

Configure el NAC Amenaza-céntrico del 2.1 ISE (TC-NAC) con el AMP y los servicios de la postura

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Flujo detallado](#)

[Nube de la configuración AMP](#)

[Paso 1. Conector de la descarga de la nube AMP](#)

[Configuración ISE](#)

[Paso 1. Directivas y condiciones de la postura de la configuración](#)

[Paso 2. Perfil de la postura de la configuración](#)

[Paso 3. Perfil de la configuración AMP](#)

[Paso 2. Aplicaciones de la carga y perfil XML al ISE](#)

[Paso 3. Módulo de la conformidad de AnyConnect de la descarga](#)

[Paso 4. Agregue la configuración de AnyConnect](#)

[Paso 5. Reglas del aprovisionamiento del cliente de la configuración](#)

[Paso 6. Directivas de la autorización de la configuración](#)

[Paso 7. Servicios del permiso TC-NAC](#)

[Paso 8. Adaptador de la configuración AMP](#)

[Verificación](#)

[Punto final](#)

[Nube AMP](#)

[ISE](#)

[Troubleshooting](#)

Introducción

Este documento describe cómo configurar el NAC Amenaza-céntrico con la protección anticipada de Malware (AMP) en el 2.1 del Identity Services Engine (ISE). Los niveles de gravedad de la amenaza y los resultados de la evaluación de vulnerabilidades se pueden utilizar para controlar dinámicamente el nivel de acceso de un punto final o de un usuario. Los servicios de la postura son también se cubran como una parte de este documento.

Note: El propósito del documento es describir la integración del 2.1 ISE con el AMP, Posture los servicios se muestra como los requieren cuando provision el AMP del ISE.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

- Motor del servicio de la identidad de Cisco
- Protección anticipada de Malware

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 2.1 del motor del servicio de la identidad de Cisco
- Regulador del Wireless LAN (WLC) 8.0.121.0
- Cliente VPN 4.2.02075 de AnyConnect
- Service Pack 1 de Windows 7

Configurar

Diagrama de la red



Flujo detallado

1. El cliente conecta con la red, se asigna el **AMP_Profile** y reorientan al usuario al portal de disposición de Anyconnect. Si Anyconnect no se detecta en la máquina, todos los módulos configurados (VPN, AMP, postura) están instalados. La configuración se avanza para cada

módulo junto con ese perfil

2. Una vez que Anyconnect está instalado, la evaluación de la postura se ejecuta
3. El módulo del Enabler AMP instala el conector de FireAMP
4. Cuando el cliente intenta descargar el software malévolo, el conector AMP lanza un mensaje de advertencia y lo señala a la nube AMP
5. La nube AMP envía esta información al ISE

Nube de la configuración AMP

Paso 1. Conector de la descarga de la nube AMP

Para descargar el conector, navegue al conector de la Administración > de la descarga. Entonces seleccione el tipo y la **descarga** FireAMP (Windows, Android, mac, Linux). En este caso la **auditoría** fue seleccionada y el archivo de instalación de FireAMP para Windows.

The screenshot shows the Cisco AMP for Endpoints interface. At the top, there's a navigation bar with the Cisco logo and 'AMP for Endpoints'. To the right, it shows '3 Installs', '1 detection (7 days)', and links for 'Announcements', 'Support', 'Help', 'My Account', and 'Log Out'. Below this is a secondary navigation bar with 'Dashboard', 'Analysis', 'Outbreak Control', 'Reports', 'Management', and 'Accounts'. A search bar is on the right. The main content area is titled 'Download Connector'. There's a 'Group' dropdown menu set to 'Audit'. Below this, there are four connector cards for different operating systems: Windows, Mac, Linux, and Android. Each card shows the connector name, a gear icon for configuration, and a list of options with checkboxes. For Windows, the options are 'Flash Scan on Install' and 'Redistributable'. For Mac, it's 'Flash Scan on Install'. For Linux, it's 'Flash Scan on Install'. For Android, it's 'Default FireAMP Android'. Each card has 'Show URL' and 'Download' buttons.

Note: Descargar este archivo genera un archivo del .exe llamado **Audit_FireAMPSetup.exe** en el ejemplo. Este archivo fue enviado al servidor Web para estar disponible una vez que el usuario pide la configuración del AMP.

Configuración ISE

Paso 1. Directivas y condiciones de la postura de la configuración

Navegue a la directiva > a los elementos > a las condiciones > a la postura > al archivo Condition.You de la directiva puede ver que una condición simple para la existencia del archivo se ha creado. El archivo tiene que existir si el punto final es ser obediente con la directiva verificada por el módulo de la postura:

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

* File Operator: Exists

C:\test.bt

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

Esta condición se utiliza para un requisito:

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

El requisito se utiliza en la directiva de la postura para los sistemas de Microsoft Windows:

Status	Rule Name	Identity Groups	Operating Systems	Compliance Module	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Windows_Posture	if Any	and Windows All	and Any version	and	then File_Requirement

Paso 2. Perfil de la postura de la configuración

- Navegue a la directiva > a los elementos de la directiva > a los resultados > al aprovisionamiento > a los recursos del cliente y agregue el perfil de la postura del agente del Network Admission Control (NAC) o del agente de AnyConnect
- Seleccione Anyconnect

ISE Posture Agent Profile Settings > **New Profile**

Posture Agent Profile Settings

AnyConnect

* Name: AC Posture Profile

Description:

Agent Behavior

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

- De la sección de protocolo de la postura agregue * para permitir que el agente conecte con todos los servidores

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

Paso 3. Perfil de la configuración AMP

El perfil AMP contiene la información donde se localiza el instalador de Windows. El instalador de

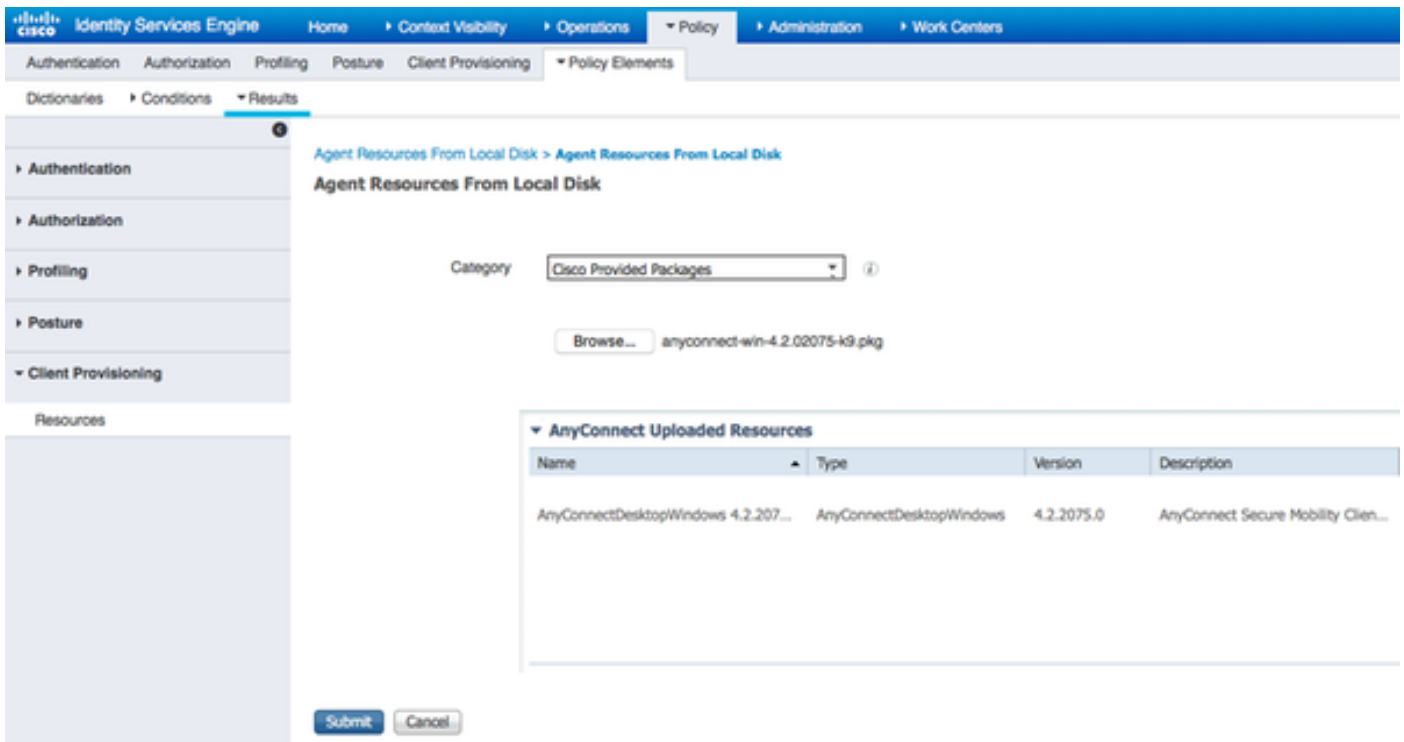
Windows fue descargado anterior de la nube AMP. Debe ser accesible de la máquina del cliente. El certificado del servidor HTTPS, donde se localiza el instalador se debe confiar en por la máquina del cliente también.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Elements > Results. The left sidebar shows a navigation menu with 'Client Provisioning' selected. The main content area is titled 'AMP Enabler Profile Settings > New Profile' and 'AMP Enabler Profile'. The form includes the following fields and options:

