

# ISE 리디렉션 상태 구현

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[Connectiondata.xml](#)

[Call Home 목록](#)

[설계](#)

[구성](#)

[네트워크 디바이스 그룹\(선택 사항\)](#)

[네트워크 장치](#)

[클라이언트 프로비저닝](#)

[수동 프로비저닝\(사전 구축\)](#)

[클라이언트 프로비저닝 포털\(웹 구축\)](#)

[클라이언트 프로비저닝 정책](#)

[Authorization\(권한 부여\)](#)

[권한 부여 프로파일](#)

[권한 부여 정책](#)

[문제 해결](#)

[Cisco Secure Client 및 ISE에 적용할 수 없는 상태\(보류 중\)를 준수합니다.](#)

[부실/팬텀 세션](#)

[식별](#)

[솔루션](#)

[Performance](#)

[식별](#)

[솔루션](#)

[어카운팅](#)

[관련 정보](#)

## 소개

이 문서에서는 리디렉션 없는 상태 흐름 및 문제 해결 팁의 사용 및 컨피그레이션에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE의 상태 흐름
- ISE의 상태 구성 요소 구성
- ISE 포털로 리디렉션

나중에 설명하는 개념을 더 잘 이해하려면 다음 단계를 거치는 것이 좋습니다.

[이전 ISE 버전을 ISE 2.2의 ISE Posture Flow와 비교](#)  
[ISE 세션 관리 및 상태](#)

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 3.1
- Cisco Secure Client 5.0.01242

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 Posture 플로우는 다음 단계로 구성됩니다.

0. 인증/권한 부여 일반적으로 상태 흐름이 시작되기 직전에 수행되지만 PRA(Posture Reassessment)와 같은 특정 활용 사례에 대해서는 우회할 수 있습니다. 인증 자체가 포스처 검색을 트리거하지 않으므로 이는 모든 포스처 플로우에 필수적인 것으로 간주되지 않습니다.

1. 검색. 현재 활성 세션의 PSN 소유자를 찾기 위해 Secure Client ISE Posture 모듈이 수행하는 프로세스입니다.
2. 클라이언트 프로비저닝. 해당 Cisco Secure Client(이전의 AnyConnect) ISE Posture 모듈 및 Compliance Module 버전으로 클라이언트를 프로비저닝하기 위해 ISE에서 수행하는 프로세스입니다. 이 단계에서는 특정 PSN에 포함되어 서명된 상태 프로파일의 로컬 복사본도 클라이언트에 푸시됩니다.
3. 시스템 검사. ISE에 구성된 포스처 정책은 규정 준수 모듈에 의해 평가됩니다.
4. 교정(선택 사항). 포스처 정책이 규정을 준수하지 않을 경우 수행됩니다.
5. 코에이 최종(Compliant 또는 Not Compliant) 네트워크 액세스를 부여하려면 재인증이 필요합니다.

이 문서에서는 ISE Posture 플로우의 검색 프로세스를 중점적으로 살펴봅니다.

검색 프로세스에는 리디렉션을 사용하는 것이 좋지만, 리디렉션이 지원되지 않는 서드파티 네트워크 디바이스를 사용하는 경우와 같이 리디렉션을 구현할 수 없는 경우가 있습니다. 이 문서에서는 이러한 환경에서 리디렉션 없는 상태를 구현하고 트러블슈팅하기 위한 일반적인 지침 및 모범 사례를 제공하는 것을 목적으로 합니다.

리디렉션 없는 플로우에 대한 전체 설명은 ISE [2.2에서 이전 ISE 버전을 ISE Posture 플로우와 비교에 설명되어 있습니다.](#)

리디렉션을 사용하지 않는 두 가지 유형의 상태 검색 프로브가 있습니다.

- 1. Connectiondata.xml
- 2. Call Home 목록

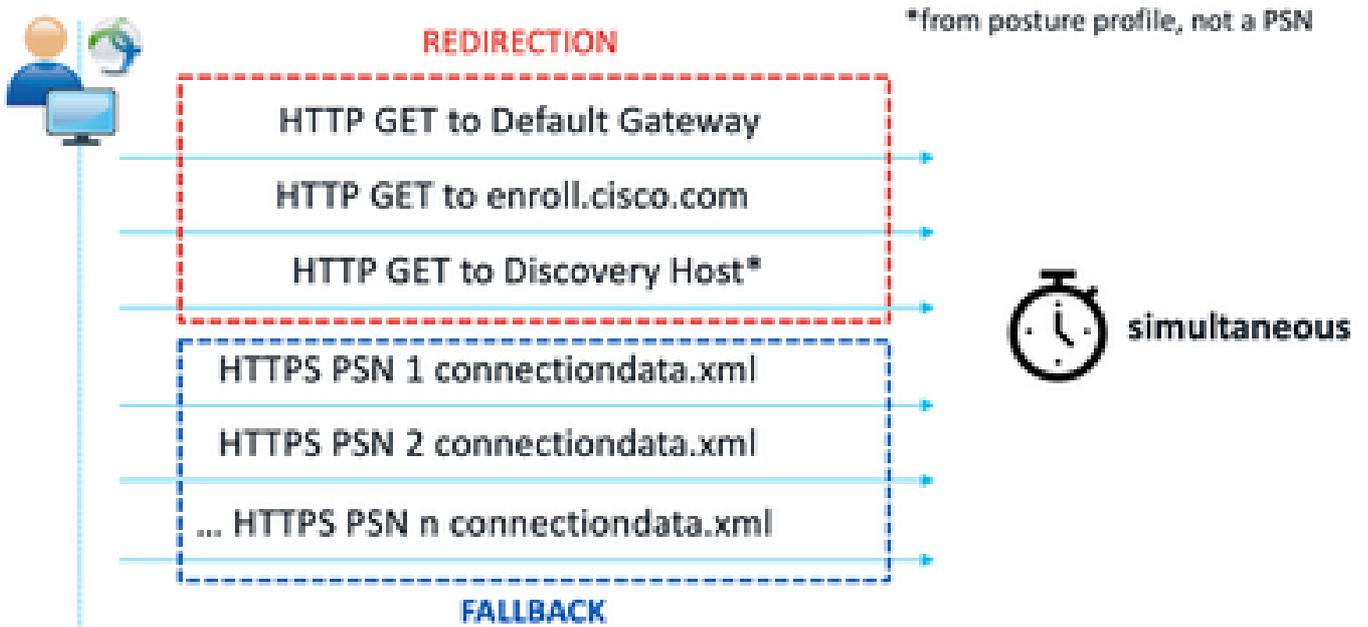
### Connectiondata.xml

Connectiondata.xml은 Cisco Secure Client에서 자동으로 생성 및 관리되는 파일입니다. 클라이언트가 이전에 포스처를 위해 성공적으로 연결한 PSN 목록으로 구성됩니다. 따라서 이 파일은 로컬 파일일 뿐이며 모든 엔드포인트에서 내용이 지속적이지 않습니다.

connectiondata.xml의 주요 목적은 1단계 및 2단계 검색 프로브에 대한 백업 메커니즘으로 작동하는 것입니다. 리디렉션 또는 Call Home List 프로브가 활성 세션이 있는 PSN을 찾을 수 없는 경우 Cisco Secure Client는 connectiondata.xml에 나열된 각 서버에 직접 요청을 보냅니다.

