Configurar o 2.1 NAC Ameaça-céntrico ISE (TC-NAC) com AMP e serviços da postura

Índice

Introdução

Este original descreve como configurar o NAC Ameaça-céntrico com proteção avançada do malware (AMP) no 2.1 do Identity Services Engine (ISE). Os níveis de seriedade da ameaça e os resultados da avaliação da vulnerabilidade podem ser usados para controlar dinamicamente o nível de acesso de um valor-limite ou de um usuário. Os serviços da postura são sejam cobertos igualmente como parte de este original.

> Nota: A finalidade do original é descrever a integração do 2.1 ISE com AMP, Posture serviços está mostrada como são exigidos quando nós provision o AMP do ISE.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Motor do serviço da identidade de Cisco
- Proteção avançada do malware

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 2.1 do motor do serviço da identidade de Cisco
- Controlador do Wireless LAN (WLC) 8.0.121.0
- Cliente VPN 4.2.02075 de AnyConnect
- Pacote de serviços 1 de Windows 7

Configurar

Diagrama de Rede

Fluxo detalhado

1. O cliente conecta à rede, o **AMP_Profile** é atribuído e o usuário é reorientado ao portal do abastecimento de Anyconnect. Se Anyconnect não é detectado na máquina, todos os módulos configurados (VPN, AMP, postura) estão instalados. A configuração é incrementada cada módulo junto com esse perfil

2. Uma vez que Anyconnect é instalado, a avaliação da postura é executado

3. O módulo AMP Habilitador instala o conector de FireAMP

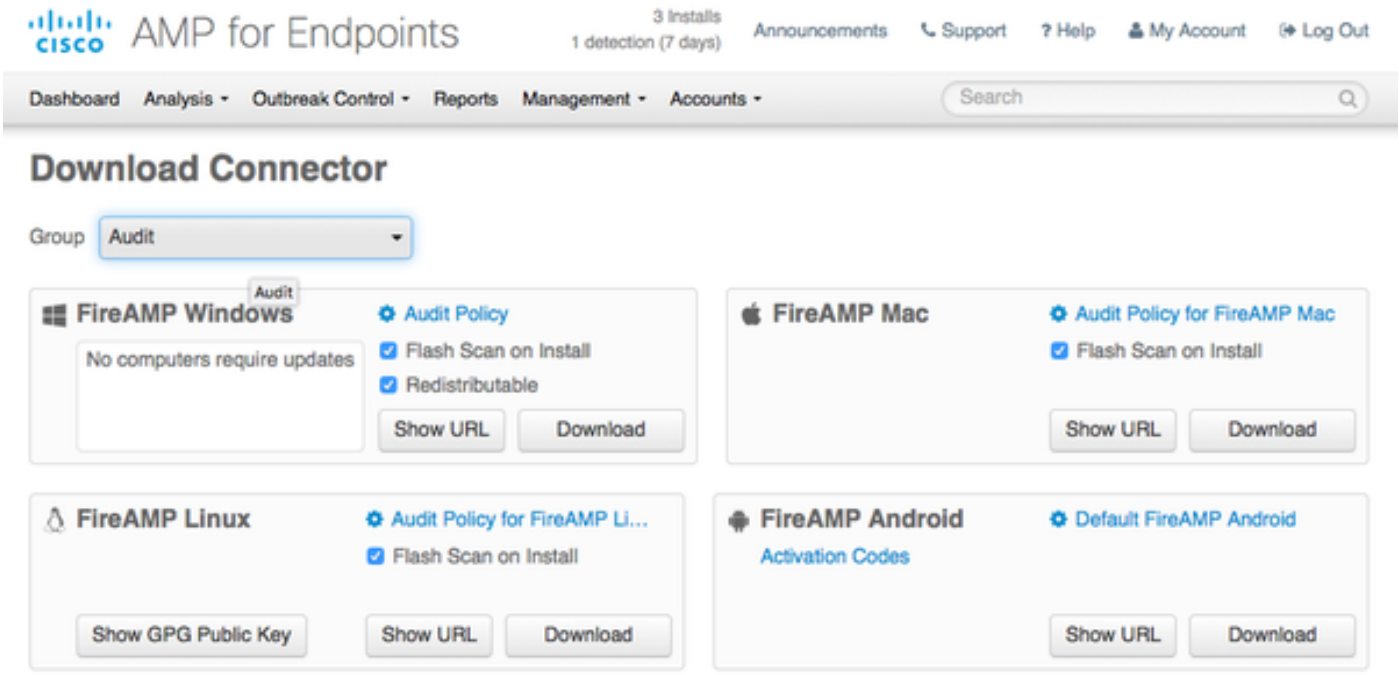
4. Quando o cliente tenta transferir o software malicioso, o conector AMP joga um mensagem de advertência e relata-o à nuvem AMP

5. A nuvem AMP envia esta informação ao ISE

Configurar a nuvem AMP

Etapa 1. Conector da transferência da nuvem AMP

A fim transferir o conector, navegue ao conector do Gerenciamento > da transferência. Selecione então o tipo e a **transferência** FireAMP (Windows, Android, Mac, Linux). **A auditoria** foi selecionada neste caso e o arquivo de instalação de FireAMP para Windows.

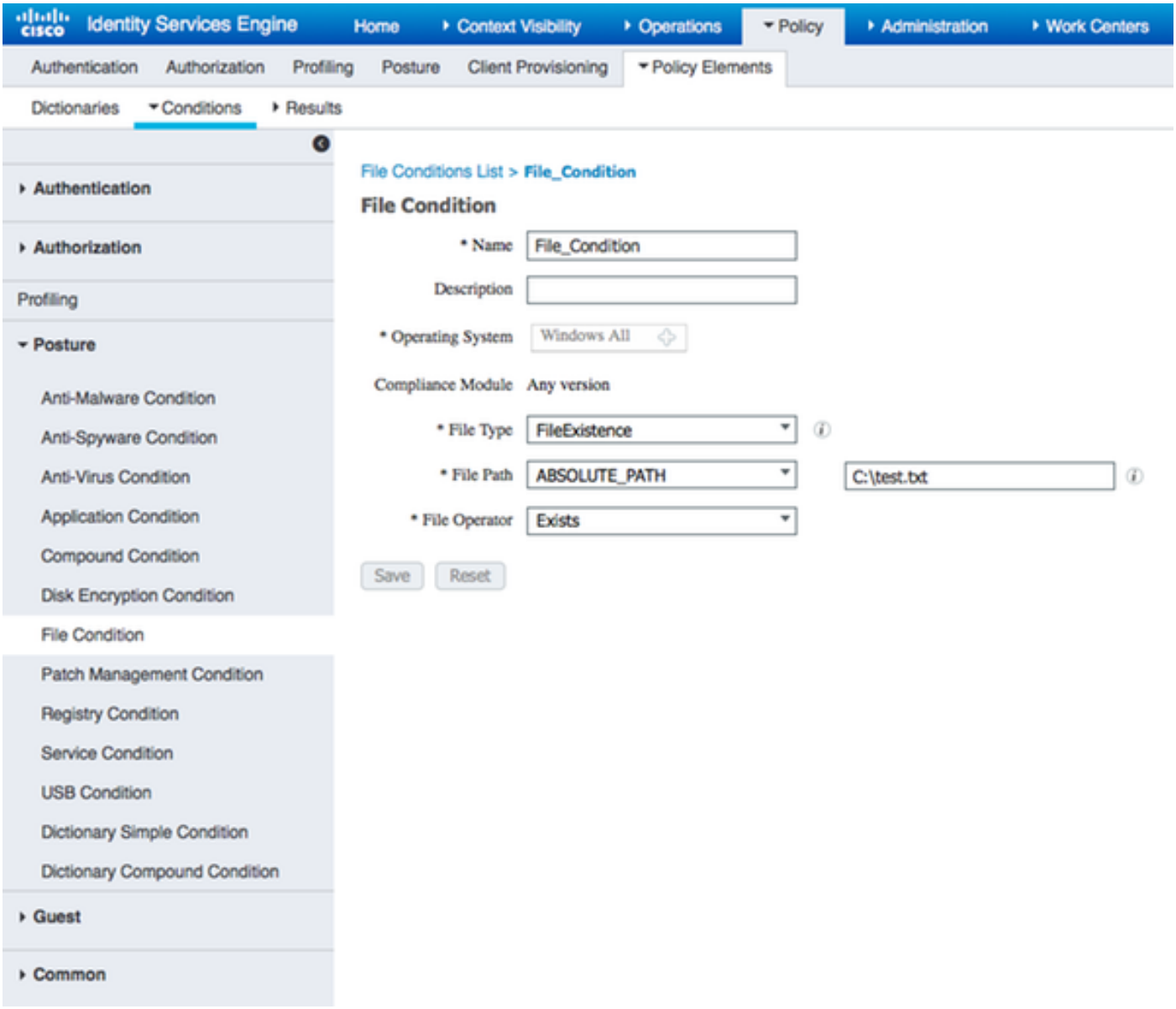


> Nota: Transferir este arquivo gerencie um arquivo do .exe chamado **Audit_FireAMPSetup.exe no** exemplo. Este arquivo esteve enviado ao servidor de Web para estar disponível uma vez que o usuário pede a configuração do AMP.

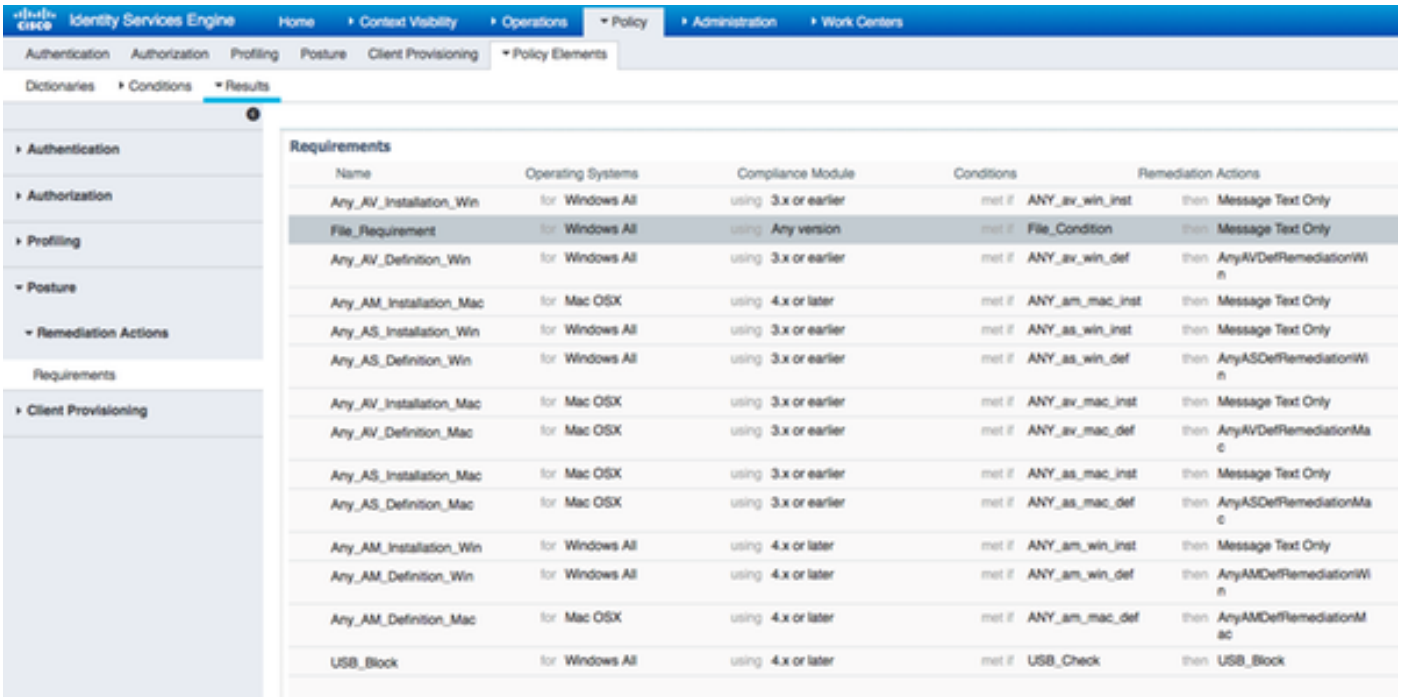
Configurar o ISE

Etapa 1. Configurar políticas e condições da postura

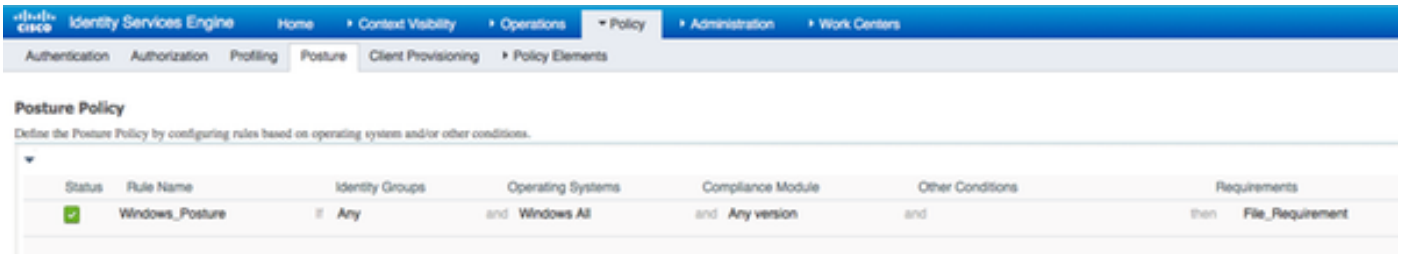
Navegue à política > aos elementos > às condições > à postura > ao arquivo Condition.You da política pode ver que uma condição simples para a existência do arquivo esteve criada. O arquivo tem que existir se o valor-limite é ser complacente com a política verificada pelo módulo da postura:



Esta circunstância é usada para uma exigência:

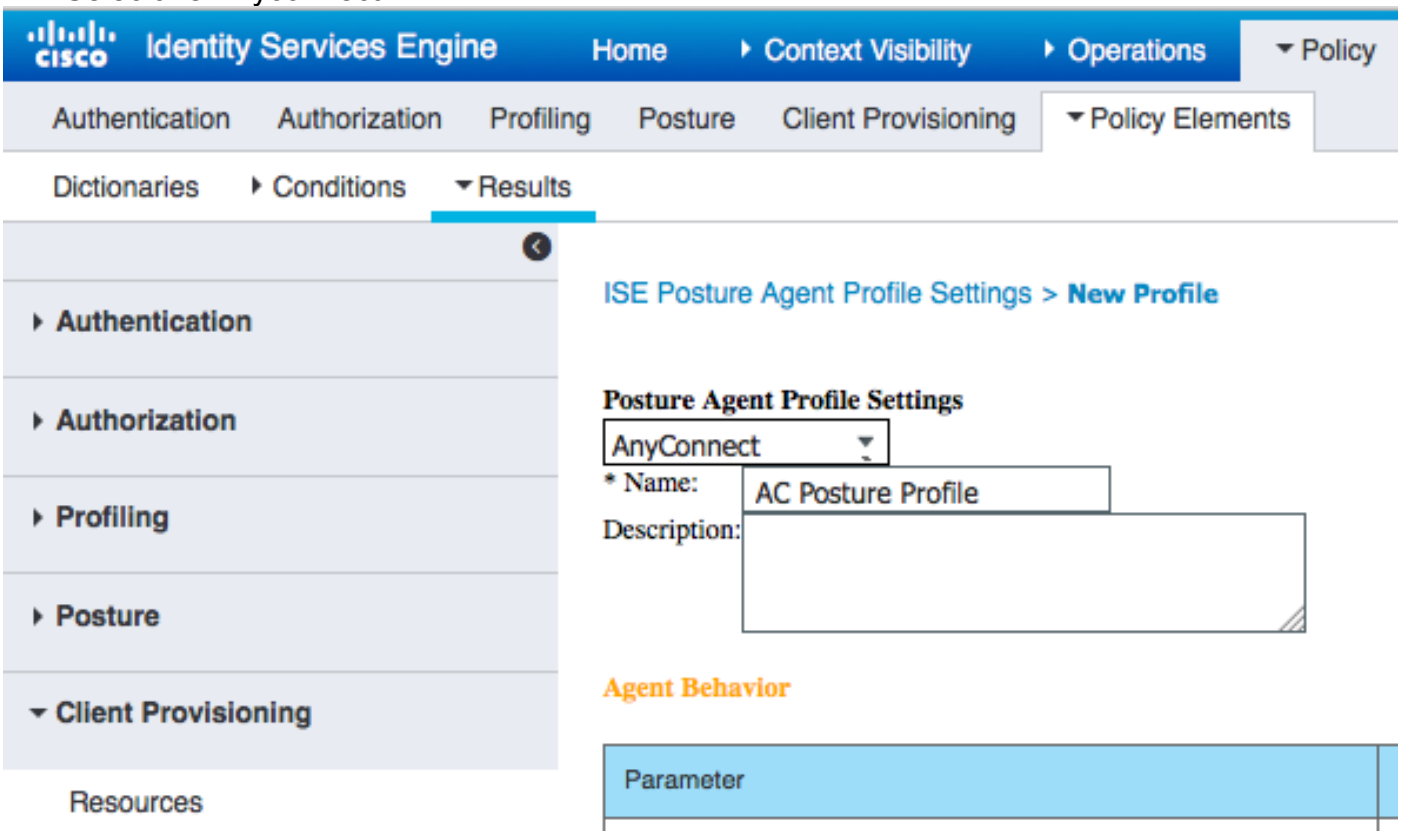


A exigência é usada na política da postura para sistemas de Microsoft Windows:

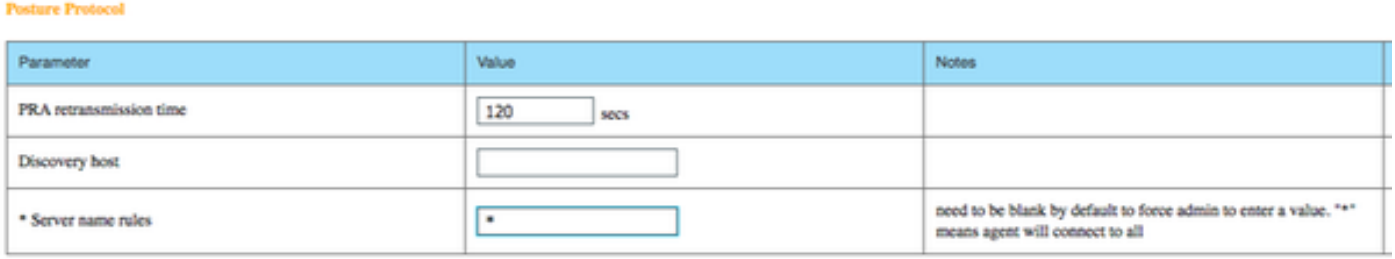


Etapa 2. Configurar o perfil da postura

- Navegue à política > aos elementos da política > aos resultados > ao abastecimento > aos recursos do cliente e adicionar o perfil da postura do agente do Network Admission Control (NAC) ou do agente de AnyConnect
- Selecione Anyconnect



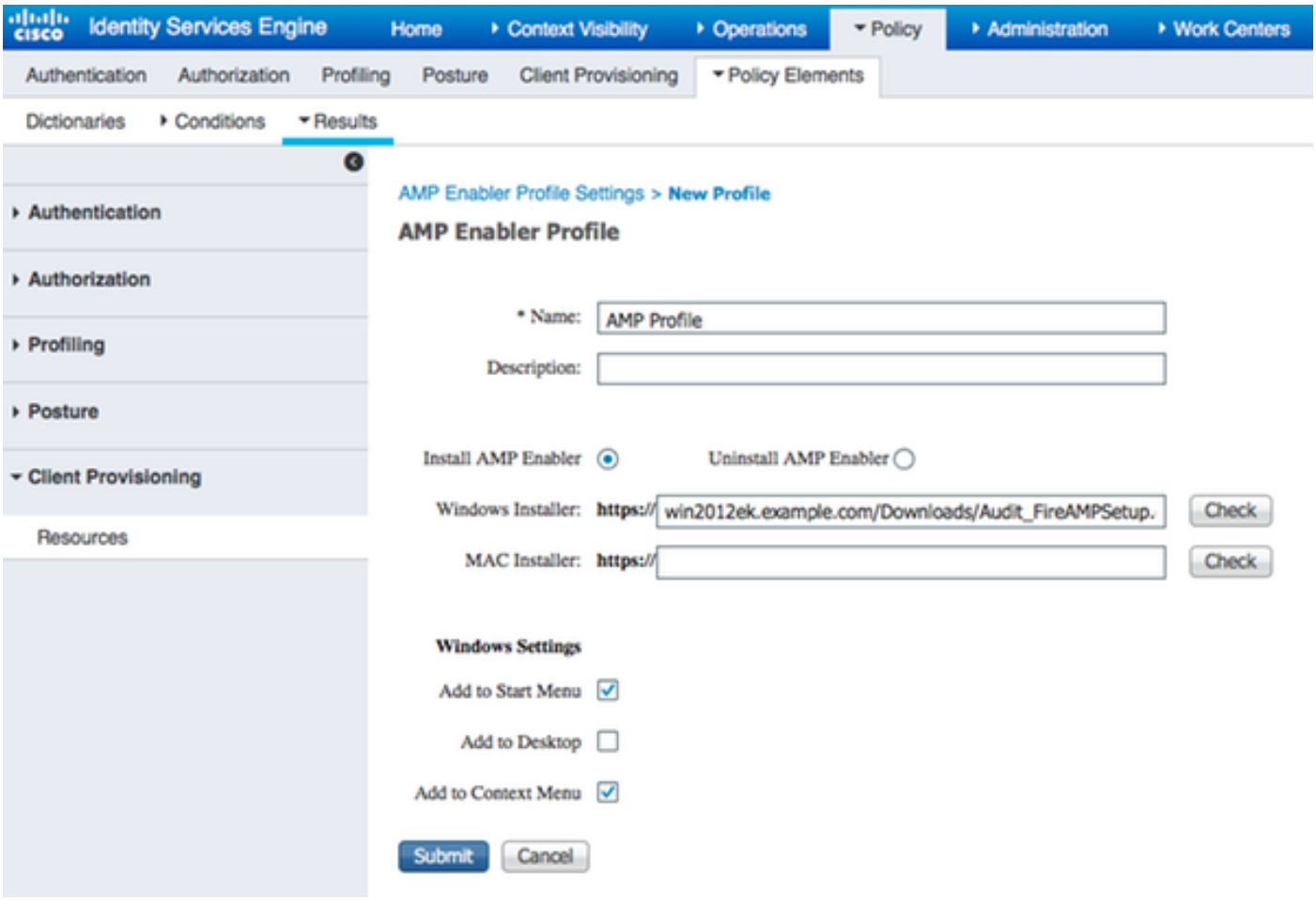
- Da seção de protocolo da postura adicionar * a fim permitir que o agente conecte a todos os server



Etapa 3. Configurar o perfil AMP

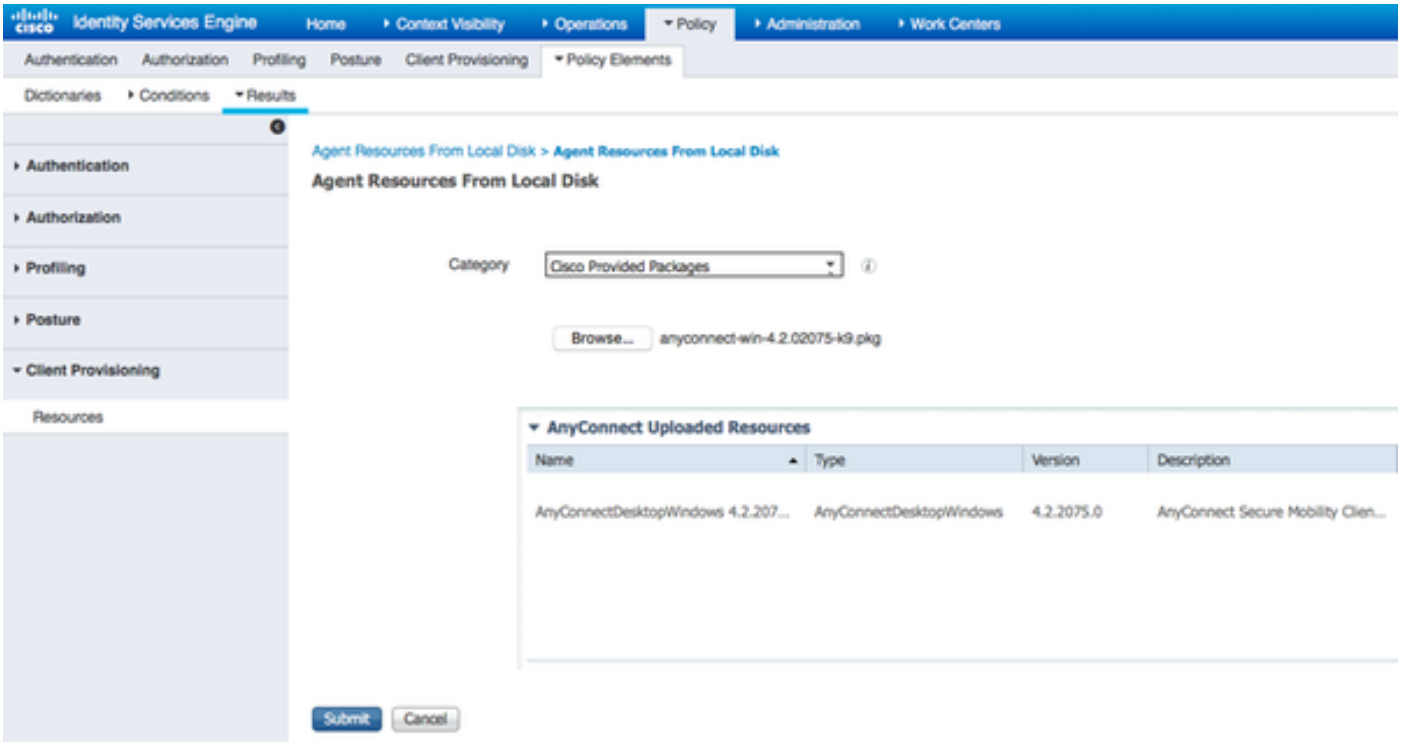
O perfil AMP contém a informação onde o instalador de Windows é encontrado. O instalador de

Windows foi transferido mais cedo da nuvem AMP. Deve ser acessível da máquina cliente. O certificado do servidor HTTPS, onde o instalador é encontrado deve ser confiado pela máquina cliente também.

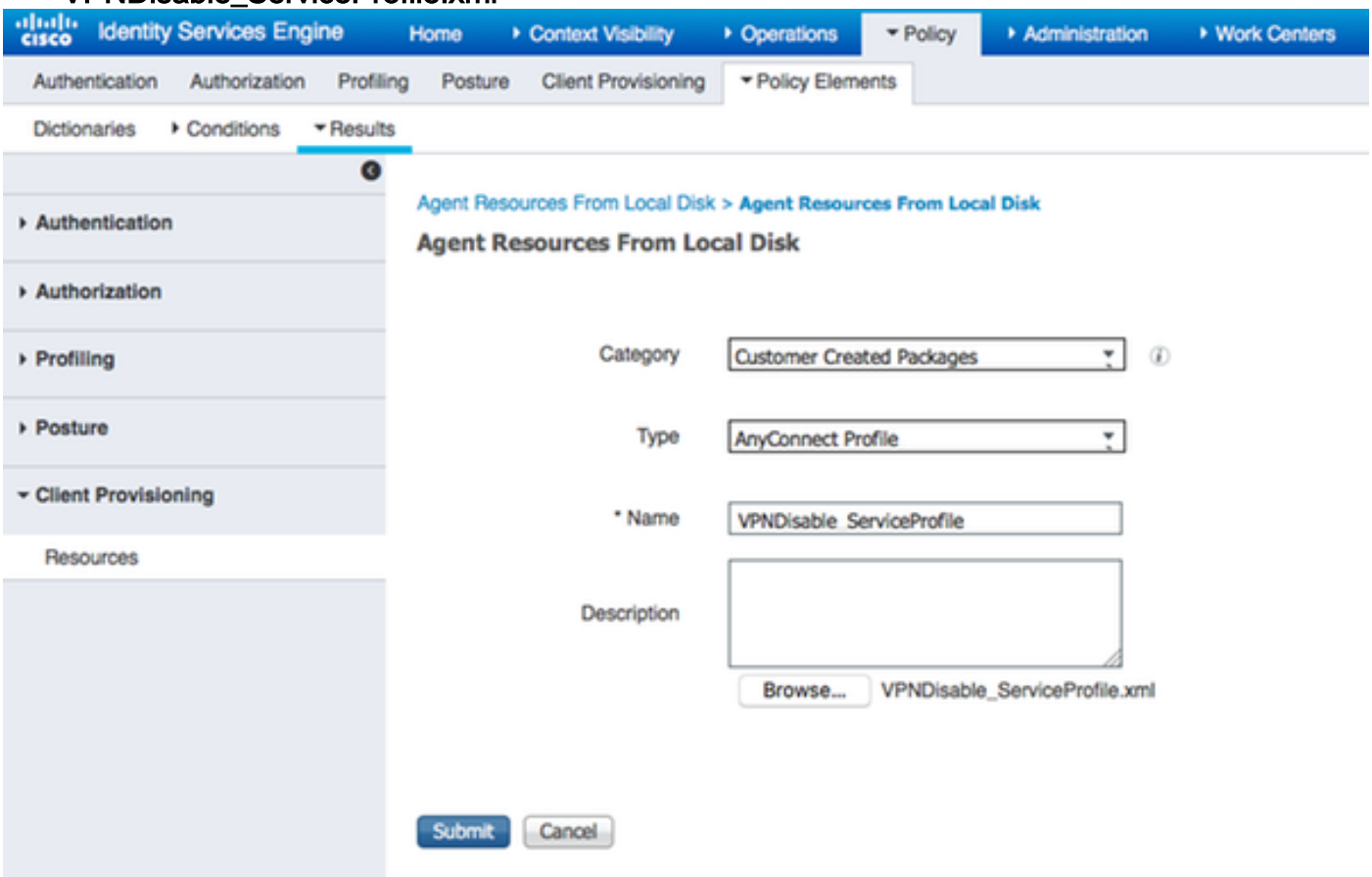


Etapa 2. Aplicativos da transferência de arquivo pela rede e perfil XML ao ISE

- Transfira o aplicativo manualmente do local de Cisco do oficial: **anyconnect-win-4.2.02075-k9.pkg**
- No ISE, navegue à política > aos elementos da política > aos resultados > ao abastecimento > aos recursos do cliente, e adicionar **recursos de agente do disco local**
- Escolha **Cisco forneceu pacotes** e **anyconnect-win-4.2.02075-k9.pkg** seleto