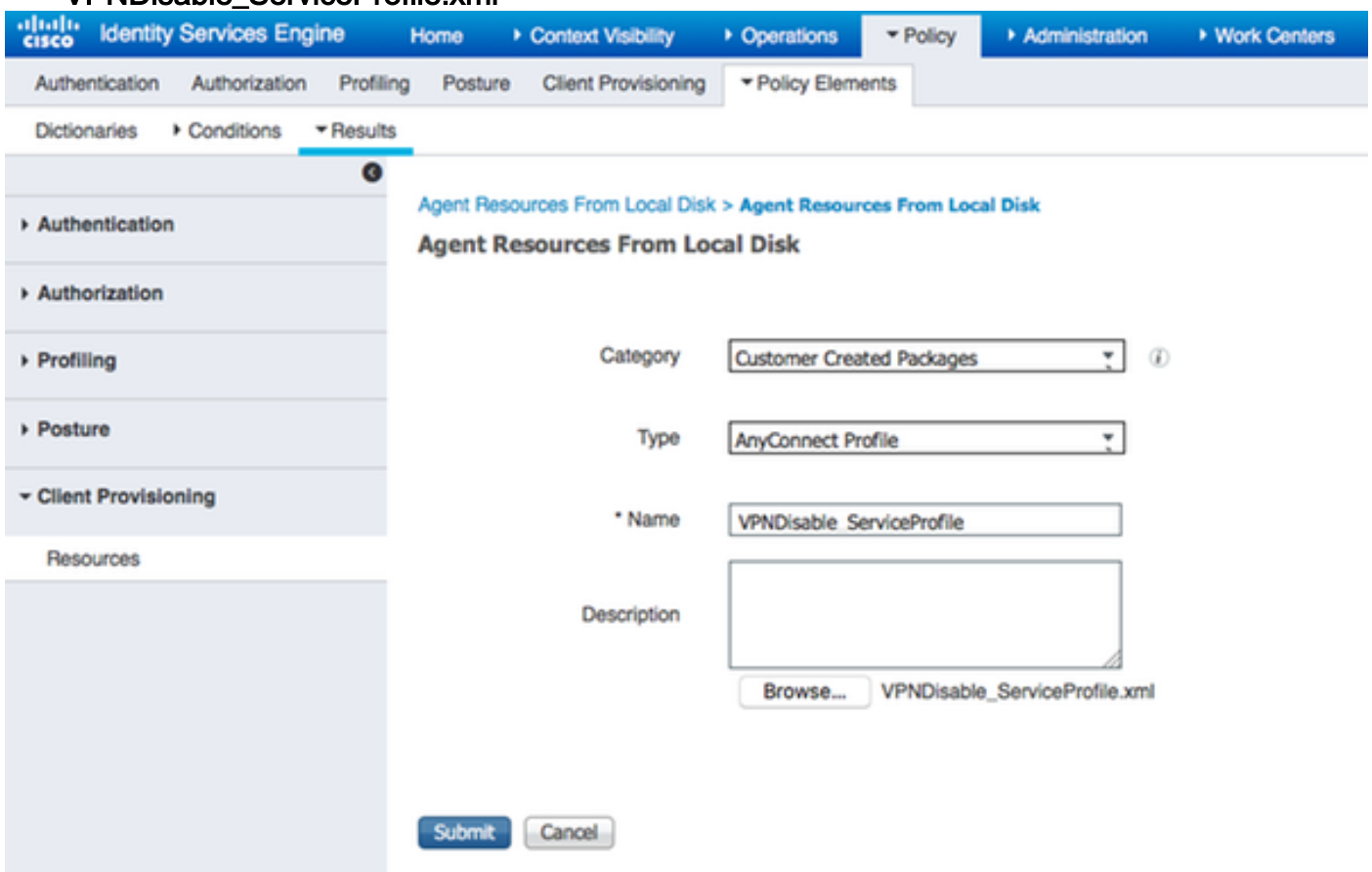
- * Name: AMP Profile
- Description: (empty field)
- Install AMP Enabler: (selected)
- Uninstall AMP Enabler:
- Windows Installer: [https://win2012ek.example.com/Downloads/Audit_FireAMPSetup.](https://win2012ek.example.com/Downloads/Audit_FireAMPSetup) [Check]
- MAC Installer: <https://> [Check]
- Windows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

Paso 2. Aplicaciones de la carga y perfil XML al ISE

- Descargue la aplicación manualmente del sitio de Cisco del funcionario: **anyconnect-win-4.2.02075-k9.pkg**
- En el ISE, navegue a la directiva > a los elementos de la directiva > a los resultados > al aprovisionamiento > a los recursos del cliente, y agregue a los **recursos del agente del disco local**
- Elija Cisco proporcionó a los paquetes y a **anyconnect-win-4.2.02075-k9.pkg** selecto



- Navegue a la directiva > a los elementos de la directiva > a los resultados > al aprovisionamiento > a los recursos del cliente y agregue a los **recursos del agente del disco local**
- Elija los **paquetes** y el **perfil creado cliente de AnyConnect** del tipo. Seleccione **VPNDisable_ServiceProfile.xml**



Note: **VPNDisable_ServiceProfile.xml** se utiliza para ocultar el título VPN, puesto que este ejemplo no utiliza el módulo VPN. Éste es el contenido de **VPNDisable_ServiceProfile.xml**:

```

xmlns <AnyConnectProfile de " http://schemas.xmlsoap.org/encoding/" del xmlns=: xsi del
xsi= el " http://www.w3.org/2001/XMLSchema-instance": schemaLocation= "
http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd " >
<ClientInitialization>
<ServiceDisable>true</ServiceDisable>
</ClientInitialization>
</AnyConnectProfile>

```

Paso 3. Módulo de la conformidad de AnyConnect de la descarga

- Navegue a la directiva > a los elementos de la directiva > a los resultados > al aprovisionamiento > a los recursos del cliente y agregue a los **recursos del agente del sitio de Cisco**
- Seleccione el **módulo 3.6.10591.2 de la conformidad de AnyConnect Windows** y haga clic en la **salvaguardia**

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 1.2.1 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

Paso 4. Agregue la configuración de AnyConnect

- Navegue a la directiva > a los elementos de la directiva > a los resultados > al aprovisionamiento > a los recursos del cliente, y agregue la **configuración de AnyConnect**
- Configure el nombre y seleccione el módulo y todos los módulos requeridos de AnyConnect (VPN, AMP, y la postura) de la conformidad
- En la **selección del perfil**, elija el perfil configurado anterior para cada módulo

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Profiling

Posture

Client Provisioning

Resources

AnyConnect Configuration > AnyConnect Configuration AMP

* Select AnyConnect Package: AnyConnectDesktopWindows 4.2.2075.0

* Configuration Name: AnyConnect Configuration AMP

Description:

DescriptionValue

* 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

Web Security

AMP Enabler: AMP Profile

Network Visibility

Customer Feedback

Paso 5. Reglas del aprovisionamiento del cliente de la configuración

La configuración de AnyConnect creada anterior se refiere a las reglas del aprovisionamiento del cliente

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
<input checked="" type="checkbox"/> Windows_Posture_AMP	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration AMP

Paso 6. Directivas de la autorización de la configuración

Primero el cambio de dirección al portal de disposición del cliente ocurre. Las directivas estándar de la autorización para la postura se utilizan.