## Stage 1 discovery probes

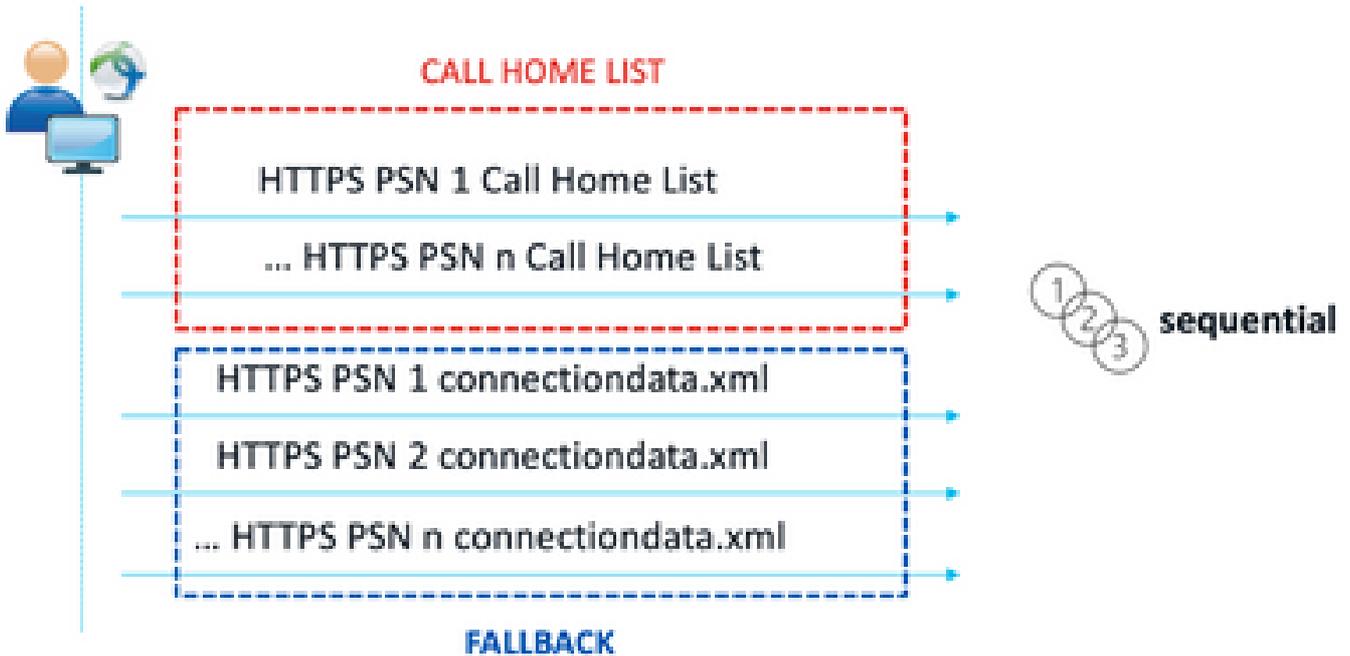
### No-MnT stage probes



1단계 검색 프로브

# Stage 2 discovery probes

## MnT stage probes



### 2단계 검색 프로브

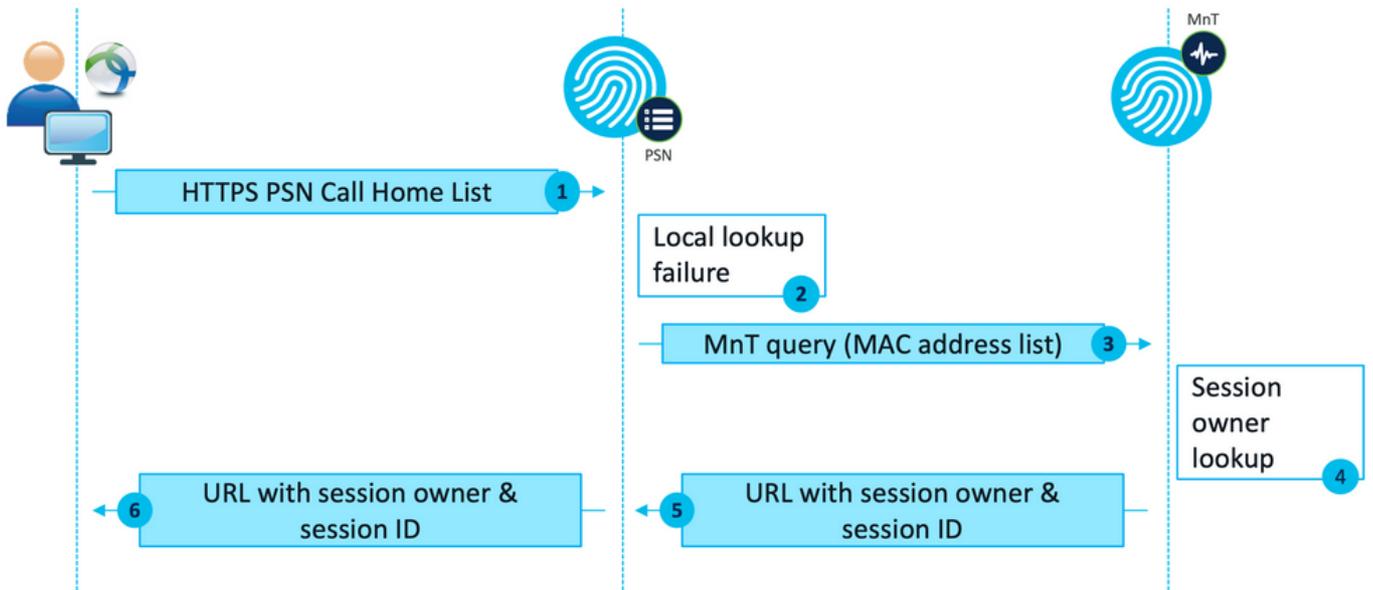
connectiondata.xml 프로브의 사용으로 인해 발생하는 일반적인 문제는 엔드포인트에서 보낸 HTTPS 요청이 많아 ISE 구축에 과부하가 발생하는 것입니다. connectiondata.xml은 리디렉션 및 리디렉션 없는 상태 메커니즘 모두에 대한 전체 종단을 방지하기 위한 백업 메커니즘으로서 효과적이지만, 상태 환경에 대한 지속 가능한 솔루션이 아니므로, 기본 검색 프로브의 실패를 야기하고 검색 문제를 초래하는 설계 및 컨피그레이션 문제를 진단하고 해결해야 합니다.

### Call Home 목록

Call Home List(콜 홈 목록)는 포스터에 사용하도록 PSN 목록이 지정된 포스터 프로필의 섹션입니다. connectiondata.xml과 달리 이 파일은 ISE 관리자가 생성 및 유지 관리하며 최적의 구성을 위해 설계 단계가 필요할 수 있습니다. Call Home List(콜 홈 목록)의 PSN 목록은 RADIUS를 위한 네트워크 디바이스 또는 로드 밸런서에 구성된 인증 및 어카운팅 서버 목록과 일치해야 합니다.

Call Home List 프로브는 PSN에서 로컬 조회가 실패할 경우 활성 세션 검색 중에 MnT 조회를 사용할 수 있도록 합니다. 단계 2 검색 중에 사용되는 경우에만 connectiondata.xml 프로브에도 동일한 기능이 확장됩니다. 이러한 이유로 2단계 프로브는 모두 New Generation 프로브라고도 합니다.