- Navegue à política > aos elementos da política > aos resultados > ao abastecimento > aos recursos do cliente e adicionar **recursos de agente do disco local**
- Escolha **pacotes** e o tipo **criados cliente perfil de AnyConnect**. Selecione **VPNDisable_ServiceProfile.xml**



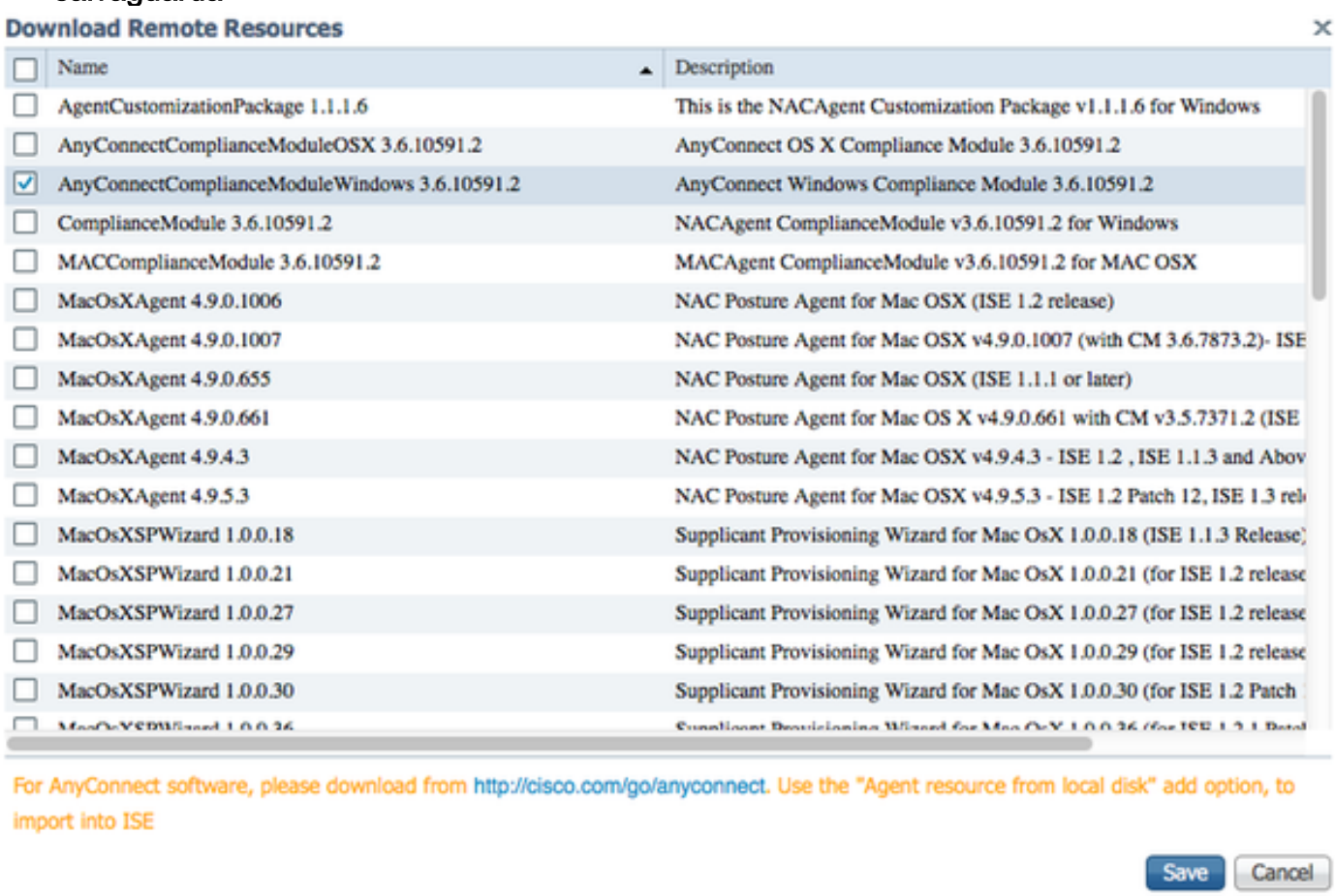
Nota: **VPNDisable_ServiceProfile.xml** é usado para esconder o título VPN, desde que este exemplo não usa o módulo de VPN. Este é o índice de VPNDisable_ServiceProfile.xml**:**

xmlns <AnyConnectProfile de " http://schemas.xmlsoap.org/encoding/" do xmlns=: xsi do

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

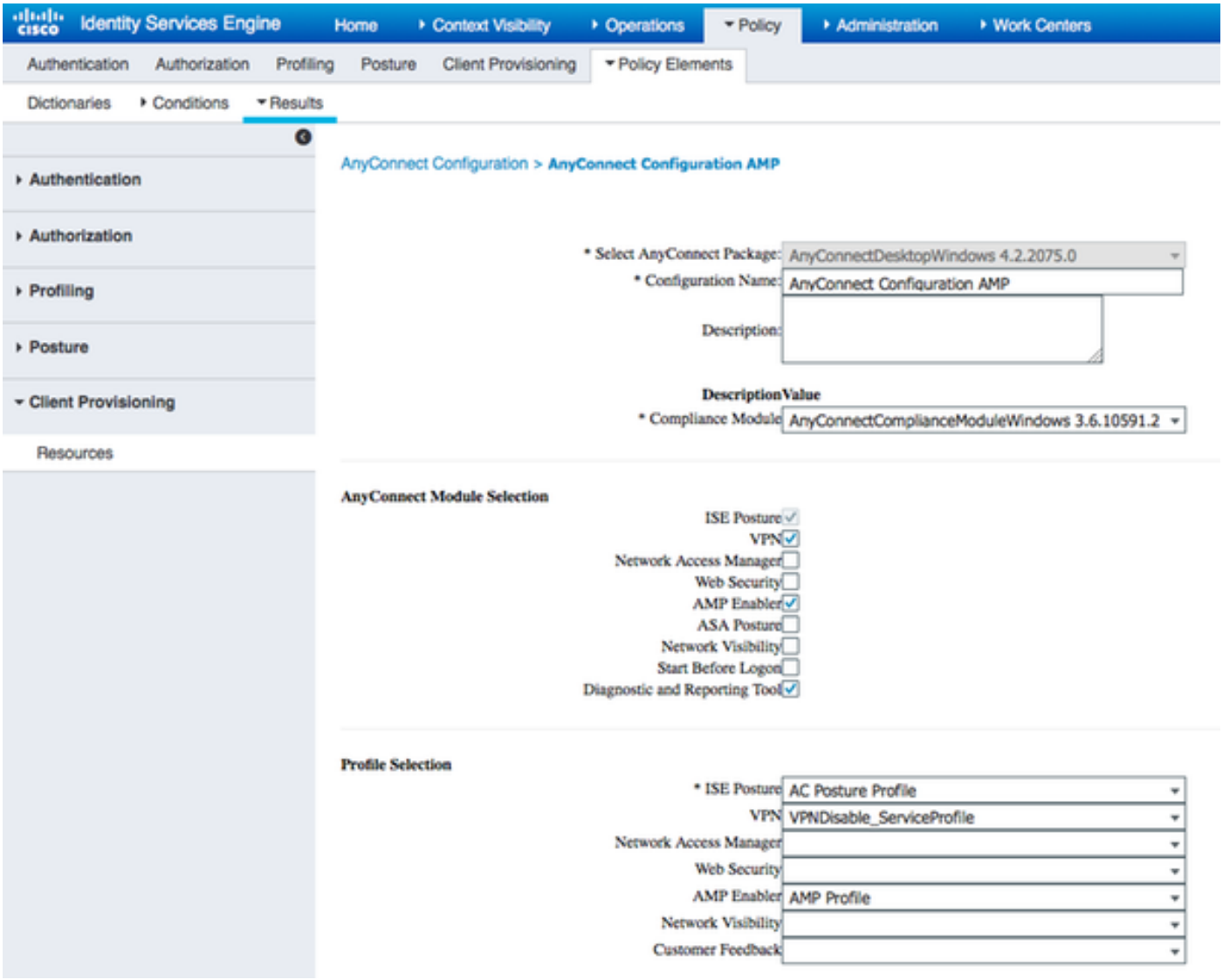
Etapa 3. Módulo da conformidade de AnyConnect da transferência

- Navegue à política > aos elementos da política > aos resultados > ao abastecimento > aos recursos do cliente e adicionar **recursos de agente do local de Cisco**
- Selecione o **módulo 3.6.10591.2 da conformidade de AnyConnect Windows** e clique sobre a **salvaguarda**



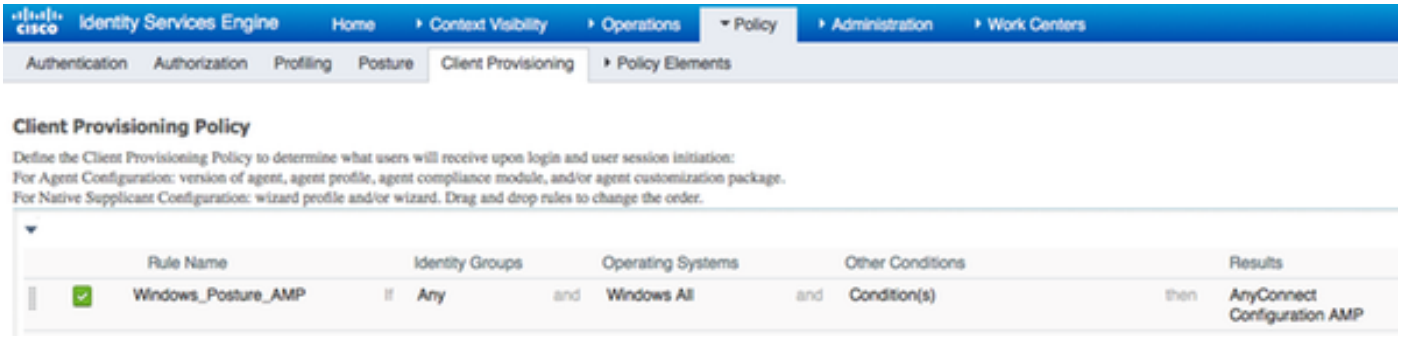
Etapa 4. Adicionar a configuração de AnyConnect

- Navegue à política > aos elementos da política > aos resultados > ao abastecimento > aos recursos do cliente, e adicionar a **configuração de AnyConnect**
- Configurar o nome e selecione módulo da conformidade e todos os módulos exigidos de AnyConnect (VPN, AMP, e a postura)
- **Na seleção do perfil**, escolha o perfil configurado mais cedo para cada módulo



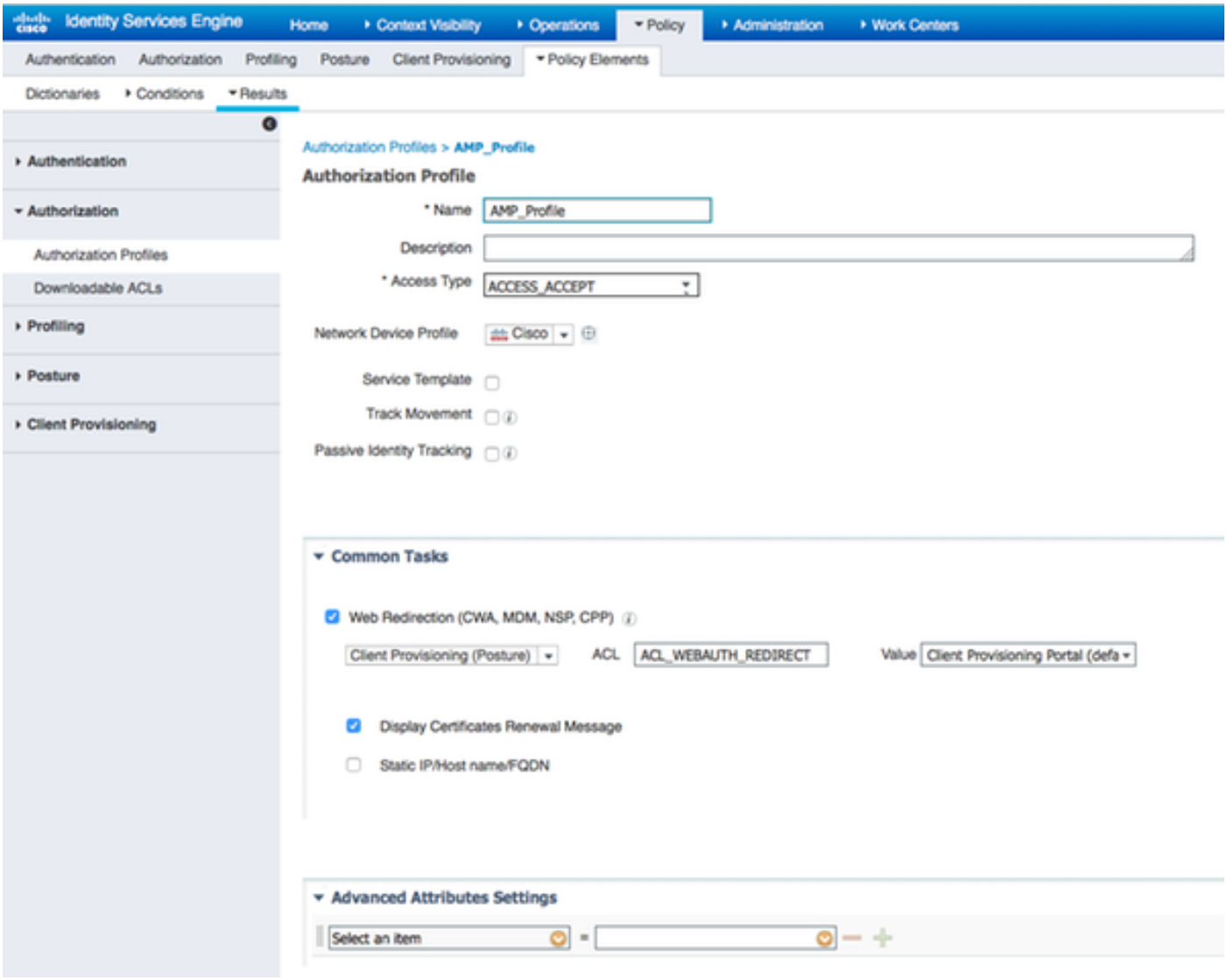
Etapa 5. Configurar regras do abastecimento do cliente

A configuração de AnyConnect criada mais cedo é provida nas regras do **abastecimento do cliente**