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 =

Luego, una vez que es obediente, se asigna el acceso total

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

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

Paso 7. Servicios del permiso TC-NAC

Los servicios del permiso TC-NAC bajo la administración > despliegue > editan el nodo.
Checkbox **céntrico** del servicio del NAC de la amenaza del permiso del control.

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**

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

Paso 8. Adaptador de la configuración AMP

Navegue a la administración > al NAC > a los terceros proveedores céntricos de la amenaza > Add. Haga clic en la **salvaguardia**

Identity Services Engine Administration Work Centers

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

Third Party Vendors

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

Vendor * AMP : THREAT

Instance Name * AMP_THREAT

Cancel Save

Debe transición **alistar para configurar el estado**. Haga clic en **listo para configurar**

Identity Services Engine 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

<input type="checkbox"/>	Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
<input type="checkbox"/>	QualysVA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active
<input type="checkbox"/>	AMP_THREAT	AMP	THREAT		Disconnected	Ready to configure

Seleccione la **nube** y haga clic en **después**

Identity Services Engine Administration Work Centers

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

Third Party Vendors

Vendor Instances > AMP

Cloud

US Cloud

Which public cloud would you like to connect to

Cancel Next

Haga clic el link y el login de FireAMP como admin en FireAMP.

Third Party Vendors

Vendor Instances > AMP

root

SAS External URL

Please click on the link below to open an external web page. Login as admin and approve the registration to complete configuration. You will be redirect back into IRF upon approval

https://api.amp.sourcefire.com/authorize?client_id=mbga79xvh3tq7aafywt7yhsb90ktz5p&response_type=code&redirect_uri=https://ise21-3ek.example.com/admin/vrfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize&scope=recv_events

Cancel

El tecleo **permite** en el panel de las **aplicaciones** autorizar la petición de la exportación del evento que fluye. Después esa acción, le reorientan de nuevo a Cisco ISE

Applications

The AMP Adaptor 62f6204b-751f-4ef5-9d93-e9f02500d842 (IRF) Defense Center with URL of https://ise21-3ek.example.com/admin/vrfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize, is requesting the following authorizations:

Streaming event export.

Allow Deny

Event Export Groups All groups selected.

If you are going to authorize the request, please select which groups will have their events exported to this application:

[Empty selection box]

Allow Deny

Applications external to FireAMP, such as Sourcefire's Defense Center, can be authorized to access your business' data.

Here an application is asking for your authorization to gain access to some specific services. Review the requested authorizations and approve or deny the request as appropriate.

Deny the request if you don't recognize the application or you did not initiate this request for integration from the application.

Authorization can always be revoked at a later time from the FireAMP web console, and the application completely deregistered from the system.

Search Groups

- Audit**
Audit Group for Cisco - ekomeyc
- Domain Controller**
Domain Controller Group for Cisco - ekomeyc
- Protect**
Protect Group for Cisco - ekomeyc
- Server**
Server Group for Cisco - ekomeyc
- Triage**

Seleccione los eventos (por ejemplo, descarga sospechosa, conexión al dominio sospechoso, malware ejecutado, compromiso de las Javas) esos usted quisiera monitorear. El resumen de la configuración del caso del adaptador se visualiza en la página de resumen de la configuración. Transiciones del caso del adaptador al estado conectado/activo.

