

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

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Flusso dettagliato](#)

[Configurare AMP Cloud](#)

[Passaggio 1. Scaricare il connettore da AMP Cloud](#)

[Configurare ISE](#)

[Passaggio 1. Configurare criteri e condizioni di postura](#)

[Passaggio 2. Configurare il profilo della postura](#)

[Passaggio 3. Configurare il profilo AMP](#)

[Passaggio 2. Caricamento di applicazioni e profili XML in ISE](#)

[Passaggio 3. Scarica il modulo di conformità AnyConnect](#)

[Passaggio 4. Aggiunta della configurazione AnyConnect](#)

[Passaggio 5. Configurazione delle regole di provisioning client](#)

[Passaggio 6. Configurare i criteri di autorizzazione](#)

[Passaggio 7. Abilitare i servizi TC-NAC](#)

[Passaggio 8. Configurare l'adattatore AMP](#)

[Verifica](#)

[Endpoint](#)

[AMP Cloud](#)

[ISE](#)

[Risoluzione dei problemi](#)

## 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.

The screenshot shows the AMP for Endpoints web interface. At the top, there is a navigation bar with the Cisco logo and 'AMP for Endpoints' text. To the right, there are statistics: '3 installs', '1 detection (7 days)', and links for 'Announcements', 'Support', 'Help', 'My Account', and 'Log Out'. Below the navigation bar is a search bar and a menu with 'Dashboard', 'Analysis', 'Outbreak Control', 'Reports', 'Management', and 'Accounts'. The main content area is titled 'Download Connector'. A dropdown menu shows 'Group' set to 'Audit'. There are four connector cards:

- FireAMP Windows**: Includes 'Audit Policy', 'Flash Scan on Install', and 'Redistributable' options. Buttons: 'Show URL', 'Download'.
- FireAMP Mac**: Includes 'Audit Policy for FireAMP Mac' and 'Flash Scan on Install' options. Buttons: 'Show URL', 'Download'.
- FireAMP Linux**: Includes 'Audit Policy for FireAMP Li...' and 'Flash Scan on Install' options. Buttons: 'Show GPG Public Key', 'Show URL', 'Download'.
- FireAMP Android**: Includes 'Default FireAMP Android' and 'Activation Codes' options. Buttons: 'Show URL', 'Download'.

**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:

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

Description

\* Operating System

Compliance Module Any version

\* File Type  ⓘ

\* File Path   ⓘ

\* File Operator

- 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

Questa condizione viene utilizzata per un requisito:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

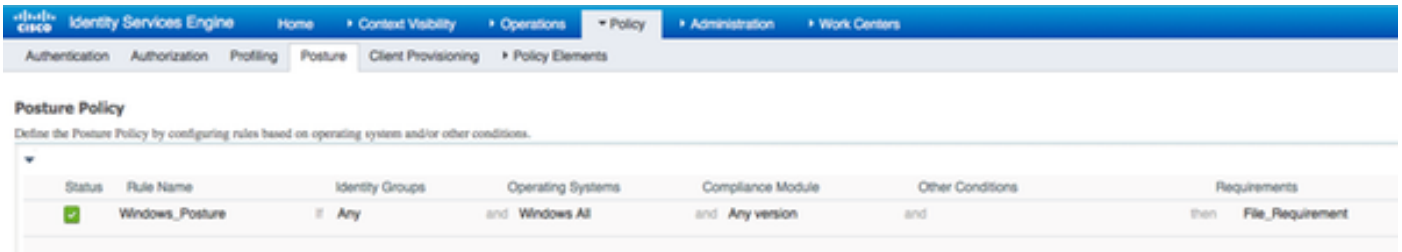
Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

