用AMP和状态服务配置ISE 2.1威胁中心NAC (TC-NAC)

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Network Diagram
详细的流
配置AMP Cloud
步骤1.从AMP Cloud的下载连接器
配置ISE
步骤1.配置状态策略和情况
步骤2.配置状态配置文件
步骤3.配置AMP配置文件
步骤2.加载应用程序和XML配置文件对ISE
步骤3.下载AnyConnect标准模块
步骤4.添加AnyConnect配置
步骤5.配置客户端设置规则
步骤6.配置授权策略
步骤7. Enable (event) TC-NAC服务
步骤8.配置AMP适配器
Verify
终端
AMP Cloud
ISE
Troubleshoot

Introduction

本文描述如何用预先的Malware保护(AMP)配置威胁中心NAC在身份服务引擎(ISE) 2.1。威胁告警级别和弱点评估结果可以用于动态地控制终端或用户的访问级别。状态服务是也被覆盖，本文的部分。

> **Note**:本文的目的将描述与AMP的ISE 2.1集成，摆服务姿势显示，需要他们，当我们设置从ISE时的AMP。

Prerequisites

Requirements

Cisco建议您有这些题目基础知识：

- Cisco身份服务引擎
- 预先的Malware保护

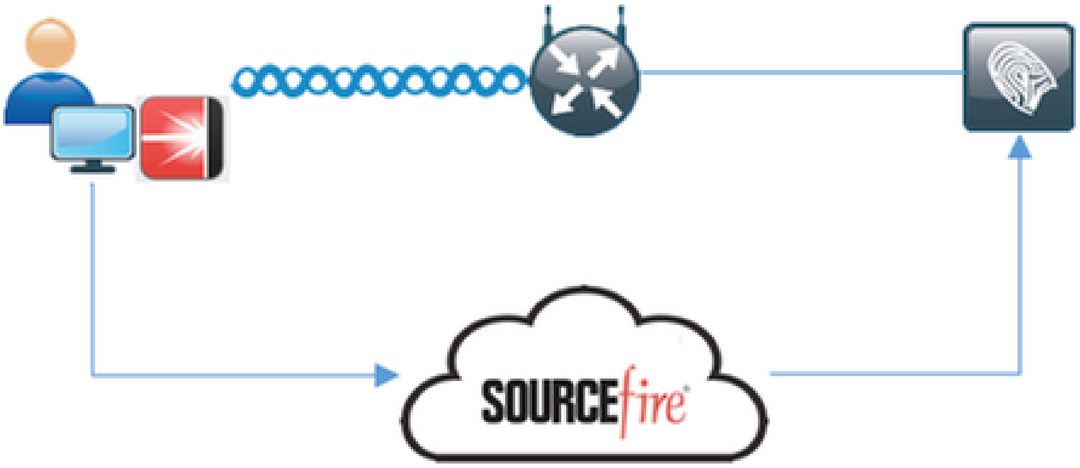
Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco身份服务引擎版本2.1
- 无线局域网控制器(WLC) 8.0.121.0
- AnyConnect VPN客户端4.2.02075
- Windows 7服务包1

Configure

Network Diagram



详细的流

1. 客户端连接到网络， **AMP_Profile**分配，并且用户重定向到Anyconnect设置的门户。如果Anyconnect在机器没有被发现， AMP，状态)安装所有被配置的模块(VPN。配置争取每个模块与该配置文件一起

2. 一旦安装Anyconnect，状态评估运行

3. AMP启动器模块安装FireAMP连接器

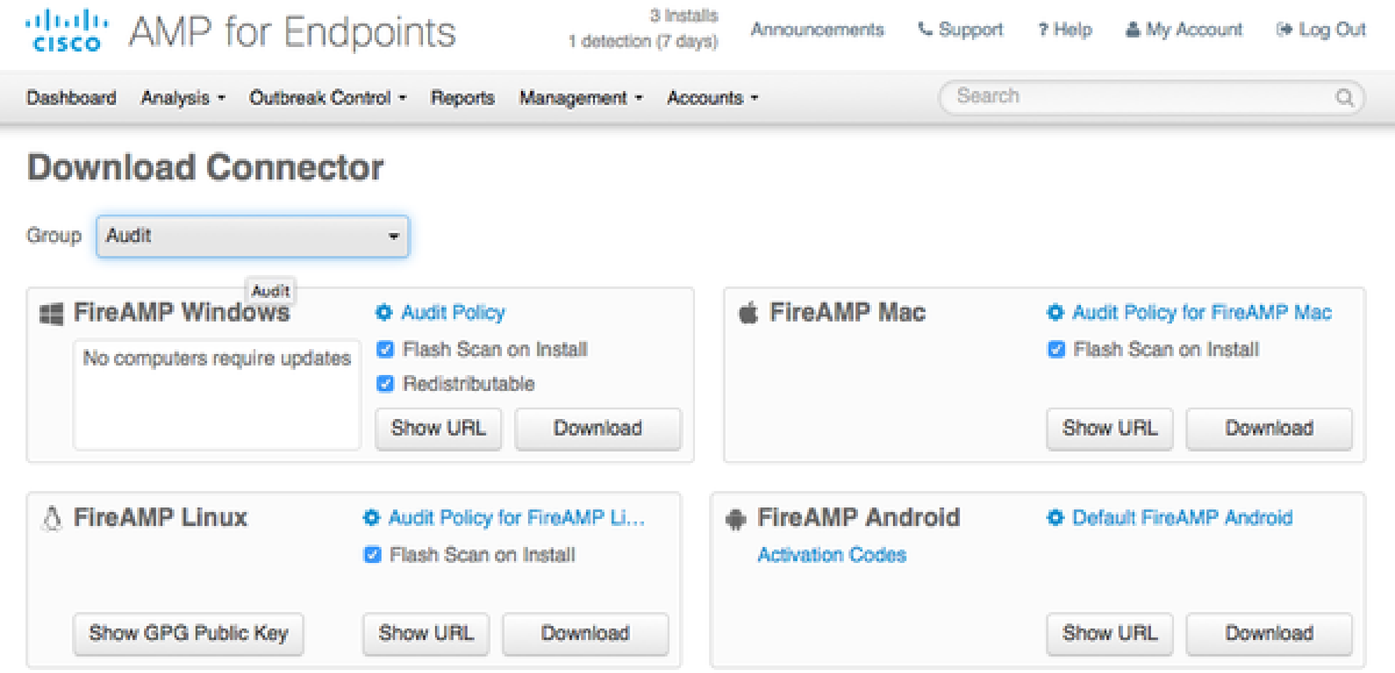
4. 当客户端设法下载恶意的软件时， AMP连接器投掷警告消息并且它向AMP Cloud报告

5. AMP Cloud发送此信息到ISE

配置AMP Cloud

步骤1.从AMP Cloud的下载连接器

为了下载连接器，请连接到Management>下载连接器。然后请选择类型和**下载**FireAMP (Windows，机器人、Mac， Linux)。在这种情况下**审计**为Windows选择了和FireAMP安装文件。