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

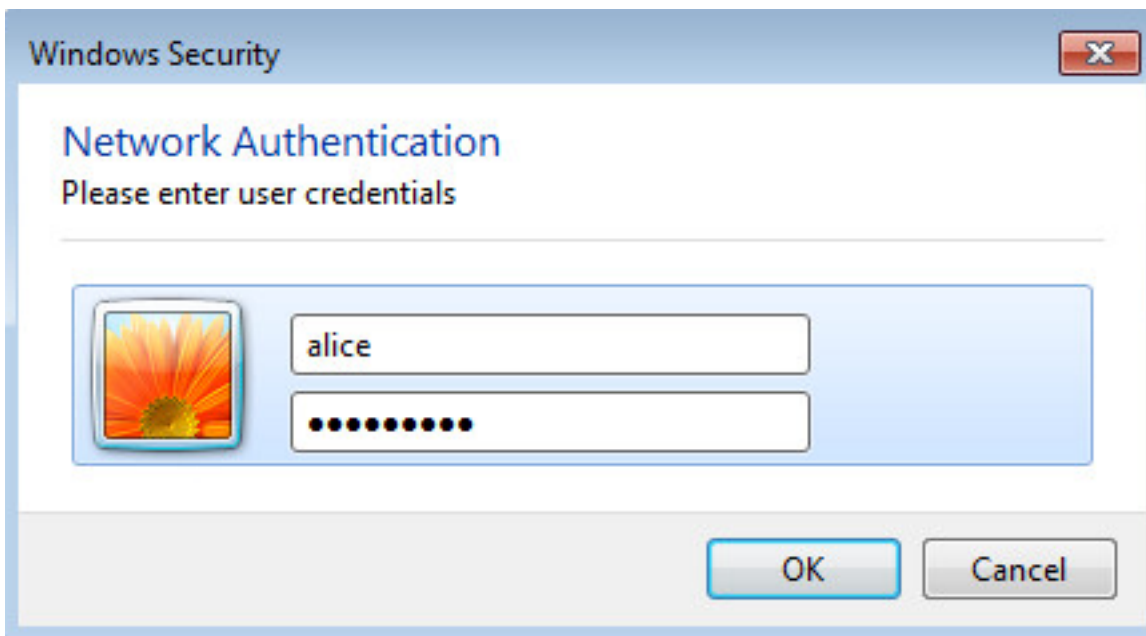
Refresh Add Trash Edit Filter Settings

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

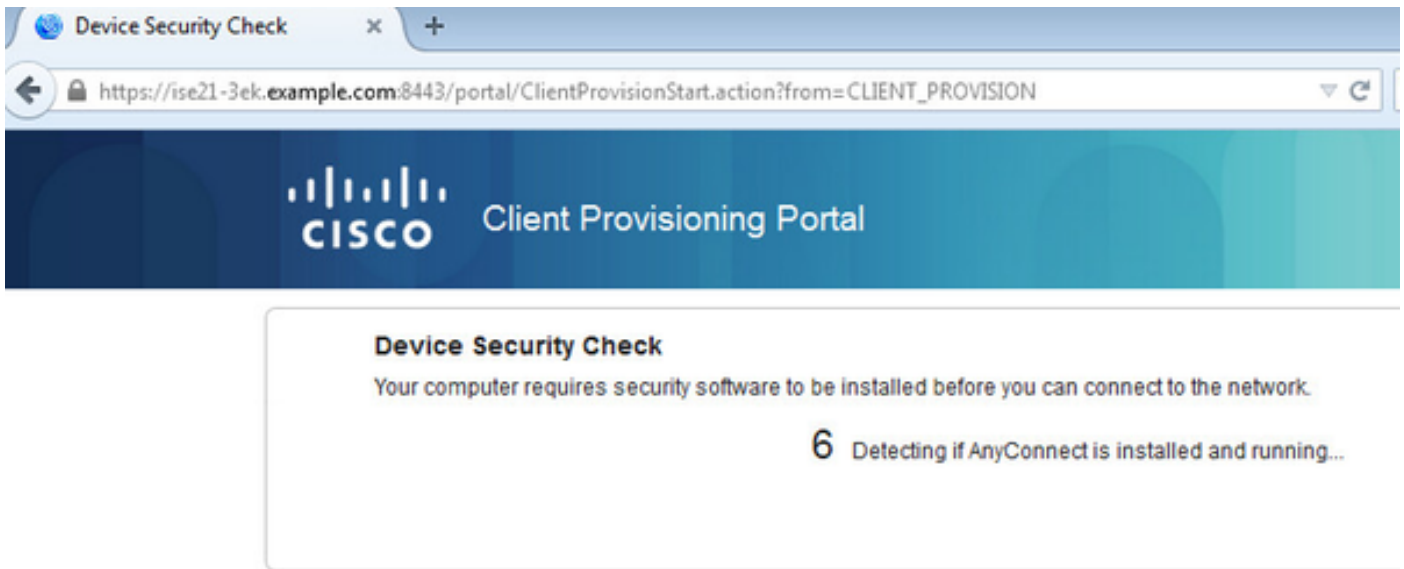
Verificación

Punto final

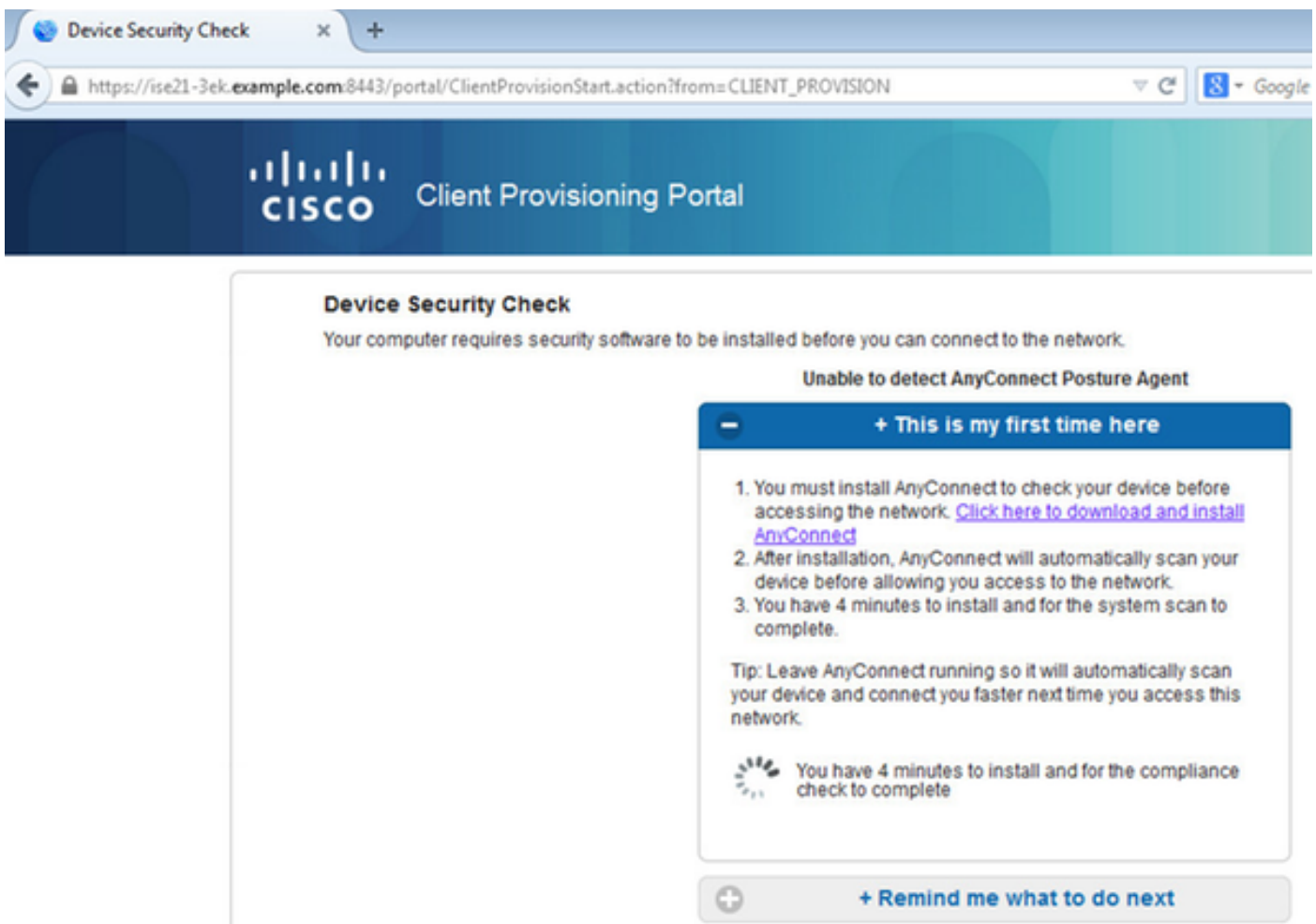
Conecte con la red inalámbrica vía PEAP (MSCHAPv2).



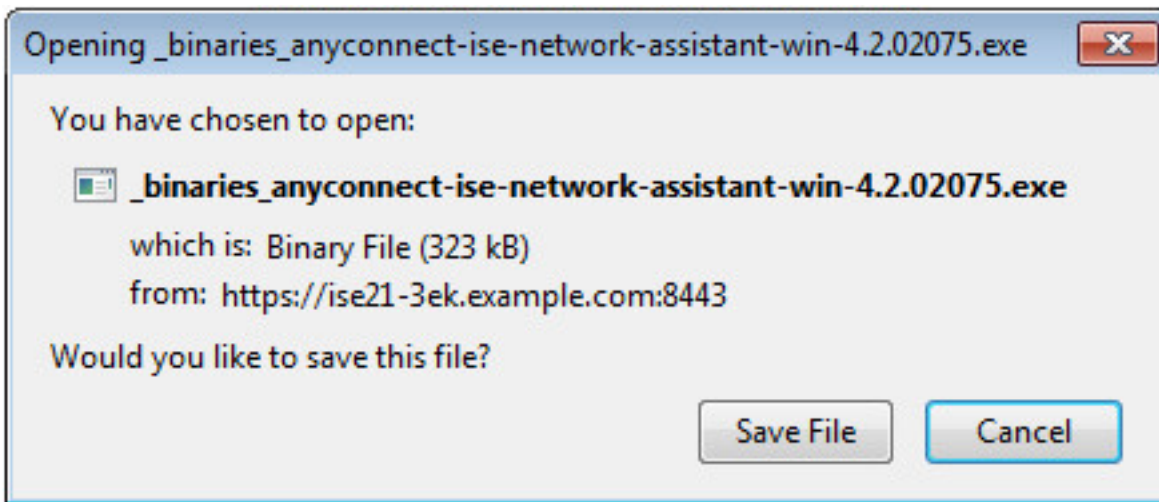
Una vez que está conectado el cambio de dirección con el portal de disposición del cliente ocurre.



