

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

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Fluxo detalhado](#)

[Configurar a nuvem AMP](#)

[Etapa 1. Conector da transferência da nuvem AMP](#)

[Configurar o ISE](#)

[Etapa 1. Configurar políticas e condições da postura](#)

[Etapa 2. Configurar o perfil da postura](#)

[Etapa 3. Configurar o perfil AMP](#)

[Etapa 2. Aplicativos da transferência de arquivo pela rede e perfil XML ao ISE](#)

[Etapa 3. Módulo da conformidade de AnyConnect da transferência](#)

[Etapa 4. Adicionar a configuração de AnyConnect](#)

[Etapa 5. Configurar regras do abastecimento do cliente](#)

[Etapa 6. Configurar políticas da autorização](#)

[Etapa 7. Permita serviços TC-NAC](#)

[Etapa 8. Configurar o adaptador AMP](#)

[Verificar](#)

[Valor-limite](#)

[Nuvem AMP](#)

[ISE](#)

[Troubleshooting](#)

Introdução

Este original descreve como configurar o NAC Ameaça-cêntrico 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.

The screenshot shows the Cisco 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 links for '3 Installs', '1 detection (7 days)', 'Announcements', 'Support', 'Help', 'My Account', and 'Log Out'. Below the navigation bar, there is a search bar and a 'Download Connector' section. A dropdown menu is set to 'Audit'. There are four connector cards: 'FireAMP Windows' (with 'No computers require updates' and audit policy options), 'FireAMP Mac', 'FireAMP Linux', and 'FireAMP Android'. Each card has a 'Download' button and a 'Show URL' button.

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:

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

Esta circunstância é usada para uma exigência:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

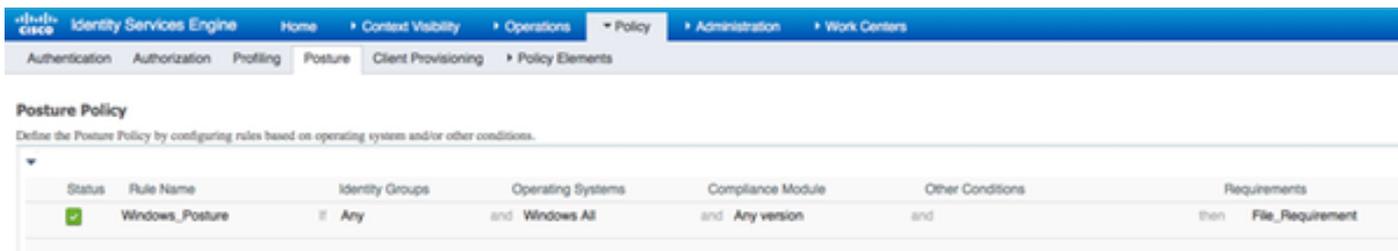
Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Requirements

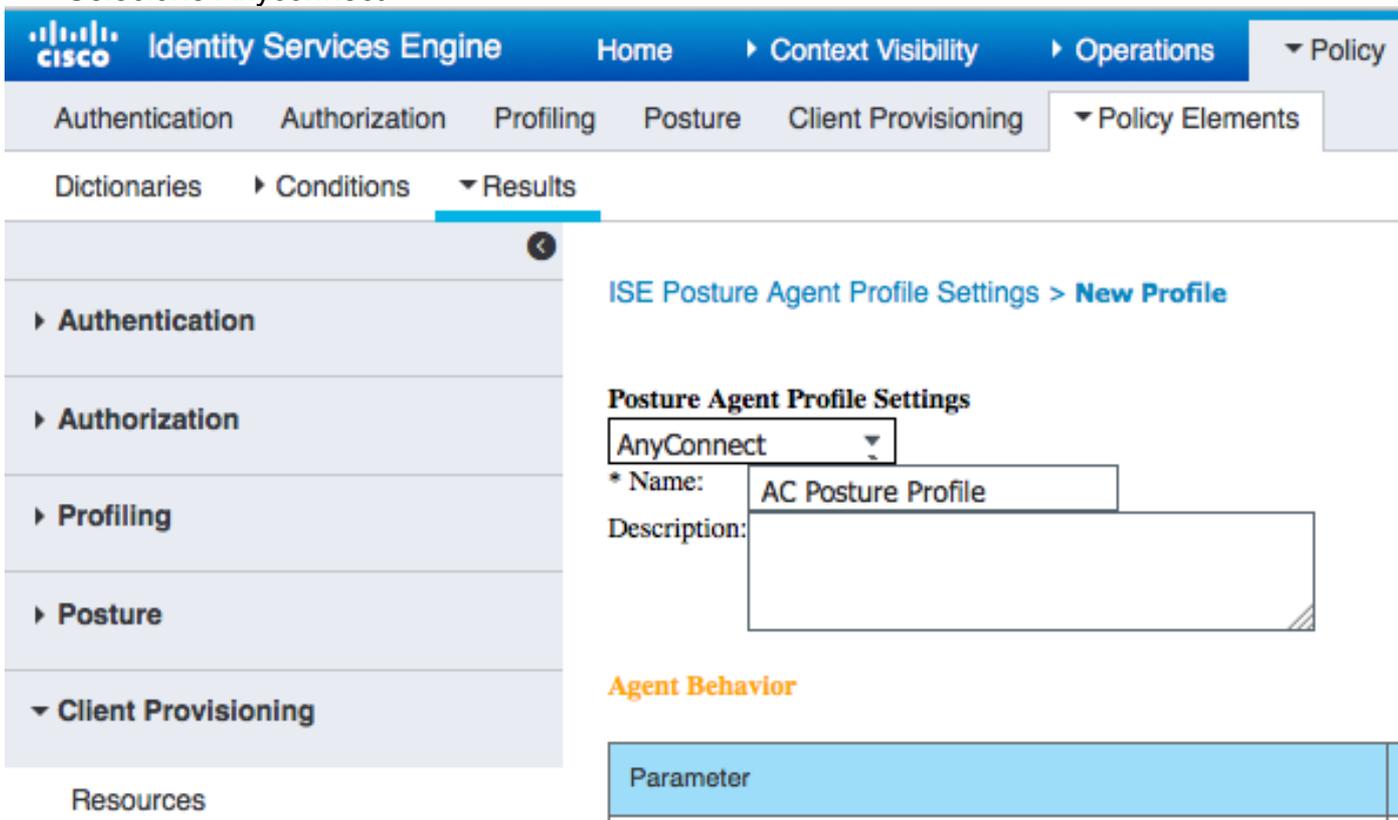
Name	Operating Systems	Compliance Module	Conditions	Remediation Actions
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	met if ANY_av_win_inst	then Message Text Only
File_Requirement	for Windows All	using Any version	met if File_Condition	then Message Text Only
Any_AV_Definition_Win	for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

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

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

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.