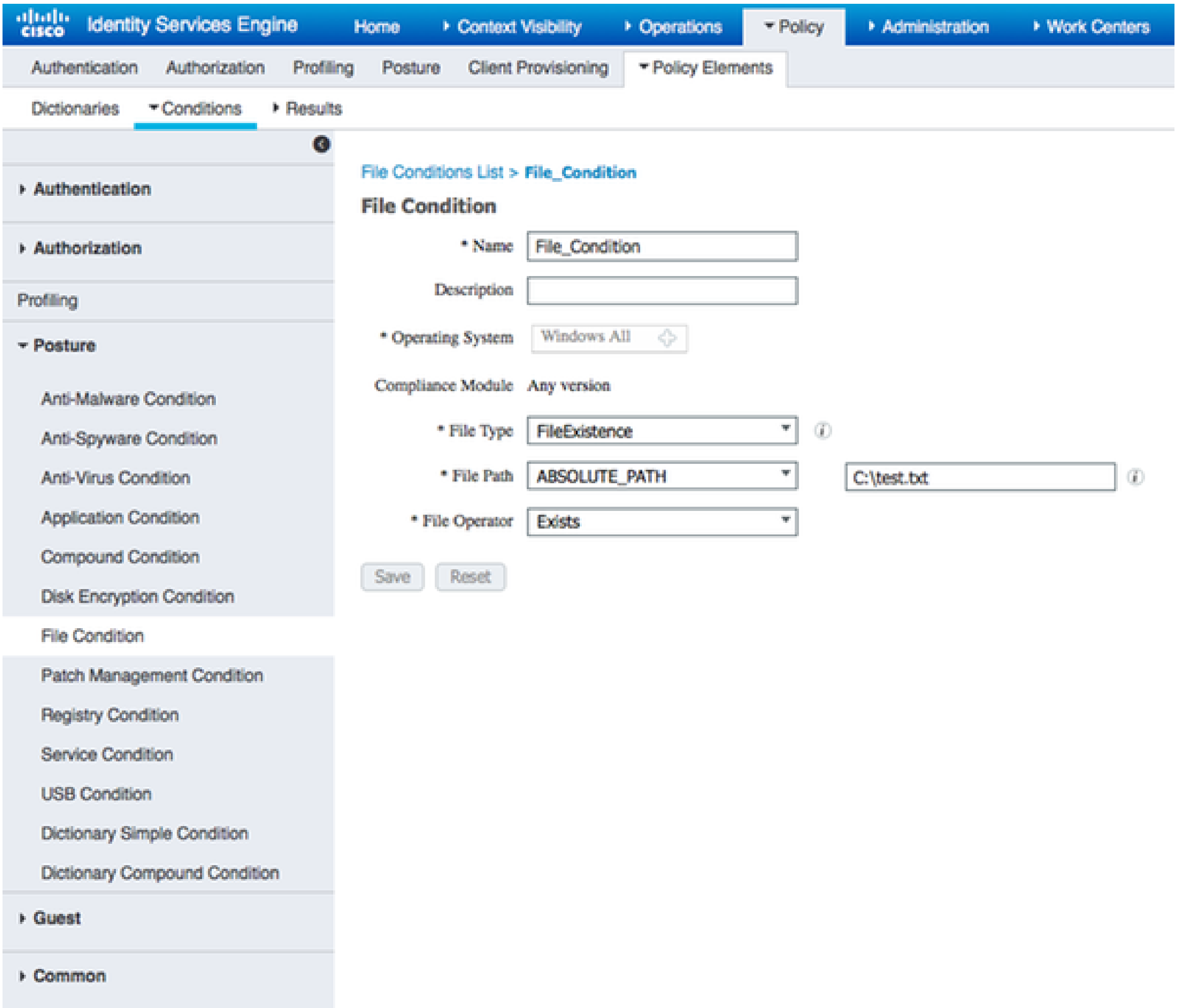


> **Note**:下载此文件生成名为**在**示例的**Audit_FireAMPSetup.exe的**一个.exe文件。一旦用户请求AMP的配置，此文件被发送到Web服务器是可用的。

配置ISE

步骤1.配置状态策略和情况

连接对策略>Policy元素>情况>状态>文件Condition.You能看到文件存在的一个单纯条件被创建了。如果终端是兼容的与状态模块，验证的策略文件必须存在：

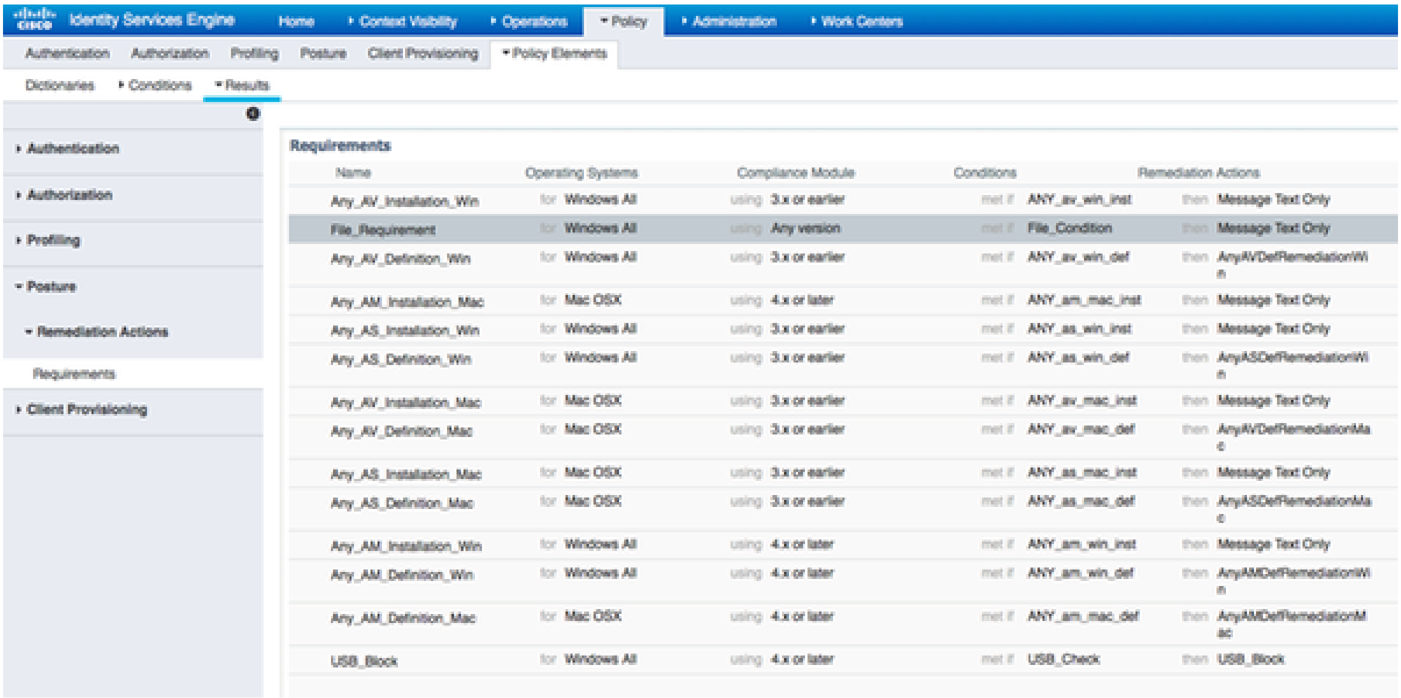


File Conditions List > File_Condition

File Condition

* Name	File_Condition
Description	
* Operating System	Windows All
Compliance Module	Any version
* File Type	FileExistence
* File Path	ABSOLUTE_PATH C:\test.txt
* File Operator	Exists

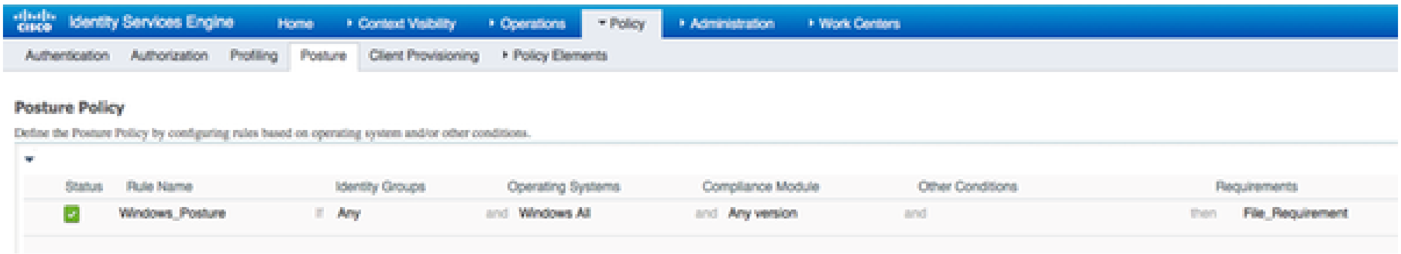
此情况使用需求：



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

需求用于状态策略微软视窗系统：



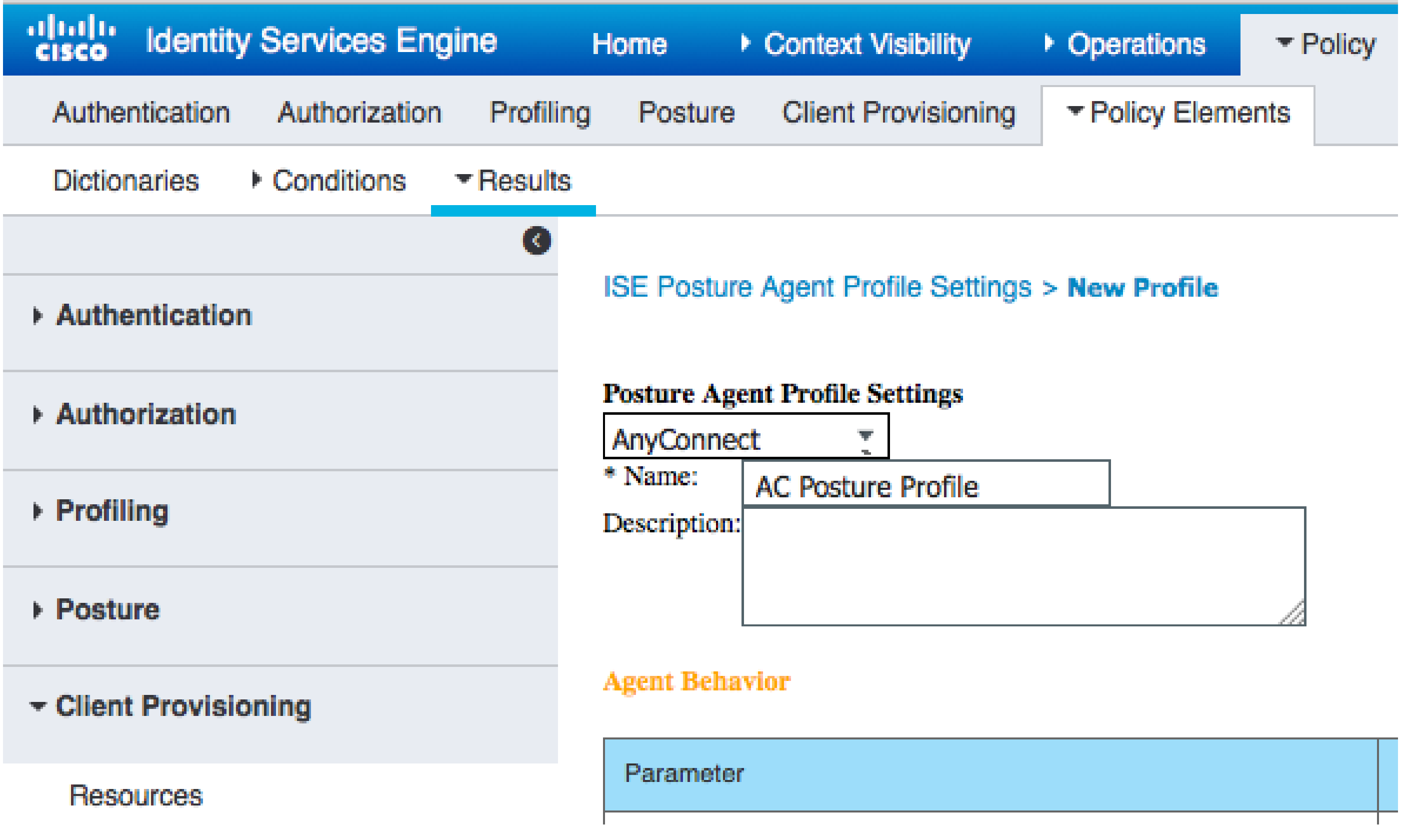
Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Rule Name		Identity Groups		Operating Systems		Compliance Module		Other Conditions		Requirements
✓	Windows_Posture	If	Any	and	Windows All	and	Any version	and		then	File_Requirement