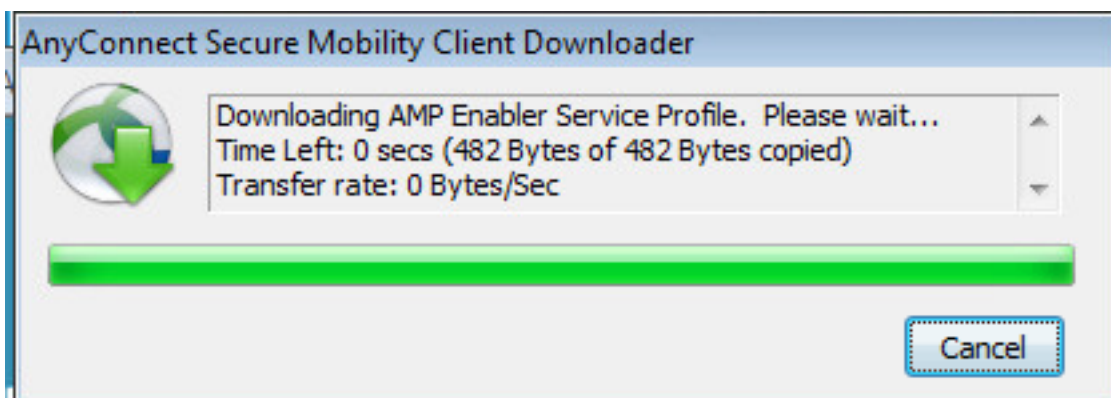
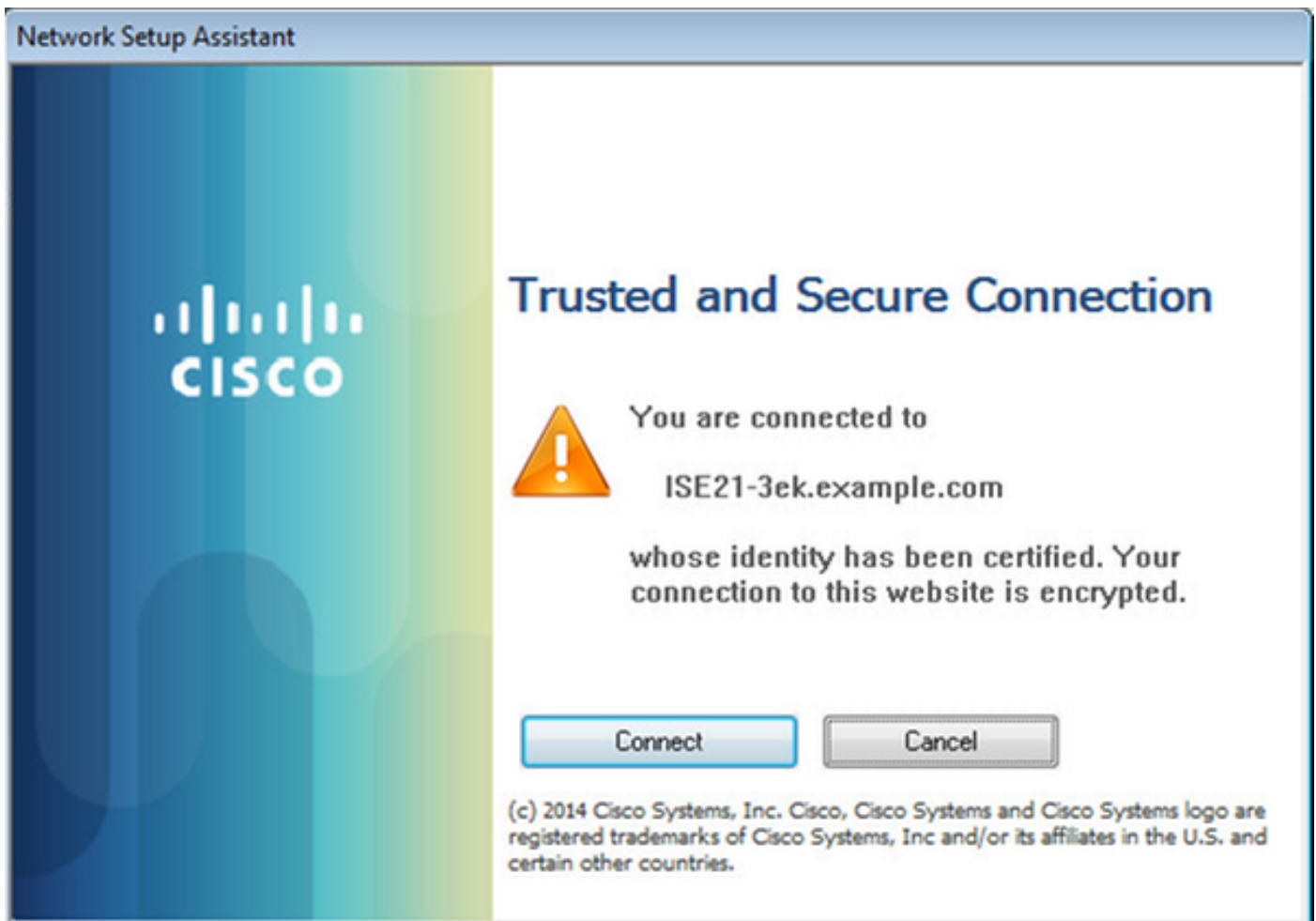
Puesto que no hay nada instalado en la máquina del cliente, el ISE indica para la instalación del cliente de AnyConnect.

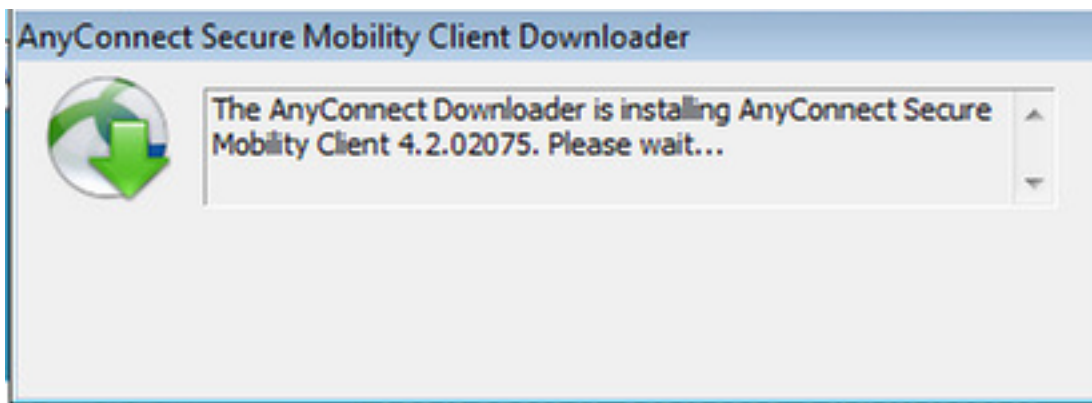


La aplicación auxiliar de la configuración de la red (NSA) se debe descargar y funcionamiento de la máquina del cliente.

