에이전트 없는 상태 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

배경 정보

시작하기

- 사전 요구 사항:
- 지원되는 상태 조건
- 지원되지 않는 상태 조건

ISE 구성

- 상태 피드 업데이트
- 에이전트 없는 상태 컨피그레이션 흐름
- 에이전트 없는 상태 컨피그레이션
  - 상태 조건
  - 포스처 요구 사항
  - 상태 정책
  - 클라이언트 프로비저닝
  - AgentlessAuthorization 프로파일
  - 교정을 사용하는 대체 방법(선택 사항)
  - 교정 권한 부여 프로파일(선택 사항)
  - 에이전트 없는 권한 부여 규칙
  - 엔드포인트 로그인 자격 증명 구성

Windows 끝점 구성 및 문제 해결

- 사전 요구 사항 확인 및 문제 해결
  - 포트 5985에 대한 TCP 연결 테스트
  - 포트 5985에서 PowerShell을 허용하기 위한 인바운드 규칙 만들기
  - 셸 로그인을 위한 클라이언트 자격 증명에는 로컬 관리자 권한이 있어야 합니다
  - WinRM 수신기 유효성 검사
  - PowerShell 원격 WinRM 사용
  - Powershell은 v7.1 이상이어야 합니다. 클라이언트에는 cURL v7.34 이상이 있어야 합니다.
  - Windows 디바이스에서 PowerShell 및 cURL 버전 확인을 위한 출력
  - 추가 컨피그레이션
  - MacOS
  - Powershell은 v7.1 이상이어야 합니다. 클라이언트에는 cURL v7.34 이상이 있어야 합니다.
  - MacOS 클라이언트의 경우 클라이언트에 액세스하려면 SSH에 액세스하기 위한 포트 22가 열려 있어야 합니다
  - MacOS의 경우 엔드포인트에서 인증서 설치 실패를 방지하려면 sudoers 파일에서 이 항목이 업데이트되어야 합니다.

소개

이 문서에서는 ISE에서 Posture Agentless를 구성하는 방법과 엔드포인트에서 Agentless 스크립트

를 실행하기 위해 필요한 사항에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Identity Services Engine (ISE).
- 상태.
- PowerShell 및 SSH
- Windows 10 이상

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE(Identity Services Engine) 3.3 버전.
- CiscoAgentlessWindows 5.1.6.6 패키지
- Windows 10

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

ISE Posture는 클라이언트측 평가를 수행합니다. 클라이언트는 ISE로부터 상태 요구 사항 정책을 수신하고, 상태 데이터 수집을 수행하고, 결과를 정책과 비교하고, 평가 결과를 ISE로 다시 전송합니다.

그런 다음 ISE는 Posture Report(포스처 보고서)를 기반으로 디바이스가 불만인지 또는 규정준수를 준수하지 않는지 결정합니다.

에이전트 없는 포스처는 클라이언트에서 포스처 정보를 수집하고 최종 사용자의 작업 없이 완료 시 자동으로 제거되는 포스처 방법 중 하나입니다. 에이전트 없는 상태는 관리 권한을 사 항목으로 클라이언트에 연결 됩니다.

시작하기

사전 요구 사항:

- 클라이언트는 IPv4 또는 IPv6 주소를 통해 연결할 수 있어야 하며 해당 IP 주소는 RADIUS 어카운팅에서 사용할 수 있어야 합니다.

- IPv4 또는 IPv6 주소를 통해 Cisco ISE(Identity Services Engine)에서 클라이언트에 연결할 수

있어야 합니다. 또한 이 IP 주소는 RADIUS 어카운팅에서 사용할 수 있어야 합니다.

- Windows 및 Mac 클라이언트가 현재 지원됩니다.
    - Windows 클라이언트의 경우 클라이언트에서 powershell에 액세스하기 위한 포트 5985가 열려 있어야 합니다. Powershell은 v7.1 이상이어야 합니다. 클라이언트에는 cURL v7.34 이상이 있어야 합니다.
    - MacOS 클라이언트의 경우 클라이언트에 액세스하려면 SSH에 액세스하기 위한 포트 22가 열려 있어야 합니다. 클라이언트에는 cURL v7.34 이상이 있어야 합니다.
- 셸 로그인을 위한 클라이언트 자격 증명에는 로컬 관리자 권한이 있어야 합니다.
- 컨피그레이션 단계에 설명된 대로 포스처 피드 업데이트를 실행하여 최신 클라이언트를 가져옵니다. 다음을 확인하십시오.
- MacOS의 경우 엔드포인트에서 인증서 설치 실패를 방지하기 위해 sudoers 파일에서 이 항목이 업데이트되었는지 확인합니다. 다음을 확인하십시오.

<macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

- MacOS의 경우 구성된 사용자 계정은 관리자 계정이어야 합니다. MacOS용 에이전트 없는 상태는 추가 권한을 부여하더라도  다른 계정 유형에서는 작동하지 않습니다.이 창을 보려면 메뉴 ( )를 클릭하고 **관리 > 시스템 > 설정 > 엔드포인트 스크립트** > 로그인 **구성 > MAC Local User를 선택합니다.**

- Microsoft의 업데이트로 인해 Windows 클라이언트에서 포트 관련 활동이 변경되는 경우 Windows 클라이언트에 대한 에이전트 없는 상태 컨피그레이션 워크플로를 다시 구성해야 합니다.

지원되는 상태 조건

- USER_DESKTOP

및 USER_PROFILE 파일 경로를 사용하는 조건을 제외한 파일 조건

- 서비스 상태(macOS에서 시스템 데몬 및 데몬 또는 사용자 에이전트 검사 제외)
- 애플리케이션 조건
- 외부 데이터 원본 조건
- 복합 조건
- 안티멀웨어 상태
- 패치 관리 조건(EnabledAndUp **To Datecondition** 검사 제외)
- 방화벽 조건
- 암호화 위치 기반 조건 검사를 제외한 디스크 암호화 조건
- HCSK를 루트 키로 사용하는 조건을 제외한 레지스트리 조건

지원되지 않는 상태 조건

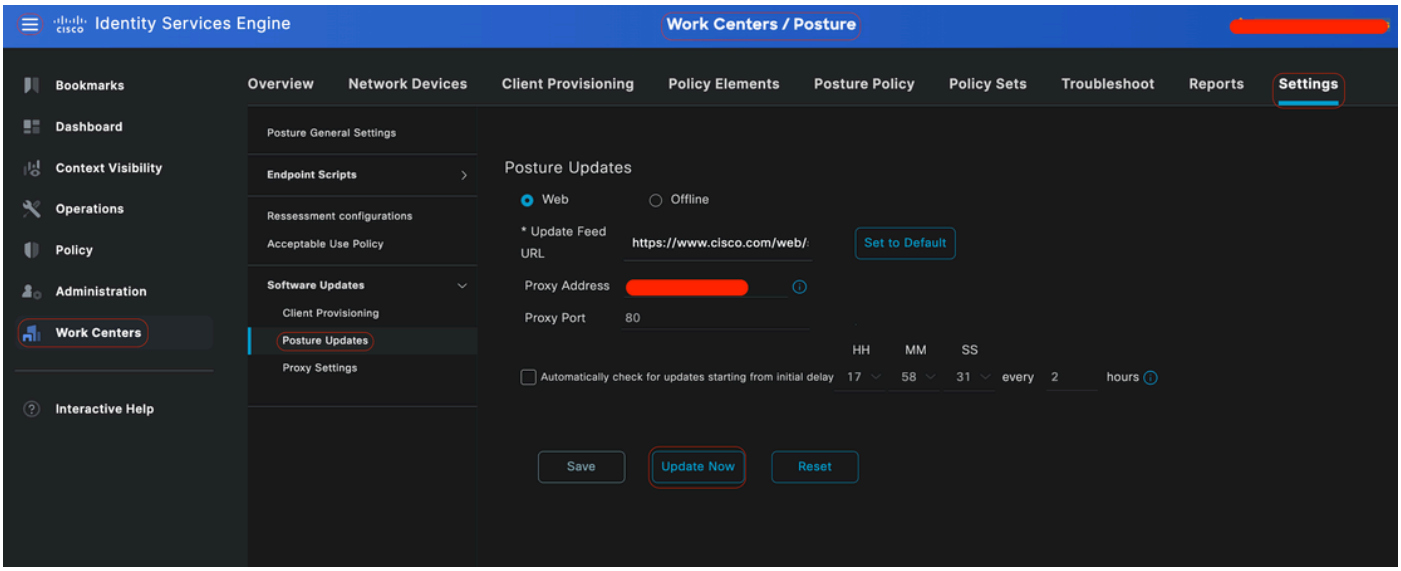
- 교정
- 유예 기간
- 정기 재평가
- 수락 가능 한 사용 정책

ISE 구성

상태 피드 업데이트

포스처 구성을 시작하기 전에 포스처 피드를 업데이트하는 것이 좋습니다.

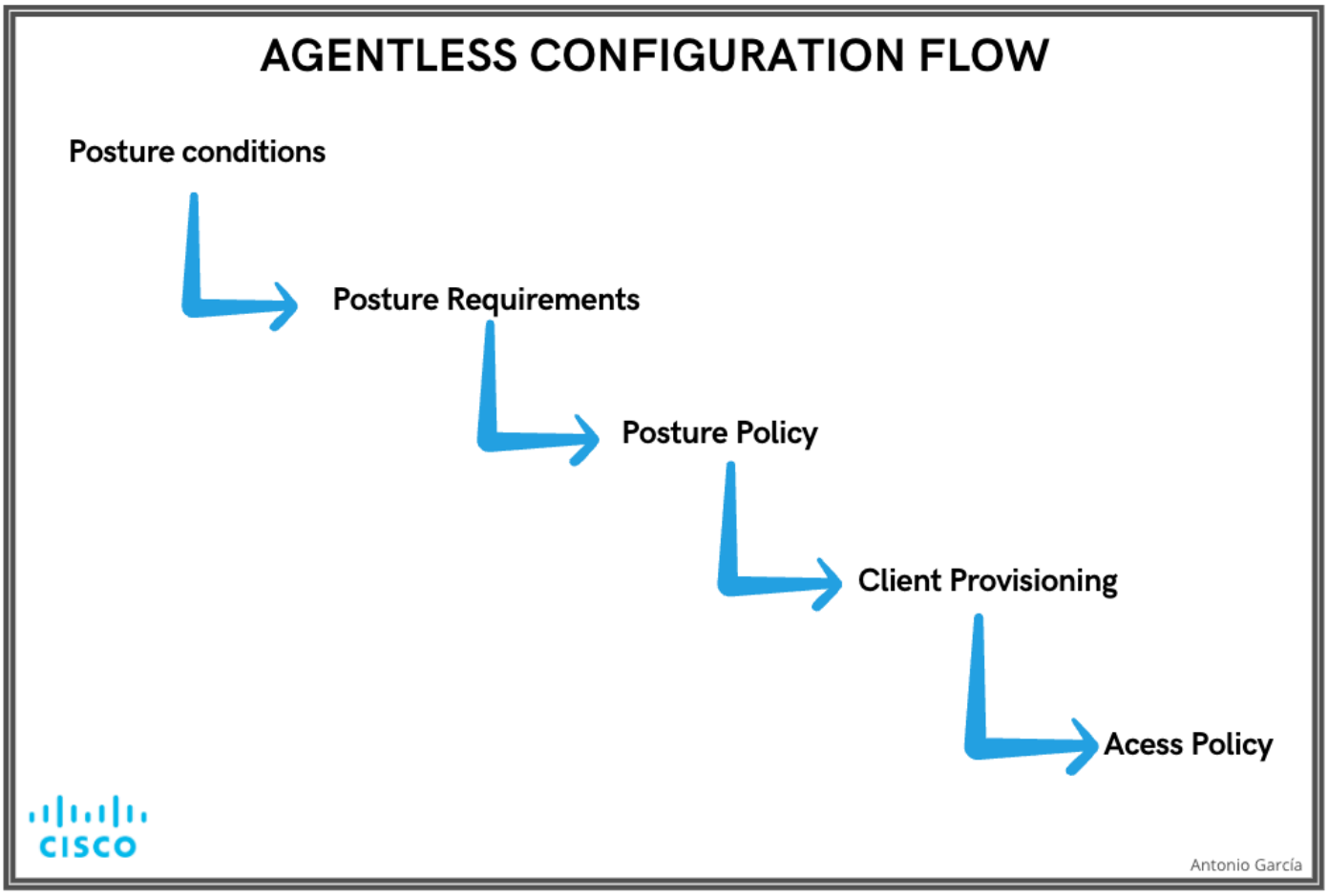
Cisco ISE GUI에서 Menuicon ( )을 클릭하고 **Work Centers(작업 센터) > Posture(포스처) > Settings(설정) > Software Updates(소프트웨어 업데이트**) > Update Now(지금 업데이트)를 선택합니다.



상태 피드 업데이트

에이전트 없는 상태 컨피그레이션 흐름

첫 번째 컨피그레이션이 다음 컨피그레이션에 필요하므로 Posture Agentless를 순서대로 구성해야 합니다. 리미디에이션은 흐름에 포함되지 않습니다. 그러나 나중에 이 문서에서는 리미디에이션을 구성하는 대안을 다룹니다.



에이전트 없는 컨피그레이션 흐름

에이전트 없는 상태 컨피그레이션

상태 조건

포스처 조건은 호환 엔드포인트를 정의하는 보안 정책의 규칙 집합입니다. 이러한 항목 중 일부는 방화벽 설치, 안티바이러스 소프트웨어, 안티멀웨어, 핫픽스, 디스크 암호화 등을 포함합니다.

Cisco ISE GUI에서 Menuicon(메뉴)을 클릭하고 **Work Centers(작업 센터) > Posture(포스처) > Policy Elements(정책 요소) > Conditions(**조건)를 선택한 다음 Add(추가)를 클릭하고 에이전트 없는 포스처**를 사용하여 요구 사항을 식별하는** 하나 이상의 포스처 조건**을 생성합니다.** Condition이 **생성되면** Save**를 클릭합니다**.

이 시나리오에서는 "Agentless_**Condition_Application"이라는 애플리케이션 조건**이 다음 매개변수로 구성되었습니다.

·운영 체제: Windows All

이 조건은 Windows 운영 체제의 모든 버전에 적용되므로 서로 다른 Windows 환경 간의 폭넓은 호환성이 보장됩니다.

·검사자: 프로세스

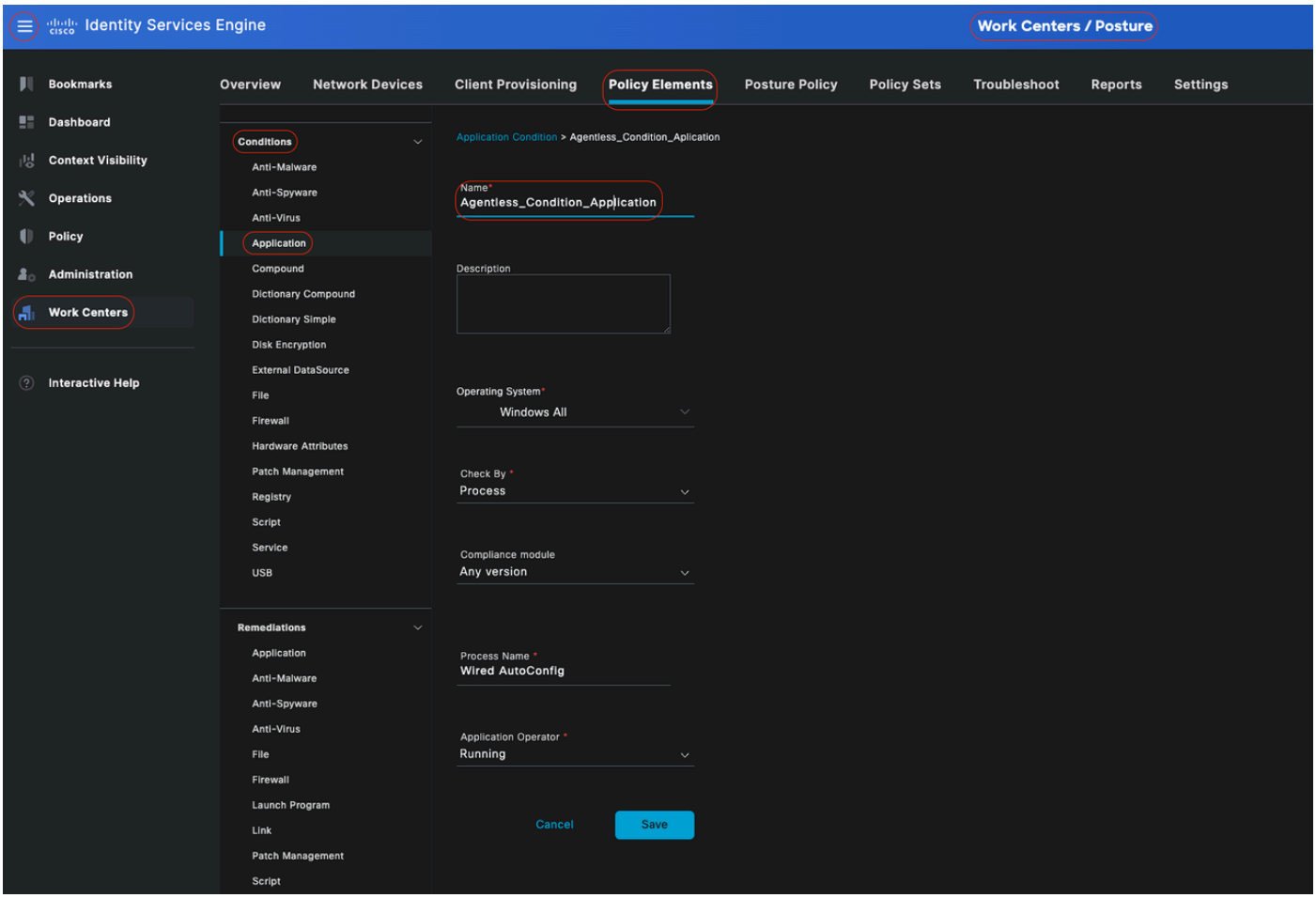
시스템은 디바이스 내의 프로세스를 모니터링합니다. **프로세스** 또는 애플리케이션을 선택할 수 있습니다. **이** 경우 프로세스**가** 선택됩니다.