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

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

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** seletor

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

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...	AnyConnectDesktopWindows	4.2.2075.0	AnyConnect Secure Mobility Clen...

Submit Cancel

- 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**

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

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:

Browse... VPNDisable_ServiceProfile.xml

Submit Cancel

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**

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 releas
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE 1.2 releas
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE 1.2 releas
<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

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**

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
Windows_Posture_AMP	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration AMP

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > AMP_Profile

Authorization Profile

* Name AMP_Profile

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL ACL_WEBAUTH_REDIRECT Value Client Provisioning Portal (defa

Display Certificates Renewal Message

Static IP/Host name/FQDN

Advanced Attributes Settings

Select an item =

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

Authorization Policy

Define the Authorization Policy by configuring rules based on Identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

Exceptions (1)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
2. <input checked="" type="checkbox"/>	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
1. <input checked="" type="checkbox"/>	Non_Compliant_Devices_Access	if Session:PostureStatus NOT_EQUALS Compliant	then AMP_Profile
<input type="checkbox"/>	Employee_EAP-TLS	if (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD
<input type="checkbox"/>	Employee_Onboarding	if (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD
<input checked="" type="checkbox"/>	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests
<input checked="" type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then VA_Scan
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

Etapa 7. Permite serviços TC-NAC

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

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** Make Primary

Monitoring Role **PRIMARY** Persons Other Monitoring Node

Policy Service

Enable Session Services i Include Node in Node Group **None** i

Enable Profiling Service

Enable Threat Centric NAC Service i

Etapa 8. Configurar o adaptador AMP

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

The screenshot shows the 'Third Party Vendors' page in the Cisco Identity Services Engine. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Threat Centric NAC. The page title is 'Third Party Vendors'. Below the title, it says 'Vendor Instances > New' and 'Input fields marked with an asterisk (*) are required.' There are two input fields: 'Vendor *' with a dropdown menu showing 'AMP : THREAT' and 'Instance Name *' with a text box containing 'AMP_THREAT'. At the bottom, there are 'Cancel' and 'Save' buttons.

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

The screenshot shows the 'Third Party Vendors' page in the Cisco Identity Services Engine. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Threat Centric NAC. The page title is 'Third Party Vendors'. Below the title, it says 'Vendor Instances' and '0 Selected'. There are several action buttons: Refresh, Add, Trash, and Edit. There is also a Filter button and a settings icon. Below the buttons is a table with the following columns: Instance Name, Vendor Na..., Type, Hostname, Connectivity, and Status. The table contains two rows: 'QualysVA' with status 'Active' and 'AMP_THREAT' with status 'Ready to configure'.

Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
QualysVA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active
AMP_THREAT	AMP	THREAT		Disconnected	Ready to configure

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

The screenshot shows the 'Third Party Vendors' page in the Cisco Identity Services Engine. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Threat Centric NAC. The page title is 'Third Party Vendors'. Below the title, it says 'Vendor Instances > AMP'. There is a 'Cloud' dropdown menu with 'US Cloud' selected. Below the dropdown, it says 'Which public cloud would you like to connect to'. At the bottom, there are 'Cancel' and 'Next' buttons.

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

Third Party Vendors

Vendor Instances > AMP

root

SAS External URL

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

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

Cancel

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

The screenshot shows the Cisco AMP for Endpoints dashboard. At the top, there's a navigation bar with 'AMP for Endpoints' and various utility links like '3 Installs', '1 detection (7 days)', 'Announcements', 'Support', 'Help', 'My Account', and 'Log Out'. Below the navigation bar, there's a search bar and a menu with options like 'Dashboard', 'Analysis', 'Outbreak Control', 'Reports', 'Management', and 'Accounts'. The main content area is titled 'Applications' and contains a detailed authorization request. The request is from 'The AMP Adaptor 62f6204b-751f-4ef5-9d93-e9f02500d842 (IRF) Defense Center' and is asking for 'Streaming event export' permissions. Below the request, there are 'Allow' and 'Deny' buttons. A section titled 'Event Export Groups' indicates that 'All groups selected' and provides instructions on how to select specific groups. A list of available groups is shown, including 'Audit', 'Domain Controller', 'Protect', 'Server', and 'Triage'. Each group has a description, such as 'Audit Group for Cisco - ekomeyc'.

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.