## MnT lookup



MnT 조회 흐름

## 설계

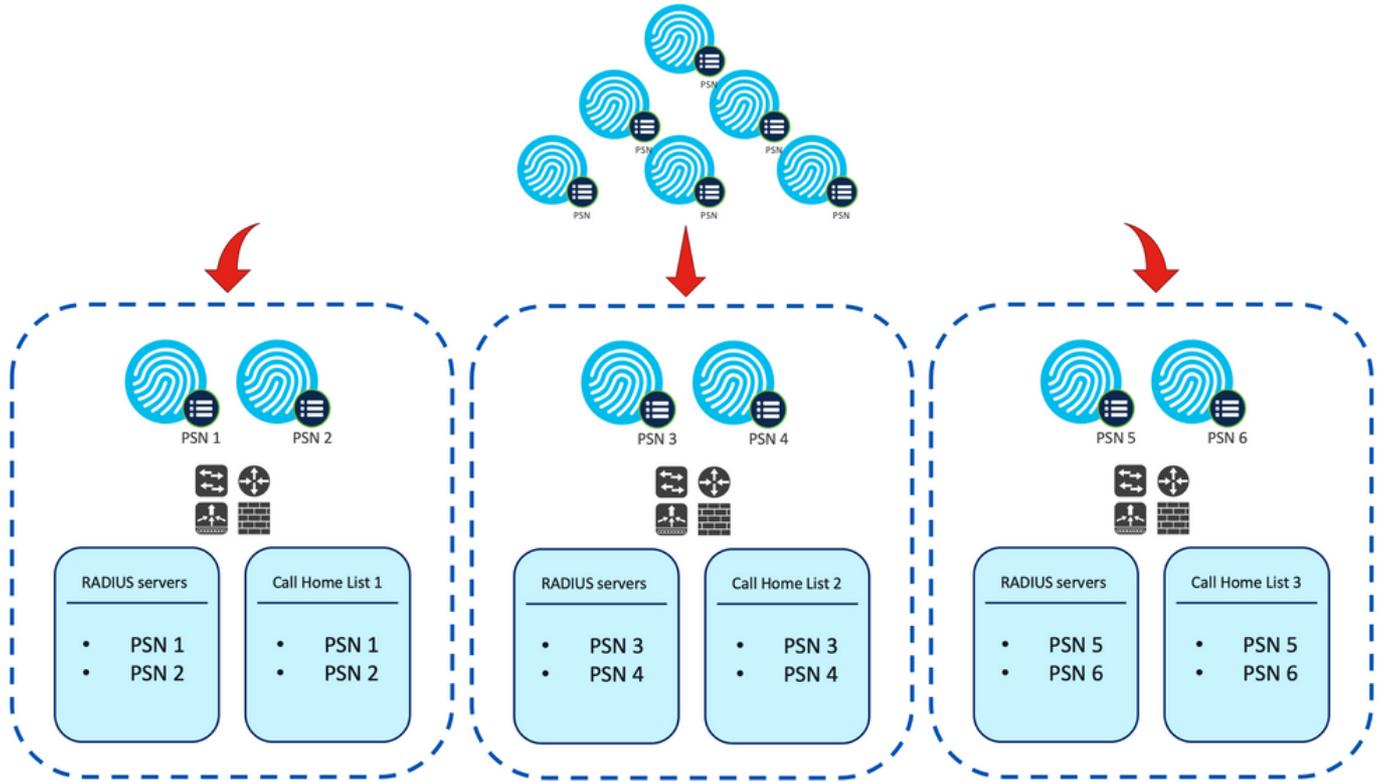
리디렉션 없는 검색 프로세스에는 리디렉션 플로우에 비해 PSN 및 MnT에서 더 복잡한 플로우와 더 많은 양의 처리가 수반되므로, 구현 중에 발생할 수 있는 두 가지 일반적인 문제가 있습니다.

1. 효과적인 검색
2. ISE 구축의 성능

이러한 과제에 대응하려면 특정 엔드포인트가 포스처에 사용할 수 있는 PSN 수를 제한하도록 Call Home 목록을 설계하는 것이 좋습니다. 중간 규모 및 대규모 구축의 경우 PSN 수가 감소된 여러 Call Home 목록을 생성하려면 구축을 분산해야 합니다. 따라서 특정 네트워크 디바이스에 대한 RADIUS 인증에 사용되는 PSN 목록을 해당 Call Home 목록과 일치하도록 동일한 방법으로 제한해야 합니다.

각 Call Home 목록에서 최대 PSN 수를 결정하기 위해 PSN 배포 전략을 개발할 때 다음 측면을 고려할 수 있습니다.

- 구축의 PSN 수
- PSN 및 MnT 노드의 하드웨어 사양
- 구축의 최대 동시 포스처 세션 수
- 네트워크 디바이스 수
- 하이브리드 환경(동시 리디렉션 및 리디렉션 없는 상태 구현)
- 엔드포인트에서 사용하는 어댑터 수
- 네트워크 디바이스 및 PSN의 위치
- 상태(유선, 무선, VPN)에 사용되는 네트워크 연결 유형



예. 리디렉션 없는 상태를 위한 PSN 배포

팁: [네트워크 디바이스 그룹](#)을 사용하여 설계에 따라 네트워크 디바이스를 분류합니다.

## 구성

### 네트워크 디바이스 그룹(선택 사항)

네트워크 디바이스 그룹은 네트워크 디바이스를 식별하고 해당 RADIUS 서버 목록 및 Call Home 목록과 매칭하는 데 사용할 수 있습니다. 하이브리드 환경의 경우, 그렇지 않은 디바이스에서 리디렉션을 지원하는 디바이스를 식별하는 데에도 사용될 수 있습니다.

설계 단계에서 개발된 배포 전략이 네트워크 디바이스 그룹을 사용하는 경우 다음 단계에 따라 ISE에서 구성합니다.

1. Administration > Network Resources Network Resource Groups로 이동합니다.
2. Add(추가)를 클릭하여 새 그룹을 추가하고 이름을 입력한 다음 해당되는 경우 상위 그룹을 선택합니다.
3. 2단계를 반복하여 필요한 모든 그룹을 생성합니다.

이 가이드에서 사용하는 예에서는 위치 장치 그룹을 사용하여 RADIUS 서버 목록 및 콜 홈 목록을 식별하고 사용자 지정 포스처 장치 그룹을 사용하여 리디렉션 없는 포스처 장치에서 리디렉션을 식별합니다.

<input type="checkbox"/> Name	Description	No. of Network Devices
<input type="checkbox"/> > All Device Types	All Device Types	--
<input type="checkbox"/> > All Locations	All Locations	--
<input type="checkbox"/> > US		0
<input type="checkbox"/> CENTRAL		0
<input type="checkbox"/> EST		1
<input type="checkbox"/> WEST		1
<input type="checkbox"/> > Is IPSEC Device	Is this a RADIUS over IPSEC Device	--
<input type="checkbox"/> > Posture	Posture redirection or redirectionless group	--
<input type="checkbox"/> Redirection		0
<input type="checkbox"/> Redirectionless		1

네트워크 장치 그룹

## 네트워크 장치

1. RADIUS 인증, 권한 부여 및 계정 관리를 위해 네트워크 디바이스를 구성해야 합니다. 컨피그 레이션 단계는 각 공급업체 설명서를 참조하십시오. 해당 Call Home List(콜 홈 목록)에 따라 RADIUS 서버 목록을 구성합니다.
2. ISE에서 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동하고 Add(추가)를 클릭합니다. 설계에 따라 네트워크 디바이스 그룹을 구성하고 RADIUS 인증 설정을 활성화하여 공유 암호를 구성합니다.

• Device Profile Cisco

Model Name

Software Version

• Network Device Group

Location	WEST	<input type="button" value="Set To Default"/>
IPSEC	No	<input type="button" value="Set To Default"/>
Device Type	All Device Types	<input type="button" value="Set To Default"/>
Posture	Redirectionless	<input type="button" value="Set To Default"/>

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

• Shared Secret

네트워크 디바이스 컨피그레이션

### 클라이언트 프로비저닝

리디렉션 없는 환경에서 포스처를 수행할 수 있는 올바른 소프트웨어 및 프로필을 클라이언트에 프로비저닝하는 방법에는 두 가지가 있습니다.