·프로세스 이름: 유선 자동 구성

Wired **AutoConfig** 프로세스는 Compliant Module이 디바이스를 체크인하는 프로세스입니다. 이 프로세스는 IEEE 802.1X 인증을 포함하여 유선 네트워크 연결을 구성하고 관리하는 역할을 합니다.

·애플리케이션 운영자: 실행

Compliance Module에서는 유선 AutoConfig **프로세스**가 현재 디바이스에서 실행 중인지 확인합니다. Running(실행 중) 또는 Not Running(**실행 중** 아님)을 선택할 수 **있습니다**. 이 경우 프로세스**가** 활성 상태인지 확인하기 위해 Running(실행 중)을 선택했습니다.



에이전트 없는 조건

상태 요구 사항

포스처 요건은 복합 조건의 집합이거나 역할 및 운영 체제와 연결할 수 있는 하나의 조건입니다. 네트워크에 연결하는 모든 클라이언트는 상태 평가 중에 필수 요구 사항을 충족해야 네트워크에서 규정을 준수합니다.

Cisco ISE GUI에서 Menuicon (

)을 클릭하고 **Work Centers(작업 센터) > Posture(포스처)** > **Policy Elements(정책 요소)** > Requirement(요건)를 선택합니다**. 아래쪽 화살표**를 클릭하고 **Insert new Requirement**를 선택하고, Agentless Posture를 사용하는 하나 이상의 PostureRequirement를 **생성합니다.** Requirement(**요구 사항)**가 생성되면 Done(완료)을 클릭한 **다음 Save(저장)**를 **클릭합니다**.

이 경우 "Agentless_Requirement_**Application"이라는 애플리케이션 요구 사항**이 다음 조건으로 구성되었습니다.

· **운영 체제:** Windows All

이 요구 사항은 Windows 운영 체제의 모든 버전에 적용되므로 모든 Windows 환경에 적용할 수 있습니다.

· **상태 유형:** 에이전트 없음

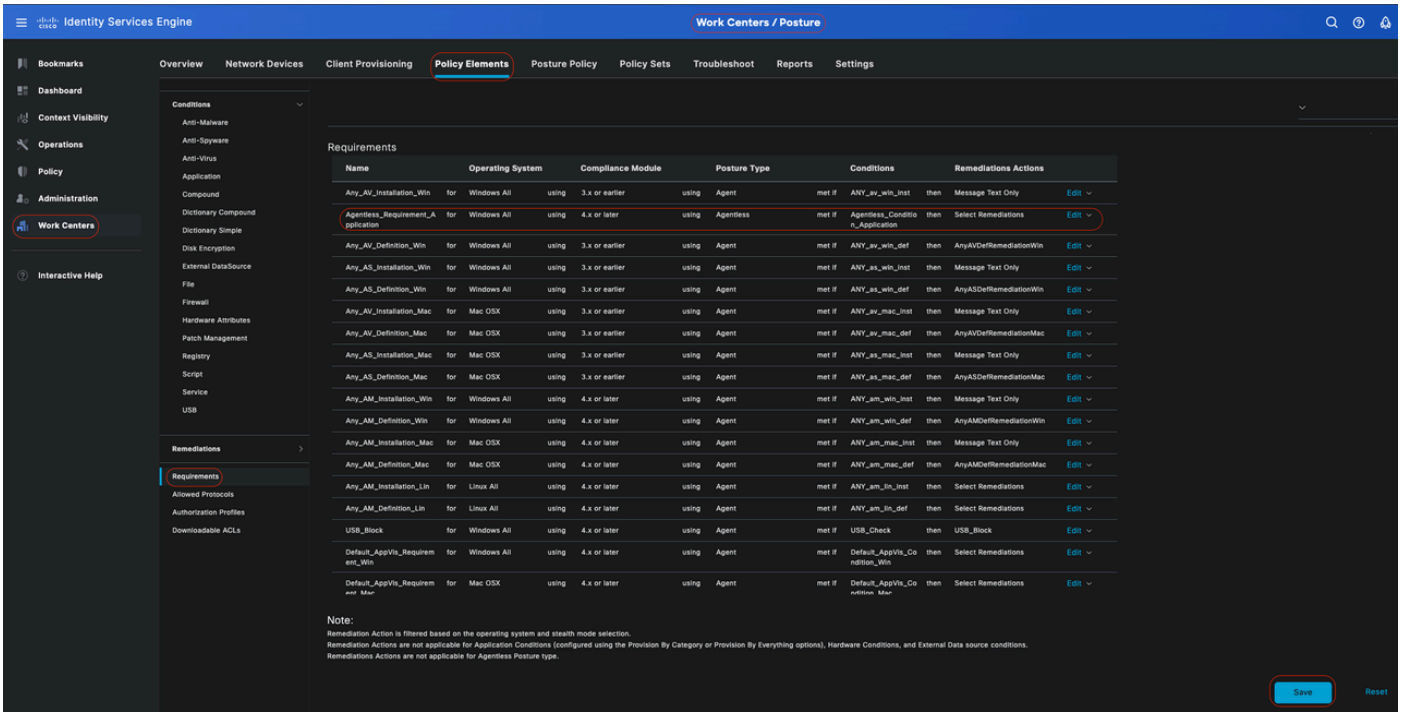
이 구성은 에이전트 없는 환경에 대해 설정됩니다. 사용 가능한 옵션에는 **에이전트**, **에이전트 스텔스**, 임시 **에이전트** 및 에이전트가 **포함됩니다**. 이 시나리오에서는 **Agentless**가 선택되었습니다.

· **조건: Agentless_Condition_Application**

이는 ISE Posture Module 및 Compliance Module이 디바이스의 프로세스 내에서 점검할 조건을 지정합니다. 선택한 조건은 **Agentless_Condition_Application입니다**.

· **리미디에이션 조치:**

이 컨피그레이션은 에이전트 없는 환경을 위한 것이므로 교정 작업은 지원되지 않으며 이 필드는 회색으로 표시됩니다.



에이전트 없는 요구 사항

상태 정책

Cisco ISE GUI에서 Menu(메뉴)를 클릭하고 **Work Centers**(작업 **센터)** > Posture(**포스처)** > Posture(포스처) Policy(정책)**를** 선택합니다**. 아래쪽** 화살표를 클릭하고 **Insert new Requirement(새 요구 사항 삽입**)를 선택하고, 해당 Posture Requirement(상태 요구 사항)에 대해 Agentless **Posture**(에이전트 없는 상태)를 사용하는 하나 이상의 지원되는 상태 정책 규칙을 생성합니다. Posture Policy**가** 생성되면 Done(완료)을 클릭한 **다음** Save(저장)를 **클릭합니다**.

이 시나리오에서 "Agentless_Policy_**Application"이라는 포스처 정책**이 다음 매개변수로 구성되었습니다.

·**규칙 이름:** Agentless_Policy_Application

이 컨피그레이션 예에서는 Posture Policy에 대해 지정된 이름입니다.

·**운영 체제:** Windows All

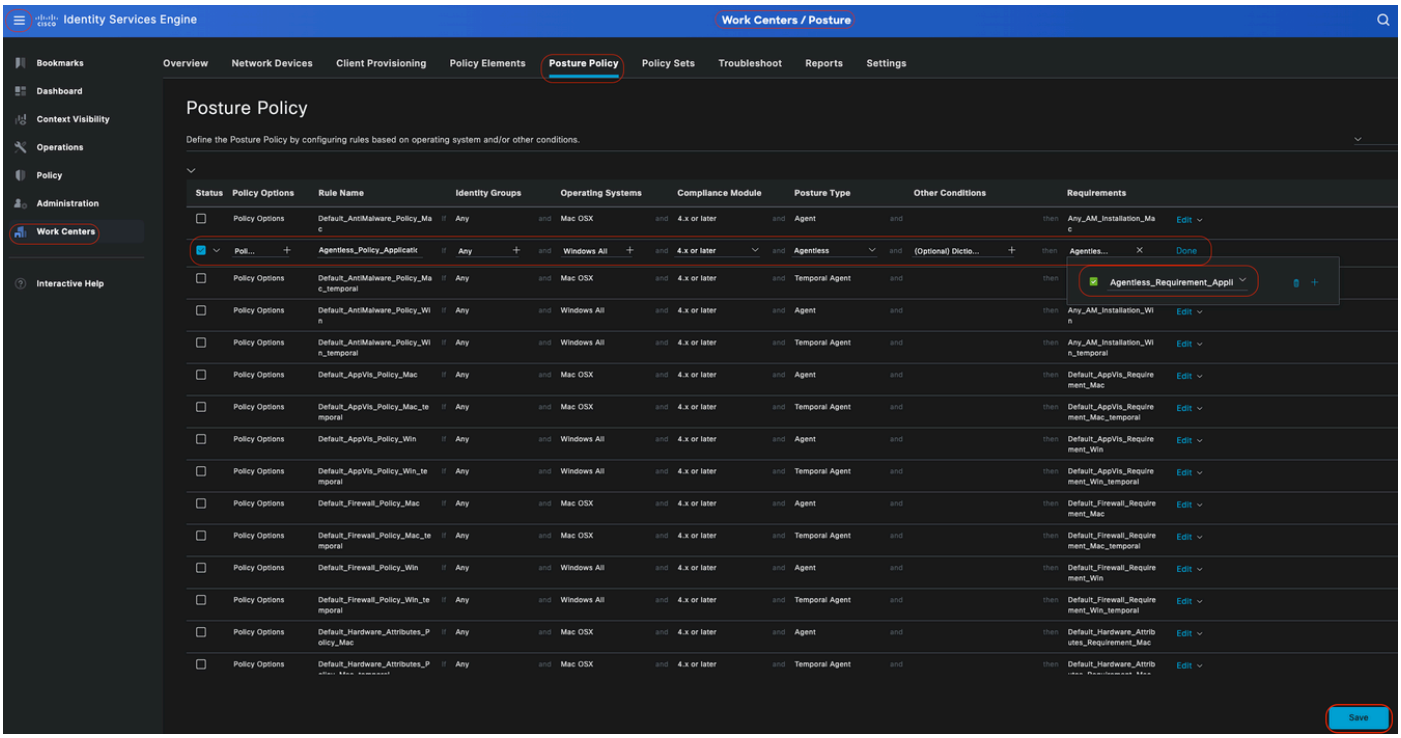
정책은 Windows 운영 체제의 모든 버전에 적용되도록 설정되므로 서로 다른 Windows 환경 간의 폭넓은 호환성이 보장됩니다.

·**상태 유형:** 에이전트 없음

이 구성은 에이전트 없는 환경에 대해 설정됩니다. 사용 가능한 옵션에는 **에이전트**, **에이전트 스텔스**, 임시 **에이전트** 및 에이전트가 **포함됩니다**. 이 시나리오에서는 **에이전트** 없음이 선택되었습니다.

·**기타 조건:**

이 컨피그레이션 예에서는 추가 조건이 생성되지 않았습니다. 그러나 특정 조건을 구성하여 네트워크의 모든 Windows 장치가 아닌 대상 장치만 이 포스처 정책의 적용을 받도록 할 수 있습니다. 이는 네트워크 세그멘테이션에 특히 유용할 수 있습니다.



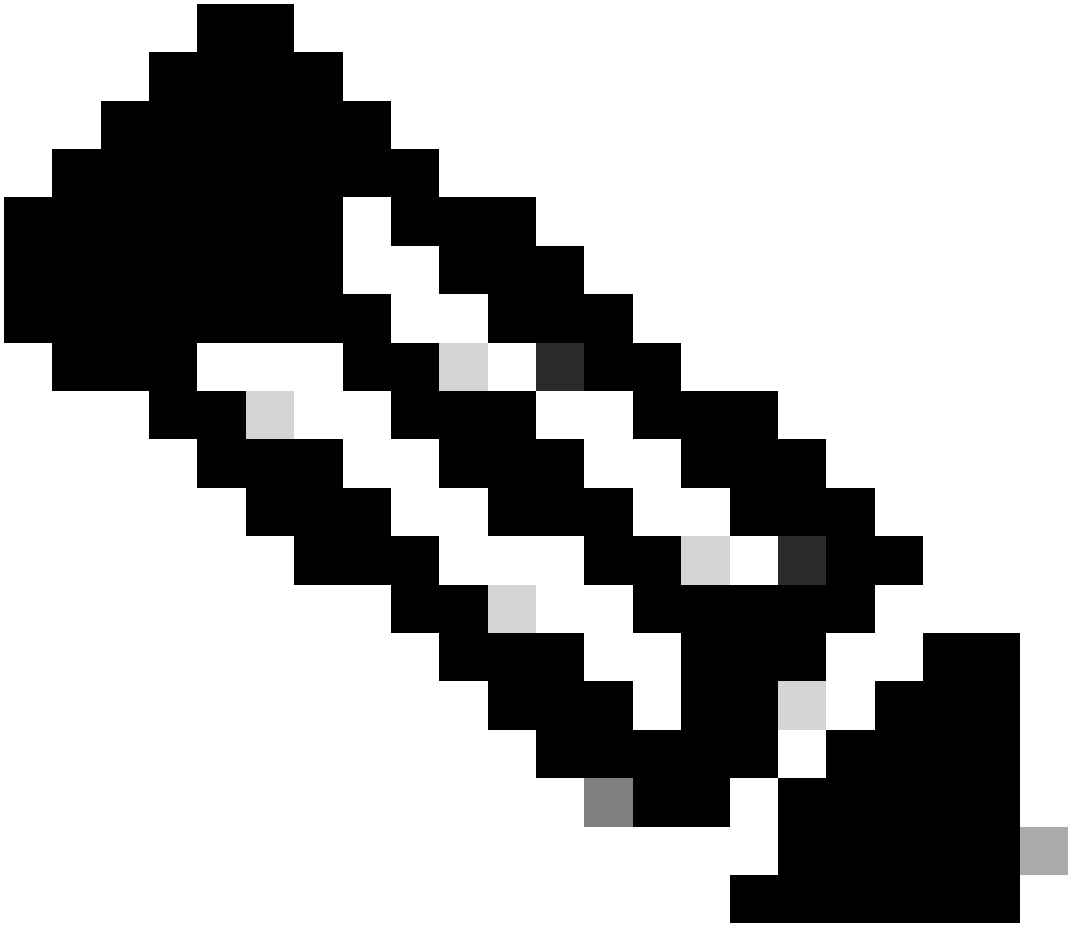
에이전트 없는 상태 정책

클라이언트 프로비저닝

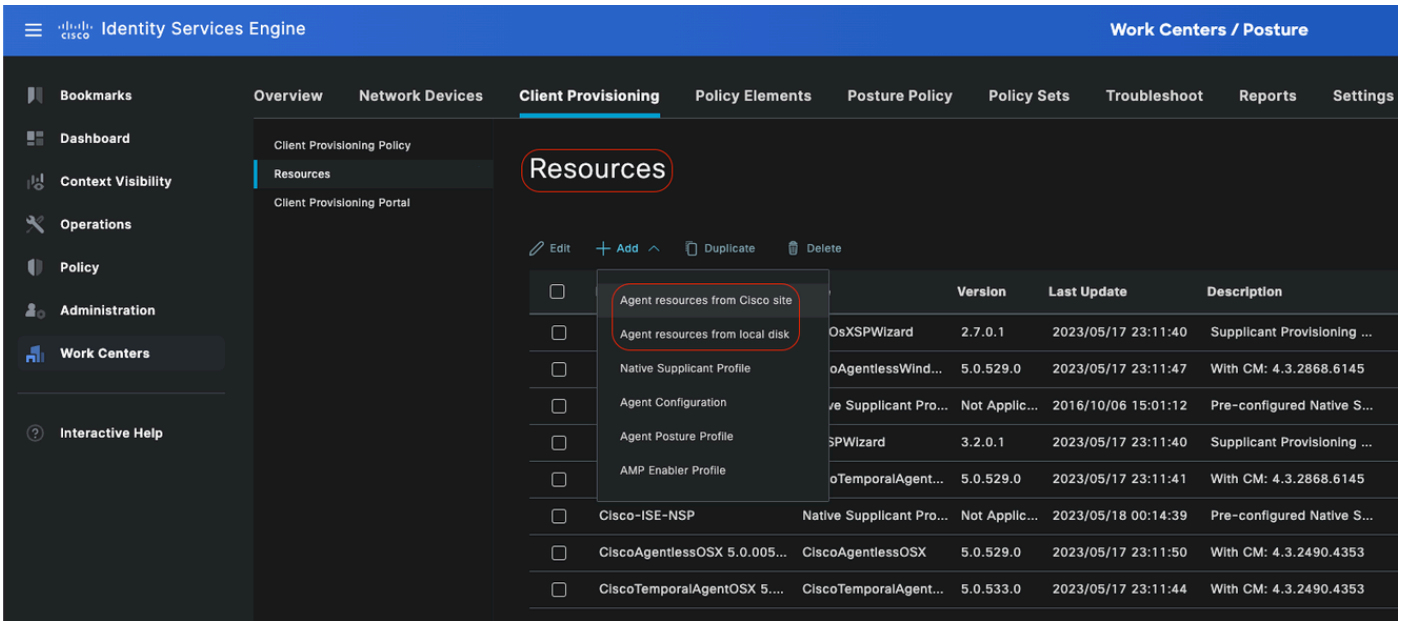
1단계 - 리소스 다운로드

클라이언트 프로비저닝 구성을 시작하려면 먼저 필요한 리소스를 다운로드하고 나중에 클라이언트 프로비저닝 정책에서 사용할 수 있도록 ISE에서 사용할 수 있도록 해야 합니다.

ISE에 리소스를 추가하는 방법에는 두 가지가 있습니다. **Cisco 사이트의 에이전트 리소스**와 **로컬 디스크의 에이전트 리소스입니다**. 에이전트 없음을 구성하므로 **Cisco** 사이트**에서 에이전트 리소스를** 거쳐야 다운로드할 수 있습니다.



참고: **Cisco** 사이트**에서** 이 **에이전트 리소스**를 사용하려면 ISE PAN에 인터넷 액세스가 필요합니다.