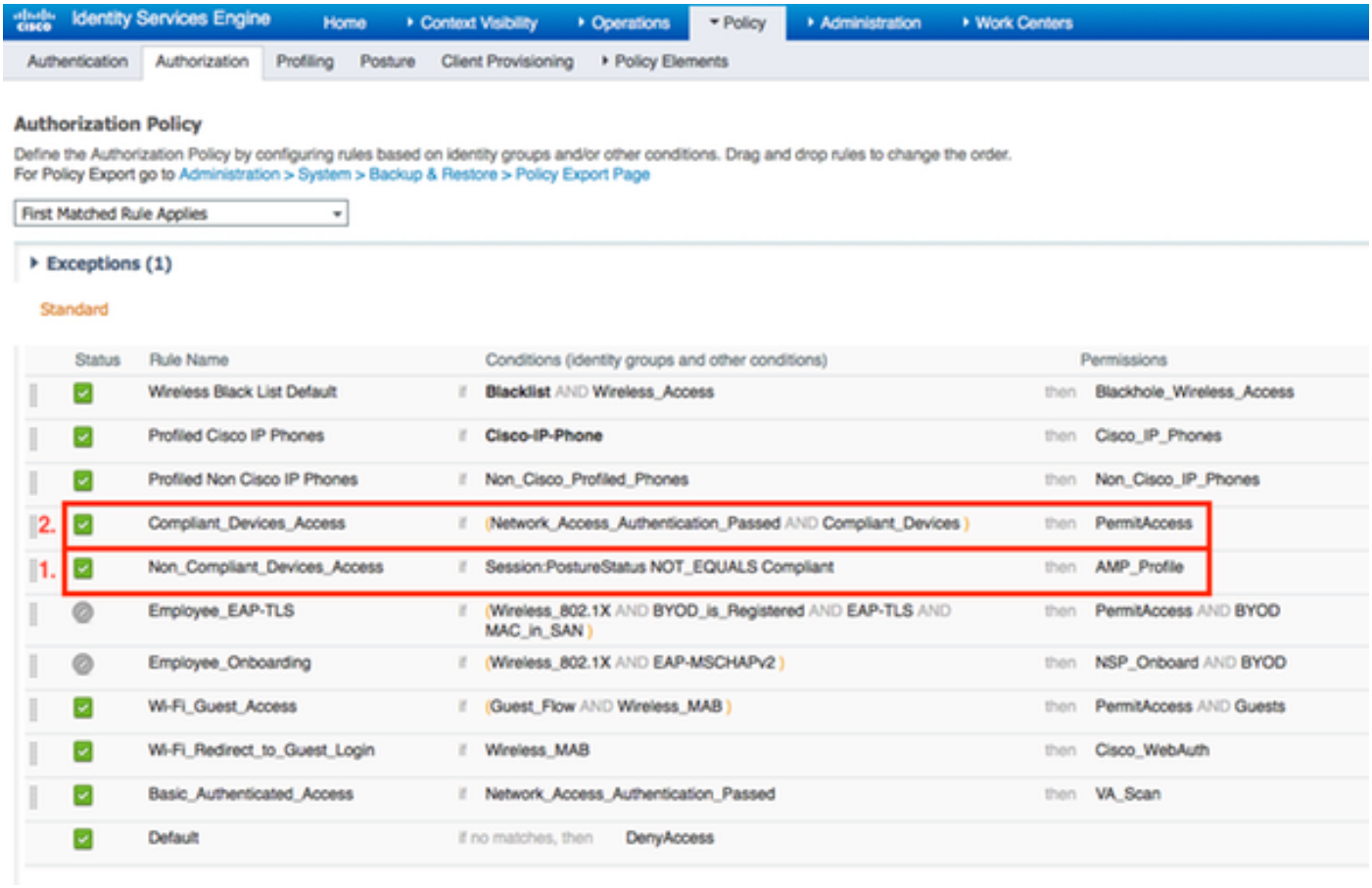


Etapa 6. Configurar políticas da autorização

Primeiramente a reorientação ao portal do abastecimento do cliente ocorre. As políticas padrão da autorização para a postura são usadas.

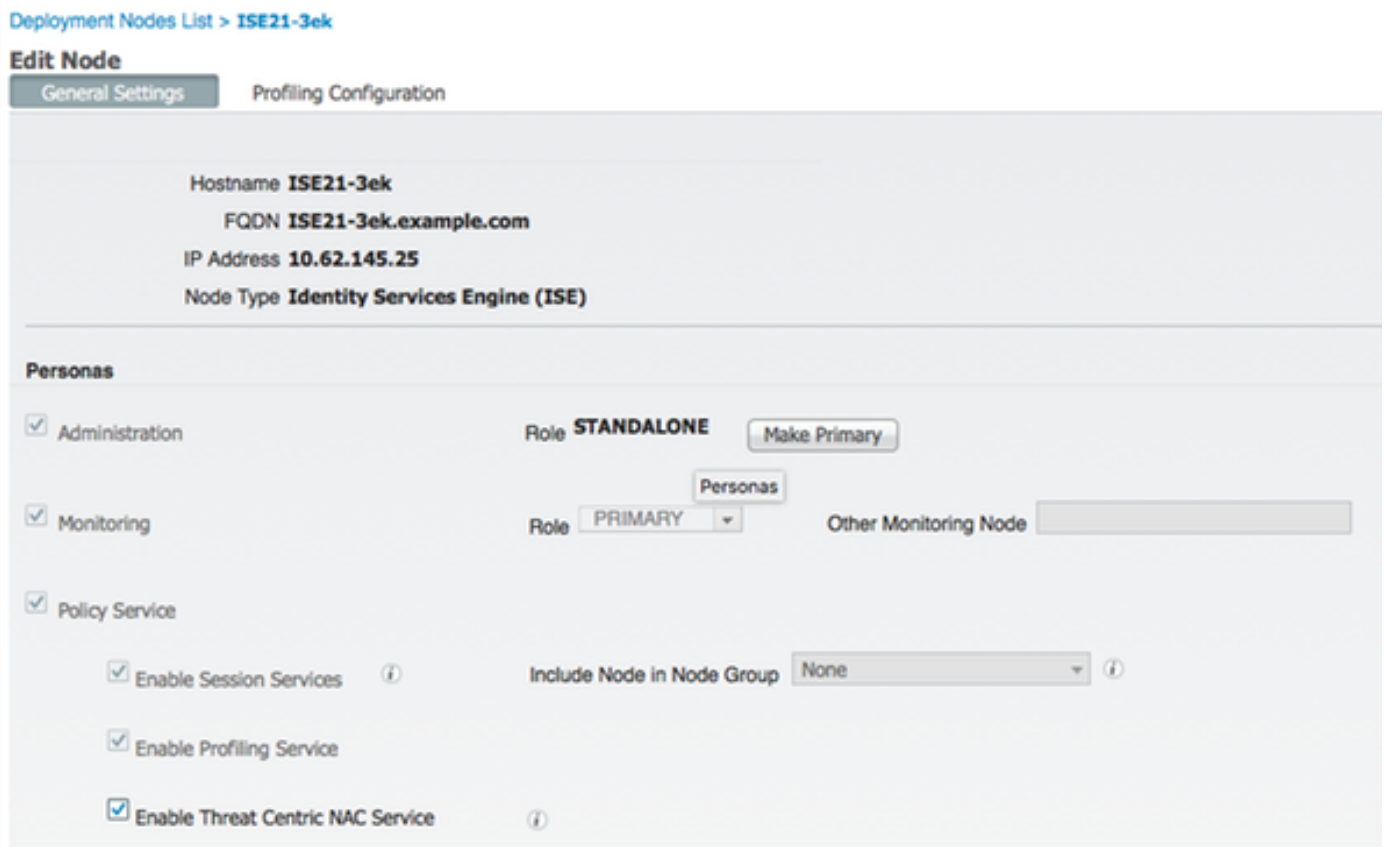


Mais tarde, uma vez que complacente, o acesso direto é atribuído



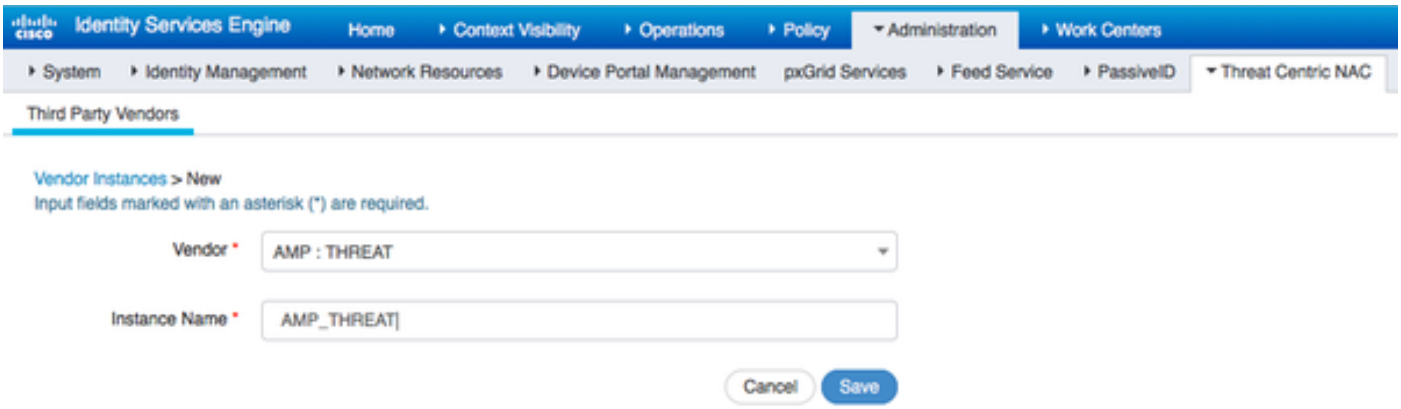
Etapa 7. Permita serviços TC-NAC

Permita serviços TC-NAC sob a administração > o desenvolvimento > editam o nó. A verificação **permite a** caixa de seleção **céntrica do serviço da ameaça NAC**.

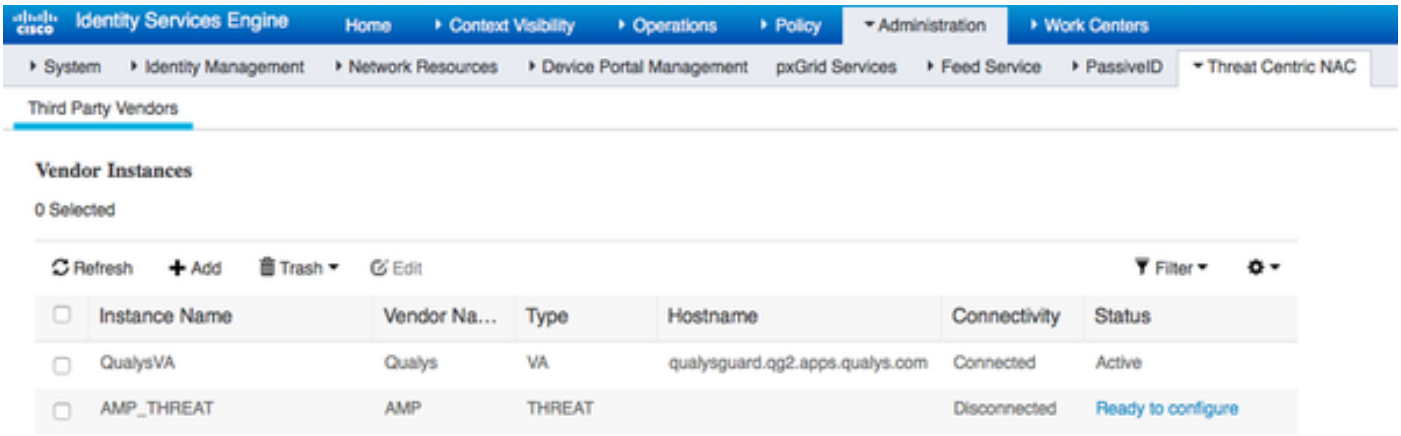


Etapa 8. Configurar o adaptador AMP

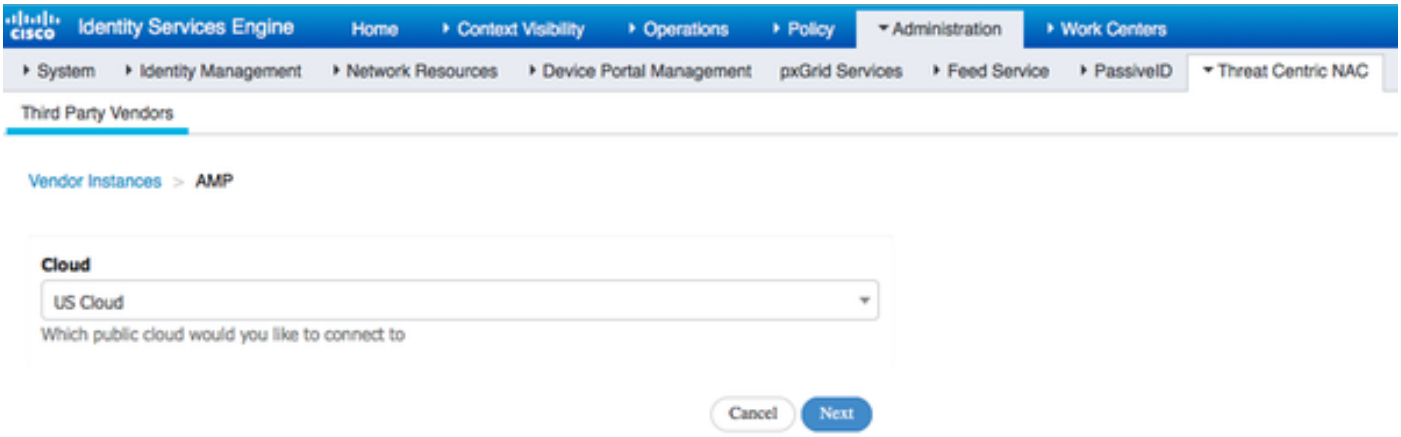
Navegue à administração > à ameaça céntricas NAC > > Add dos fornecedores de terceira parte. Clique sobre a **salvaguarda**



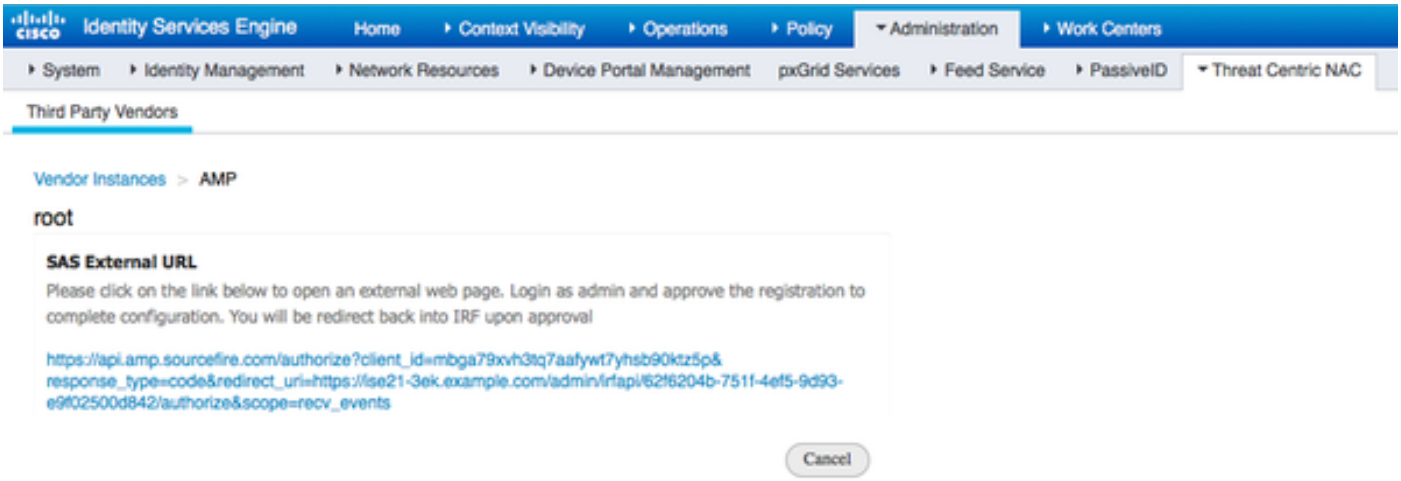
Deve transição **aprontar-se para configurar o** estado. Clique sobre **pronto para configurar**



