

AMP 및 Posture Services로 ISE 2.1 TC-NAC(Threat-Centric NAC) 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[자세한 흐름](#)

[AMP 클라우드 구성](#)

[1단계. AMP 클라우드에서 커넥터 다운로드](#)

[ISE 구성](#)

[1단계. 상태 정책 및 조건 구성](#)

[2단계. 상태 프로파일 구성](#)

[3단계. AMP 프로파일 구성](#)

[2단계. ISE에 애플리케이션 및 XML 프로파일 업로드](#)

[3단계. AnyConnect Compliance 모듈 다운로드](#)

[4단계. AnyConnect 구성 추가](#)

[5단계. 클라이언트 프로비저닝 규칙 구성](#)

[6단계. 권한 부여 정책 구성](#)

[7단계. TC-NAC 서비스 활성화](#)

[8단계. AMP 어댑터 구성](#)

[다음을 확인합니다.](#)

[엔드포인트](#)

[AMP 클라우드](#)

[ISE](#)

[문제 해결](#)

소개

이 문서에서는 ISE(Identity Services Engine) 2.1에서 AMP(Advance Malware Protection)를 사용하여 Threat-Centric NAC를 구성하는 방법에 대해 설명합니다. 위협 심각도 수준 및 취약성 평가 결과를 사용하여 엔드포인트 또는 사용자의 액세스 레벨을 동적으로 제어할 수 있습니다. Posture Services도 이 문서의 일부로 포함됩니다.

참고: 이 문서의 목적은 ISE에서 AMP를 프로비저닝할 때 필요한 ISE 2.1 AMP와의 통합, 포스처 서비스를 설명하는 것입니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- Cisco Identity Service Engine
- 지능형 악성코드 차단

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Service Engine 버전 2.1
- WLC(Wireless LAN Controller) 8.0.121.0
- AnyConnect VPN 클라이언트 4.2.02075
- Windows 7 서비스 팩 1

구성

네트워크 다이어그램



자세한 흐름

1. 클라이언트가 네트워크에 연결되고, **AMP_Profile**이 할당되고, 사용자가 Anyconnect 프로비저닝 포털로 리디렉션됩니다. 시스템에서 AnyConnect가 탐지되지 않으면 구성된 모든 모듈(VPN, AMP, Posture)이 설치됩니다. 해당 프로필과 함께 각 모듈에 대한 컨피그레이션이 푸시됩니다.
2. AnyConnect가 설치되면 상태 평가가 실행됩니다.
3. AMP Enabler 모듈이 FireAMP 커넥터를 설치합니다.

4. 클라이언트가 악성 소프트웨어를 다운로드하려고 하면 AMP 커넥터는 경고 메시지를 던져서 AMP 클라우드에 보고합니다.

5. AMP Cloud는 이 정보를 ISE로 전송합니다.

AMP 클라우드 구성

1단계. AMP 클라우드에서 커넥터 다운로드

커넥터를 다운로드하려면 Management(관리) > Download Connector(커넥터 다운로드)로 이동합니다. 그런 다음 type(유형)과 **Download FireAMP**(Windows, Android, Mac, Linux)를 선택합니다. 이 경우 **Audit(감사)**가 선택되었고 FireAMP for Windows 설치 파일이 선택됩니다.

The screenshot shows the AMP for Endpoints management console. At the top, there's a navigation bar with 'AMP for Endpoints' and various links like '3 Installs', '1 detection (7 days)', 'Announcements', 'Support', 'Help', 'My Account', and 'Log Out'. Below the navigation bar, there's a search bar and a 'Download Connector' section. A dropdown menu is set to 'Audit'. There are four connector cards: 'FireAMP Windows' (with 'Audit Policy' and 'Flash Scan on Install' checked), 'FireAMP Mac' (with 'Audit Policy for FireAMP Mac' and 'Flash Scan on Install' checked), 'FireAMP Linux' (with 'Audit Policy for FireAMP Li...' and 'Flash Scan on Install' checked), and 'FireAMP Android' (with 'Default FireAMP Android Activation Codes'). Each card has 'Show URL' and 'Download' buttons.

참고: 이 파일을 다운로드하면 이 예제에서 **Audit_FireAMPSetup.exe**라는 .exe 파일이 생성됩니다. 사용자가 AMP 컨피그레이션을 요청하면 이 파일을 사용할 수 있도록 웹 서버로 전송했습니다.

ISE 구성

1단계. 상태 정책 및 조건 구성

Policy(정책) > Policy Elements(정책 요소) > Conditions(조건) > Posture(포스처) > File Condition(파일 조건)으로 이동합니다. 파일 존재에 대한 간단한 조건이 생성되었음을 확인할 수 있습니다. 엔드포인트가 Posture 모듈에서 확인한 정책을 준수하는 경우 파일이 있어야 합니다.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

File Conditions List > File_Condition

File Condition

* Name: File_Condition

Description:

* Operating System: Windows All

Compliance Module: Any version

* File Type: FileExistence

* File Path: ABSOLUTE_PATH C:\test.bt

* File Operator: Exists

Save Reset

- Authentication
- Authorization
- Profiling
- Posture
 - Anti-Malware Condition
 - Anti-Spyware Condition
 - Anti-Virus Condition
 - Application Condition
 - Compound Condition
 - Disk Encryption Condition
 - File Condition
 - Patch Management Condition
 - Registry Condition
 - Service Condition
 - USB Condition
 - Dictionary Simple Condition
 - Dictionary Compound Condition
- Guest
- Common

이 조건은 요구 사항에 사용됩니다.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

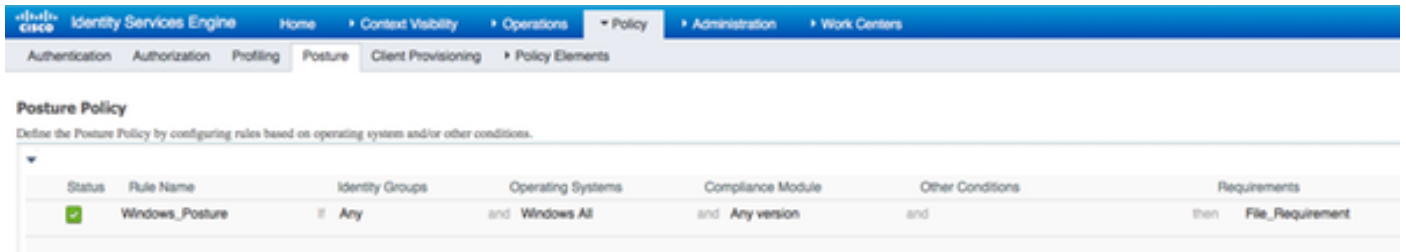
Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Requirements

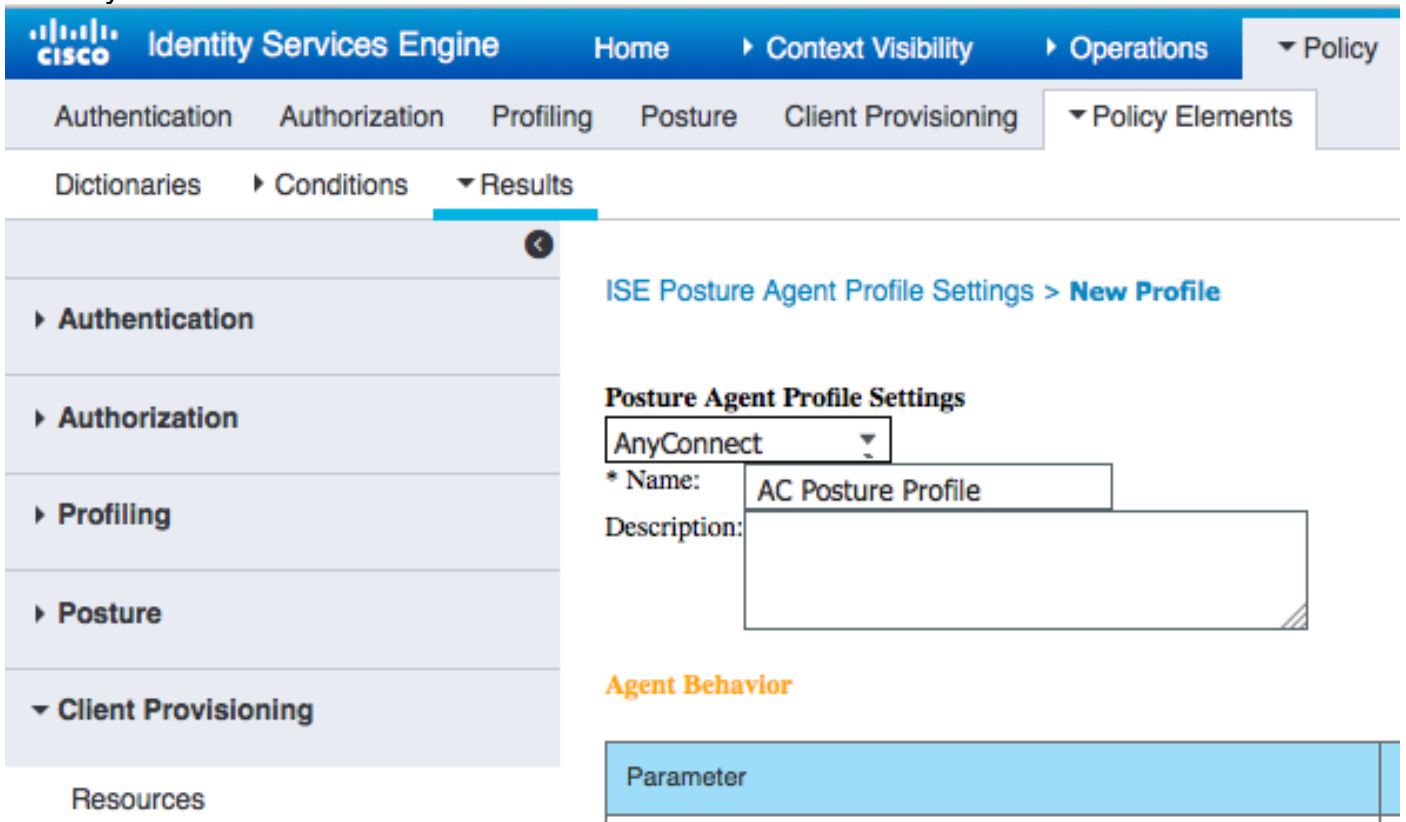
Name	Operating Systems	Compliance Module	Conditions	Remediation Actions
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	met if ANY_av_win_inst	then Message Text Only
File_Requirement	for Windows All	using Any version	met if File_Condition	then Message Text Only
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	met if ANY_av_win_def	then AnyAVDefRemediationWin
Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	met if ANY_am_mac_inst	then Message Text Only
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	met if ANY_as_win_inst	then Message Text Only
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	met if ANY_as_win_def	then AnyASDefRemediationWin
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	met if ANY_av_mac_inst	then Message Text Only
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	met if ANY_av_mac_def	then AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	met if ANY_as_mac_inst	then Message Text Only
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	met if ANY_as_mac_def	then AnyASDefRemediationMac
Any_AM_Installation_Win	for Windows All	using 4.x or later	met if ANY_am_win_inst	then Message Text Only
Any_AM_Definition_Win	for Windows All	using 4.x or later	met if ANY_am_win_def	then AnyAMDefRemediationWin
Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	met if ANY_am_mac_def	then AnyAMDefRemediationMac
USB_Block	for Windows All	using 4.x or later	met if USB_Check	then USB_Block

