Configurazione di ISE 2.1 TC-NAC (Threat-Centric NAC) con AMP e servizi di postura

Sommario

Introduzione

In questo documento viene descritto come configurare un NAC basato sulle minacce con Advanced Malware Protection (AMP) su Identity Services Engine (ISE) 2.1. I livelli di gravità delle minacce e i risultati della valutazione della vulnerabilità possono essere utilizzati per controllare in modo dinamico il livello di accesso di un endpoint o di un utente. Come parte del presente documento, è anche trattata la questione dei servizi postali.

> **Nota:** Lo scopo del documento è descrivere l'integrazione di ISE 2.1 con AMP; i servizi di postura vengono mostrati come sono richiesti quando effettuiamo il provisioning di AMP da ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Cisco Identity Service Engine
- Advanced Malware Protection

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Service Engine versione 2.1
- Controller LAN wireless (WLC) 8.0.121.0
- AnyConnect VPN Client 4.2.02075
- Windows 7 Service Pack 1

Configurazione

Esempio di rete

Flusso dettagliato

1. Il client si connette alla rete, **AMP_Profile** viene assegnato e l'utente viene reindirizzato al portale di provisioning di Anyconnect. Se Anyconnect non viene rilevato sul computer, vengono installati tutti i moduli configurati (VPN, AMP, Posture). Push della configurazione per ogni modulo

insieme al profilo

2. Una volta installato Anyconnect, viene eseguita la valutazione della postura

3. Il modulo AMP Enabler installa il connettore FireAMP

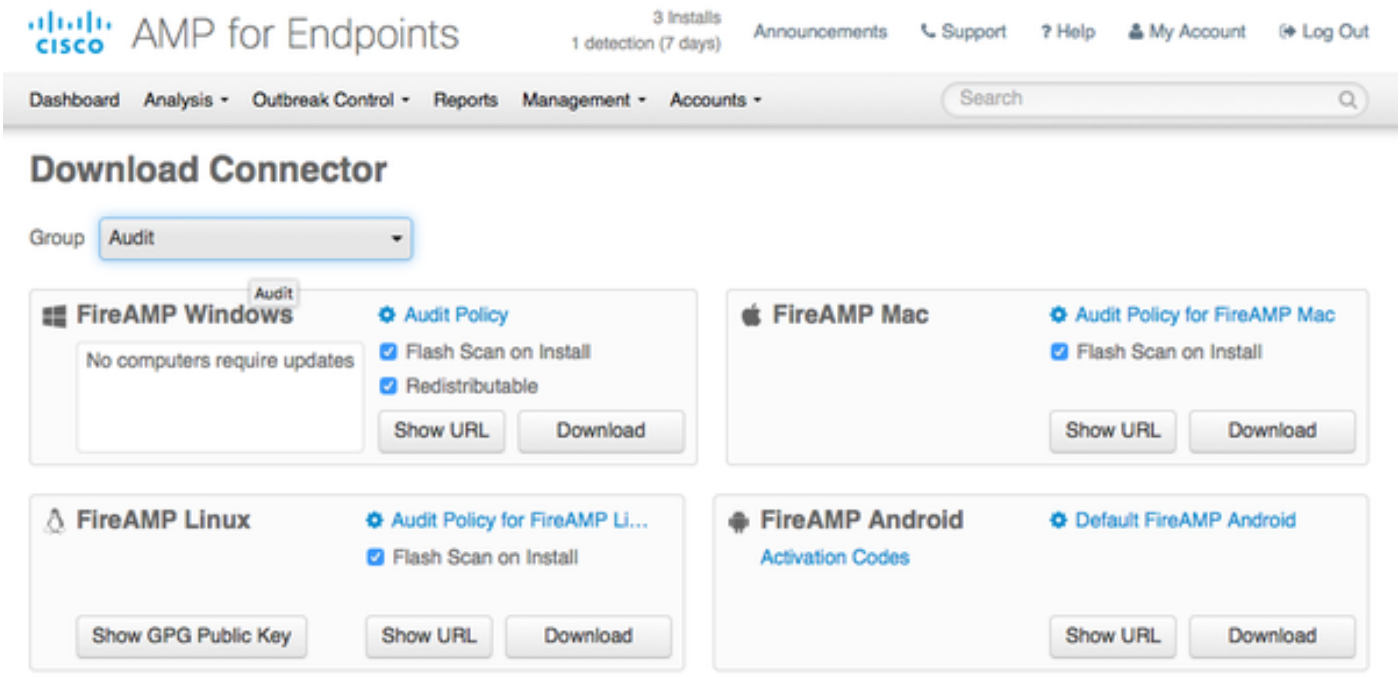
4. Quando il client tenta di scaricare software dannoso, AMP Connector genera un messaggio di avviso e lo segnala ad AMP Cloud

5. AMP Cloud invia queste informazioni ad ISE

Configurare AMP Cloud

Passaggio 1. Scaricare il connettore da AMP Cloud

Per scaricare il connettore, selezionare Gestione > Scarica connettore. Quindi selezionare type and **Download** FireAMP (Windows, Android, Mac, Linux). In questo caso è stato selezionato **Audit** e il file di installazione di FireAMP for Windows.

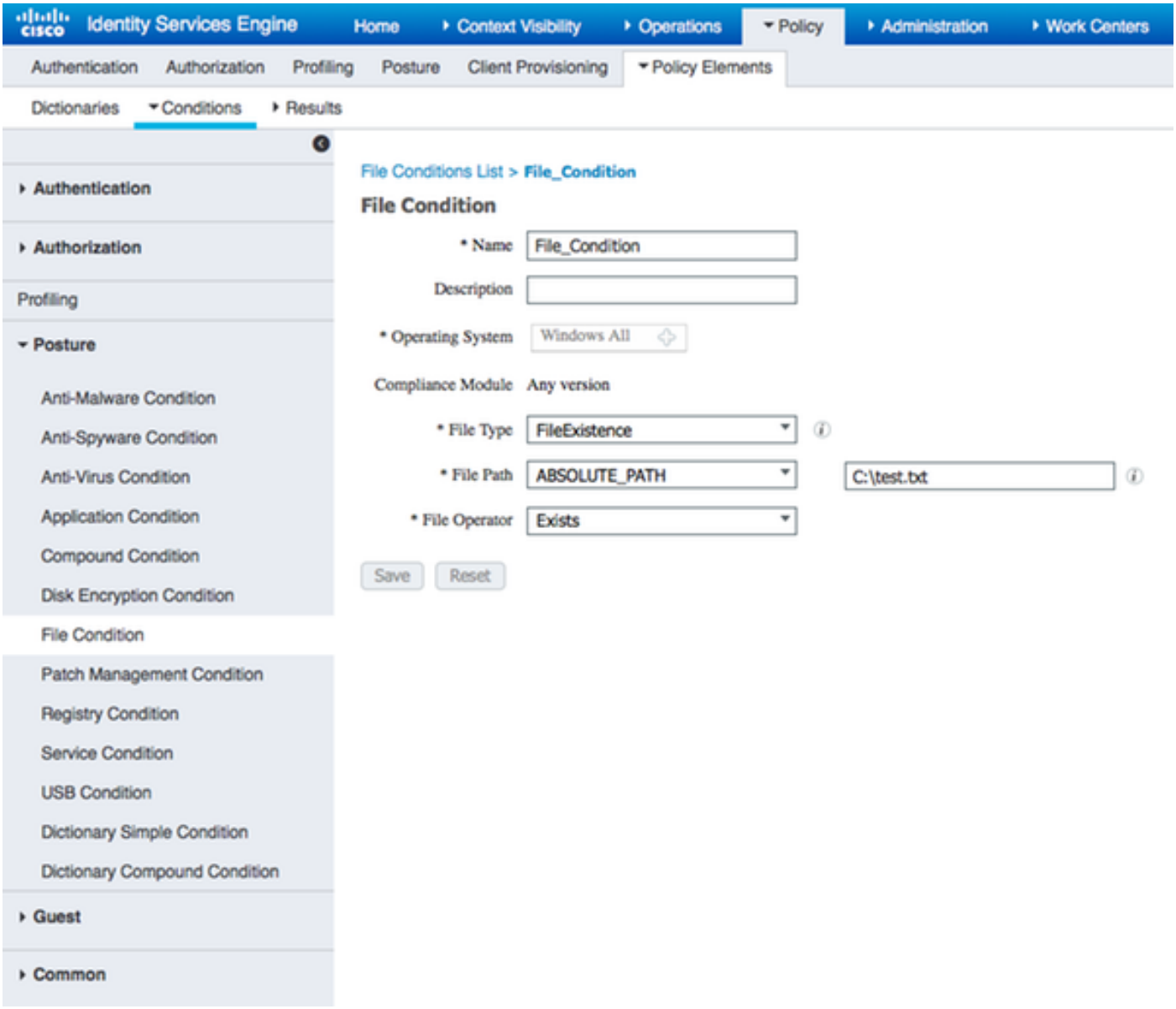


> **Nota:** Il download di questo file genera un file con estensione exe denominato **Audit_FireAMPSetup.exe** nell'esempio. Il file è stato inviato al server Web per essere disponibile quando l'utente richiede la configurazione di AMP.

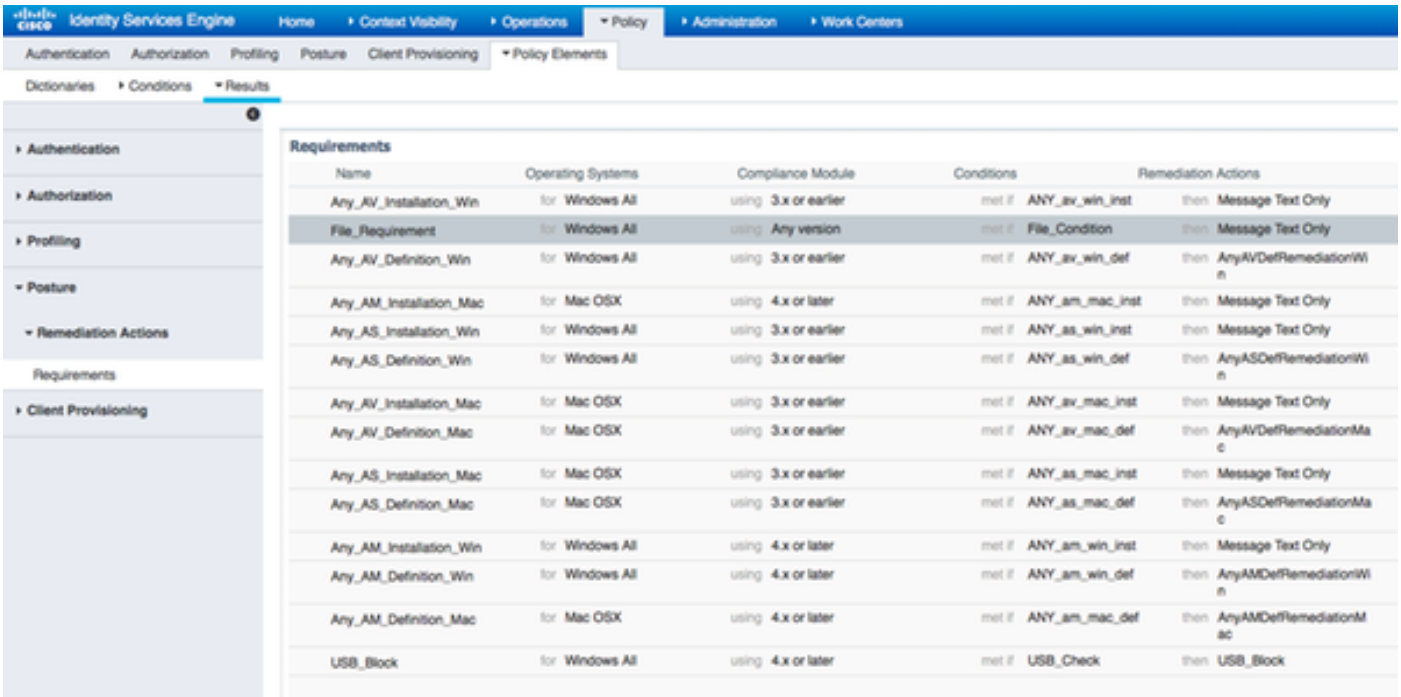
Configurare ISE

Passaggio 1. Configurare criteri e condizioni di postura

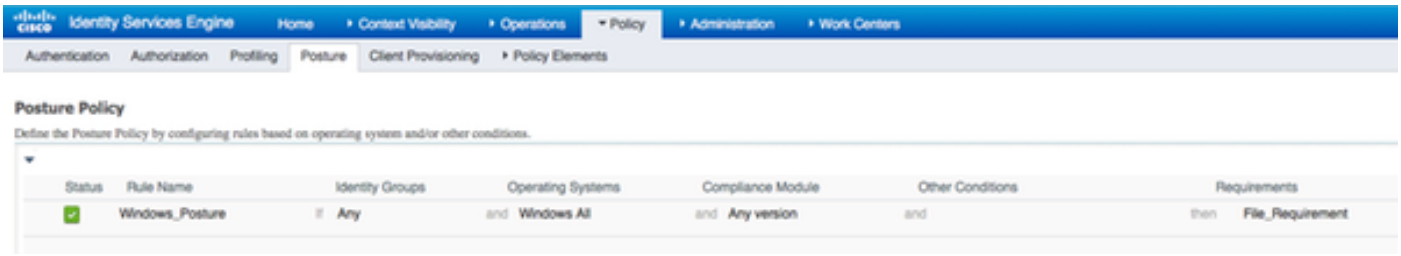
Passare a Criterio > Elementi criterio > Condizioni > Postura > Condizione file.È possibile notare che è stata creata una semplice condizione per l'esistenza del file. Il file deve esistere se l'endpoint deve essere conforme ai criteri verificati dal modulo Posture:



Questa condizione viene utilizzata per un requisito:

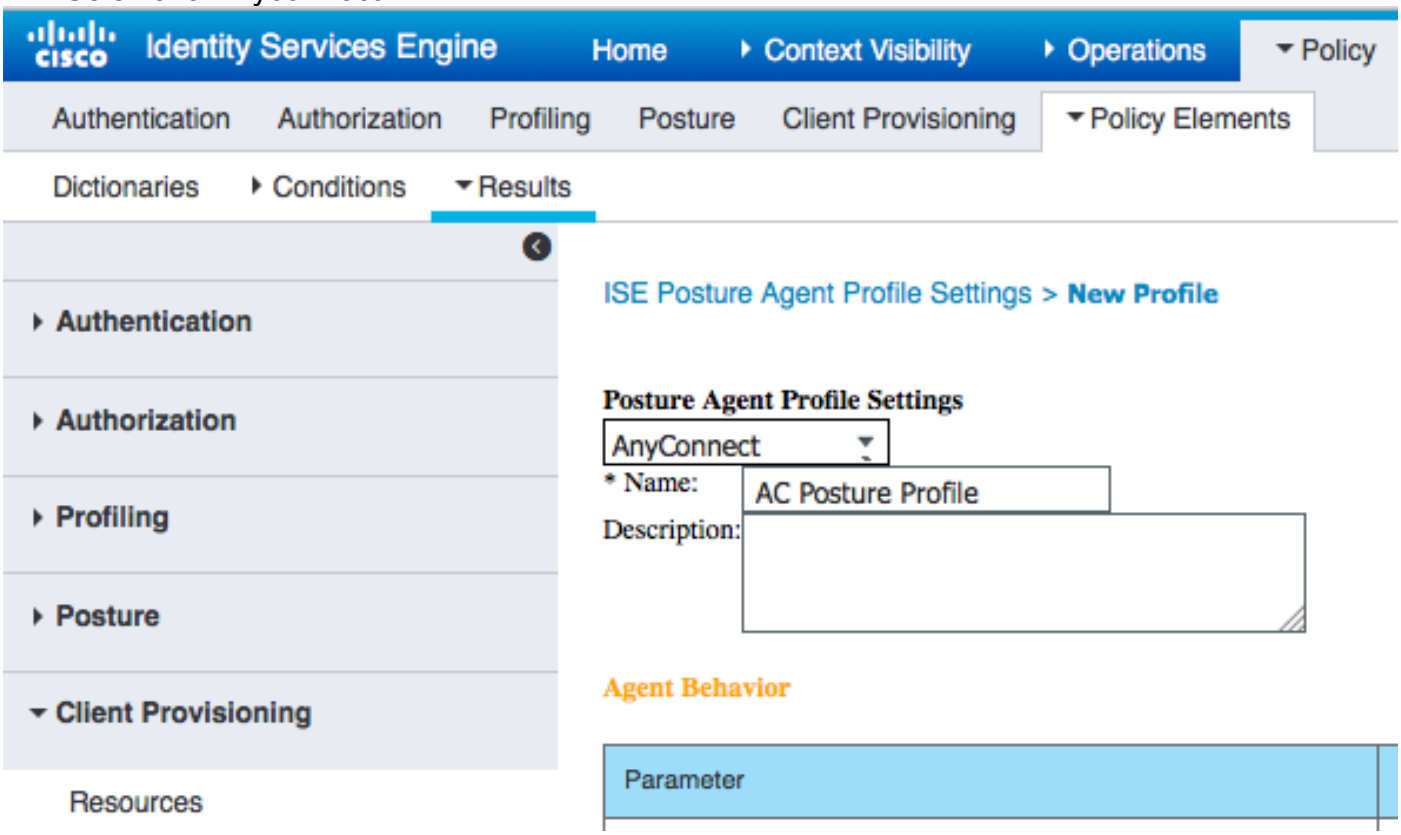


Il requisito è utilizzato nei criteri di postura per i sistemi Microsoft Windows:

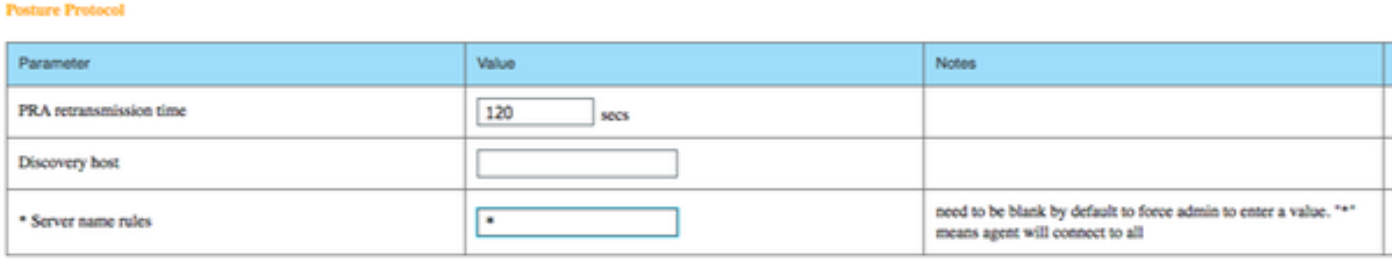


Passaggio 2. Configurare il profilo della postura

- Selezionare Policy > Elementi della policy > Risultati > Client Provisioning > Risorse e aggiungere l'agente Network Admission Control (NAC) o il profilo di postura dell'agente AnyConnect
- Seleziona Anyconnect



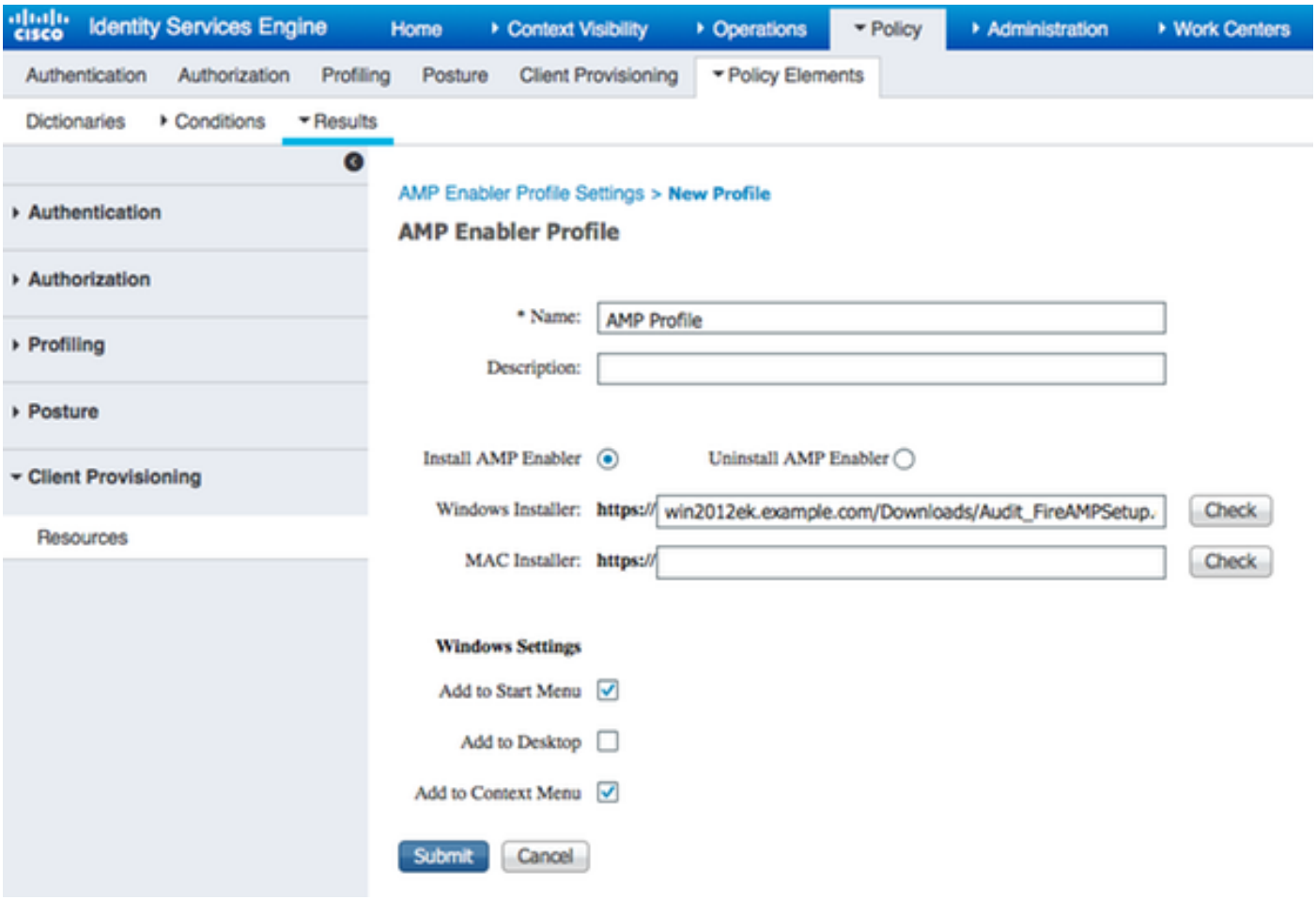
- Dalla sezione Posture Protocol aggiungere * per consentire all'agente di connettersi a tutti i server



Passaggio 3. Configurare il profilo AMP

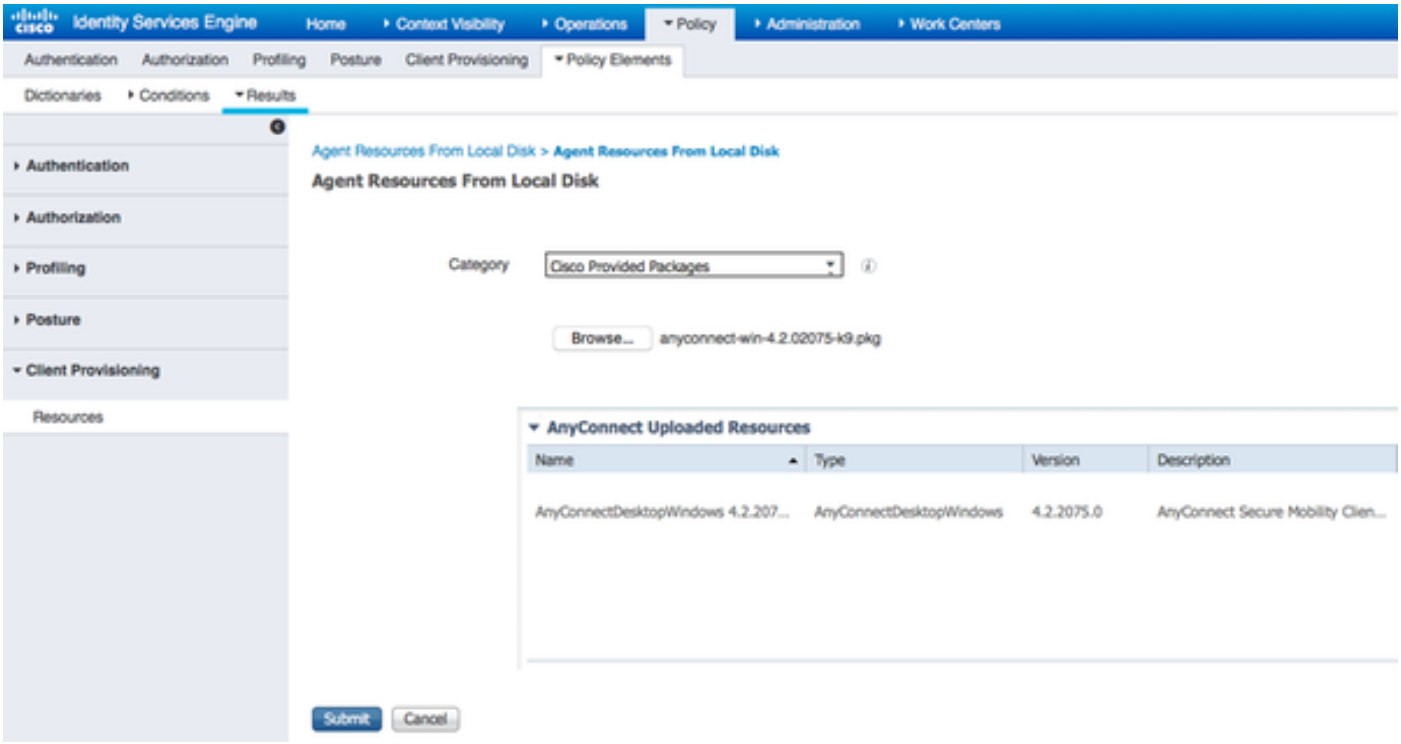
Profilo AMP contiene informazioni sulla posizione di Windows Installer. Windows Installer è stato

scaricato in precedenza da AMP Cloud. Deve essere accessibile dal computer client. Il certificato del server HTTPS in cui si trova il programma di installazione deve essere considerato attendibile anche dal computer client.

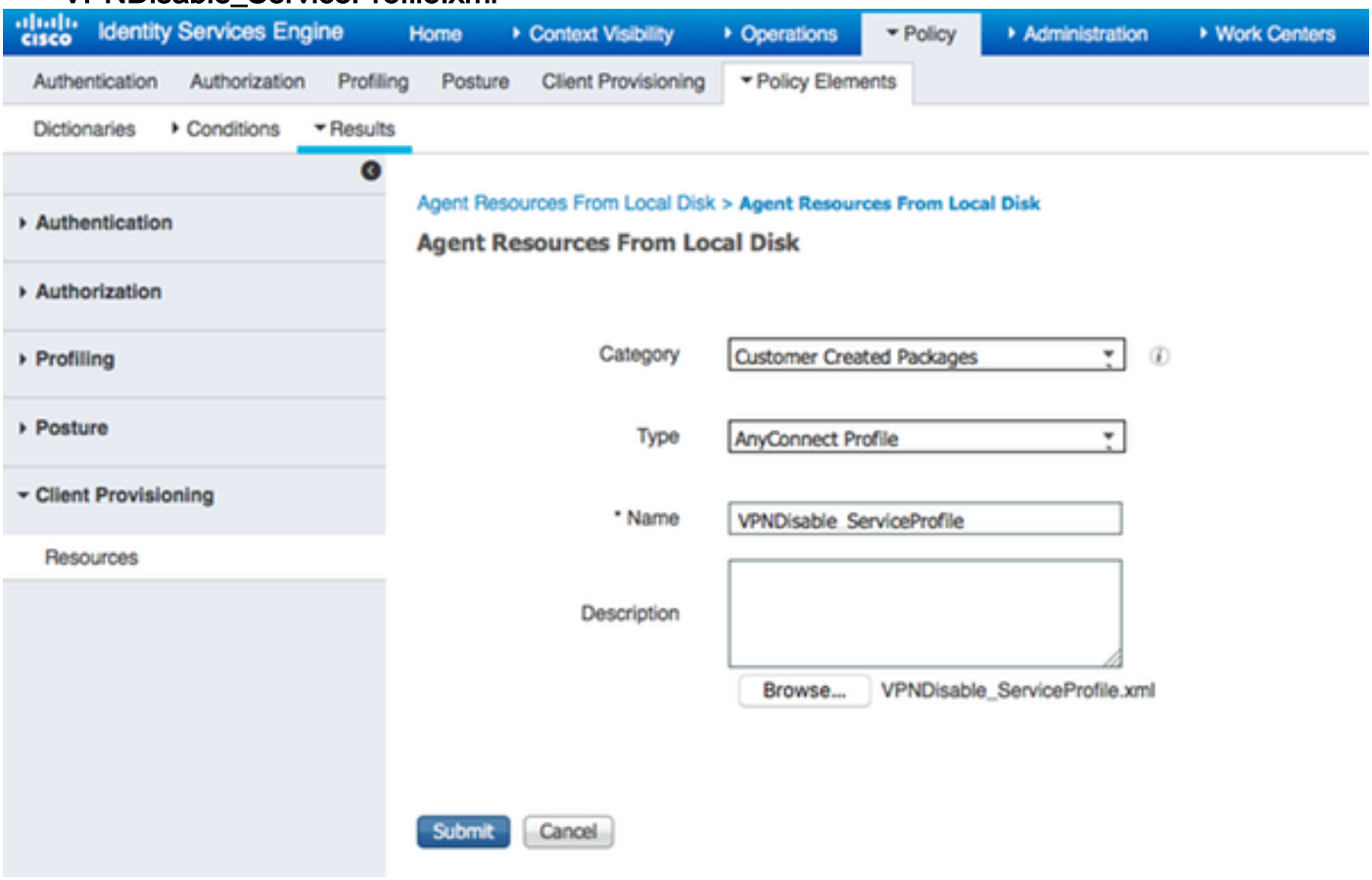


Passaggio 2. Caricamento di applicazioni e profili XML in ISE

- Scaricare l'applicazione manualmente dal sito ufficiale Cisco: **anyconnect-win-4.2.02075-k9.pkg**
- Ad ISE, selezionare Policy > Policy Elements > Results > Client Provisioning > Resources, quindi aggiungere le **risorse dell'agente dal disco locale**
- Selezionare **Cisco Provided Packages** (Pacchetti forniti da Cisco) e selezionare **anyconnect-win-4.2.02075-k9.pkg**