步骤2.配置状态配置文件

- 连接对策略>Policy元素>结果>客户端设置>资源并且添加网络准入控制(NAC)代理程序或AnyConnect代理程序状态配置文件
- 选择Anyconnect



ISE Posture Agent Profile Settings > New Profile

Posture Agent Profile Settings

AnyConnect

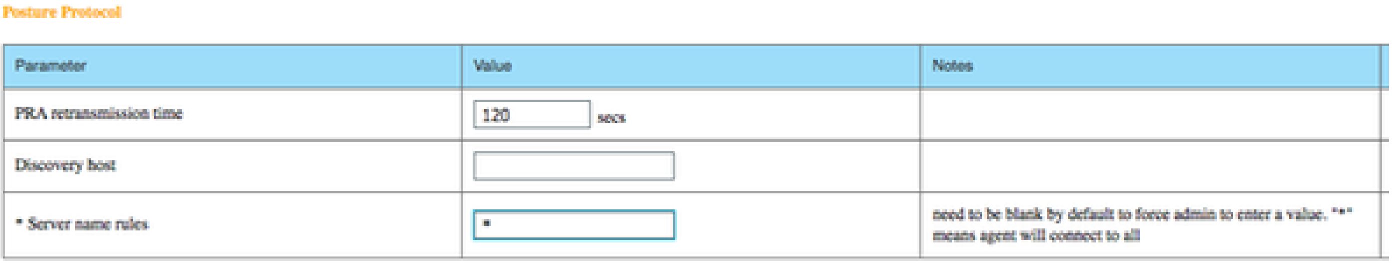
* Name: AC Posture Profile

Description:

Agent Behavior

Parameter

- 从状态协议部分请添加*为了允许代理程序连接到所有服务器

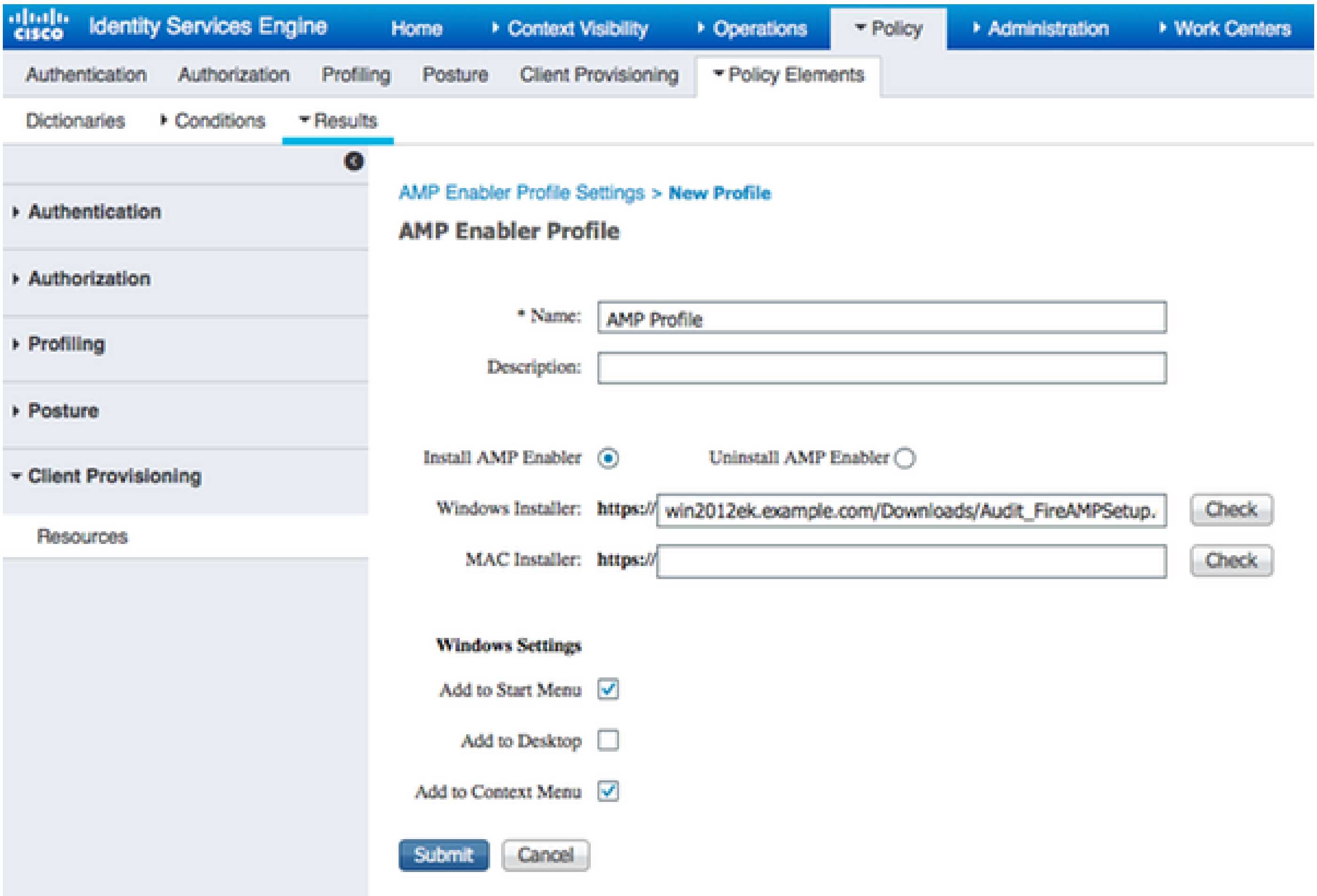


Posture Protocol

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

步骤3.配置AMP配置文件

AMP配置文件包含找出Windows安装程序的信息。Windows安装程序从AMP Cloud下载了前。它应该是可访问的从客户端机器。应该由客户端机器委托HTTPS服务器的认证，安装程序找出。



AMP Enabler Profile Settings > New Profile

AMP Enabler Profile

* Name: AMP Profile

Description:

Install AMP Enabler ● Uninstall AMP Enabler ○

Windows Installer: https:// win2012ek.example.com/Downloads/Audit_FireAMPSetup.