### Requirements

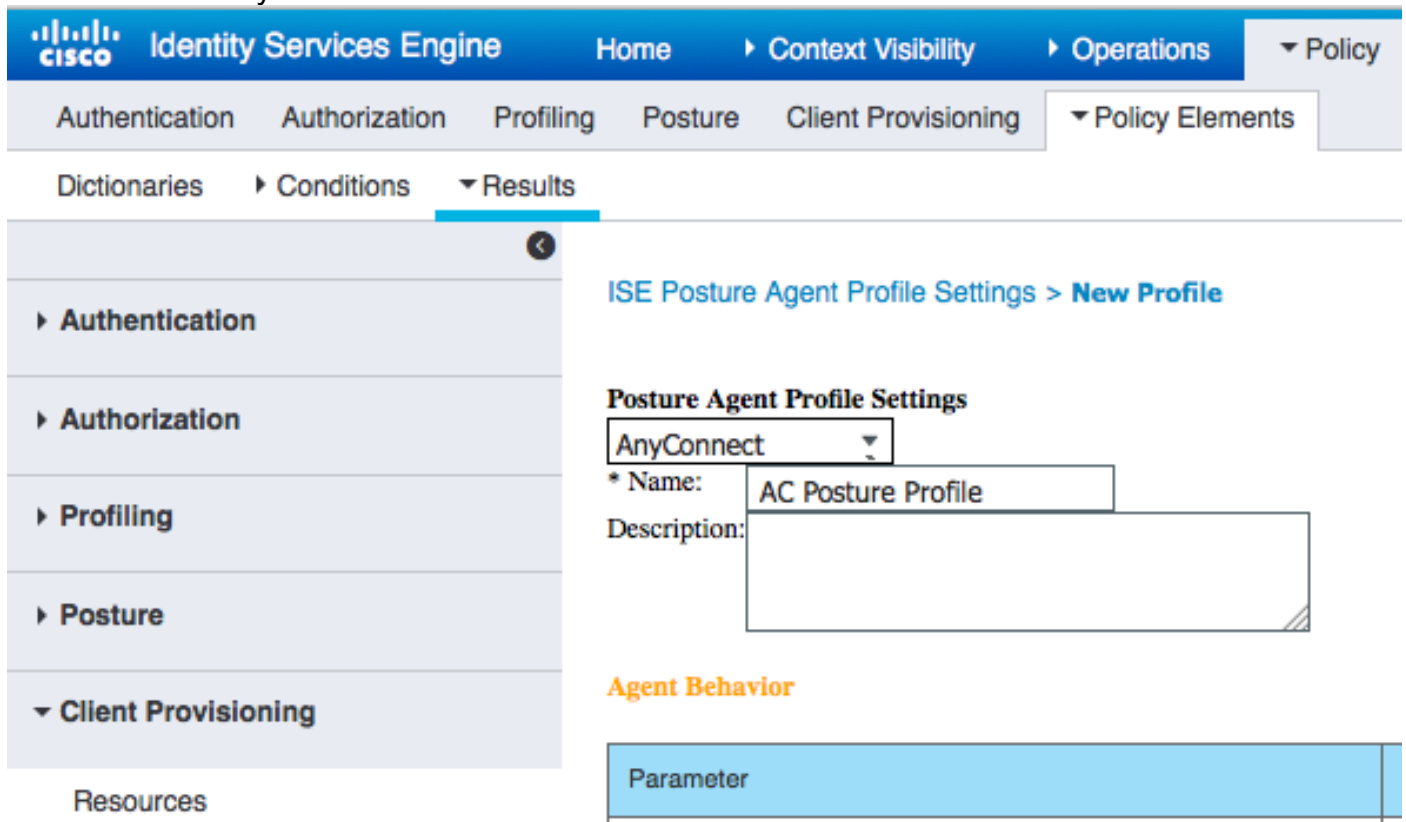
Name	Operating Systems	Compliance Module	Conditions	Remediation Actions
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	met if ANY_av_win_inst	then Message Text Only
File_Requirement	for Windows All	using Any version	met if File_Condition	then Message Text Only
Any_AV_Definition_Win	for 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

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

### 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

## 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.

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 'Policy' menu is expanded to show 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. The 'Results' sub-menu is selected. The left sidebar shows a navigation tree with 'Authentication', 'Authorization', 'Profiling', 'Posture', and 'Client Provisioning' (which is expanded to show 'Resources'). The main content area is titled 'AMP Enabler Profile Settings > New Profile' and 'AMP Enabler Profile'. It contains the following fields and options:

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

## 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**

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

Agent Resources From Local Disk > Agent Resources From Local Disk

### Agent Resources From Local Disk

Category: Cisco Provided Packages

Browse... anyconnect-win-4.2.02075-k9.pkg

AnyConnect Uploaded Resources			
Name	Type	Version	Description
AnyConnectDesktopWindows 4.2.2075.0	AnyConnectDesktopWindows	4.2.2075.0	AnyConnect Secure Mobility Clen...

Submit Cancel

- 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**

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

Agent Resources From Local Disk > Agent Resources From Local Disk

### Agent Resources From Local Disk

Category: Customer Created Packages

Type: AnyConnect Profile

\* Name: VPNDisable\_ServiceProfile

Description: [Empty text area]

Browse... VPNDisable\_ServiceProfile.xml

Submit Cancel

**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**

**Download Remote Resources** ✕

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

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

### 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



The screenshot shows the configuration page for 'AnyConnect Configuration AMP' in the Cisco Identity Services Engine. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Elements > Client Provisioning > Results > AnyConnect Configuration > AnyConnect Configuration AMP.

Configuration details:

- Select AnyConnect Package: AnyConnectDesktopWindows 4.2.2075.0
- Configuration Name: AnyConnect Configuration AMP
- Description: (empty text box)
- Description Value: (empty text box)
- Compliance Module: AnyConnectComplianceModuleWindows 3.6.10591.2

**AnyConnect Module Selection**

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

**Profile Selection**

- ISE Posture: AC Posture Profile
- VPN: VPNDisable\_ServiceProfile
- Network Access Manager: (empty dropdown)
- Web Security: (empty dropdown)
- AMP Enabler: AMP Profile
- Network Visibility: (empty dropdown)
- Customer Feedback: (empty dropdown)

## Passaggio 5. Configurazione delle regole di provisioning client

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

The screenshot shows the 'Client Provisioning Policy' configuration page. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Elements > 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

## 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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary 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 =

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

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 <b>Blacklist</b> AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if <b>Cisco-IP-Phone</b>	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

## 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**.

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

## Passaggio 8. Configurare l'adattatore AMP

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

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

Vendor \* AMP : THREAT

Instance Name \* AMP\_THREAT

Cancel Save

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

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

<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

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

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 > AMP

Cloud  
US Cloud  
Which public cloud would you like to connect to

Cancel Next

Fare clic sul collegamento FireAMP e accedere come admin in 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=mbga79xvh3tq7aafywt7yhsb90kz5p&response\\_type=code&redirect\\_uri=https://ise21-3ek.example.com/admin/vrfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize&scope=recv\\_events](https://api.amp.sourcefire.com/authorize?client_id=mbga79xvh3tq7aafywt7yhsb90kz5p&response_type=code&redirect_uri=https://ise21-3ek.example.com/admin/vrfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize&scope=recv_events)

Cancel

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

The screenshot shows the Cisco AMP for Endpoints console. At the top, there's a navigation bar with the Cisco logo and 'AMP for Endpoints'. Below that, a dashboard menu includes 'Dashboard', 'Analysis', 'Outbreak Control', 'Reports', 'Management', and 'Accounts'. A search bar is also present. The main content area is titled 'Applications' and displays an authorization request from the AMP Adaptor 62f6204b-751f-4ef5-9d93-e9f02500d842 (IRF) Defense Center. The request is for 'Streaming event export'. There are 'Allow' and 'Deny' buttons. Below this, there's a section for 'Event Export Groups' with a note that all groups are selected. A list of groups is shown, including Audit, Domain Controller, Protect, Server, and Triage. Each group has a description like 'Audit Group for Cisco - ekomeyc'.