1. 수동 프로비저닝(사전 구축)
2. 클라이언트 프로비저닝 포털(웹 구축)

## 수동 프로비저닝(사전 구축)

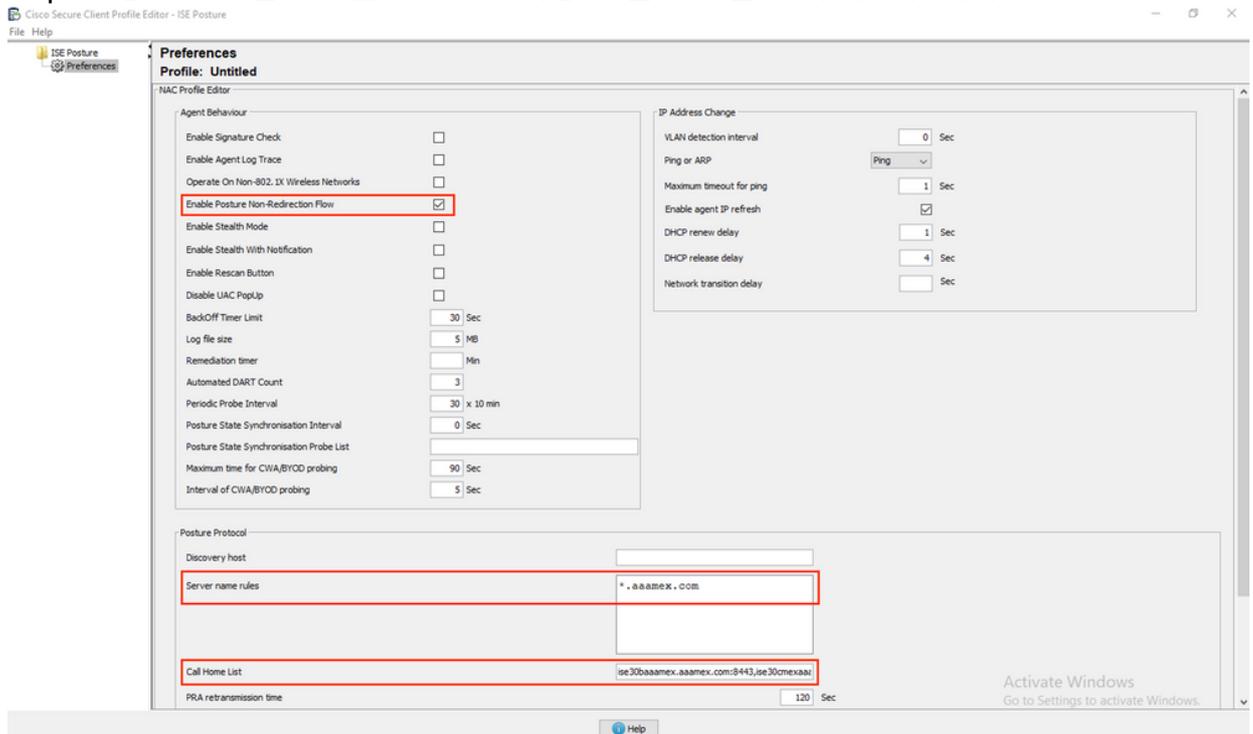
### 1. Cisco Software Download에서 Cisco Secure Client Profile Editor를 다운로드하고 설치합니다



프로파일 편집기 패키지

### 2. ISE Posture 프로파일 편집기를 엽니다.

- Enable Posture Non-Redirection Flow(포스처 비리디렉션 플로우 활성화)가 활성화되어 있는지 확인합니다.
- 쉽표로 구분된 서버 이름 규칙을 구성합니다. PSN에 대한 연결을 허용하려면 단일 별표 (\*)를 사용하고, 특정 도메인의 PSN에 대한 연결을 허용하려면 와일드카드 값을 사용하거나, 특정 PSN에 대한 연결을 제한하려면 PSN FQDN을 사용합니다.
- 쉽표로 구분된 PSN 목록을 지정하도록 Call Home List를 구성합니다. FQDN:port 또는 IP:port 형식으로 클라이언트 프로비저닝 포털 포트를 추가해야 합니다.



프로파일 편집기를 통한 포스처 프로파일 컨피그레이션

참고: 필요한 경우 클라이언트 프로비저닝 포털 포트를 확인하는 방법에 대한 지침은 클라이언트 프로비저닝 정책 섹션의 4단계를 참조하십시오.

### 3. 사용 중인 각 Call Home 목록에 대해 2단계를 반복합니다.

### 4. Cisco Software Download에서 Cisco Secure Client 사전 구축 패키지를 다운로드합니다.

### Cisco Secure Client 사전 구축 패키지

5. 프로파일을 ISPostureCFG.xml로 저장합니다.
6. 프로파일 및 설치 파일을 아카이브 파일로 배포하거나 클라이언트에 복사합니다.

경고: 연결할 헤드엔드(Secure Firewall ASA, ISE 등)에도 동일한 Cisco Secure Client 파일이 있는지 확인합니다. 수동 프로비저닝을 사용하는 경우에도 해당 소프트웨어 버전으로 클라이언트 프로비저닝을 위해 ISE를 구성해야 합니다. 자세한 지침은 클라이언트 프로비저닝 정책 컨피그레이션 섹션을 참조하십시오.

7. 클라이언트에서 zip 파일을 열고 Setup(설정)을 실행하여 Core 및 ISE Posture 모듈을 설치합니다. 또는 개별 msi 파일을 사용하여 각 모듈을 설치할 수 있습니다. 이 경우 core-vpn 모듈을 먼저 설치해야 합니다.

Name	Type
Profiles	File folder
Setup	File folder
cisco-secure-client-win-5.0.01242-core-vpn-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-dart-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-iseposture-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-nam-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-nvm-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-posture-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-sbl-predeploy-k9	Windows Installer Package
cisco-secure-client-win-5.0.01242-umbrella-predeploy-k9	Windows Installer Package
Setup	Application
setup	HTML Application

### Cisco Secure Client 사전 구축 패키지 콘텐츠

Select the Cisco Secure Client 5.0.01242 modules you wish to install:

- Core & AnyConnect VPN
- Start Before Login
- Network Access Manager
- Secure Firewall Posture
- Network Visibility Module
- Umbrella
- ISE Posture
- Select All
  
- Diagnostic And Reporting Tool
  
- Lock Down Component Services

Install Selected

Cisco Secure Client 설치 관리자

팁: 문제 해결을 위해 사용할 진단 및 보고 도구를 설치합니다.

8. 설치가 완료되면 상태 프로파일 xml을 다음 위치에 복사합니다.
  - Windows: %ProgramData%\Cisco\Cisco Secure Client\ISE 상태
  - MacOS: /opt/cisco/secureclient/iseposture/

클라이언트 프로비저닝 포털(웹 구축)

ISE 클라이언트 프로비저닝 포털을 사용하여 Cisco Secure Client ISE Posture 모듈 및 ISE의 포스처 프로파일을 설치할 수 있으며, ISE Posture 모듈이 클라이언트에 이미 설치되어 있는 경우 포스처 프로파일만 푸시하는 데에도 사용할 수 있습니다.

1. Work Centers(작업 센터) > Posture(상태) > Client Provisioning(클라이언트 프로비저닝) > Client Provisioning Portal(클라이언트 프로비저닝 포털)로 이동하여 포털 컨피그레이션을 엽니다. Portal Settings(포털 설정) 섹션을 확장하고 Authentication Method(인증 방법) 필드를 찾은 다음 포털에서 인증에 사용할 Identity Source Sequence(ID 소스 시퀀스)를 선택합니다.
2. 클라이언트 프로비저닝 포털을 사용 할 권한 이 있는 내부 및 외부 ID 그룹을 구성 합니다.