- Passare a Criterio > Elementi criterio > Risultati > Provisioning client > Risorse e aggiungere **Risorse agente dal disco locale**
- Selezionare **Pacchetti creati dal cliente** e digitare **AnyConnect Profile**. Selezionare **VPNDisable_ServiceProfile.xml**

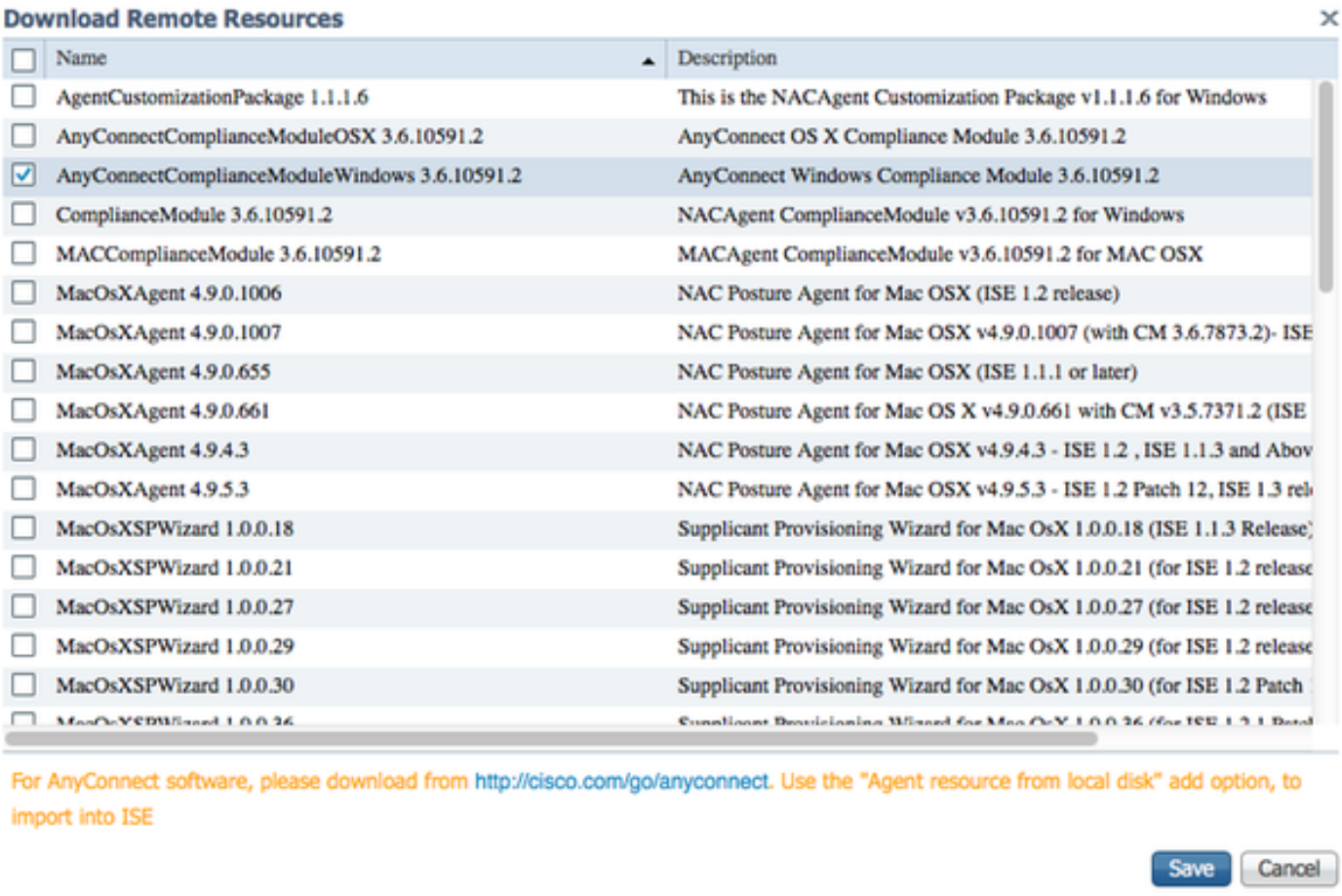


Nota: VPNDisable_ServiceProfile.xml viene utilizzato per nascondere il titolo della VPN, poiché in questo esempio non viene utilizzato il modulo VPN. Questo è il contenuto di **VPNDisable_ServiceProfile.xml**:

```
<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">
 <Inizializzazione client>
 <ServiceDisable>true</ServiceDisable>
 </Inizializzazione client>
</AnyConnectProfile>
```

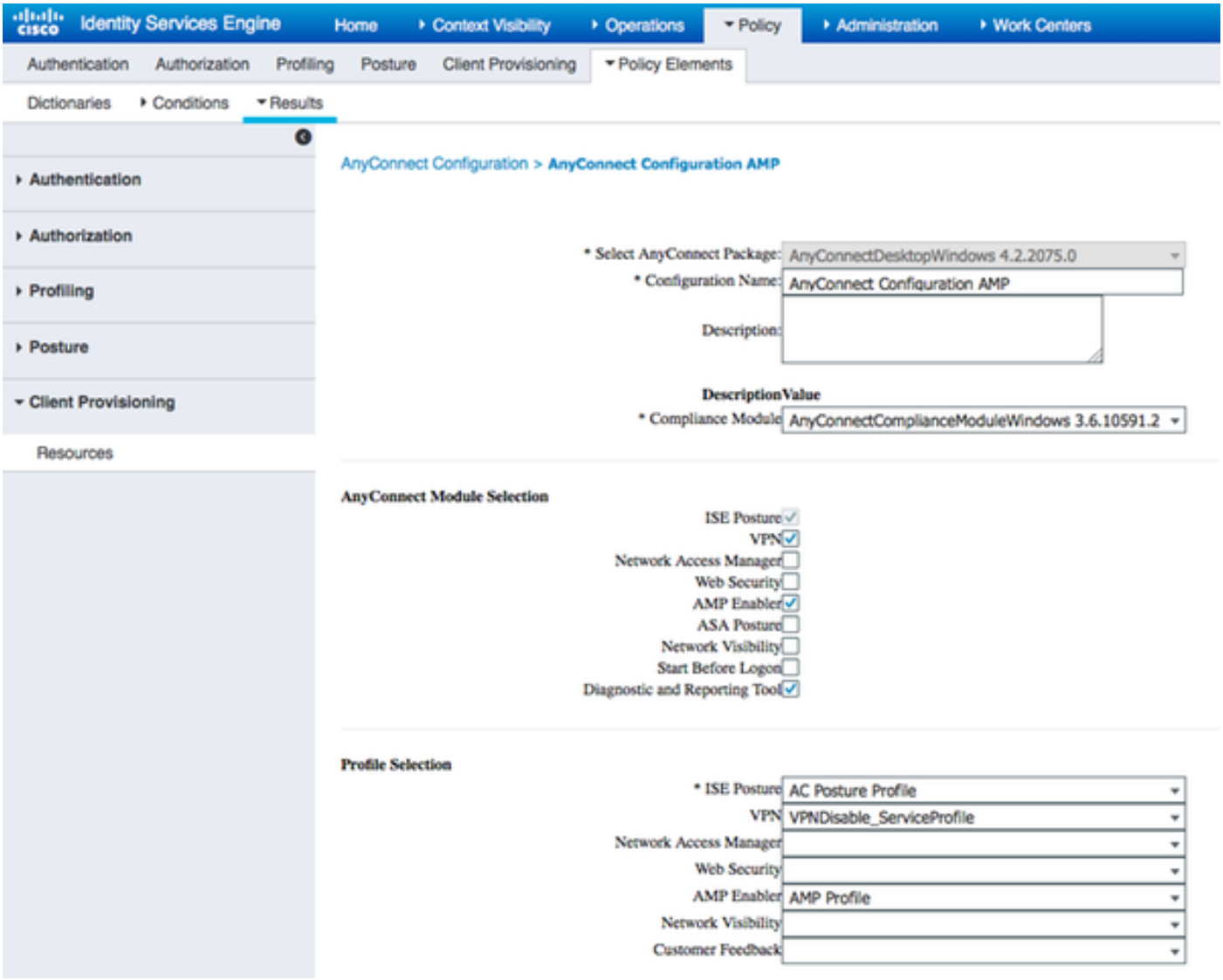
Passaggio 3. Scarica il modulo di conformità AnyConnect

- Selezionare Criteri > Elementi criterio > Risultati > Provisioning client > Risorse e aggiungere **risorse agente dal sito Cisco**
- Selezionare **AnyConnect Windows Compliance Module 3.6.10591.2** e fare clic su **Salva**



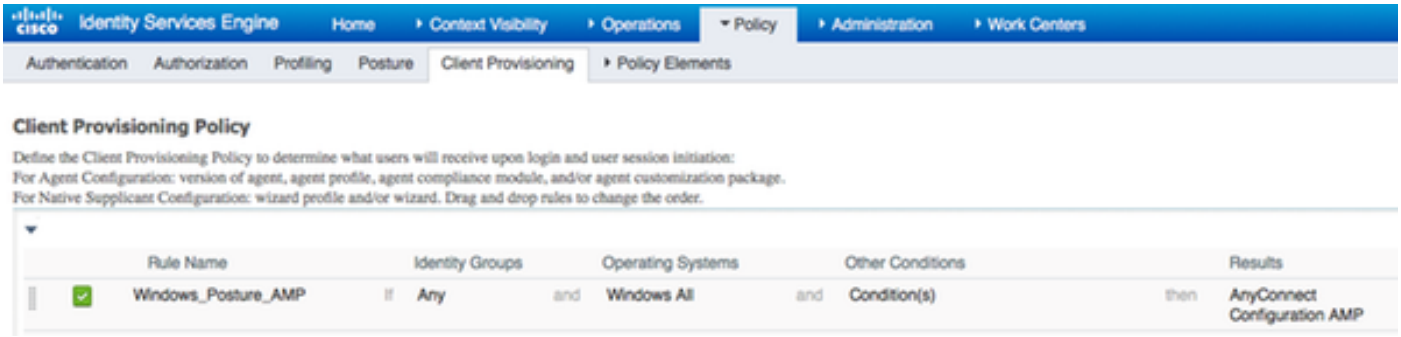
Passaggio 4. Aggiunta della configurazione AnyConnect

- Selezionare Criteri > Elementi dei criteri > Risultati > Provisioning client > Risorse e aggiungere la **configurazione AnyConnect**
- Configurare il nome e selezionare il modulo di conformità e tutti i moduli AnyConnect richiesti (VPN, AMP e Posture)
- In **Selezione profilo**, scegliere il profilo configurato in precedenza per ciascun modulo



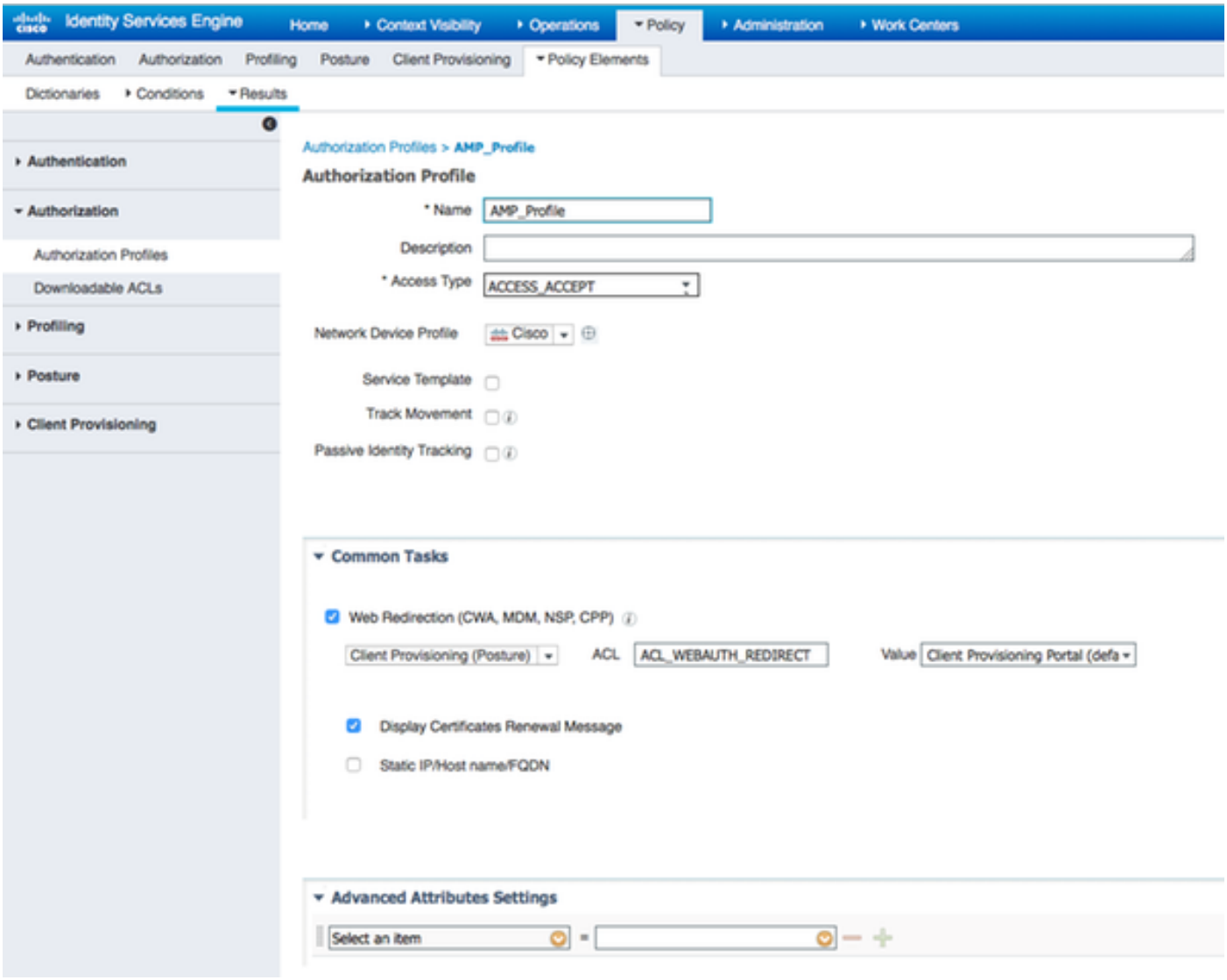
Passaggio 5. Configurazione delle regole di provisioning client

Le regole di **provisioning client** fanno riferimento alla configurazione AnyConnect creata in precedenza