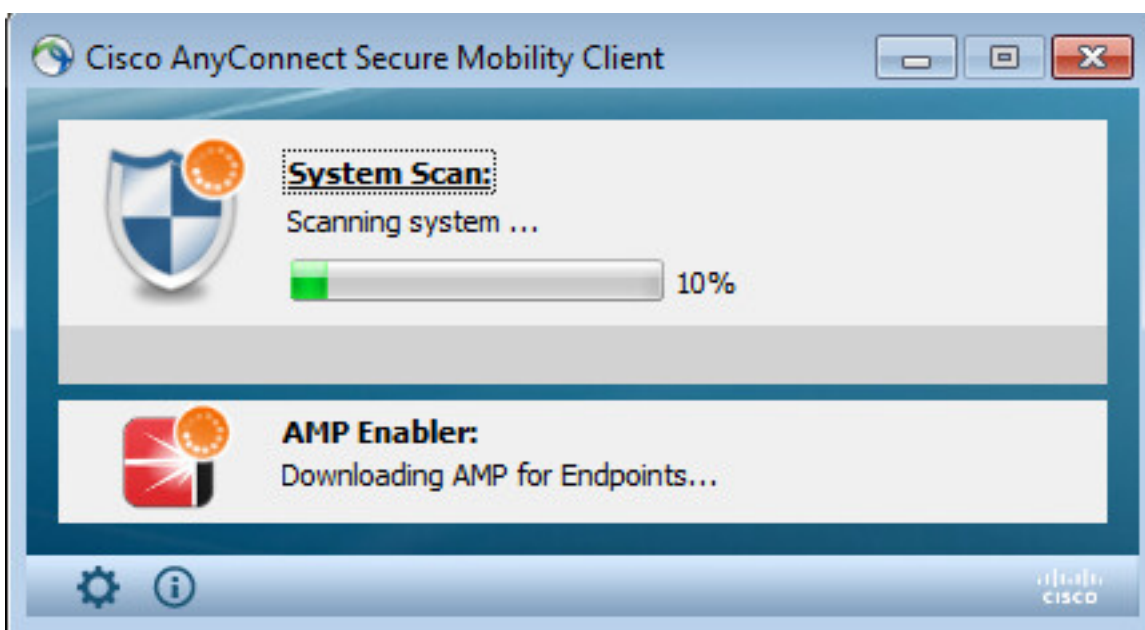
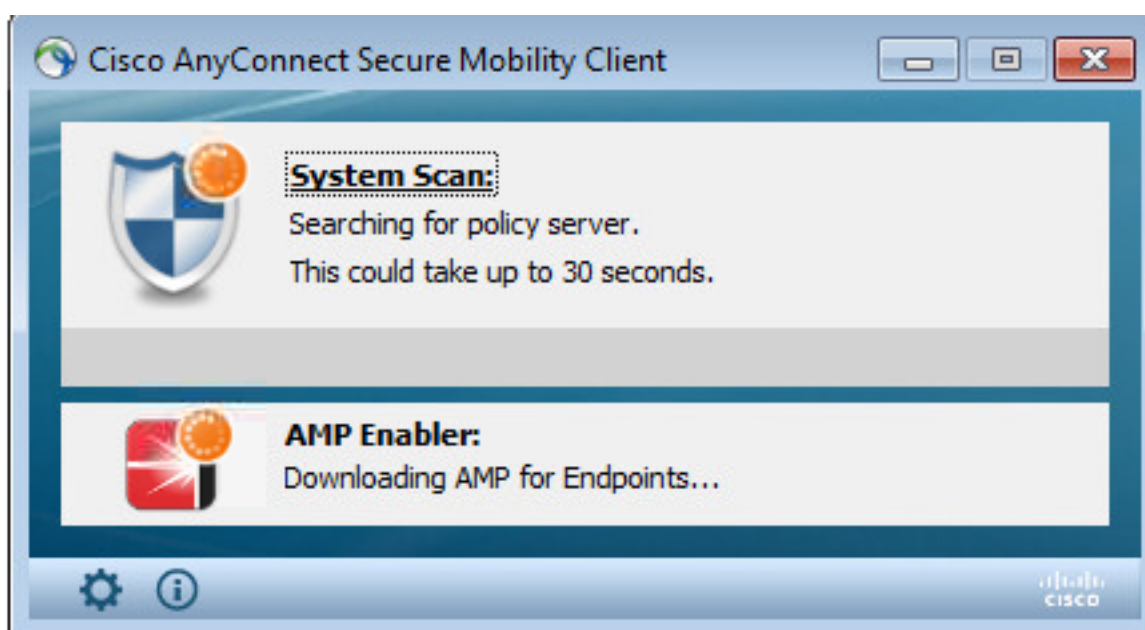


El NSA toma el cuidado de instalar los componentes requeridos y los perfiles.

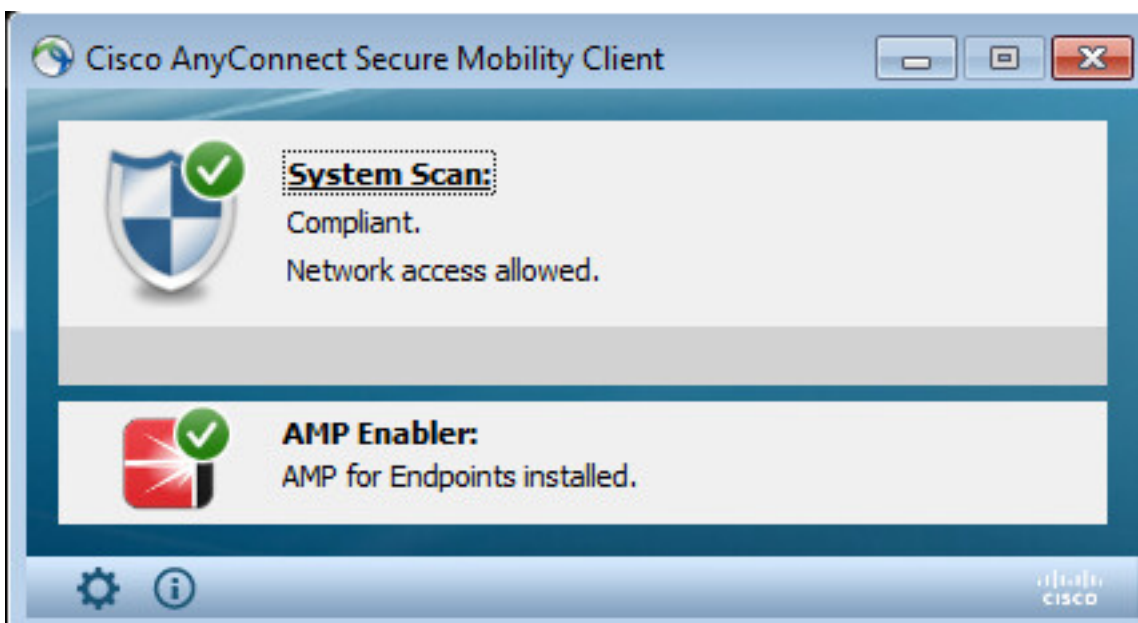
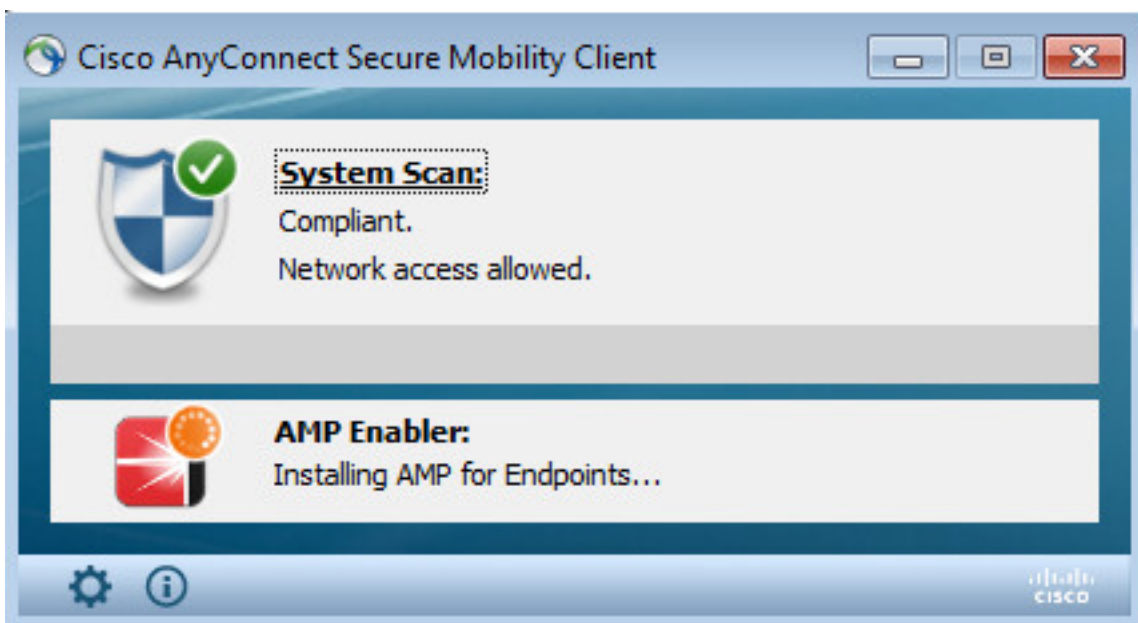
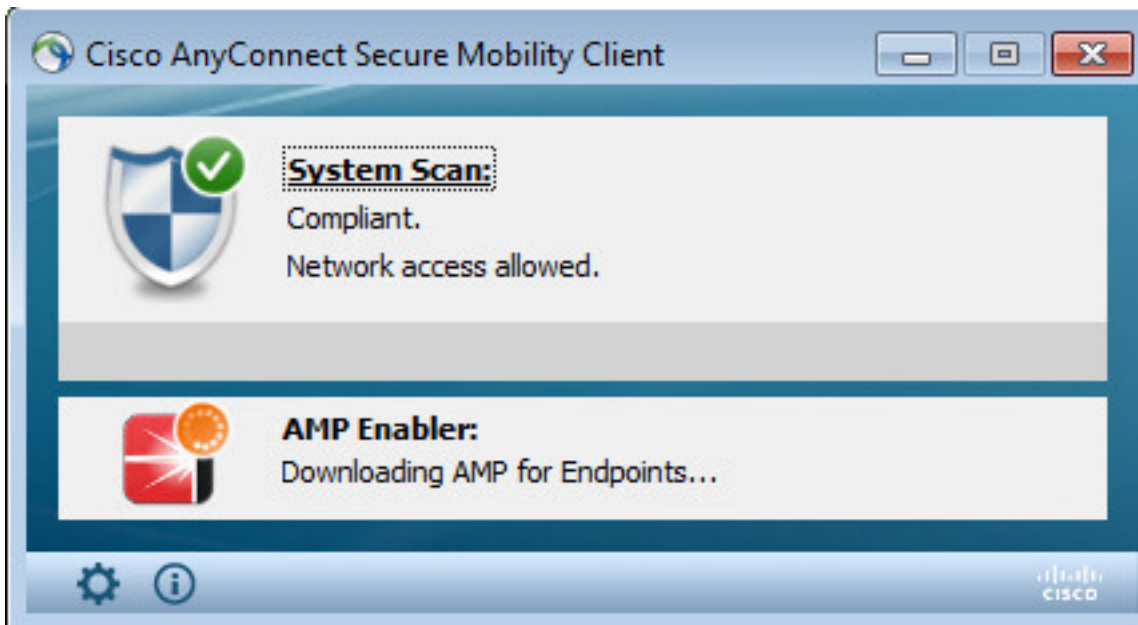