리소스

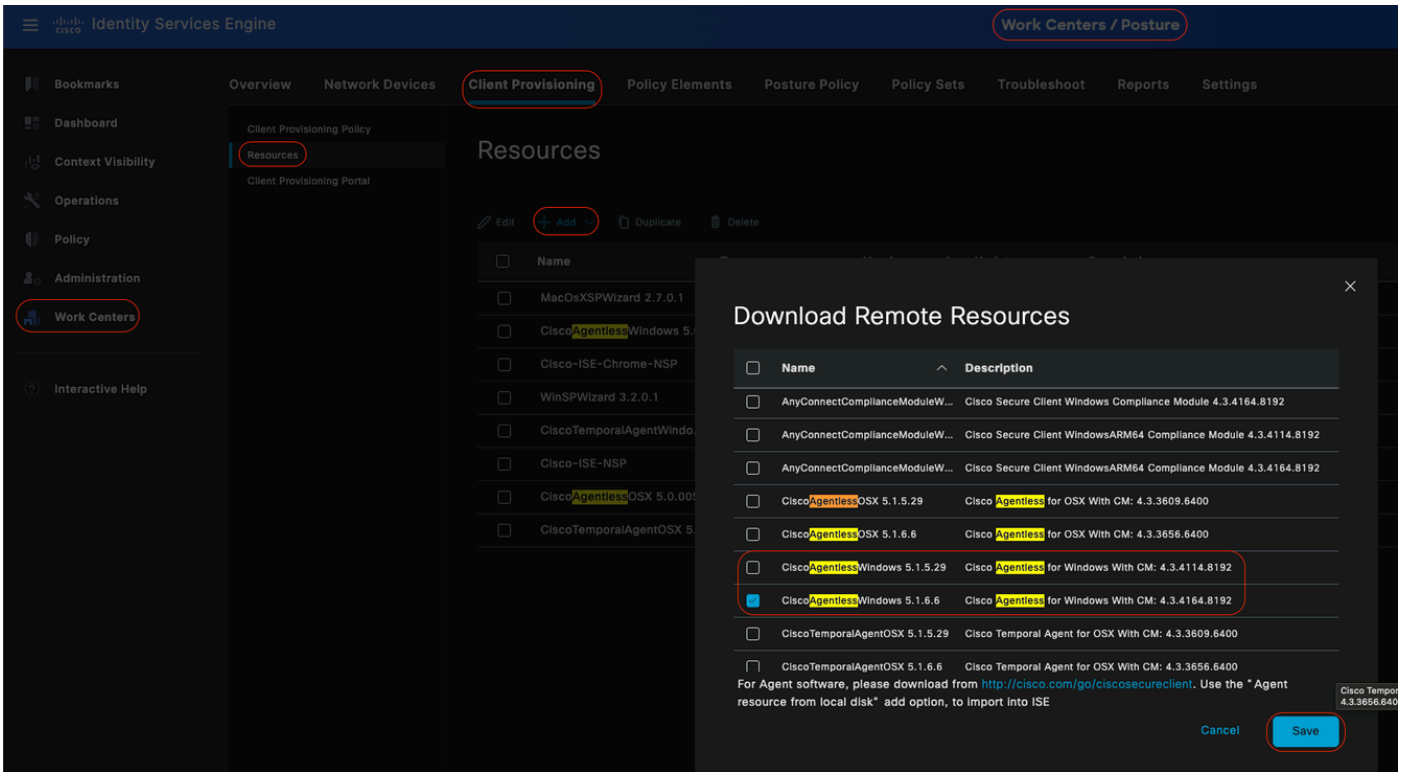
Cisco 사이트의 에이전트 리소스

Cisco ISE GUI에서 Menuicon ( )을 클릭하고 **Work Centers(작업 센터)** > Posture(포스처) **> Client Provisioning(클라이언트 프로비저닝)** > Resources(리소스)를 선택합니다**.** Add(**추가**)를 클릭하고 **Cisco 사이트에서 Agent Resources(에이전트 리소스)**를 선택한 후 Save(**저장)를 클릭합니다**.

Cisco 사이트에서는 Compliance Module만 다운로드할 수 있습니다. 다운로드할 최신 Compliance Module이 두 개 표시됩니다. 리소스 패키지 **CiscoAgentlessWindows 5.1.6.6**이 이 컨피그레이션 예에 대해 선택되었습니다. 이는 Windows 디바이스에만 적용됩니다.

.

Cisco 사이트의



에이전트 리소스

2단계 - 클라이언트 프로비저닝 정책 구성

포스처 에이전트를 구성할 때 두 가지 리소스(AnyConnect 또**는 보안 클라이언트** 및 **규정 준수 모듈**)가 필요합니다.

클라이언트 프로비저닝 정책에서 이 **에이전트 컨피그레이션**을 사용할 수 있도록 **에이전트** 포스처 **프로필**과 함께 **에이전트 컨피그레이션** 아래의 두 리소스**를 매핑합니다.**

그러나 포스처 에이전트 없음을 구성할 때 **에이전트 컨피그레이션 또는 에이전트 포스처 프로파일**을 구성할 필요가 없습니다. 대신 **Cisco 사이트**의 **에이전트 리소스에서 에이전트** 없는 패키지만 다운로드해야 **합니다**.

Cisco ISE GUI에서 Menuicon (

)을 클릭하고 **Work Centers(작업 센터)** > Posture(포스처) **>** Client Provisioning(**클라이언트 프로비저닝)** > Client Provisioning Policy(클라이언트 프로비저닝 정책)를 선택합니다**.** 아래쪽 화살표를 클릭하고 **Insert new policy above**(위에 **새 정책 삽입) 또는** Insert **new policy below(아래에 새 정책 삽입**), Duplicate above(위에 **중복) 또는 Insert** Duplicate below(아래에 복제)를 선택합니다.

- **규칙 이름: Agentless_Client_Provisioning_Policy**

클라이언트 프로비저닝 정책의 이름을 지정합니다.

- **운영 체제:** Windows All

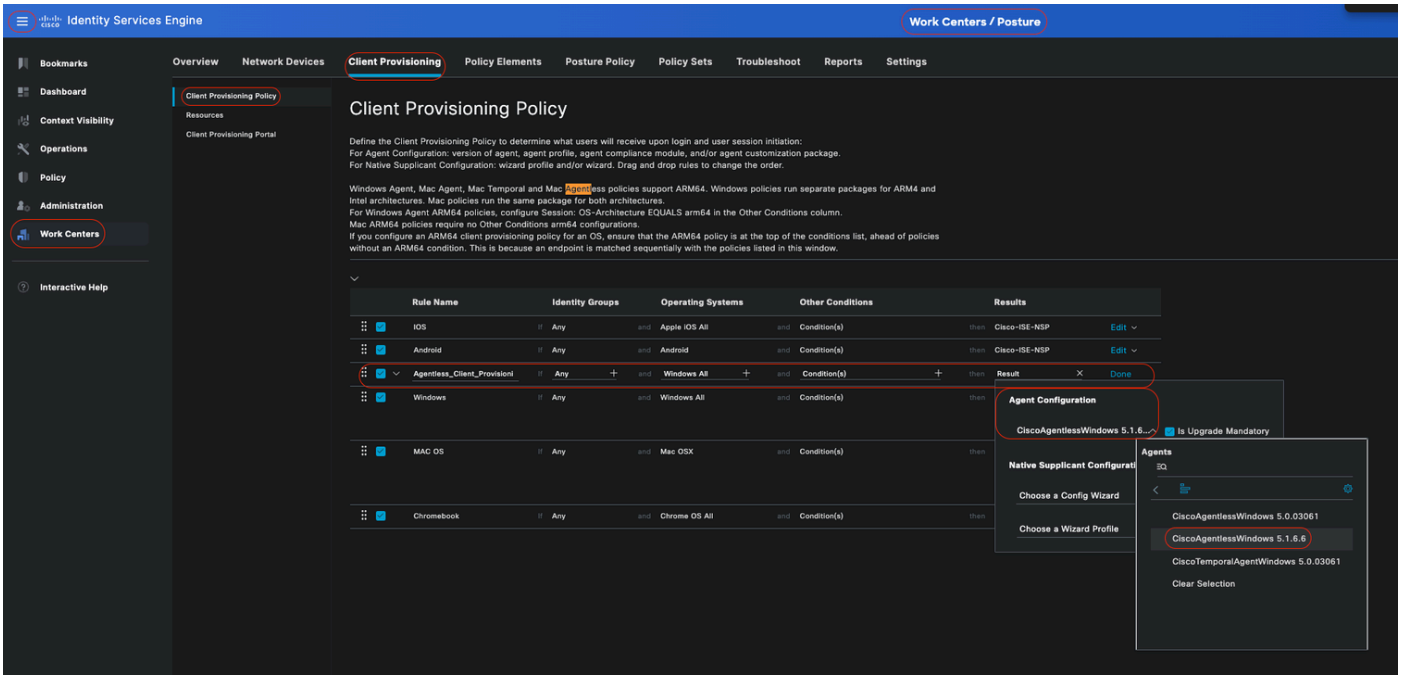
이렇게 하면 정책이 모든 버전의 Windows 운영 체제에 적용됩니다.

- **기타 조건:** 이 예에서는 특정 조건이 구성되지 않습니다. 그러나 네트워크의 모든 Windows 장치가 아니라 원하는 장치만 이 클라이언트 프로비저닝 정책과 일치하는지 확인하는 조건을 구성할 수 있습니다. 이는 네트워크 분할에 특히 유용합니다.

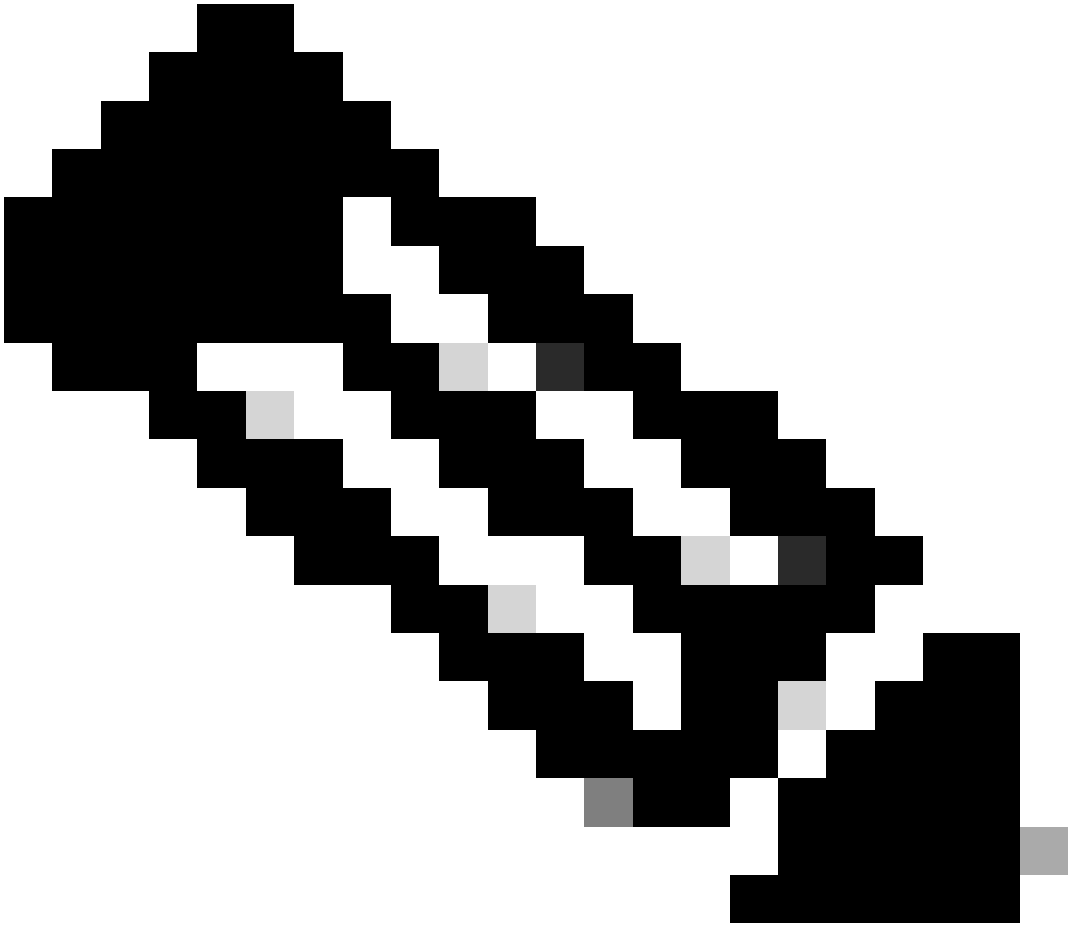
예: Active Directory를 사용 중인 경우 Active Directory 그룹을 정책에 통합하여 영향을 받는 디바이스를 세분화할 수 있습니다.

- **결과:** 적절한 패키지 또는 구성 에이전트를 선택합니다. 에이전트 없는 환경에 대해 구성 중이므로 **Cisco 사이트**의 **에이전트 리소스**에서 이전에 다운로드한 **CiscoAgentlessWindows 5.1.6.6 패키지를** 선택합니다. 이 에이전트 없는 패키지에는 에이전트 없는 상태**를 실행하는** 데 필요한 모든 리소스(에이전트 없는 **소프트웨어** 및 **규정 준수 모듈**)가 포함되어 있습니다.

· Save(**저장**)를 클릭합니다.



에이전트 없는 클라이언트 프로비저닝 정책



참고: 하나의 클라이언트 프로비저닝 정책만 지정된 인증 시도에 대한 조건을 충족하는지 확인하십시오. 여러 정책을 동시에 평가할 경우 예기치 않은 동작 및 잠재적 충돌을 초래할 수 있습니다.

에이전트 없는 **권한 부여 프로파일**

Cisco ISE GUI에서 Menuicon

(메뉴)을 클릭하고 Policy(정책) > Policy Elements(정책 **요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)**를 선택하고 **Agentless Posture에서 결과를 평가하는 Authorization Profile(권한 부여 프로파일)을 생성합니다.**

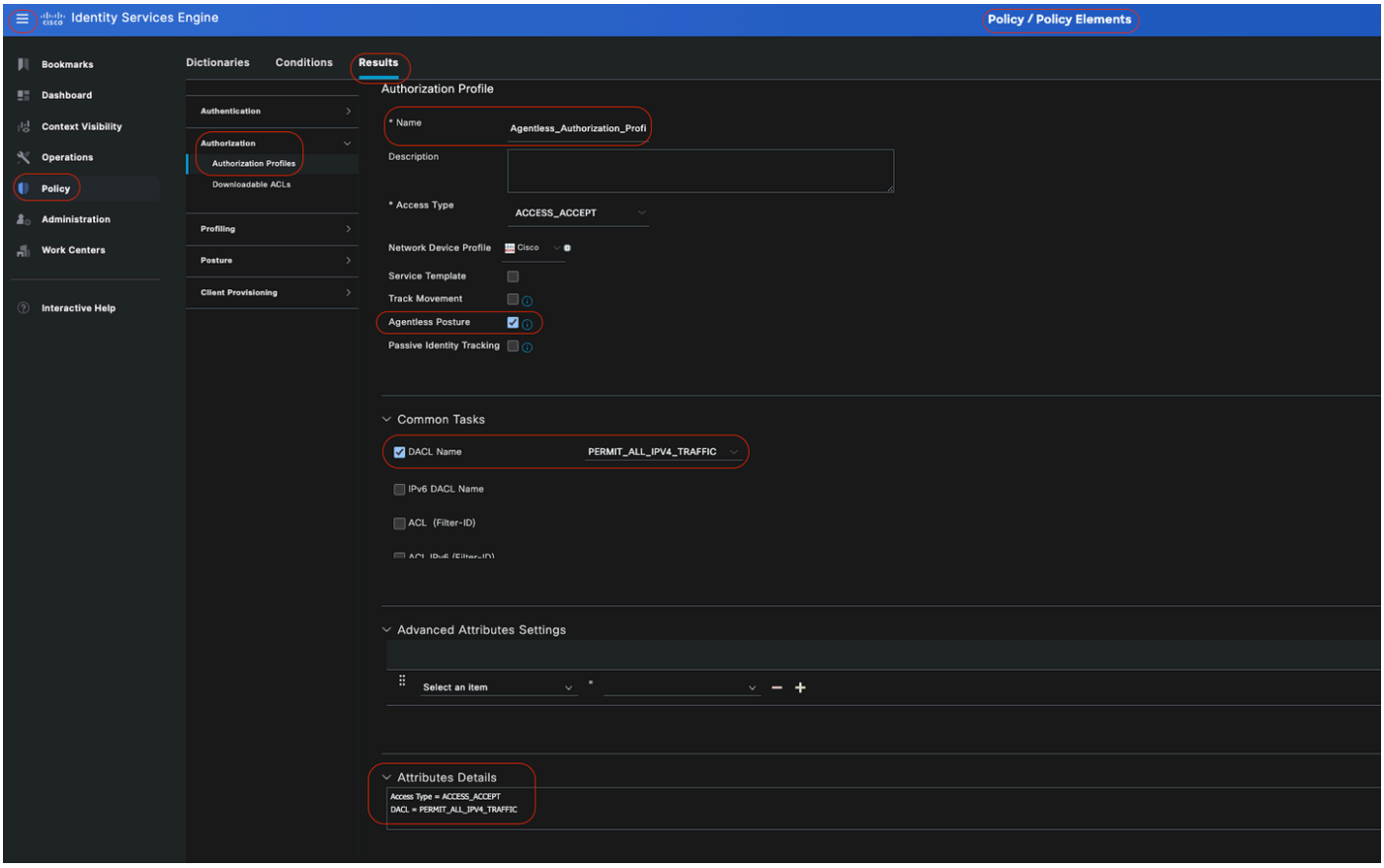
- 이 컨피그레이션 예에서는 Authorization Profile을 Agentless_Authorization_**Profile로 명명했습니다**.

- 권한 부여 프로파일에서 Agentless Posture를 활성화합니다.

- 이 프로파일은 에이전트 없는 **포스처에만 사용합니다**. 다른 포스처 유형에도 이 옵션을 사용하지 마십시오.

- CWA 및 리디렉션 ACL은 에이전트 없는 상태에 필요하지 않습니다. VLAN, DACL 또는 ACL을 세그멘테이션 규칙의 일부로 사용할 수 있습니다. 이 컨피그레이션 예에서는 간소화를 위해 Agentless Posture 검사 외에 dACL(모든 ipv4 트래픽 허용)만 구성합니다.