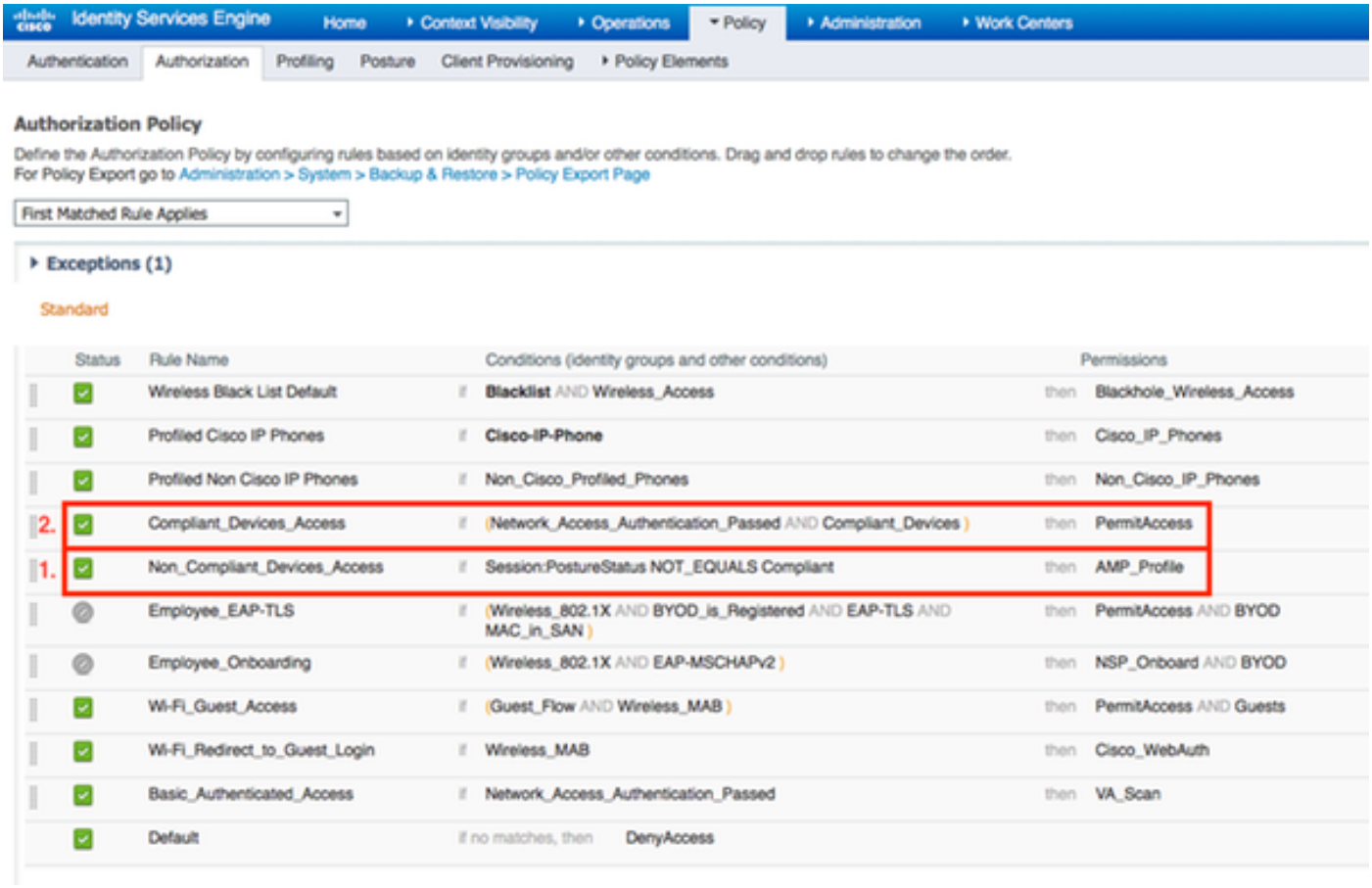


Passaggio 6. Configurare i criteri di autorizzazione

Innanzitutto viene eseguito il reindirizzamento al portale di provisioning client. Vengono utilizzati criteri di autorizzazione standard per la postura.

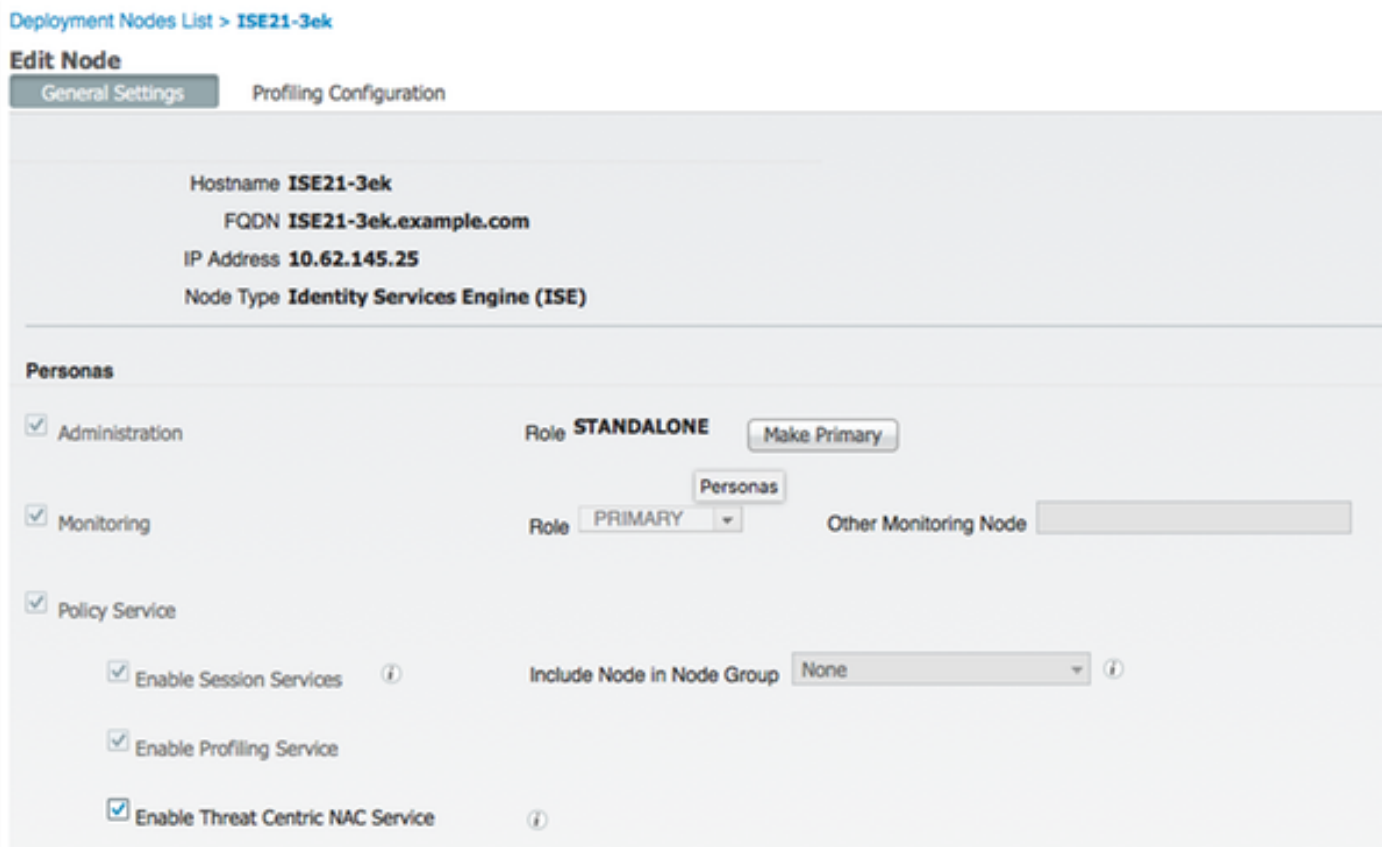


In seguito, una volta ottenuta la conformità, viene assegnato l'accesso completo



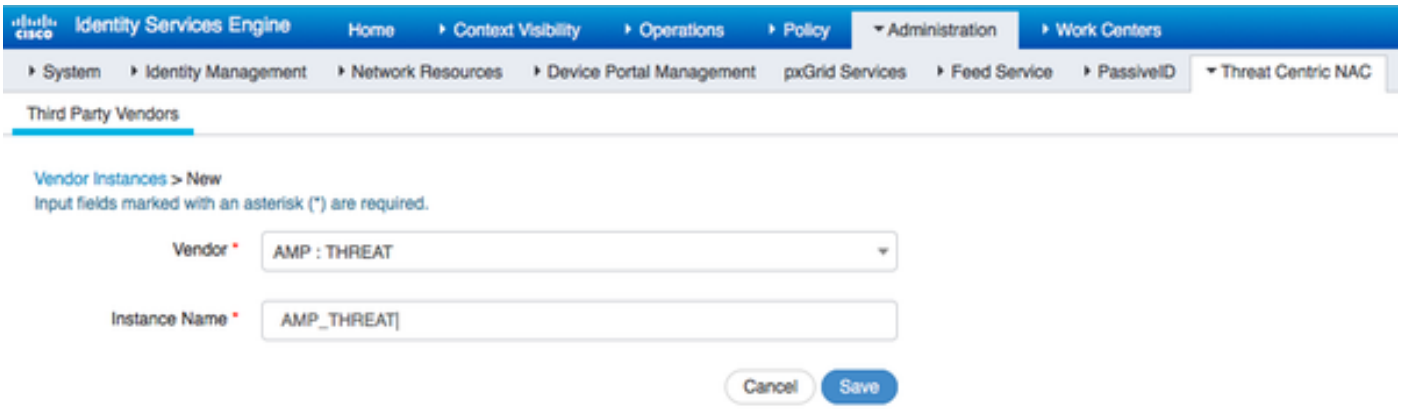
Passaggio 7. Abilitare i servizi TC-NAC

Abilitare TC-NAC Services in Amministrazione > Distribuzione > Modifica nodo. Selezionare la casella di controllo **Abilita servizio NAC basato sulle minacce**.

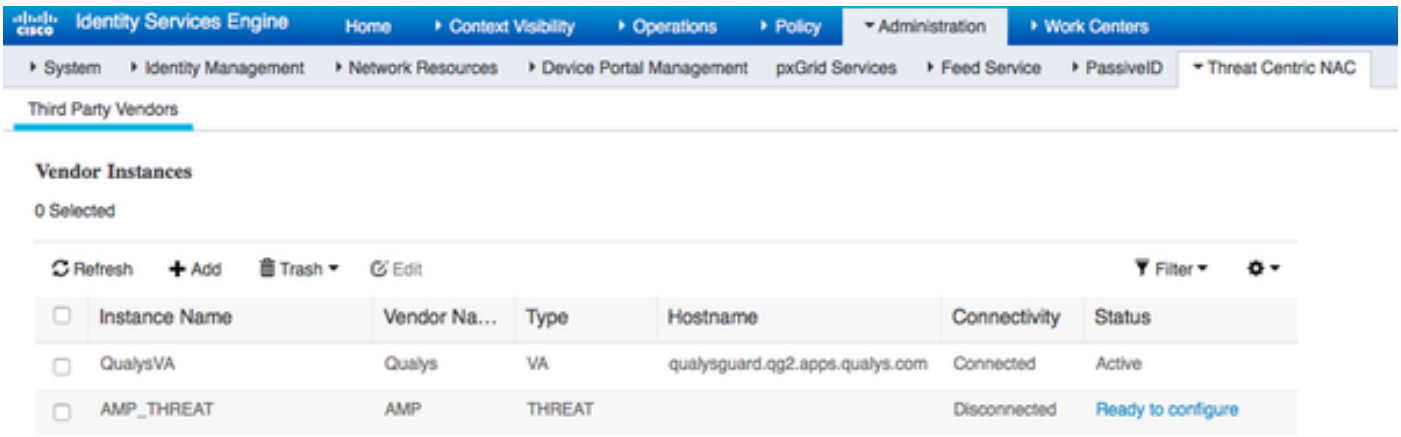


Passaggio 8. Configurare l'adattatore AMP

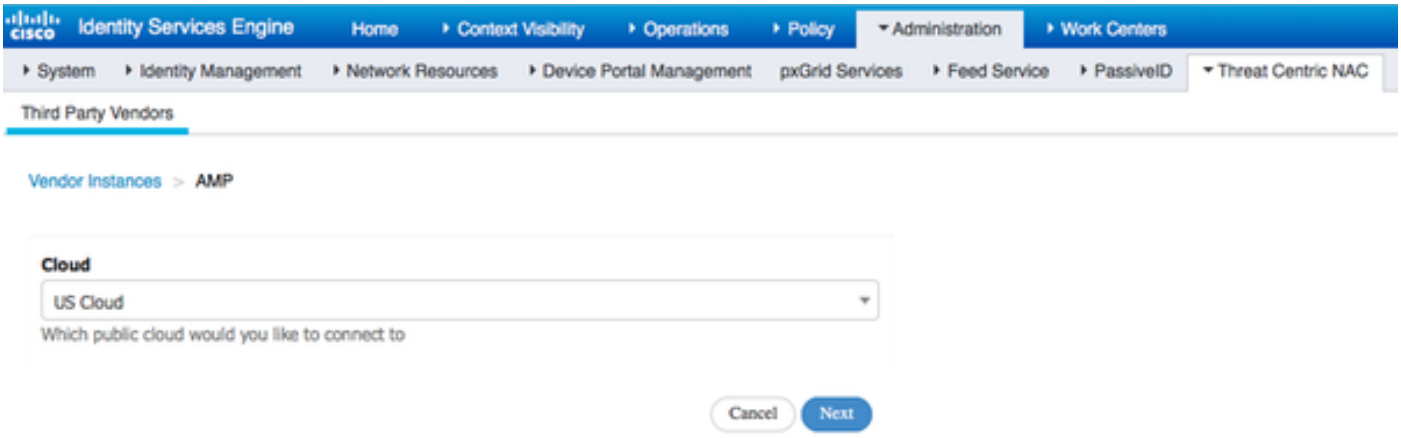
Passare a Amministrazione > NAC incentrato sulle minacce > Fornitori terzi > Aggiungi. Fare clic su **Salva**



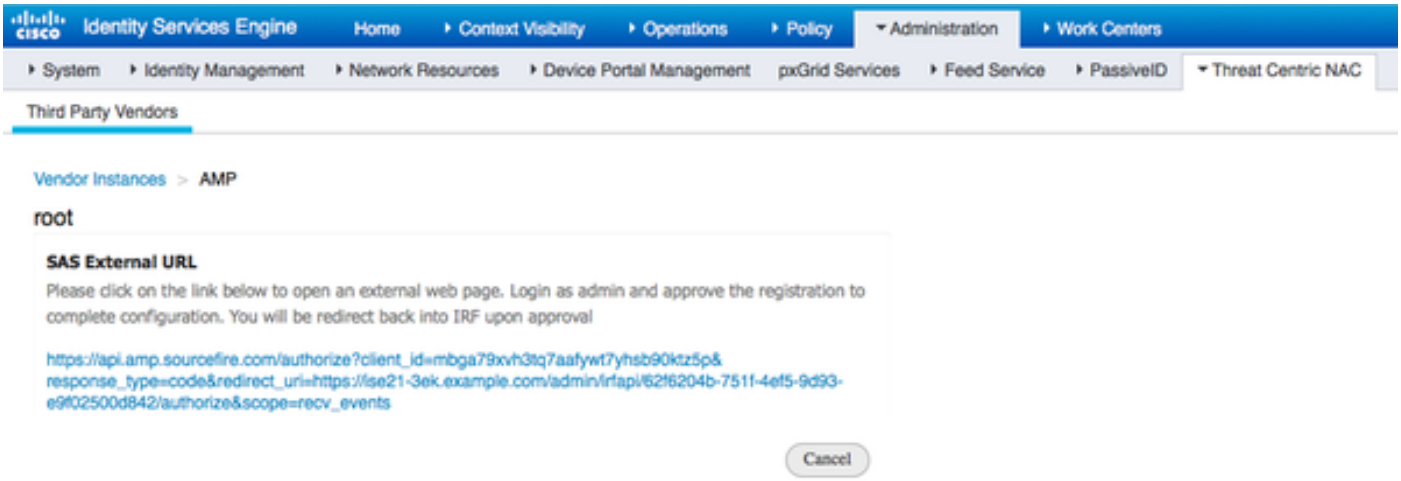
Dovrebbe passare allo stato **Pronto per la configurazione**. Fare clic su **Pronto per la configurazione**