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

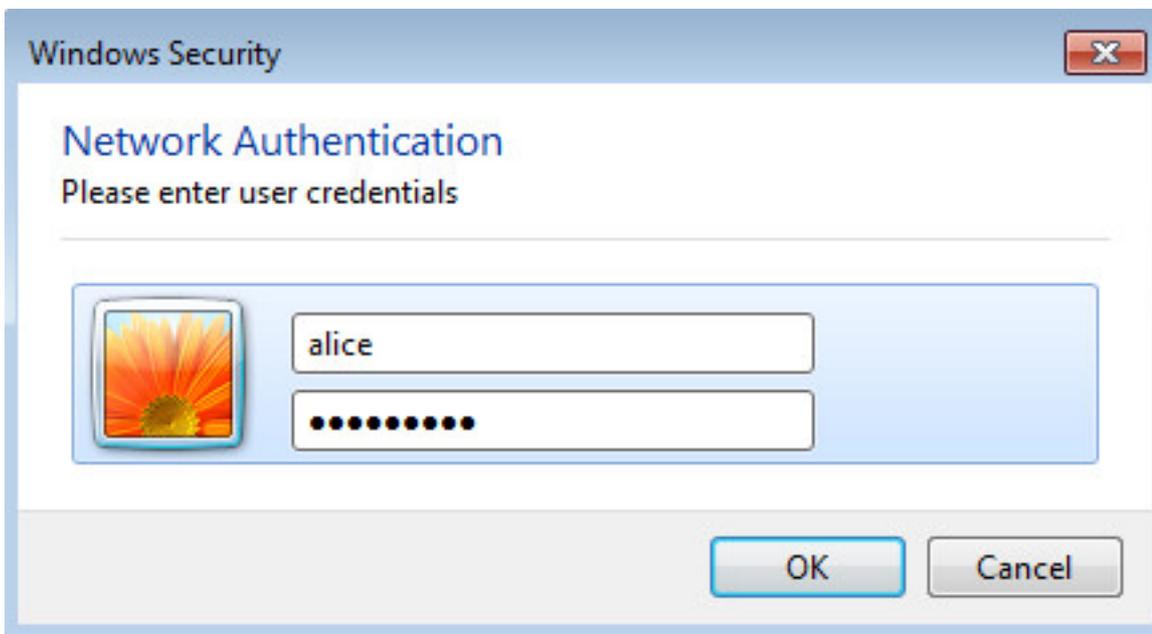
Refresh Add Trash Edit Filter Settings

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

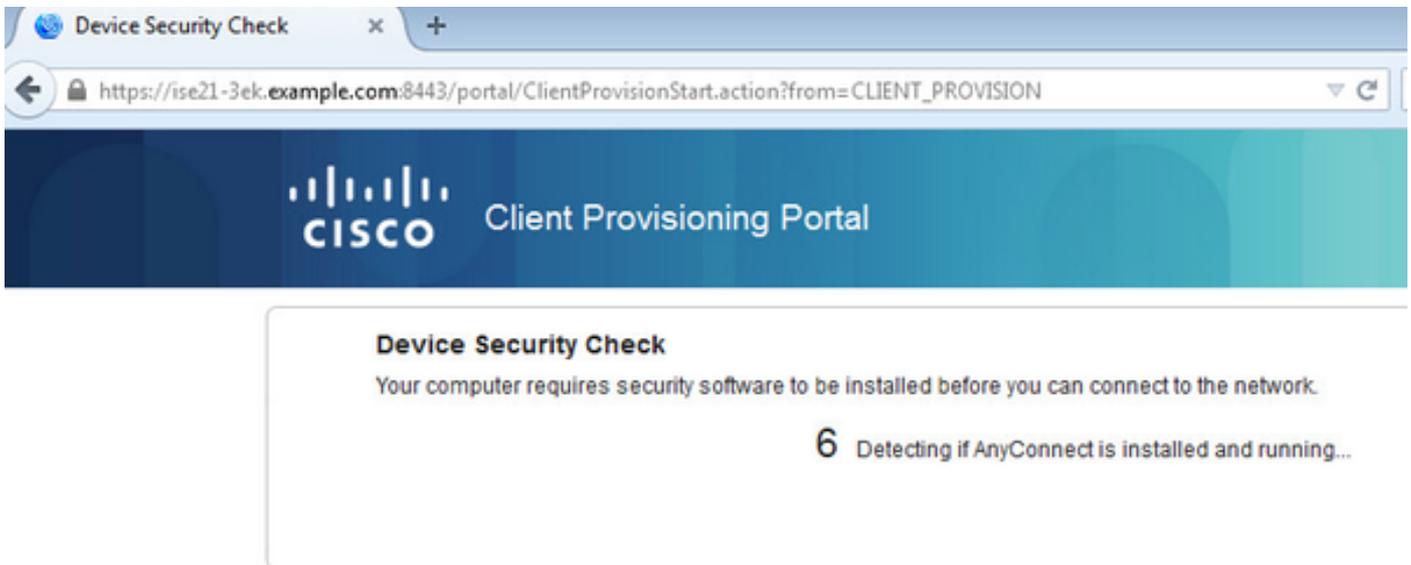
Verificar

Valor-limite

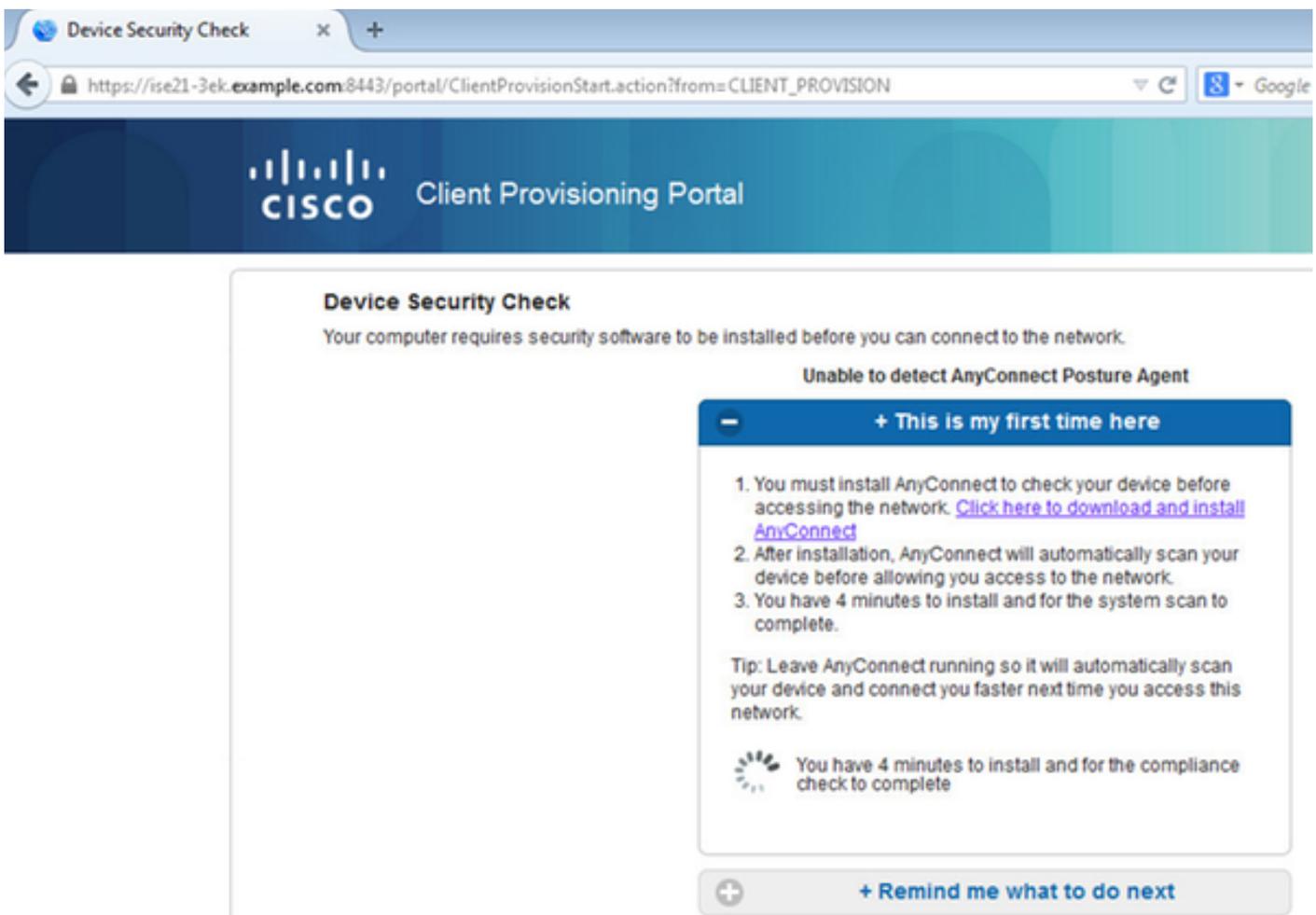
Conecte à rede Wireless através de PEAP (MSCHAPv2).



