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

Contenido

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

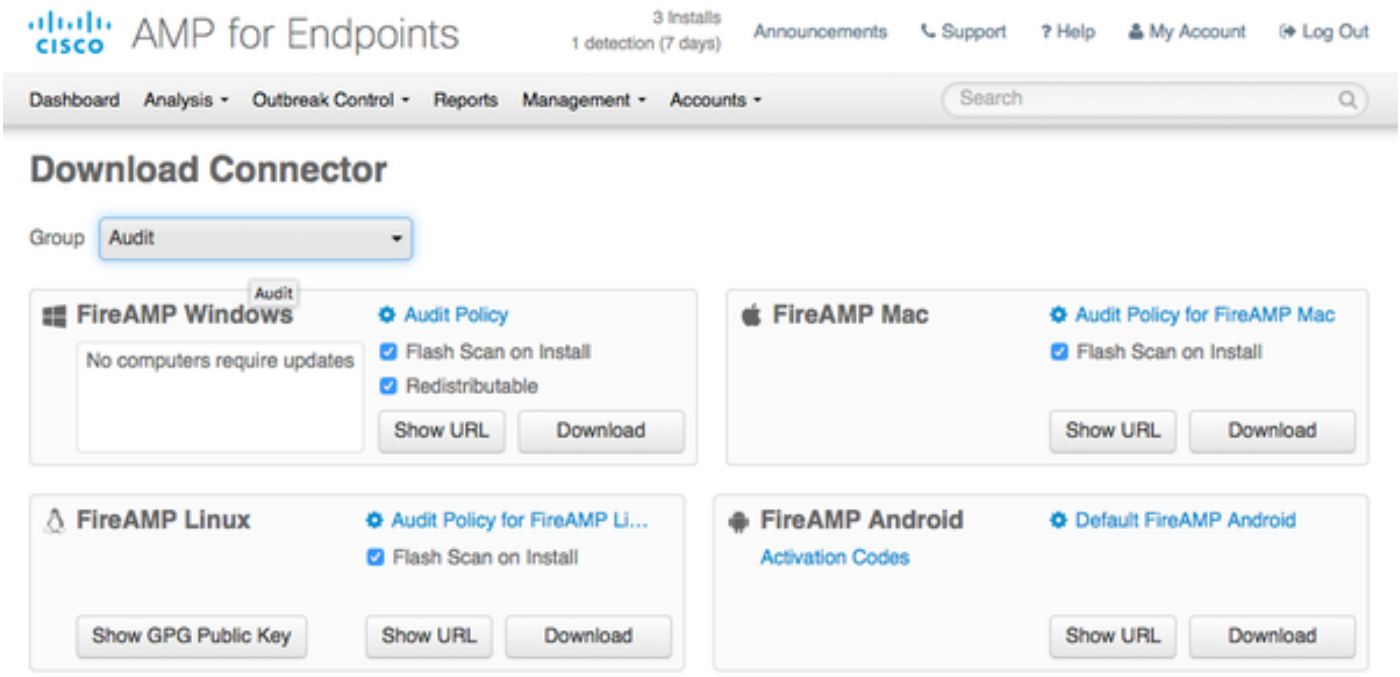
4. Cuando el cliente intenta descargar el software malévolo, el conector AMP lanza un mensaje de advertencia y lo señala a la nube AMP

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.

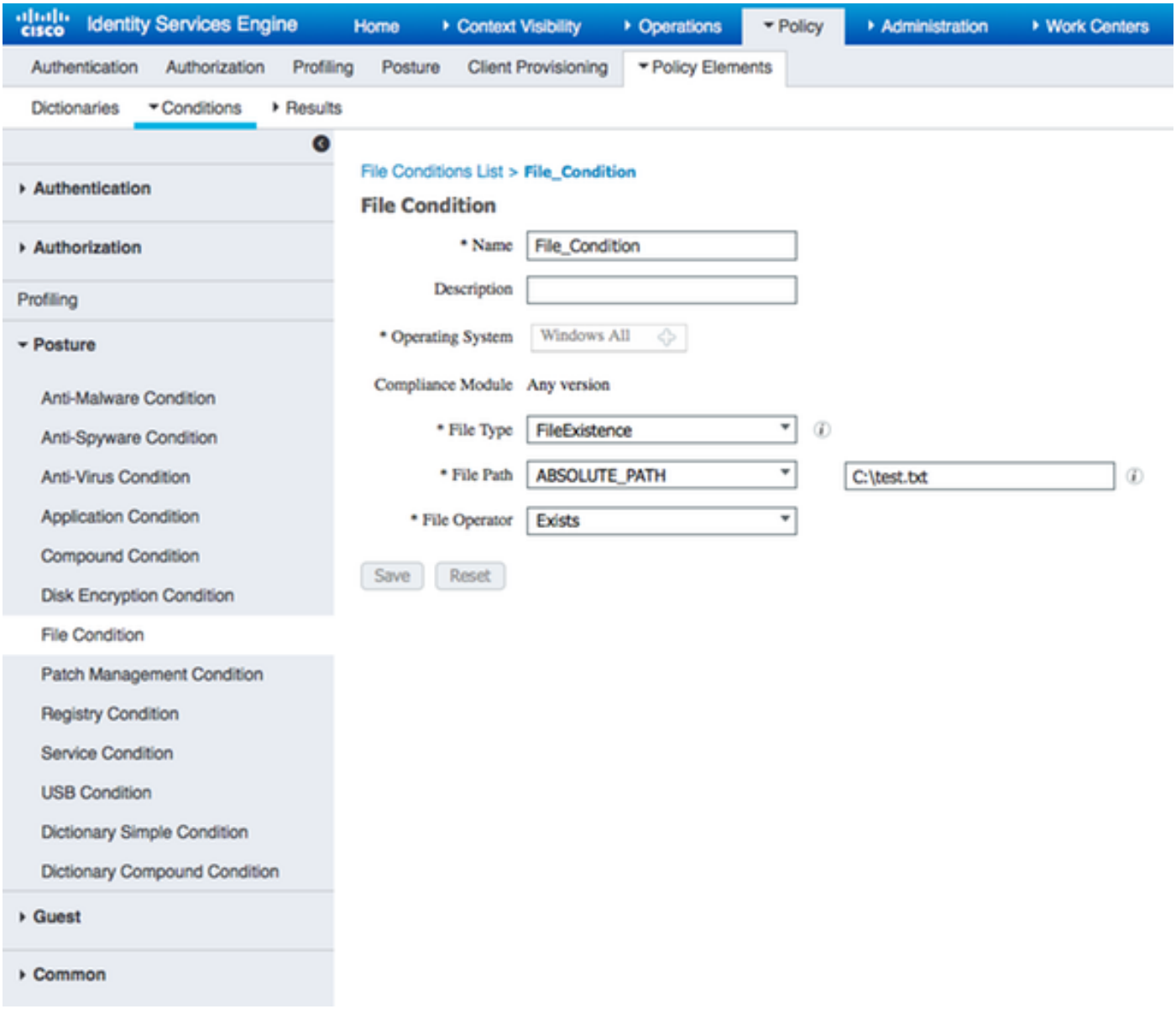


> **Note**: Descargar este archivo genera un archivo del .exe llamado **Audit_FireAMPSetup.exe en el** ejemplo. Este archivo fue enviado al servidor Web para estar disponible una vez que el usuario pide la configuración del AMP.

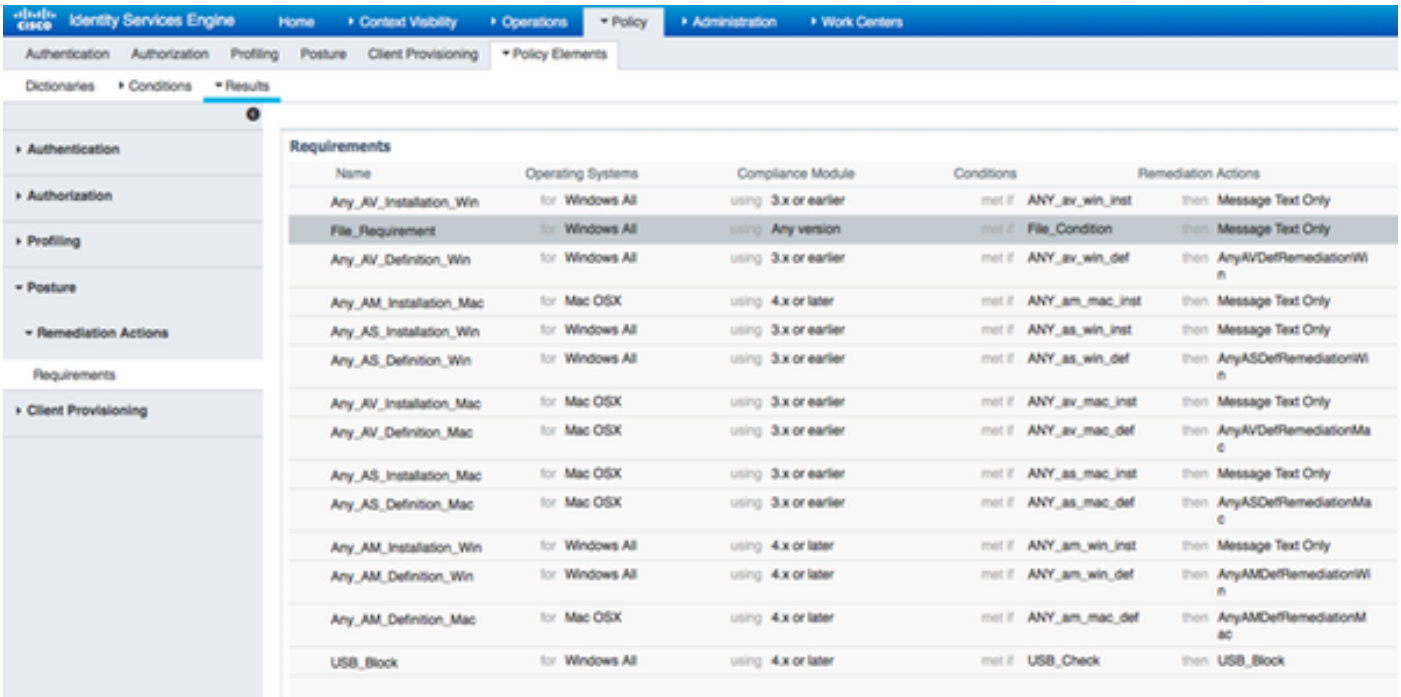
Configuración ISE

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

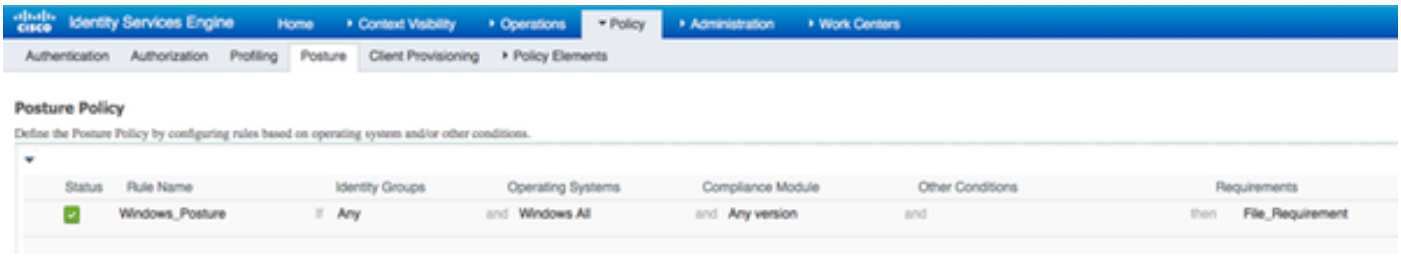
Navegue a la directiva > a los elementos > a las condiciones > a la postura > al archivo Condition.You de la directiva puede ver que una condición simple para la existencia del archivo se ha creado. El archivo tiene que existir si el punto final es ser obediente con la directiva verificada por el módulo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



Esta condición se utiliza para un requisito:

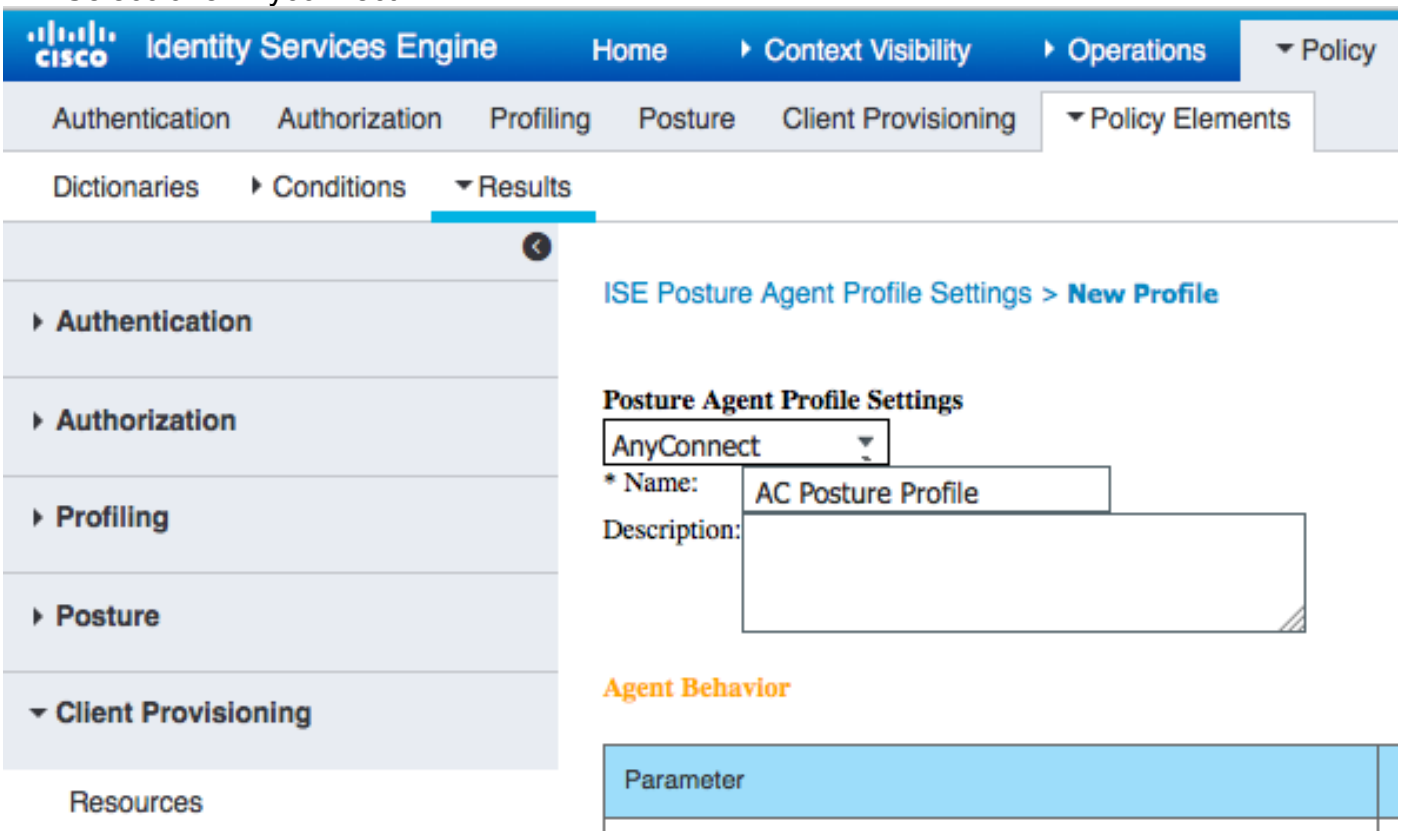


El requisito se utiliza en la directiva de la postura para los sistemas de Microsoft Windows:

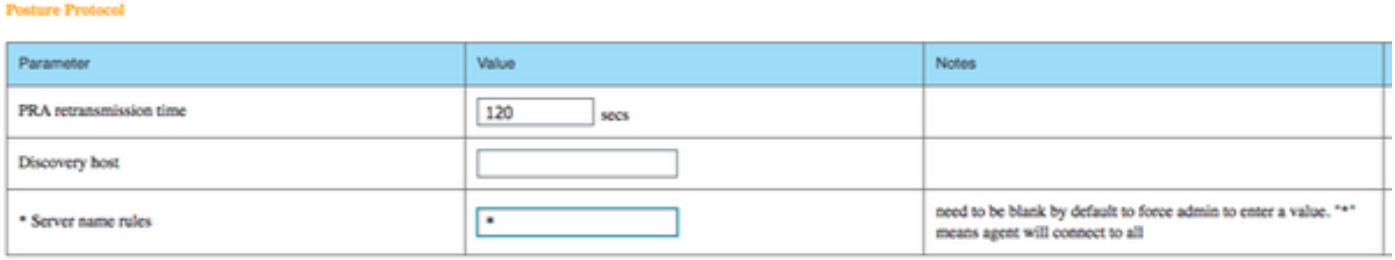


Paso 2. Perfil de la postura de la configuración

- 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



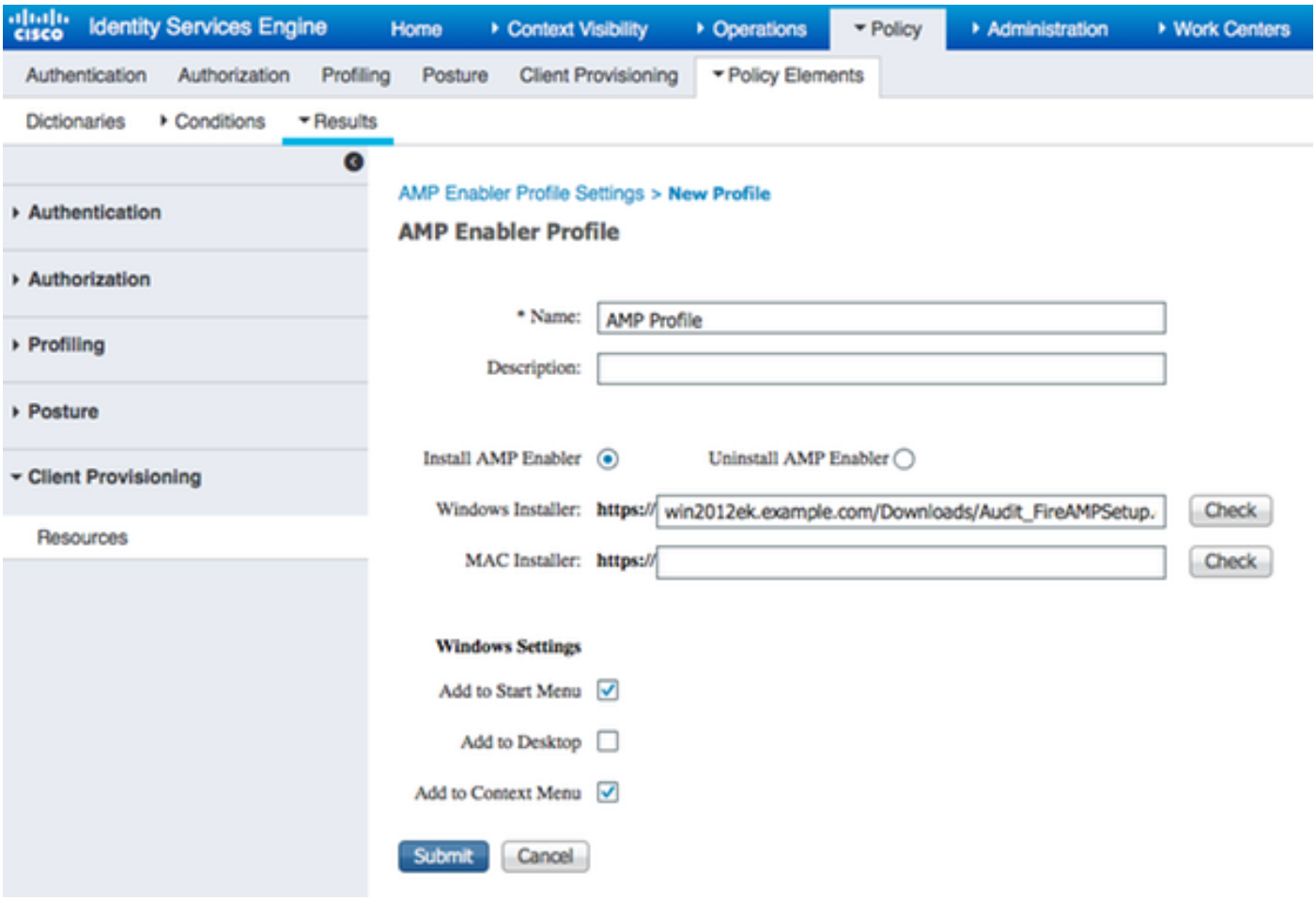
- De la sección de protocolo de la postura agregue * para permitir que el agente conecte con todos los servidores



Paso 3. Perfil de la configuración AMP

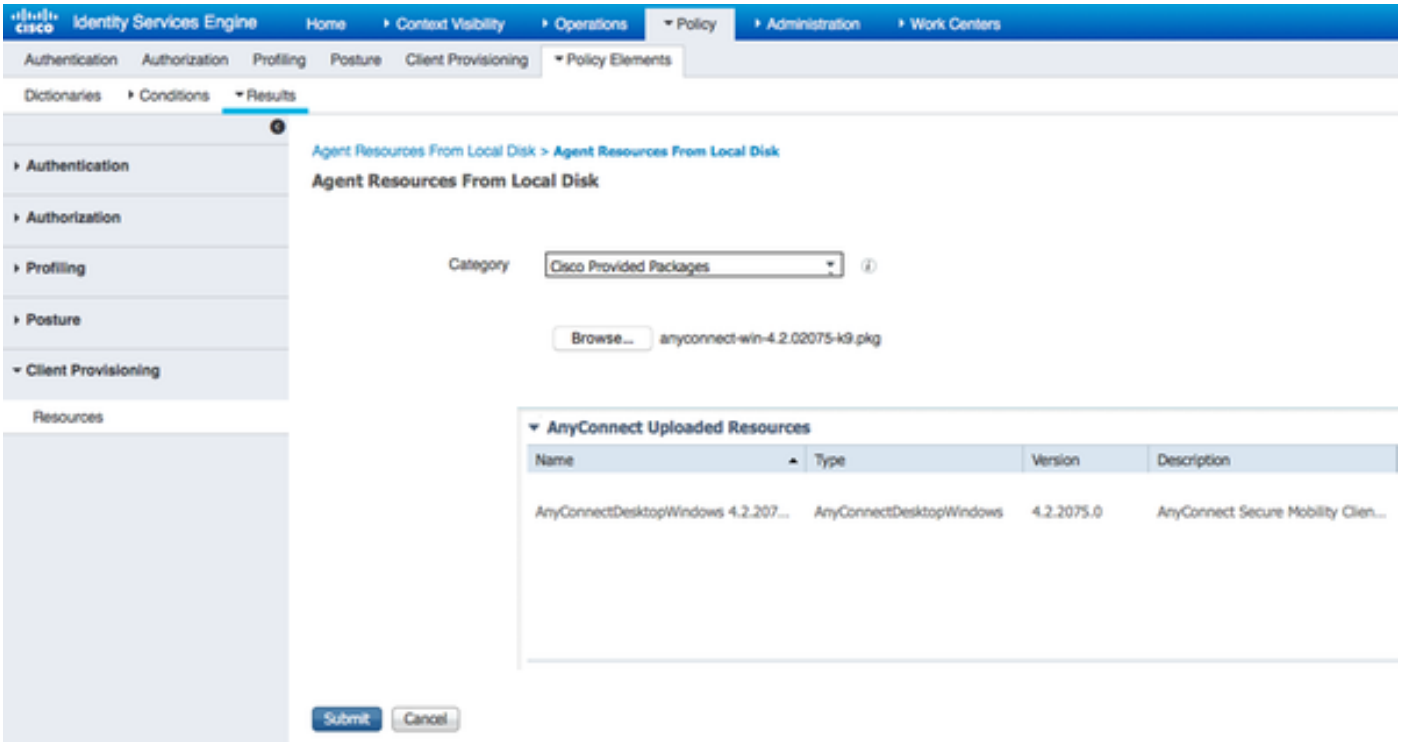
El perfil AMP contiene la información donde se localiza el instalador de Windows. El instalador de

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.

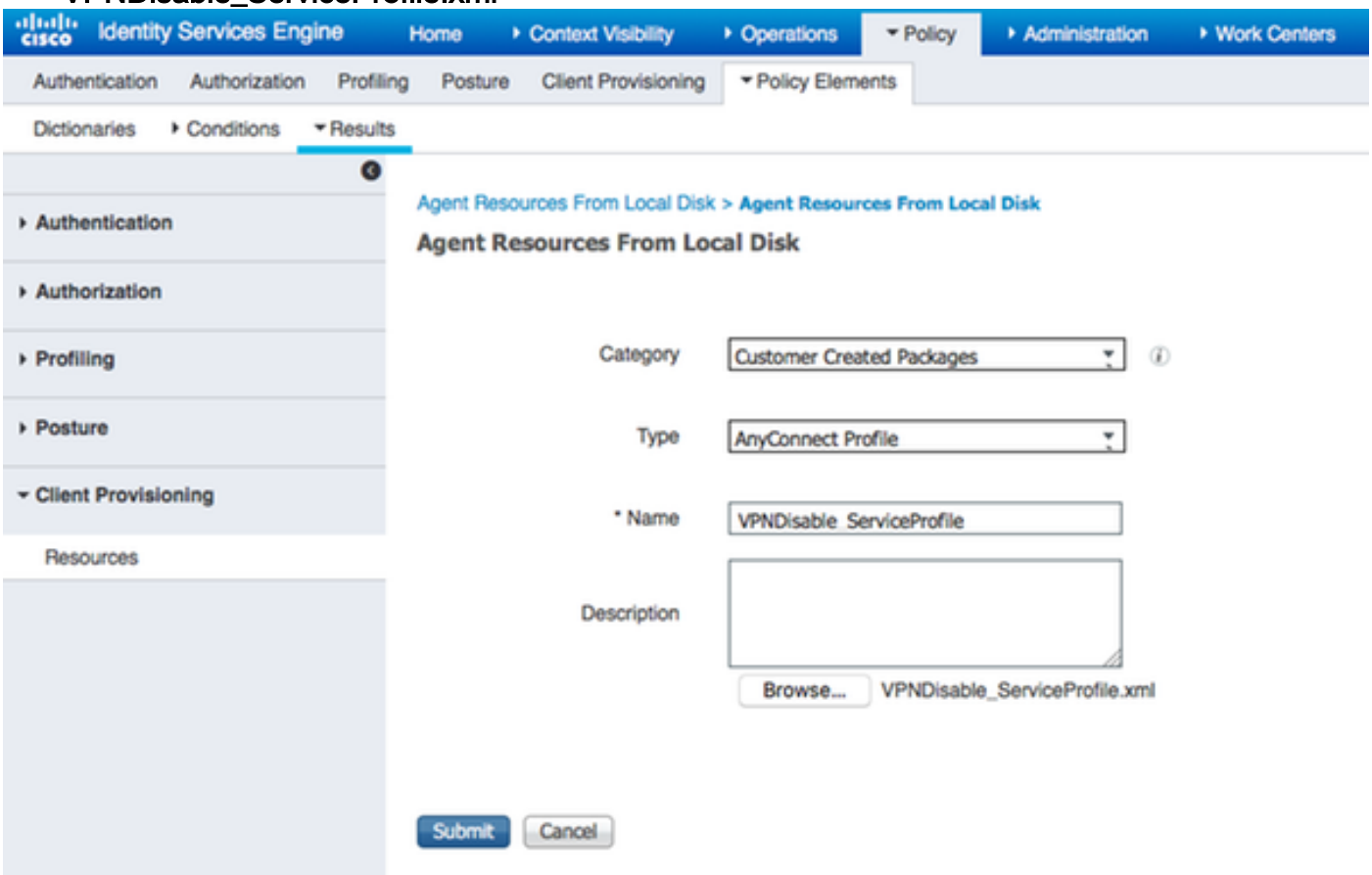


Paso 2. Aplicaciones de la carga y perfil XML al ISE

- 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 creados cliente de AnyConnect del** tipo. Seleccione **VPNDisable_ServiceProfile.xml**