Una vez que se acaba la instalación, el módulo de la postura de AnyConnect realiza el control de la conformidad.



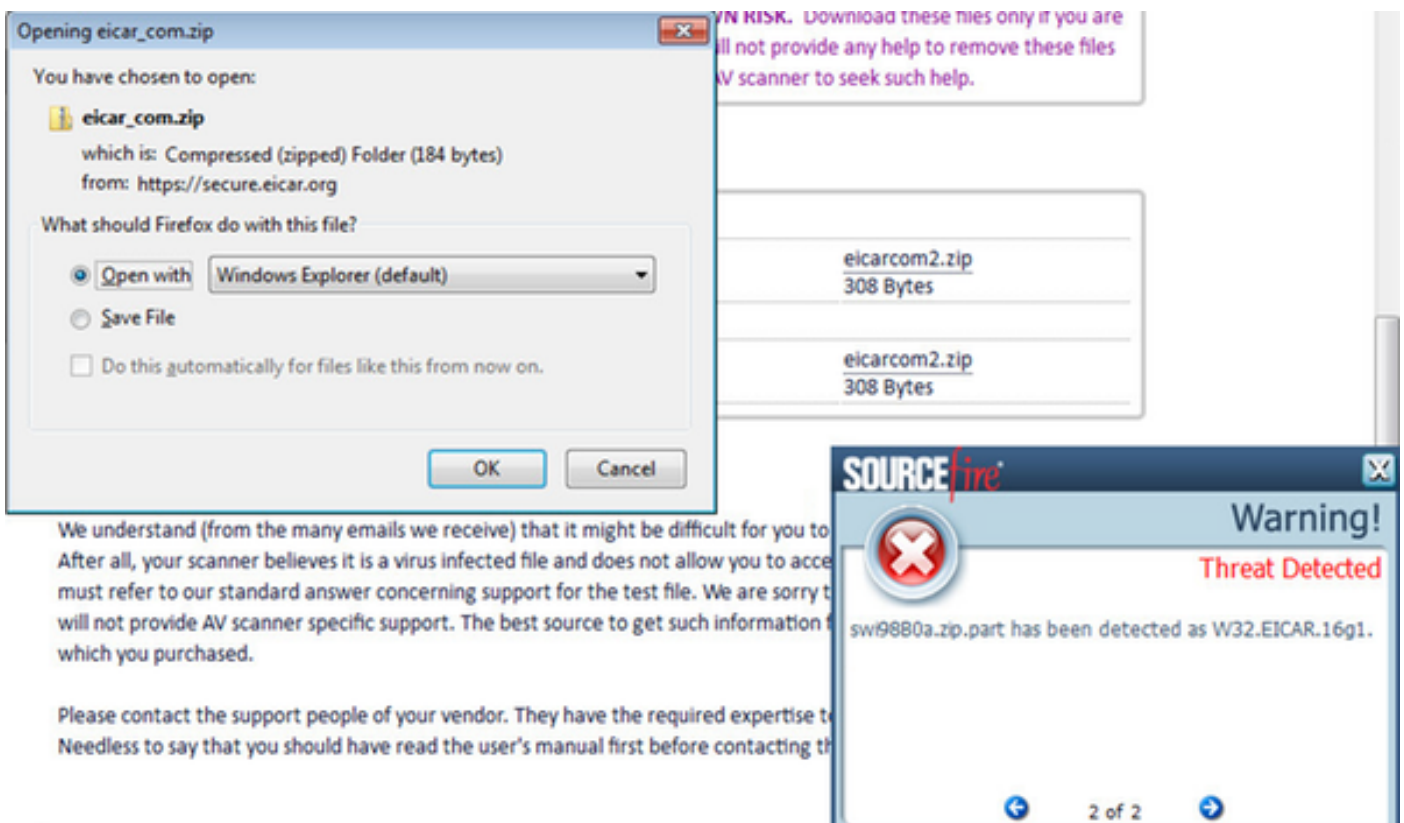
Pues se da el acceso total, si el punto final es obediente, el AMP se descarga y está instalado del web server especificado anterior en el perfil AMP.



El conector AMP aparece.



Para probar el AMP en la acción la cadena de Eicar contenida en a archivo zip se descarga. La amenaza se detecta, y está señalada a la nube AMP.



Nube AMP

Para verificar los detalles del panel de la amenaza de la nube AMP puede ser utilizado.

The dashboard displays the following sections:

- Indications of Compromise:** Shows a threat detected on `ekorneyc-pc.example.com`.
- Hosts Detecting Malware (7 days):**

Computer	Count
ekorneyc-PC.example.com	4
HARISHA-PC.example.com	1
- Malware Threats (7 days):**

Detection Name	Count
W32.EICAR.16g1	5
- Hosts Detecting Network Threats (7 days):** Shows no recent network threat detections.
- Network Threats (7 days):** Shows no recent network threat detections.

Para conseguir más detalles sobre la amenaza, filepath y los fingerprints, usted puede hacer clic en el host, donde el malware fue detectado.

The detailed view shows the following information:

- Event Type:** Threat Detected
- Filters:** Computer: `e8c02e6a-a885-47ba-aeec-2ac03bea4241`
- Sort:** Time
- Event Details:**
 - Host: `ekorneyc-pc.example.com`
 - Detection: `0M90PRxO.zip.part` as `W32.EICAR.16g1`
 - Quarantine: Not Seen
 - Timestamp: 2016-05-30 16:27:30 UTC
- File Detection Details:**

Field	Value
Detection	W32.EICAR.16g1
Fingerprint (SHA-256)	2546d0f...6e9eedad
Filename	0M90PRxO.zip.part
Filepath	C:\Users\admin\AppData\Local\Temp\0M90PRxO.zip.part
File Size (bytes)	184
Parent Fingerprint (SHA-256)	3147bd8...32d689c2
Parent Filename	Firefox.exe

Para ver o desregistrar el caso del ISE que usted puede navegar a las cuentas > a las aplicaciones

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

En ISE que sí mismo el flujo regular de la postura se considera, cambio de dirección ocurre primero para marcar la conformidad de la red. Tan pronto como el punto final sea obediente, se envía el CoA Reauth y el nuevo perfil con PermitAccess se asigna.