Authentication method: \* Certificate\_Request\_Sequence ▾  
 Configure authentication methods at:  
[Administration > Identity Management > Identity Source Sequences](#)

**Configure authorized groups**  
 User account with Super admin privilege or ERS admin privilege will have access to the portal

Available		Chosen
<input type="text"/> ADAAMEX:aaamex.com/AAAUnit/AAAGroup ADAAMEX:aaamex.com/Builtin/Account Operat ADAAMEX:aaamex.com/Builtin/Administrators ADAAMEX:aaamex.com/Builtin/Backup Operato ADAAMEX:aaamex.com/Builtin/Certificate Servi	<input type="button" value="&gt;"/>  <input type="button" value="&lt;"/>	provisioning ADAAMEX:aaamex.com/Users/Domain Users

포털 설정의 인증 방법 및 인증된 그룹

3. FQDN(Fully Qualified Domain Name) 필드에서 클라이언트가 포털에 액세스하는 데 사용하는 URL을 구성합니다. 여러 FQDN을 구성하려면 쉼표로 구분된 값을 입력합니다.

Fully qualified domain name (FQDN): clientprovisioning.aaamex

Idle timeout: 10  
 1-30 (minutes)

Display language:  Use browser locale

Fallback language: English - English ▾

Always use: English - English ▾

4. 해당 Call Home 목록의 PSN에 대한 포털 URL을 확인하도록 DNS 서버를 구성합니다.

5. ISE Posture 소프트웨어를 설치하기 위해 포털에 액세스할 최종 사용자에게 FQDN을 제공합니다.

참고: 포털 FQDN을 사용하려면 클라이언트에는 PSN 관리 인증서 체인과 신뢰할 수 있는 저장소에 설치된 포털 인증서 체인이 있어야 하며 관리 인증서에는 SAN 필드에 포털 FQDN이 포함되어야 합니다.

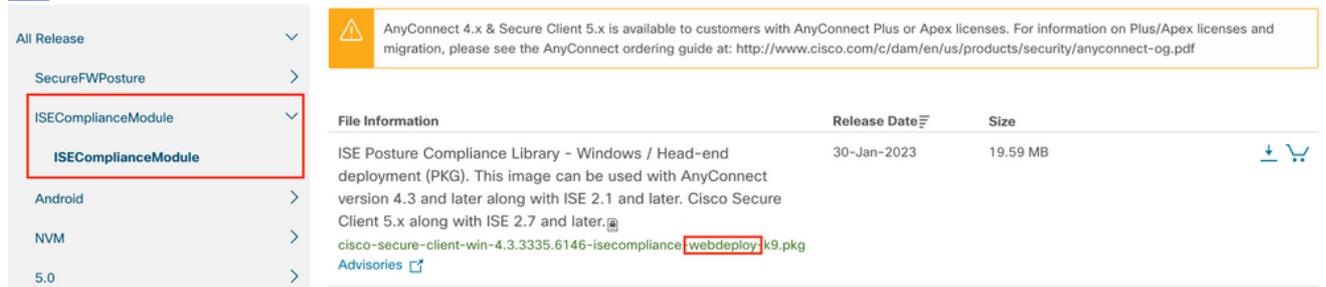
## 클라이언트 프로비저닝 정책

엔드포인트에 Cisco Secure Client를 설치하는 데 사용되는 프로비저닝 유형(사전 구축 또는 웹 구축)과 상관없이 ISE에서 클라이언트 프로비저닝을 구성해야 합니다.

1. Cisco Software Download에서 Cisco Secure Client webdeploy 패키지를 다운로드합니다.

Cisco Secure Client webdeploy 패키지

2. Cisco Software Download에서 최신 Compliance Module webdeploy 패키지를 다운로드합니다.



The screenshot shows the Cisco Software Download interface. On the left, a navigation menu has 'ISEComplianceModule' selected. The main content area displays a table with the following information:

File Information	Release Date	Size
ISE Posture Compliance Library - Windows / Head-end deployment (PKG). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later. <a href="#">cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy.k9.pkg</a>	30-Jan-2023	19.59 MB

There is also a warning banner at the top: 'AnyConnect 4.x & Secure Client 5.x is available to customers with AnyConnect Plus or Apex licenses. For information on Plus/Apex licenses and migration, please see the AnyConnect ordering guide at: <http://www.cisco.com/cj/dam/en/us/products/security/anyconnect-og.pdf>'

ISE Compliance Module webdeploy 패키지

3. ISE에서 Work Centers(작업 센터) > Posture(포스처) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동하고 Add(추가) > Agent resources from local disk(로컬 디스크에서 에이전트 리소스)를 클릭합니다. Category 드롭다운 메뉴에서 Cisco Provided Packages를 선택하고 이전에 다운로드한 Cisco Secure Client webdeploy 패키지를 업로드합



니다. 동일한 프로세스를 반복하여 Compliance Module을 업로드합니다.

Cisco 제공 패키지를 ISE에 업로드

4. Resources(리소스) 탭에서 Add(추가) > AnyConnect Posture Profile(AnyConnect 포스처 프로파일)을 클릭합니다. 프로파일에서:

- ISE 내에서 프로필을 식별하는 데 사용할 수 있는 이름을 구성합니다.
- 쉽표로 구분된 서버 이름 규칙을 구성합니다. PSN에 대한 연결을 허용하려면 단일 별표 (\*)를 사용하고, 특정 도메인의 PSN에 대한 연결을 허용하려면 와일드카드 값을 사용하거나, 특정 PSN에 대한 연결을 제한하려면 PSN FQDN을 사용합니다.
- 쉽표로 구분된 PSN 목록을 지정하도록 Call Home List를 구성합니다. FQDN:port 또는

IP:port 형식을 사용하여 클라이언트 프로비저닝 포털 포트를 추가해야 합니다.

ISE Posture 프로파일 컨피그레이션 I

Posture Protocol

Parameter	Value	Notes	Description
PAA retransmission time	120 seconds		This is the agent retry period if there is a Passive Reassessment communication failure.
Retransmission Delay	60 seconds	Default value: 60. Acceptable Range between 5 to 300. Accept only integer values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer values.	Number of retries allowed for a message.
Discovery Host		(IPv4 or IPv6) addresses or FQDNs. (IPv6) address should be without square brackets]	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
* Server name rules	*.saamtek.com	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List	svx.saamtek.com:8443	List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSNs that authenticated the endpoint doesn't respond for some reason.
Back-off timer	30 seconds	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached.

ISE Posture 프로파일 컨피그레이션 II

Call Home 목록에서 사용할 포트를 찾으려면 Work Centers(작업 센터) > Posture(상태) > Client Provisioning(클라이언트 프로비저닝) > Client Provisioning Portal(클라이언트 프로비저닝 포털)로 이동하여 사용 중인 포털을 선택하고 Portal Settings(포털 설정)를 확장합니다.

# Portals Settings and Customization

Portal Name:

Client Provisioning Portal (default)

Description:

Default portal and user experience user

Language File



Portal test URL

Portal Behavior and Flow Settings

Portal Page Customization

Portal & Page Settings

Portal Settings

HTTPS port:\*

8443

(8000 - 8999)

클라이언트 프로비저닝 포털 포트

5. Resources(리소스) 탭에서 Add(추가) > AnyConnect Configuration(AnyConnect 컨피그레이션)을 다시 클릭합니다. 사용할 Cisco Secure Client 패키지 및 Compliance Module을 선택합니다.

경고: Cisco Secure Client가 클라이언트에 미리 구축된 경우 ISE의 버전이 엔드포인트의 버전과 일치하는지 확인하십시오. ASA 또는 FTD를 웹 구축에 사용하는 경우 이 디바이스의 버전도 일치해야 합니다.