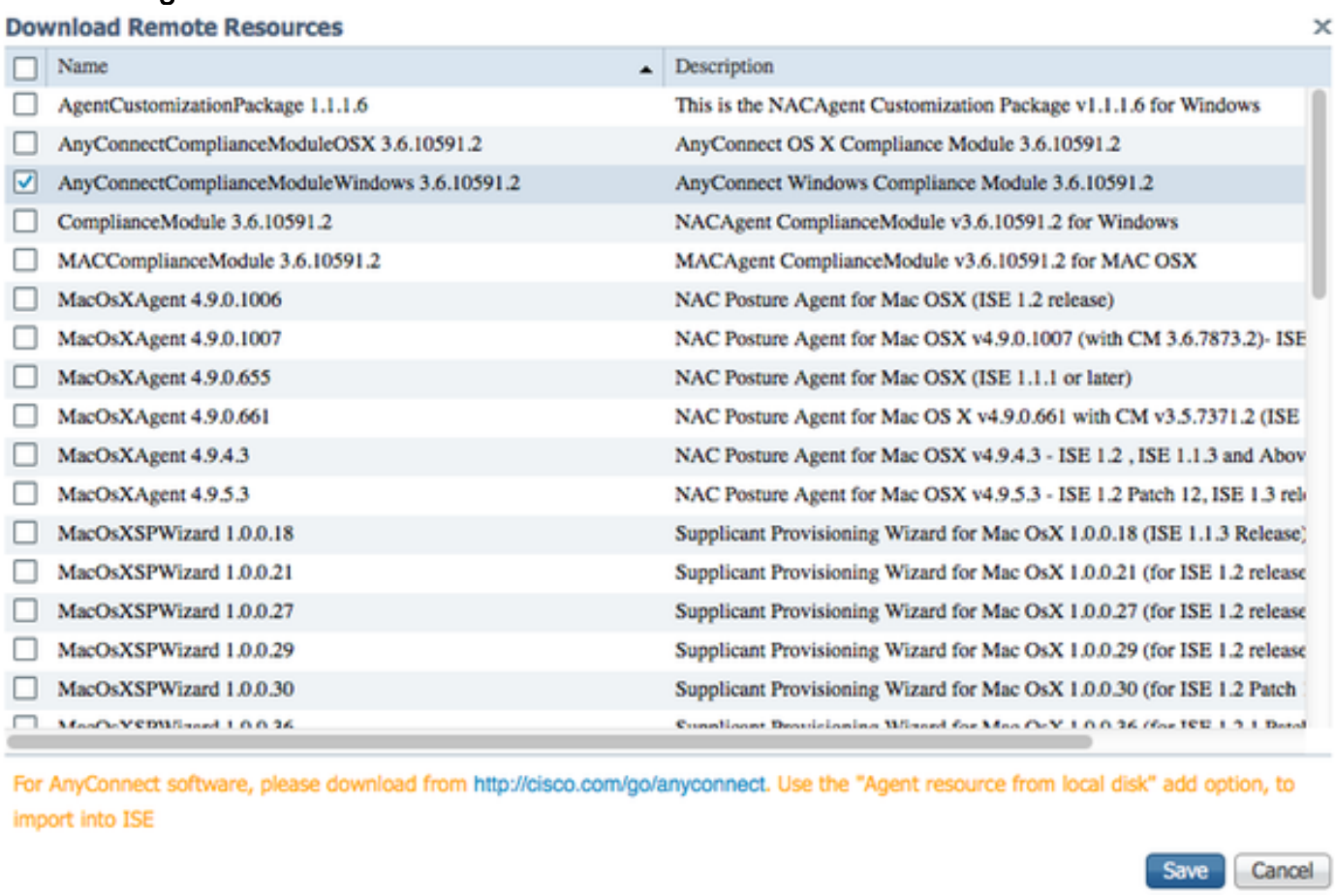


Note: **VPNDisable_ServiceProfile.xml** se utiliza para ocultar el título VPN, puesto que este ejemplo no utiliza el módulo VPN. Éste es el contenido de VPNDisable_ServiceProfile.xml**:**

```
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>
```

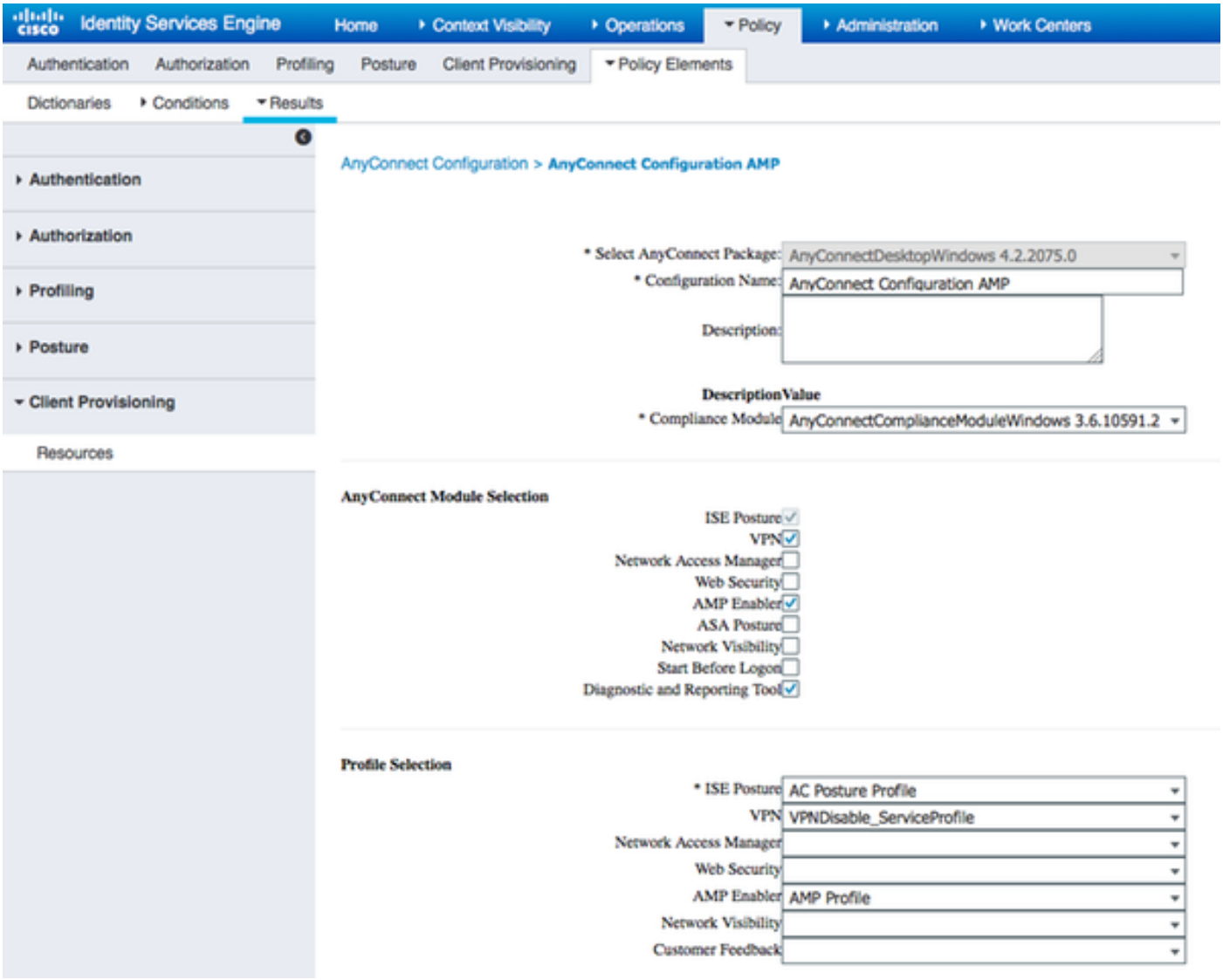
Paso 3. Módulo de la conformidad de AnyConnect de la descarga

- 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**



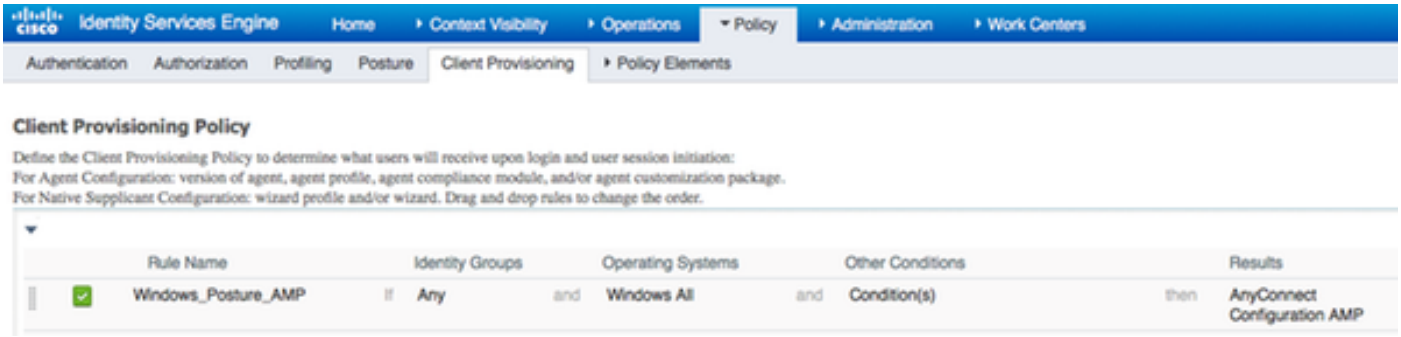
Paso 4. Agregue la configuración de AnyConnect

- 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



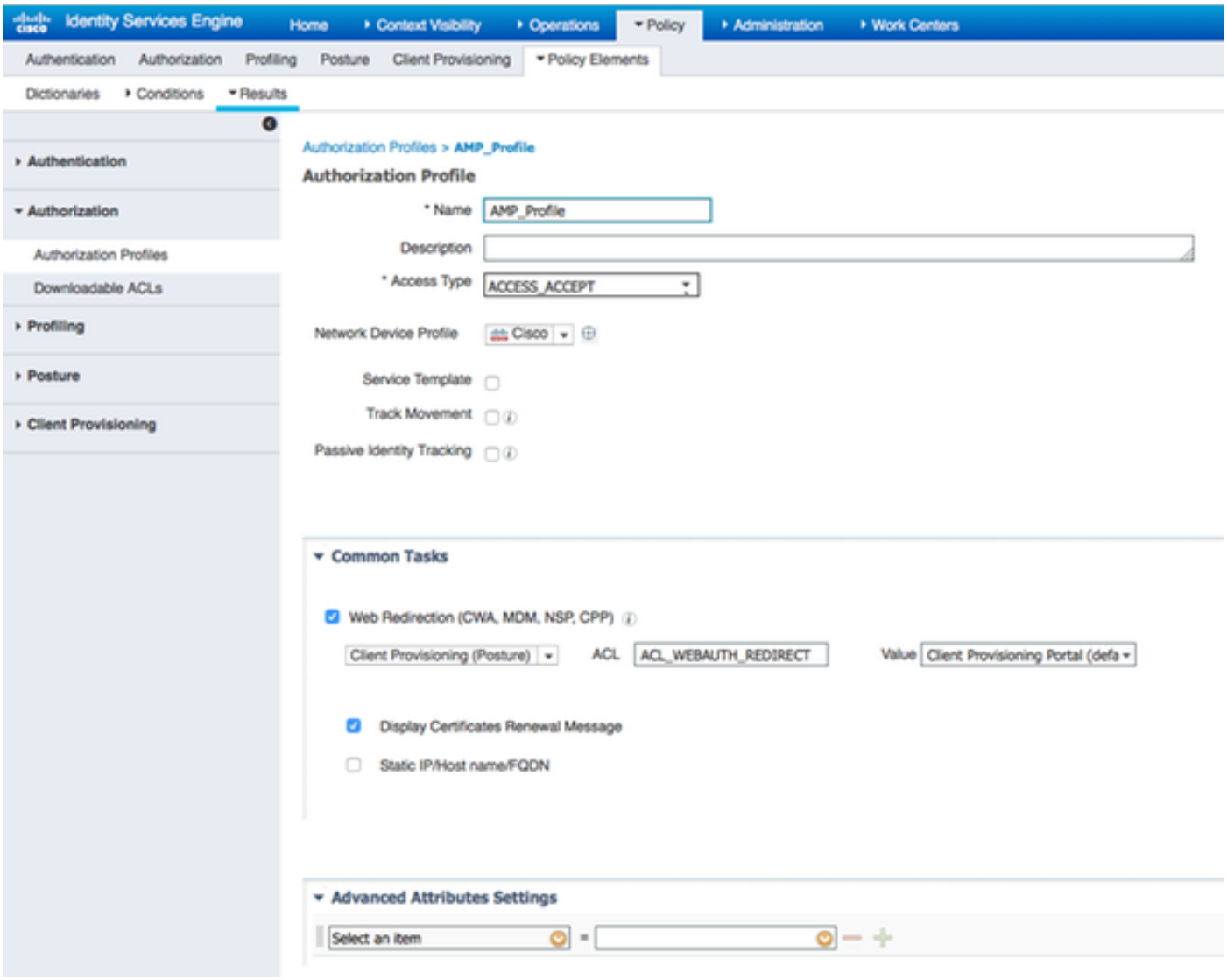
Paso 5. Reglas del aprovisionamiento del cliente de la configuración