요구 사항은 Microsoft Windows 시스템의 상태 정책에서 사용 됩니다.



2단계. 상태 프로파일 구성

- Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동하고 Network Admission Control (NAC) Agent or AnyConnect Agent Posture Profile(NAC(NAC) Agent 또는 AnyConnect 에이전트 포스처 프로파일 추가)
- AnyConnect 선택



- Posture Protocol 섹션에서 *를 추가하여 에이전트가 모든 서버에 연결할 수 있도록 합니다.

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all

3단계. AMP 프로파일 구성

AMP 프로파일에는 Windows Installer가 있는 위치에 대한 정보가 포함되어 있습니다.Windows

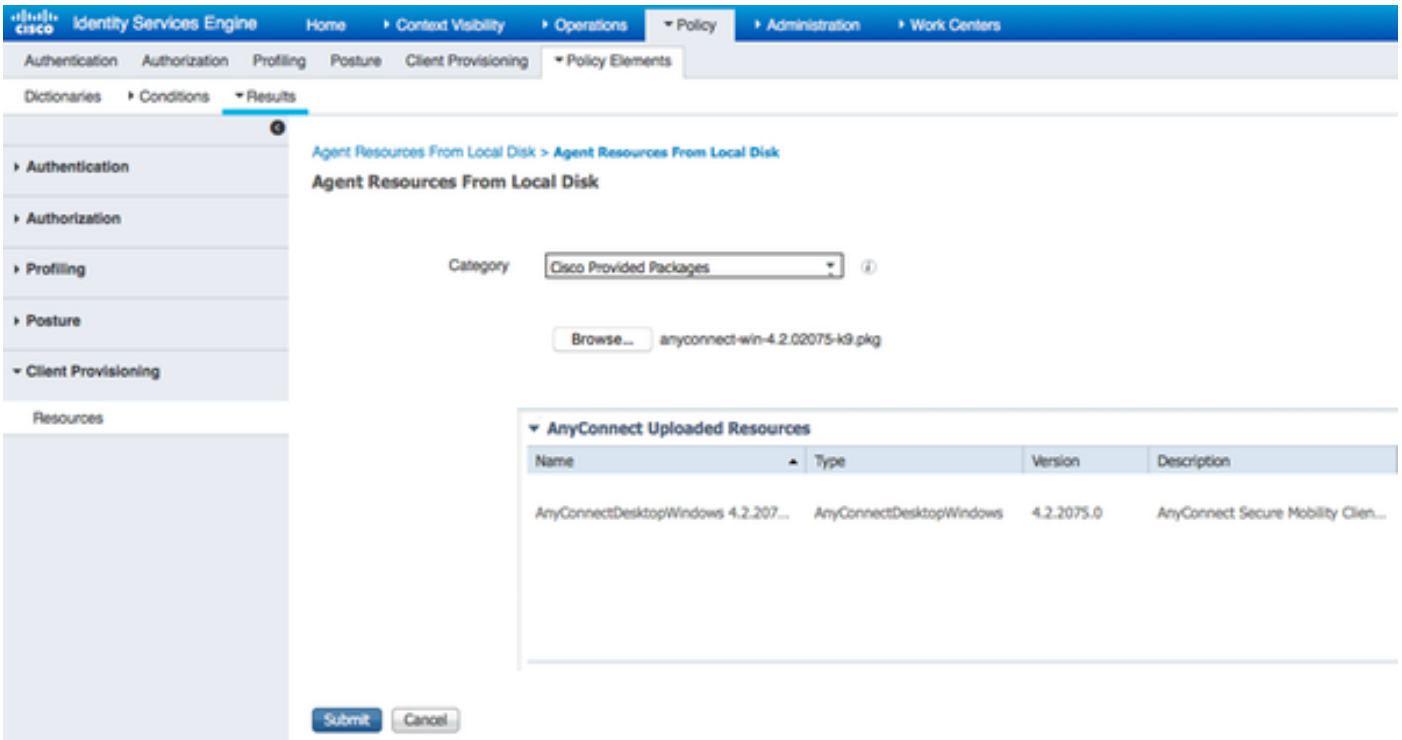
Installer가 AMP 클라우드에서 이전에 다운로드되었습니다. 클라이언트 시스템에서 액세스할 수 있어야 합니다. 설치 프로그램이 있는 HTTPS 서버의 인증서도 클라이언트 시스템에서 신뢰해야 합니다.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for creating a new AMP Enabler Profile. The breadcrumb trail is: AMP Enabler Profile Settings > New Profile. The main heading is 'AMP Enabler Profile'. The form includes the following fields and options:

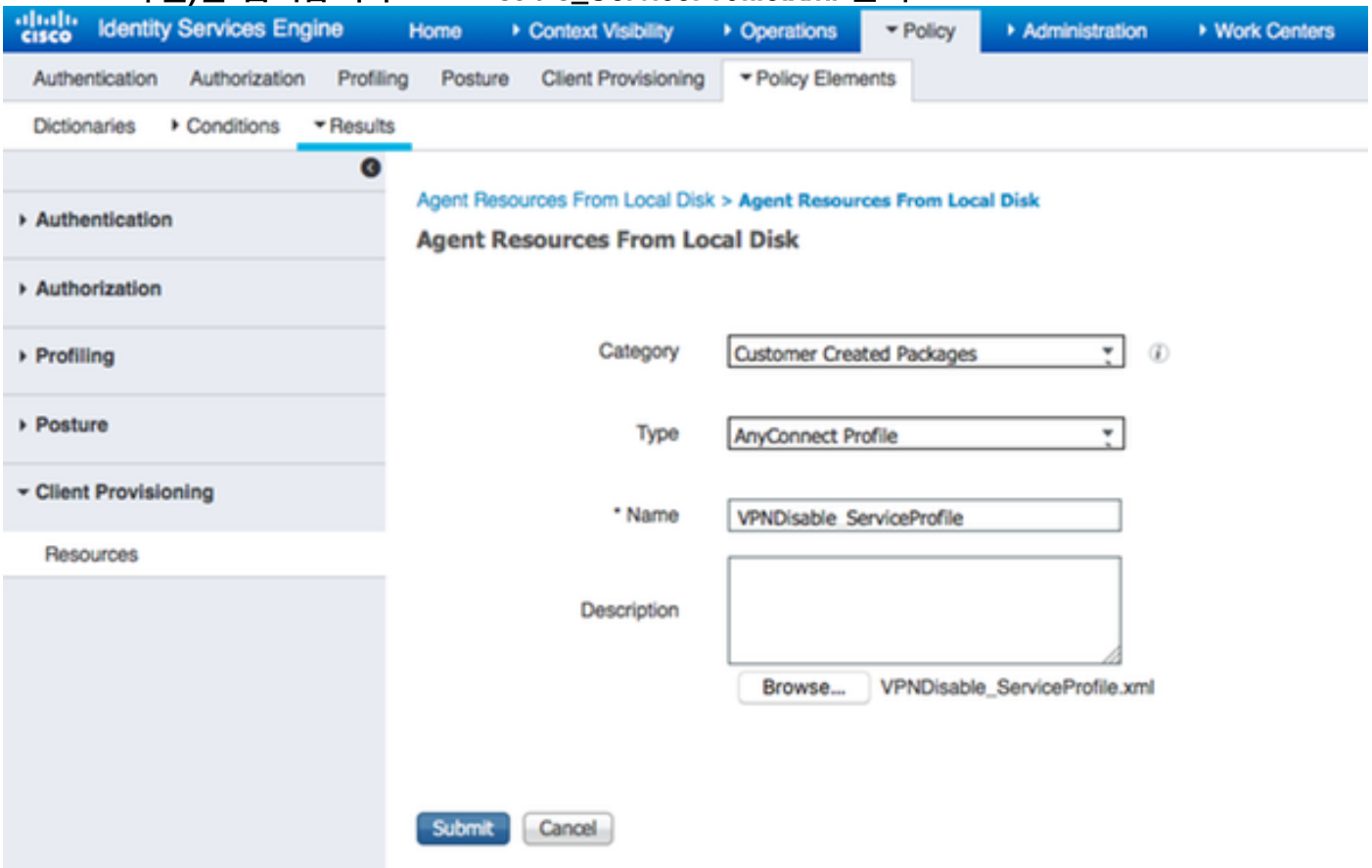
- Name:** AMP Profile
- Description:** (empty field)
- Install AMP Enabler:** (selected)
- Uninstall AMP Enabler:**
- Windows Installer:** [https://win2012ek.example.com/Downloads/Audit_FireAMPSetup.](https://win2012ek.example.com/Downloads/Audit_FireAMPSetup)
- MAC Installer:** <https://>
- Windows Settings:**
 - Add to Start Menu:**
 - Add to Desktop:**
 - Add to Context Menu:**
- Buttons:** Submit, Cancel

2단계. ISE에 애플리케이션 및 XML 프로파일 업로드

- 공식 Cisco 사이트에서 애플리케이션을 수동으로 다운로드합니다. **anyconnect win-win-4.2.02075-k9.pkg**
- ISE에서 Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동하고 로컬 디스크에서 에이전트 리소스 추가
- **Cisco Provided Packages(Cisco 제공 패키지)**를 선택하고 **anyconnect-win-4.2.02075-k9.pkg**을 선택합니다.



- Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동하고 로컬 디스크에서 에이전트 리소스 추가
- Customer Created Packages(고객 생성 패키지)를 선택하고 AnyConnect Profile(AnyConnect 프로파일)을 입력합니다.VPNDisable_ServiceProfile.xml 선택



참고:VPNDisable_ServiceProfile.xml은 VPN 모듈을 사용하지 않으므로 VPN 제목을 숨기는데 사용됩니다.VPNDisable_ServiceProfile.xml의 콘텐츠입니다.

<AnyConnectProfile xmlns="<http://schemas.xmlsoap.org/encoding/>"

```

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<클라이언트 초기화>
<ServiceDisable>true</ServiceDisable>
</ClientInitialization>
</AnyConnect 프로파일>

```

3단계. AnyConnect Compliance 모듈 다운로드

- Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동하고 Cisco 사이트에서 에이전트 리소스 추가
- AnyConnect Windows Compliance Module 3.6.10591.2를 선택하고 Save(저장)를 클릭합니다.

Download Remote Resources ✕

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Windows
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 3.6.10591.2	AnyConnect OS X Compliance Module 3.6.10591.2
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleWindows 3.6.10591.2	AnyConnect Windows Compliance Module 3.6.10591.2
<input type="checkbox"/>	ComplianceModule 3.6.10591.2	NACAgent ComplianceModule v3.6.10591.2 for Windows
<input type="checkbox"/>	MACComplianceModule 3.6.10591.2	MACAgent ComplianceModule v3.6.10591.2 for MAC OSX
<input type="checkbox"/>	MacOsXAgent 4.9.0.1006	NAC Posture Agent for Mac OSX (ISE 1.2 release)
<input type="checkbox"/>	MacOsXAgent 4.9.0.1007	NAC Posture Agent for Mac OSX v4.9.0.1007 (with CM 3.6.7873.2)- ISE
<input type="checkbox"/>	MacOsXAgent 4.9.0.655	NAC Posture Agent for Mac OSX (ISE 1.1.1 or later)
<input type="checkbox"/>	MacOsXAgent 4.9.0.661	NAC Posture Agent for Mac OS X v4.9.0.661 with CM v3.5.7371.2 (ISE
<input type="checkbox"/>	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3 and Abov
<input type="checkbox"/>	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12, ISE 1.3 rel
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1.3 Release)
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE 1.2 release
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE 1.2 release
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE 1.2 release
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE 1.2 Patch
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.36	Supplicant Provisioning Wizard for Mac OsX 1.0.0.36 (for ISE 1.2 Patch

For AnyConnect software, please download from <http://cisco.com/go/anyconnect>. Use the "Agent resource from local disk" add option, to import into ISE

4단계. AnyConnect 구성 추가

- Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동하고 AnyConnect Configuration(AnyConnect 컨피그레이션 추가)
- 이름을 구성하고 규정 준수 모듈 및 필요한 모든 AnyConnect 모듈(VPN, AMP 및 Posture)을 선택합니다.
- Profile Selection(프로필 선택)에서 각 모듈에 대해 이전에 구성된 프로필을 선택합니다.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

AnyConnect Configuration > AnyConnect Configuration AMP

- Select AnyConnect Package: AnyConnectDesktopWindows 4.2.2075.0
- Configuration Name: AnyConnect Configuration AMP
- Description: [Empty text box]
- Description Value
- Compliance Module: AnyConnectComplianceModuleWindows 3.6.10591.2

AnyConnect Module Selection

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Start Before Logon
- Diagnostic and Reporting Tool

Profile Selection

- ISE Posture: AC Posture Profile
- VPN: VPNDisable_ServiceProfile
- Network Access Manager: [Empty dropdown]
- Web Security: [Empty dropdown]
- AMP Enabler: AMP Profile
- Network Visibility: [Empty dropdown]
- Customer Feedback: [Empty dropdown]

5단계. 클라이언트 프로비저닝 규칙 구성

이전에 생성한 AnyConnect 컨피그레이션은 클라이언트 프로비저닝 규칙에서 참조됩니다.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

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
Windows_Posture_AMP	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration AMP

6단계. 권한 부여 정책 구성

먼저 클라이언트 프로비저닝 포털로 리디렉션합니다. 상태에 대한 표준 권한 부여 정책이 사용됩니다.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > AMP_Profile

Authorization Profile

* Name AMP_Profile

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL ACL_WEBAUTH_REDIRECT Value Client Provisioning Portal (defa

Display Certificates Renewal Message

Static IP/Host name/FQDN

Advanced Attributes Settings

Select an item =

규정 준수 후 전체 액세스가 할당됩니다.

Authorization Policy

Define the Authorization Policy by configuring rules based on Identity groups and/or other conditions. Drag and drop rules to change the order.
 For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (1)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
2. <input checked="" type="checkbox"/>	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
1. <input checked="" type="checkbox"/>	Non_Compliant_Devices_Access	if Session:PostureStatus NOT_EQUALS Compliant	then AMP_Profile
<input type="checkbox"/>	Employee_EAP-TLS	if (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD
<input type="checkbox"/>	Employee_Onboarding	if (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD
<input checked="" type="checkbox"/>	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests
<input checked="" type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then VA_Scan
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

7단계. TC-NAC 서비스 활성화

Administration(관리) > Deployment(구축) > Edit Node(노드 수정)에서 TC-NAC Services(TC-NAC 서비스)를 활성화합니다. Enable Threat Centric NAC Service(Threat Centric NAC 서비스 활성화) 확인란을 선택합니다.

Deployment Nodes List > ISE21-3ek

Edit Node

General Settings Profiling Configuration

Hostname **ISE21-3ek**
 FQDN **ISE21-3ek.example.com**
 IP Address **10.62.145.25**
 Node Type **Identity Services Engine (ISE)**

Personas

Administration Role **STANDALONE** Make Primary

Monitoring Role **PRIMARY** Other Monitoring Node

Policy Service

Enable Session Services Include Node in Node Group **None**

Enable Profiling Service

Enable Threat Centric NAC Service

8단계. AMP 어댑터 구성

Administration(관리) > Threat Centric NAC > Third Party Vendors(서드파티 벤더) > Add(추가)로 이동합니다. Save(저장)를 클릭합니다.

Vendor Instances > New
Input fields marked with an asterisk (*) are required.

Vendor * AMP : THREAT

Instance Name * AMP_THREAT

Cancel Save

구성 준비 상태로 전환해야 합니다. Ready to Configure(구성 준비)를 클릭합니다.

Vendor Instances
0 Selected

Refresh Add Trash Edit Filter Settings

Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
QualysVA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active
AMP_THREAT	AMP	THREAT		Disconnected	Ready to configure

Cloud(클라우드)를 선택하고 Next(다음)를 클릭합니다.