6. Posture Selection(상태 선택) 섹션까지 아래로 스크롤하여 1단계에서 생성한 프로파일을 선택합니다.



페이지 하단에서 Submit(제출)을 클릭하여 컨피그레이션을 저장합니다.

AnyConnect 컨피그레이션

## Profile Selection

* ISE Posture	CSC Redirectionless	▼
VPN		▼

프로파일 선택

7. Work Centers(작업 센터) > Posture(상태) > Client Provisioning(클라이언트 프로비저닝) > Client provisioning policy(클라이언트 프로비저닝 정책)로 이동합니다. 필요한 운영 체제에 사용되는 정책을 찾아 Edit(수정)를 클릭합니다. 결과 열에서 + 기호를 클릭하고 5단계의 에이전트 구성 섹션 아래에서 AnyConnect 구성을 선택합니다.

---

참고: 여러 Call Home 목록의 경우 Other Conditions(기타 조건) 필드를 사용하여 해당 클라이언트에 올바른 프로필을 푸시합니다. 이 예에서는 Device Location Group(디바이스 위치 그룹)을 사용하여 정책에서 푸시되는 포스처 프로파일을 식별합니다.

---

팁: 여러 클라이언트 프로비저닝 정책이 동일한 OS에 대해 구성된 경우 상호 배타적으로 설정하는 것이 좋습니다. 즉, 지정된 클라이언트는 한 번에 하나의 정책에만 도달할 수 있어야 합니다. RADIUS 특성은 Other Conditions(기타 조건) 열에서 어떤 정책을 다른 정책과 구별하는 데 사용할 수 있습니다.

---

## Agent Configuration

ect Configuration Redirectionless



Is Upgrade Mandatory

## Native Supplicant Configuration

Choose a Config Wizard



Choose a Wizard Profile



클라이언트 프로비저닝 정책 에이전트 컨피그레이션

### Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:  
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.  
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

	Rule Name	Identity Groups	Operating Systems	Other Conditions	Results	
<input checked="" type="checkbox"/>	IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP	Edit
<input checked="" type="checkbox"/>	Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP	Edit
<input checked="" type="checkbox"/>	Windows	If Any	and Windows All	and DEVICE-Location EQUALS All Locations#USHWEST	then AnyConnect Configuration Redirectionless	Edit
<input checked="" type="checkbox"/>	MAC OS	If Any	and Mac OSX	and Condition(s)	then MacOS Configuration And MacOSXSPWizard 2.7.0.1 And Cisco-ISE-NSP	Edit
<input checked="" type="checkbox"/>	Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP	Edit

Save

Reset

클라이언트 프로비저닝 정책

8. 사용 중인 각 Call Home 목록 및 해당 포스터 프로필에 대해 4~7단계를 반복합니다. 하이브리드 환경의 경우 리디렉션 클라이언트에 동일한 프로필을 사용할 수 있습니다.

### Authorization(권한 부여)

권한 부여 프로파일

1. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Downloadable ACLs(다운로드 가능 ACL)로 이동하고 Add(추가)를 클릭합니다.
2. DNS, DHCP(사용되는 경우), ISE PSN에 대한 트래픽을 허용하고 다른 트래픽을 차단하기 위한 DACL을 생성합니다. 최종 규정 준수 액세스 전에 액세스에 필요한 다른 트래픽을 허용해야 합니다.

\* Name

Description

IP version  IPv4  IPv6  Agnostic

\* DACL Content

1234567	permit udp any any eq domain
8910111	permit udp any any eq bootps
2131415	permit ip any host <ip 1 IP address>
1617181	permit ip any host <ip 2 IP address>
9202132	permit icmp any any
2324252	deny ip any any
6272829	
3031323	
3343838	
3738394	
0414343	

✓ Check DACL Syntax

DACL is valid

DACL 컨피그레이션

```

permit udp any any eq domain
permit udp any any eq bootps
permit ip any host

```

```

permit ip any host

```

```

deny ip any any

```

주의: 일부 서드파티 디바이스는 DACL을 지원하지 않을 수 있습니다. 이 경우 Filter-ID 또는 기타 벤더 특정 특성을 사용해야 합니다. 자세한 내용은 공급업체 설명서를 참조하십시오. DACL을 사용하지 않는 경우 네트워크 디바이스에서 해당 ACL을 구성해야 합니다.

3. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization profiles(권한 부여 프로파일)로 이동하고 Add(추가)를 클릭합니다. 인증 프로파일에 이름을 지정하고 일반적인 작업에서 DACL 이름을 선택합니다. 드롭다운 메뉴에서

Authorization Profile

\* Name: Redirectionless posture

Description: [Empty text area]

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Agentless Posture:

Passive Identity Tracking:

Common Tasks

DACL Name: redirectionless\_posture

2단계에서 생성한 DACL을 선택합니다.

권한 부여 프로파일

참고: DACL을 사용하지 않는 경우 일반 작업의 Filter-ID 또는 고급 특성 설정을 사용하여 해당 ACL 이름을 푸시합니다.

4. 사용 중인 각 Call Home 목록에 대해 1~3단계를 반복합니다. 하이브리드 환경에서는 리디렉션을 위한 단일 권한 부여 프로파일만 필요합니다. 리디렉션을 위한 권한 부여 프로파일 구성이 이 문서의 범위를 벗어납니다.

## 권한 부여 정책

1. Policy > Policy Sets로 이동하여 사용 중인 정책 세트를 열거나 새 정책 세트를 만듭니다.
2. 아래로 스크롤하여 Authorization Policy(권한 부여 정책) 섹션으로 이동합니다. Session PostureStatus NOT\_EQUALS Compliant를 사용하여 권한 부여 정책을 생성하고 이전 섹션에서 생성한 권한 부여 프로파일을 선택합니다.

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Compliant		Session-PostureStatus EQUALS Compliant	Compliant access x	Select from list	0	
Redirectionless	AND	DEVICE-Posture EQUALS Posture#Redirectionless DEVICE-Location EQUALS All Locations#US#WEST Session-PostureStatus NOT_EQUALS Compliant	Redirectionless posture x	Select from list	0	
Redirection	AND	Session-PostureStatus NOT_EQUALS Compliant DEVICE-Posture EQUALS Posture#Redirection	Redirection posture x	Select from list	0	
Default			DenyAccess x	Select from list	0	

### 권한 부여 정책

- 해당 Call Home List(콜 홈 목록)가 사용 중인 상태에서 각 권한 부여 프로파일에 대해 2단계를 반복합니다. 하이브리드 환경에서는 리디렉션을 위한 단일 권한 부여 정책만 필요합니다.

## 문제 해결

Cisco Secure Client 및 ISE에 적용할 수 없는 상태(보류 중)를 준수합니다.

### 부실/팬텀 세션

배포에 오래된 세션 또는 팬텀 세션이 있을 경우 리디렉션 없는 상태 검색으로 간헐적이고 무작위로 장애가 발생할 수 있으며, 이로 인해 사용자는 Cisco Secure Client UI에서 Compliant 액세스를 표시하는 동안 ISE에서 상태 Unknown/Not Applicable 액세스에 갇힐 수 있습니다.

**오래된 세션**은 더 이상 활성 상태가 아닌 이전 세션입니다. 인증 요청 및 계정 관리 시작에 의해 생성되지만 세션을 지우기 위해 PSN에서 계정 관리 중지를 수신하지 않습니다.

**팬텀 세션**은 특정 PSN에서 실제로 활성화되지 않은 세션입니다. 어카운팅 중간 업데이트에 의해 생성되지만 세션을 지울 수 있도록 PSN에서 어카운팅 중지가 수신되지 않습니다.

### 식별

부실/팬텀 세션 문제를 식별하려면 클라이언트의 시스템 검사에 사용된 PSN을 확인하고 인증을 수행하는 PSN과 비교합니다.