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.

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

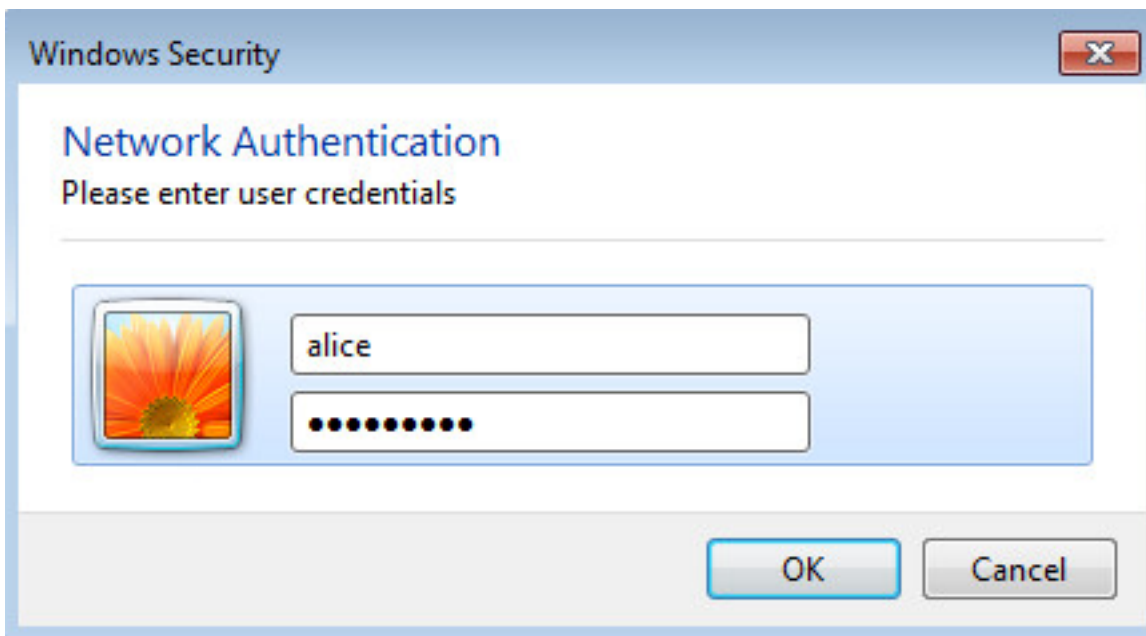
Refresh Add Trash Edit Filter Settings

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

## Verifica

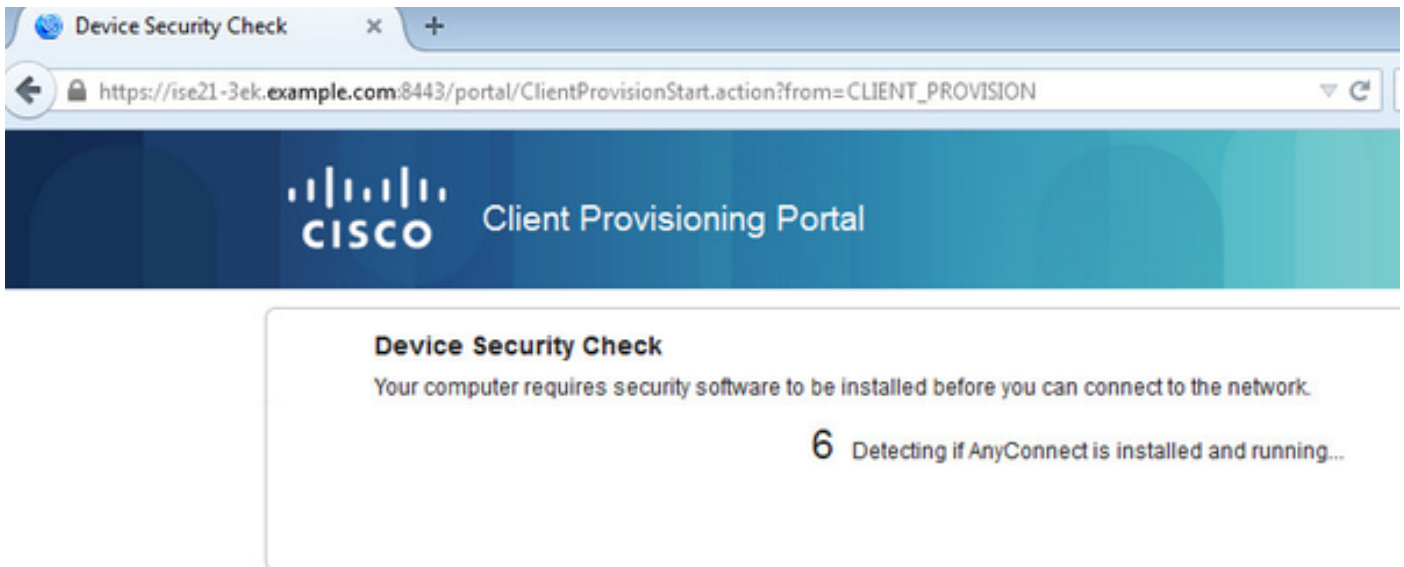
## Endpoint

Connettersi alla rete wireless tramite PEAP (MSCHAPv2).