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

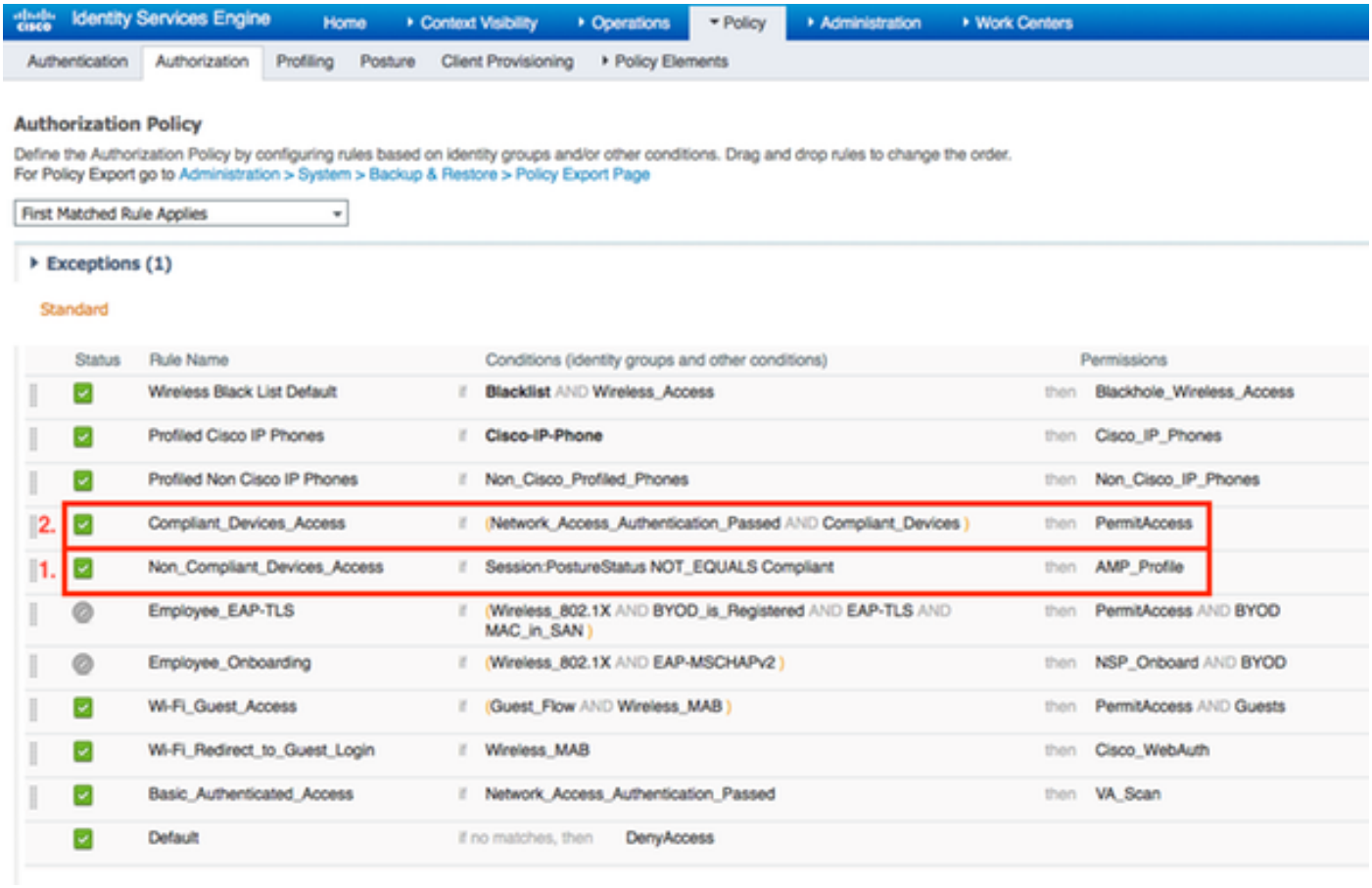


Paso 6. Directivas de la autorización de la configuración

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

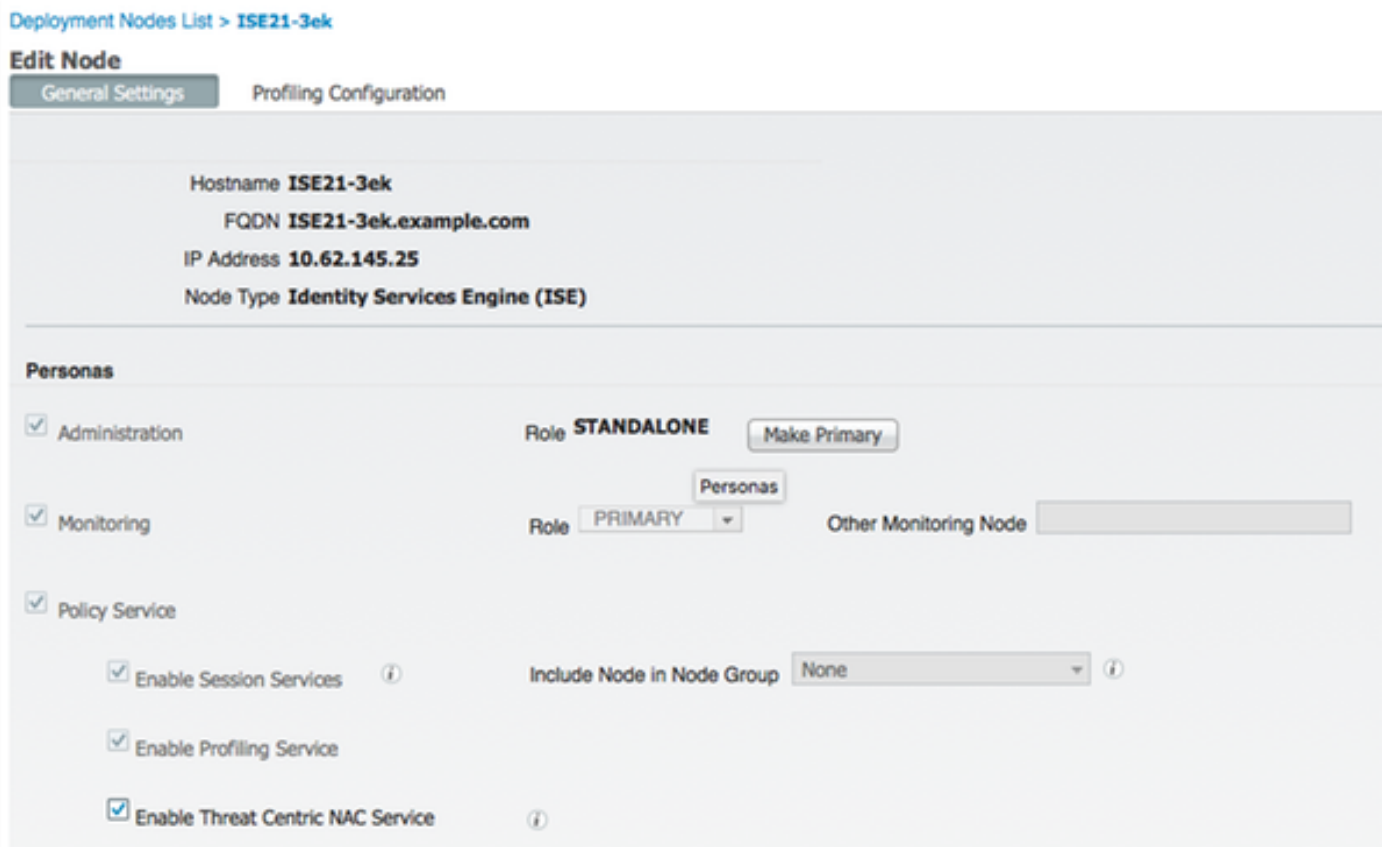


Luego, una vez que es obediente, se asigna el acceso total



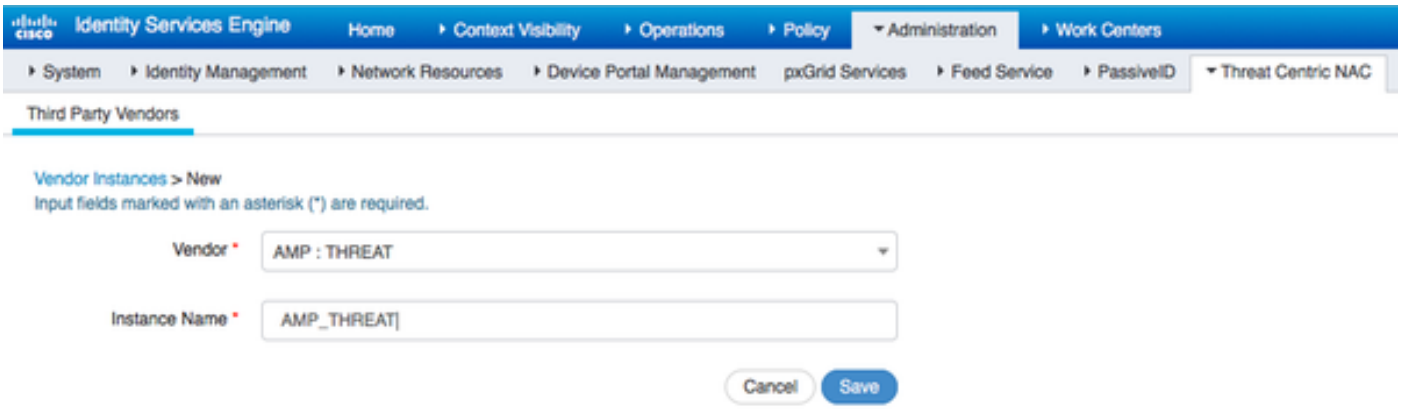
Paso 7. Servicios del permiso TC-NAC

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.

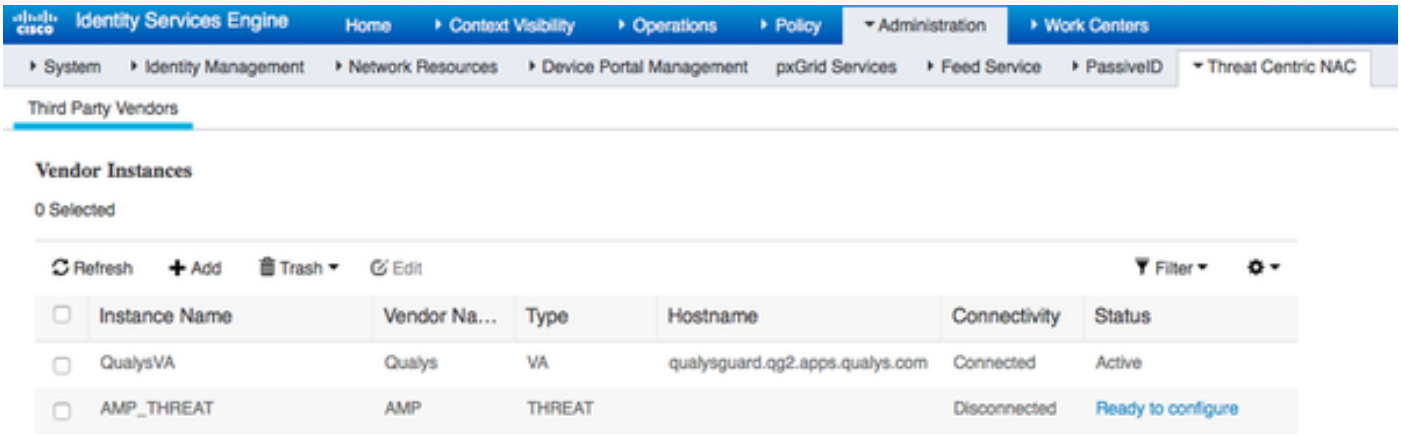


Paso 8. Adaptador de la configuración AMP

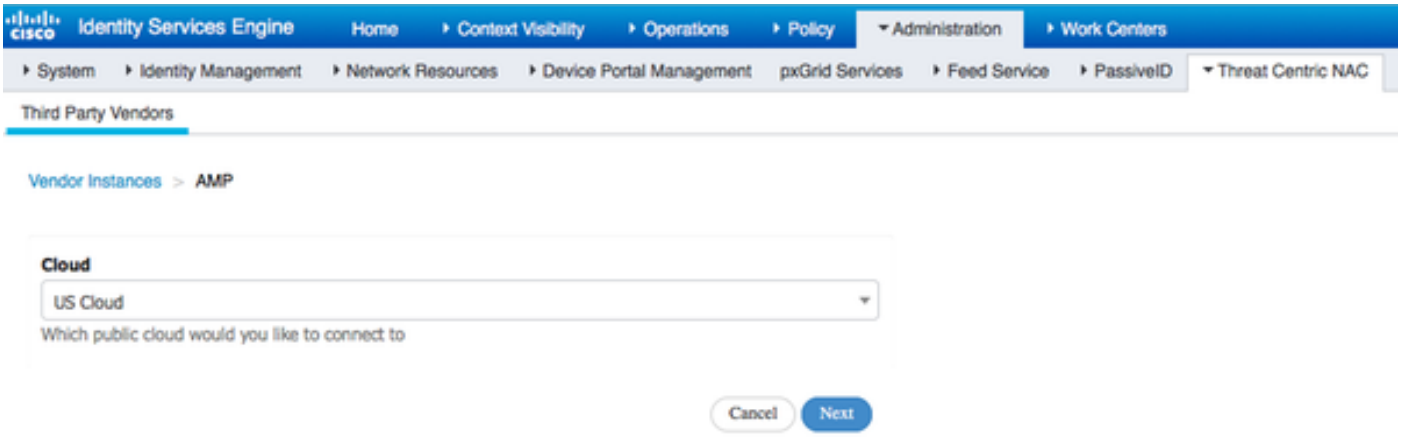
Navegue a la administración > al NAC > a los terceros proveedores céntricos de la amenaza > Add. Haga clic en la **salvaguardia**



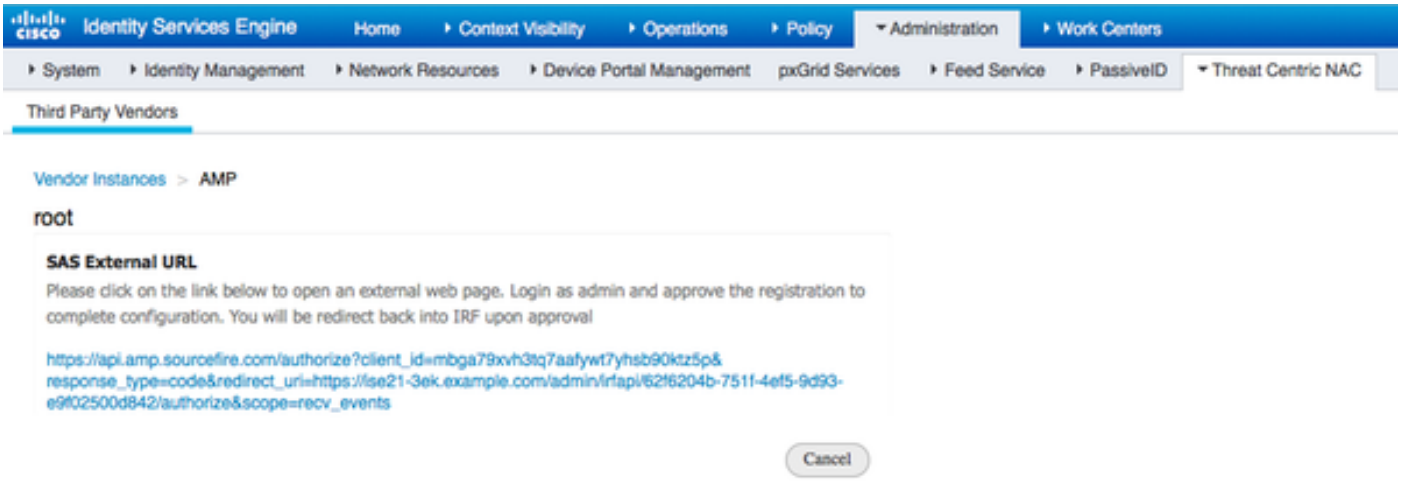
Debe transición **alistar para configurar el** estado. Haga clic en **listo para configurar**