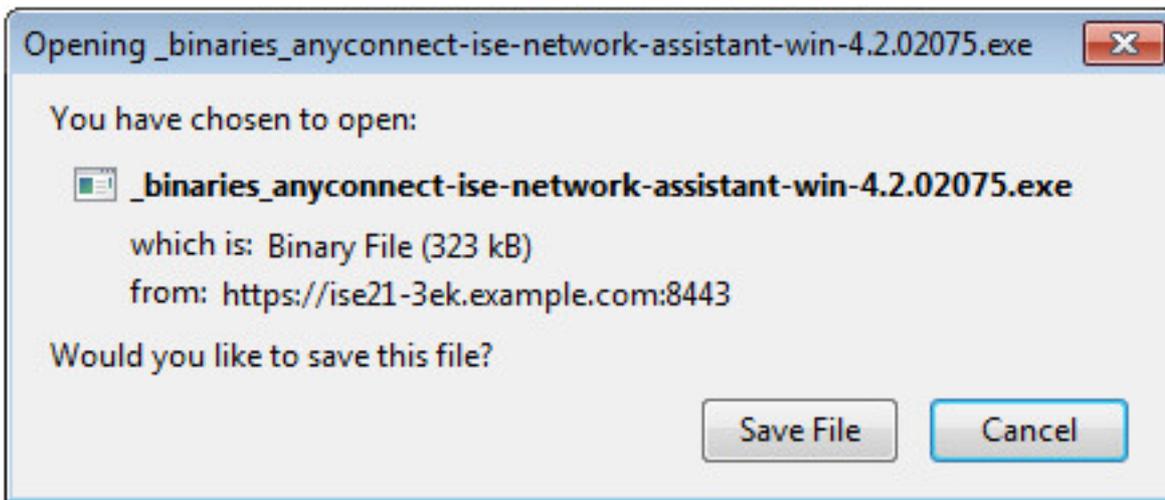
Uma vez que conectado a reorientação ao portal do abastecimento do cliente ocorre.