- **Save**(저장)를 **클릭합니다**.



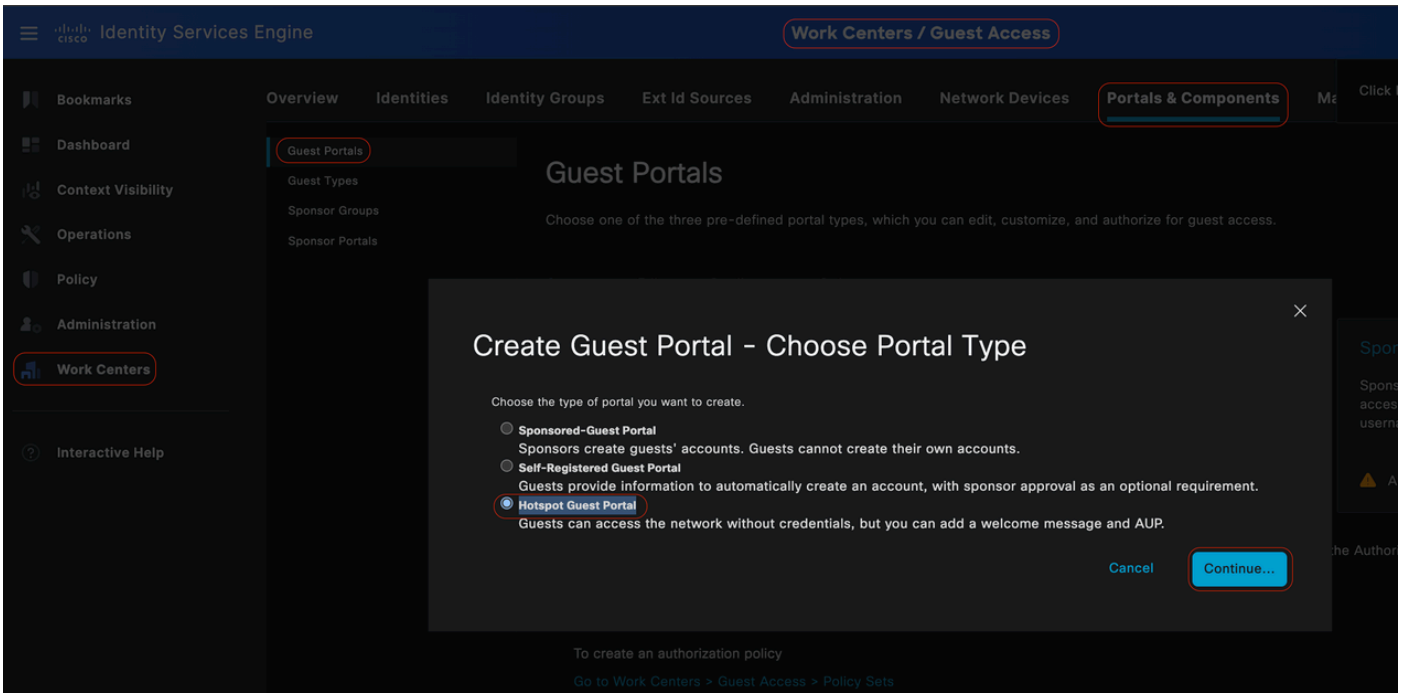
에이전트 없는 권한 부여 프로파일

교정을 사용하는 대체 방법(선택 사항)

에이전트 없는 흐름에서 교정에 대한 지원을 사용할 수 없습니다. 이를 해결하기 위해 맞춤형 핫스팟 포털을 구현하여 엔드포인트 규정준수와 관련된 사용자 인식을 개선할 수 있습니다. 엔드포인트가 규정을 준수하지 않는 것으로 확인되면 사용자가 이 포털로 리디렉션될 수 있습니다. 이러한 접근 방식을 통해 사용자는 엔드포인트의 규정 준수 상태에 대해 알 수 있으며 문제를 해결하기 위해 적절한 조치를 취할 수 있습니다.

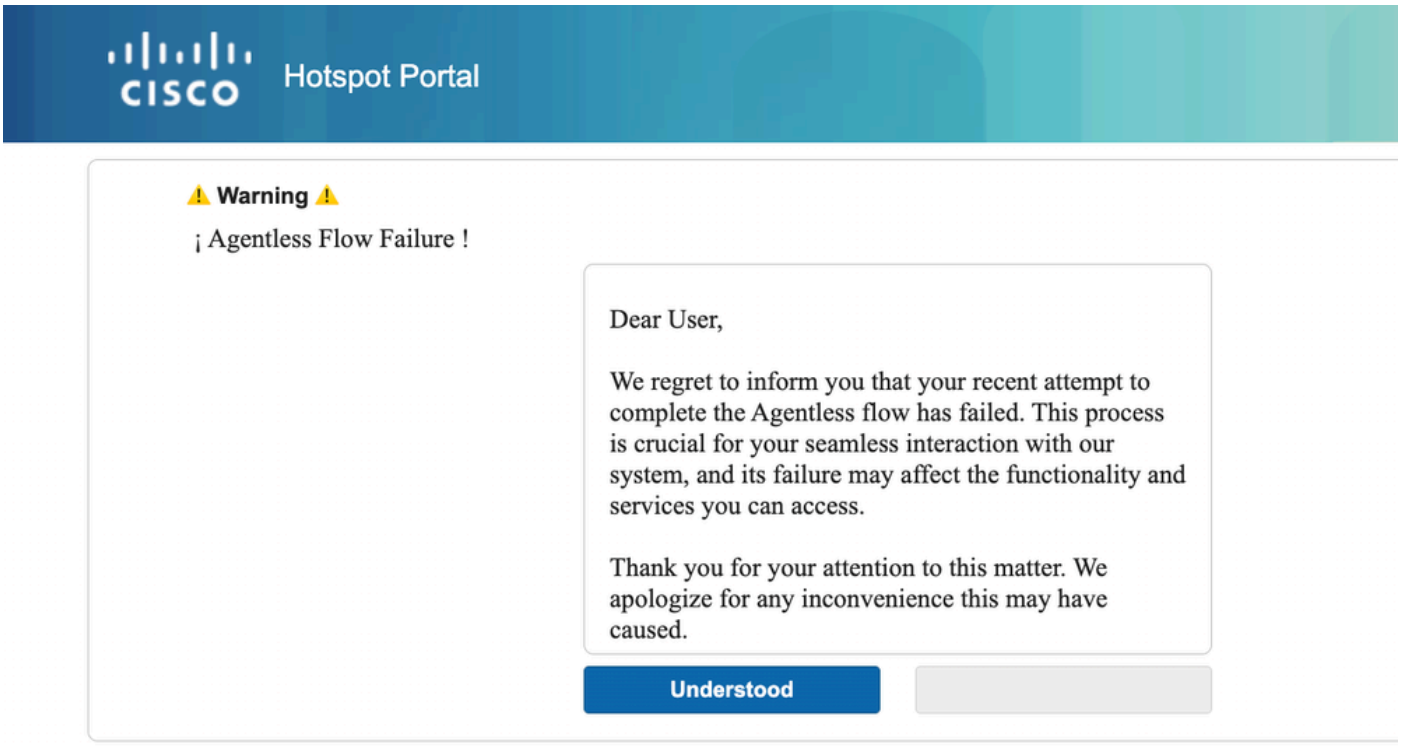
Cisco ISE GUI에서 Menuicon

(메뉴)을 클릭하고 **Work Centers(작업 센터)** > **Guest Access(게스트 액세스)** > Portals & Components(**포털 및 구성 요소)** > Guest Portals(게스트 포털)를 선택합니다. Create(**생성**) > Select **Hotspot Guest Portal(핫스팟 게스트 포털 선택)** > **Continue(계속)를 클릭합니다**. 이 컨피그레이션 예에서는 핫스팟 포털의 이름이 Agentless_**Warning**으로 **지정됩니다**.



핫스팟 게스트 포털

포털 설정에서 최종 사용자에게 표시되는 메시지를 특정 요구 사항에 맞게 사용자 지정할 수 있습니다. 이는 사용자 지정된 포털 보기의 예입니다.



에이전트 없는 상태 실패

교정 권한 부여 프로파일(선택 사항)

Cisco ISE GUI에서 Menuicon ( )을 클릭하고 Policy(정책) > Policy Elements(정책 **요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)**를 선택하고 교정을 **위한 Authorization Profile(권한 부여 프로파일)을 생성합니다.**

- 이 컨피그레이션 예에서는 Authorization Profile을 Remediation_**Authorization_Profile로 명명했습니다**.

-

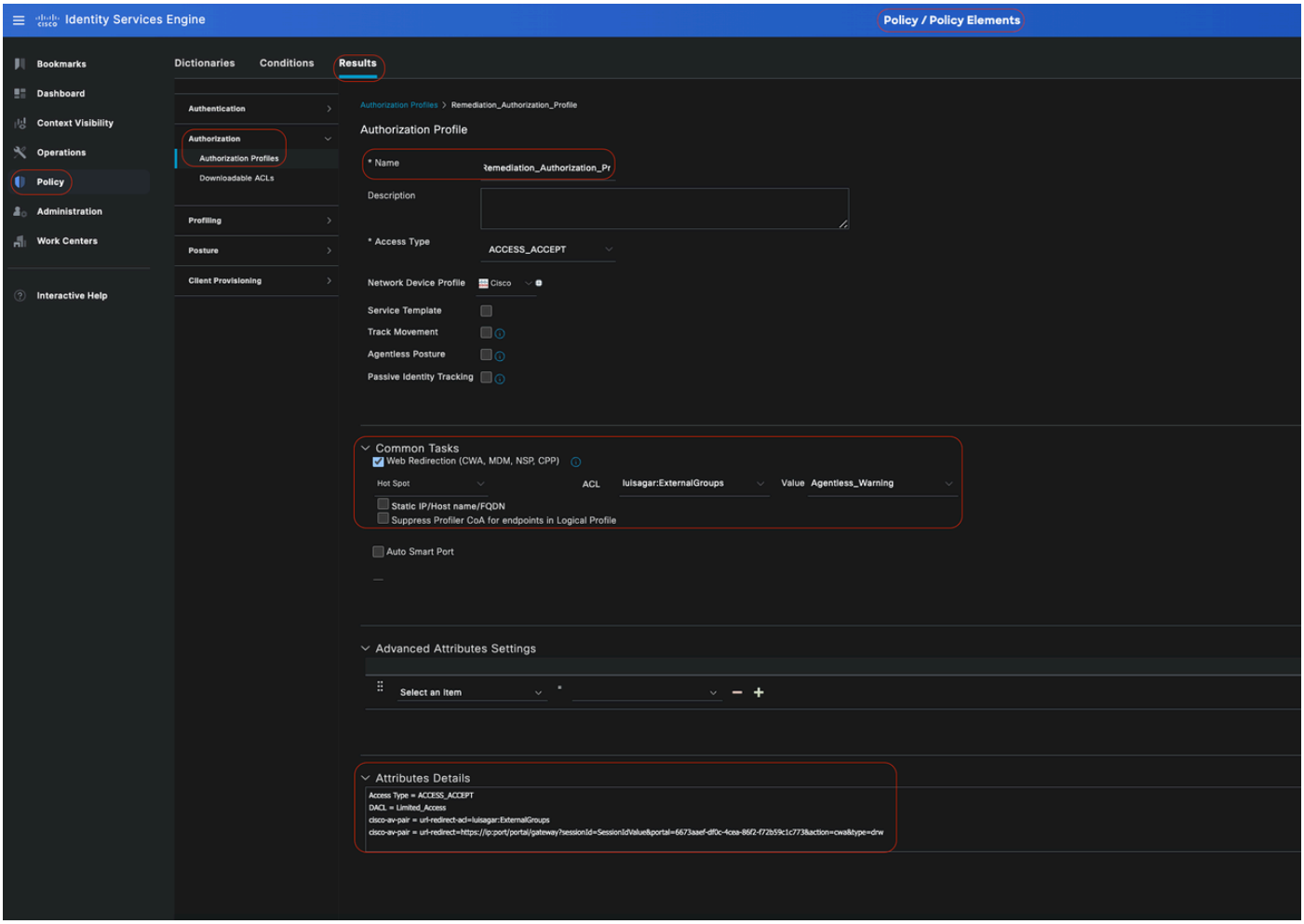
이 컨피그레이션 예에는 간소화를 위해 조직의 특정 요구 사항에 따라 제한된 액세스를 허용하는 **Limited_Access**라는 다운로드 가능한 dACL(Access Control List)만 포함되어 있습니다.

-

외부 그룹 및 핫스팟을 포함하여 **웹** 리디렉션 기능을 구성하여 엔드포인트 규정 준수에 대한 사용자 인식을 개선했습니다.

-

저장을 클릭합니다.

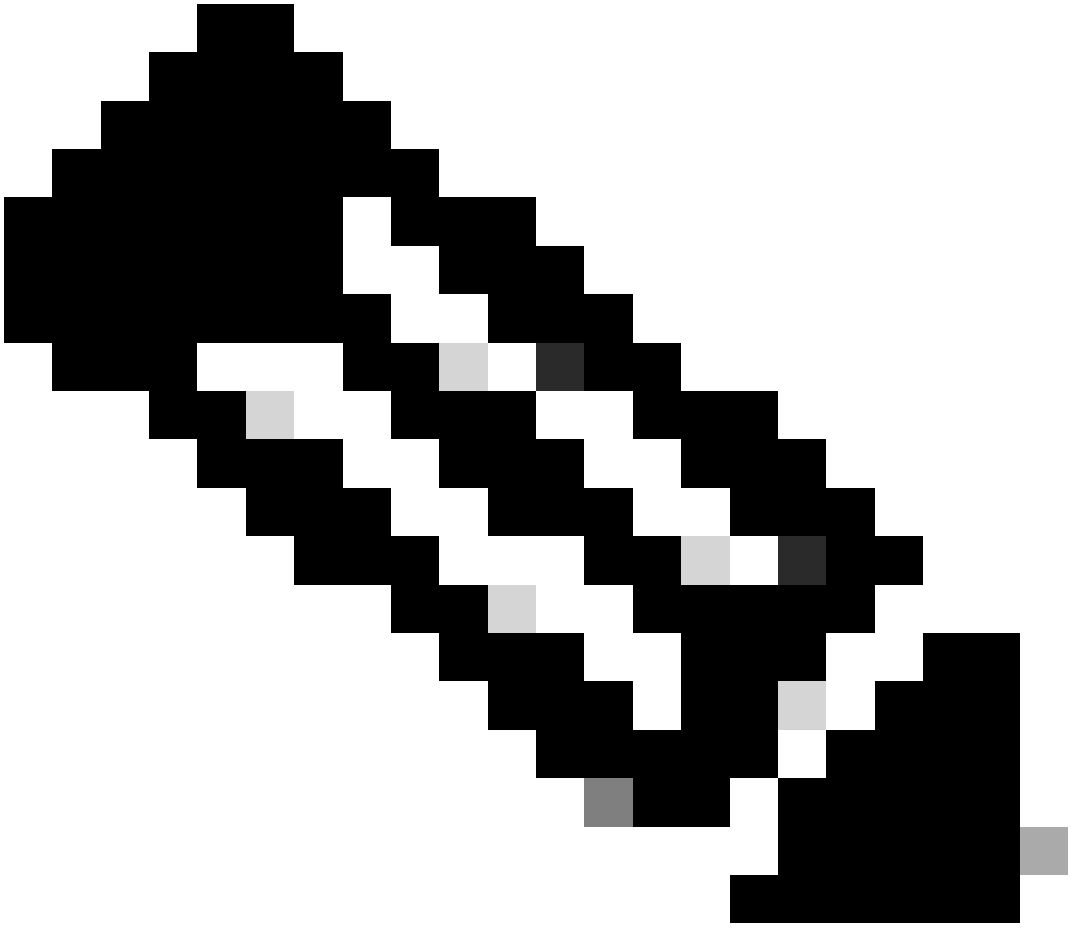


교정 권한 부여 규칙

에이전트 없는 권한 부여 규칙

Cisco ISE GUI에서 Menuicon(

)을 클릭하고 **Policy**(정책) > Policy Settings(**정책 설정)를 선택한** 다음 Authorization Policy(권한 부여 정책)**를 확장합니다.** 다음 세 가지 권한 부여 정책을 활성화하고 구성합니다.



참고: 이러한 권한 부여 규칙은 상태 흐름이 올바르게 작동하도록 지정된 순서로 구성해야 합니다.

알 수 없는 규정 준수 리디렉션:

•조건:

Network_Access_Authentication_Passed AND **Compliance_Unknown_Devices**를 결과가 Agentless Posture로 설정되도록 구성합니다. 이 조건은 에이전트 없는 플로우를 트리거합니다.

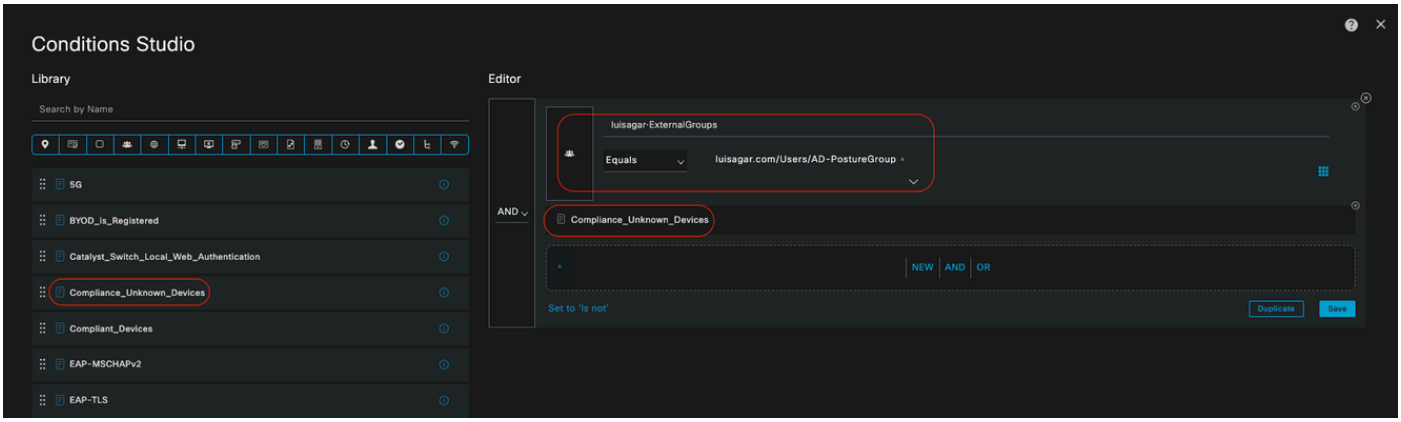
· 조건 예:

트래픽을 분할하려면 AD(Active Directory) 그룹 조건을 구성합니다.