- Cisco Secure Client UI의 왼쪽 하단 모서리에 있는 톱니바퀴 아이콘을 클릭합니다. 왼쪽 메뉴에서 ISE Posture 섹션을 열고 Statistics(통계) 탭으로 이동합니다. Connection Information(연결 정보)에서 정책 서버를 확인합니다.



Cisco Secure Client에서 ISE Posture를 위한 정책 서버

## 2. ISE에서 RADIUS 라이브 로그는 다음 사항에 유의합니다.

- 상태 변경
- 서버 변경
- 권한 부여 정책 및 권한 부여 프로파일의 변경 사항 없음
- CoA 라이브 로그 없음

Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server	Posture Status	Authorization Profiles
Apr 03, 2023 07:32:52.3...	<span style="color: blue;">●</span>		0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30cmexaaa	Compliant	Redirectionless posture
Apr 03, 2023 07:32:40.7...	<span style="color: green;">✓</span>			#ACSACL#-IP...			ise30baaamex		
Apr 03, 2023 07:32:40.6...	<span style="color: green;">✓</span>			redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30baaamex	NotApplicable	Redirectionless posture

부실/팬텀 세션에 대한 라이브 로그

## 3. 라이브 세션 또는 마지막 인증 라이브 로그 세부 정보를 엽니다. Policy Server(정책 서버)가 1단계에서 관찰된 서버와 다를 경우 오래된/가상 세션의 문제를 나타냅니다.

## Overview

Event	5200 Authentication succeeded
Username	redirectionless
Endpoint Id	00:50:56:B3:3E:0E ⓘ
Endpoint Profile	Windows10-Workstation
Authentication Policy	Posture Lab >> Default
Authorization Policy	Posture Lab >> Redirectionless
Authorization Result	Redirectionless posture

## Authentication Details

Source Timestamp	2023-04-03 19:32:40.691
Received Timestamp	2023-04-03 19:32:40.691

Policy Server	ise30baaamex
---------------	--------------

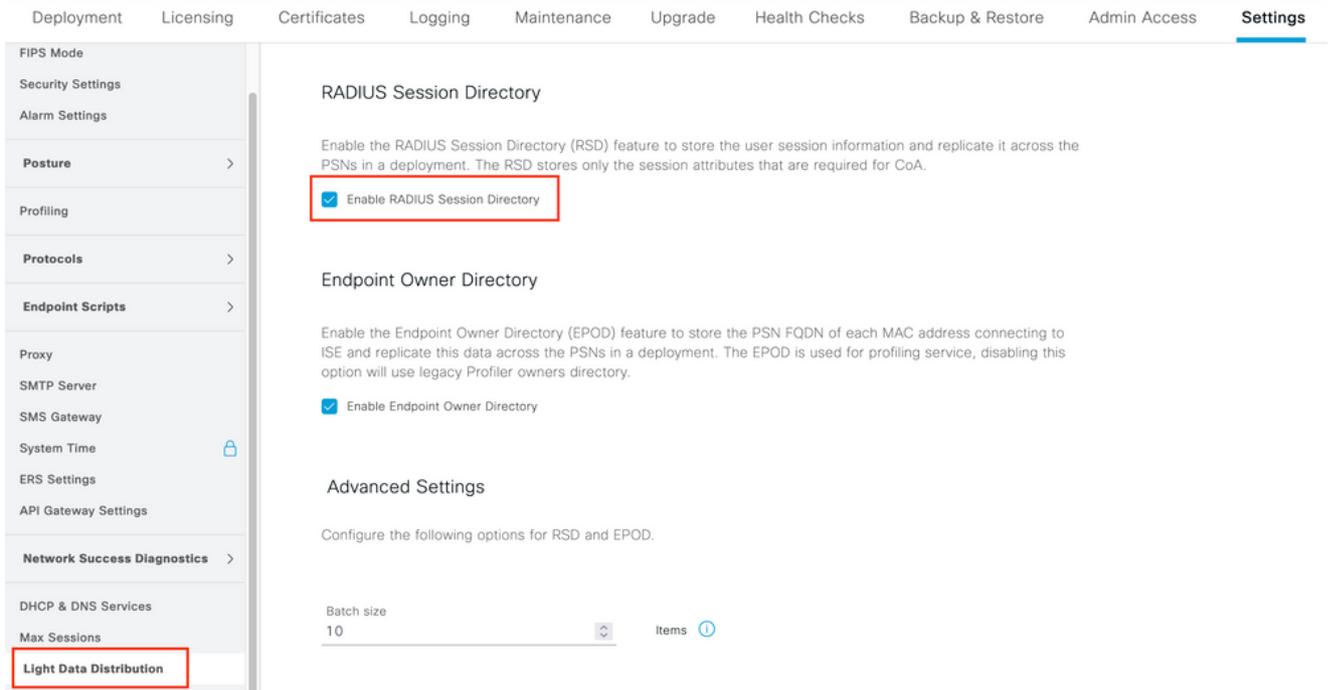
Event	5200 Authentication succeeded
Username	redirectionless

실시간 로그 세부 정보의 정책 서버

### 솔루션

ISE 2.6 패치 6 및 2.7 패치 3 위의 ISE 버전은 방향 없는 상태 흐름에서 부실/팬텀 세션 시나리오에 대한 솔루션으로 RADIUS 세션 디렉토리를 구현합니다.

1. Administration(관리) > System(시스템) > Settings(설정) > Light Data Distribution(라이트 데이터 배포)으로 이동하고 Enable RADIUS Session Directory(RADIUS 세션 디렉토리 활성화) 확인란이 활성화되어 있는지 확인합니다.