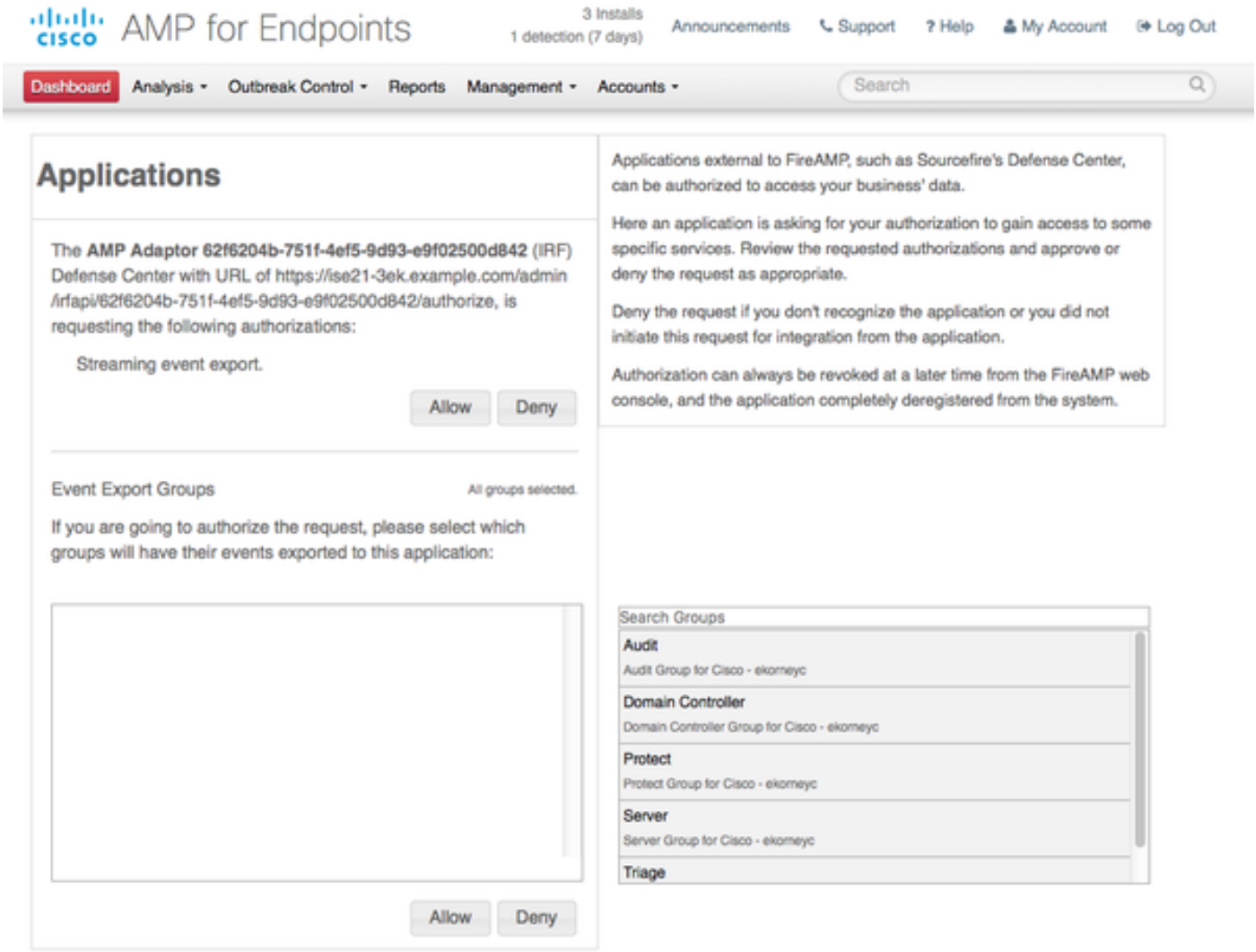
Selecione a **nuvem** e clique-a sobre **em seguida**



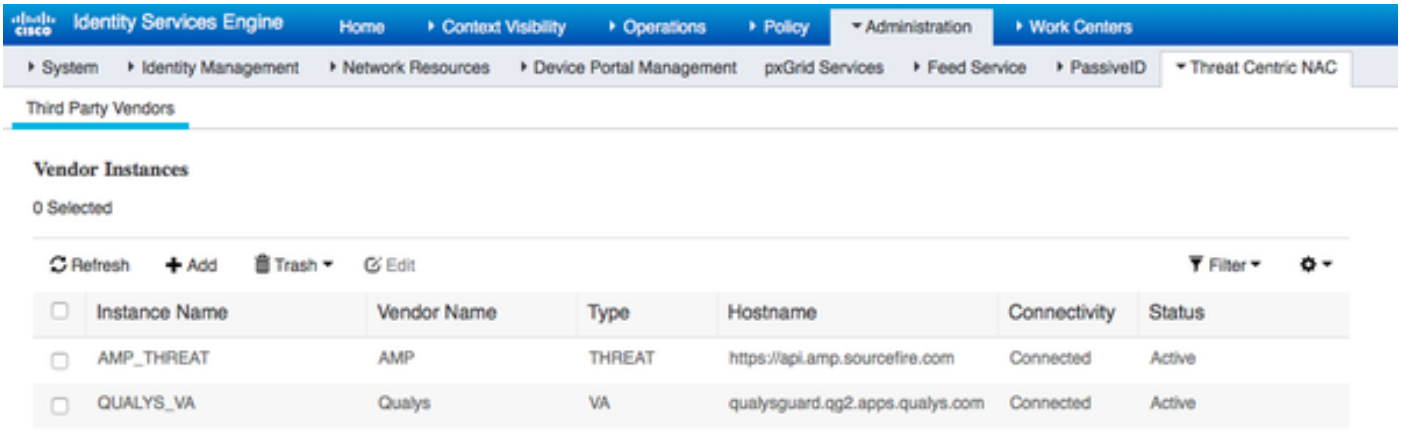
Clique a relação e o início de uma sessão de FireAMP como o admin em FireAMP.



O clique **permite no** painel dos **aplicativos** de autorizar o pedido de fluência da exportação do evento. Em seguida essa ação, você é reorientado de volta a Cisco ISE



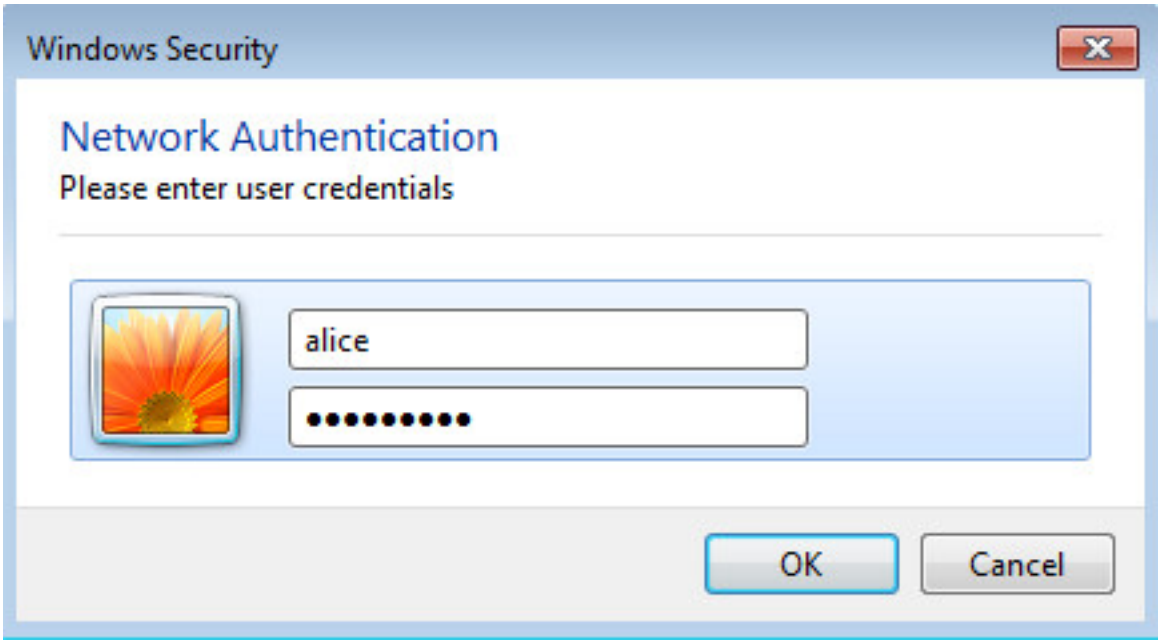
Selecione os eventos (por exemplo, transferência suspeito, conexão ao domínio suspeito, malware executado, acordo das Javas) esses você gostaria de monitorar. O sumário da configuração do exemplo do adaptador é indicado na página de sumário de configuração. Transições do exemplo do adaptador estado conectado/ativo.



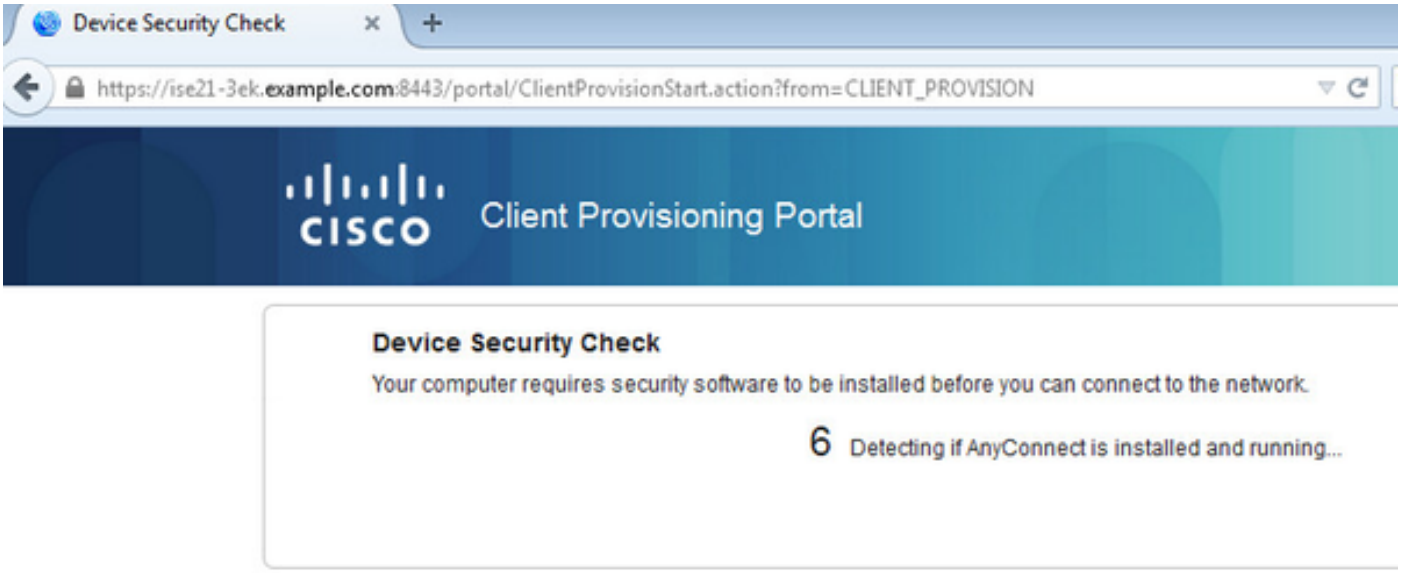
Verificar

Valor-limite

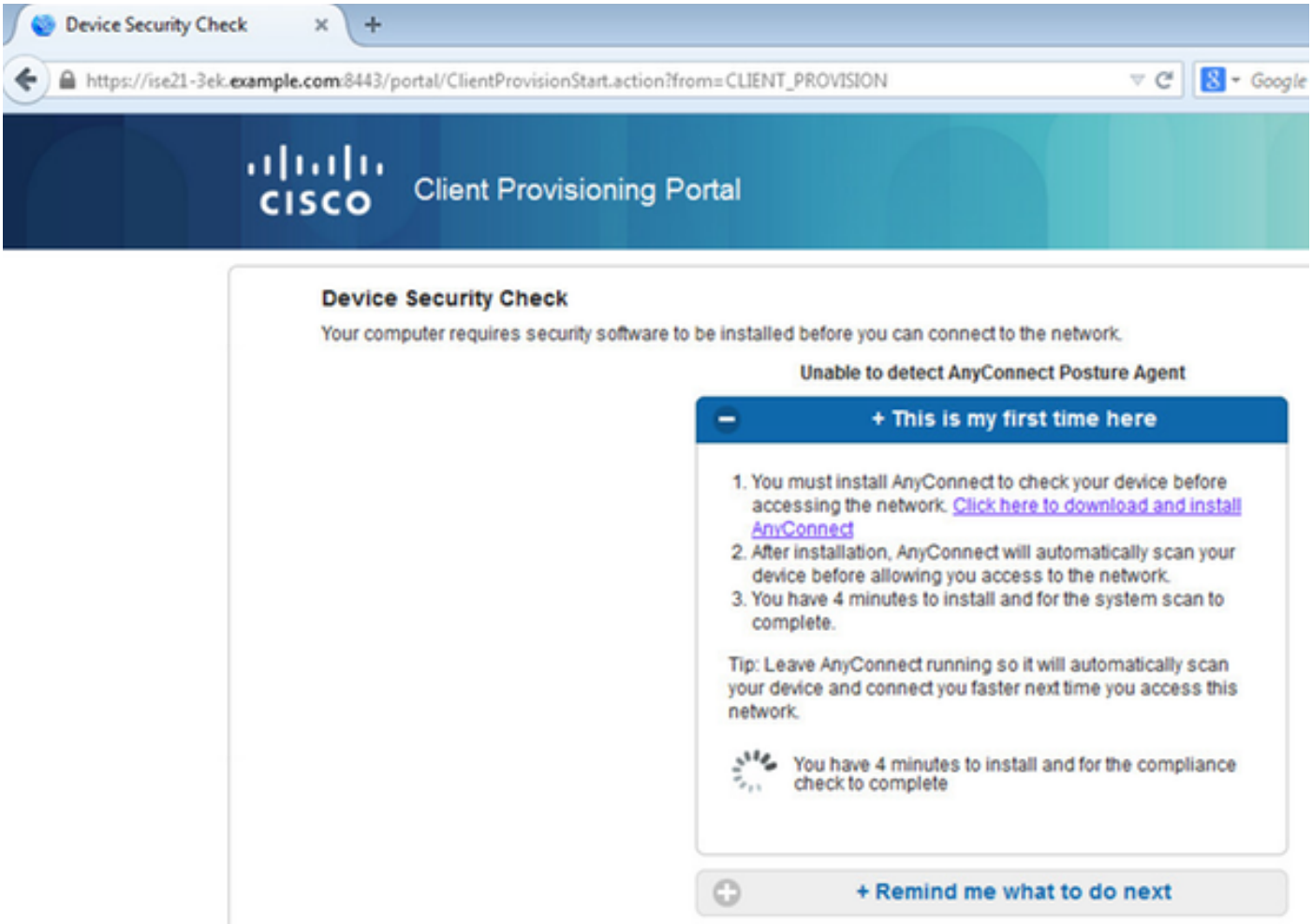
Conecte à rede Wireless através de PEAP (MSCHAPv2).



