭합니다.

View(보기**)** ()이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 규정준수 허용 목록 편집:

- Name and Description(이름 및 설명) - 이름이나 설명을 변경하려면 왼쪽 패널에서 허용 목록 이름을 클릭해 기본 허용 목록 정보를 표시한 다음 새 정보를 입력합니다.
- Allow Jailbroken Devices(탈옥 디바이스 허용) - 네트워크에서 탈옥 모바일 디바이스를 허용하려면, 왼쪽 패널에서 허용 목록 이름을 클릭해 기본 허용 목록 정보를 표시하고 **Allow Jailbroken Mobile Devices(**탈옥 모바일 디바이스 허용**)**를 활성화합니다. 이 옵션을 비활성화하면 탈옥한 디바이스가 허용 목록 위반을 생성할 수 있습니다.
- Add Allowed Host Profile(허용되는 호스트 프로파일 추가) - 허용 목록에 대한 운영체제 한정 호스트 프로파일을 생성하려면, Allowed Host Profiles(허용되는 호스트 프로파일) 옆에 있는 **Add(**추가**)** ()을 클릭하고 허용 리스트 호스트 프로필 빌드, 10 페이지에 설명된 대로 진행합니다.
- Add Shared Host Profile(공유 호스트 프로파일 추가) - 기존 공유 호스트 프로파일을 허용 목록에 추가하려면, **Add Shared Host Profile(**공유 호스트 프로파일 추가**)**을 클릭하고 추가할 공유 호스트 프로파일을 선택한 다음 **OK(**확인**)**를 클릭합니다. 공유 호스트 프로파일은 기울임꼴로 표시됩니다.
- Add Target Network(대상 네트워크 추가) - 호스트 조사 없이 새 대상 네트워크를 추가하려면, Target Networks(대상 네트워크) 옆에 있는 **Add(**추가**)** ()을 클릭하고 규정준수 허용 목록에 대한 대상 네트워크 설정, 9 페이지에 설명된 대로 진행합니다.
- Delete Host Profile(호스트 프로파일 삭제) - 공유 또는 운영체제 한정 호스트 프로파일을 허용 목록에서 삭제하려면, 호스트 프로파일 옆에 있는 **Delete(**삭제**)** ()을 클릭하고 선택을 확인합니다. 공유 호스트 프로파일을 삭제하면 허용 목록에서 해당 프로파일이 제거되지만, 이를 사용하는 다른 허용 목록의 해당 프로파일은 삭제 또는 제거되지 않습니다. 허용 목록의 전역 호스트 프로파일은 삭제할 수 없습니다.
- Delete Target Network(대상 네트워크 삭제) - 대상 네트워크를 허용 목록에서 제거하려면, 네트워크 옆에 있는 **Delete(**삭제**)** ()을 클릭하고 선택을 확인합니다.
- Edit Global Host Profile(전역 호스트 프로파일 편집) - 허용 목록의 전역 호스트 프로파일을 편집하려면 **Any Operating System(**모든 운영체제**)**을 클릭하고 허용 리스트 호스트 프로필 빌드, 10 페이지에 설명된 대로 진행합니다.
- Edit Other Host Profile(기타 호스트 프로파일 편집) - 공유 또는 운영체제 한정 호스트 프로파일을 편집하려면, 호스트 프로파일의 이름을 클릭하고 허용 리스트 호스트 프로필 빌드, 10 페이지에 설명된 대로 진행합니다.
- Edit Target Network(대상 네트워크 편집) - 대상 네트워크를 편집하려면, 네트워크의 이름을 클릭하고 규정준수 허용 목록에 대한 대상 네트워크 설정, 9 페이지에 설명된 대로 진행합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

공유 호스트 프로파일 관리

규정준수 허용리스트에서 공유 호스트 프로파일은 특정 운영체제에 연결되지만, 각 공유 호스트 프로파일을 두 개 이상의 허용리스트에서 사용할 수 있습니다. 여러 개의 허용리스트를 생성하지만 동일한 호스트 프로파일을 사용하여 허용리스트 전반에 걸쳐 특정 운영체제를 실행하는 호스트를 평가하려는 경우, 공유 호스트 프로파일을 사용합니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 공유 호스트 프로파일을 표시하며, 이러한 규칙은 편집할 수 있습니다. 상위 도메인의 공유 호스트 프로파일도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 공유 호스트 프로파일을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 공유 호스트 프로파일(내장된 프로파일 포함)을 수정하거나 내장된 애플리케이션 프로토콜, 프로토콜 또는 클라이언트를 수정하는 경우, 변경사항은 이를 사용하는 모든 허용리스트에 영향을 미칩니다. 의도하지 않은 변경사항을 적용하거나 내장된 요소를 삭제했다면, 공장 기본값으로 재설정할 수 있습니다.

프로시저

단계 **1** 허용 목록을 선택하고 **Policies(**정책**)** > **Correlation(**상관관계**)**를 클릭합니다.

단계 **2** **Edit Shared Profiles(**공유 프로파일 편집**)**를 클릭합니다.

단계 **3** 공유 호스트 프로파일 관리:

- Create Shared Host Profile(공유 호스트 프로파일 생성) - 호스트를 점검하지 않고 새 공유 호스트 프로파일을 생성하려면 Shared Host Profiles(공유 호스트 프로파일) 옆에 있는 **Add(**추가**)** ( )를 클릭하고 허용 리스트 호스트 프로필 빌드, 10 페이지에 설명된 대로 진행합니다.
- Create Shared Host Profile by Survey(조사를 통해 공유 호스트 프로파일 생성) - 네트워크를 조사해 여러 새 공유 호스트 프로파일을 생성하려면, **Add Target Network(**대상 네트워크 추가**)**를 클릭하고 규정준수 허용 목록에 대한 대상 네트워크 설정, 9 페이지에 설명된 대로 진행합니다.
- Delete(삭제) - 공유 호스트 프로파일을 삭제하려면 **Delete(**삭제**)** ( )를 클릭하고 선택을 확인합니다.
- Edit(편집) - 기존 공유 호스트 프로파일(내장된 공유 호스트 프로파일 포함)을 수정하려면, 이름을 클릭하고 허용 리스트 호스트 프로필 빌드, 10 페이지에 설명된 대로 진행합니다.
- Reset Built-In Host Profiles(내장 호스트 프로파일 재설정) - 모든 내장 호스트 프로파일을 공장 기본값으로 재설정하려면, **Built-in Host Profiles(**내장 호스트 프로파일**)**를 클릭하고 **Reset to Factory Defaults(**공장 기본값으로 재설정**)** 를 클릭한 다음 선택을 확인합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경사항을 즉시 구현하려면, **Save All Profiles(**모든 프로파일 저장**)**를 클릭합니다.