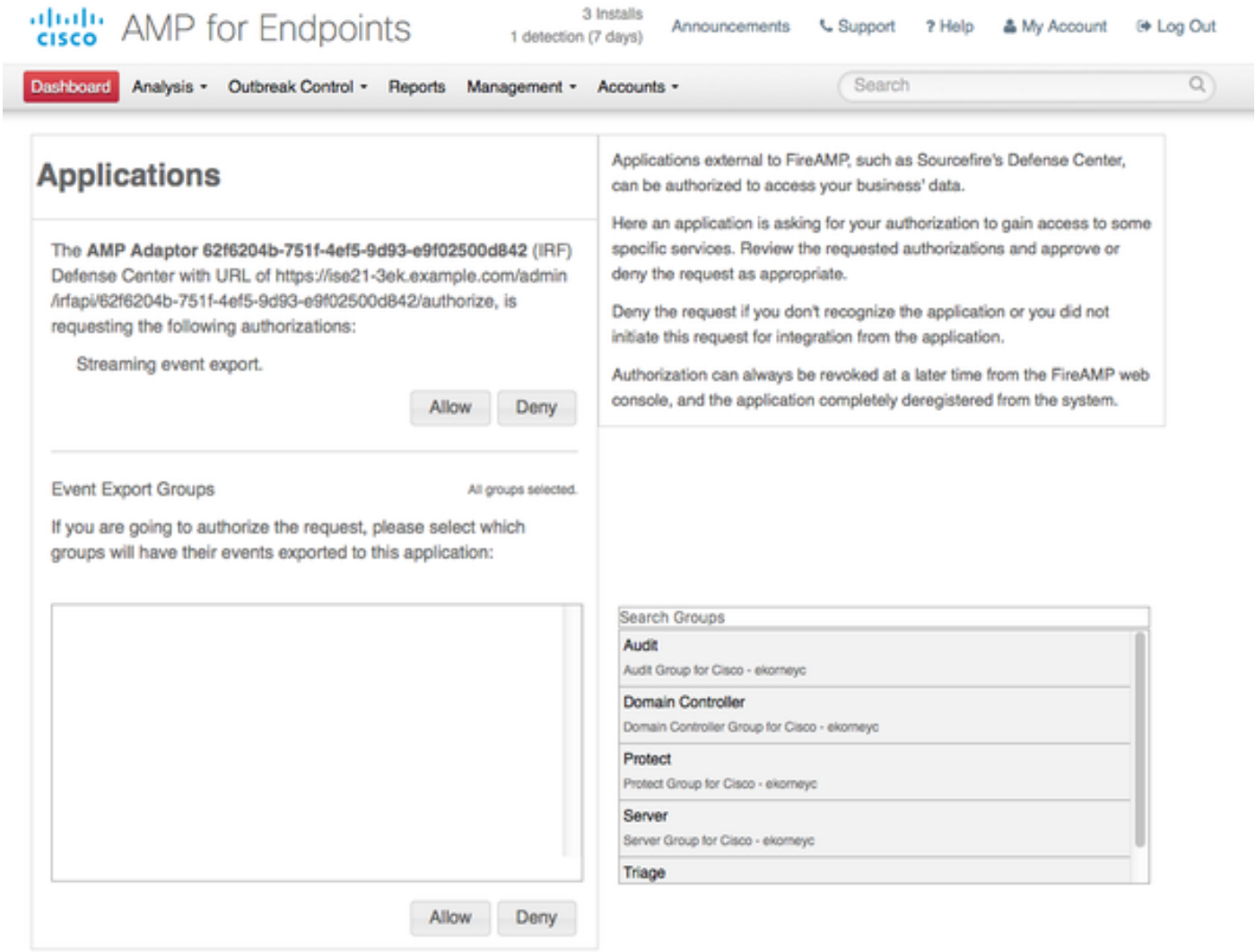
Seleccione la **nube** y haga clic en **después**



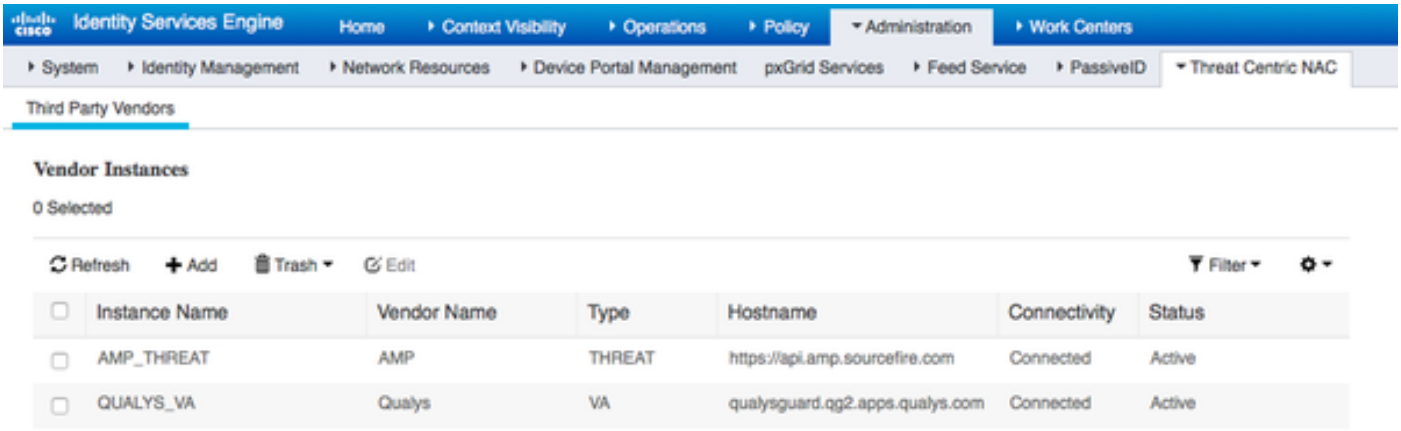
Haga clic el link y el login de FireAMP como admin en FireAMP.



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



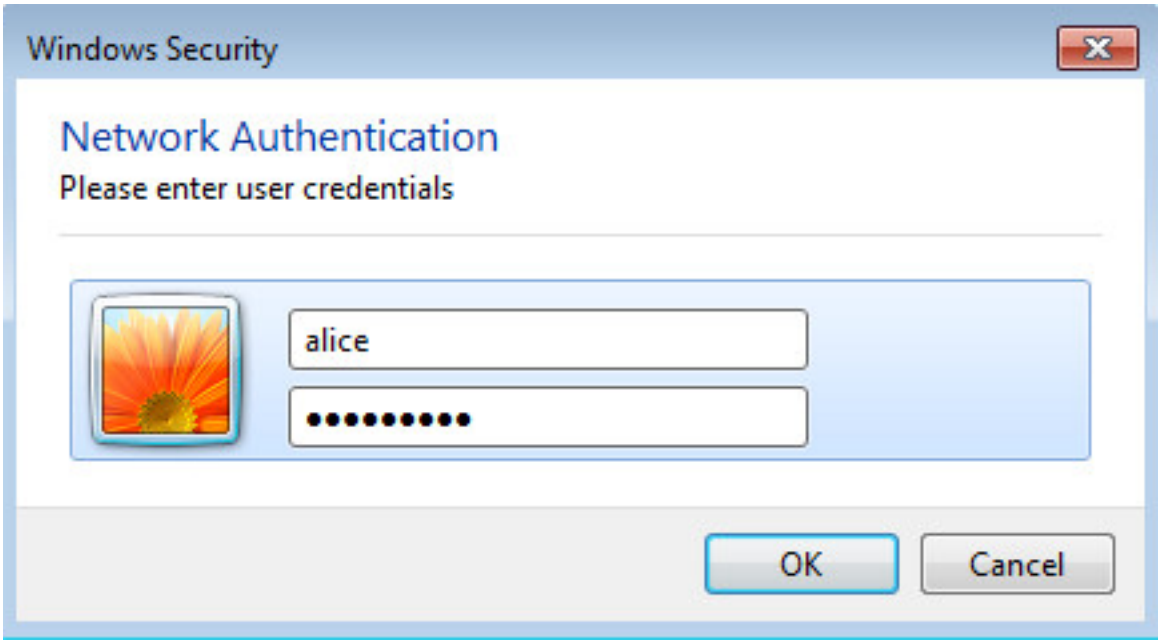
Seleccione los eventos (por ejemplo, descarga sospechosa, conexión al dominio sospechoso, malware ejecutado, compromiso de las Javas) esos usted quisiera monitorear. El resumen de la configuración del caso del adaptador se visualiza en la página de resumen de la configuración. Transiciones del caso del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



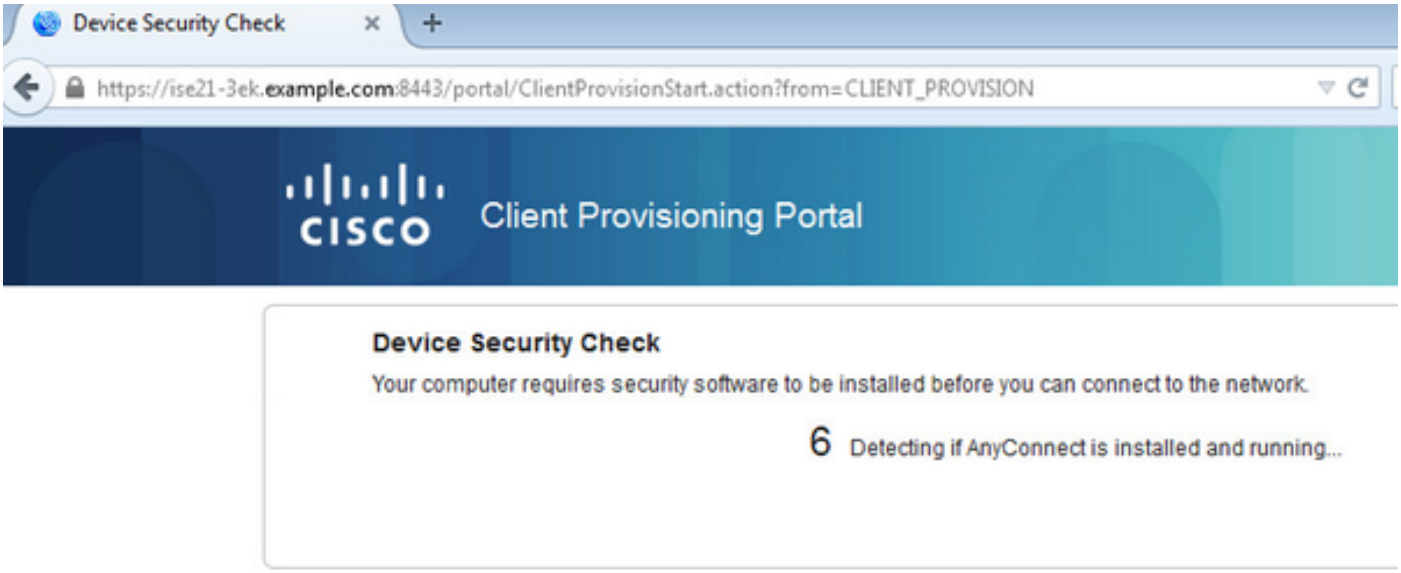
Verificación

Punto final

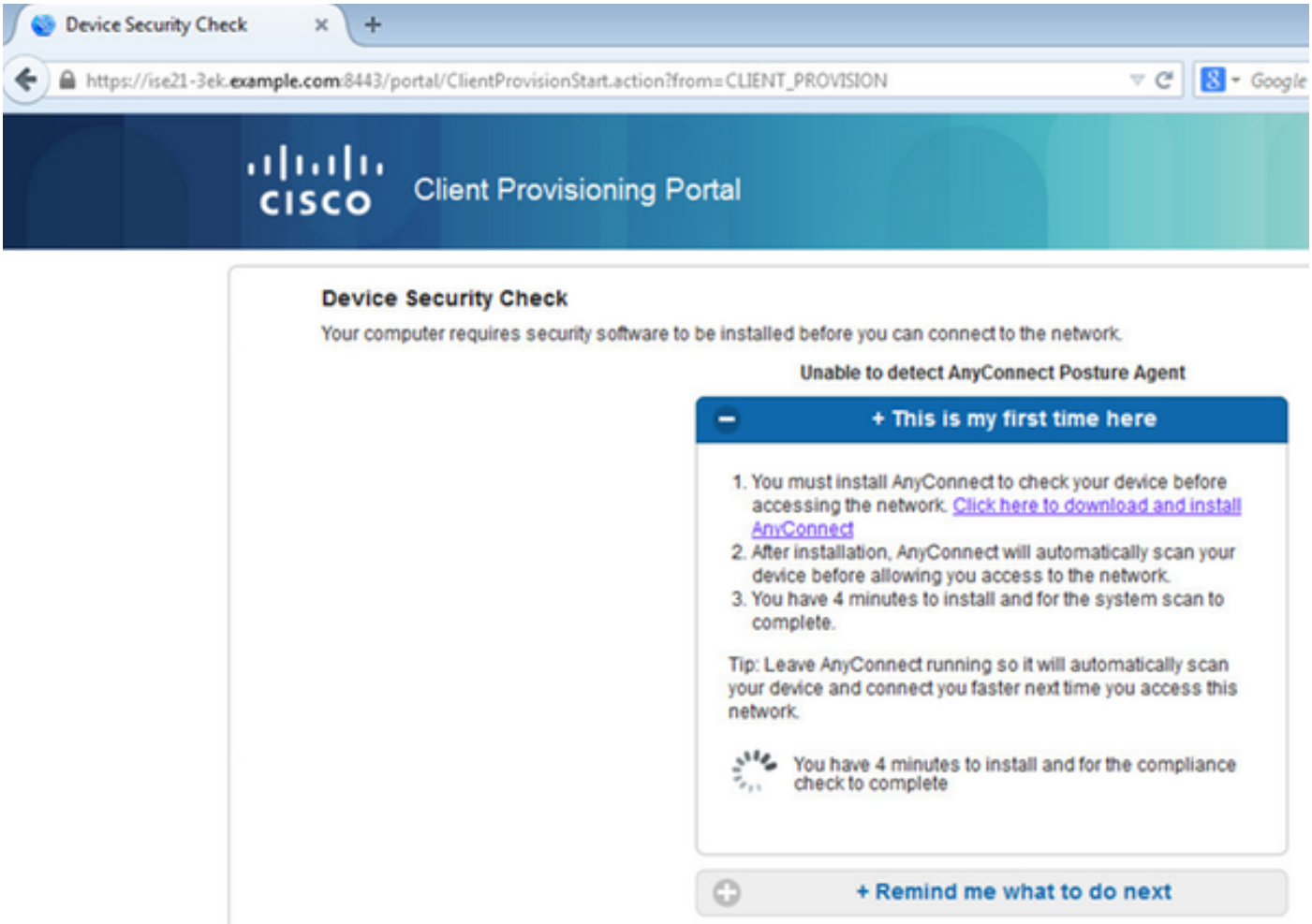
Conecte con la red inalámbrica vía PEAP (MSCHAPv2).