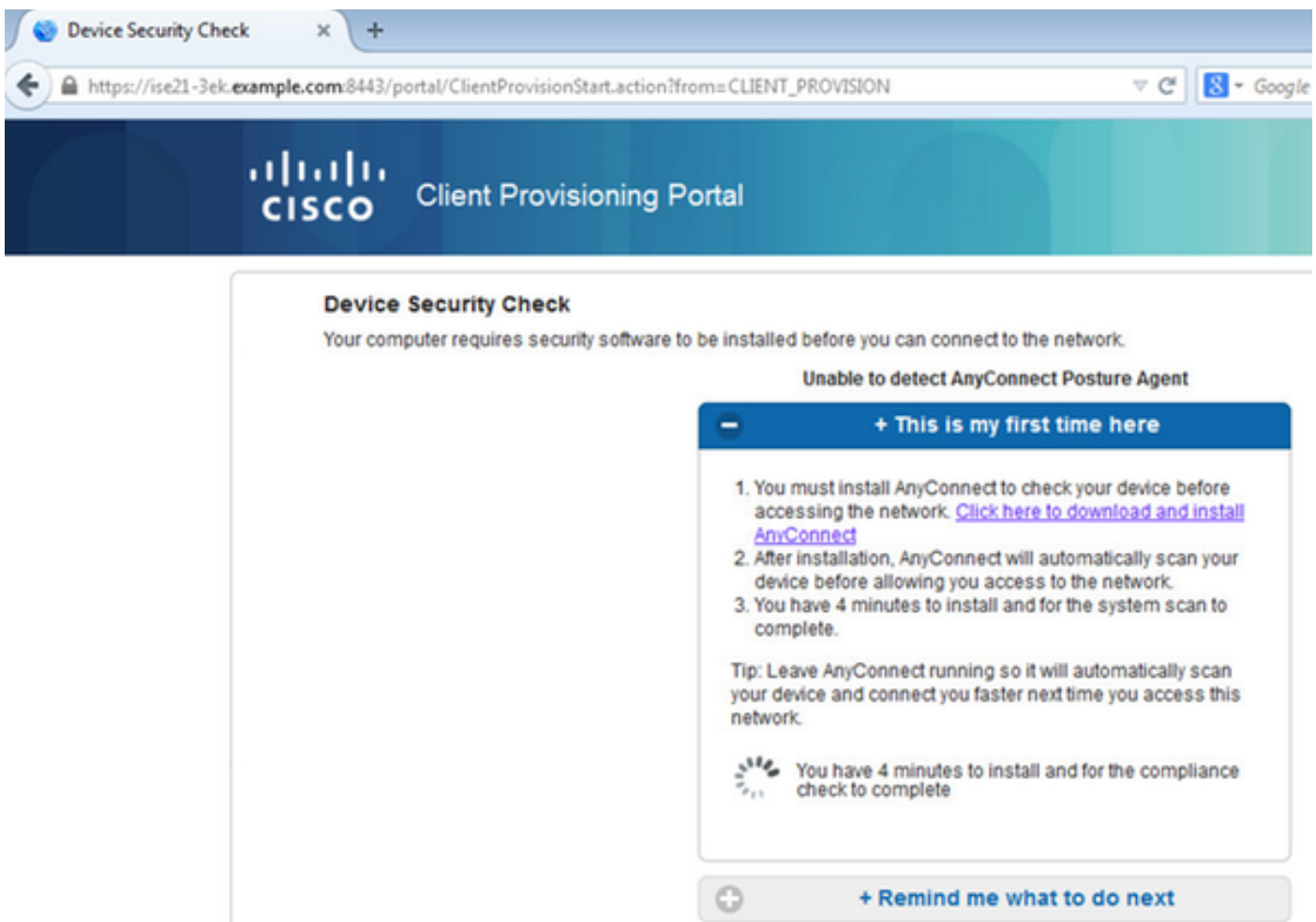


Una volta stabilita la connessione, viene eseguito il reindirizzamento al portale di provisioning client.