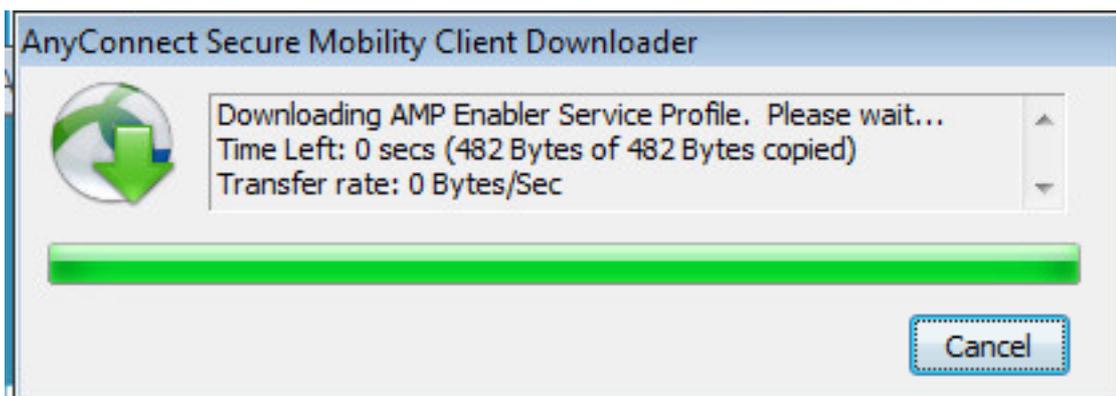
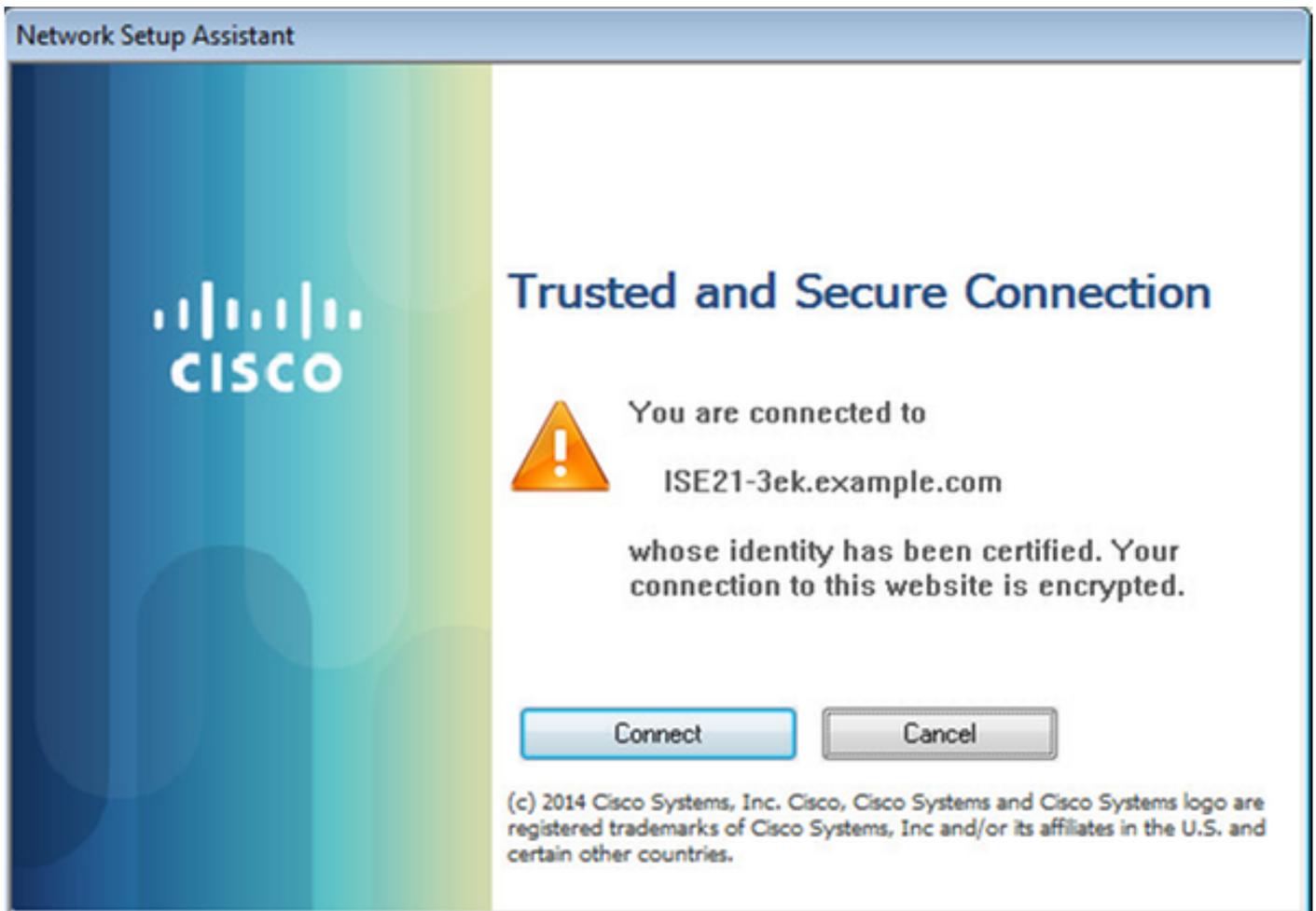
Desde que não há nada instalado na máquina cliente, o ISE alerta para a instalação de cliente de AnyConnect.

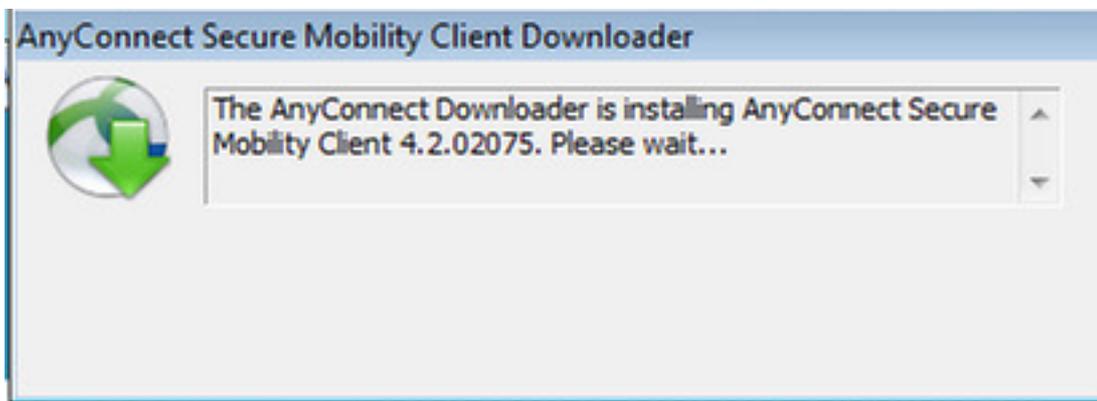


O aplicativo assistente da instalação de rede (NSA) deve ser transferido e corrida da máquina cliente.