Time	Status	Details	Repeat	Identify	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Jun 30, 2016 05:50:18.729 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 >> Non-Compliant_Devis...	AMP_Profile	
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	

Para ver las amenazas detectadas que usted puede navegar a la visibilidad > a los puntos finales del contexto > los puntos finales comprometidos

COMPROMISED ENDPOINTS BY INCIDENTS

All endpoints | Connected | Disconnected

Incident Level	Count
Unknown	0
Insignificant	0
Distracting	0
Painful	1
Damaging	0
Catastrophic	0

IMPACT LEVEL

COMPROMISED ENDPOINTS BY INDICATORS

All endpoints | Connected | Disconnected

Indicator Level	Count
Unknown	0
None	0
Low	0
Medium	0
High	0

LIKELY IMPACT LEVEL

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

Si usted selecciona el punto final y navega a la lengüeta de la amenaza, se visualizan más detalles.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main menu has 'Endpoints' and 'Network Devices'. The breadcrumb trail is 'Endpoints > C0:4A:00:14:8D:4B'. The endpoint details are: MAC Address: C0:4A:00:14:8D:4B, Username: alice, Endpoint Profile: Windows7-Workstation, Current IP Address: 10.62.148.26, Location: . The 'Threats' tab is selected, showing a 'Threat Detected' section with the following details: Type: INCIDENT, Severity: Painful, Reported by: AMP, Reported at: 2016-06-30 11:27:48.

Cuando un evento de la amenaza se detecta para un punto final, usted puede seleccionar la dirección MAC del punto final en la página comprometida de los puntos finales y aplicar una directiva ANC (si está configurado, por ejemplo cuarentena). Alternativamente usted puede publicar el cambio de la autorización de terminar la sesión.

The screenshot shows the 'Compromised Endpoints' page in the Cisco ISE interface. The page has two charts: 'COMPROMISED ENDPOINTS BY INCIDENTS' and 'COMPROMISED ENDPOINTS BY INDICATORS'. Below the charts is a table of endpoints. The 'Change Authorization' dropdown menu is open, showing options: CoA Session Result, CoA Session Terminate, CoA Port Bounce, CoA SNAet Session Query, CoA Session termination with port bounce, and CoA Session termination with port shutdown. The table below shows the following data:

Source	Threat Severity	Logical NAD Location	Connectivity	Hostname	Identity Group	Endpoint OS
AMP	Painful	Location#A1 Locations	Disconnected		Workstation	
AMP	Painful	Location#A1 Locations	Connected		Workstation	

Si se selecciona la sesión Terminate CoA, el ISE envía la desconexión CoA y el cliente pierde el acceso a la red.

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

Troubleshooting

Para habilitar los debugs en el ISE navegue a la administración > al sistema > a la configuración del registro del registro > del debug, nodo selecto TC-NAC y cambie el **registro llano del componente TC-NAC PARA HACER EL DEBUG DE**

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > PassiveID > Threat Centric NAC > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings. The left sidebar contains: Local Log Settings, Remote Logging Targets, Logging Categories, Message Catalog, Debug Log Configuration, and Collection Filters. The main content area is titled "Node List > ISE21-3ek.example.com" and "Debug Level Configuration". It has "Edit" and "Reset to Default" buttons. Below is a table with columns "Component Name", "Log Level", and "Description". The table contains one entry: TC-NAC with Log Level set to DEBUG and Description "TC-NAC log messages".

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

Registros que se marcarán - irf.log. Usted puede atarlo directamente de ISE CLI:

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

La amenaza incluso se recibe de la nube AMP

```
2016-06-30 DEBUG [IRF-AMQP-Dispatcher-Notification-0][  
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:53 de 18:27:48,617 -::: :- llamando  
el mensaje del programa piloto  
com.cisco.cpm.irf.service.IrfNotificationHandler$MyNotificationHandler@3fac8043 de la  
notificación {messageType=NOTIFICATION, messageId=THREAT_EVENT, content= {el  
"c0:4a:00:14:8d:4b": [{"incidente": {"Impact_Qualification": "Doloroso"}, "grupo fecha/hora":  
1467304068599, "vendedor": "AMP", "título": "Amenaza detectada"}]} ', priority=0, timestamp=Thu  
30 de junio 18:27:48 CEST 2016, amqpEnvelope=Envelope(deliveryTag=79, redeliver=false,  
exchange=irf.topic.events, routingKey=irf.events.threat), amqpProperties=#contentHeader<basic>  
(content-type=application/json, content-encoding=null, headers=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-a836-545416ae56f4,  
cluster-id=null)}  
2016-06-30 DEBUG [IRF-AMQP-Dispatcher-Notification-0][  
cisco.cpm.irf.service.IrfNotificationHandler:handle:140 de 18:27:48,617 -::: :- agregado a la  
cola pendiente: Mensaje {messageType=NOTIFICATION, messageId=THREAT_EVENT, content= {el  
"c0:4a:00:14:8d:4b": [{"incidente": {"Impact_Qualification": "Doloroso"}, "grupo fecha/hora":  
1467304068599, "vendedor": "AMP", "título": "Amenaza detectada"}]} ', priority=0, timestamp=Thu  
30 de junio 18:27:48 CEST 2016, amqpEnvelope=Envelope(deliveryTag=79, redeliver=false,  
exchange=irf.topic.events, routingKey=irf.events.threat), amqpProperties=#contentHeader<basic>  
(content-type=application/json, content-encoding=null, headers=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-a836-545416ae56f4,  
cluster-id=null)}  
2016-06-30 DEBUG [IRF-AMQP-Dispatcher-Notification-0][  
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:59 de 18:27:48,617 -::: :- HECHO  
procesando la notificación: #contentHeader<basic> Envelope(deliveryTag=79, del redeliver=false,  
exchange=irf.topic.events, routingKey=irf.events.threat) (content-type=application/json,  
content-encoding=null, headers=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-a836-545416ae56f4, cluster-id=null)  
2016-06-30 DEBUG [IRF-EventProcessor-0][  
cisco.cpm.irf.service.IrfEventProcessor:parseNotification:221 de 18:27:48,706 -::: :-  
notificación del análisis: Mensaje {messageType=NOTIFICATION, messageId=THREAT_EVENT, el  
content='{"c0:4a:00:14:8d:4b": [{"incidente": {"Impact_Qualification": "Doloroso"}, "grupo  
fecha/hora": 1467304068599, "vendedor": "AMP", "título": "Amenaza detectada"}]} ', priority=0,  
timestamp=Thu 30 de junio 18:27:48 CEST 2016, amqpEnvelope=Envelope(deliveryTag=79,  
redeliver=false, exchange=irf.topic.events, routingKey=irf.events.threat),  
amqpProperties=#contentHeader<basic> (content-type=application/json, content-encoding=null,  
headers=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-a836-545416ae56f4, cluster-id=null)}
```

La información sobre la amenaza se envía PARA CRITICAR

```
2016-06-30 DEBUG [IRF-EventProcessor-0][  
cisco.cpm.irf.service.IrfEventProcessor:storeEventsInES:366 de 18:27:48,724 -::: :- agregando  
la Información del evento de la amenaza para enviar PARA CRITICAR - c0:4a:00:14:8d:4b {incident=  
{Impact_Qualification=Painful}, time-stamp=1467304068599, vendor=AMP, title=Threat detectados}
```