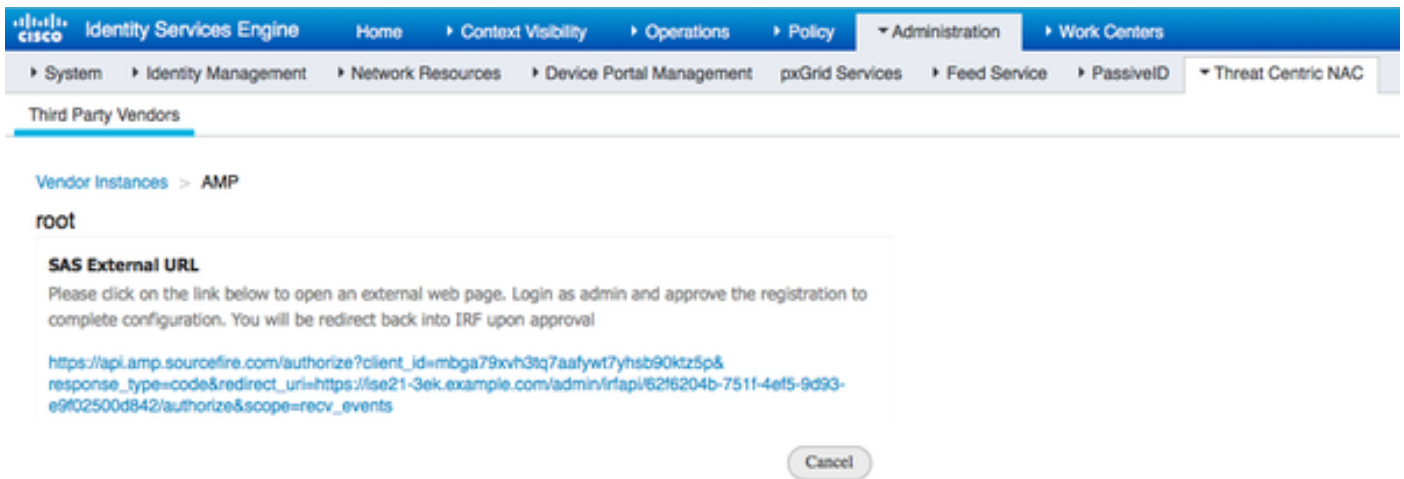
Vendor Instances > AMP

Cloud
US Cloud

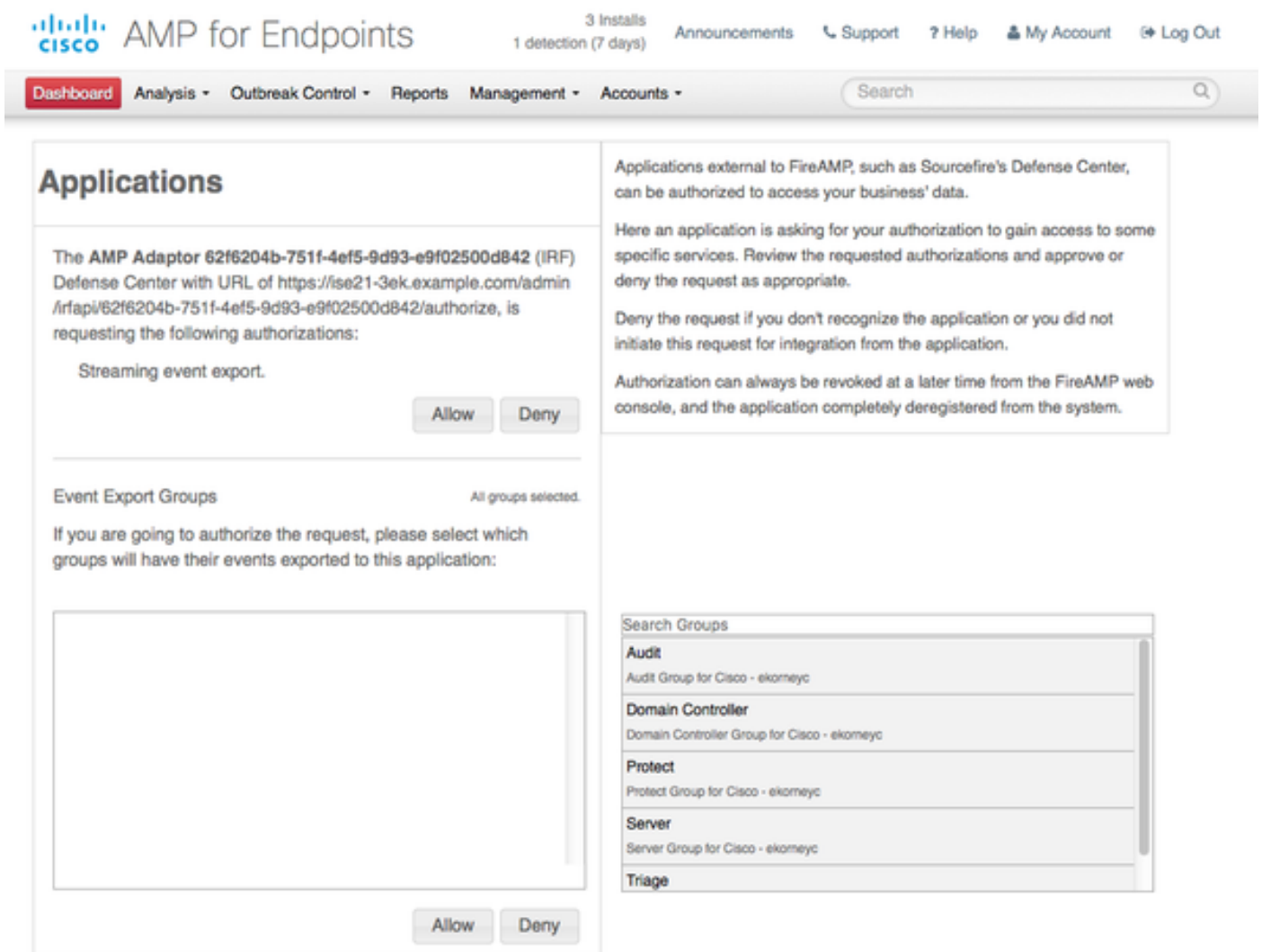
Which public cloud would you like to connect to

Cancel Next

FireAMP 링크를 클릭하고 FireAMP에서 관리자로 로그인합니다.



Applications(애플리케이션) 패널에서 Allow(허용)를 클릭하여 Streaming Event Export(스트리밍 이벤트 내보내기) 요청을 인증합니다. 해당 작업 후 Cisco ISE로 다시 리디렉션됩니다.



모니터링할 이벤트(예: 의심스러운 다운로드, 의심스러운 도메인에 대한 연결, 실행된 악성코드, java 보안 침해)를 선택합니다. 어댑터 인스턴스 구성의 요약이 구성 요약 페이지에 표시됩니다. 어댑터 인스턴스가 연결/활성 상태로 전환됩니다.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Third Party Vendors

Vendor Instances

0 Selected

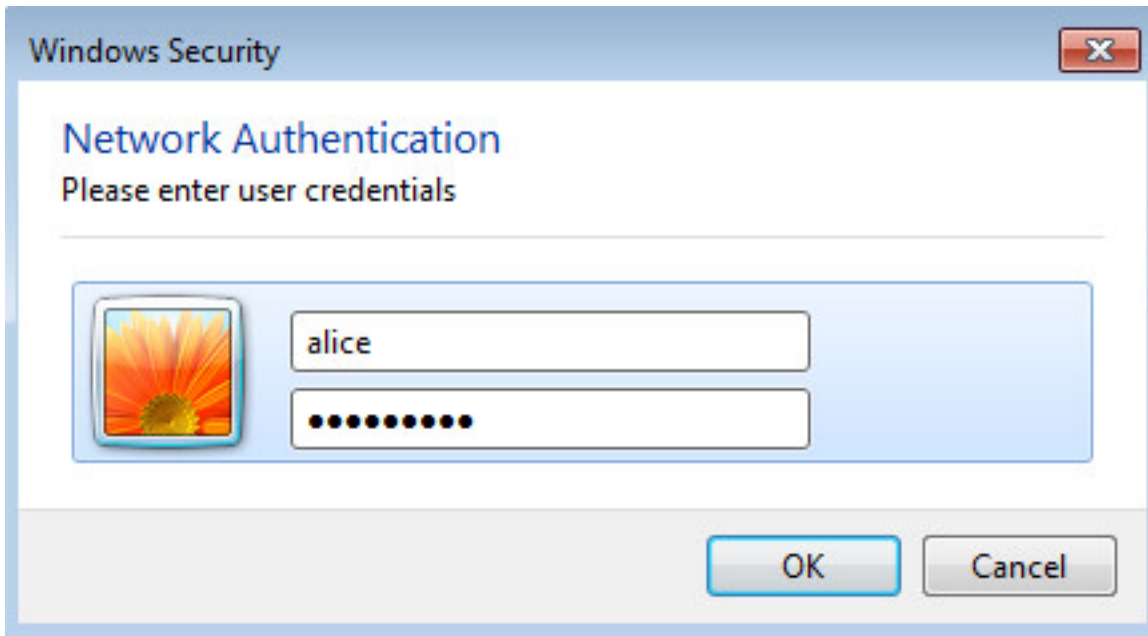
Refresh Add Trash Edit Filter Settings

Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
QUALYS_VA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active

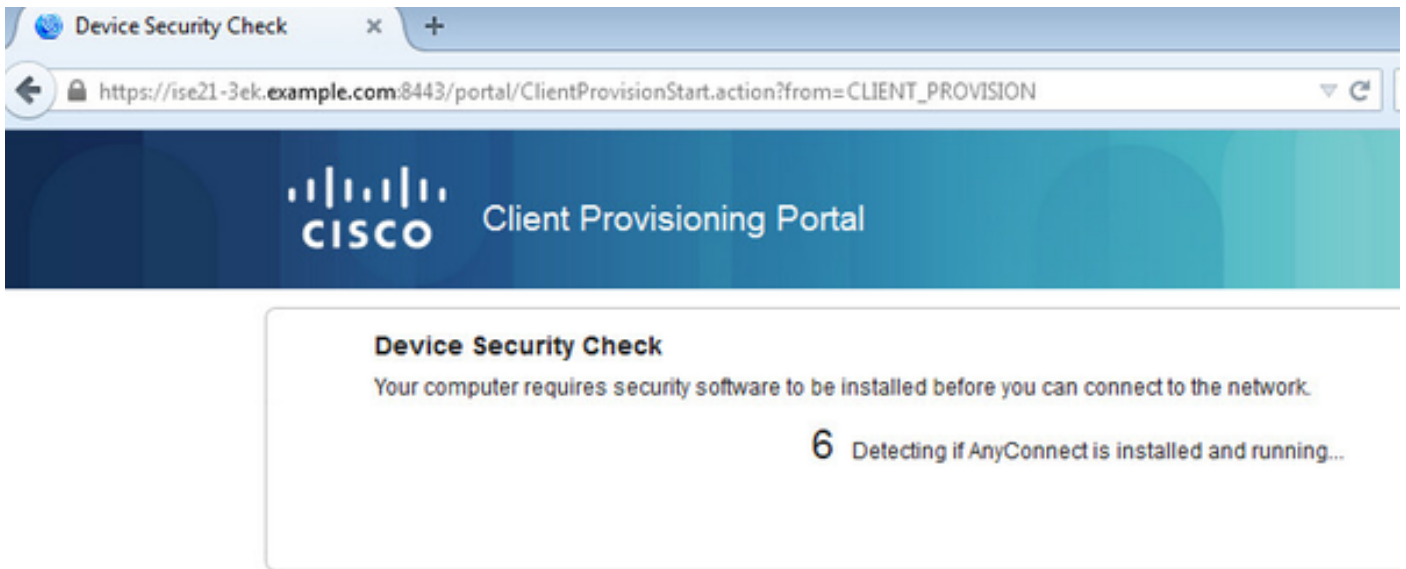
다음을 확인합니다.