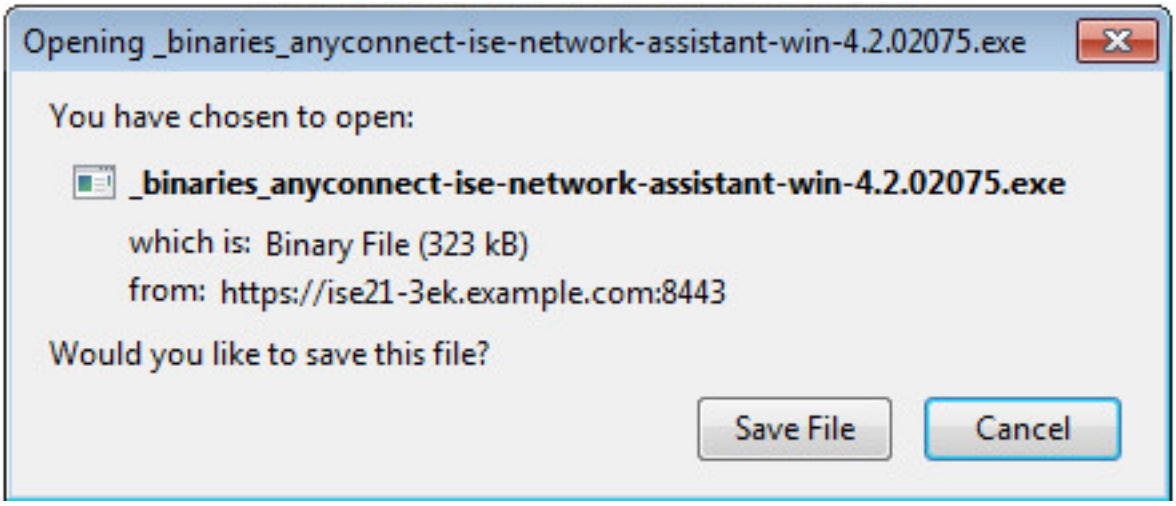
Uma vez que conectado a reorientação ao portal do abastecimento do cliente ocorre.



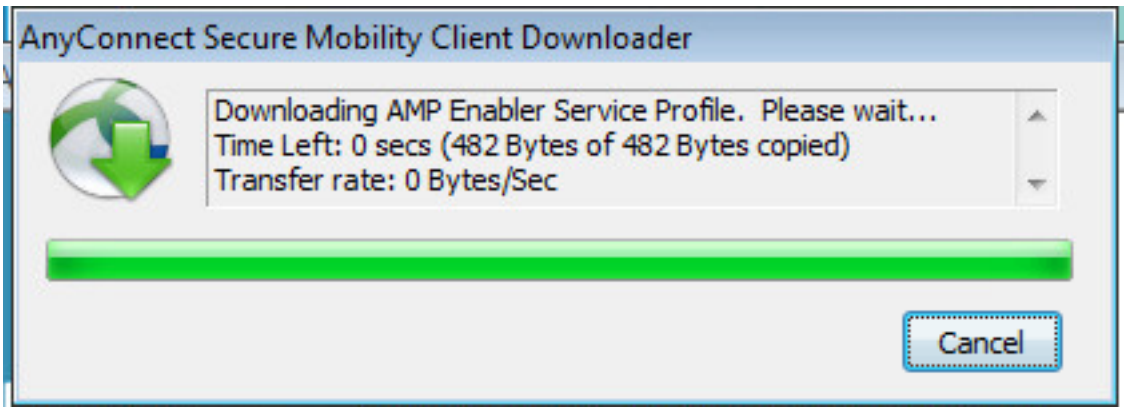
Desde que não há nada instalado na máquina cliente, o ISE alerta para a instalação de cliente de AnyConnect.

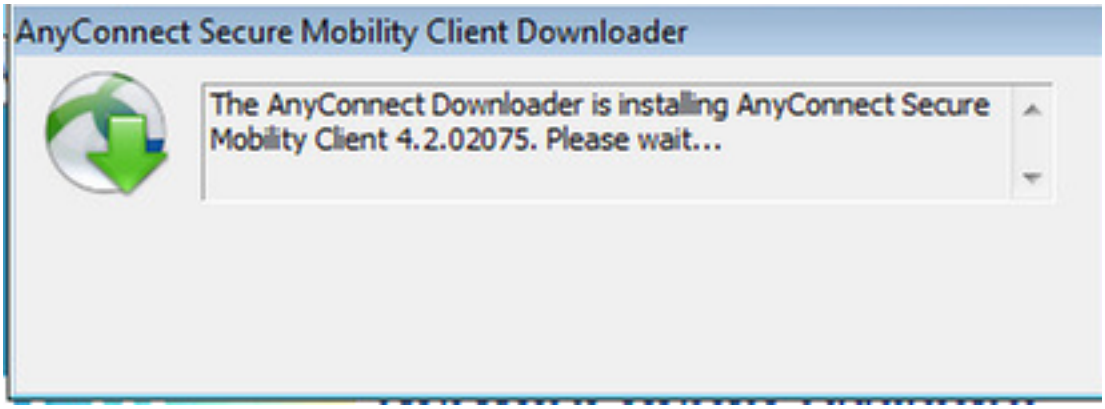


O aplicativo assistente da instalação de rede (NSA) deve ser transferido e corrida da máquina cliente.

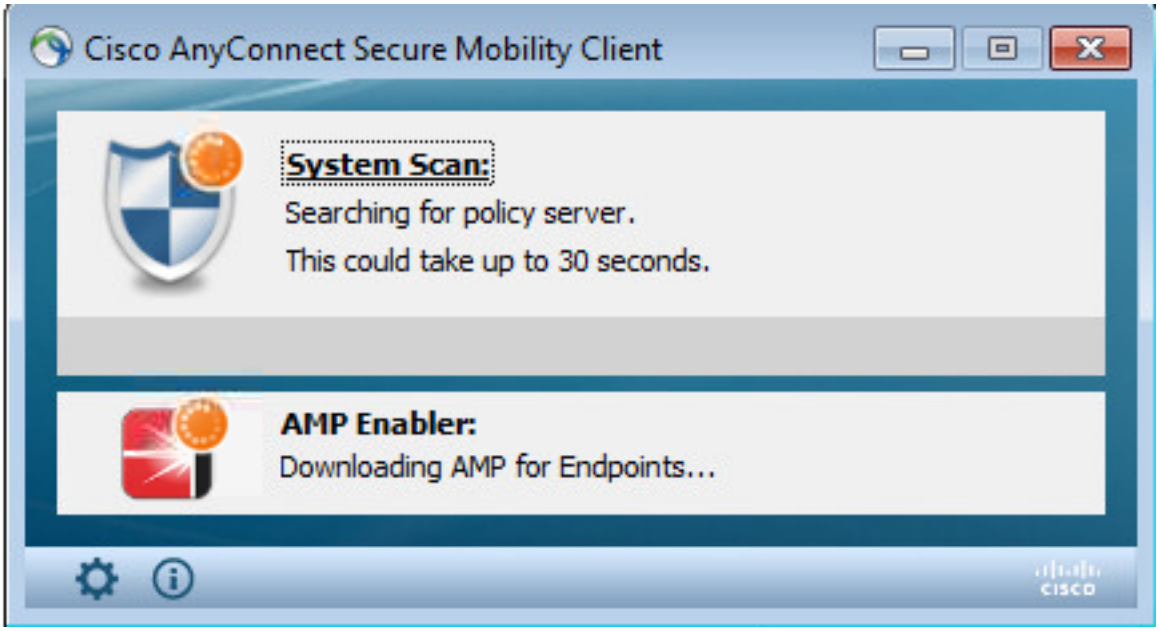


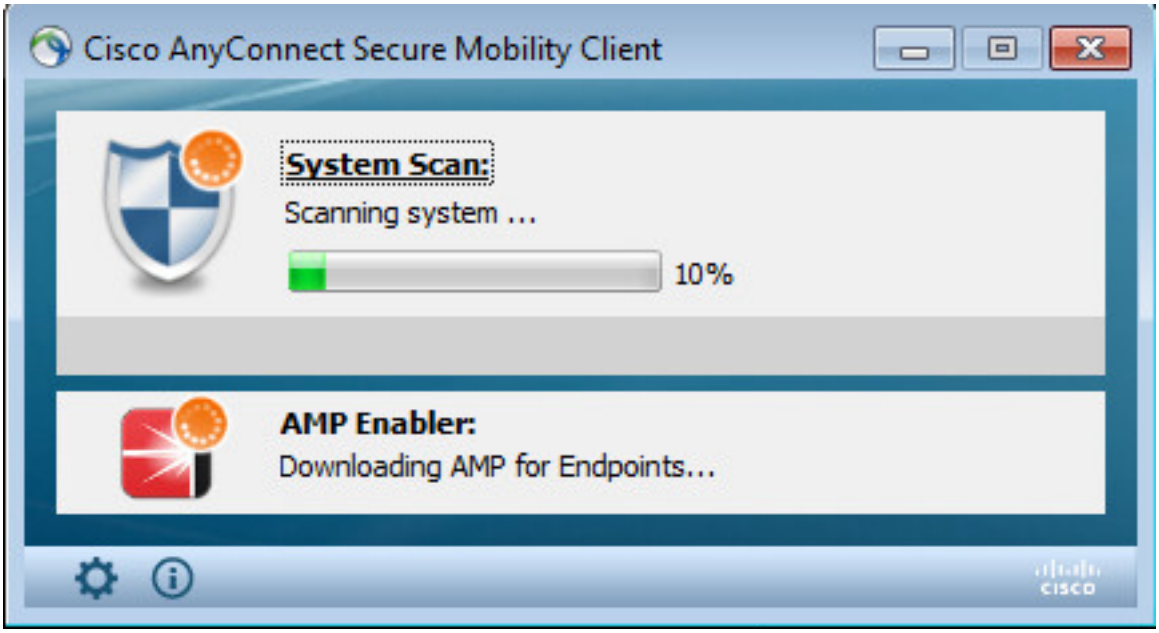
O NSA toma de instalar componentes requeridos e perfis.



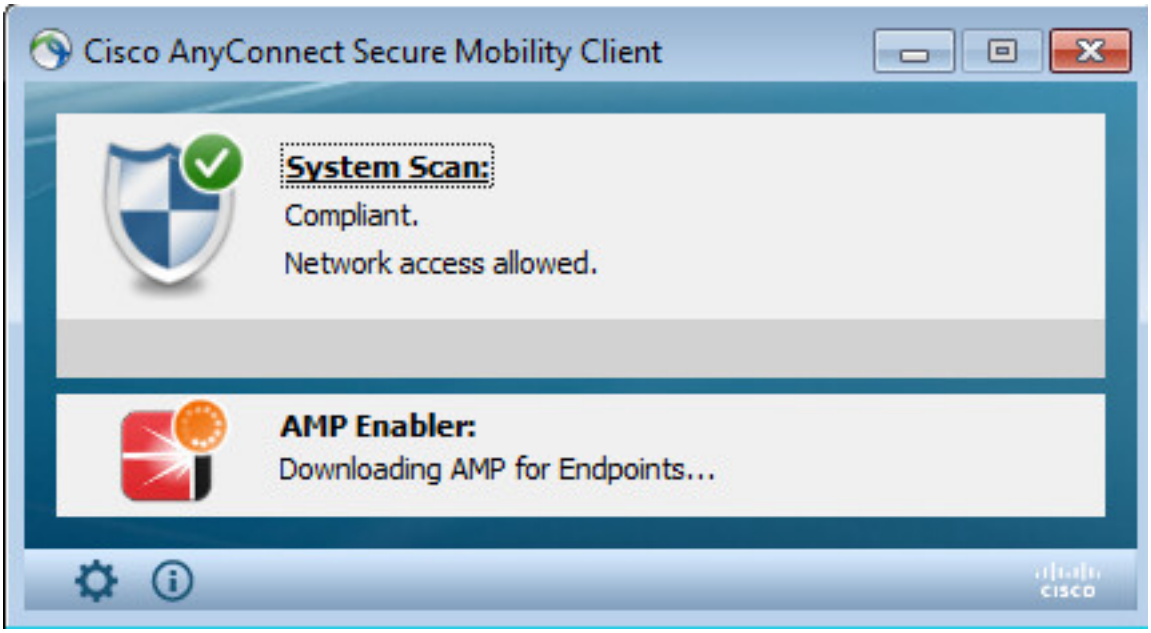


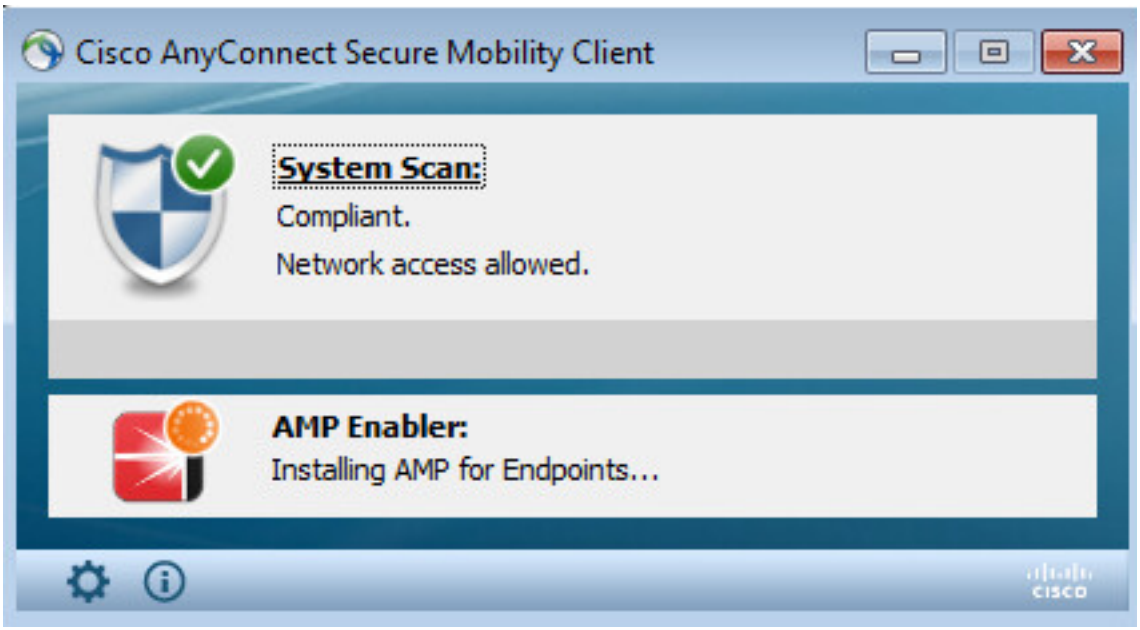
Uma vez que a instalação é terminada, o módulo da postura de AnyConnect executa a verificação da conformidade.