MAC Installer: https://

Windows Settings

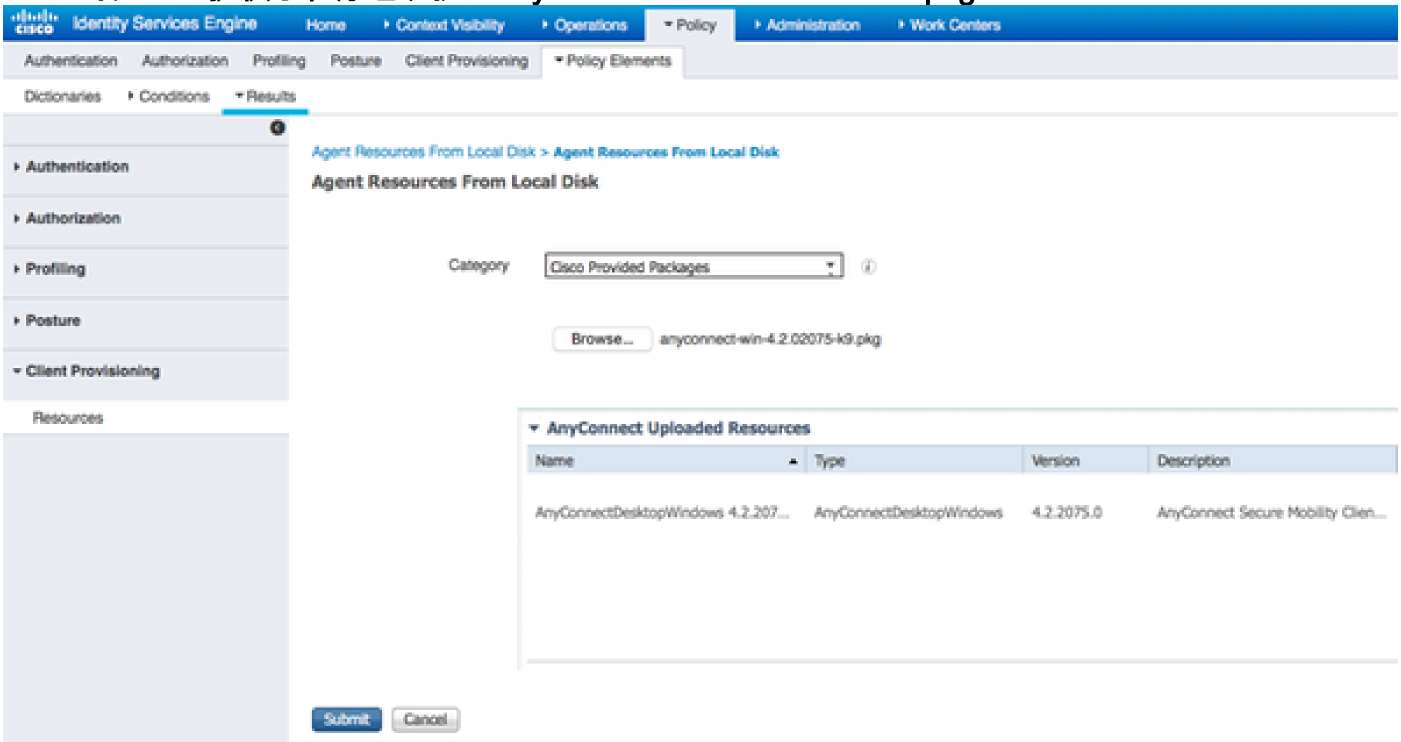
Add to Start Menu ☑

Add to Desktop □

Add to Context Menu ☑

步骤2.加载应用程序和XML配置文件对ISE

- 从正式Cisco站点手工下载应用程序：**anyconnect-win-4.2.02075-k9.pkg**
- 在ISE，请连接对策略>Policy元素>结果>客户端设置>资源，并且**从本地磁盘**添加**代理程序程序资源**
- 选择**Cisco提供了程序包**和挑选**anyconnect-win-4.2.02075-k9.pkg**



Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

Category: Cisco Provided Packages

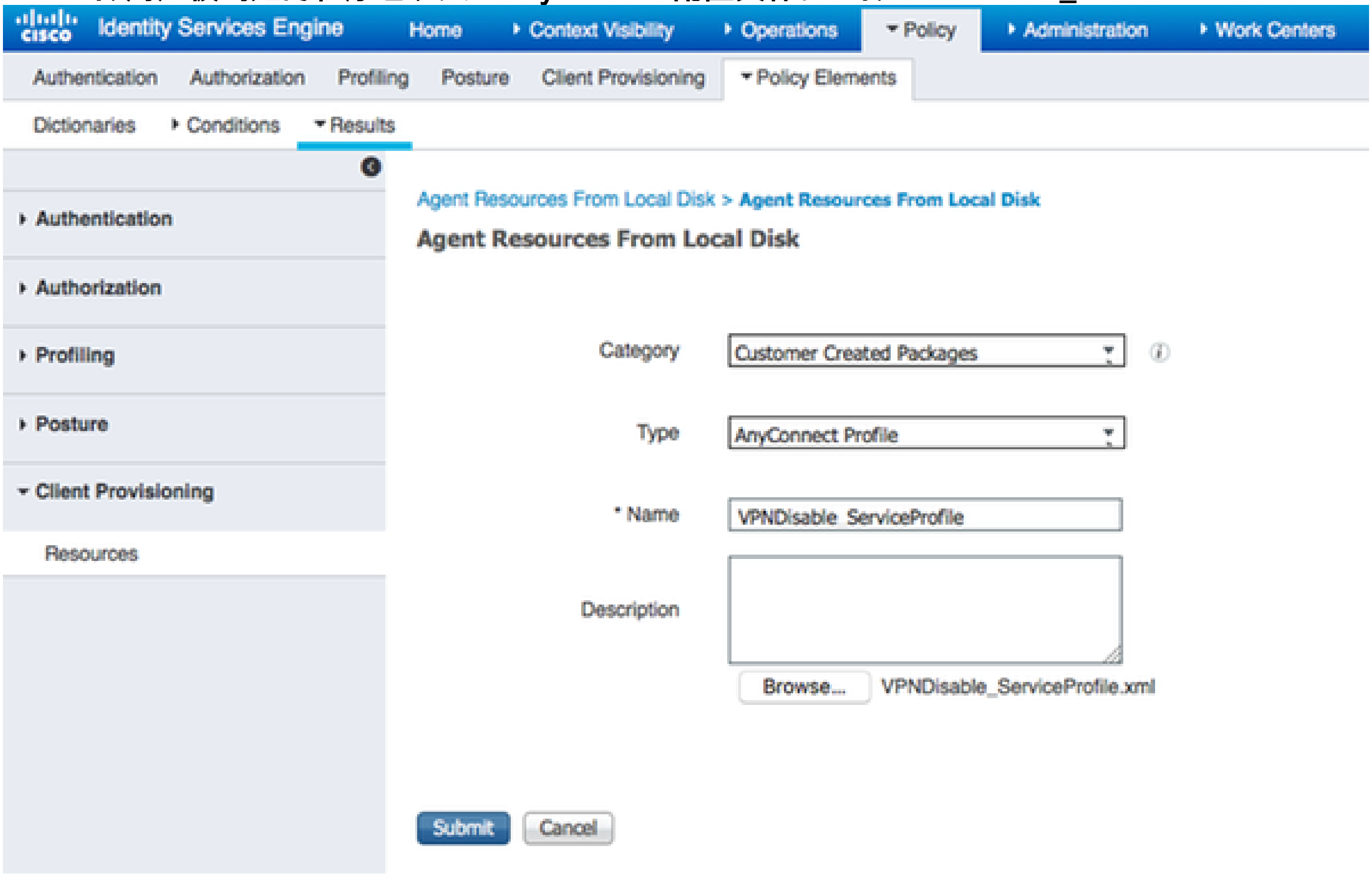
anyconnect-win-4.2.02075-k9.pkg

AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.2.207...	AnyConnectDesktopWindows	4.2.2075.0	AnyConnect Secure Mobility Clien...

- 连接对策略>Policy元素>结果>客户端设置>资源并且**从本地磁盘**添加**代理程序程序资源**

- 选择**用户被创建的程序包**和类型**AnyConnect配置文件**。选择**VPNDisable_ServiceProfile.xml**



Agent Resources From Local Disk

Category: Customer Created Packages

Type: AnyConnect Profile

* Name: VPNDisable_ServiceProfile

Description:

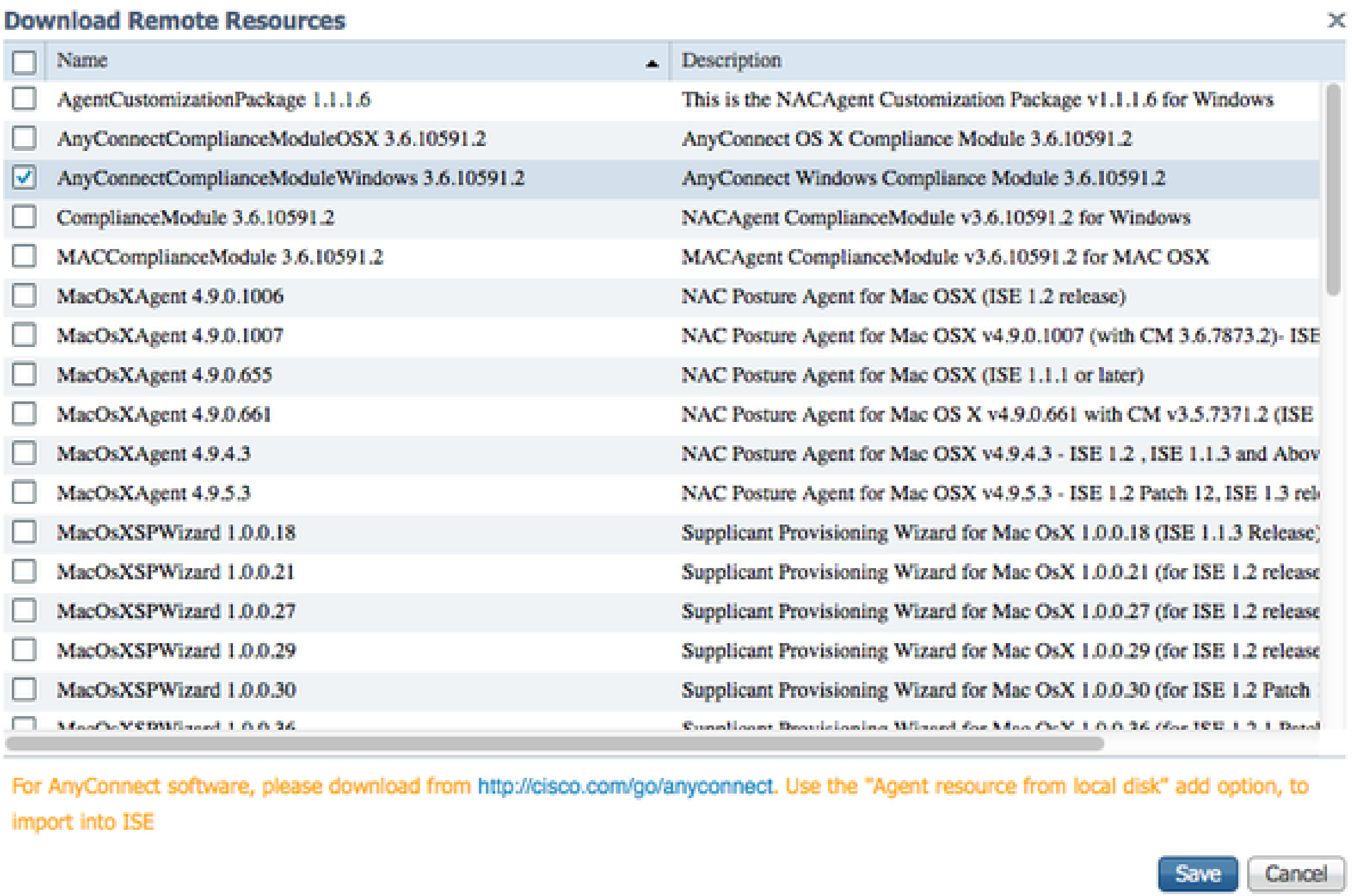
Browse... VPNDisable_ServiceProfile.xml

Note:因为此示例不使用VPN模块， **VPNDisable_ServiceProfile.xml**用于隐藏VPN标题。这是VPNDisable_ServiceProfile.xml内容：

```
<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 " >
 <ClientInitialization>
 <ServiceDisable>true</ServiceDisable>
 </ClientInitialization>
</AnyConnectProfile>
```

步骤3.下载AnyConnect标准模块

- 连接对策略>Policy元素>结果>客户端设置>资源并且**从Cisco站点**添加**代理程序资源**
- 选择**AnyConnect Windows标准模块3.6.10591.2**并且点击**“Save”**



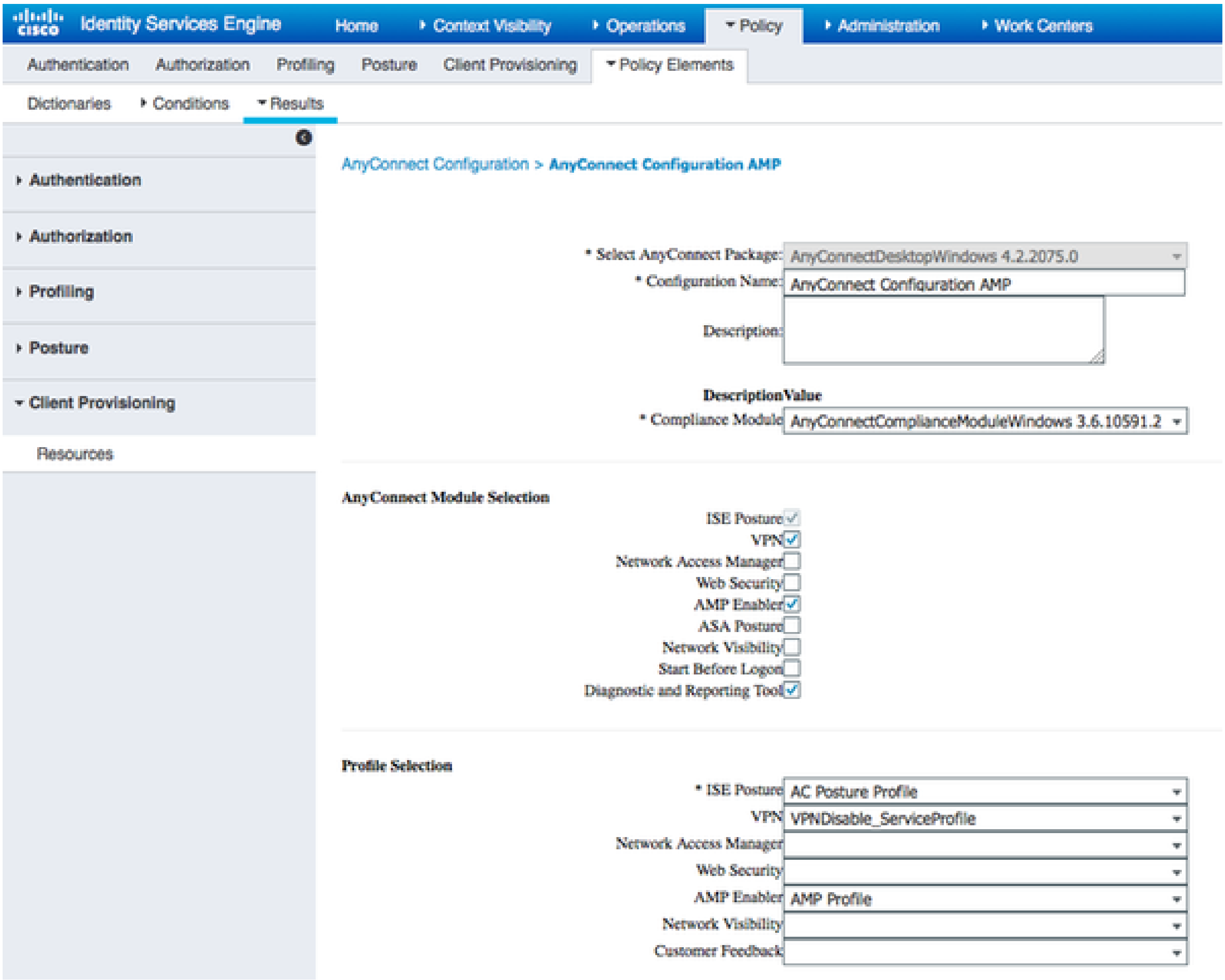
Download Remote Resources

□	Name	Description
□	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Windows
□	AnyConnectComplianceModuleOSX 3.6.10591.2	AnyConnect OS X Compliance Module 3.6.10591.2
☑	AnyConnectComplianceModuleWindows 3.6.10591.2	AnyConnect Windows Compliance Module 3.6.10591.2
□	ComplianceModule 3.6.10591.2	NACAgent ComplianceModule v3.6.10591.2 for Windows
□	MACComplianceModule 3.6.10591.2	MACAgent ComplianceModule v3.6.10591.2 for MAC OSX
□	MacOsXAgent 4.9.0.1006	NAC Posture Agent for Mac OSX (ISE 1.2 release)
□	MacOsXAgent 4.9.0.1007	NAC Posture Agent for Mac OSX v4.9.0.1007 (with CM 3.6.7873.2)- ISE
□	MacOsXAgent 4.9.0.655	NAC Posture Agent for Mac OSX (ISE 1.1.1 or later)
□	MacOsXAgent 4.9.0.661	NAC Posture Agent for Mac OS X v4.9.0.661 with CM v3.5.7371.2 (ISE
□	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3 and Abov
□	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12, ISE 1.3 rel
□	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1.3 Release)
□	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE 1.2 release
□	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE 1.2 release
□	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE 1.2 release
□	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE 1.2 Patch
□	MacOsXSPWizard 1.0.0.36	Supplicant Provisioning Wizard for Mac OsX 1.0.0.36 (for ISE 1.2.1 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

步骤4.添加AnyConnect配置

- 连接对策略>Policy元素>结果>客户端设置>资源，并且添加**AnyConnect配置**
- 配置名字并且选择标准模块和全部必需AnyConnect模块(VPN、AMP和状态)
- 在**配置文件选择**，请选择为每个模块配置的前配置文件



AnyConnect Configuration > **AnyConnect Configuration AMP**

* Select AnyConnect Package: AnyConnectDesktopWindows 4.2.2075.0

* Configuration Name: AnyConnect Configuration AMP

Description:

DescriptionValue

* Compliance Module AnyConnectComplianceModuleWindows 3.6.10591.2

AnyConnect Module Selection

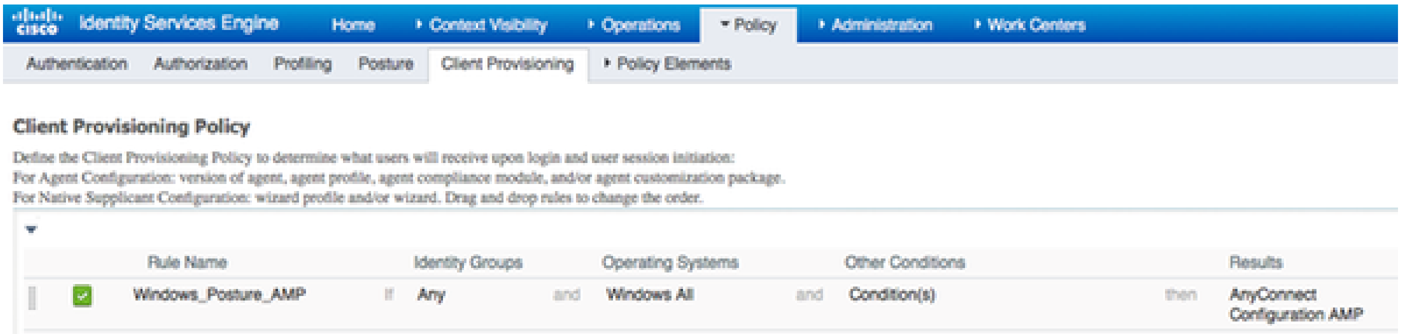
ISE Posture ☑
VPN ☑
Network Access Manager □
Web Security □
AMP Enabler ☑
ASA Posture □
Network Visibility □
Start Before Logon □
Diagnostic and Reporting Tool ☑

Profile Selection

* ISE Posture: AC Posture Profile
VPN: VPNDisable_ServiceProfile
Network Access Manager:
Web Security:
AMP Enabler: AMP Profile
Network Visibility:
Customer Feedback:

步骤5.配置客户端设置规则

及早被创建的AnyConnect配置被参考**客户端设置**规则



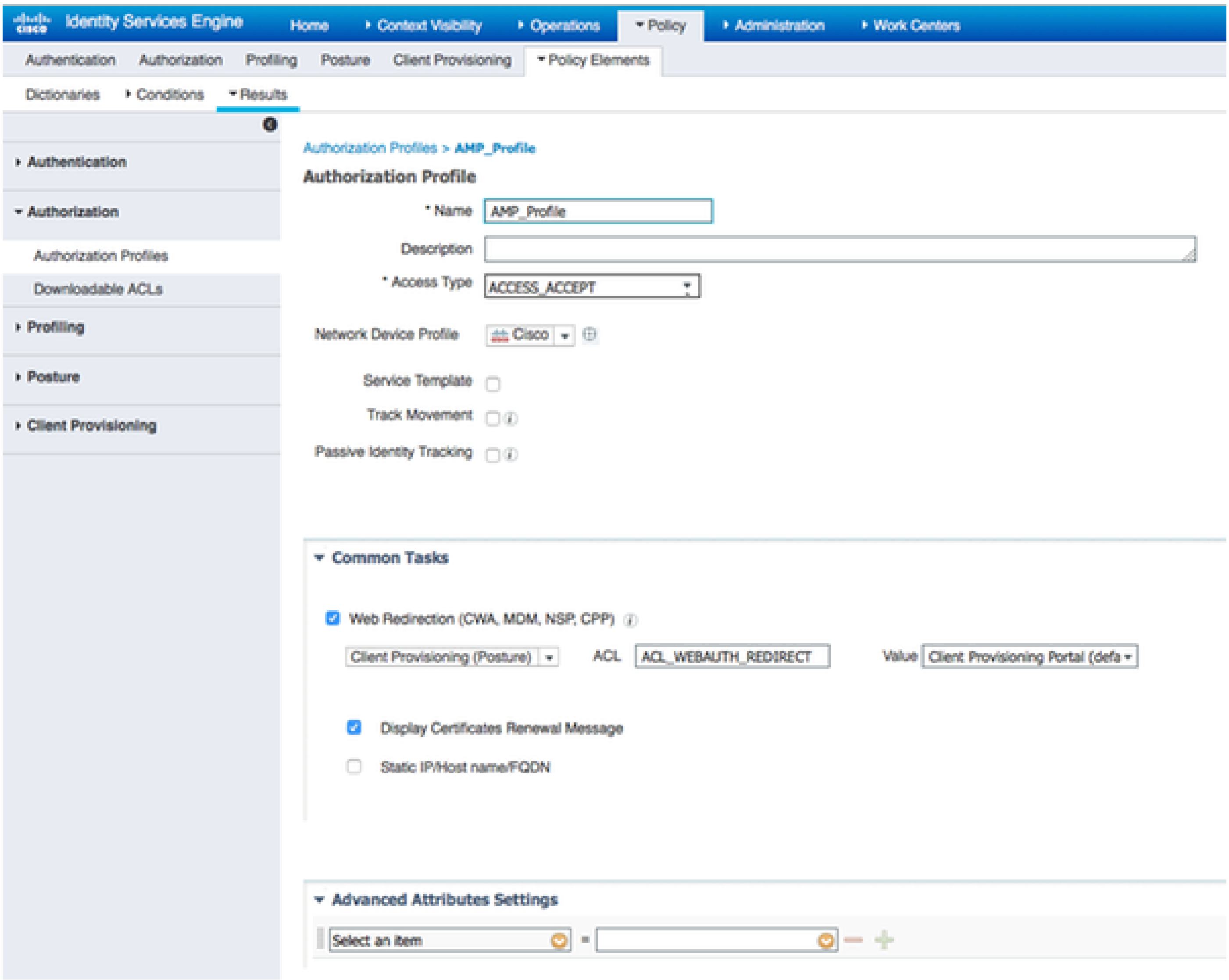
Client Provisioning Policy

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
✓	Windows_Posture_AMP	If	Any	and	Windows All	and	Condition(s)	then	AnyConnect Configuration AMP