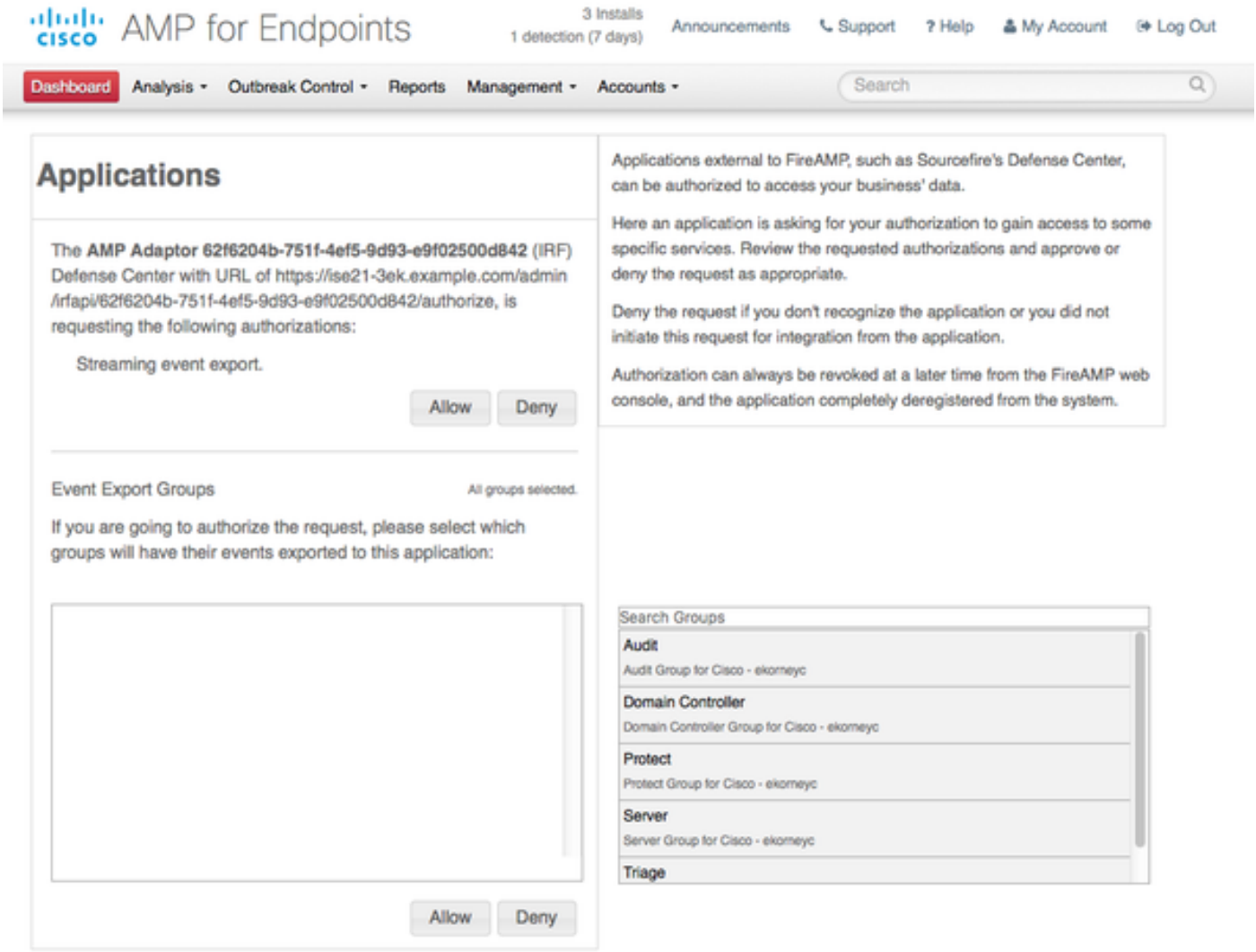
Selezionare **Cloud** e fare clic su **Next**



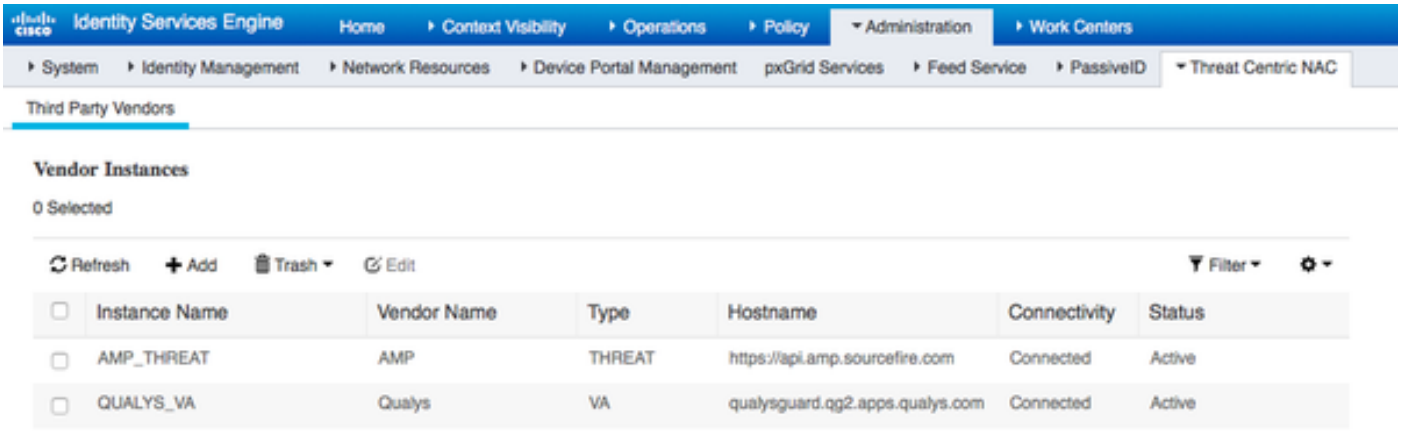
Fare clic sul collegamento FireAMP e accedere come admin in FireAMP.



Fate clic su **Consenti** nel pannello **Applicazioni** per autorizzare la richiesta di esportazione degli eventi di streaming. Dopo questa azione, verrai reindirizzato a Cisco ISE



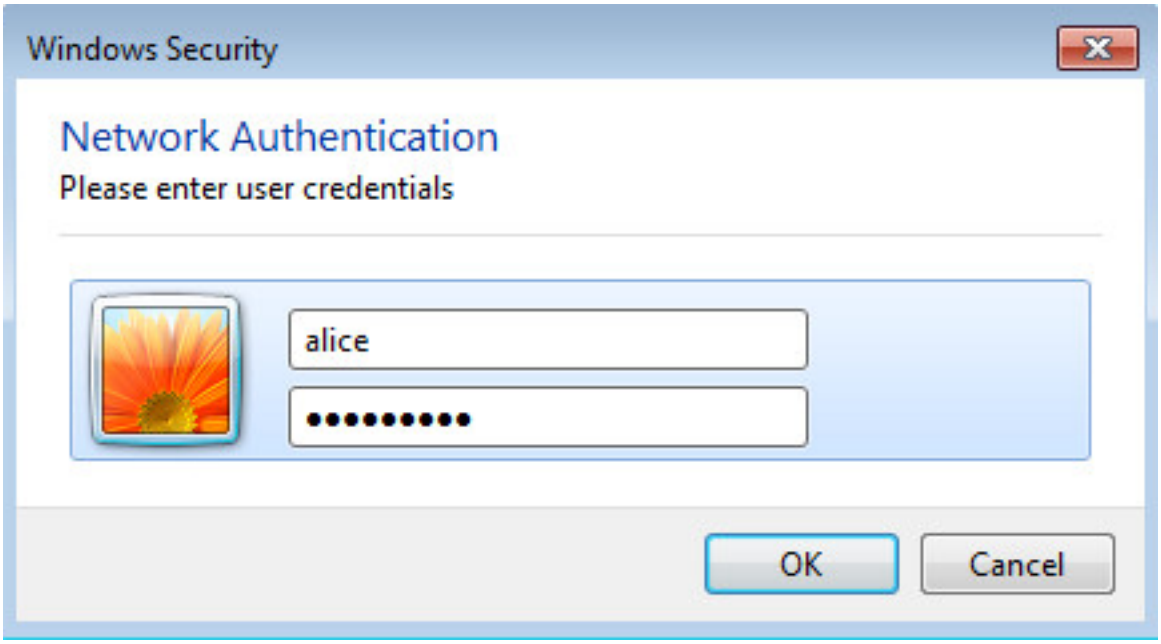
Selezionare gli eventi (ad esempio, download sospetto, connessione a dominio sospetto, malware eseguito, compromissione Java) che si desidera monitorare. Il riepilogo della configurazione dell'istanza dell'adattatore viene visualizzato nella pagina di riepilogo della configurazione. L'istanza della scheda passa allo stato Connesso/Attivo.



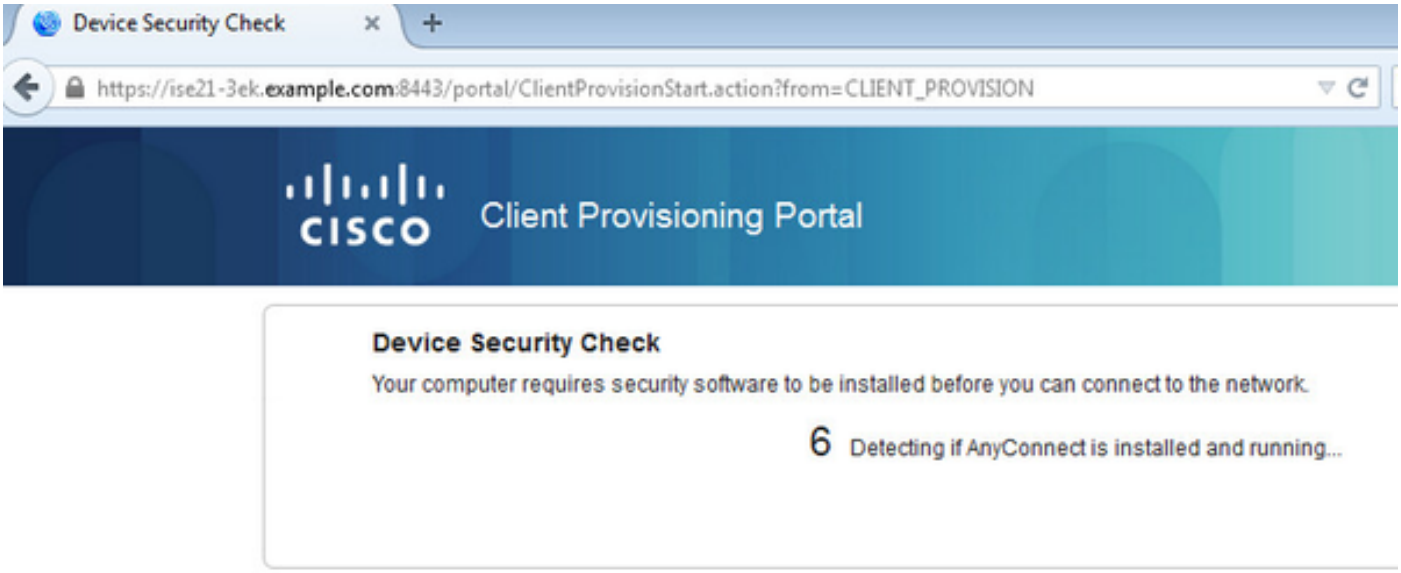
Verifica

Endpoint

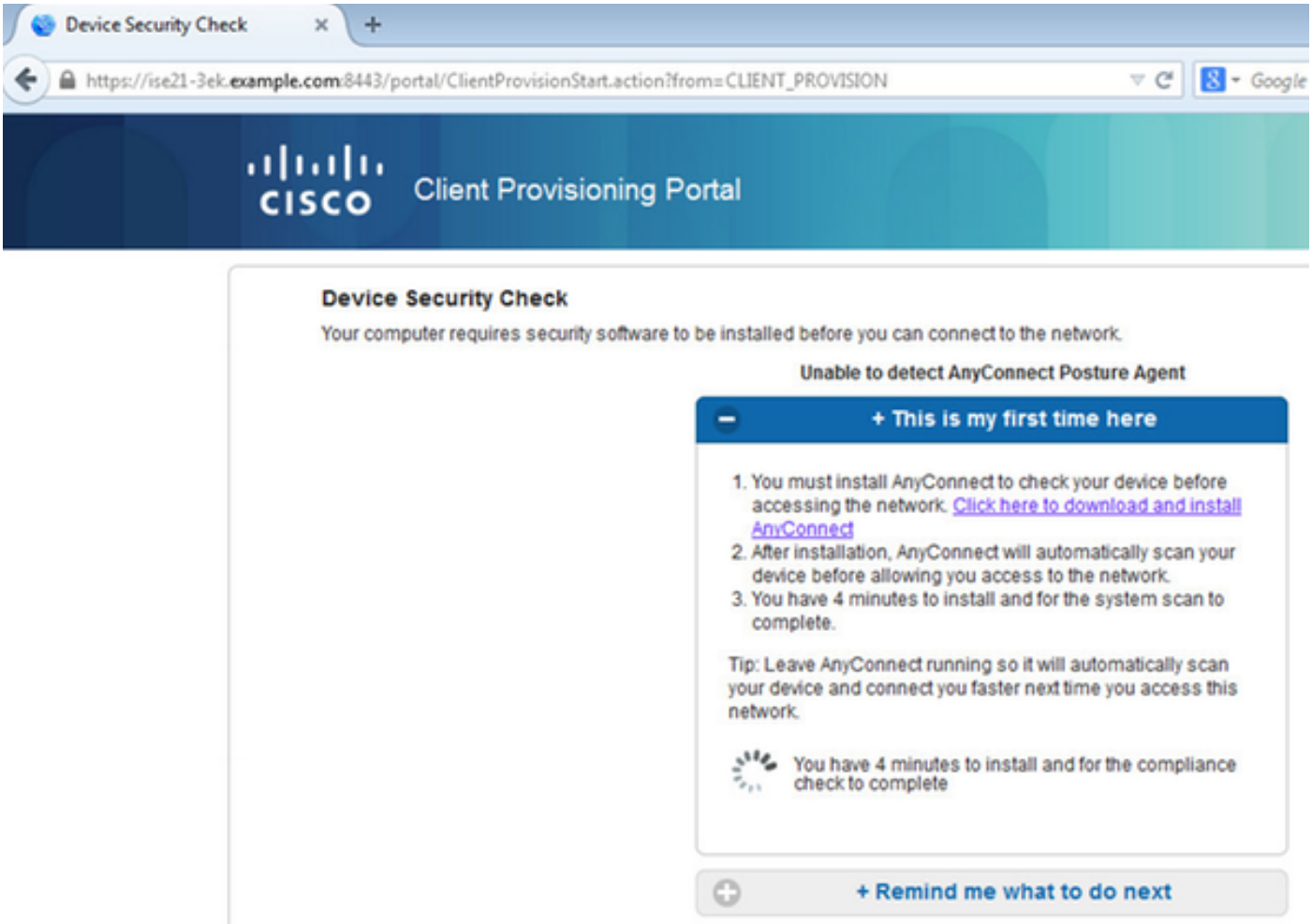
Connettersi alla rete wireless tramite PEAP (MSCHAPv2).