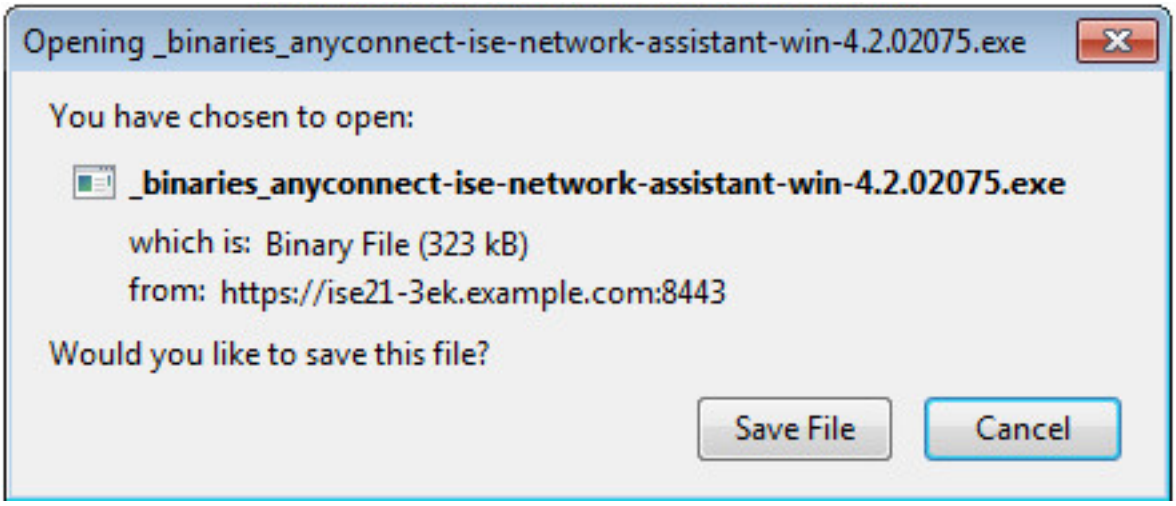
Una vez que está conectado el cambio de dirección con el portal de disposición del cliente ocurre.



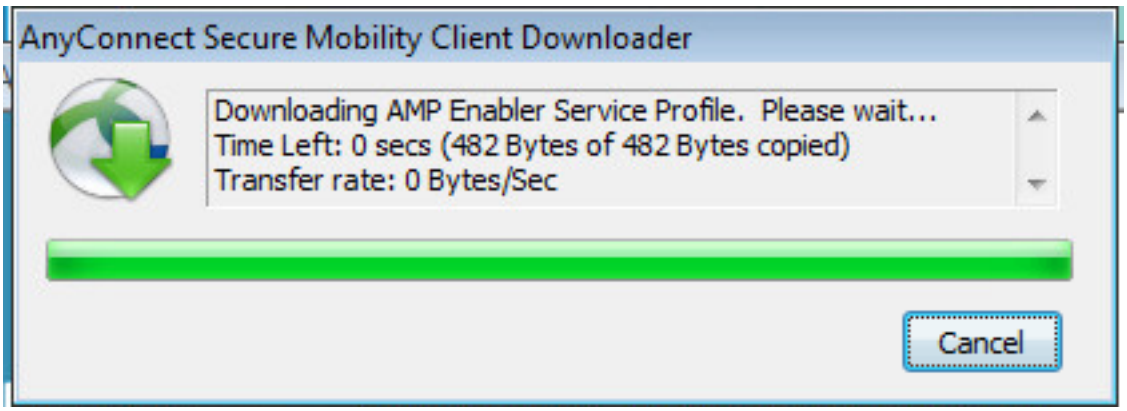
Puesto que no hay nada instalado en la máquina del cliente, el ISE indica para la instalación del cliente de AnyConnect.

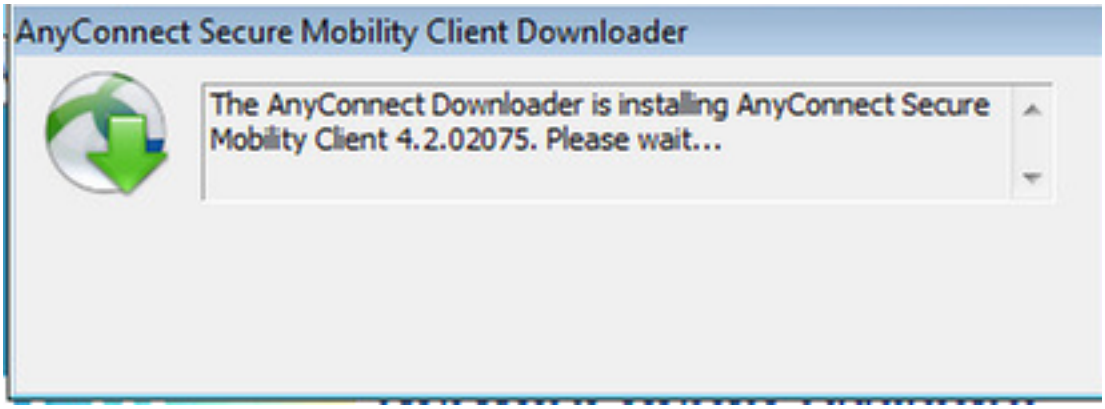


La aplicación auxiliar de la configuración de la red (NSA) se debe descargar y funcionamiento de la máquina del cliente.

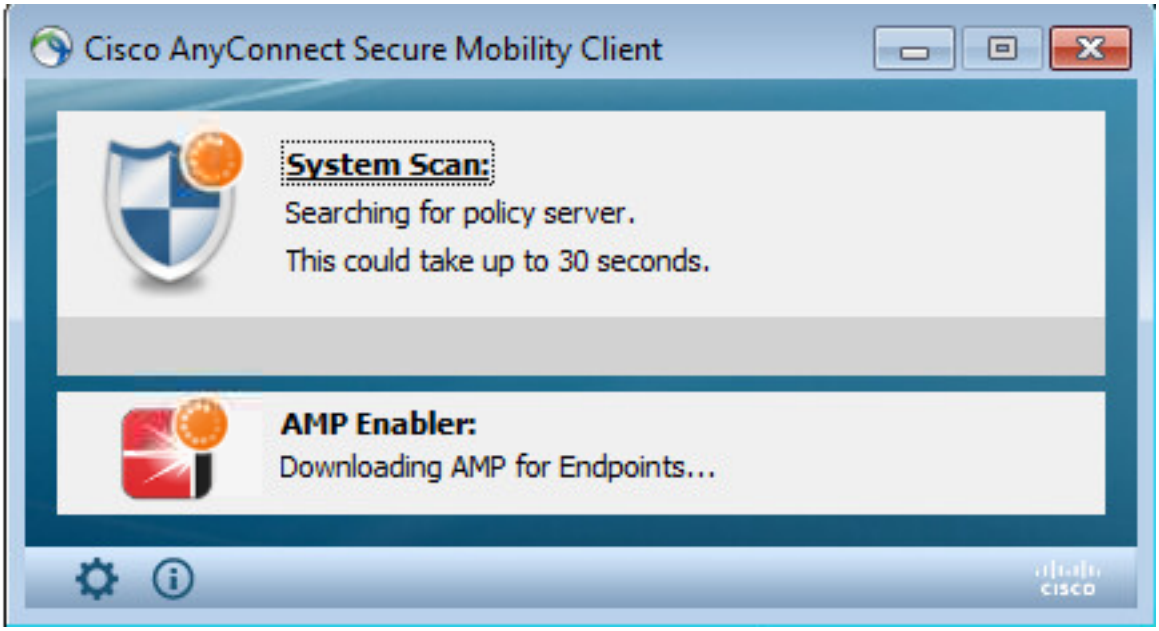


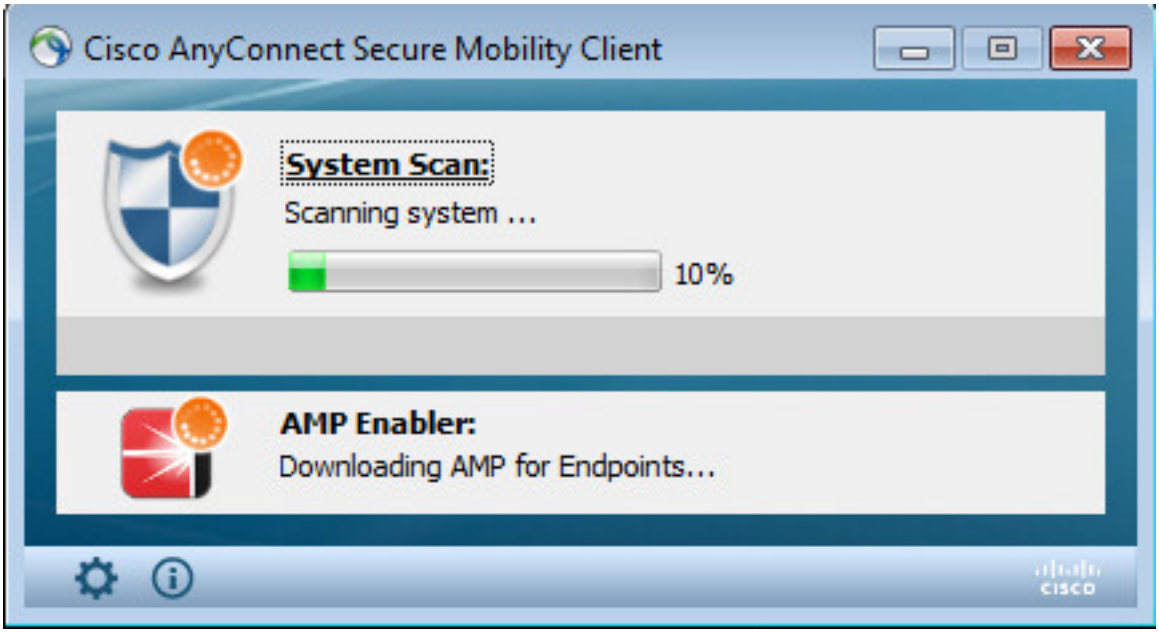
El NSA toma el cuidado de instalar los componentes requeridos y los perfiles.



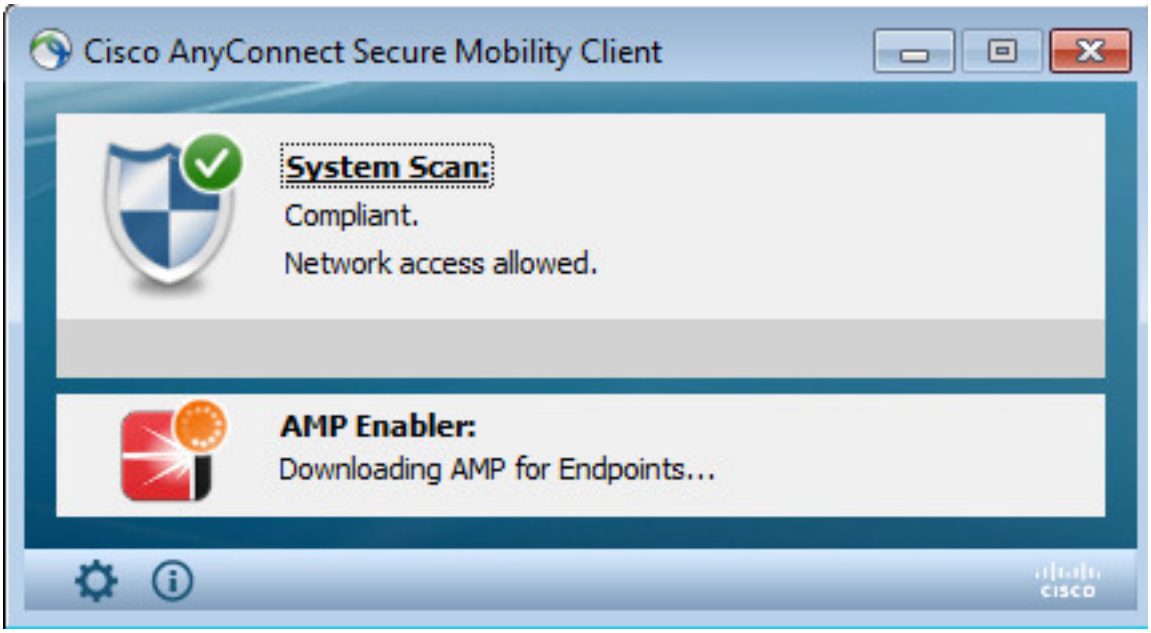


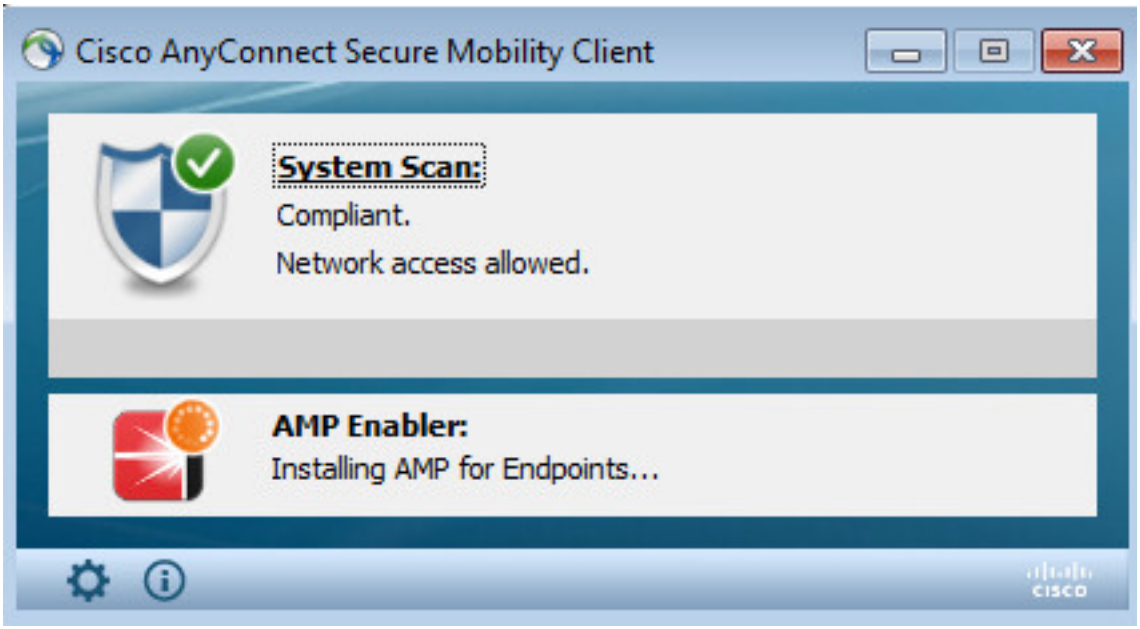
Una vez que se acaba la instalación, el módulo de la postura de AnyConnect realiza el control de la conformidad.