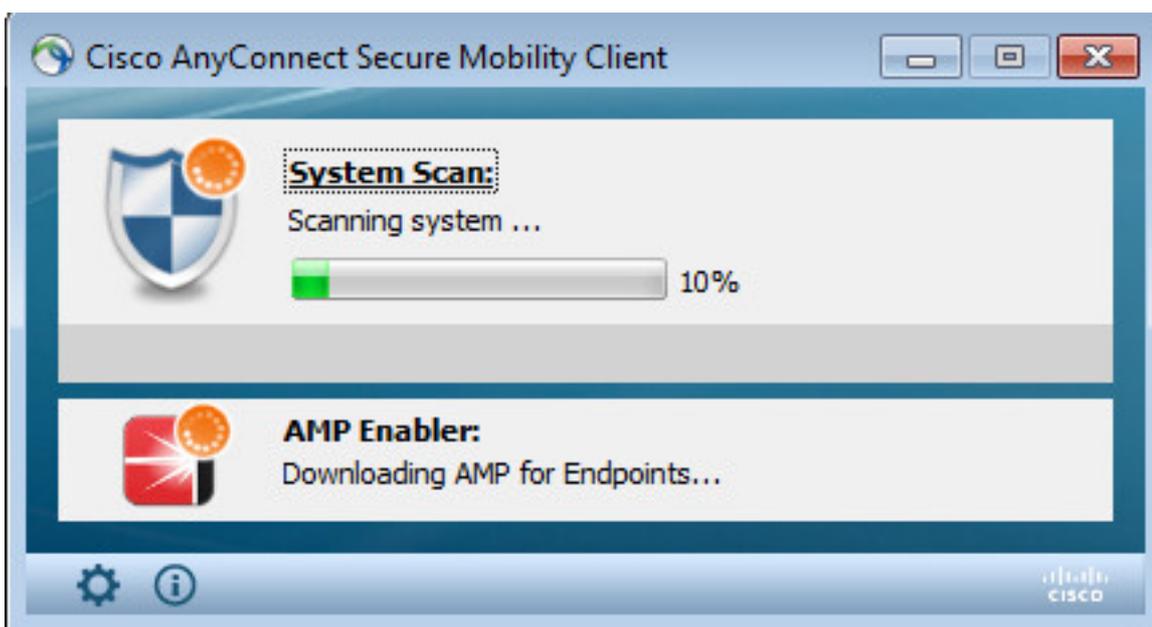
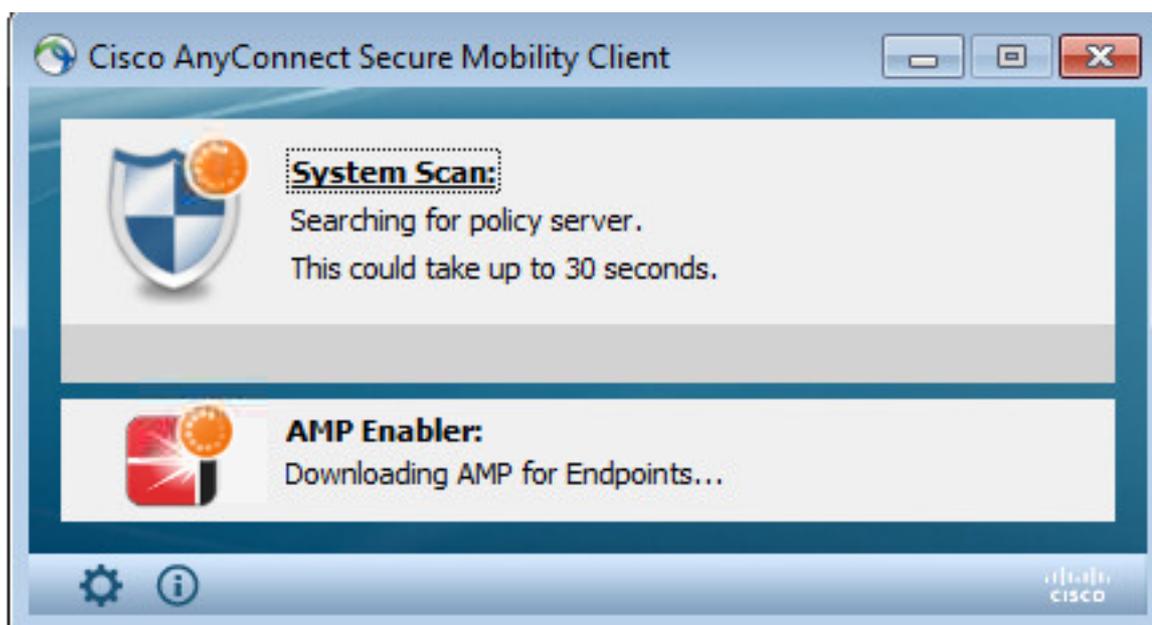


O NSA toma de instalar componentes requeridos e perfis.