RADIUS 세션 디렉토리 활성화

2. ISE CLI에서 명령을 실행하여 ISE 메시징 서비스가 모든 PSN에서 실행 중인지 확인합니다 애플리케이션 상태 ise를 표시합니다.

```
lise30cmexaaa/admin# show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	12434
Database Server	running	112 PROCESSES
Application Server	running	33093
Profiler Database	running	19622
ISE Indexing Engine	running	42923
AD Connector	running	60317
M&T Session Database	running	19361
M&T Log Processor	running	33283
Certificate Authority Service	disabled	
EST Service	disabled	
SXP Engine Service	disabled	
Docker Daemon	running	14791
TC-NAC MongoDB Container	running	18594
TC-NAC Core Engine Container	running	18981
VA Database	running	53465
VA Service	running	53906
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
PassiveID WMI Service	running	55480
PassiveID Syslog Service	running	56312
PassiveID API Service	running	57153
PassiveID Agent Service	running	58079
PassiveID Endpoint Service	running	59138
PassiveID SPAN Service	running	60059
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	
ISE Messaging Service	running	16526
ISE API Gateway Database Service	running	18463
ISE API Gateway Service	running	23052

실행 중인 ISE 메시징 서비스

참고: 이 서비스는 PSN 간의 RSD에 사용되며 ISE UI에서 설정할 수 있는 syslog에 대한 ISE 메시징 서비스 설정의 상태에 관계없이 실행해야 하는 통신 방법을 나타냅니다.

3. ISE Dashboard(ISE 대시보드)로 이동하고 Alarms(경보) dashlet을 찾습니다. Queue Link Error 경보가 있는지 확인합니다. 자세한 내용을 보려면 경보의 이름을 클릭합니다.

Severity	Name	Occu...	Last Occurred
▼	queue	x	
	Queue Link Error	2143	37 mins ago

Last refreshed: 2023-04-03 14:45:19

대기열 링크 오류 경보

#### 4. 포스터에 사용되는 PSN 간에 경보가 생성되는지 확인합니다.

Alarms: Queue Link Error

##### Description

The queue link between two nodes in the ISE deployment is down.

##### Suggested Actions

Please check and restore connectivity between the nodes. Ensure that the nodes and the ISE Messaging Service are up and running. Ensure that ISE Messaging Service ports are not blocked by firewall. Please note that these alarms could occur between nodes, when the nodes are being registered to deployment or manually-synced from PSPAN or when the nodes are in out-of-sync state or when the nodes are getting restarted.

Rows/Page 100 << 1 / 22 >> Go 2143 Total Rows

Refresh Acknowledge

<input type="checkbox"/> Time Stamp	Description	Cause= {ts_alert;" unknown Ca"}	Details
<input type="checkbox"/> Apr 03 2023 21:07:00.977 PM	Queue Link Error: Message=From ise30cmexaaa.aaamex.com To ise30baaamex.aaamex.com; Cause={ts_alert;" unkno...		
<input type="checkbox"/> Apr 03 2023 21:07:00.959 PM	Queue Link Error: Message=From ise30baaamex.aaamex.com To ise30cmexaaa.aaamex.com; Cause={ts_alert;" unkno...		

대기열 링크 오류 경보 세부 정보

- 경보 설명 위에 마우스 커서를 올려 놓으면 전체 세부 정보를 볼 수 있으며 Cause(원인) 필드에 주의할 수 있습니다. 대기열 링크 오류의 가장 일반적인 두 가지 원인은 다음과 같습니다.
  - 시간 초과: 노드가 포트 8671의 다른 노드로 보낸 요청이 임계값 내에 응답하지 않음을 나타냅니다. 문제를 해결하려면 노드 간에 TCP 포트 8671이 허용되는지 확인합니다.
  - 알 수 없는 CA: ISE 메시징 인증서를 서명하는 인증서 체인이 잘못되었거나 불완전함을 나타냅니다. 이 오류를 해결하려면

- a. Administration > System > Certificates > Certificate signing requests로 이동합니다.
- b. Generate Certificate Signing Requests (CSR)를 클릭합니다.
- c. 드롭다운 메뉴에서 ISE Root CA(ISE 루트 CA)를 선택하고 Replace ISE Root CA Certificate chain(ISE 루트 CA 인증서 체인 대체)을 클릭합니다.  
ISE 루트 CA를 사용할 수 없는 경우 Certificate Authority > Internal CA settings로 이동하고 Enable Certificate Authority를 클릭한 다음 CSR로 돌아가 루트 CA를 다시 생성합니다.
- d. 새 CSR을 생성하고 드롭다운 메뉴에서 ISE 메시징 서비스를 선택합니다.
- e. 구축에서 모든 노드를 선택 하고 인증서를 다시 생성 합니다.

참고: 인증서가 재생성되는 동안 원인을 알 수 없는 CA 또는 Econnrejected로 대기열 링크 오류 경보를 관찰하고, 인증서 생성 후 경보를 모니터링하여 문제가 해결되었는지 확인합니다.

## Performance

### 식별

PSN 및 MnT 노드에 영향을 미칠 수 있으며 종종 다음 이벤트가 수반되거나 선행됩니다.

- 임의 또는 간헐적 Cisco Secure Client에서 정책 서버가 오류를 탐지하지 않음
- 포털 서비스 스레드 풀에 대한 최대 리소스 제한 도달 보고서가 임계값 이벤트에 도달했습니다. Operations(운영) > Reports(보고서) > Reports(보고서) > Audit(감사) > Operations Audit(운영 감사)으로 이동하여 보고서를 확인합니다.
- MNT에 대한 포스터 쿼리 조회가 높은 알람입니다. 이러한 경보는 ISE 3.1 이상 버전에서만 생성됩니다.

### 솔루션

구축 성능이 리디렉션 없는 상태의 영향을 받는 경우, 이는 종종 비효율적인 구현을 나타냅니다. 다음과 같은 측면을 수정하는 것이 좋습니다.

- Call Home 목록당 사용된 PSN 수입입니다. 설계에 따라 엔드포인트 또는 네트워크 디바이스당 포스터에 사용할 수 있는 PSN 수를 줄이는 것을 고려하십시오.
- Call Home 목록의 클라이언트 프로비저닝 포털 포트 포털 포트 번호가 각 노드의 IP 또는 FQDN 뒤에 포함되어 있는지 확인하십시오.

### 영향을 완화하려면

1. Cisco Secure Client 폴더에서 파일을 제거하여 엔드포인트에서 connectiondata.xml을 지우고 ISE Posture 서비스 또는 Cisco Secure Client를 다시 시작합니다. 서비스를 다시 시작하지 않으면 이전 파일이 다시 생성되고 변경 사항이 적용되지 않습니다. 이 작업은 Call Home 목록을 수정 및 수정한 후에도 수행해야 합니다.

2. DACL 또는 기타 ACL을 사용하여 관련이 없는 네트워크 연결에 대해 ISE PSN으로 가는 트래픽을 차단합니다.

- 권한 부여 정책에서 포스처가 적용되지 않지만 Cisco Secure Client ISE Posture 모듈이 설치된 엔드포인트에 적용되는 연결의 경우 클라이언트에서 TCP 포트 8905 및 클라이언트 프로비저닝 포털 포트에 대한 모든 ISE PSN으로의 트래픽을 차단합니다. 이 작업은 리디렉션 구현이 있는 포스처에 대해서도 권장됩니다.
- 권한 부여 정책에서 포스처가 적용되는 연결의 경우 클라이언트에서 인증 PSN으로 가는 트래픽을 허용하고 구축에서 다른 PSN으로 가는 트래픽을 차단합니다. 이 작업은 설계를 수정하는 동안 임시로 구현할 수 있습니다.

Authorization Profiles > Redirectionless-PSN1

Authorization Profile

\* Name: Redirectionless PSN1

Description: Authorization profile for redirectionless posture with DACL allowing traffic only to PSN1, DNS and DHCP

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:  ⓘ

Agentless Posture:  ⓘ

Passive Identity Tracking:  ⓘ

Common Tasks

DACL Name: redirectionless\_posture\_psn1

단일 PSN에 대한 DACL를 사용 하는 인증 프로파일

Compliant	AND	Session-PostureStatus EQUALS Compliant	Compliant access
Redirectionless PSN1	AND	DEVICE-Posture EQUALS Posture#Redirectionless	Redirectionless PSN1
		DEVICE-Location EQUALS All Locations#US#WEST	
		Session-PostureStatus NOT_EQUALS Compliant	
Redirectionless PSN2	AND	DEVICE-Posture EQUALS Posture#Redirectionless	Redirectionless PSN2
		DEVICE-Location EQUALS All Locations#US#WEST	
		Session-PostureStatus NOT_EQUALS Compliant	
Redirection	AND	Session-PostureStatus NOT_EQUALS Compliant	Redirection posture
		DEVICE-Posture EQUALS Posture#Redirection	

PSN당 권한 부여 정책

## 어카운팅

RADIUS 어카운팅은 ISE의 세션 관리에 필수적입니다. 포스처는 수행할 활성 세션에 의존하므로,

어카운팅 컨피그레이션이 잘못되거나 부족한 경우에도 포스처 검색 및 ISE 성능에 영향을 줄 수 있습니다. 각 세션에 대한 단일 PSN에 인증 요청, 계정 관리 시작, 계정 관리 중지 및 계정 관리 업데이트를 보낼 수 있도록 네트워크 장치에 계정 관리가 올바르게 구성되어 있는지 확인하는 것이 중요합니다.

ISE에서 수신된 어카운팅 패킷을 확인하려면 Operations(운영) > Reports(보고서) > Reports(보고서) > Endpoints and Users(엔드포인트 및 사용자) > RADIUS Accounting(RADIUS 어카운팅)으로 이동합니다.

## 관련 정보

- [Cisco 기술 지원 및 다운로드](#)

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.