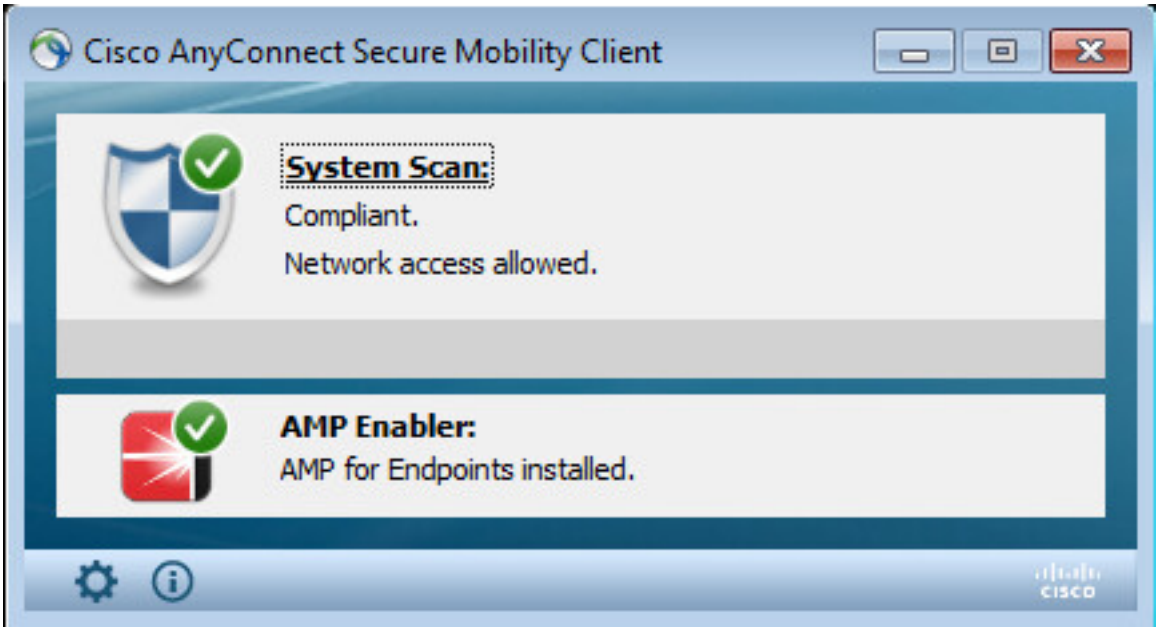




Pues se da el acceso total, si el punto final es obediente, el AMP se descarga y está instalado del web server especificado anterior en el perfil AMP.

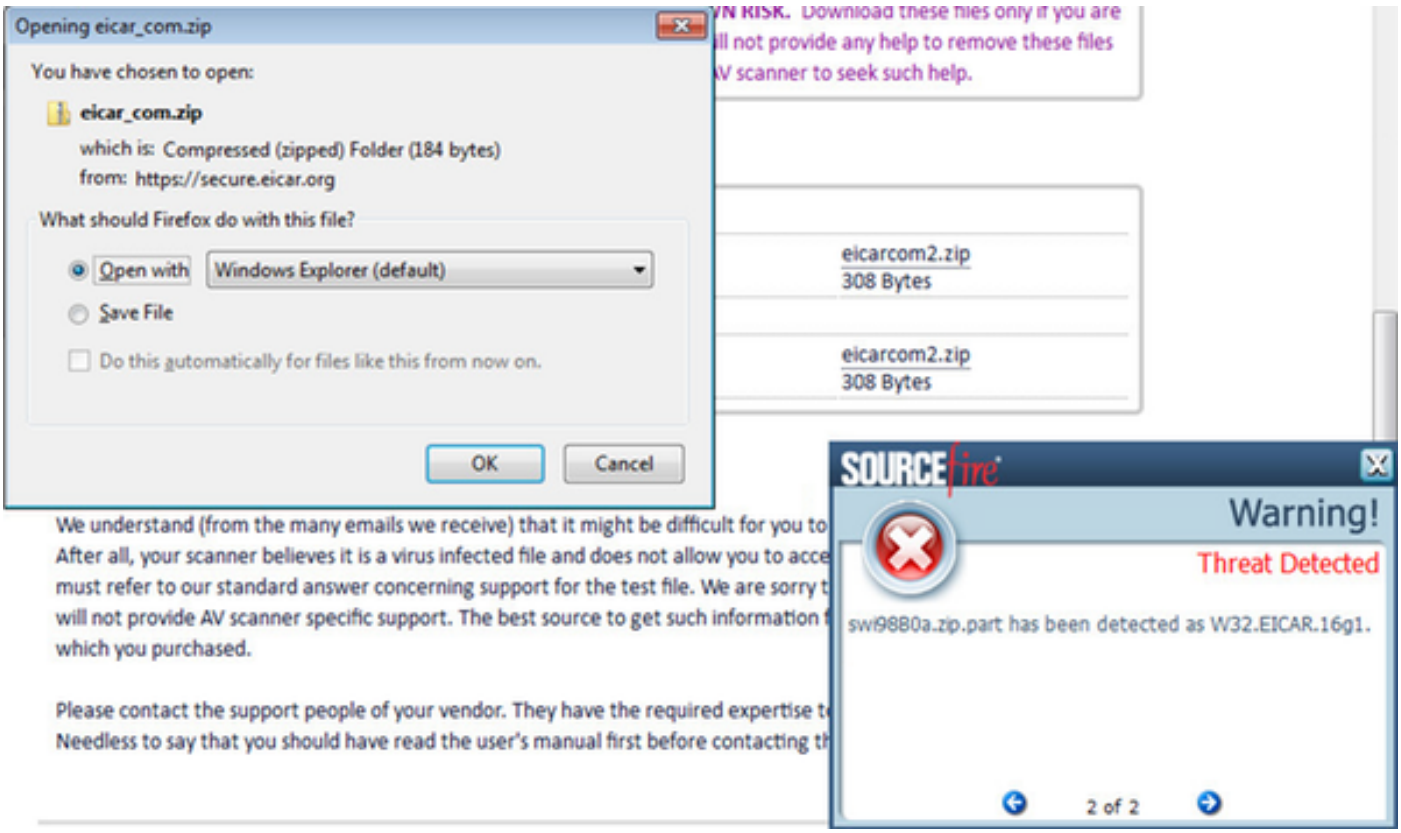






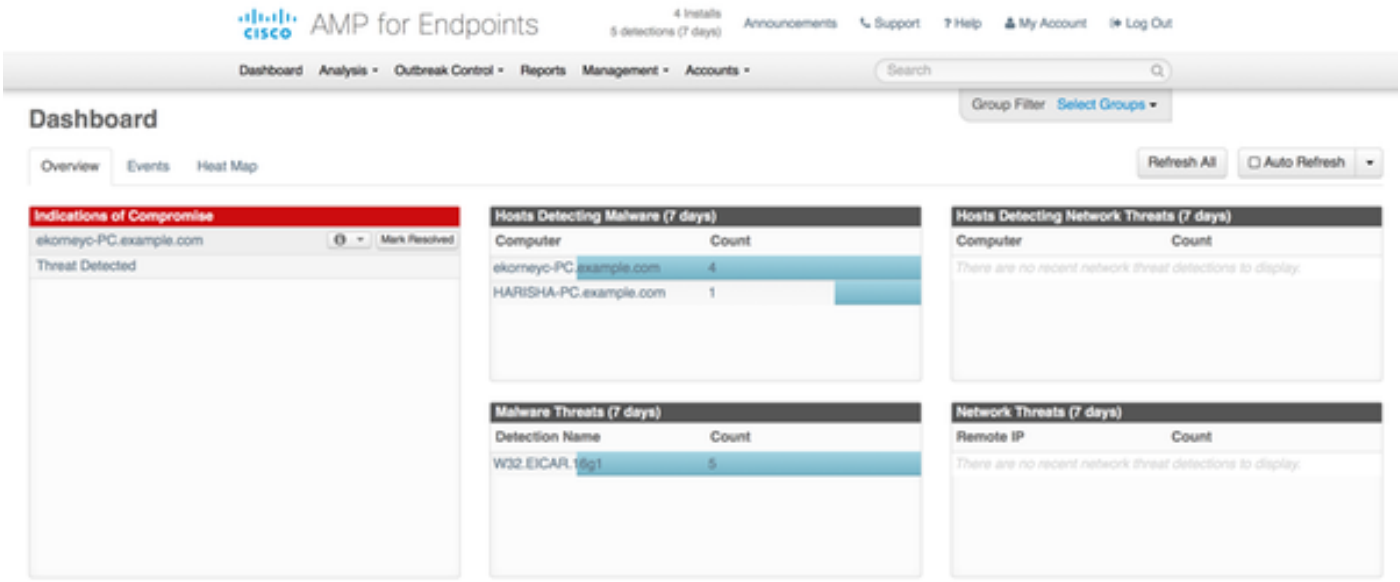
El conector AMP aparece.

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.

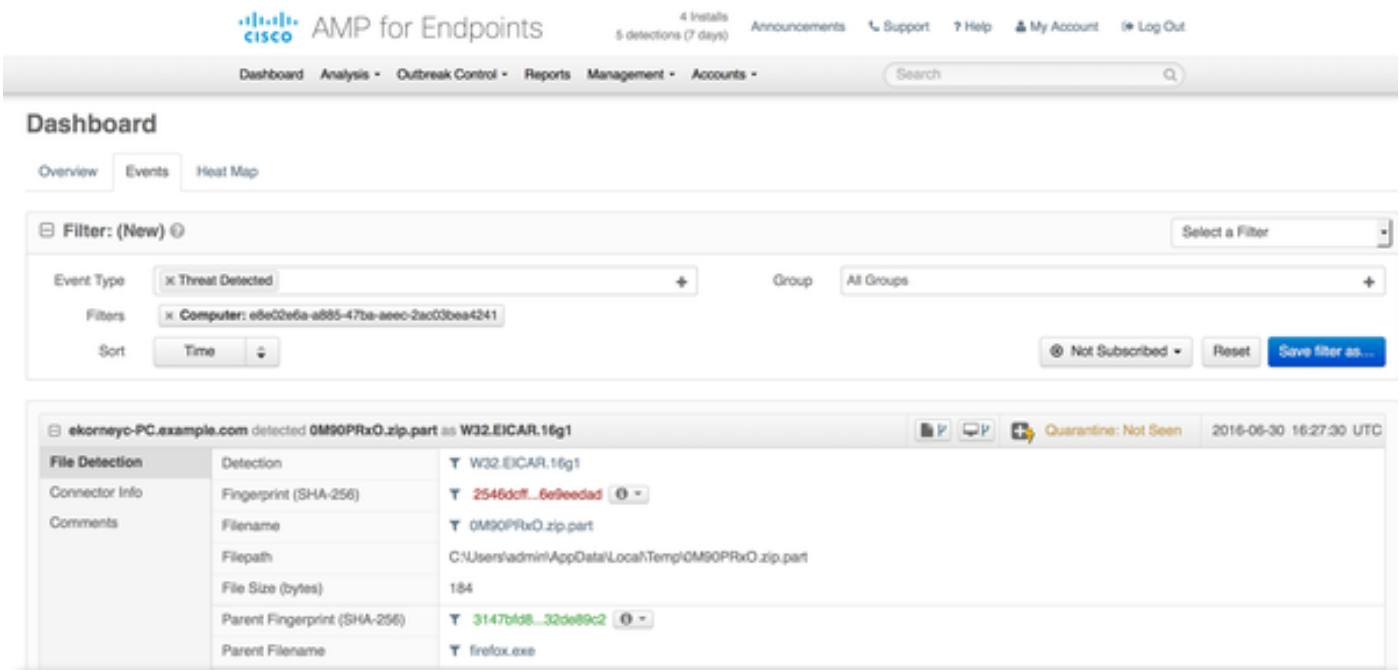


Nube AMP

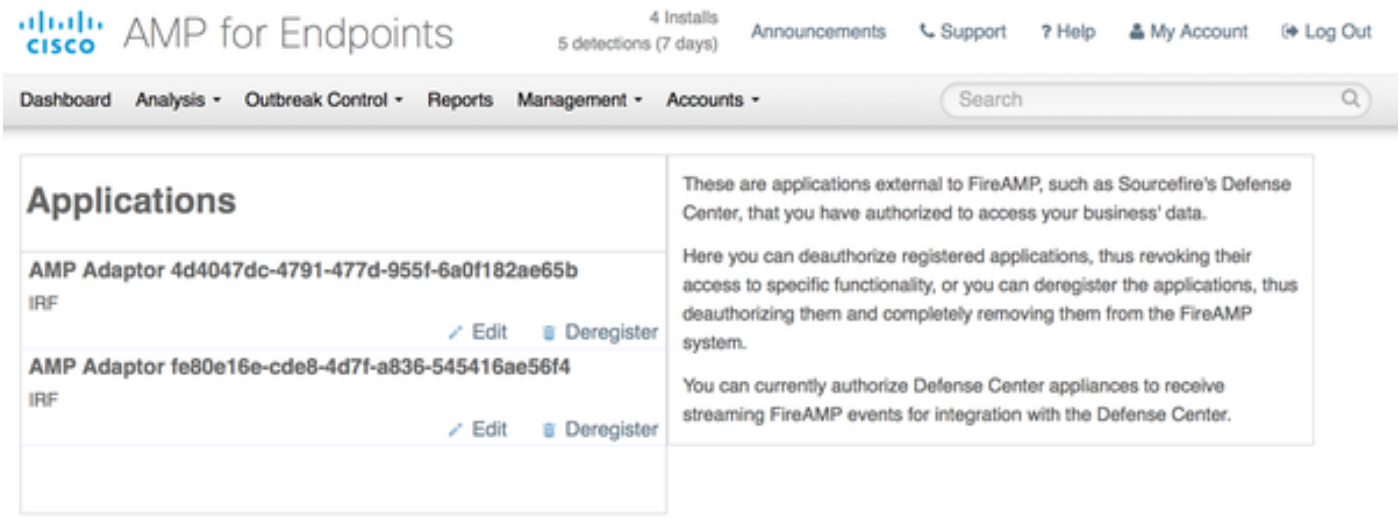
Para verificar los detalles del panel de la amenaza de la nube AMP puede ser utilizado.