엔드포인트

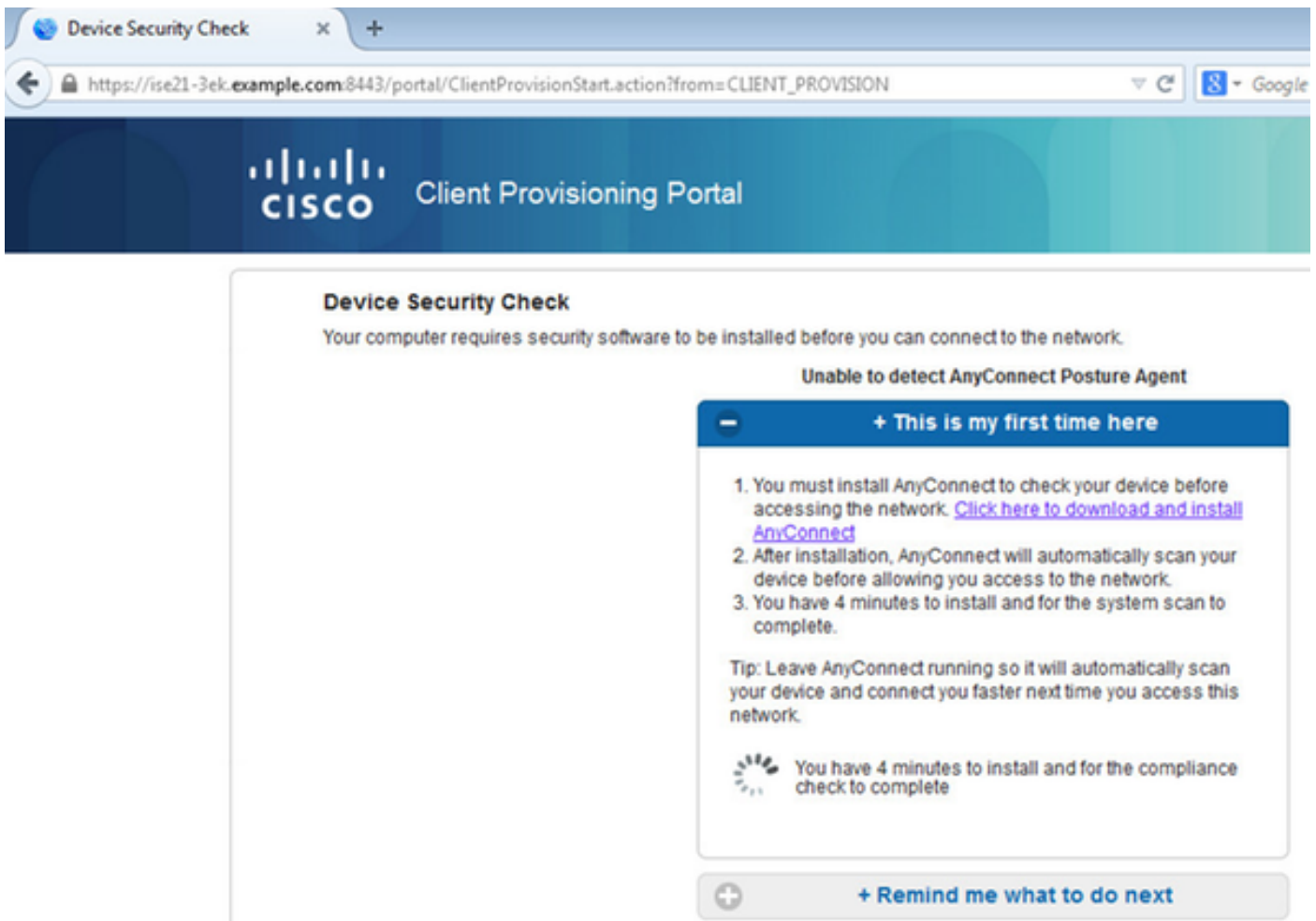
PEAP(MSCHAPv2)를 통해 무선 네트워크에 연결합니다.



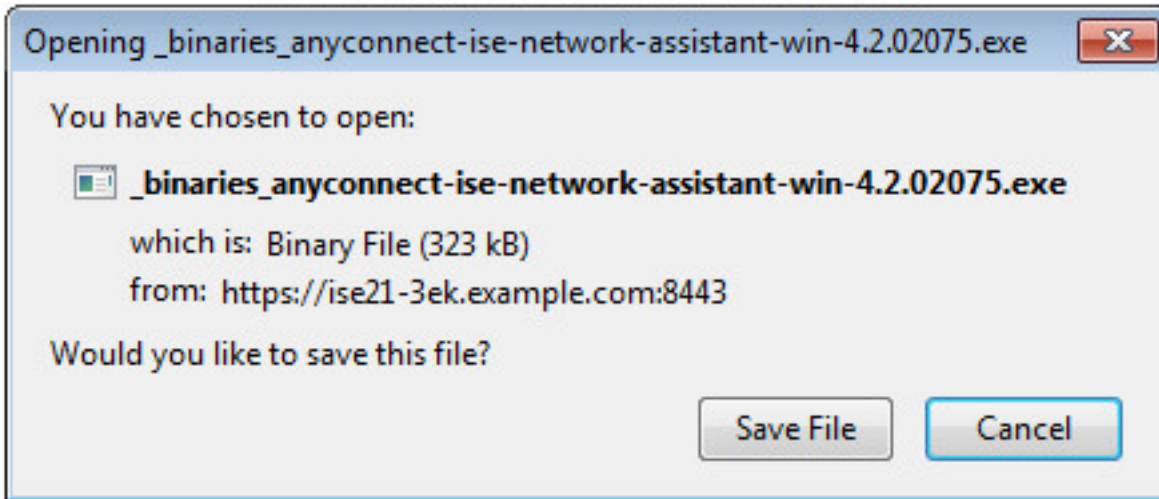
클라이언트 프로비저닝 포털에 연결된 리디렉션이 수행됩니다.



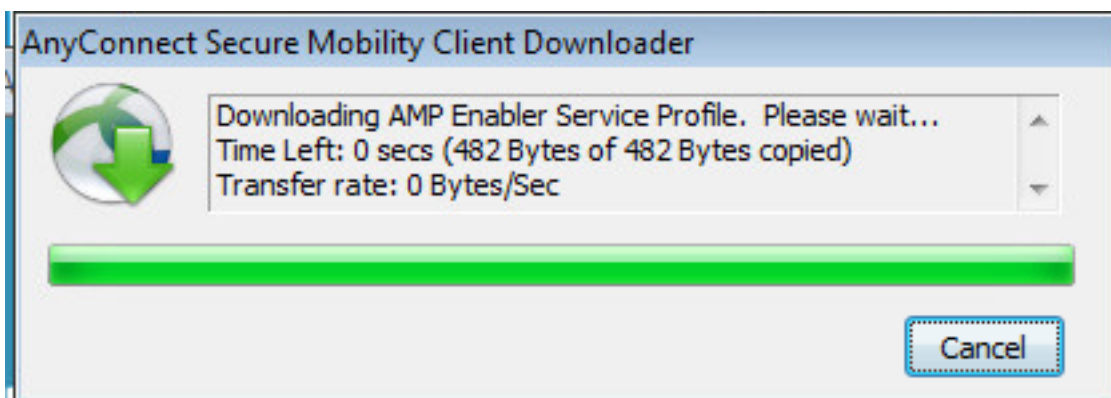
클라이언트 시스템에 아무것도 설치되어 있지 않으므로 ISE는 AnyConnect 클라이언트 설치를 묻는 메시지를 표시합니다.

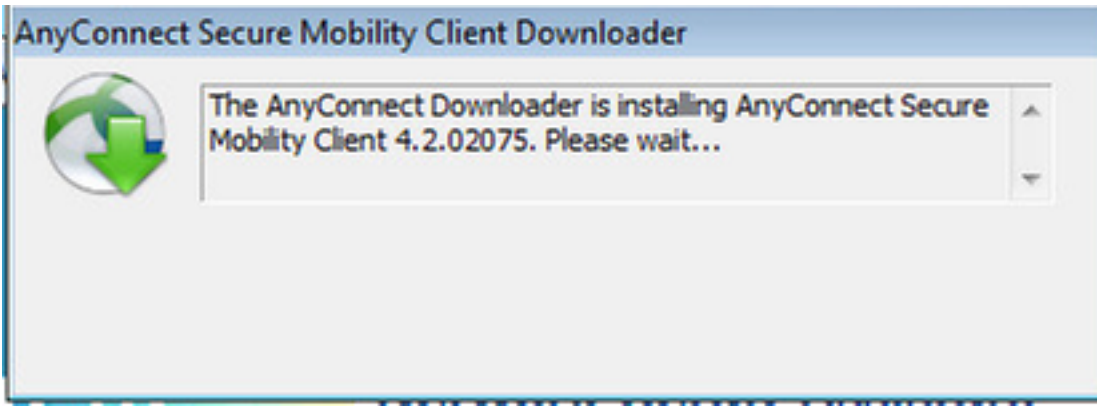


NSA(Network Setup Assistant) 애플리케이션은 클라이언트 시스템에서 다운로드하여 실행해야 합니다.