步骤6.配置授权策略

首先对客户端设置的门户的重定向发生。使用状态的标准的授权策略。



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

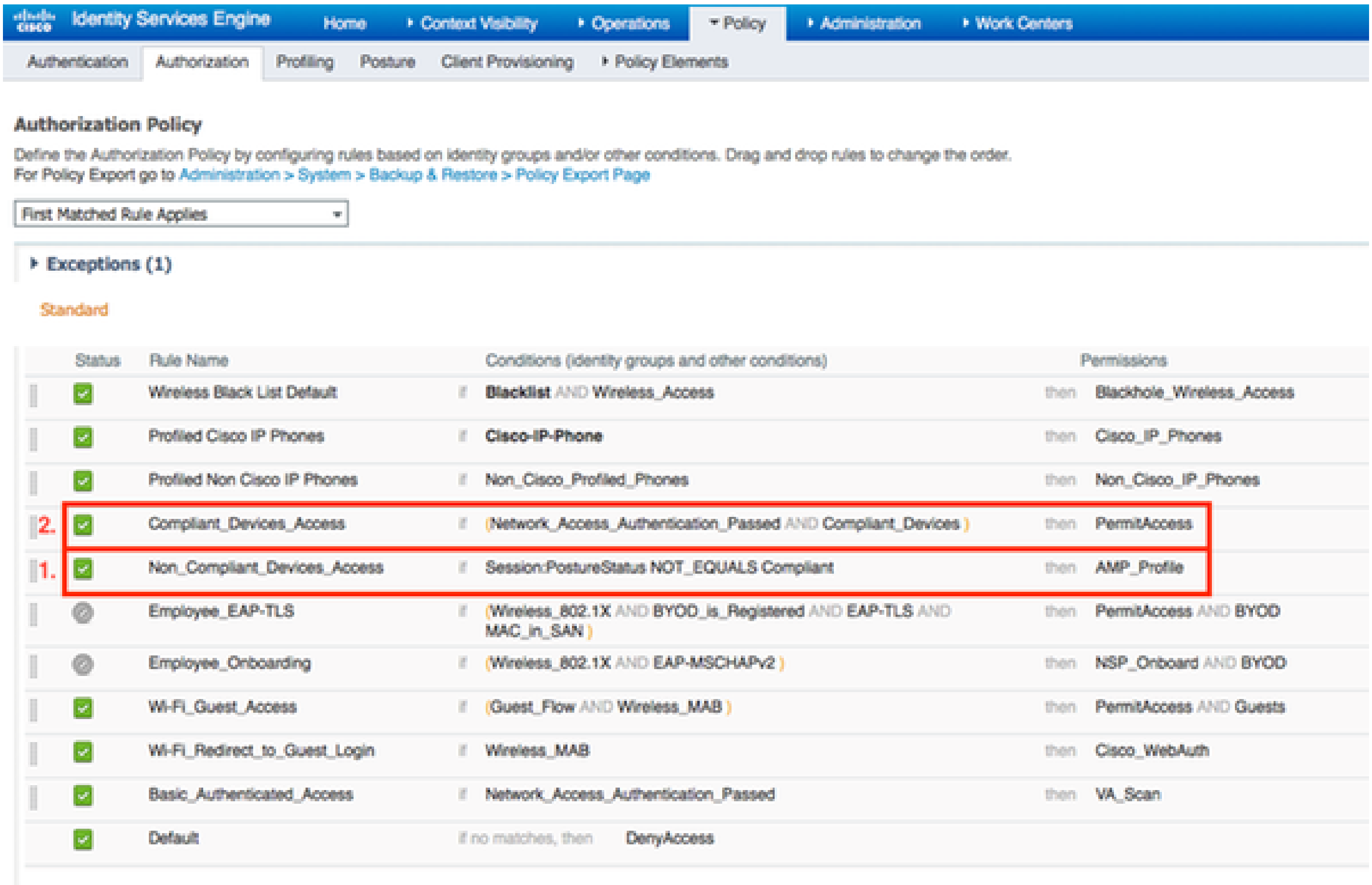
☑ Display Certificates Renewal Message

□ Static IP/Host name/FQDN

Advanced Attributes Settings

Select an item =

之后，一旦兼容，全部存取分配



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 ▾

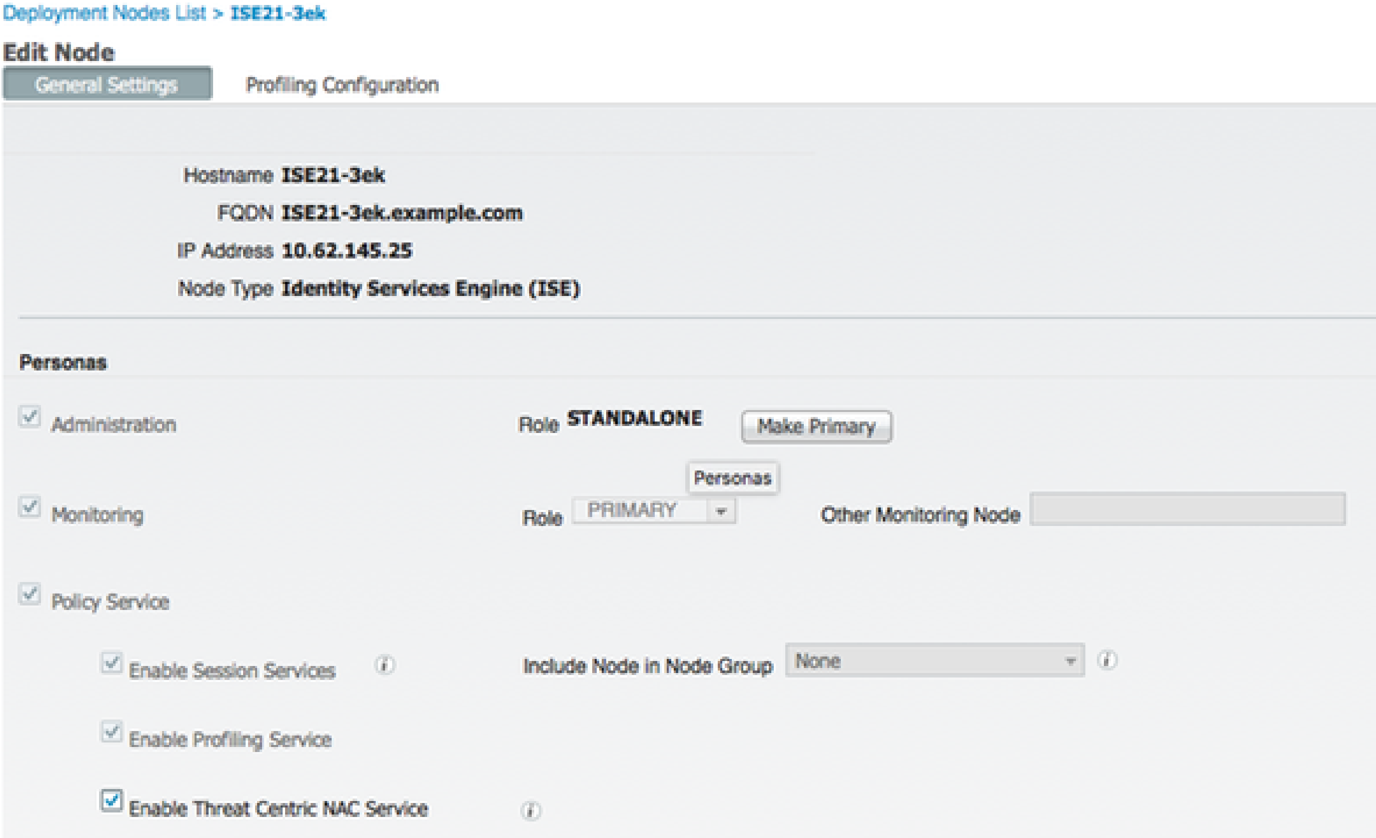
▸ Exceptions (1)

Standard

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

步骤7. Enable (event) TC-NAC服务

在Administration >配置> Edit下的Enable (event) TC-NAC服务节点。检查**Enable (event)威胁中心NAC服务**复选框。



Deployment Nodes List > ISE21-3ek

Edit Node

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 ▾　Other Monitoring Node

☑ Policy Service

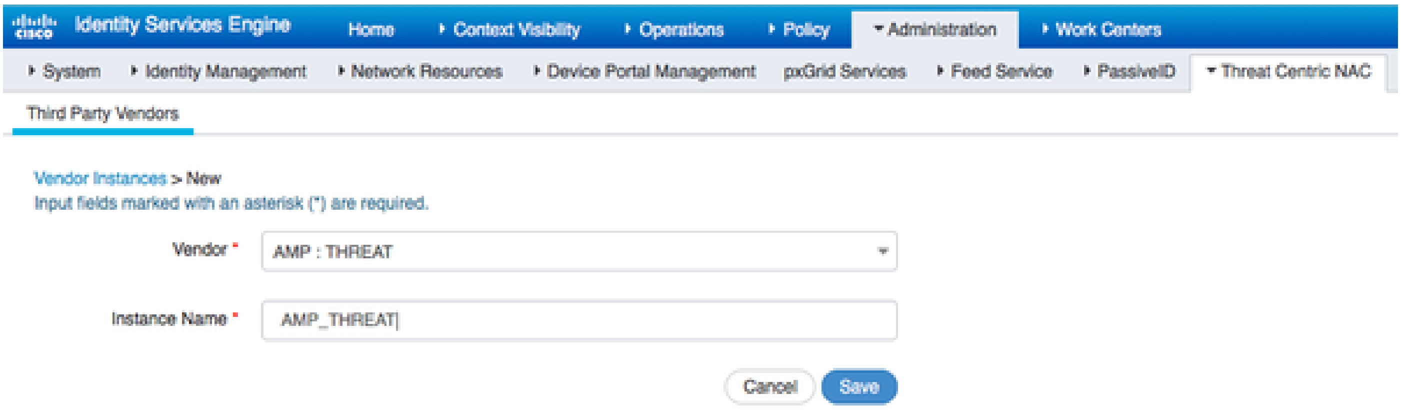
☑ Enable Session Services　Include Node in Node Group None ▾

☑ Enable Profiling Service

☑ Enable Threat Centric NAC Service

步骤8.配置AMP适配器

连接对中心的Administration >的威胁NAC >第三方供应商>Add。点击**“Save”**

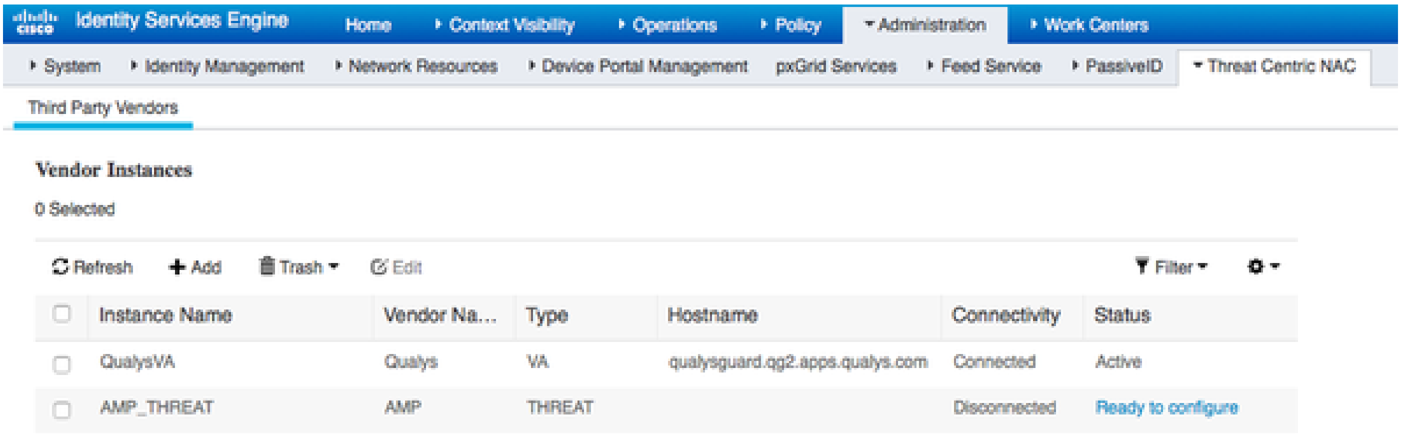


Vendor Instances > New
Input fields marked with an asterisk (*) are required.