Compliance_**Unknown_Devices 조건**은 초기 상태 상태를 알 수 없음으로 구성해야 합니다.

· 권한 부여 프로파일:

장치**가 Agentless Posture 흐름**을 통과하도록 하려면 이 권한 부여 규칙에 Agentless_Authorization_Profile을 할당합니다. 이 조건에는 에이전트 없는 흐름이 포함되어 있으므로 이 프로필을 적중하는 디바이스는 에이전트 없는 흐름을 시작할 수 있습니다.



알 수 없는 권한 부여 규칙

NonCompliant_Devices_Redirect:

· 조건: Network_Access_Authentication_Passed 및 Non_Compliant_Devices를 DenyAccess로 설정합니다. 또는 이 예에서 설명한 것처럼 교정 옵션을 사용할 수 있습니다.

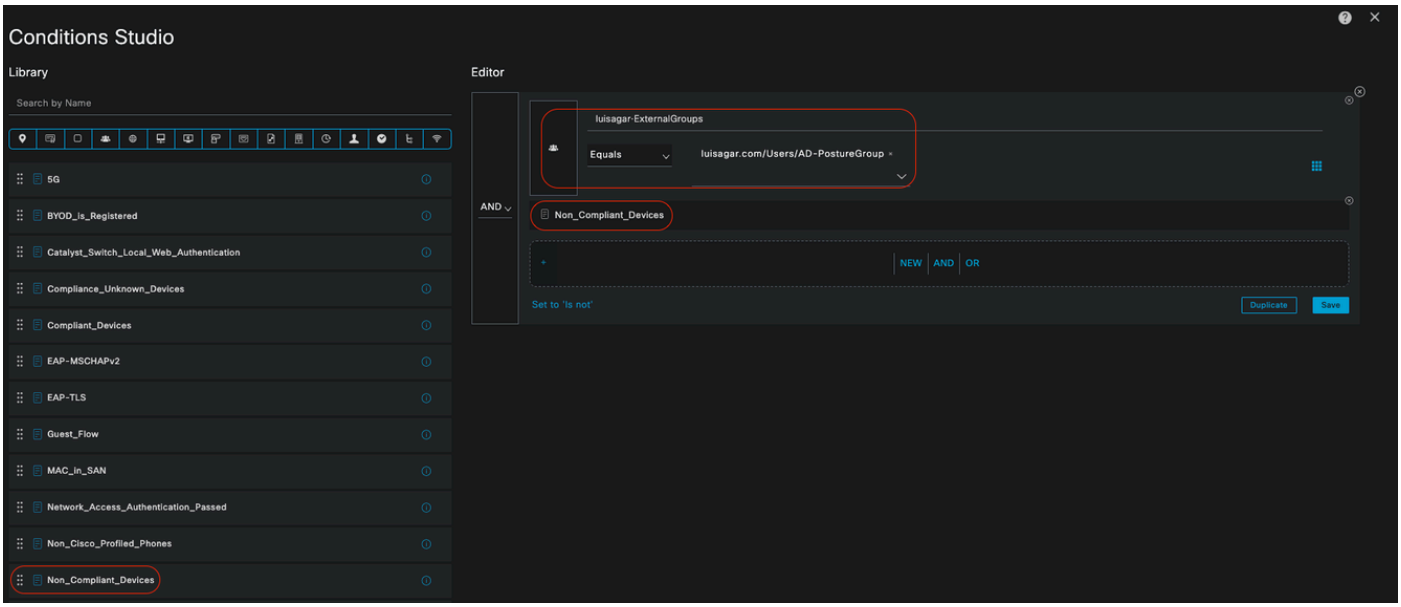
· 조건 예:

트래픽을 분할할 AD 그룹 조건을 구성합니다.

상태**가 비규격** 인 경우 제한 된 리소스를 할당 하는 Compliance_Unknown_Devices 조건을 구성 해야 합니다.

· 권한 부여 프로파일:

Remediation_**Authorization_Profile**을 이 권한 부여 규칙에 할당하여 **핫스팟** 포털을 통해 규정준수가 아닌 디바이스에 현재 상태를 알리거나 **액세스를 거부합니다**.



규정 미준수 권한 부여 규칙

Compliant_Devices_Access:

•조건:

결과가 PermitAccess로 설정된 Network_Access_Authentication_Passed 및 **Compliant**_Devices를 구성합니다.

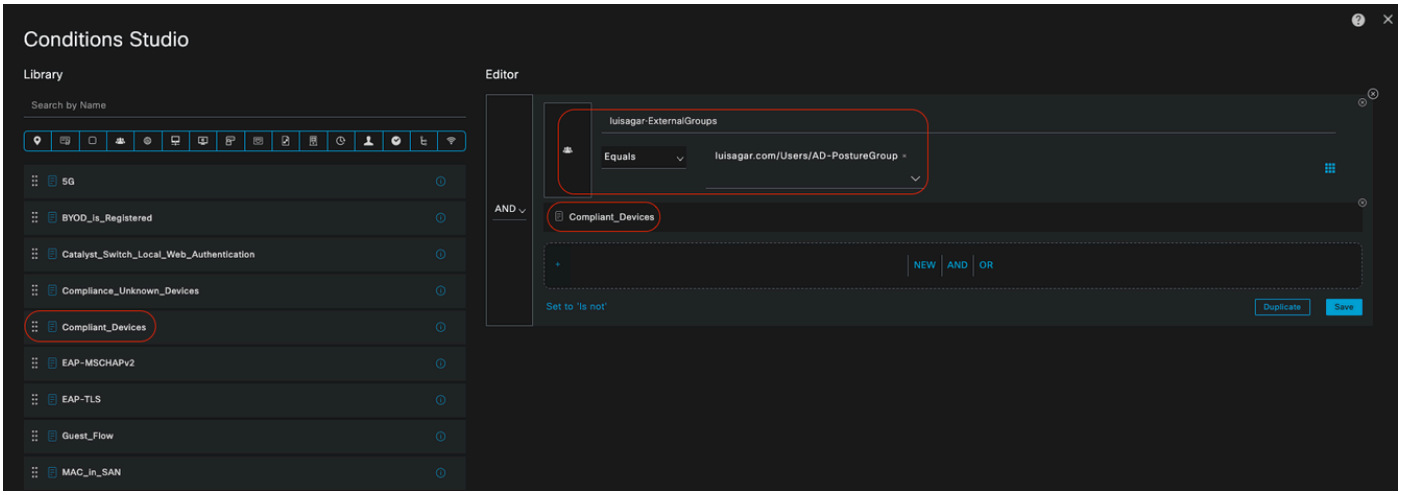
· 조건 예:

트래픽을 분할할 AD 그룹 조건을 구성합니다.

Compliance_**Unknown_Devices 조건**은 규정 준수 디바이스에 적절한 액세스 권한이 부여되도록 구성해야 합니다.

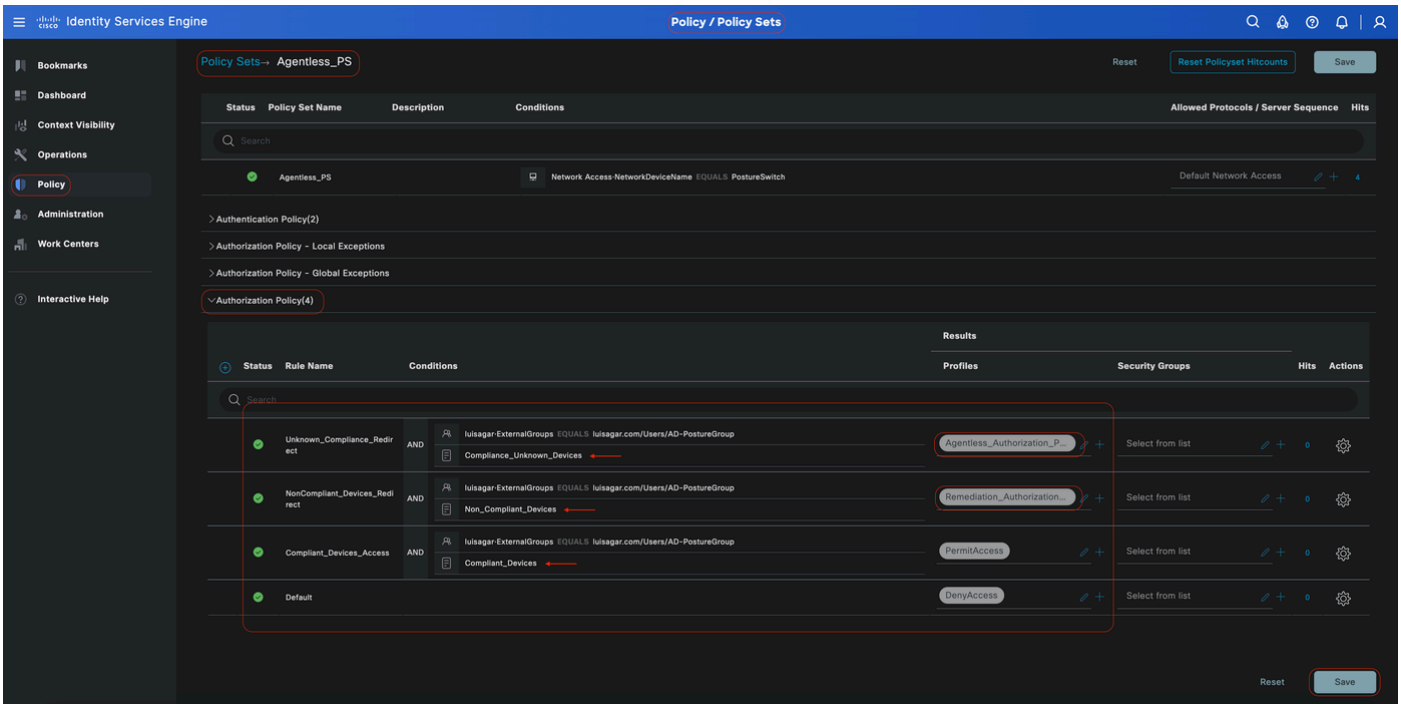
· 권한 부여 프로파일:

PermitAccess를 이 권한 부여 규칙에 할당하여 규격 장치의 액세스 권한을 확인합니다. 이 프로필은 조직의 요구에 맞게 사용자 지정할 수 있습니다.



호환 권한 부여 규칙

모든 권한 부여 규칙



권한 부여 규칙

엔드포인트 로그인 자격 증명 구성

Cisco ISE GUI에서 Menuicon( )을 클릭하고 **Administration(관리)** > Settings(**설정)** > Endpoint Scripts(**엔드포인트 스크립트**) > Login Configuration(로그인 컨피그레이션)을 **선택하고** 클라이언트**에 로그온할 클라이언트 자격 증명을 구성합니다.**

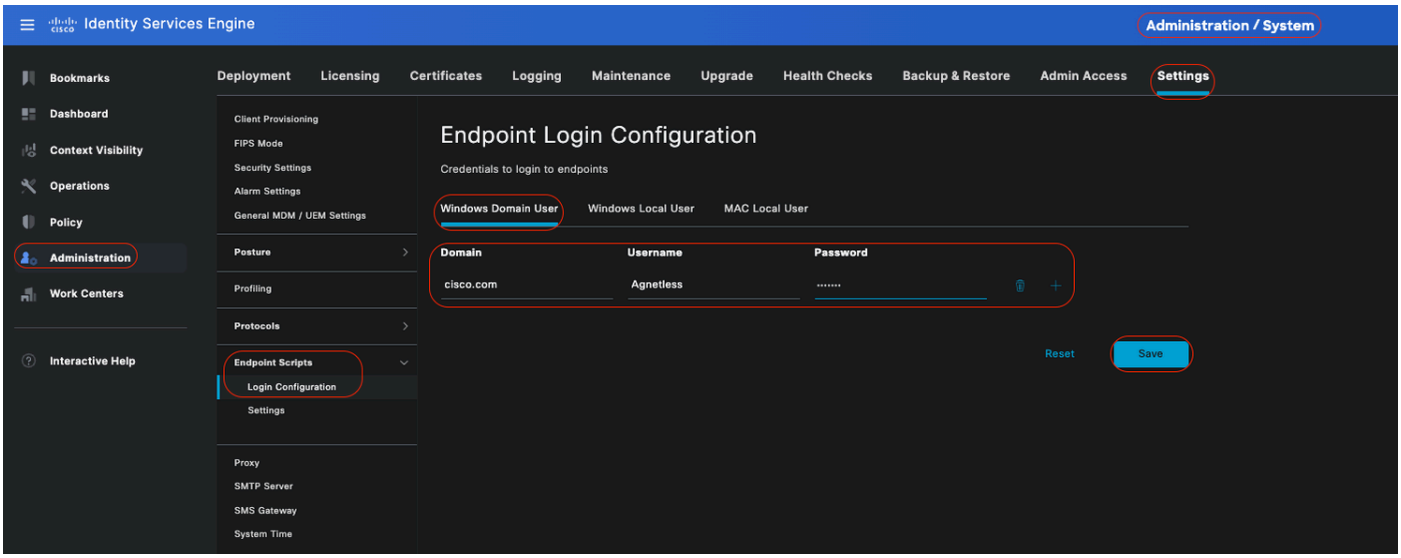
Cisco ISE가 클라이언트에 로그인할 수 있도록 엔드포인트 스크립트에서도 동일한 자격 증명을 사용합니다.

Windows 디바이스의 경우 처음 두 탭(**Windows 도메인 사용자 및 Windows 로컬 사용자**)만 구성합니다

- **Windows 도메인 사용자:**

Cisco ISE가 SSH를 통해 클라이언트에 로그인하는 데 사용해야 하는 도메인 자격 증명을 구성합니다. Plus(플러시콘)를 클릭하고 필요한 만큼 Windows 로그인을 입력합니다. 각 도메인에 대해 Domain, Username 및 Passwordfields에 필수 값을 입력합니다. 도메인 자격 증명을 구성하면 Windows 로컬 사용자 탭에 구성된 로컬 사용자 자격 증명이 무시됩니다.

Active Directory 도메인을 통해 에이전트 없는 상태 평가를 활용하는 Windows 엔드포인트를 관리하는 경우 로컬 관리 권한을 소유한 자격 증명과 함께 도메인 이름을 제공해야 합니다.

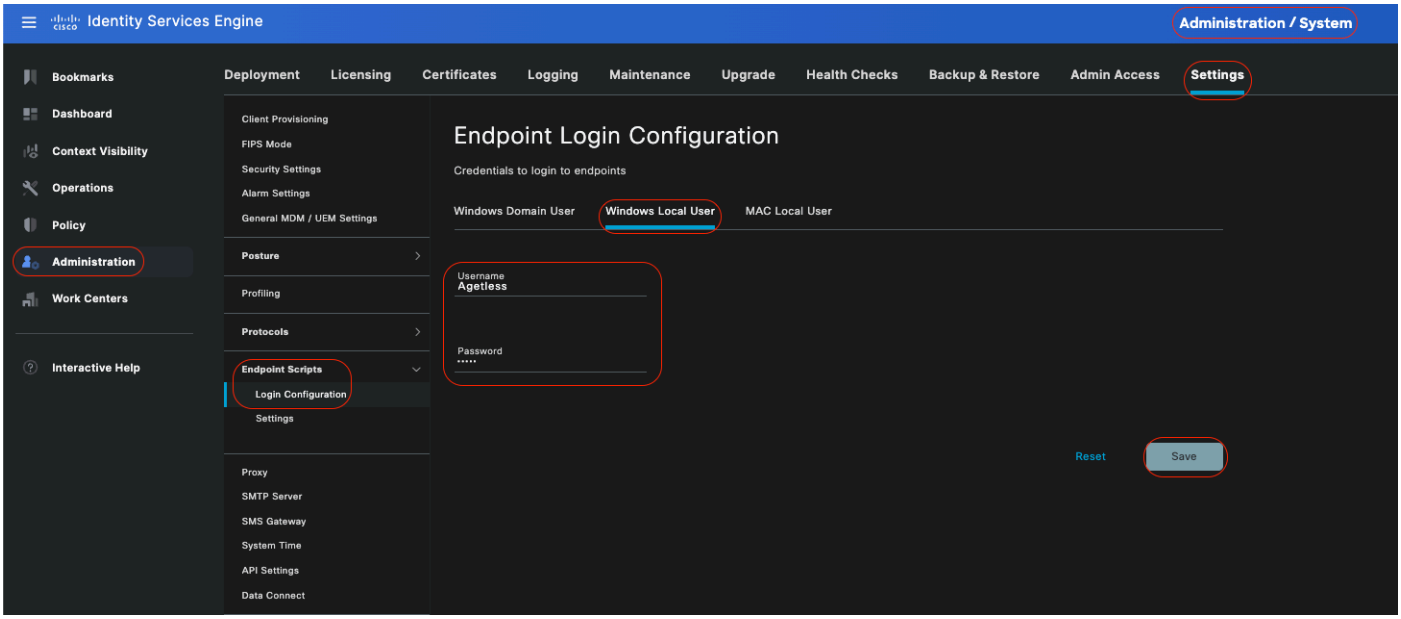


Windows 도메인 사용자

- **Windows 로컬 사용자:**

Cisco ISE가 SSH를 통해 클라이언트에 액세스하는 데 사용하는 로컬 계정을 구성합니다. 로컬 계정은 Powershell 및 Powershell 원격 계정을 실행할 수 있어야 합니다.

Active Directory 도메인을 통해 에이전트 없는 상태 평가를 사용하는 Windows 엔드포인트를 관리하지 **않는** 경우 로컬 관리 권한이 있는 자격 증명을 제공해야 합니다.