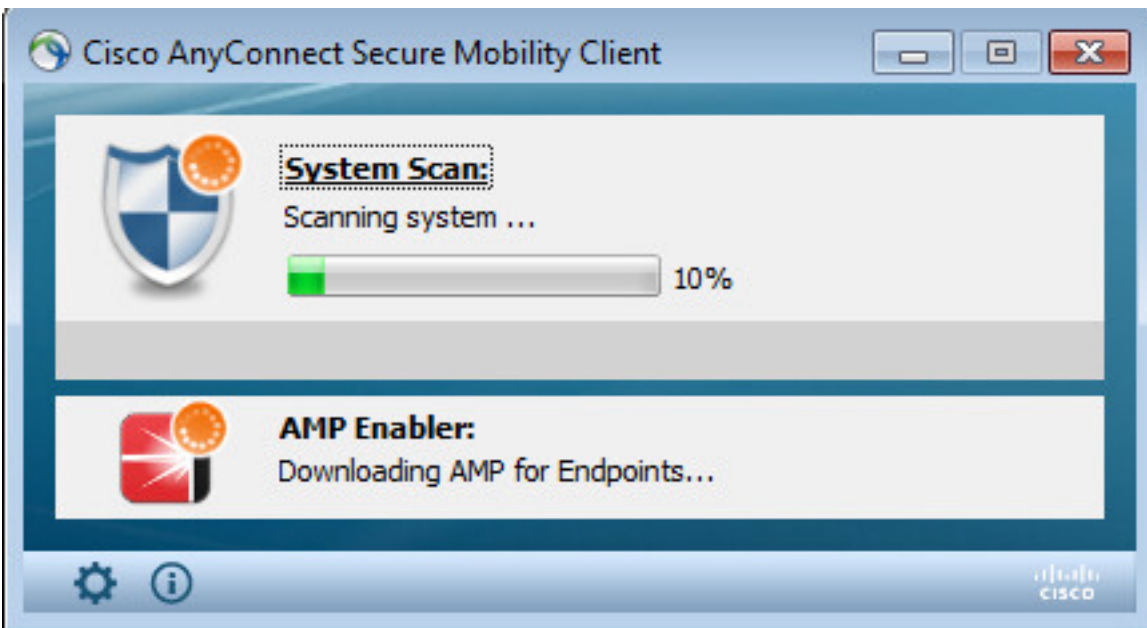
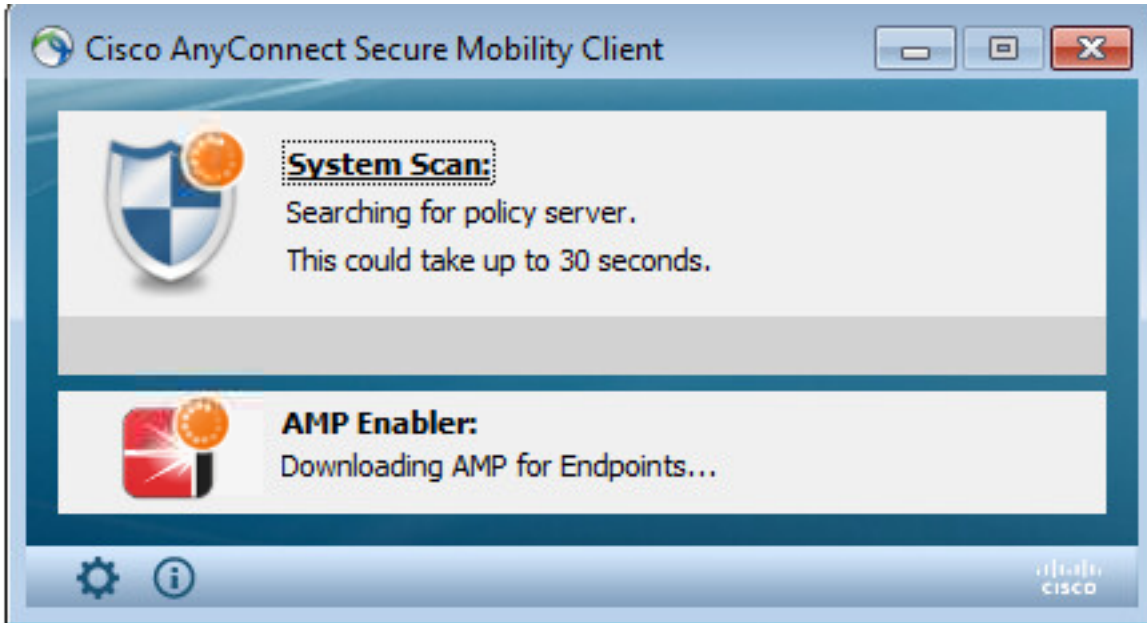


NSA는 필요한 구성 요소 및 프로파일을 설치하는 것을 관리한다.

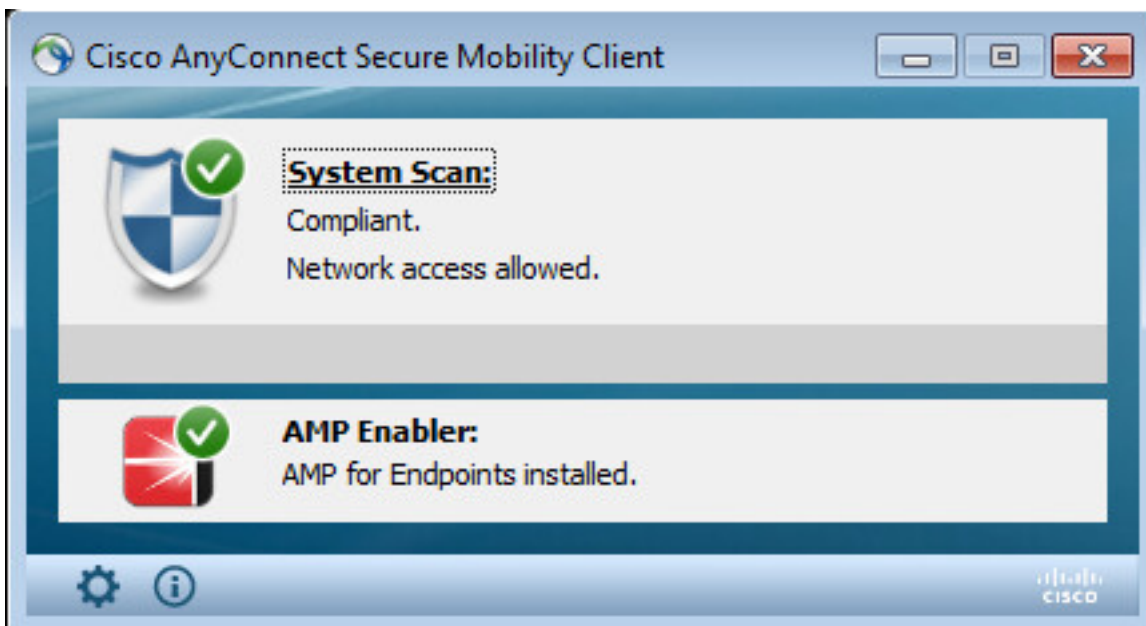
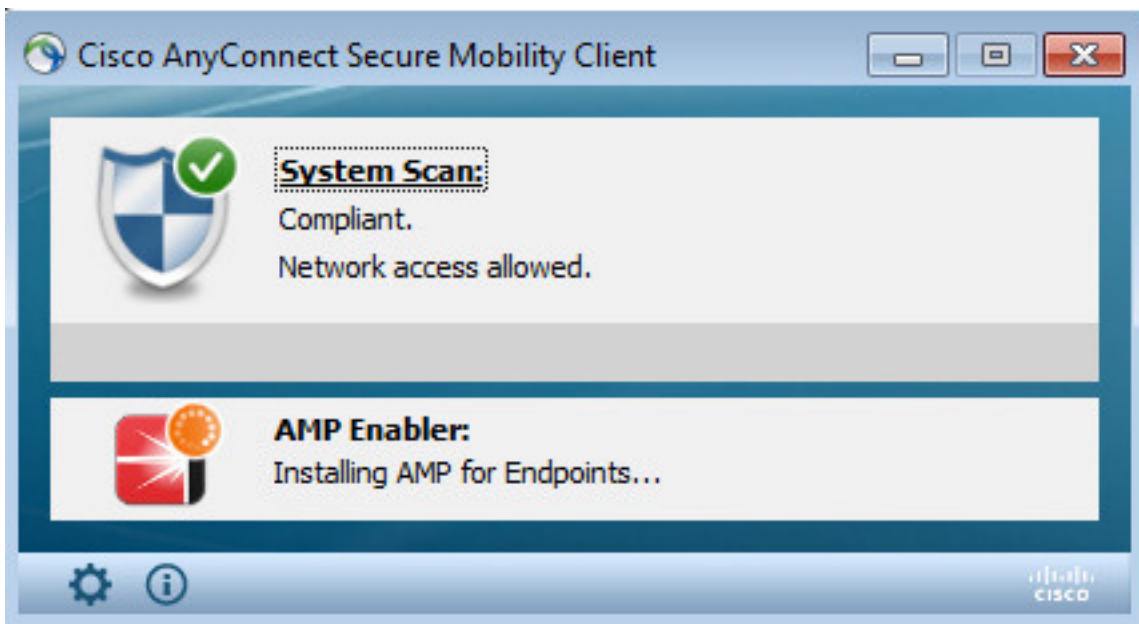
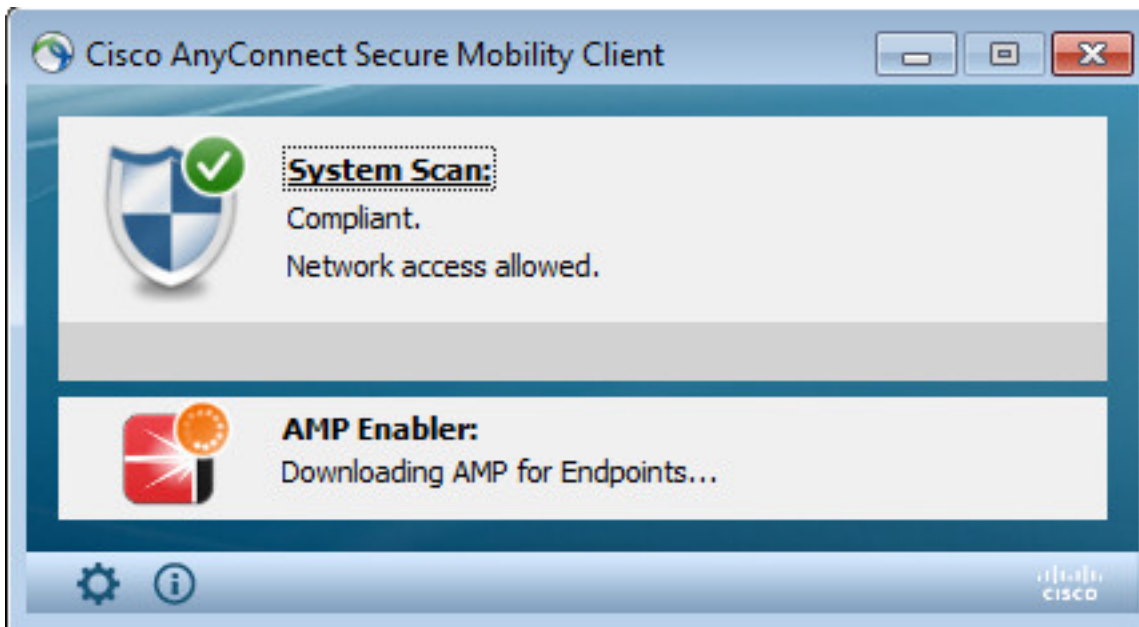




설치가 완료되면 AnyConnect Posture 모듈은 규정 준수 확인을 수행합니다.