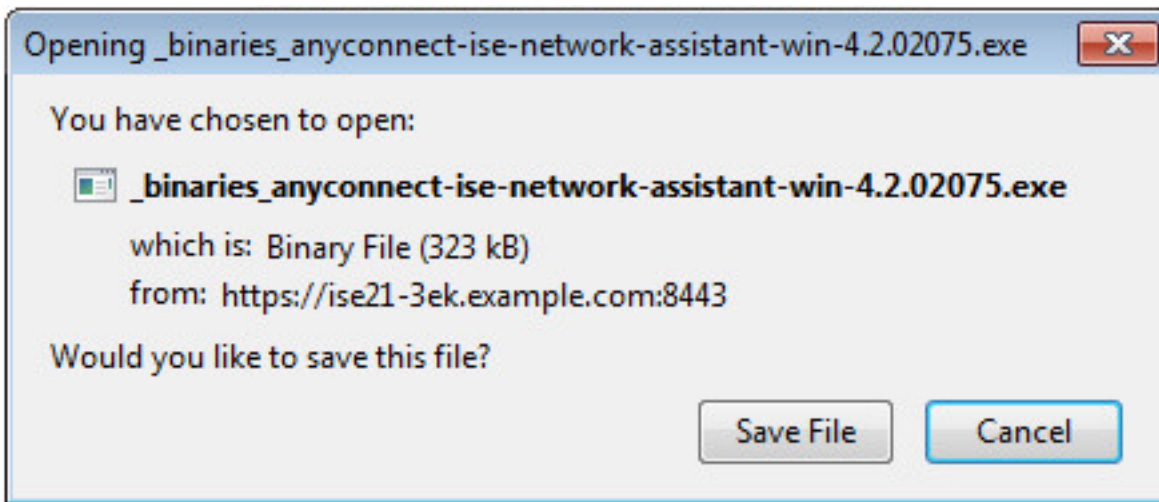




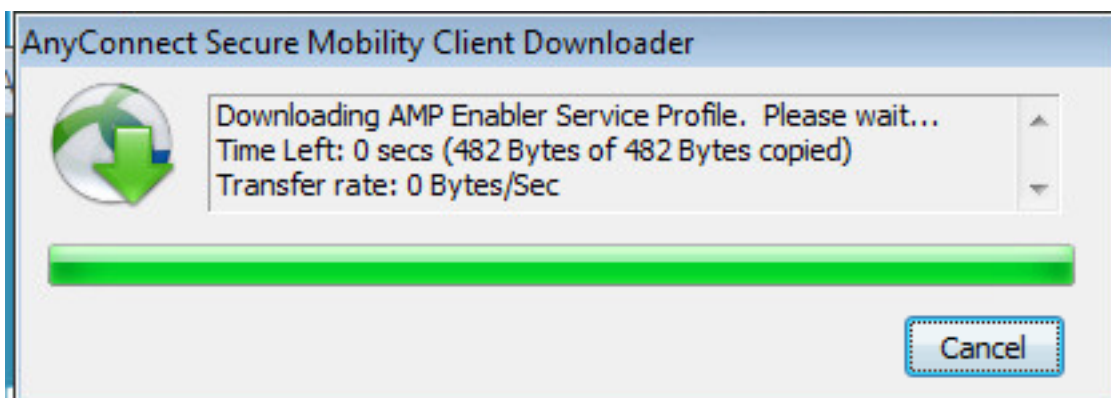
Poiché sul computer client non è installato nulla, ISE richiede l'installazione del client AnyConnect.

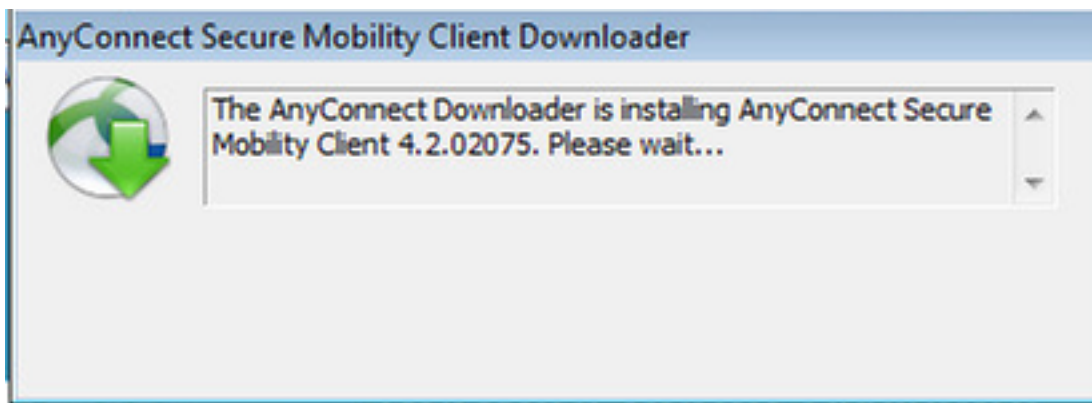


L'applicazione NSA (Network Setup Assistant) deve essere scaricata ed eseguita dal computer client.