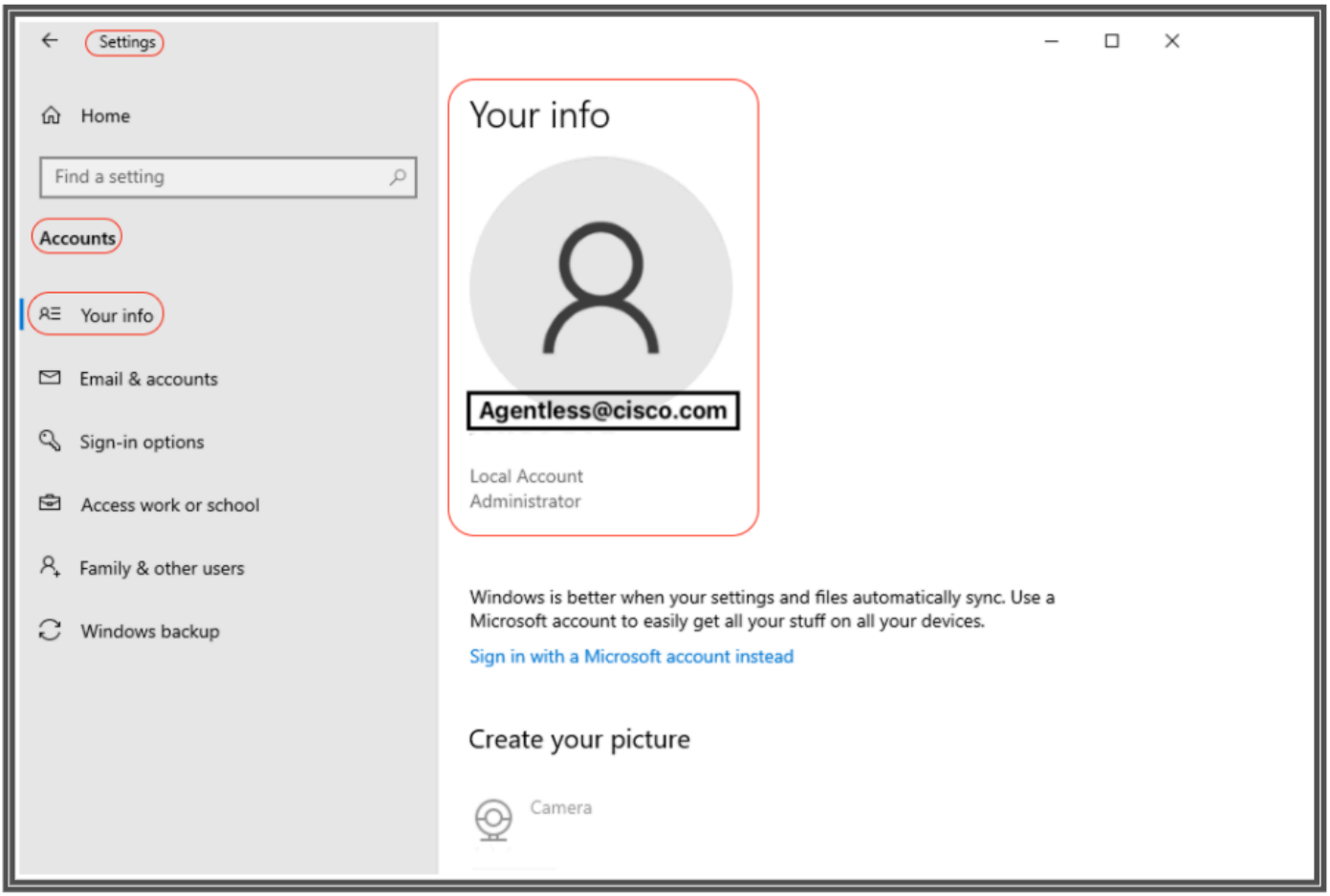


Windows 로컬 사용자

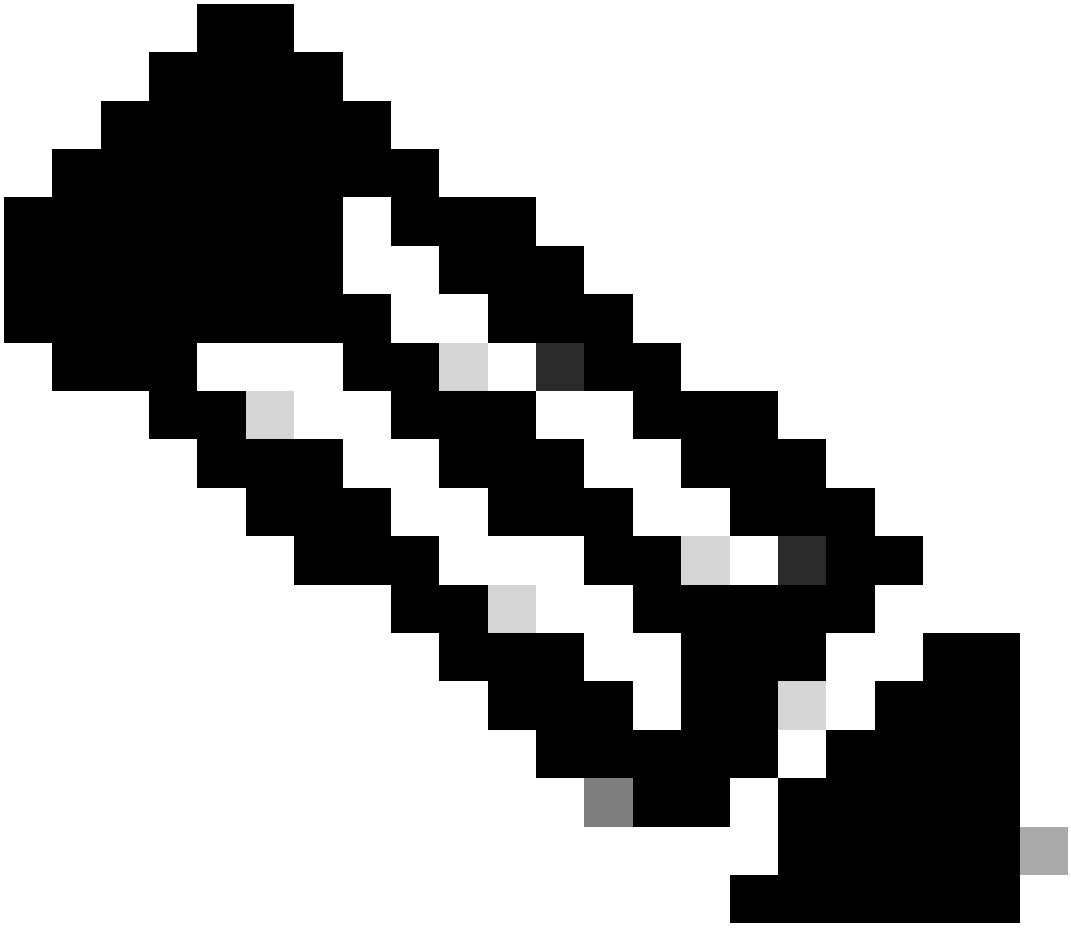
어카운트 확인

엔드포인트 로그인 자격 증명에서 적절한 데이터를 정확하게 추가할 수 있도록 Windows 도메인 사용자 및 Windows 로컬 사용자 계정을 확인하려면 다음 절차를 사용하십시오.

Windows 로컬 사용자: GUI(설정 앱) 사용 **WindowsStart** 버튼을 클릭하고 **설정**(톱니바퀴 아이콘)을 선택한 다음 **계정**을 클릭하고 사용자 정보를 선택합니다^.


Settings
Home
Find a setting
Accounts
Your info
Email & accounts
Sign-in options
Access work or school
Family & other users
Windows backup
Your info
Agentless@cisco.com
Local Account
Administrator
Windows is better when your settings and files automatically sync. Use a Microsoft account to easily get all your stuff on all your devices.
Sign in with a Microsoft account instead
Create your picture
Camera

계정 확인



참고: MacOS의 경우 **MAC Local User(MAC 로컬 사용자)**를 참조할 수 있습니다. 그러나 이 컨피그레이션 예에서는 MacOS 컨피그레이션이 표시되지 않습니다.

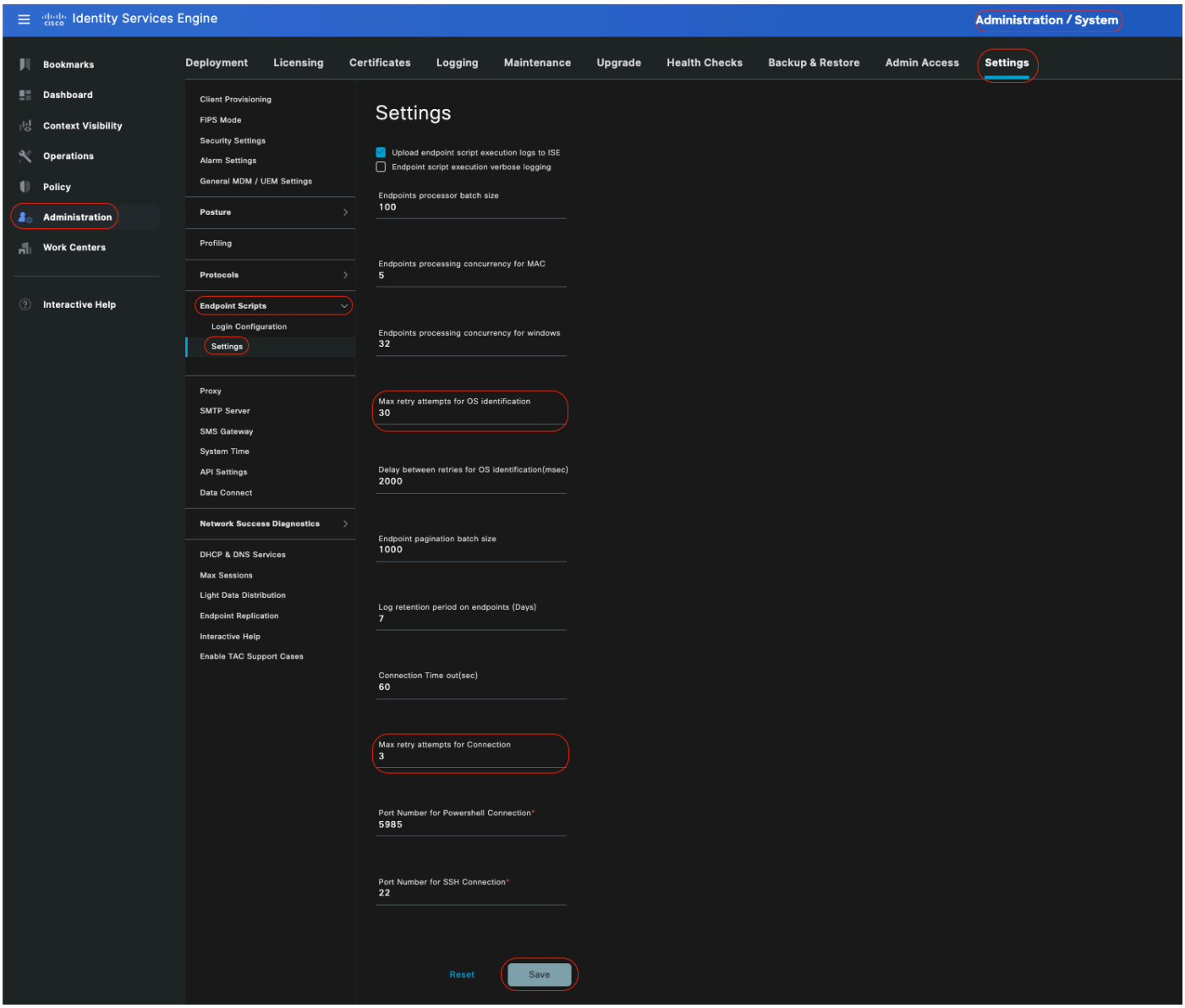
- **MAC 로컬 사용자:** Cisco ISE가 SSH를 통해 클라이언트에 액세스하기 위해 사용하는 로컬 계정을 구성합니다. 로컬 계정은 Powershell 및 Powershell 원격 계정을 실행할 수 있어야 합니다. 사용자 이름 필드에 로컬 계정의 계정 이름을 입력합니다.

Mac OS 계정 이름을 보려면 터미널에서 다음whoami 명령을 실행합니다.

설정

Cisco ISE GUI에서 Menuicon( )을 클릭하고 **Administration(관리) > Settings(설정) > Endpoint Scripts(엔드포인트 스크립트) > Settings(설정)를 선택하고** OS 식별에 대한 **최대 재시도 횟수**, OS 식별에 **대한 재시도 간격 지연 등을 구성합니다.** 이러한 설정에 따라 연결 문제를 확인할 수 있는 속도가 결정됩니다. 예를 들어, PowerShell 포트가 열려 있지 않다는 오류는 모든 재시도가 소진되지 않은 후에만 로그에 표시됩니다.

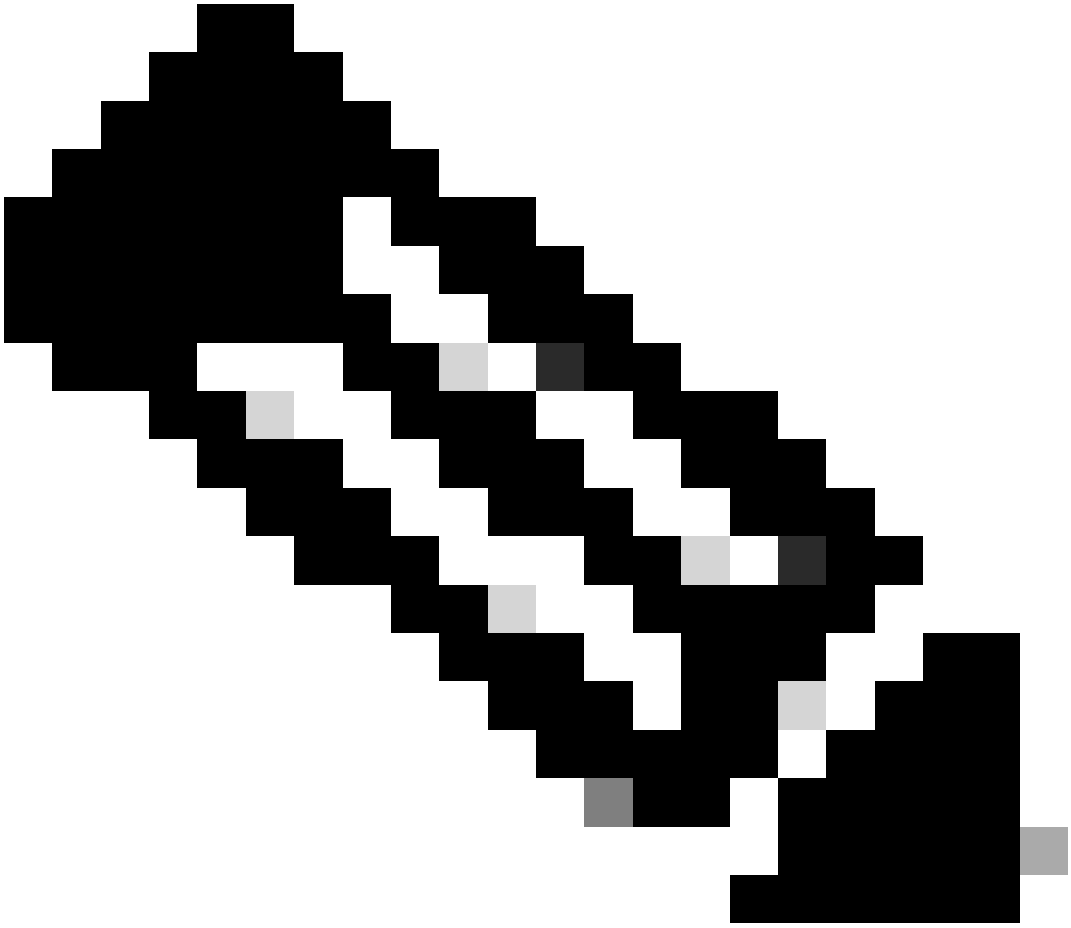
이 스크린샷은 기본값 설정을 보여줍니다.



엔드포인트 스크립트 설정

클라이언트가 에이전트 없는 상태로 연결할 때 라이브 로그에서 볼 수 있습니다.

Windows 끝점 구성 및 문제 해결



참고: Windows 장치에서 확인하고 적용해야 할 몇 가지 권장 사항입니다. 그러나 사용자 권한, PowerShell 액세스 등의 문제가 발생할 경우 Microsoft 설명서를 참조하거나 Microsoft 지원에 문의해야 합니다.