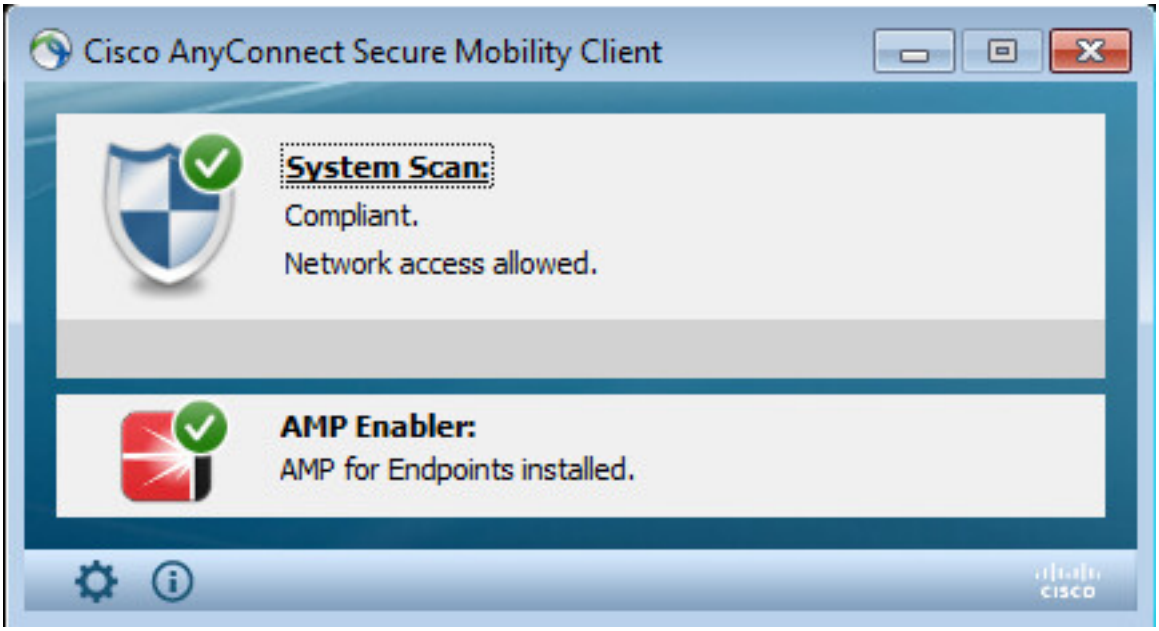




Porque o acesso direto está dado, se o valor-limite é complacente, o AMP está transferido e instalado do web server especificado mais cedo no perfil AMP.

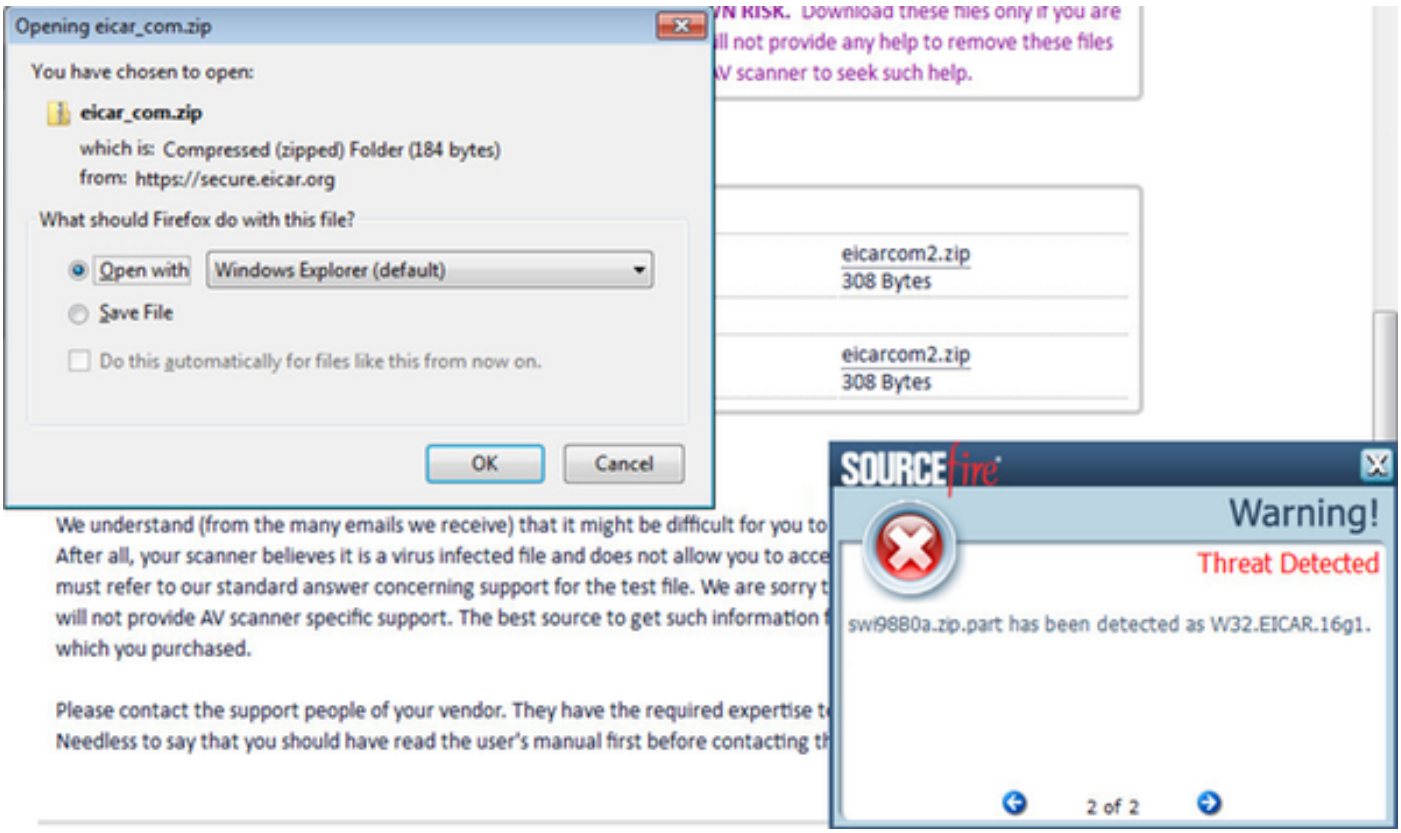






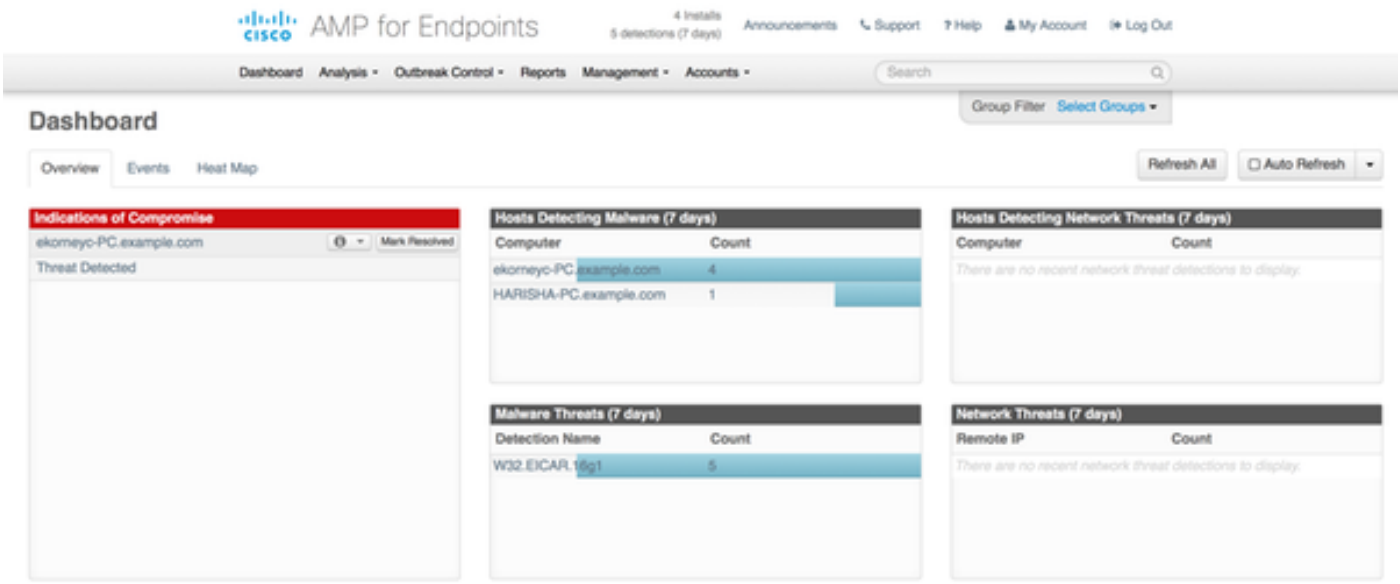
O conector AMP aparece.

Para testar o AMP na ação a corda de Eicar contida em um arquivo zip é transferida. A ameaça é detectada, e relatada à nuvem AMP.

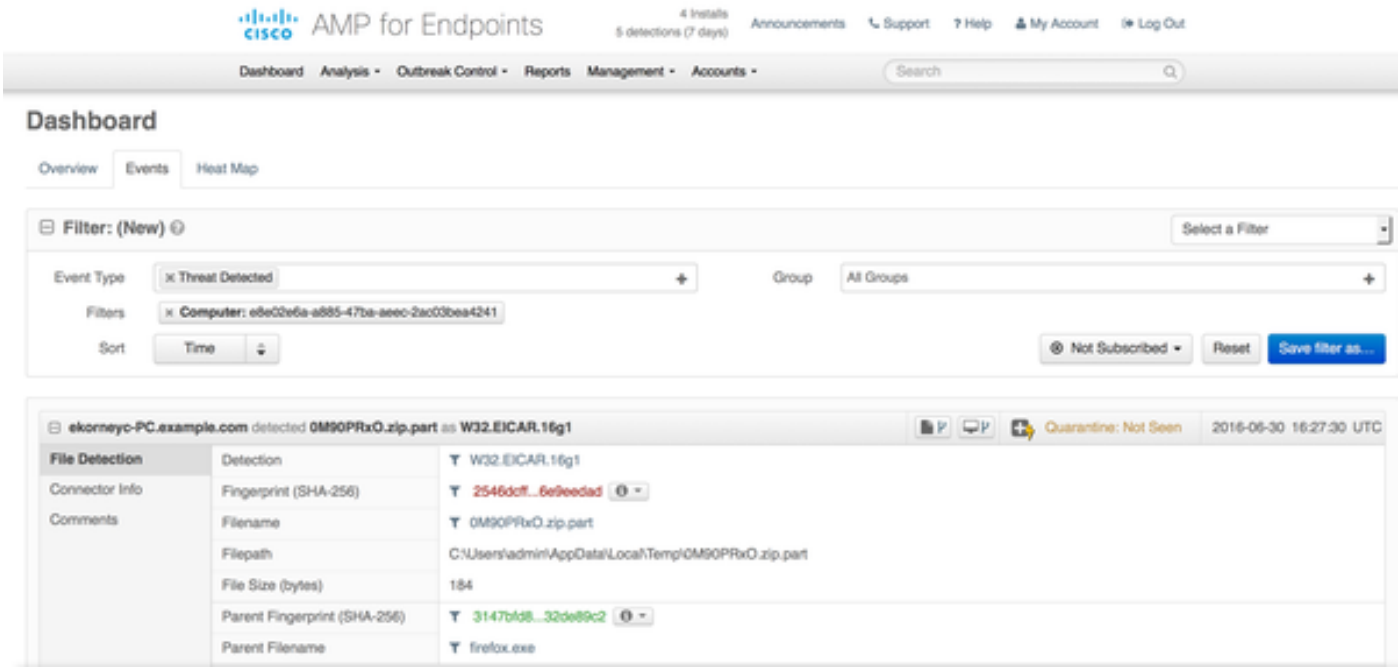


Nuvem AMP

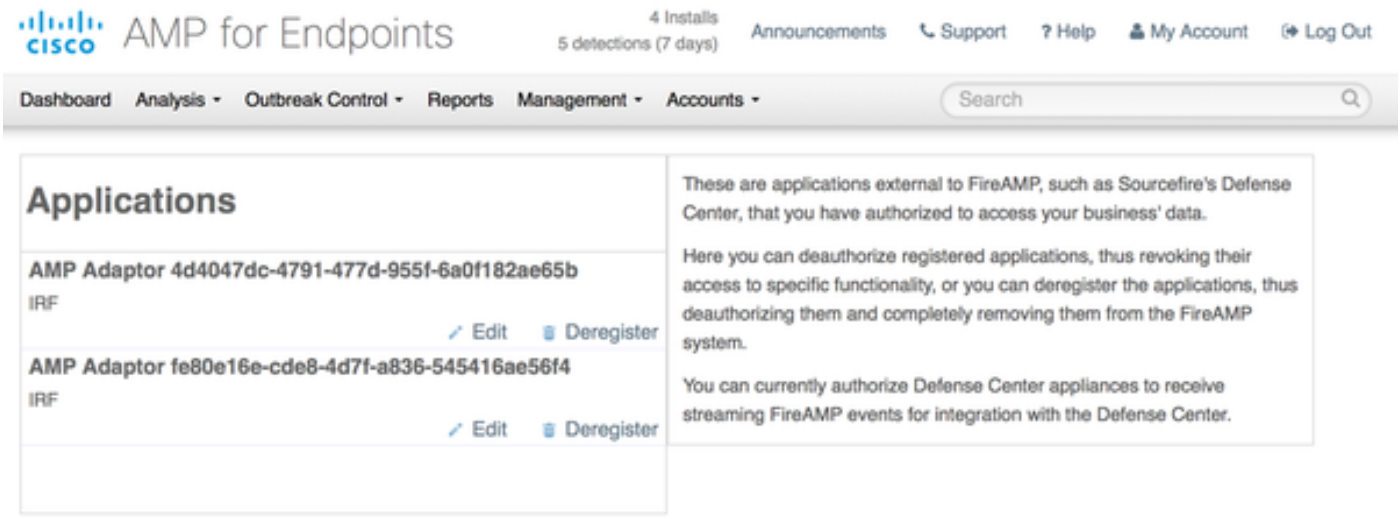
Para verificar os detalhes do painel da ameaça da nuvem AMP pode ser usada.



A fim obter mais detalhes sobre a ameaça, caminho do arquivo e fingerpints, você pode clicar sobre o host, onde o malware foi detectado.