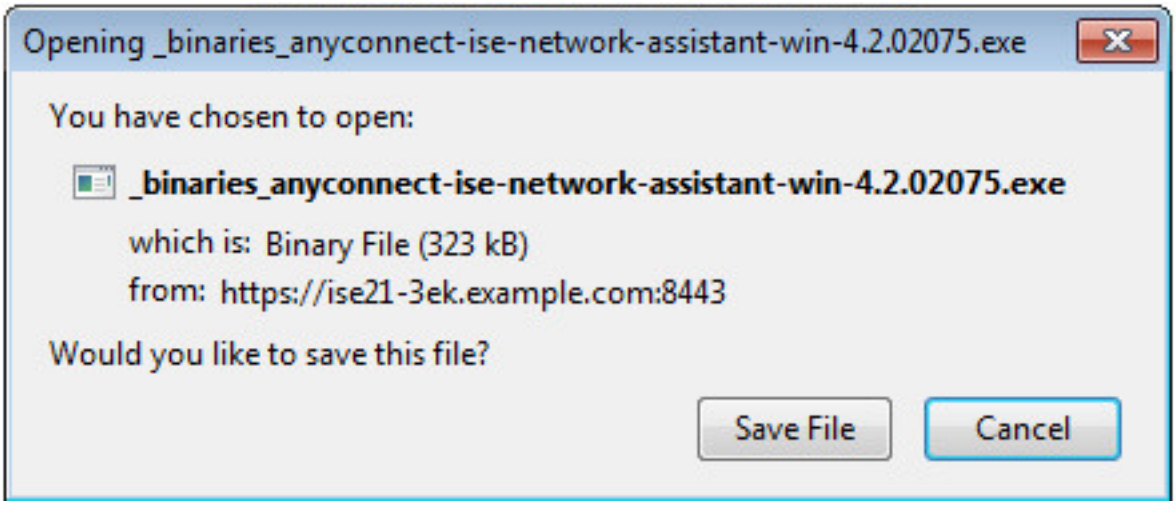
Una volta stabilita la connessione, viene eseguito il reindirizzamento al portale di provisioning client.



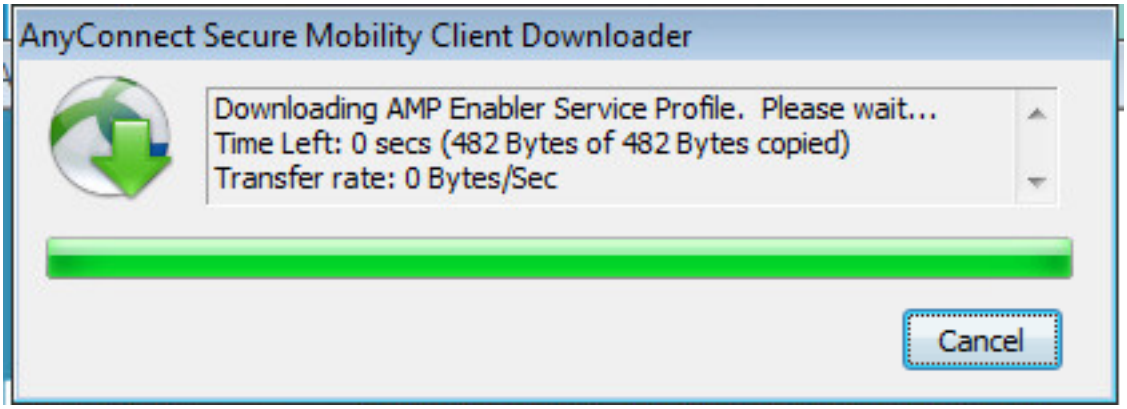
Poiché sul computer client non è installato nulla, ISE richiede l'installazione del client AnyConnect.

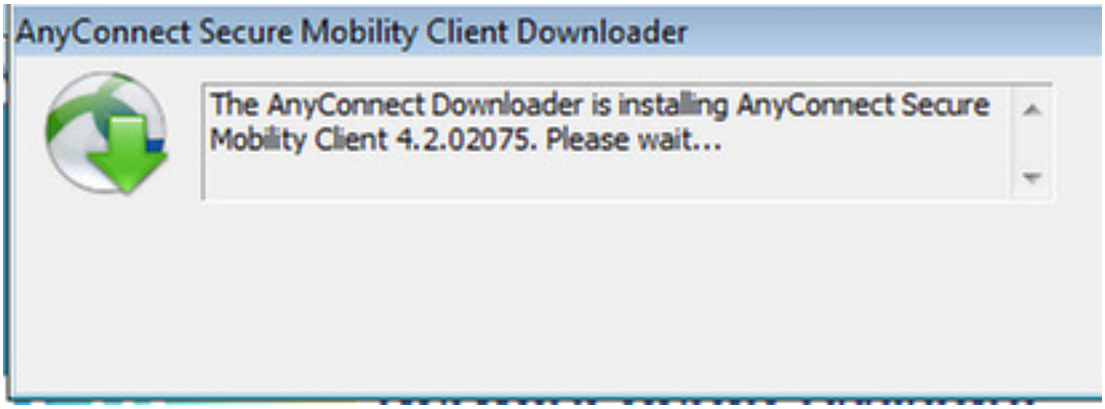


L'applicazione NSA (Network Setup Assistant) deve essere scaricata ed eseguita dal computer client.

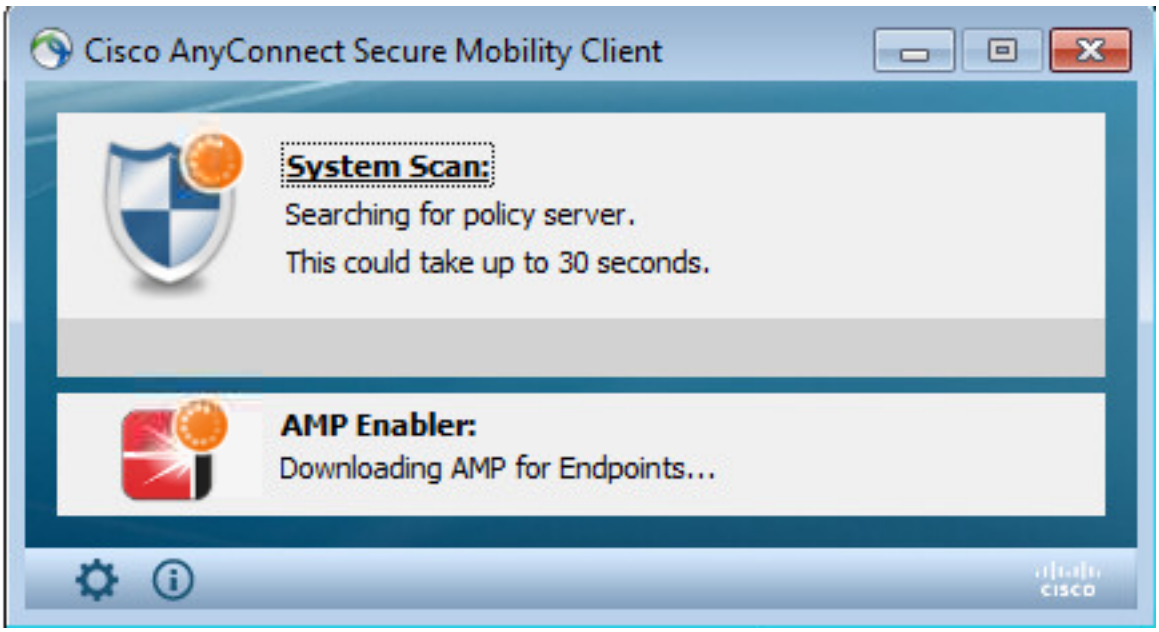


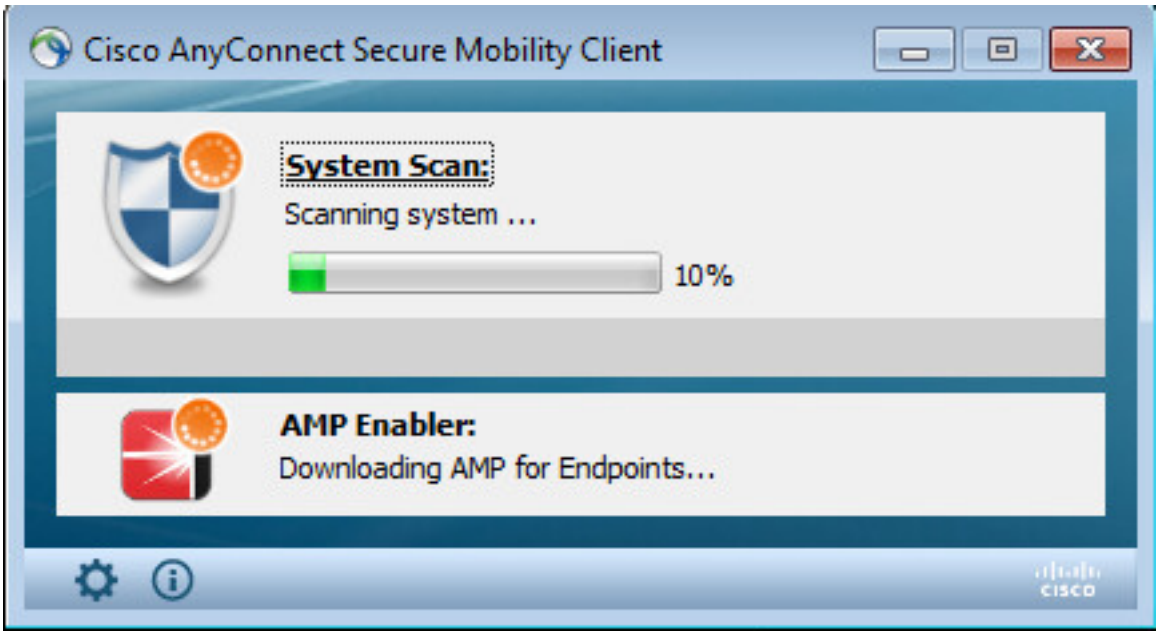
NSA si occupa di installare i componenti e i profili richiesti.



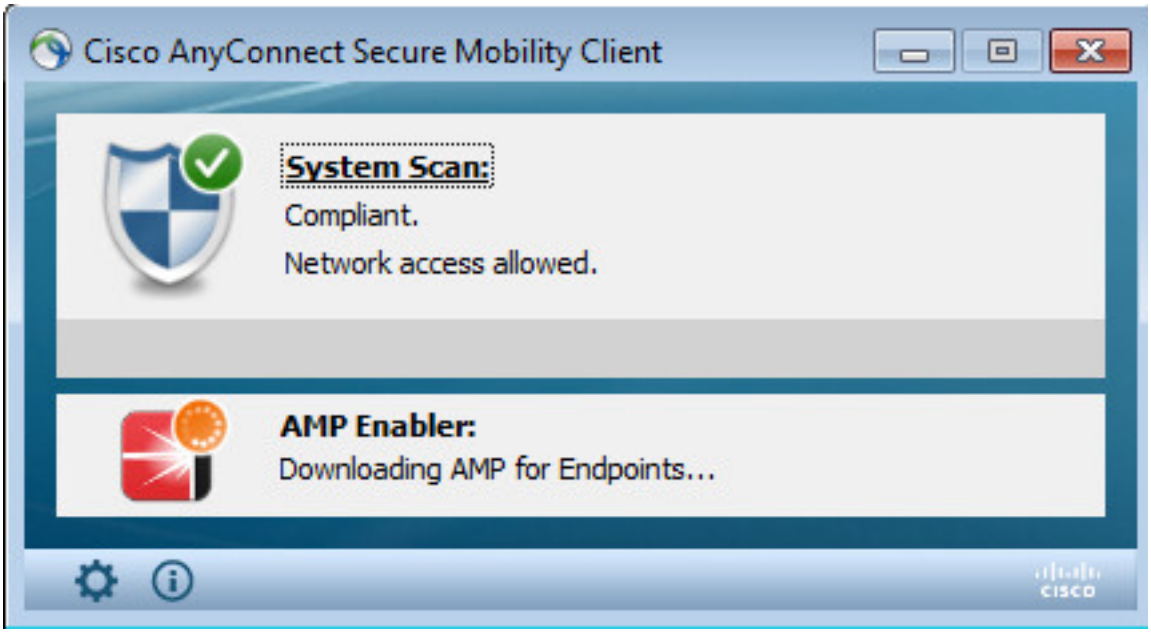


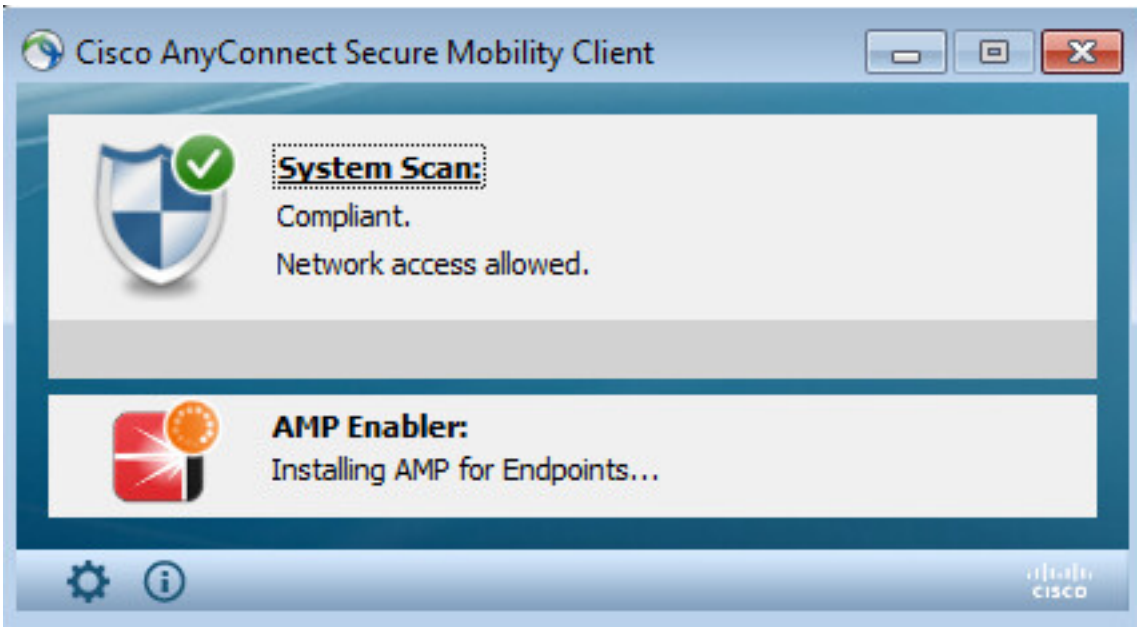
Al termine dell'installazione, il modulo AnyConnect Posture esegue il controllo della conformità.