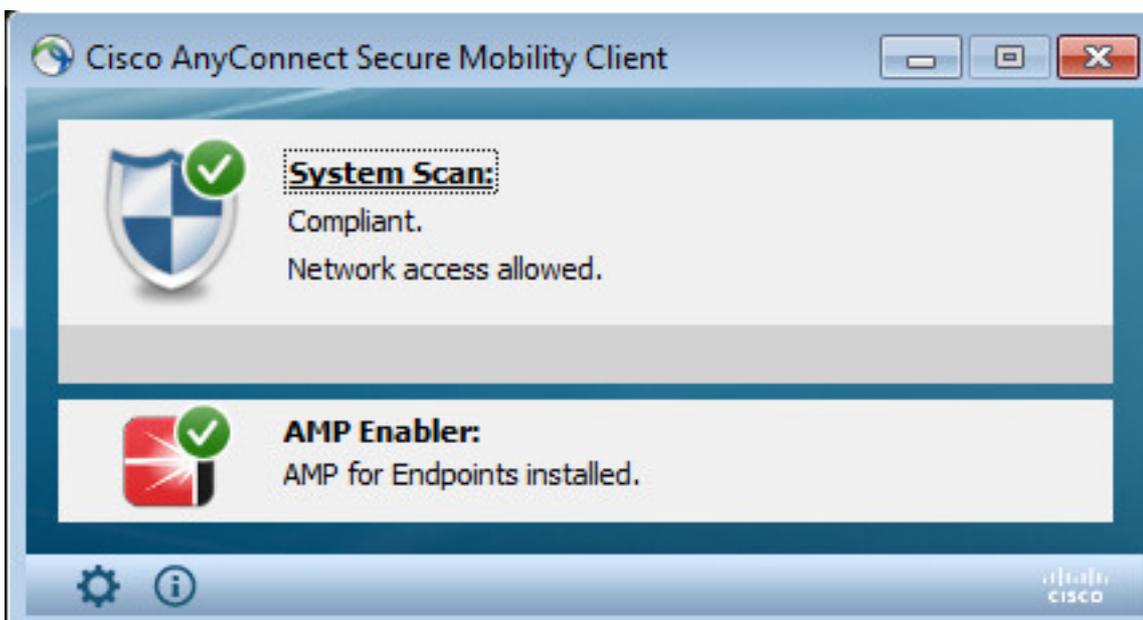
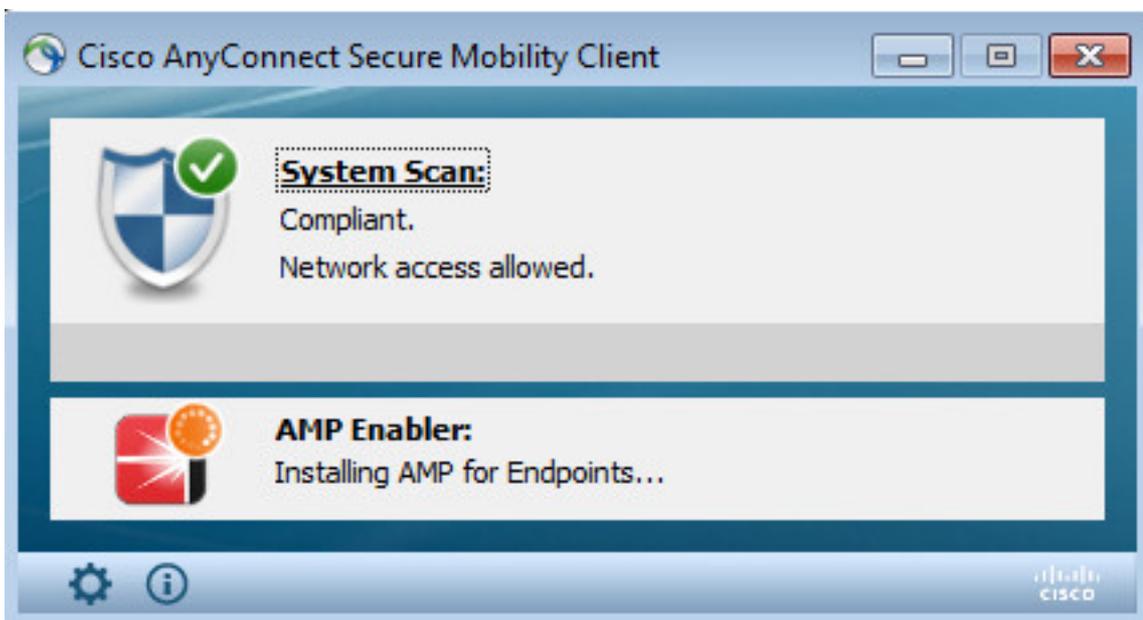
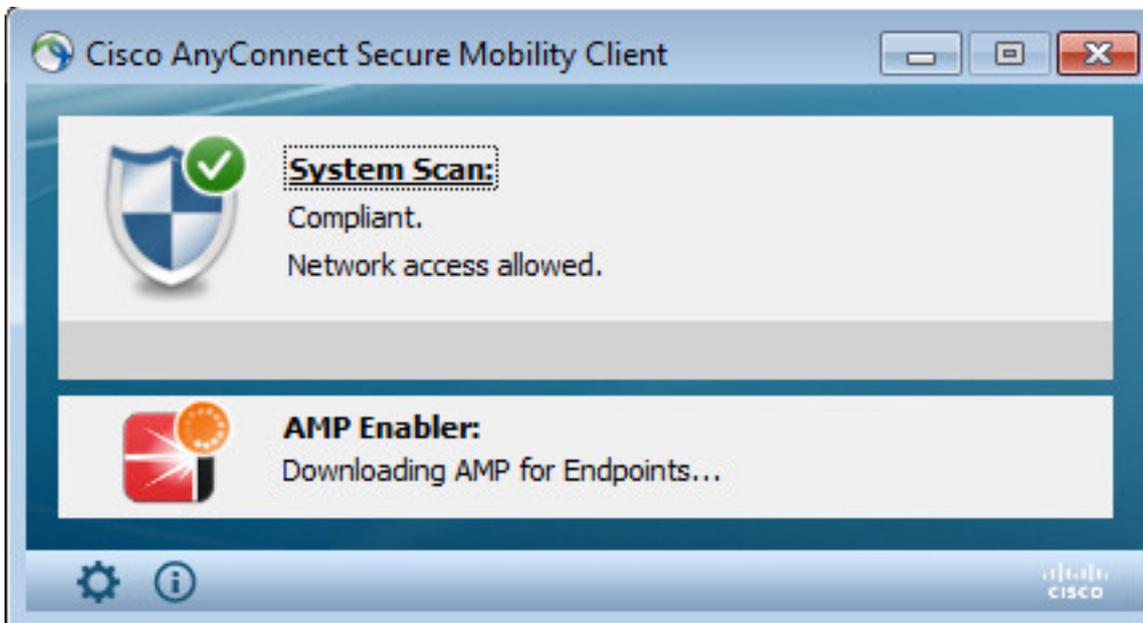




Uma vez que a instalação é terminada, o módulo da postura de AnyConnect executa a verificação da conformidade.