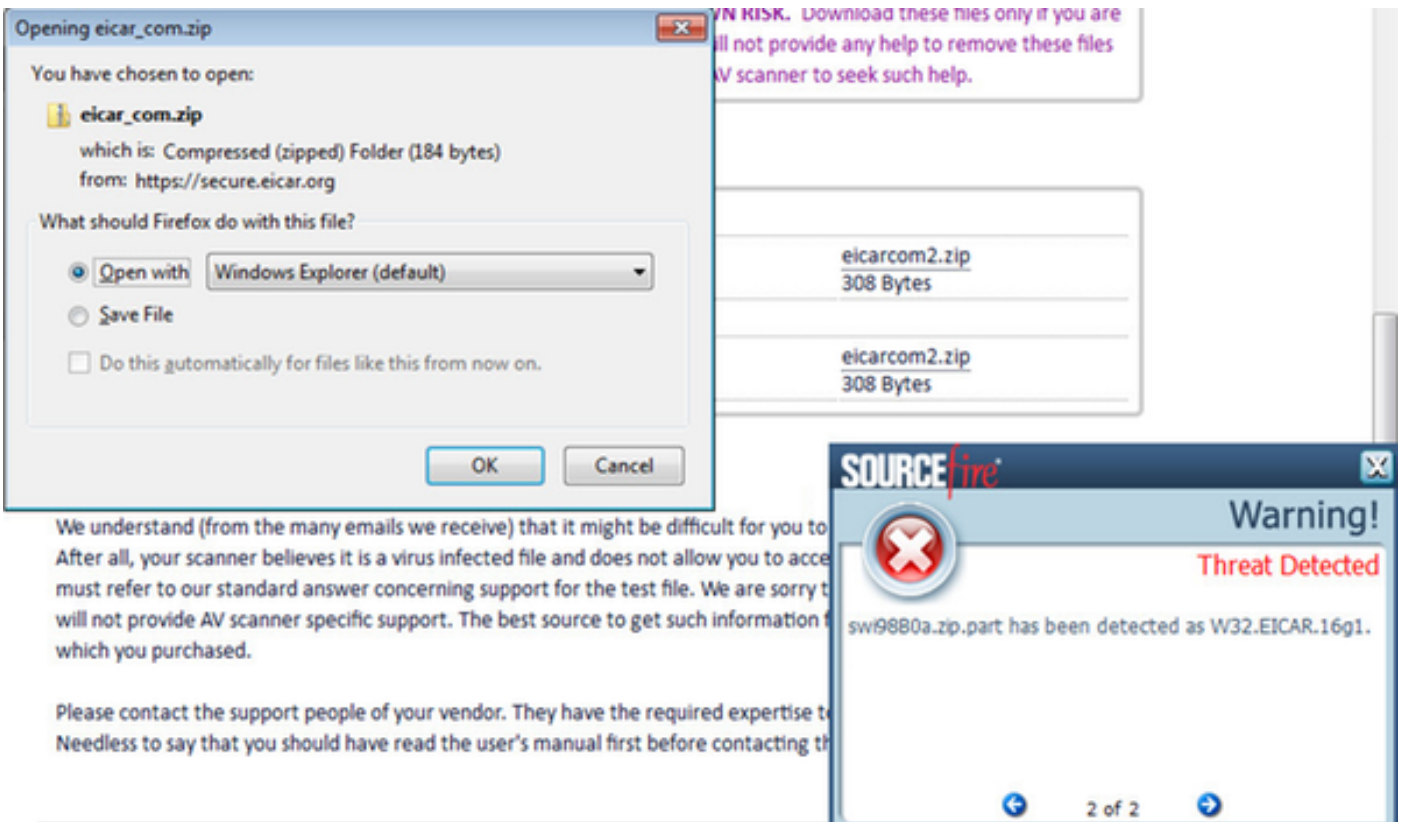
전체 액세스 권한이 부여되면 엔드포인트가 규정을 준수하는 경우 AMP 프로파일의 앞부분에서 지정한 웹 서버에서 AMP를 다운로드하여 설치합니다.



AMP Connector가 나타납니다.

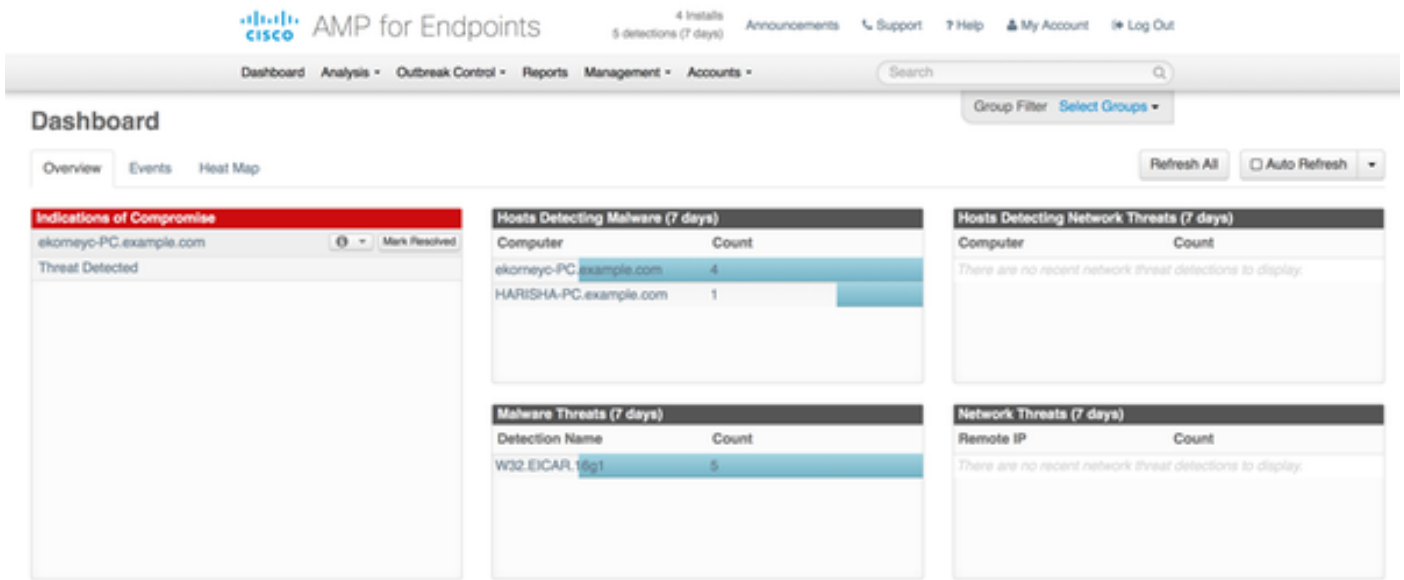


AMP를 실제로 테스트하려면 zip 파일에 포함된 Eicar 문자열이 다운로드됩니다. 위협이 탐지되어 AMP 클라우드에 보고됩니다.

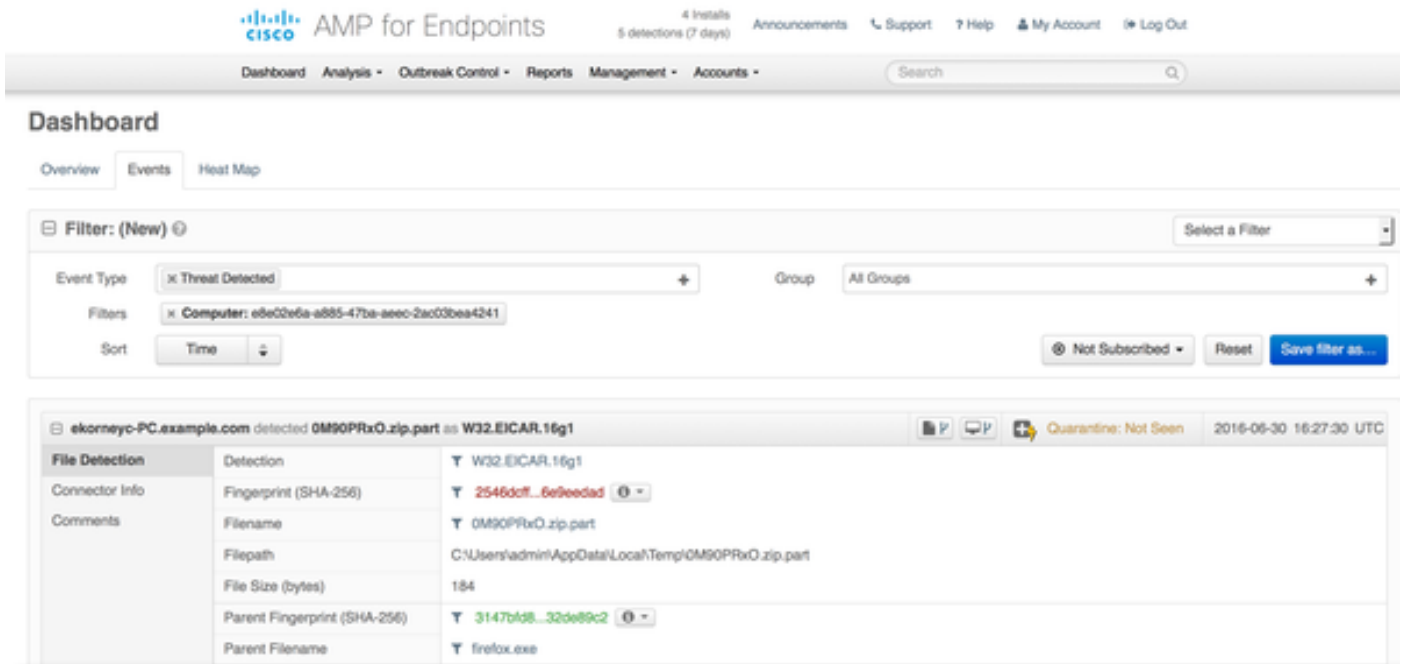


AMP 클라우드

위협 대시보드의 세부 정보를 확인하려면 AMP 클라우드의 대시보드를 사용할 수 있습니다.