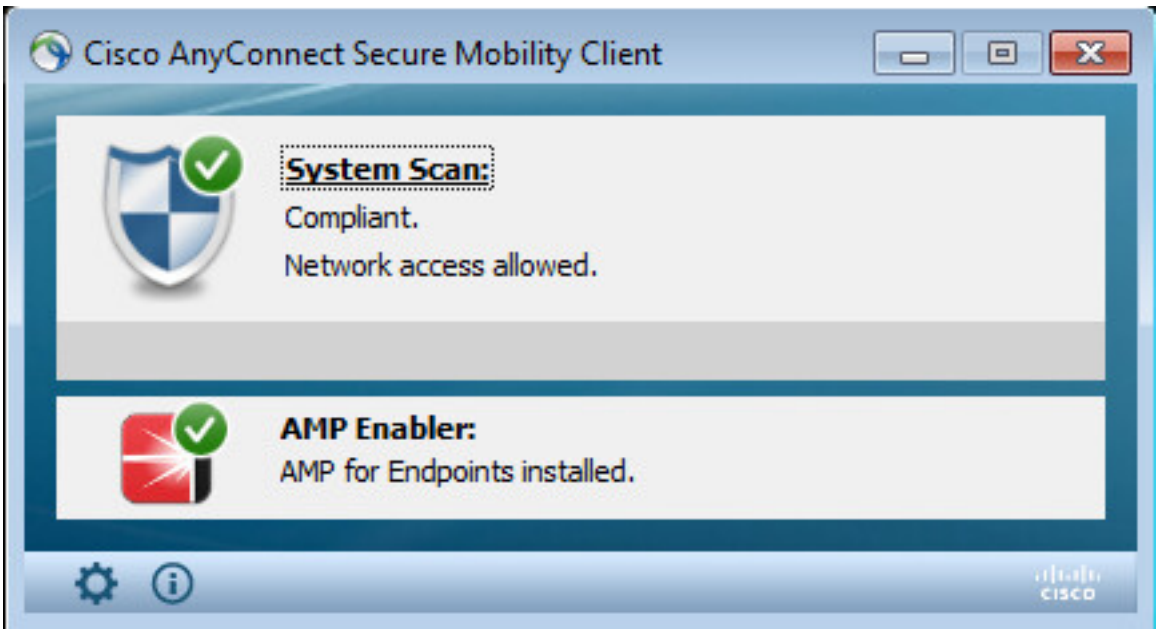




Quando viene concesso l'accesso completo, se l'endpoint è conforme, AMP viene scaricato e installato dal server Web specificato in precedenza nel profilo AMP.

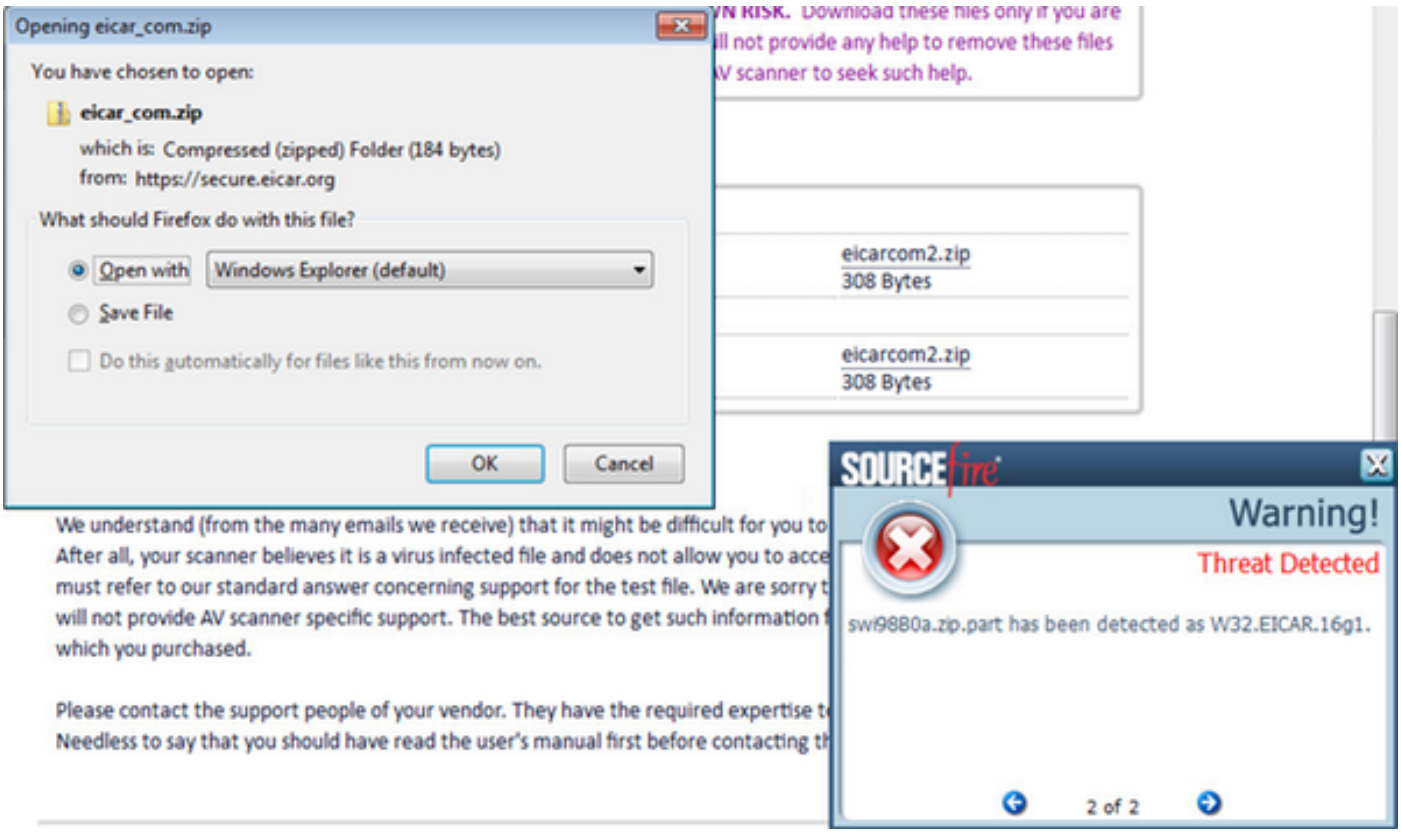






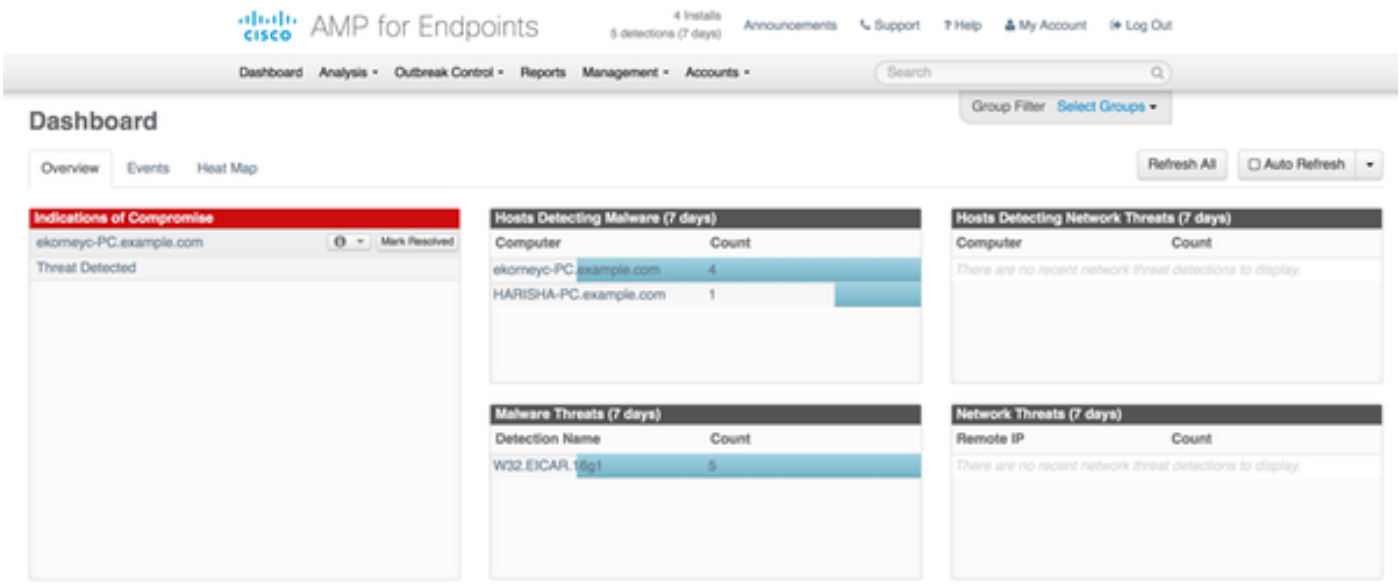
Viene visualizzato il connettore AMP.

Per eseguire il test di AMP, viene scaricata la stringa Eicar contenuta in un file zip. La minaccia viene rilevata e segnalata ad AMP Cloud.

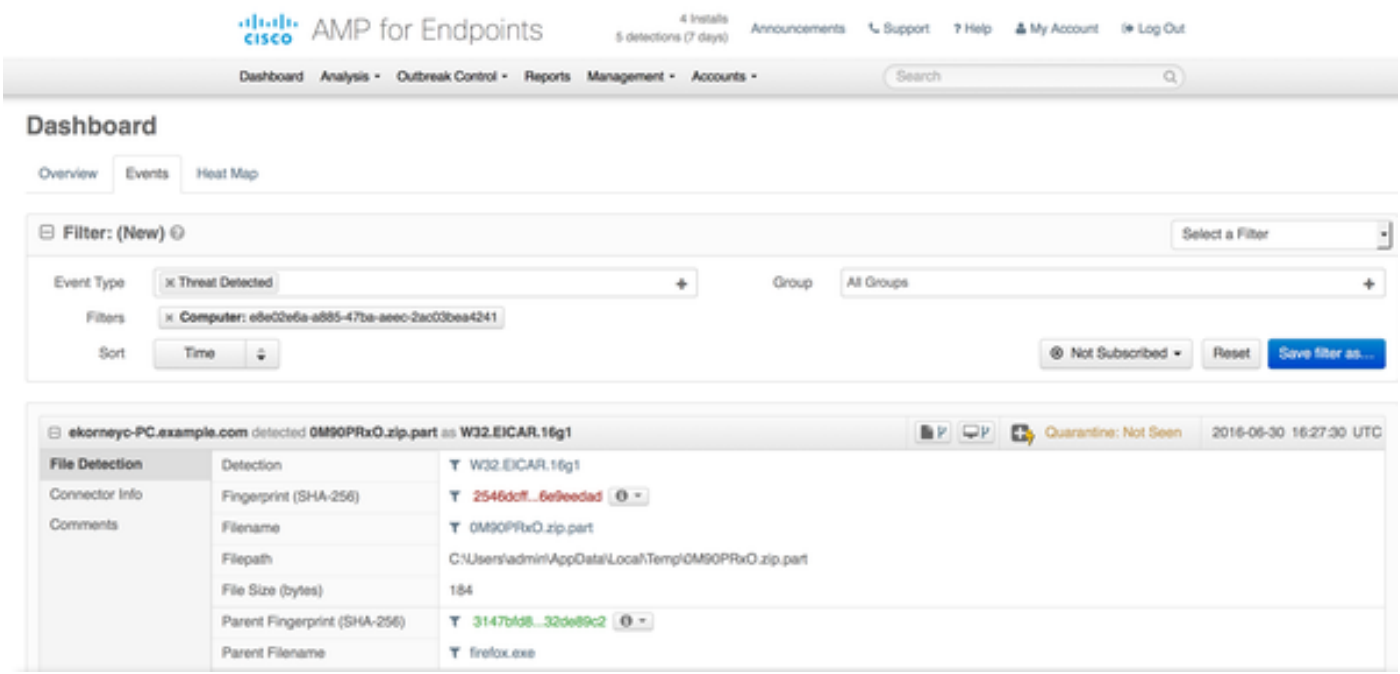


AMP Cloud

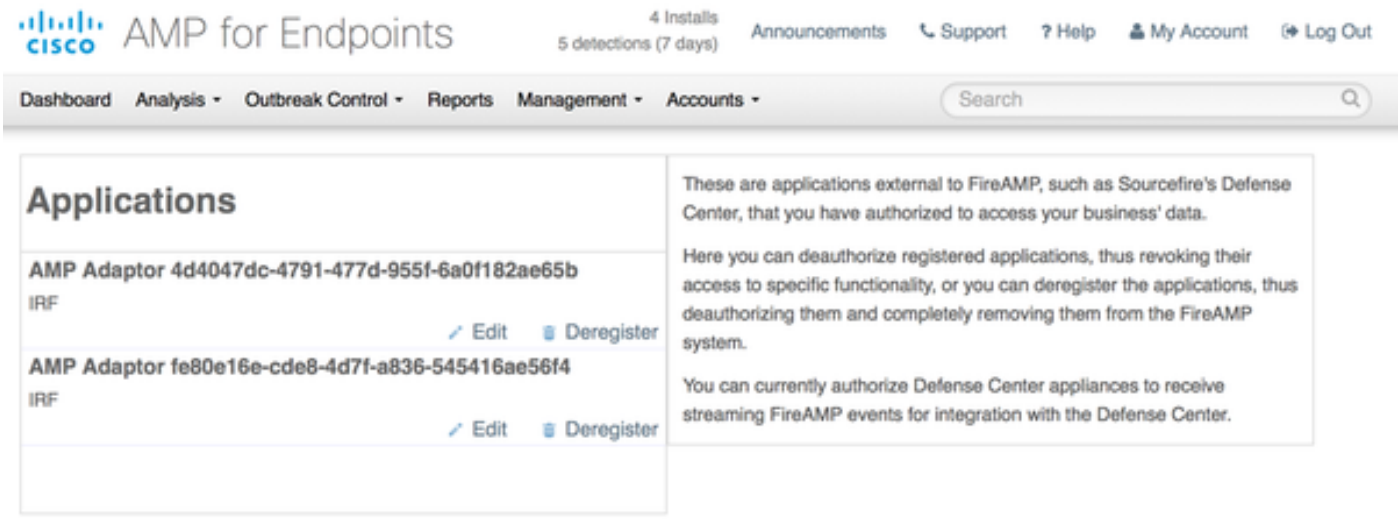
Per verificare i dettagli del Dashboard minacce del cloud AMP è possibile utilizzare.



Per ulteriori dettagli sulla minaccia, il percorso del file e le impronte digitali, è possibile fare clic sull'host in cui è stato rilevato il malware.