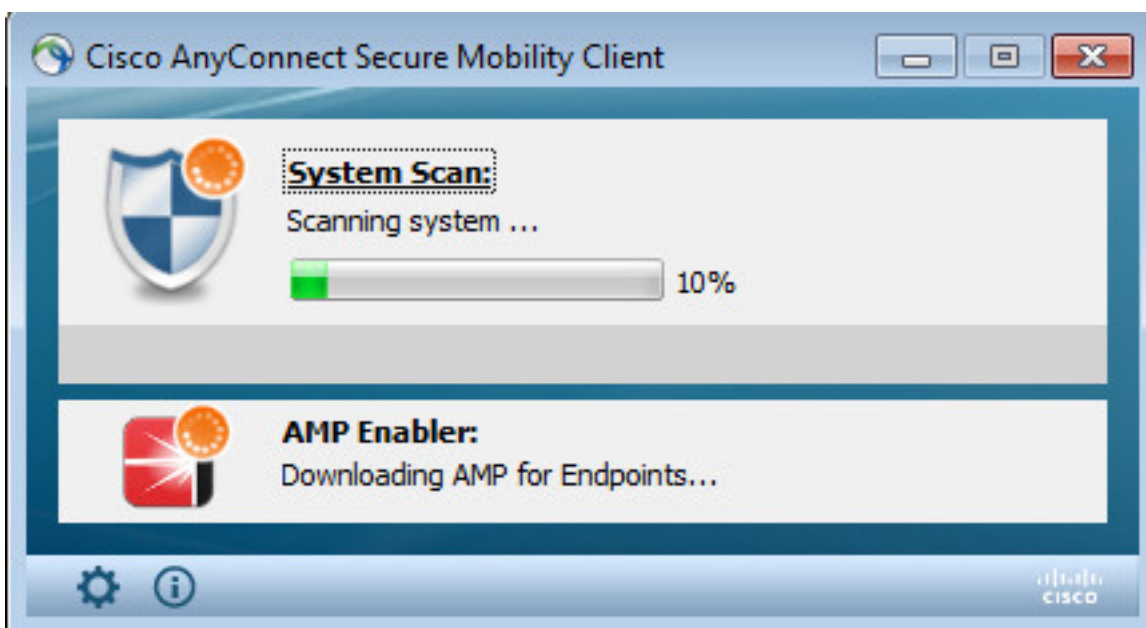
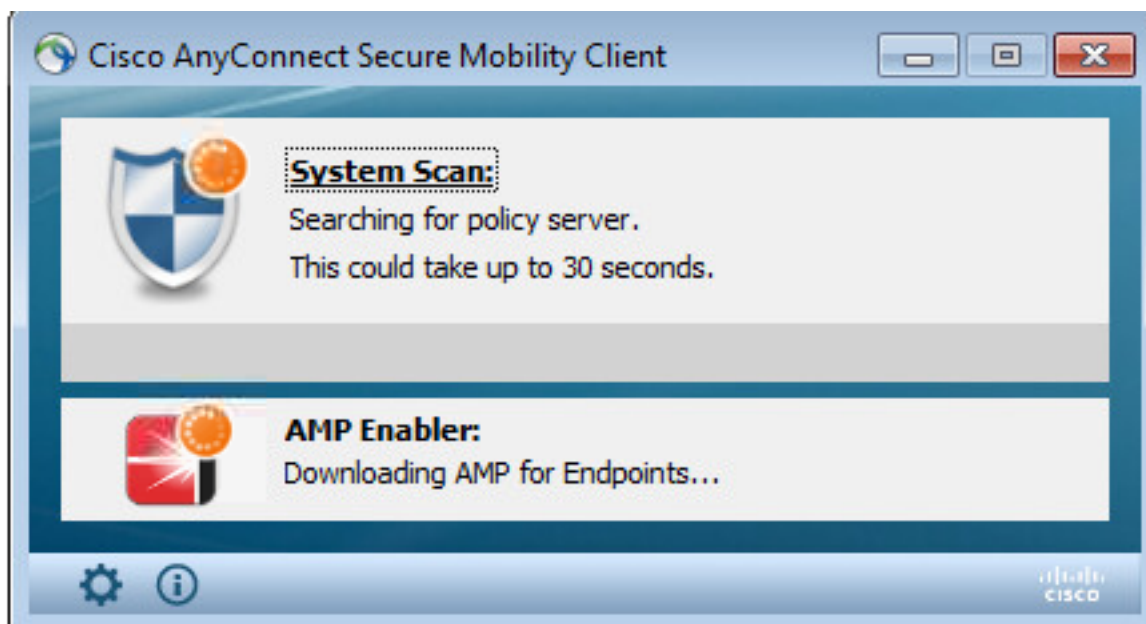


NSA si occupa di installare i componenti e i profili richiesti.