위협, 파일 경로 및 핑거핀에 대한 자세한 내용을 보려면 악성코드가 탐지된 호스트를 클릭할 수 있습니다.



ISE의 인스턴스를 보거나 등록 취소하려면 Accounts > Applications로 이동할 수 있습니다

Applications

AMP Adaptor 4d4047dc-4791-477d-955f-6a0f182ae65b IRF	Edit Deregister
AMP Adaptor fe80e16e-cde8-4d7f-a836-545416ae56f4 IRF	Edit Deregister

These are applications external to FireAMP, such as Sourcefire's Defense Center, that you have authorized to access your business' data.

Here you can deauthorize registered applications, thus revoking their access to specific functionality, or you can deregister the applications, thus deauthorizing them and completely removing them from the FireAMP system.

You can currently authorize Defense Center appliances to receive streaming FireAMP events for integration with the Defense Center.

ISE

ISE 자체에서 일반 상태 플로우가 확인되면 네트워크 규정 준수를 확인하기 위해 리디렉션이 먼저 수행됩니다. 엔드포인트가 규정을 준수하는 즉시 CoA Reauth가 전송되고 PermitAccess가 포함된 새 프로파일이 할당됩니다.

Summary Metrics:

- Misconfigured Supplicants: 0
- Misconfigured Network Devices: 0
- RADIUS Drops: 14
- Client Stopped Responding: 3
- Repeat Counter: 0

Time	Status	Details	Repeat	Identify	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Jun 30, 2016 05:50:18.728 PM	●		0	alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Compliant_Device_A...	PermitAccess	10.62.148.26
Jun 30, 2016 05:49:26.479 PM	●			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Compliant_Device_A...	PermitAccess	
Jun 30, 2016 05:49:34.437 PM	●			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Compliant_Device_A...	PermitAccess	
Jun 30, 2016 05:42:56.536 PM	●			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Non-Compliant_Devis...	AMP_Profile	

탐지된 위협을 보려면 Context Visibility(상황 가시성) > Endpoints(엔드포인트) > Compromised Endpoints(감염된 엔드포인트)로 이동할 수 있습니다.

COMPROMISED ENDPOINTS BY INCIDENTS

IMPACT LEVEL: Unknown, Insignificant, Distracting, Painful, Damaging, Catastrophic

COMPROMISED ENDPOINTS BY INDICATORS

LIKELY IMPACT LEVEL: Unknown, None, Low, Medium, High

MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivity
02-4A:00:14-8D-4B	alice	10.62.148.26	Threat Detected	AMP	Painful	Location/FBI Locations	Connected

엔드포인트를 선택하고 Threat(위협) 탭으로 이동하면 추가 세부사항이 표시됩니다.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there are navigation tabs: Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below these are sub-tabs for Endpoints and Network Devices. The main content area displays details for an endpoint with MAC address C0:4A:00:14:8D:4B. The endpoint's username is 'alice', profile is 'Windows7-Workstation', and current IP address is '10.62.148.26'. Below the details, there are tabs for Attributes, Authentication, Threats, and Vulnerabilities. The 'Threats' tab is active, showing a 'Threat Detected' event. The event details are: Type: INCIDENT, Severity: Painful, Reported by: AMP, and Reported at: 2016-06-30 11:27:48.

엔드포인트에 대해 위협 이벤트가 탐지되면 Comproted Endpoints(감염된 엔드포인트) 페이지에서 엔드포인트의 MAC 주소를 선택하고 ANC 정책(구성된 경우, 격리 등)을 적용할 수 있습니다. 또는 Change of Authorization을 실행하여 세션을 종료할 수 있습니다.

The screenshot shows the 'Compromised Endpoints' page in the Cisco ISE interface. It features two bar charts: 'COMPROMISED ENDPOINTS BY INCIDENTS' and 'COMPROMISED ENDPOINTS BY INDICATORS'. Below the charts, there is a table of threat events. The table has columns for Source, Threat Severity, Logical NAD Location, Connectivity, Hostname, Identity Group, and Endpoint OS. A dropdown menu is open over the 'Change Authorization' button, showing options like 'CoA Session Result', 'CoA Session Terminate', 'CoA Port Bounce', 'CoA SArat Session Query', 'CoA Session termination with port bounce', and 'CoA Session termination with port shutdown'. The table shows two entries: one with Source 'AMP', Threat Severity 'Painful', and Connectivity 'Disconnected', and another with Source 'AMP', Threat Severity 'Painful', and Connectivity 'Connected'.

CoA Session Terminate(CoA 세션 종료)를 선택하면 ISE는 CoA Disconnect를 전송하고 클라이언트는 네트워크에 대한 액세스 권한을 잃게 됩니다.

Other Attributes

ConfigVersionId	72
Acct-Terminate-Cause	Admin Reset
Event-Timestamp	1467305830
NetworkDeviceProfileName	Cisco
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
IsThirdPartyDeviceFlow	false
AcsSessionID	cfec88ac-6d2c-4b54-9fb6-716914f18744
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
Device IP Address	10.62.148.120
CiscoAVPair	audit-session-id=0a3e9478000009ab5775481d

문제 해결

ISE에서 디버그를 활성화하려면 Administration(관리) > System(시스템) > Logging(로깅) > Debug Log Configuration(디버그 로그 컨피그레이션)으로 이동하여 TC-NAC Node(TC-NAC 노드)를 선택하고 TC-NAC 구성 요소의 **Log Level(로그 레벨)**을 DEBUG로 변경합니다.

Component Name	Log Level	Description
TC-NAC	DEBUG	TC-NAC log messages

확인할 로그 - irf.log. ISE CLI에서 직접 확인할 수 있습니다.

```
ISE21-3ek/admin# show logging application irf.log tail
```

AMP 클라우드에서 위협 수신까지

```
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:53 -:::--
com.cisco.cpm.irf.irf.service.IrfIrfIrfMessageHandler{MessageType =NOTIFICATION,
messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b":[{"":{"Impact_Qualification":""}, "
":1467304068599, "": "AMP", "": "Threat Detected"}]', priority=0, timestamp=Thu Jun 30 18:27:48
CEST 2016, amqpEnvelope=Envelope=79, redeliver=false, exchange=irf.topic.events,
routingKey=irf.events.threat), amqpProperties=#contentHeader<basic>(content-
type=application/json-encoding headers=null, content-encoding headers=null=null, delivery-
mode=null, priority=0, correlation-id=null, reply-to=null, expiration=null, message-
id=THREAT_EVENT, timestamp=null, type=NOTIFICATION, user-id=null, app-id=fe80e16e-cde8-4d7f-
a836-5455456ae5556f4, cluster-id=null)}
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.service.IrfNotificationHandler:handle:140 -:::--      .{messageType=NOTIFICATION,
messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b":[{"":{"Impact_Qualification":""}, "
":1467304068599, "": "AMP", "": "Threat Detected"}]}'', priority=0, timestamp=Thu 30 18:27:48 CEST
2016, amqpEnvelope=Envelope=79, redeliver=false, exchange=irf.topic.events,
routingKey=irf.events.threat), amqpProperties=#contentHeader<basic>(content-
type=application/json, content-encoding, content-headers=null, null, delivery Null, mode=null,
priority=0, correlation-id=null, reply-to=null, expiration=null, message-id=THREAT_EVENT,
timestamp=null, type=NOTIFICATION, user-id=null, app-id=fe80e-cde8-4d7f-a836-54545416ae556f4,
cluster-id=null)}
2016-06-30 18:27:48,617 [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:59 -:::-- DONE
:Envelope(deliveryTag=79, redeliver=false, exchange=irf.topic.events,
routingKey=irf.events.threat) #contentHeader<basic>(content-type=application/json, content-
encoding=null, headers=null, delivery-mode=null, priority=null, correlation-id=null,
correlation-id=null, reply-to=null, message-id=THREAT_EVENT, timestamp=null, type=null,
type=type=NOTIFICATION, USER-ID=USER-ID=ME, APP-ID=FE=NULL, APP-ID=NULL, APP-ID=FEID=NULL, APP-
ID=NULL, APP-ID=NULL, APP-ID=FEID=NULL, APP-ID=FEID=NULL, APP-ID=NULL, APP-ID=FEID=NULL, APP-
ID=NULL, APP-ID=NULL, APP-ID=FEID=NULL, APP-ID 116E-CDE8-4D7F-A836-545416AE56F4, CLUSTER-
ID=NULL)
2016-06-30 18:27:48,706 [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:parseNotification:221 -:::--      :
{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b":[{"":{"
":{"Impact_Qualification":""}, "":1467304068599, "": "AMP", "": "Threat Detected"}]}'', priority=0,
timestamp=Thu 30 18:27:48 CEST 2016, amqpEnvelope=Envelope=79, redeliver=false,
exchange=irf.topic.events, routingKey=irf.events.threat),
amqpProperties=#contentHeader<basic>(content-type=application/json, content-encoding, content-
headers=null, null, delivery Null, mode=null, priority=0, correlation-id=null, reply-to=null,
expiration=null, message-id=THREAT_EVENT, timestamp=null, type=NOTIFICATION, user-id=null, app-
id=fe80e-cde8-4d7f-a836-54545416ae556f4, cluster-id=null)}
```

위협에 대한 정보가 PAN으로 전송됩니다.

```
2016-06-30 18:27:48,724 DEBUG [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:storeEventsInES:366 -:::-- PAN      -
c:0:0:4a0:0:0:0:4a 14:8d:4b {incident={impact_Qualification= Fighting}, =1467304068599,
vendor=AMP, title=Threat Detected}
```