사전 요구 사항 확인 및 문제 해결

포트 5985에 대한 TCP 연결 테스트

Windows 클라이언트의 경우 클라이언트에서 powershell에 액세스하기 위한 포트 5985를 열어야 합니다. 이 명령을 실행하여 포트 5985에 대한 TCP 연결을 확인합니다. **Test-NetConnection -ComputerName localhost -Port 5985**

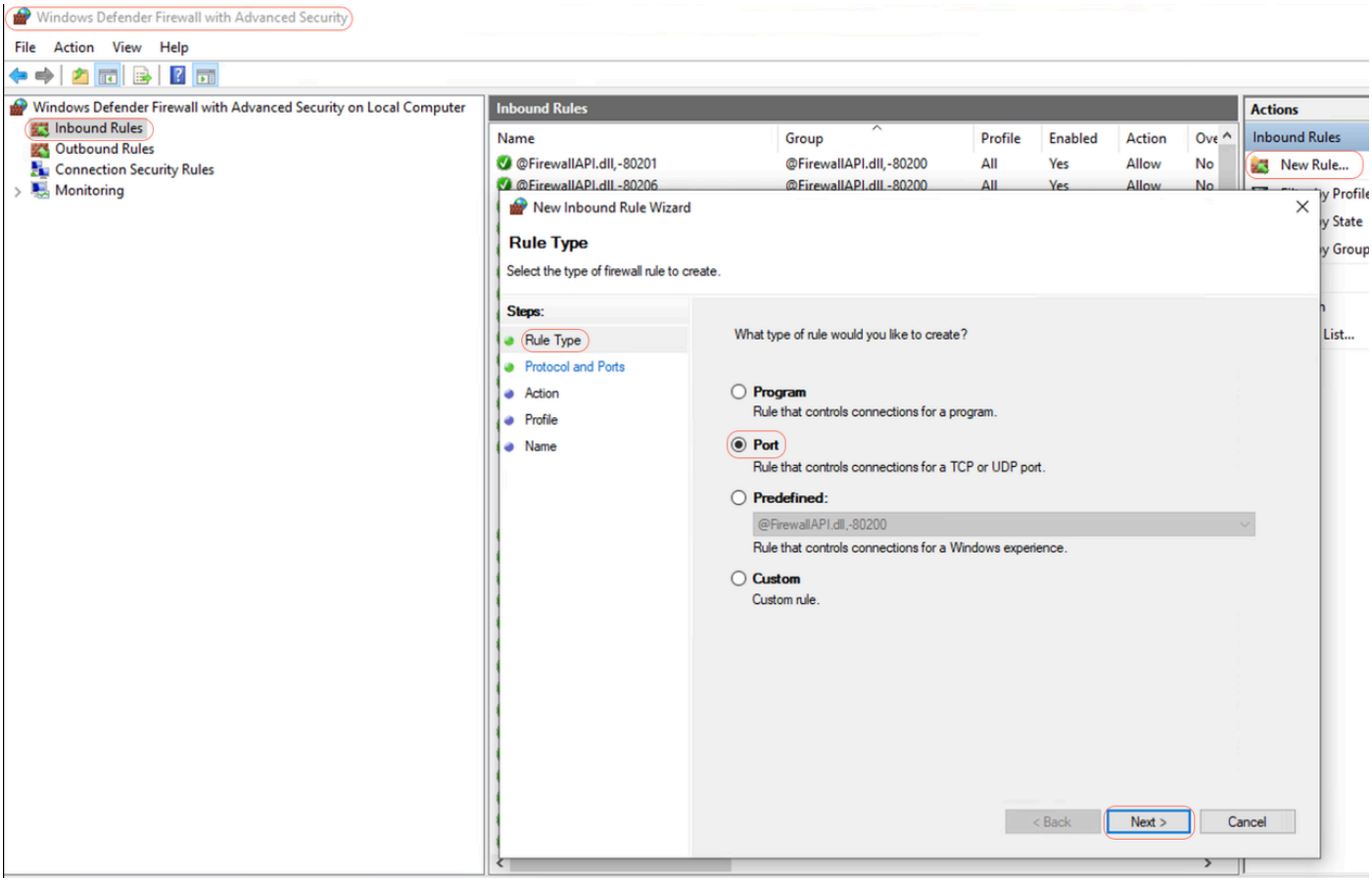
이 스크린샷에 표시된 출력은 localhost에서 포트 5985에 대한 TCP 연결이 실패했음을 나타냅니다. 즉, 포트 5985를 사용하는 WinRM(Windows Remote Management) 서비스가 실행되고 있지 않거나 올바르게 구성되어 있지 않습니다.

```
PS C:\Windows\system32> Test-NetConnection -Computer localhost -Port 5985
WARNING: TCP connect to (::1 : 5985) failed
WARNING: TCP connect to (127.0.0.1 : 5985) failed


ComputerName            : localhost
RemoteAddress           : ::1
RemotePort              : 5985
InterfaceAlias          : Loopback Pseudo-Interface 1
SourceAddress           : ::1
PingSucceeded           : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded        : False



PS C:\Windows\system32> ^C
```

Connection failed to WinRM

포트 5985에서 PowerShell을 허용하기 위한 인바운드 규칙 만들기

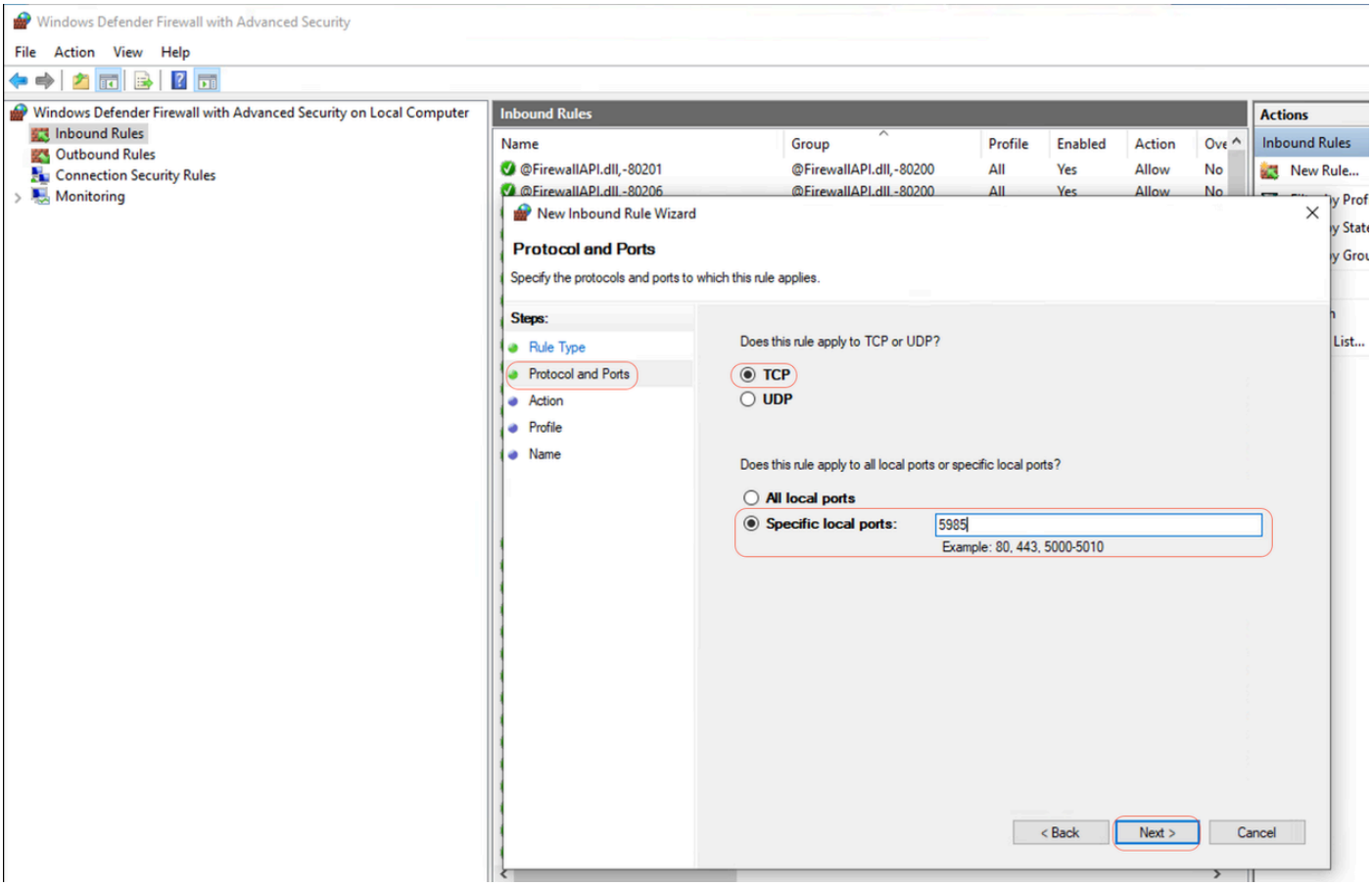
1단계- Windows GUI에서 검색 표시줄로 이동하여 Windows Firewall with Advanced Security를 입력하고 이를 클릭한 다음 Run as administrator(관리자로 실행) > Inbound Rules(인바운드 규칙) > New Rule(새 규칙) > Rule Type(규칙 유형) > Port(포트) > Next(다음)를 선택합니다.



새 인바운드 규칙 - 포트

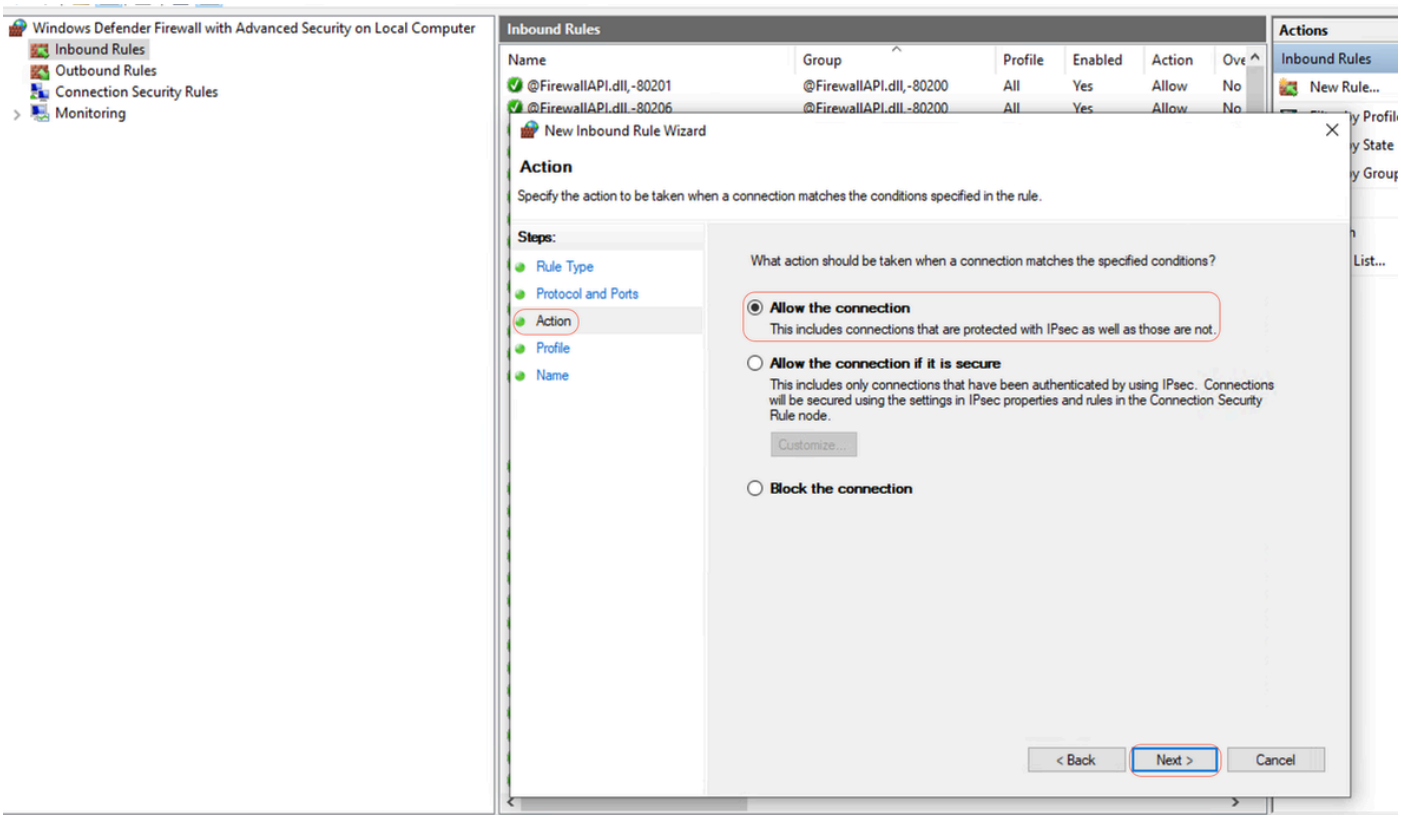
2단계- Protocols and Ports(프로토콜 및 포트)에서 TCP를 선택하고 Specify local ports(로컬 포트 지정)를 선택한 다음 포트 번호

5985(PowerShell 원격의 기본 포트)를 입력하고 Next(다음)**를 클릭합니다.**



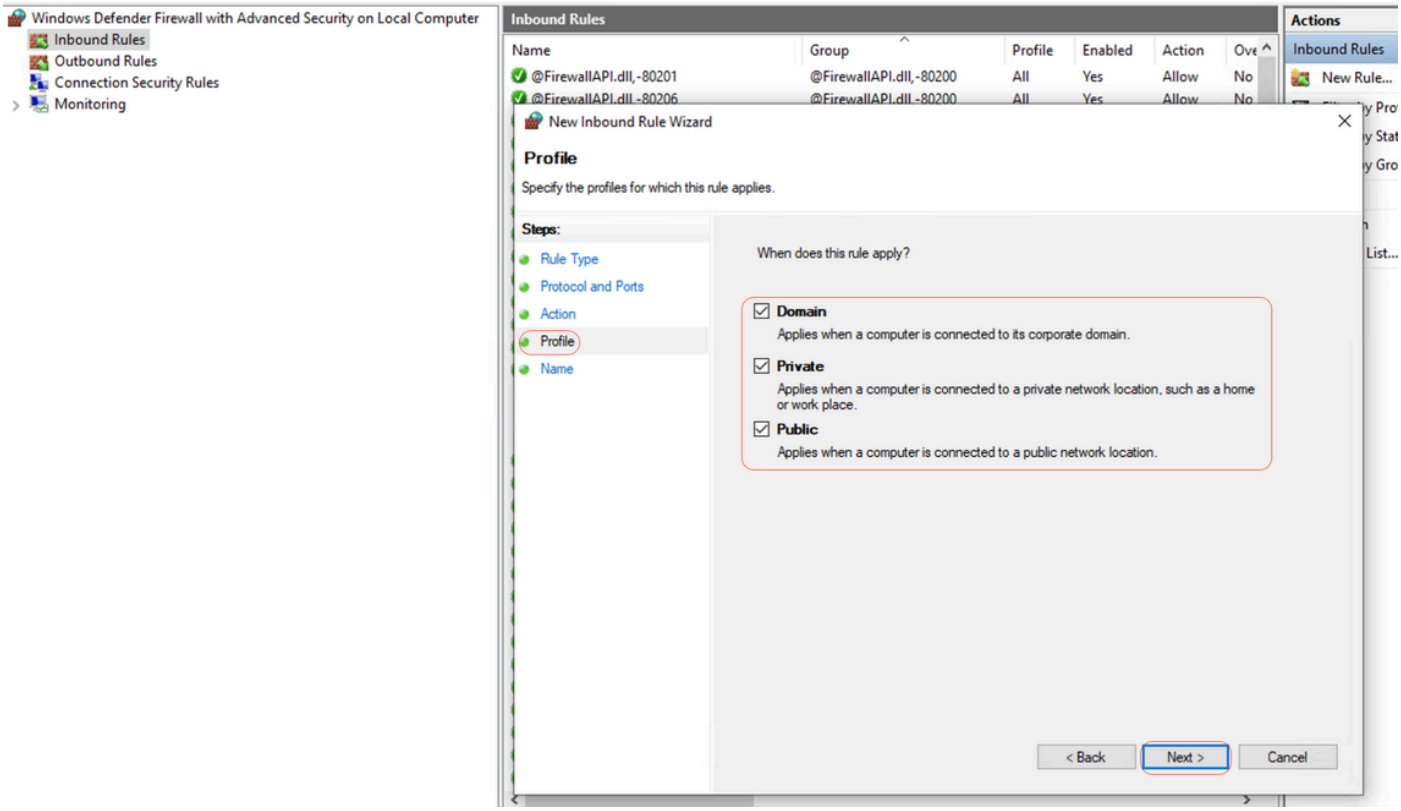
프로토콜 및 포트

3단계 - Action(작업) > **Allow** the connection(**연결 허용)** > Next(**다음**)**를 선택합니다**.



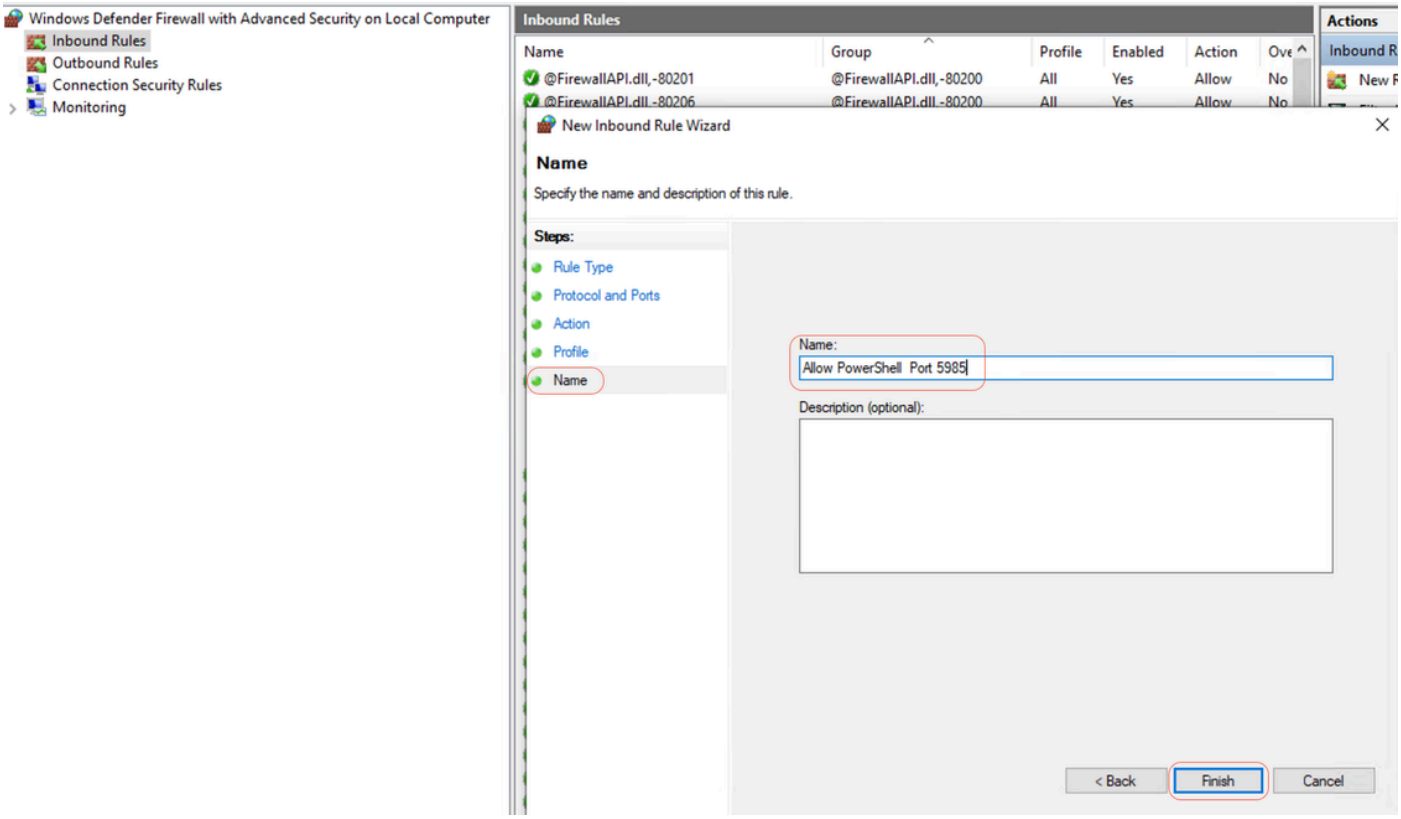
작업

4단계- Profile(프로필) 아래에서 Domain, Private, Public(**도메인, 프라이빗** 및 **퍼블릭) 확인란**을 선택하고 Next(다음)를 **클릭합니다.**



프로필

5단계- Name(**이름**)에서 Allow PowerShell on Port 5985(**포트 5985**에서 PowerShell 허용)와 같은 규칙 **이름을** 입력하고 **Finish(마침)**를 클릭합니다.