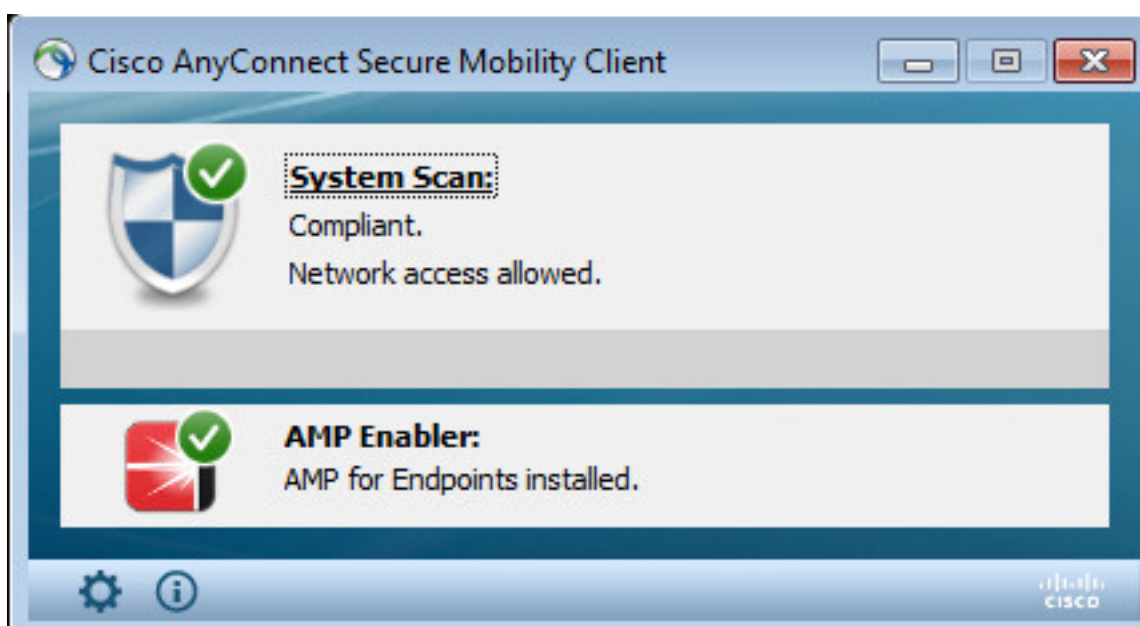
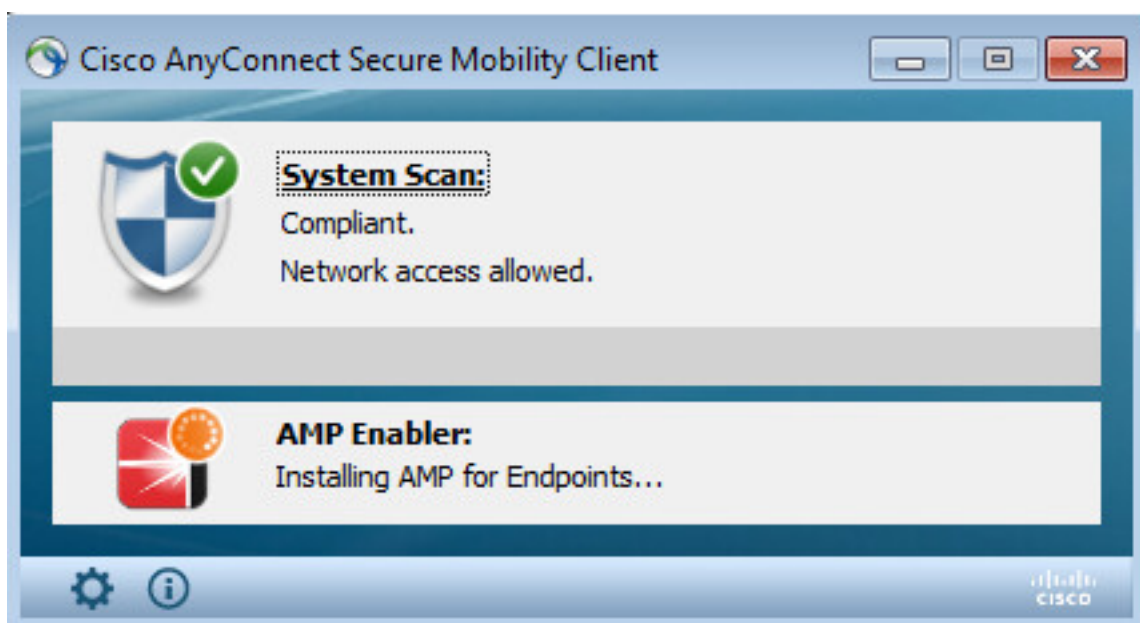
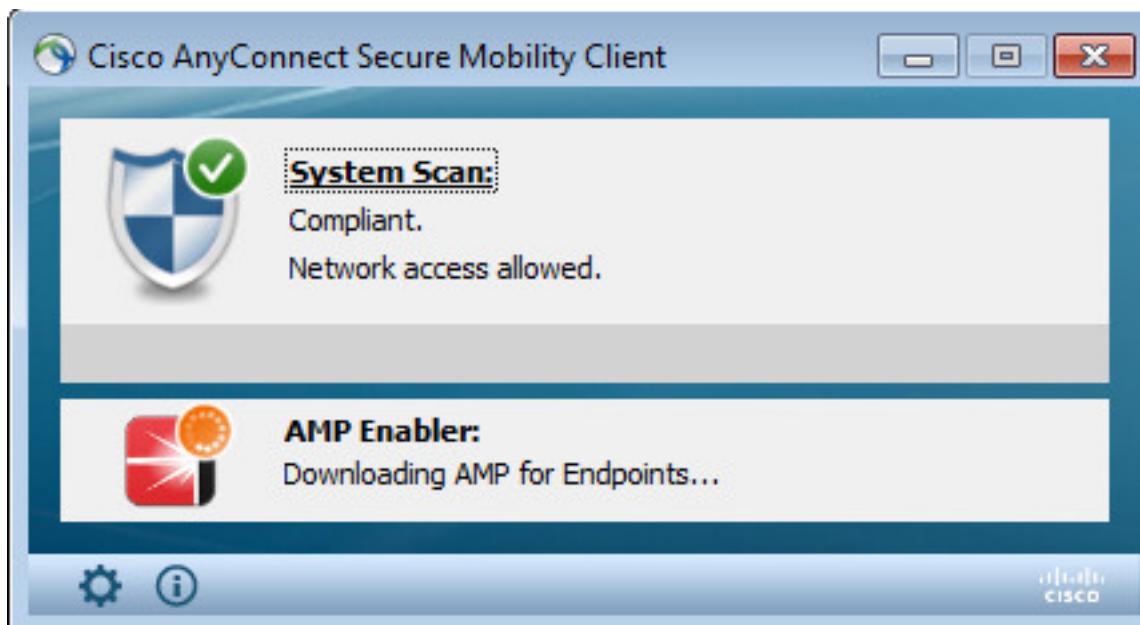




Al termine dell'installazione, il modulo AnyConnect Posture esegue il controllo della conformità.



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.