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

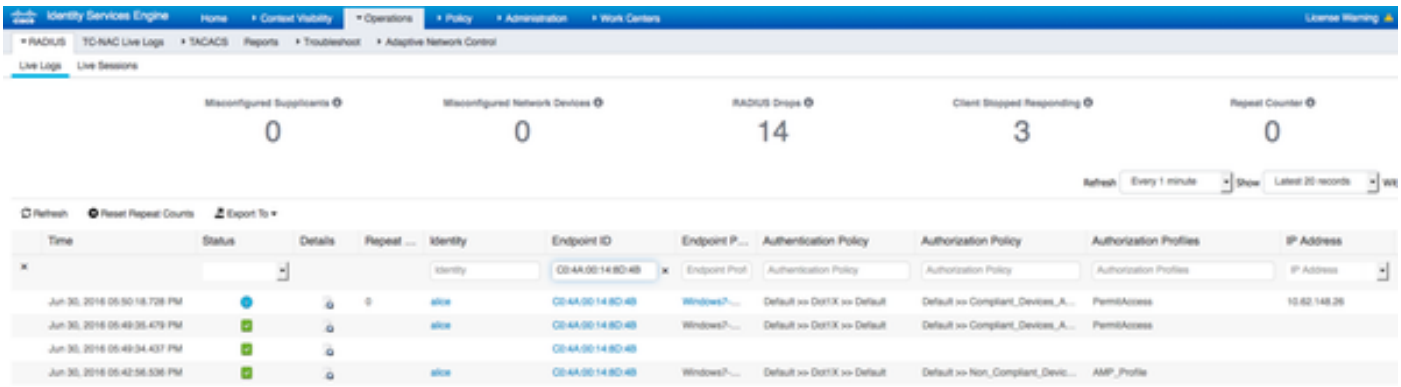


Para ver o desregistrar el caso del ISE que usted puede navegar a las cuentas > a las aplicaciones

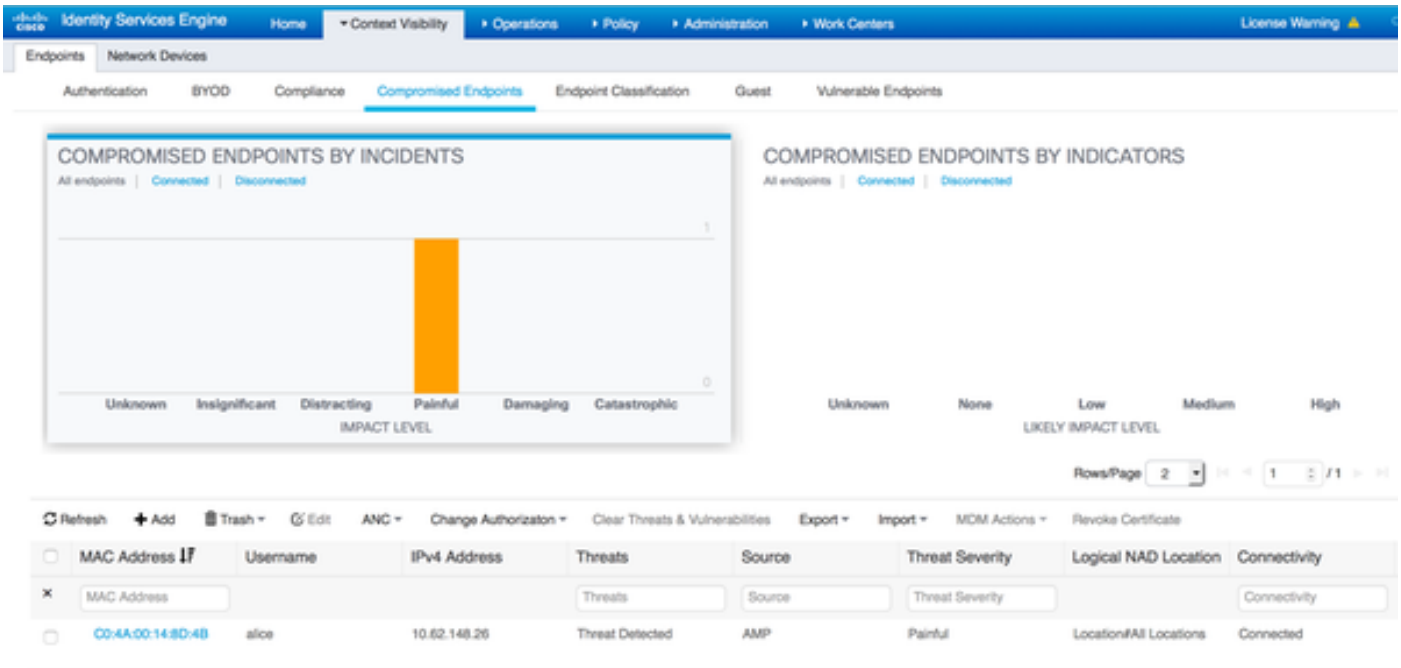


ISE

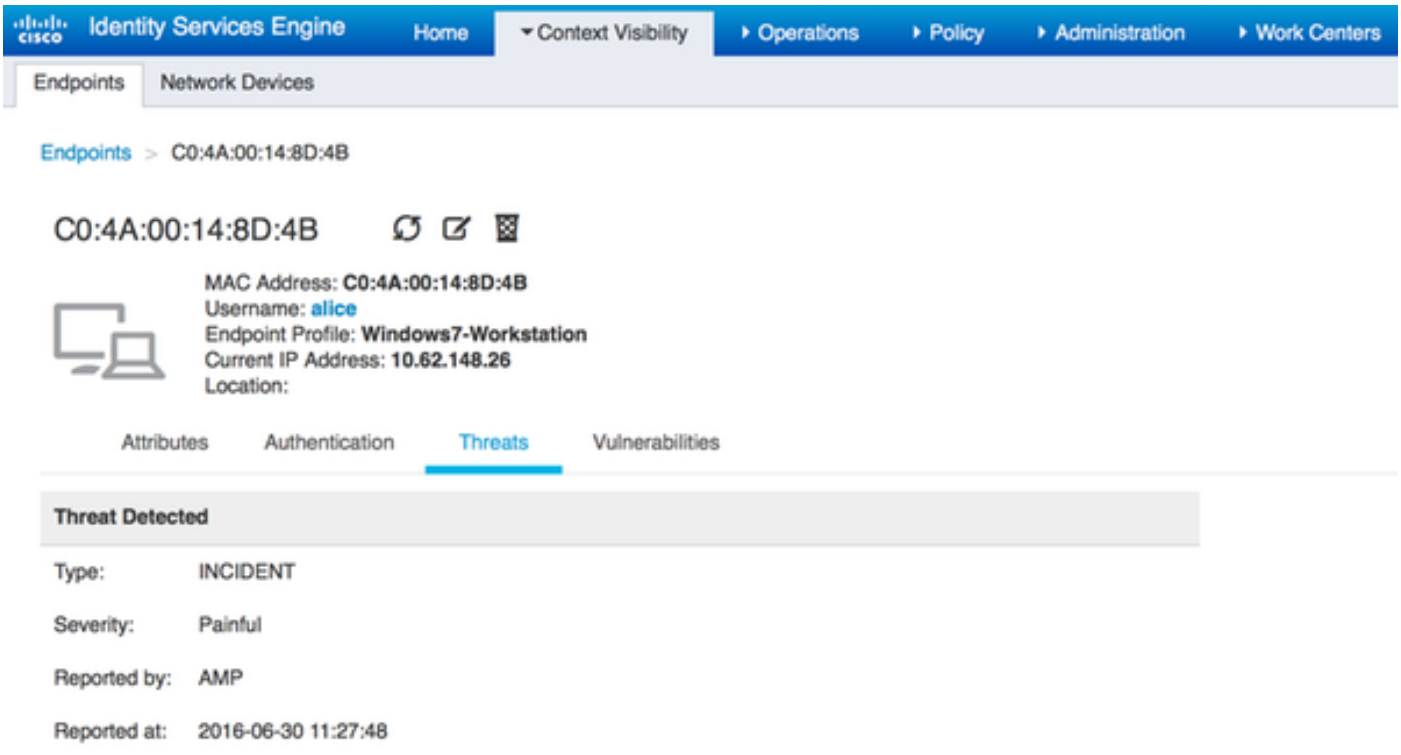
En ISE que sí mismo el flujo regular de la postura se considera, cambio de dirección ocurre primero para marcar la conformidad de la red. Tan pronto como el punto final sea obediente, se envía el CoA Reauth y el nuevo perfil con PermitAccess se asigna.



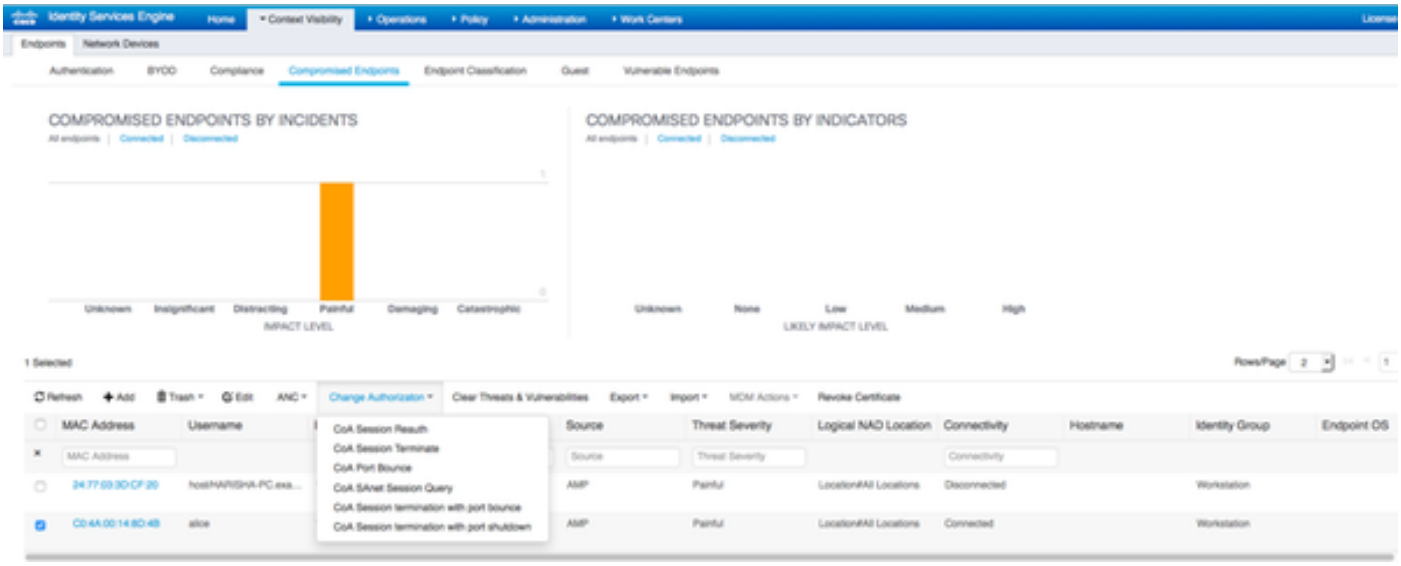
Para ver las amenazas detectadas que usted puede navegar a la visibilidad > a los puntos finales del contexto > los puntos finales comprometidos



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



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.



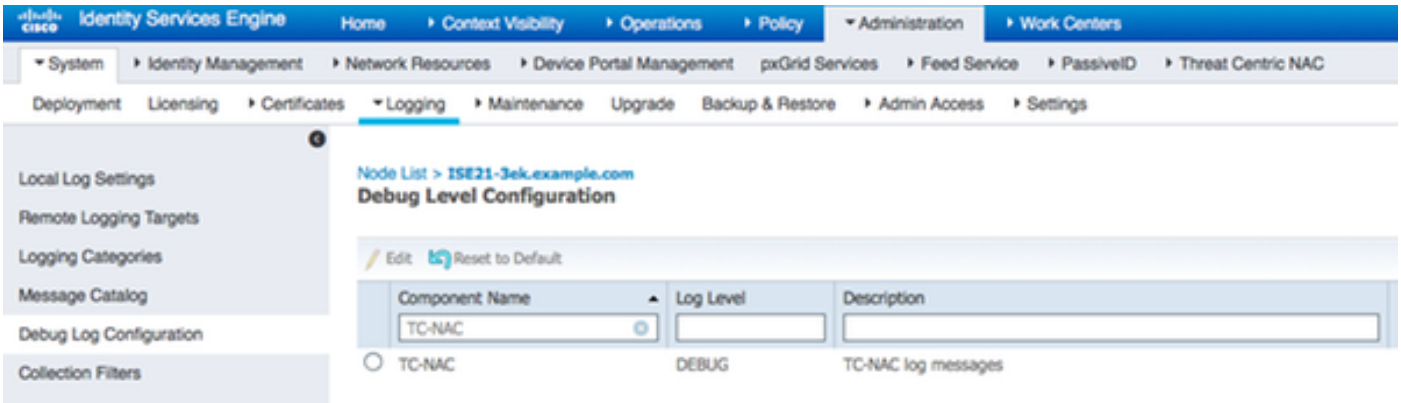
Si se selecciona la sesión Terminate CoA, el ISE envía la desconexión CoA y el cliente pierde el acceso a la red.

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**



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}