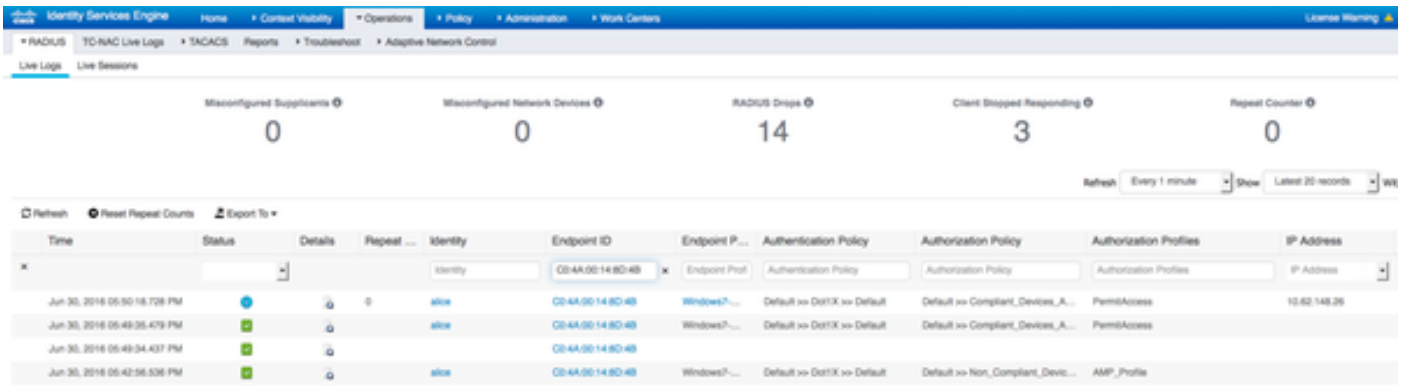


Para ver ou exemplo do desfazer/cancelar registro do ISE que você pode navegar às contas > aos aplicativos

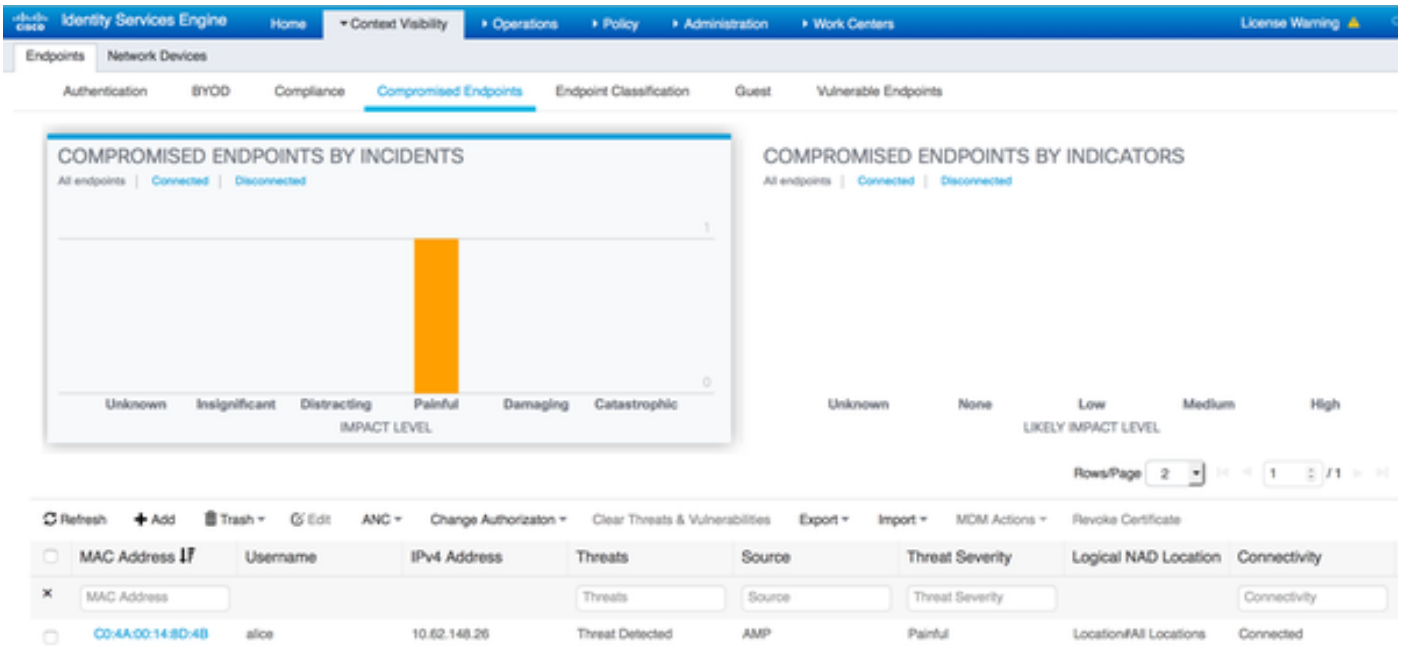


ISE

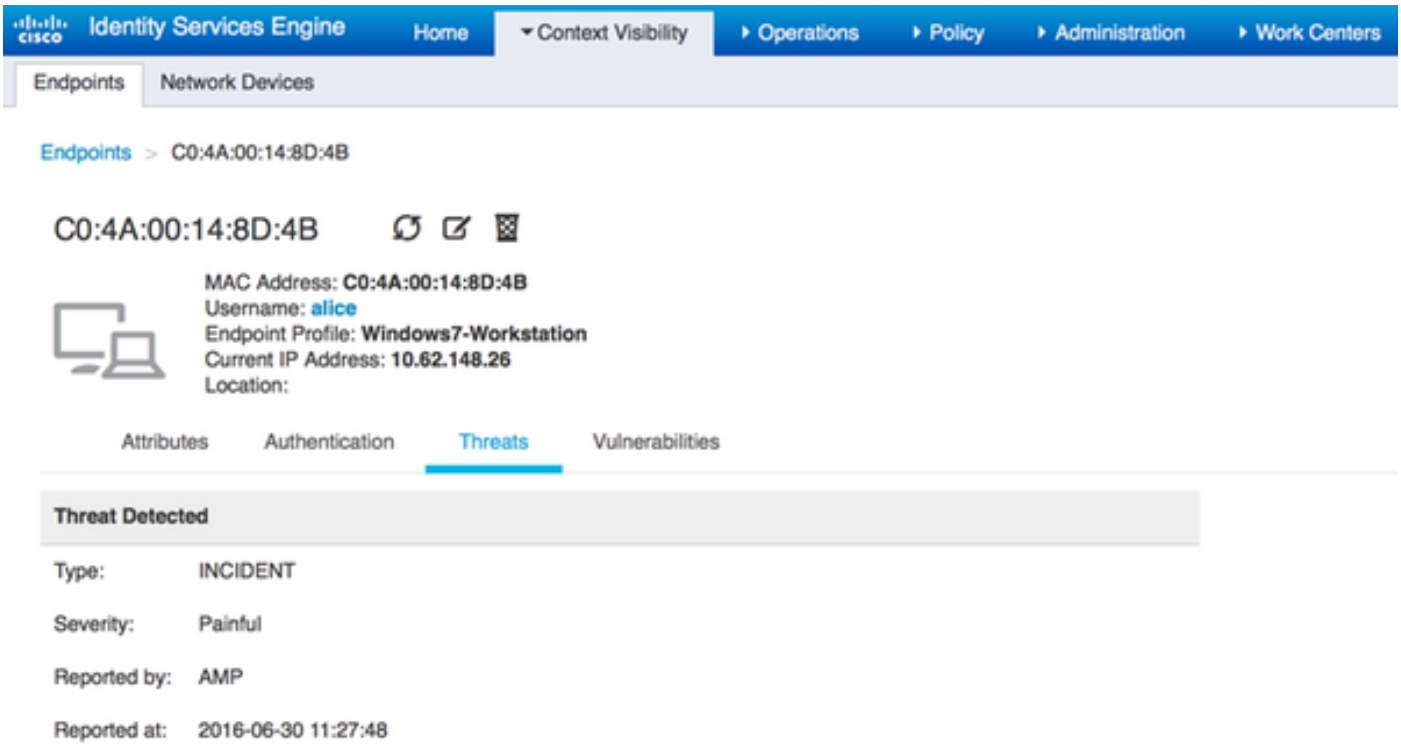
Em ISE que próprio o fluxo regular da postura é considerado, reorientação ocorre primeiramente para verificar a conformidade da rede. Assim que o valor-limite for complacente, o CoA Reauth está enviado e o perfil novo com PermitAccess é atribuído.



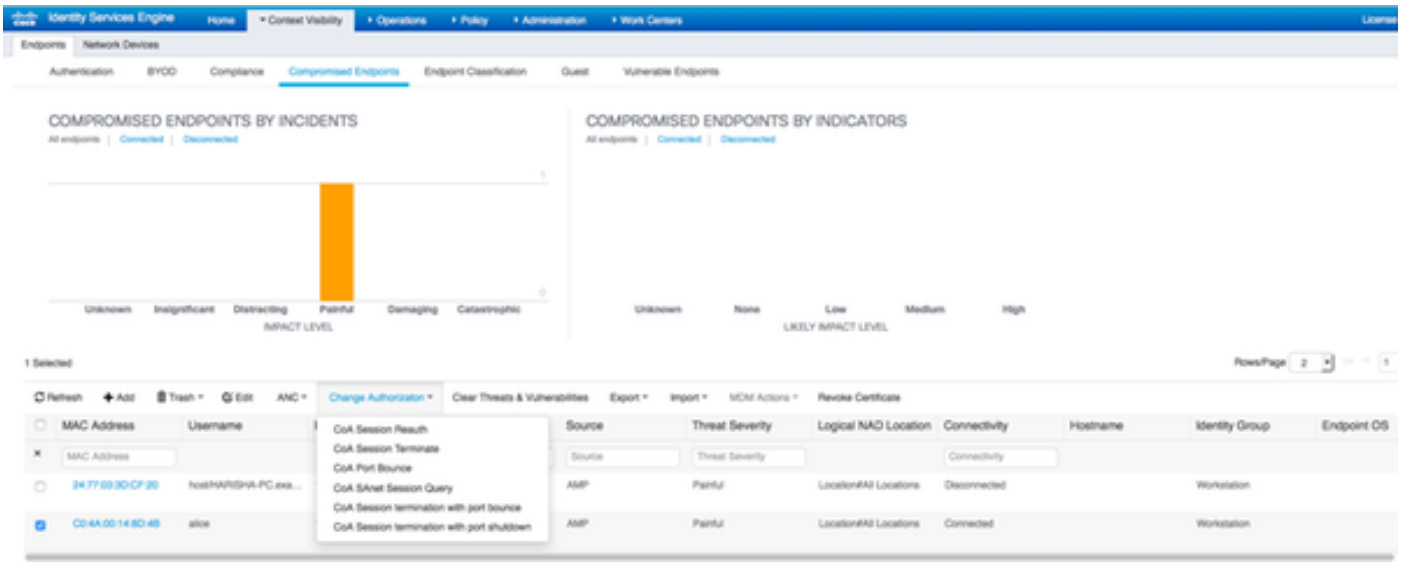
Para ver as ameaças que detectadas você pode navegar à visibilidade > aos valores-limite do contexto > valores-limite comprometidos



Se você seleciona o valor-limite e navega à aba da ameaça, mais detalhes estão indicados.



Quando um evento de ameaça é detectado para um valor-limite, você pode selecionar o MAC address do valor-limite na página comprometida dos valores-limite e aplicar uma política ANC (se configurado, por exemplo quarentena). Alternativamente você pode emitir a mudança da autorização terminar a sessão.



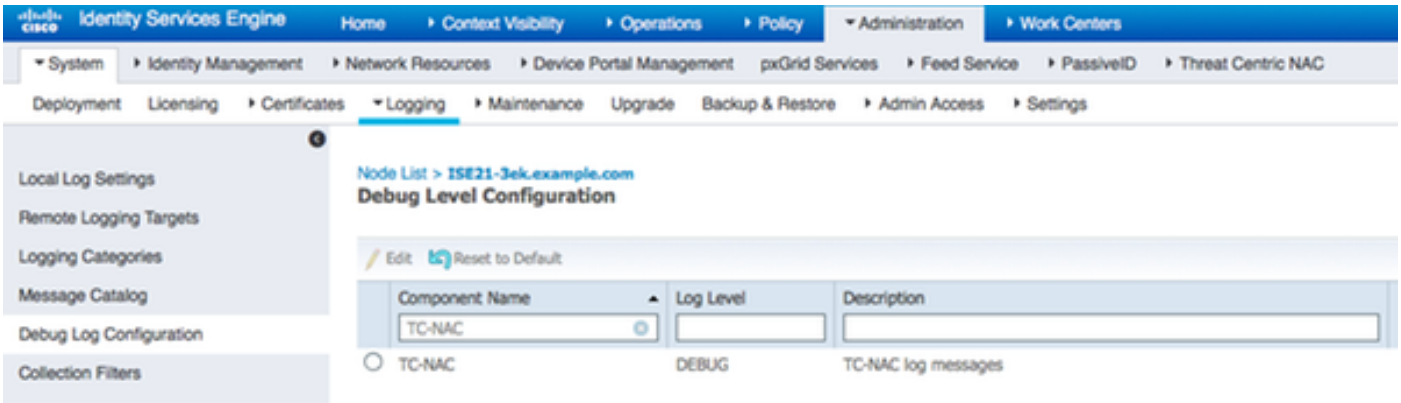
Se a sessão Terminate CoA é selecionada, o ISE envia a disconexão CoA e o cliente perde o acesso à rede.

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

A fim permitir debuga no ISE navegam à administração > ao sistema > registrando > debugam a configuração do log, nó seleto TC-NAC e mudam o **log em nível do** componente TC-NAC **PARA DEBUGAR**



Logs a ser verificados - irf.log. Você pode atá-lo diretamente de ISE CLI:

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

A ameaça mesmo é recebida da nuvem AMP

2016-06-30 18:27:48,617 DEBUGAM [IRF-AMQP-Dispatcher-Notification-0][] cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:53 -:::: :- chamando a mensagem do alimentador com.cisco.cpm.irf.service.IrfNotificationHandler$MyNotificationHandler@3fac8043 da notificação {messageType=NOTIFICATION, messageId=THREAT_EVENT, content= {“**c0:4a:00:14:8d:4b**": [{“incidente”: {“Impact_Qualification”: “Doloroso”}, “marcador temporal”: 1467304068599, “vendedor”: “AMP”, “título”: “**Ameaça detectada**”}]} ', priority=0, timestamp=Thu o 30 de junho 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 18:27:48,617 DEBUGAM [IRF-AMQP-Dispatcher-Notification-0][] cisco.cpm.irf.service.IrfNotificationHandler:handle:140 -:::: :- adicionado à fila pendente: Mensagem {messageType=NOTIFICATION, messageId=THREAT_EVENT, content= {“**c0:4a:00:14:8d:4b**": [{“incidente”: {“Impact_Qualification”: “**Doloroso**”}, “marcador temporal”: 1467304068599, “vendedor”: “**AMP**”, “título”: “Ameaça detectada”}]} ', priority=0, timestamp=Thu o 30 de junho 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 18:27:48,617 DEBUGAM [IRF-AMQP-Dispatcher-Notification-0][] cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:59 -:::: :- FEITO processando a notificação: #contentHeader<basic> Envelope(deliveryTag=79, de 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 18:27:48,706 DEBUGAM [IRF-EventProcessor-0][] cisco.cpm.irf.service.IrfEventProcessor:parseNotification:221 -:::: :- notificação da análise gramatical: Mensagem {messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b": [{“incidente”: {“Impact_Qualification”: “Doloroso”}, “marcador temporal”: 1467304068599, “vendedor”: “AMP”, “título”: “Ameaça detectada”}]} ', priority=0, timestamp=Thu o 30 de junho 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)}

A informação sobre a ameaça é enviada PARA FILTRAR

2016-06-30 18:27:48,724 DEBUGAM [IRF-EventProcessor-0][] cisco.cpm.irf.service.IrfEventProcessor:storeEventsInES:366 -:::: :- **adicionando a informação de evento de ameaça para enviar PARA FILTRAR** - **c0:4a:00:14:8d:4b** {incident= {Impact_Qualification=Painful}, time-stamp=1467304068599, vendor=AMP, title=Threat detectados}