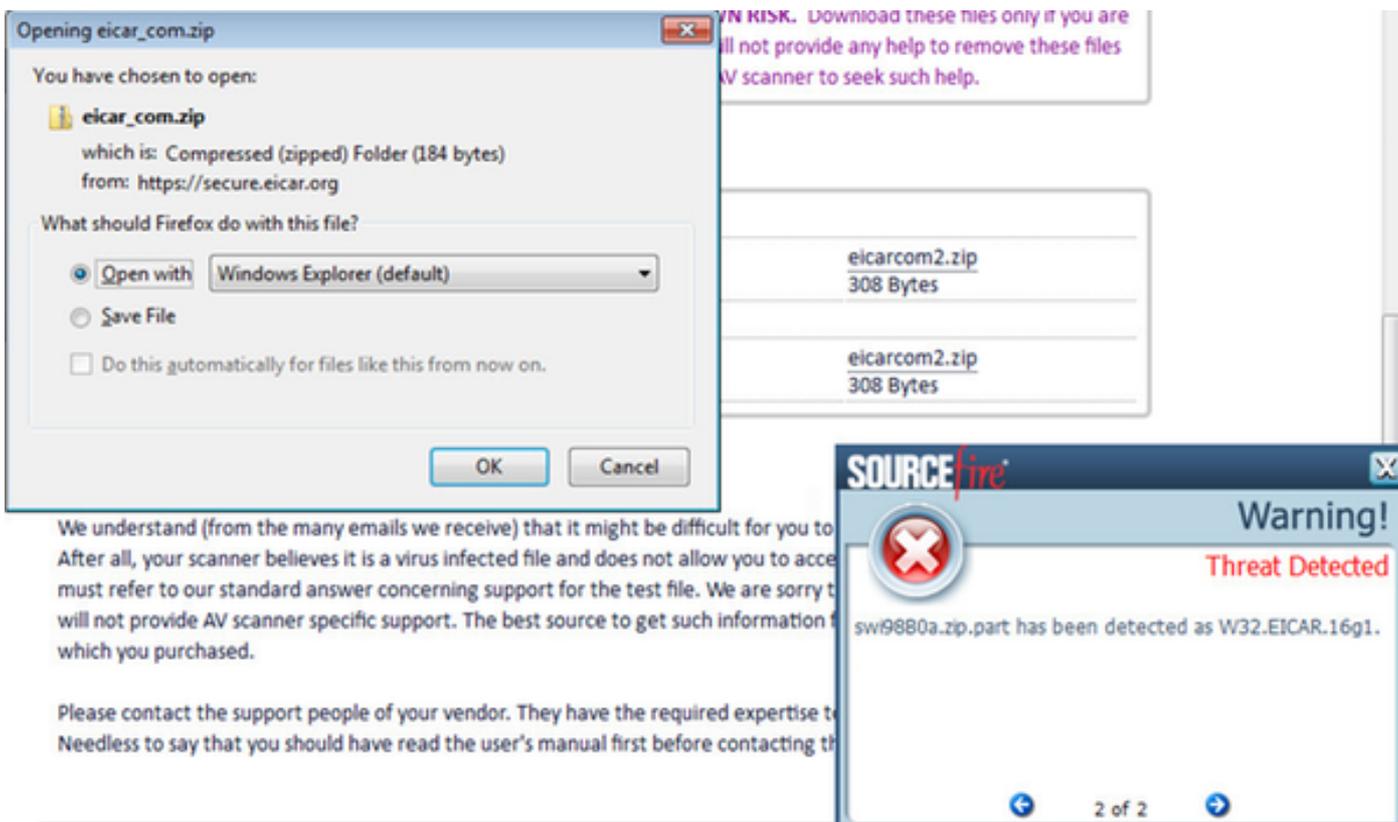
Porque o acesso direto está dado, se o valor-limite é complacente, o AMP está transferido e instalado do web server especificado mais cedo no perfil AMP.



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.



Nuven AMP

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

The dashboard displays several key metrics:

- 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.

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

The detailed view shows the following information:

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

Field	Value
Detection	W32.EICAR.16g1
Fingerprint (SHA-256)	2546dcff...6e9eedad
Filename	0M90PRxO.zip.part
Filepath	C:\Users\admin\AppData\Local\Temp\0M90PRxO.zip.part
File Size (bytes)	184
Parent Fingerprint (SHA-256)	3147bd8...32de89c2
Parent Filename	Firefox.exe

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

Applications

AMP Adaptor 4d4047dc-4791-477d-955f-6a0f182ae65b IRF	Edit Deregister
AMP Adaptor fe80e16e-cde8-4d7f-a836-545416ae56f4 IRF	Edit Deregister

These are applications external to FireAMP, such as Sourcefire's Defense Center, that you have authorized to access your business' data.

Here you can deauthorize registered applications, thus revoking their access to specific functionality, or you can deregister the applications, thus deauthorizing them and completely removing them from the FireAMP system.

You can currently authorize Defense Center appliances to receive streaming FireAMP events for integration with the Defense Center.

ISE

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.

Summary Statistics:

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

Time	Status	Details	Repeat	Identify	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Jun 30, 2016 05:50:18.729 PM	●		0	alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Compliant_Device_A...	PermitAccess	10.62.148.26
Jun 30, 2016 05:49:26.479 PM	●			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Compliant_Device_A...	PermitAccess	
Jun 30, 2016 05:49:34.437 PM	●			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Non_Compliant_Devis...	AMP_Profile	
Jun 30, 2016 05:42:56.536 PM	●			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Non_Compliant_Devis...	AMP_Profile	

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

COMPROMISED ENDPOINTS BY INCIDENTS

Unknown	Insignificant	Distracting	Painful	Damaging	Catastrophic
---------	---------------	-------------	---------	----------	--------------

COMPROMISED ENDPOINTS BY INDICATORS

Unknown	None	Low	Medium	High
---------	------	-----	--------	------

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

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

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Below this, there are tabs for 'Endpoints' and 'Network Devices'. The main content area shows the endpoint 'C0:4A:00:14:8D:4B' with a refresh, edit, and delete icon. Below the endpoint name, there is a laptop icon and the following details: 'MAC Address: C0:4A:00:14:8D:4B', 'Username: alice', 'Endpoint Profile: Windows7-Workstation', 'Current IP Address: 10.62.148.26', and 'Location:'. Below these details are tabs for 'Attributes', 'Authentication', 'Threats', and 'Vulnerabilities'. The 'Threats' tab is active, showing a 'Threat Detected' section with the following information: 'Type: INCIDENT', 'Severity: Painful', 'Reported by: AMP', and 'Reported at: 2016-06-30 11:27:48'.

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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Below this, there are tabs for 'Endpoints' and 'Network Devices'. The main content area shows two charts: 'COMPROMISED ENDPOINTS BY INCIDENTS' and 'COMPROMISED ENDPOINTS BY INDICATORS'. The 'COMPROMISED ENDPOINTS BY INCIDENTS' chart shows a bar for 'Painful' with a value of 1. The 'COMPROMISED ENDPOINTS BY INDICATORS' chart shows a bar for 'Painful' with a value of 1. Below the charts, there is a table with 1 selected row. The table has columns for 'Source', 'Threat Severity', 'Logical NAD Location', 'Connectivity', 'Hostname', 'Identity Group', and 'Endpoint OS'. The selected row is for 'C0:4A:00:14:8D:4B' with a threat severity of 'Painful' and connectivity of 'Connected'. A dropdown menu is open over the 'Change Authorization' button, showing options: 'CoA Session Result', 'CoA Session Terminate', 'CoA Port Bounce', 'CoA SNAnt Session Query', 'CoA Session termination with port bounce', and 'CoA Session termination with port shutdown'.

Se a sessão Terminate CoA é selecionada, o ISE envia a desconexão 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 seletor TC-NAC e mudam o **log em nível do componente TC-NAC PARA DEBUGAR**

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar contains: System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > PassiveID > Threat Centric NAC. 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

Logs a ser verificados - irf.log. Você pode até-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}
```