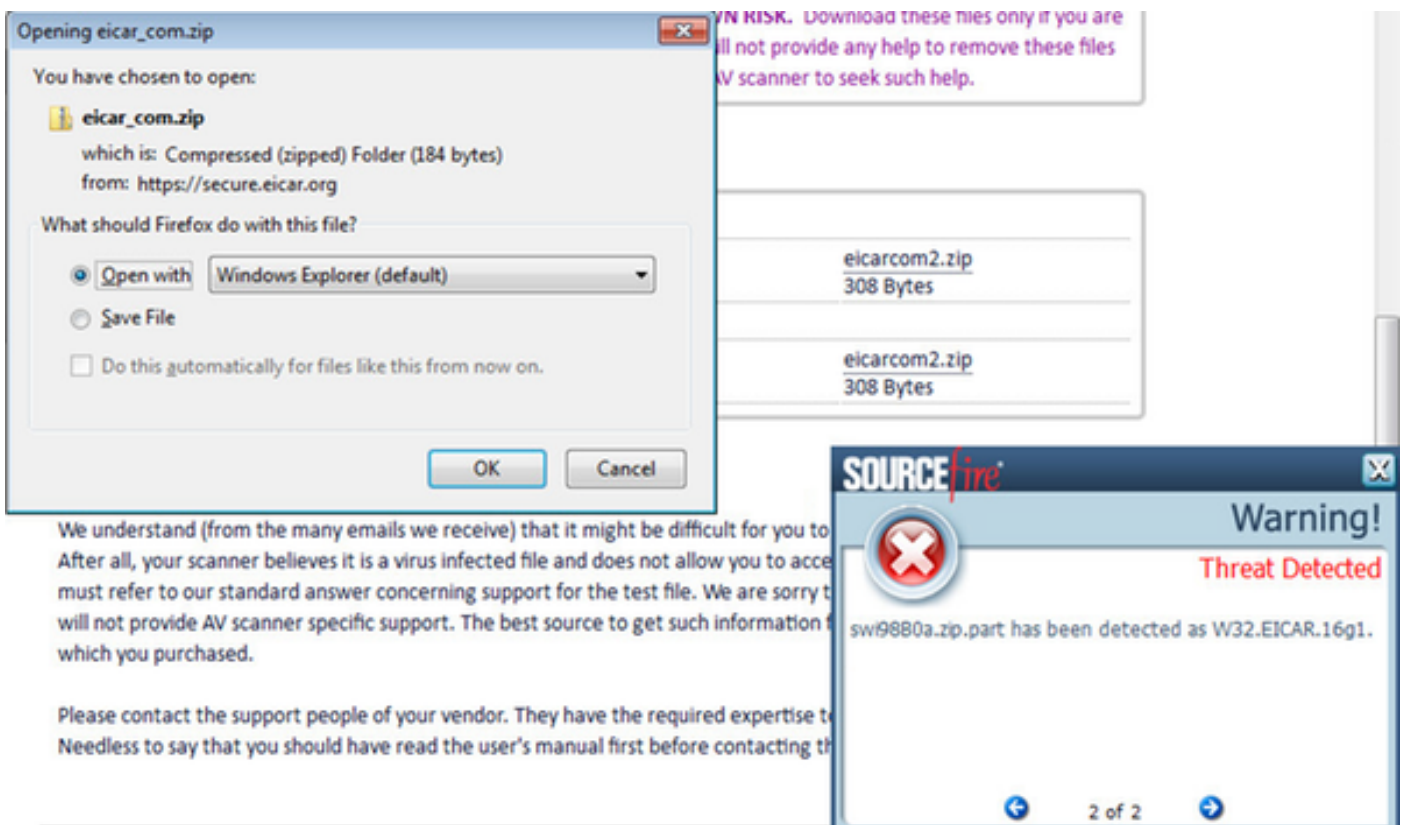


Viene visualizzato il connettore AMP.





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.

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):** No recent network threat detections to display.
- Network Threats (7 days):** No recent network threat detections to display.

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.

The detailed view shows the following information:

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

Field	Value
Detection	W32.EICAR.16g1
Fingerprint (SHA-256)	2546d0ff...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

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



## Applications

AMP Adaptor 4d4047dc-4791-477d-955f-6a0f182ae65b IRF	<a href="#">Edit</a> <a href="#">Deregister</a>
AMP Adaptor fe80e16e-cde8-4d7f-a836-545416ae56f4 IRF	<a href="#">Edit</a> <a href="#">Deregister</a>

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

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.

Summary Metrics:

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

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Jun 30, 2016 05:50:18.729 PM	<span style="color: blue;">●</span>		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	<span style="color: green;">●</span>			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Compliant_Device_A...	PermitAccess	
Jun 30, 2016 05:49:34.437 PM	<span style="color: green;">●</span>			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Non_Compliant_Devis...	AMP_Profile	
Jun 30, 2016 05:42:56.526 PM	<span style="color: green;">●</span>			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Non_Compliant_Devis...	AMP_Profile	

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

COMPROMISED ENDPOINTS BY INCIDENTS

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

COMPROMISED ENDPOINTS BY INDICATORS

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

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

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

**Identity Services Engine** Home Context Visibility Operations Policy Administration Work Centers

Endpoints Network Devices

Endpoints > C0:4A:00:14:8D:4B

C0:4A:00:14:8D:4B

MAC Address: C0:4A:00:14:8D:4B  
 Username: **alice**  
 Endpoint Profile: **Windows7-Workstation**  
 Current IP Address: **10.62.148.26**  
 Location:

Attributes Authentication **Threats** Vulnerabilities

**Threat Detected**

Type: INCIDENT  
 Severity: Painful  
 Reported by: AMP  
 Reported at: 2016-06-30 11:27:48

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.

**Identity Services Engine** Home Context Visibility Operations Policy Administration Work Centers

Endpoints Network Devices

Authentication BYOD Compliance **Compromised Endpoints** Endpoint Classification Guest Vulnerable Endpoints

COMPROMISED ENDPOINTS BY INCIDENTS  
 All endpoints | Connected | Documented

Unknown Insignificant Distracting **Painful** Damaging Catastrophic  
 IMPACT LEVEL

COMPROMISED ENDPOINTS BY INDICATORS  
 All endpoints | Connected | Documented

Unknown None Low Medium High  
 LIKELY IMPACT LEVEL

1 Selected Rows/Page 2

Refresh Add Trash Edit ANC **Change Authorization** Clear Threats & Vulnerabilities Export Import MDM Actions Revoke Certificate

MAC Address	Username	Source	Threat Severity	Logical NAD Location	Connectivity	Hostname	Identity Group	Endpoint OS
24:77:03:3D:CF:20	notHARISHA-PC.aka...	AMP	Painful	Location#AI Locations	Disconnected		Workstation	
C0:4A:00:14:8D:4B	alice	AMP	Painful	Location#AI Locations	Connected		Workstation	

CoA Session Result  
 CoA Session Terminate  
 CoA Port Bounce  
 CoA SNAnt Session Query  
 CoA Session termination with port bounce  
 CoA Session termination with port shutdown

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**

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Administration > 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 features an "Edit" button and a "Reset to Default" button. Below this is a table with columns for 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

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 sospenso:  
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}
```