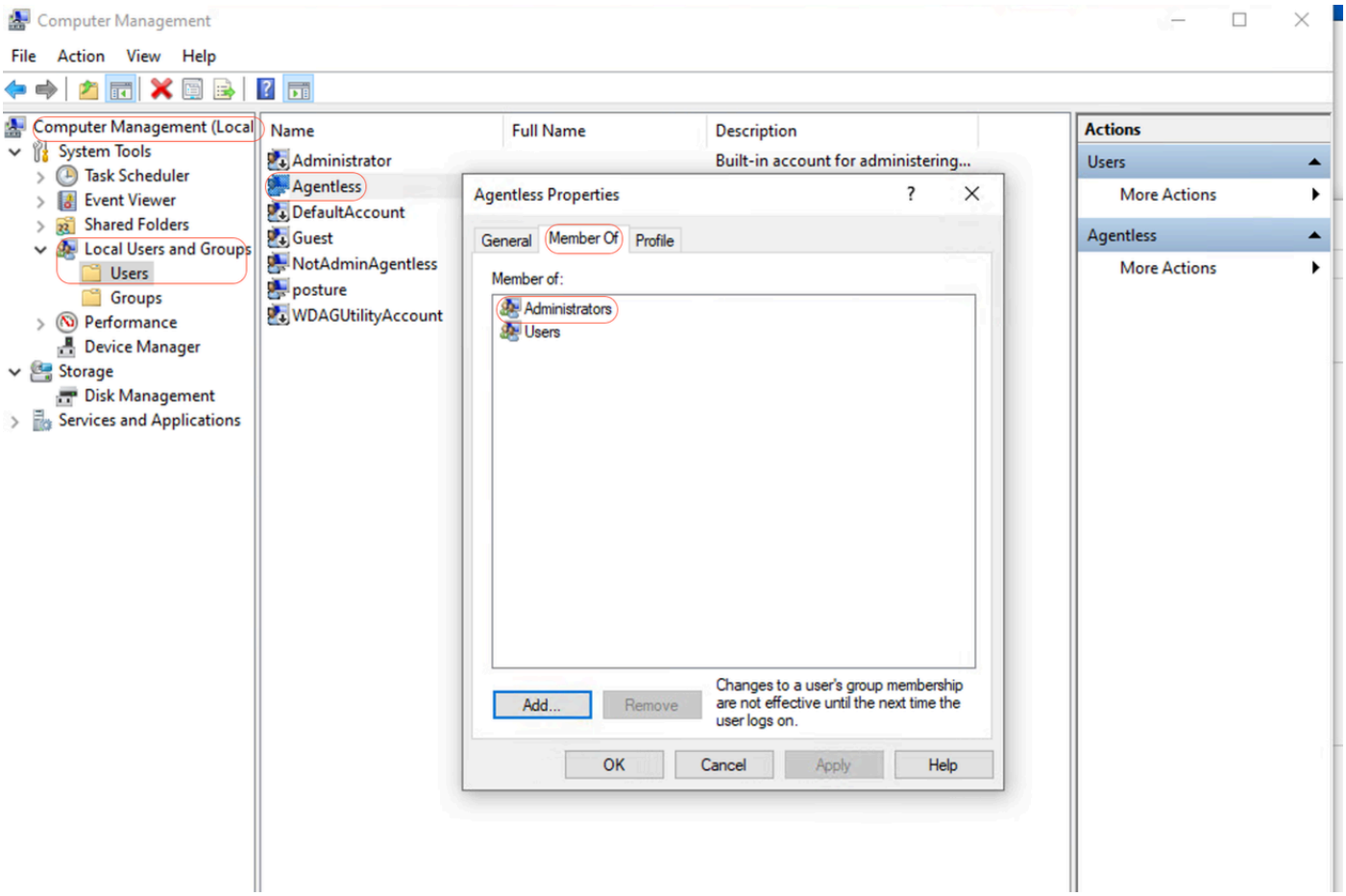


이름

셸 로그인을 위한 클라이언트 자격 증명에는 로컬 관리자 권한이 있어야 합니다

셸 로그인을 위한 클라이언트 자격 증명에는 로컬 관리자 권한이 있어야 합니다. 관리자 권한이 있는지 확인하려면 다음 단계를 확인하십시오.

Windows GUI에서 Settings(설정) > Computer Management(컴퓨터 관리) > Local Users and Groups(로컬 사용자 및 그룹) > Users(사용자) > Select the User Account(사용자 계정 선택)(이 예에서는 Agentless Account(에이전트 없는 계정)**가 선택됨)** > **Member of(구성원), Account must have Administrators Group(어카운트에 관리자 그룹이 있어야 함)으로** 이동합니다.



로컬 관리자 권한

WinRM 수신기 유효성 검사

WinRM 수신기가 포트 5985에서 **HTTP**에 대해 구성되었는지 **확인합니다**.

C: \Windows\system32> **winrm enumerate winrm/config/listener** Listener Address = * **Transport = HTTP Port = 5985** Hostname Enabled = true URLPrefix = wsman CertificateThumbprint C: \Windows\system32>

PowerShell 원격 WinRM 사용

서비스가 실행 중이고 자동으로 시작되도록 구성되었는지 확인하려면 다음 단계를 수행하십시오.

Enable the WinRM service **Enable-PSRemoting -Force** # Start the WinRM service **Start-Service WinRM** # Set the WinRM service to start

automatically **Set-Service -Name WinRM -StartupType Automatic**

예상 출력:

C: \Windows\system32> **Enable-PSRemoting -Force** WinRM is already set up to receive requests on this computer. WinRM has been updated for remote management. WinRM firewall exception enabled. -Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

C: \Windows\system32> **Start-Service WinRM**

C: \Windows\system32> **Set-Service -Name WinRM -StartupType Automatic**

Powershell은 v7.1 이상이어야 합니다. 클라이언트에는 cURL v7.34 이상이 있어야 합니다.

Windows에서 PowerShell 및 cURL 버전을 확인하는 방법

적절한 버전의 PowerShell을 사용하고 있는지 확인합니다. cURL은 에이전트 없는 상태를 위해 반드시 필요합니다.

PowerShell 버전 확인

Windows의 경우:

1. **개방형 PowerShell:**

・Win + X를 누르고 **Windows PowerShell 또는 Windows PowerShell(Admin)을 선택합니다**.

2. 다음 명령을 실행합니다.$PSVersionTable.PSVersion

・이 명령은 시스템에 설치된 PowerShell의 버전 세부 정보를 출력합니다.

cURL 버전 확인

Windows의 경우:

1. 명령 프롬프트 열기:

・Win + R을 누르고 cmd를 입력한 다음 Enter를 **클릭합니다**.

2. 명령을 실행합니다. curl --version

・시스템에 설치된 cURL 버전을 표시합니다.

Windows 디바이스에서 PowerShell 및 cURL 버전 확인을 위한 출력

C: \Windows\system32> **$PSVersionTable.PSVersion** Major Minor Build Revision ----- ----- ----- ----- 7 1 19041 4291

C: \Windows\system32>

C: \Windows\system32>

C: \Windows \system32>**curl --version curl 8.4.0 (Windows) libcurl/8.4.0 Schannel WinIDN** Release-Date: 2023-10-11 Protocols: dict file

ftp ftps http https imap imaps pop3 pop3s smtp smtps telnet tftp ftps http https Features: AsynchNS HSTS HTTPS-proxy IDN IPv6 Kerberos Largefile NTLM SPNEGO SSL SSPI threadsafe Unicode UnixSockets c: \Windows\system32>

추가 컨피그레이션

이 명령은 WinRM 연결을 위한 특정 원격 호스트를 신뢰하도록 시스템을 구성합니다. Set-Item WSMan:\localhost\Client\TrustedHosts -Value <Client-IP>

C: \Windows\system32> **Set-Item WSMan:\localhost\Client\TrustedHosts -Value x.x.x.x** WinRM Security Configuration. This command modifies the TrustedHosts list for the WinRM client. The computers in the TrustedHosts list cannot be authenticated. The client can send credential information to these computers. Are you sure that you want to modify this list? [Y] Yes [N] No [S] Suspend [?] Help (default is "y"): **Y** PS C: \Windows \system32> -

-Authentication Negotiate 및 -Credential 매개 변수와 함께 test-wsman cmdlet은 원격 컴퓨터에서 WinRM 서비스의 가용성 및 구성을 확인할 수 있는 강력한 도구입니다. test-wsman <Client-IP> -Authentication Negotiate -Credential <Accountname>

MacOS

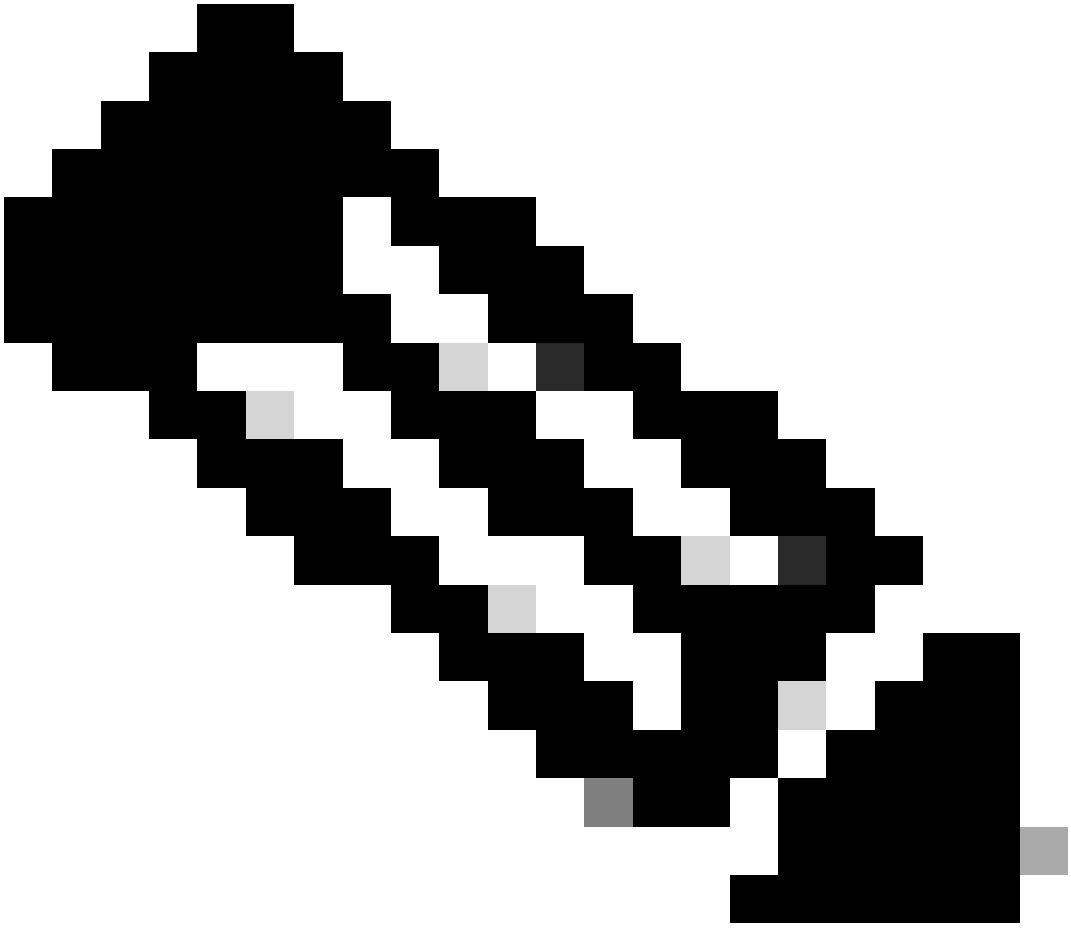
Powershell은 v7.1 이상이어야 합니다. 클라이언트에는 cURL v7.34 이상이 있어야 합니다.

macOS의 경우:

1. **개방터미널**

· **Applications(애플리케이션) > Utilities(유틸리티)**에서 터미널을 찾을 수 있습니다.

2. 명령을 실행합니다. pwsh -Command '$PSVersionTable.PSVersion'



참고: 참고: · PowerShell Core(pwsh)가 설치되어 있는지 확인하십시오. 그렇지 않은 경우 Homebrew를 통해 설치할 수 있습니다(Himebrew 설치 여부 확인). brew install --cask powershell

---

macOS의 경우:

1. **개방터미널**

· **Applications(애플리케이션) > Utilities(유틸리티)**에서 터미널을 찾을 수 있습니다.

2. 명령을 실행합니다. curl --version

· 이 명령은 시스템에 설치된 cURL 버전을 표시해야 합니다.

MacOS 클라이언트의 경우 클라이언트에 액세스하려면 SSH에 액세스하기 위한 포트 22가 열려 있어야 합니다

단계별 가이드:

1. **시스템 환경 설정 열기:**

・Apple 메뉴에서 **System** Preferences로 이동합니다.

2. **원격 로그인 활성화:**

・공유로 **이동합니다**.

・**원격 로그인** 옆의 상자를 **선택합니다**.

・**Allow access for(**액세스 **허용) 옵션**이 적절한 사용자 또는 그룹으로 설정되어 있는지 확인합니다. **All users**(**모든 사용자**)를 선택하면 Mac에서 유효한 계정을 가진 모든 사용자가 SSH를 통해 로그인할 수 있습니다.

3. **방화벽 설정 확인:**

・방화벽이 활성화된 경우 SSH 연결을 허용해야 합니다.

・**System** Preferences(**시스템 환경 설정) > Security & Privacy(보안 및 개인정보 보호) > Firewall(방화벽)로 이동합니다**.

・**Firewall Options(방화벽 옵션) 버튼**을 클릭합니다.

・**원격** 로그인 **또는 SSH**가 나열되고 허용되는지 확인합니다. 목록에 없는 경우 추가 버튼(+)을 클릭하여 추가합니다.

4. **터미널을 통한 개항 22(필요한 경우)**

・Applications(애플리케이션) > **Utilities(유틸리티)**에서 **터미널 애플리케이션을 엽니다**.

・pfctl 명령을 사용하여 현재 방화벽 규칙을 확인하고 포트 22가 열려 있는지 확인합니다. sudo pfctl -sr | grep 22

・포트 22가 열려 있지 않은 경우 SSH:echo "any에서 any 포트 22로 proto tcp 전달"을 허용하는 규칙을 수동으로 추가할 수 있습니다. | sudo pfctl -ef -

5. **SSH 액세스 테스트**

・다른 디바이스에서 터미널 또는 SSH 클라이언트를 엽니다.

・IP 주소를 사용하여 macOS 클라이언트에 연결을 시도합니다.ssh username@<macOS-client-IP>

・**사용자** 이름을 적절한 사용자 계정으로 바꾸고 <macOS-client-IP>를 macOS 클라이언트의 IP 주소로 바꿉니다.

MacOS의 경우 엔드포인트에서 인증서 설치 실패를 방지하려면 sudoers 파일에서 이 항목이 업데이트되어야 합니다.

macOS 엔드포인트를 관리할 때는 비밀번호 프롬프트 없이 특정 관리 명령을 실행할 수 있어야 합니다.

사전 요구 사항

・macOS 시스템에서 관리자 액세스

・Terminal 명령에 대한 기본 지식

Sudoers 파일 업데이트 단계

1. **개방터미널**

・**Applications(애플리케이션) > Utilities(유틸리티)**에서 터미널을 찾을 수 있습니다.

2. **Sudoers 파일을 편집합니다.**

・sudoers 파일을 안전하게 편집하려면 visudo 명령을 사용합니다. 이렇게 하면 파일을 저장하기 전에 구문 오류가 발생합니다

・관리자 암호를 입력하라는 메시지가 표시됩니다.

3. **해당 섹션을 찾습니다.**

・Visudo 편집기에서 사용자별 규칙이 정의된 섹션으로 이동합니다. 일반적으로 파일의 아래쪽을 향합니다.

4. **필수 항목을 추가합니다.**

・지정된 사용자에게 비밀번호 없이 security 및 osascript 명령을 실행할 수 있는 권한을 부여하려면 다음 행을 추가합니다
. <macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript

・**<macadminusername>**을 macOS 관리자의 실제 사용자 이름으로 바꿉니다.

5. **저장 및 종료:**

・기본 편집기(nano)를 사용하는 경우 Ctrl + X를 눌러 종료한 다음 Y를 눌러 변경 사항을 확인하고 마지막으로 Enter를 눌러 파일을 저장합니다.

・**vi 또는** vim을 사용하는 **경우** Esc 키를 누르고 :wq를 입력한 다음 Enter를 눌러 저장하고 종료합니다.

6. **변경 사항을 확인합니다.**

・변경 내용이 적용되도록 하려면 업데이트된 sudo 권한이 필요한 명령을 실행할 수 있습니다. 예를 들면 다음과 같습니다.

sudo /usr/bin/security find-certificate -a sudo /usr/bin/osascript -e 'tell application "Finder" to display dialog "Test"'

・이러한 명령은 암호를 묻는 메시지 없이 실행할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.