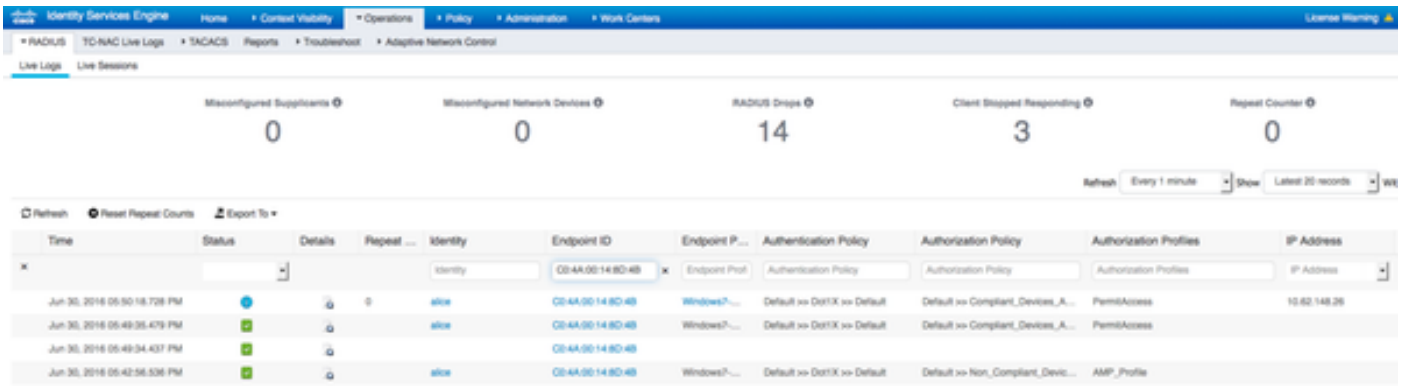


Per visualizzare o annullare la registrazione di un'istanza di ISE, passare a Conti > Applicazioni

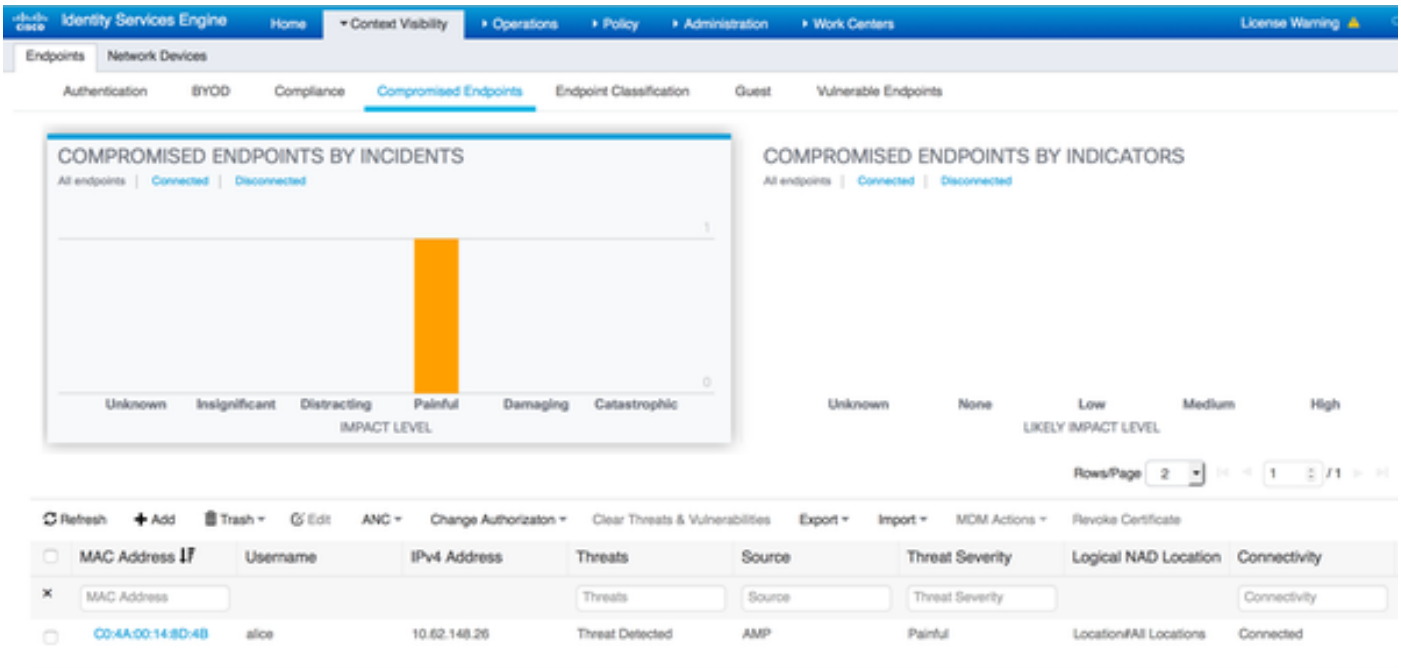


ISE

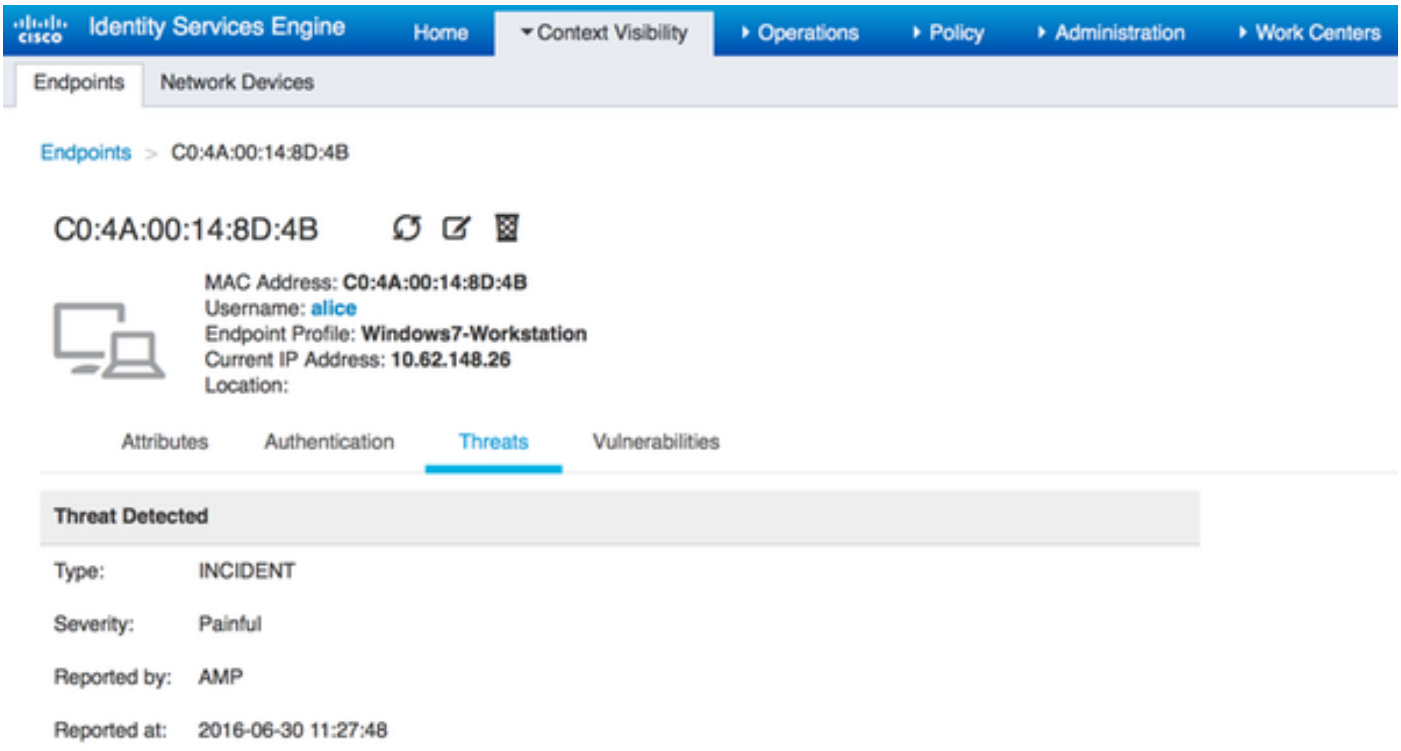
Nell'ISE è stato osservato un flusso di postura regolare; il reindirizzamento ha luogo per primo per verificare la conformità della rete. Non appena l'endpoint è conforme, viene inviata una nuova autorizzazione CoA e viene assegnato un nuovo profilo con PermitAccess.



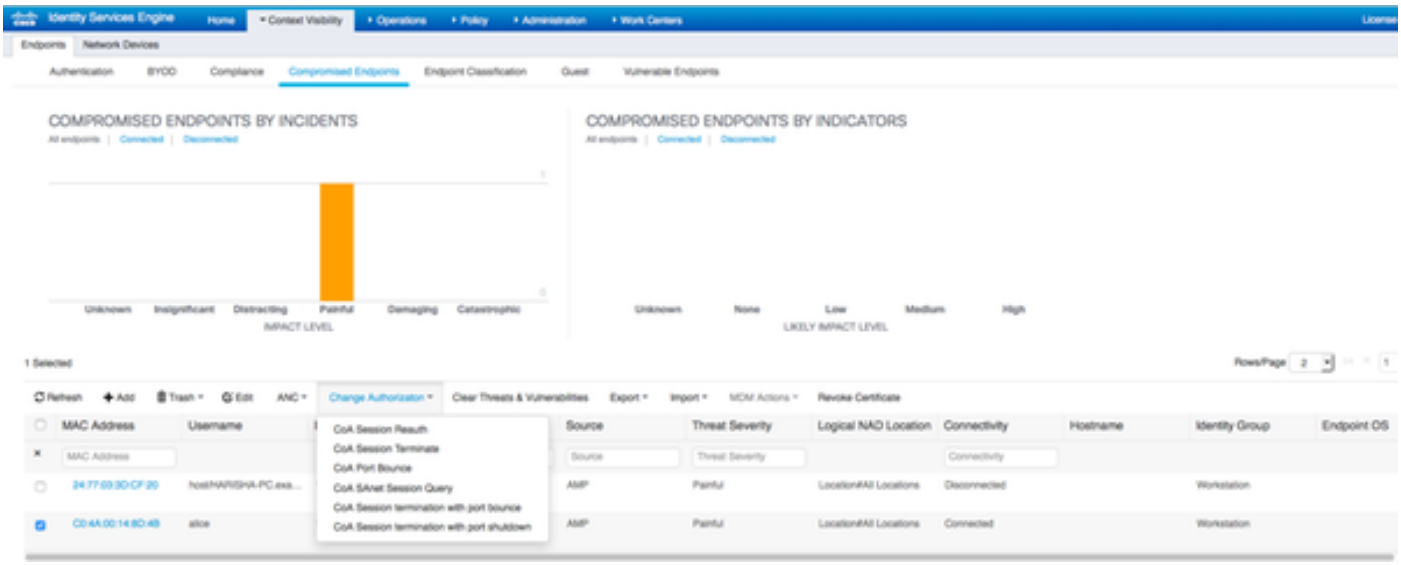
Per visualizzare le minacce rilevate, è possibile passare a Visibilità contesto > Endpoint > Endpoint compromessi



Se si seleziona l'endpoint e si passa alla scheda Minaccia, vengono visualizzati ulteriori dettagli.



Quando viene rilevato un evento di minaccia per un endpoint, è possibile selezionare l'indirizzo MAC dell'endpoint nella pagina Endpoint compromessi e applicare un criterio ANC (se configurato, ad esempio Quarantena). In alternativa, è possibile eseguire il comando Modifica di autorizzazione per terminare la sessione.



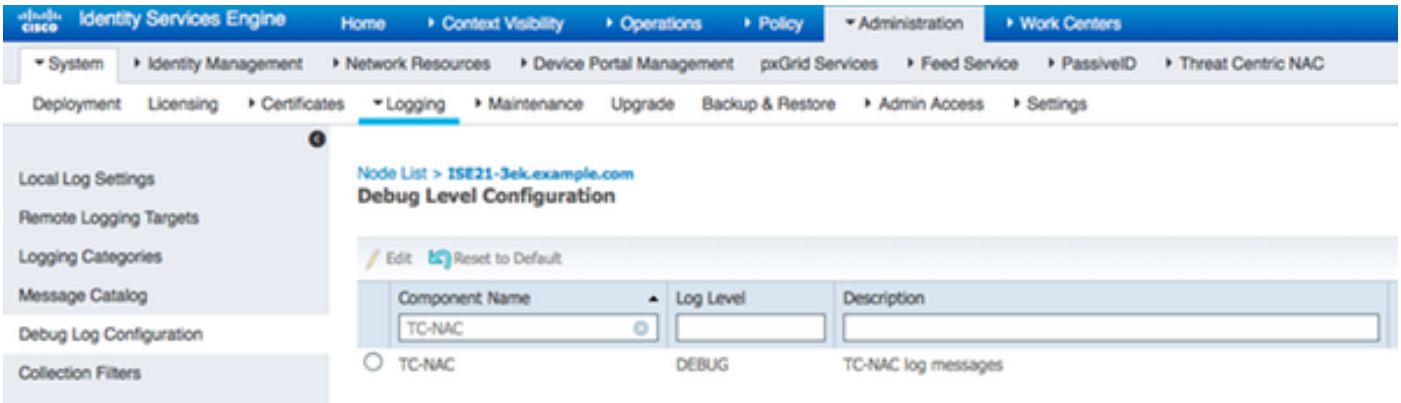
Se si seleziona Termina sessione CoA, ISE invia la disconnessione CoA e il client perde l'accesso alla rete.

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

Risoluzione dei problemi

Per abilitare i debug su ISE, selezionare Amministrazione > Sistema > Registrazione > Configurazione log di debug, selezionare TC-NAC Node e modificare il **livello** di **log** del componente TC-NAC in **DEBUG**



Registri da controllare - irf.log. È possibile archiviarlo direttamente dalla CLI di ISE:

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

Threat Even viene ricevuto da AMP Cloud

2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:53 -:::: - chiamando il gestore delle
notifiche com.cisco.cpm.irf.service.IrfNotificationHandler$MyNotificationHandler@3fac8043
Message{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"**c0:4a:0 12:14:8d:4b**":
[{"incidente": {"Impact_Qualification": "Doloroso"}, "indicatore orario": 1467304068599,
"fornitore": "AMP", "title": "**Threat Detected**"}]}', priority=0, timestamp=Thu Jun 30 18:27:48
CEST 2016, amqpEnvelope=Envelope(deliveryTag=79, redelivery=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-code8-4d7f-a836-545416ae56f4, cluster-id=null)}
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.service.IrfNotificationHandler:handle:140 -:::: - Aggiunto alla coda in sospeso:
Message{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"**c0:4a:00:14:8d:4b**":
[{"incidente": {"Impact_Qualification": "**Doloroso**"}, "indicatore orario": 1467304068599,
"fornitore": "**AMP**", "title": "Threat Detected"}]}', priority=0, timestamp=Thu Jun 30 18:27:48
CEST 2016, amqpEnvelope=Envelope(deliveryTag=79, redelivery=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-null=null, expiration=null, message-id=THREAT_EVENT, timestamp=null,
type=NOTIFICATION, user-id=null, app-id=fe80e16e-code8-4d7f-a836-545416ae56f4, cluster-id=null)}
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:59 -:::: - NOTIFICA ELABORAZIONE
COMPLETATA: Envelope(deliveryTag=79, redelivery=false, exchange=irf.topic.events,
routingKey=irf.events.threat) #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-code8-4d7f-a8 36-545416ae56f4, cluster-id=null)
2016-06-30 18:27:48,706 DEBUG [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:parseNotification:221 -::::- notifica di analisi:
Message{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b":
[{"incidente": {"Impact_Qualification": "Doloroso"}, "indicatore orario": 1467304068599,
"fornitore": "AMP", "title": "Threat Detected"}]}', priority=0, timestamp=Thu Jun 30 18:27:48
CEST 2016, amqpEnvelope=Envelope(deliveryTag=79, redelivery=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-null=null, expiration=null, message-id=THREAT_EVENT, timestamp=null,
type=NOTIFICATION, user-id=null, app-id=fe80e16e-code8-4d7f-a836-545416ae56f4, cluster-id=null)}

Le informazioni sulla minaccia vengono inviate alla rete PAN

2016-06-30 18:27:48,724 DEBUG [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:storeEventsInES:366 -::::::- **Aggiunta di informazioni
sugli eventi di minaccia da inviare alla PAN - c0:4a:00:14:8d:4b**
{incidente={Impact_Qualification=Painful}, timestamp=14 7304068599, vendor=AMP, title=Rilevata
minaccia}