Vendor * AMP : THREAT

Instance Name * AMP_THREAT

它应该过渡**准备配置**状态。点击**准备好配置**

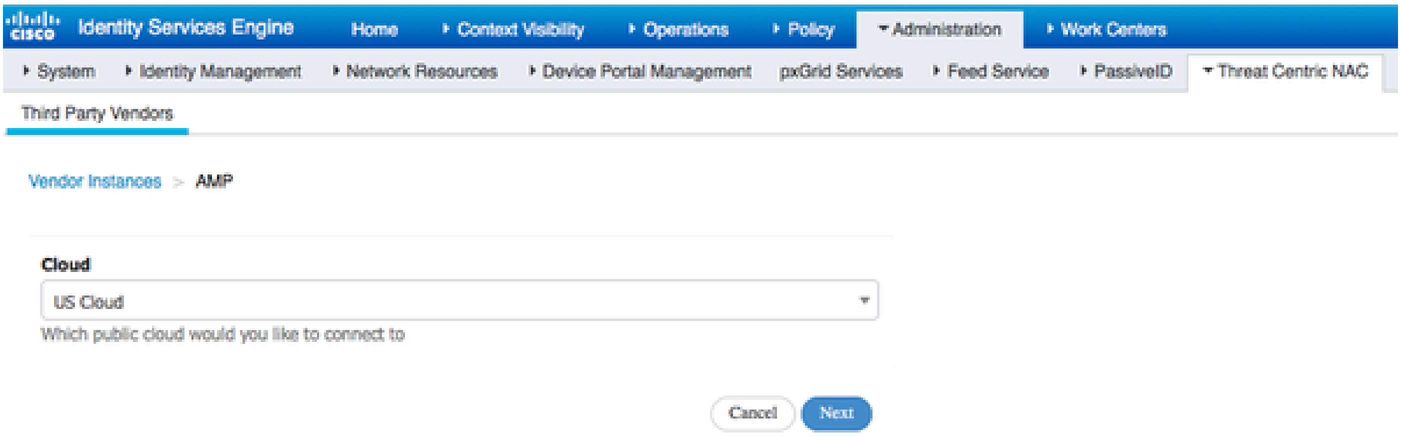


Vendor Instances

0 Selected

□	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

选择**Cloud**并且**其次**点击



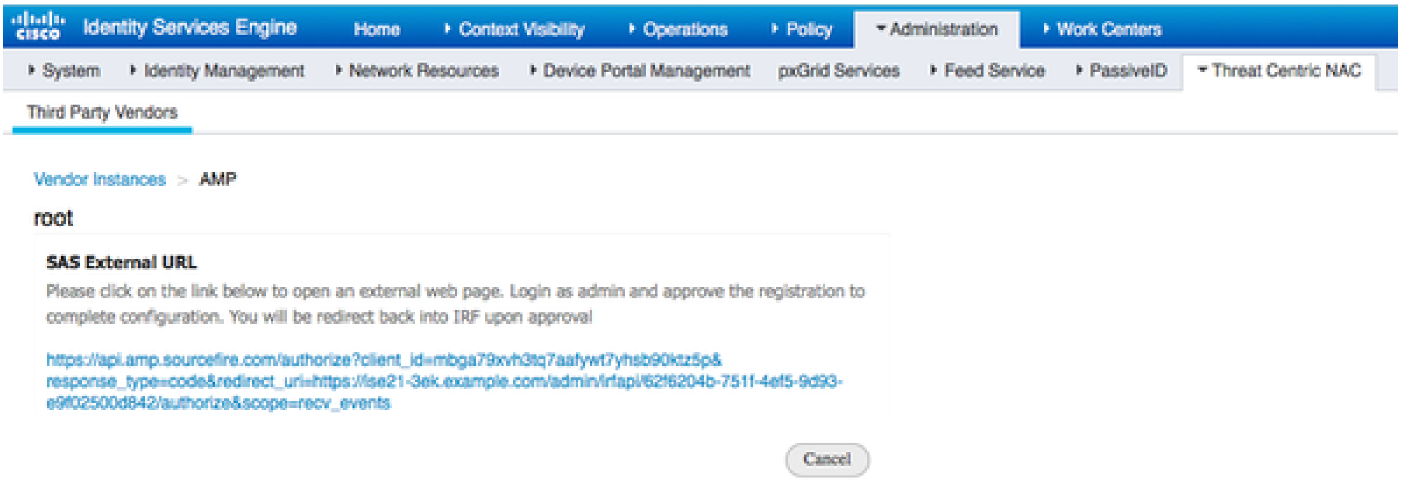
Vendor Instances > AMP

Cloud

US Cloud

Which public cloud would you like to connect to

点击FireAMP链路和登录作为admin在FireAMP。



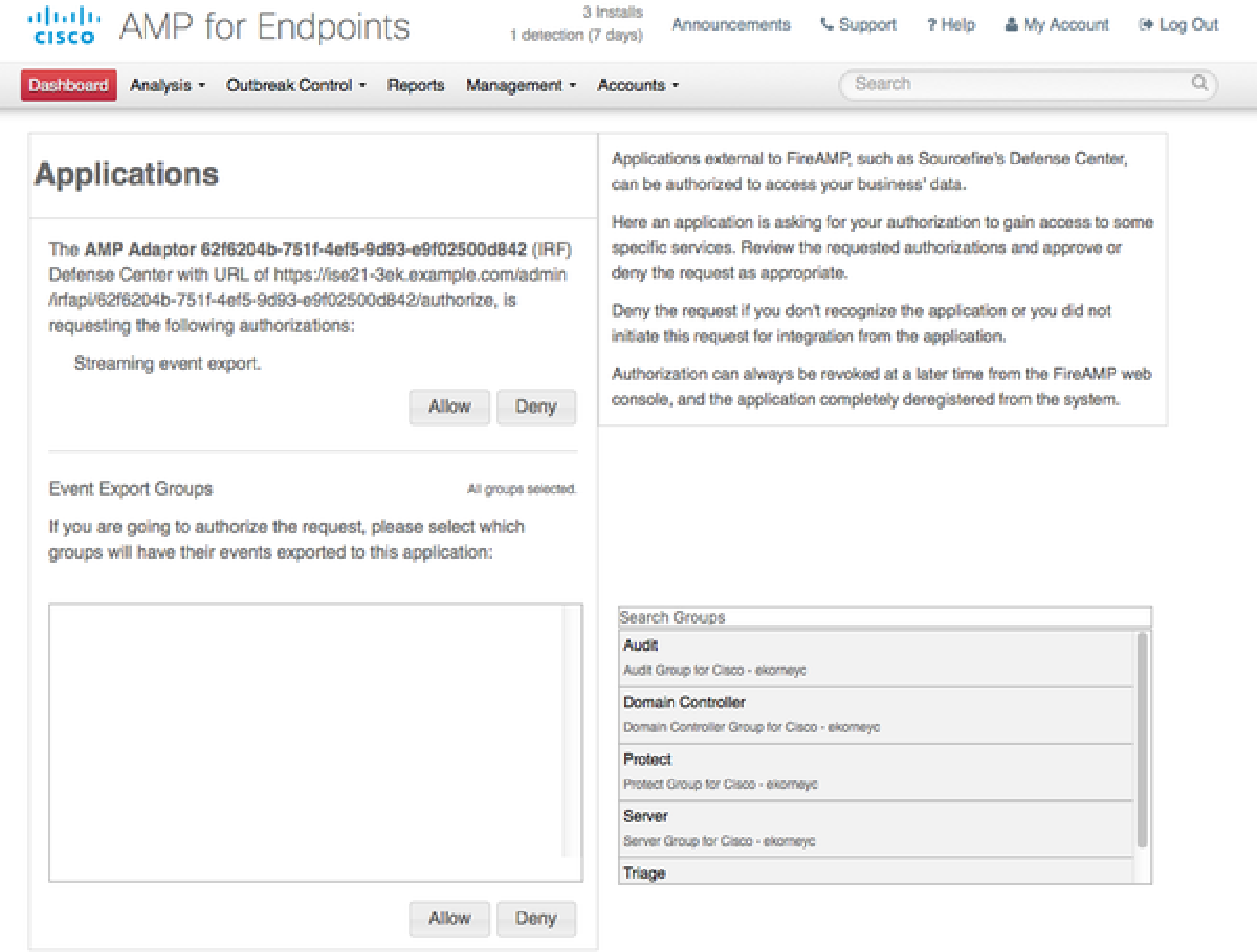
root

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/irfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize&scope=recv_events

点击**允许**在**应用程序**面板核准Export请求放出的事件。以后该动作，您重定向回到Cisco ISE



Applications

The **AMP Adaptor 62f6204b-751f-4ef5-9d93-e9f02500d842** (IRF) Defense Center with URL of https://ise21-3ek.example.com/admin/irfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize, is requesting the following authorizations:

Streaming event export.

Applications external to FireAMP, such as Sourcefire's Defense Center, can be authorized to access your business' data.

Here an application is asking for your authorization to gain access to some specific services. Review the requested authorizations and approve or deny the request as appropriate.

Deny the request if you don't recognize the application or you did not initiate this request for integration from the application.

Authorization can always be revoked at a later time from the FireAMP web console, and the application completely deregistered from the system.

Event Export Groups

All groups selected.

If you are going to authorize the request, please select which groups will have their events exported to this application:

Audit
Audit Group for Cisco - ekorneyc

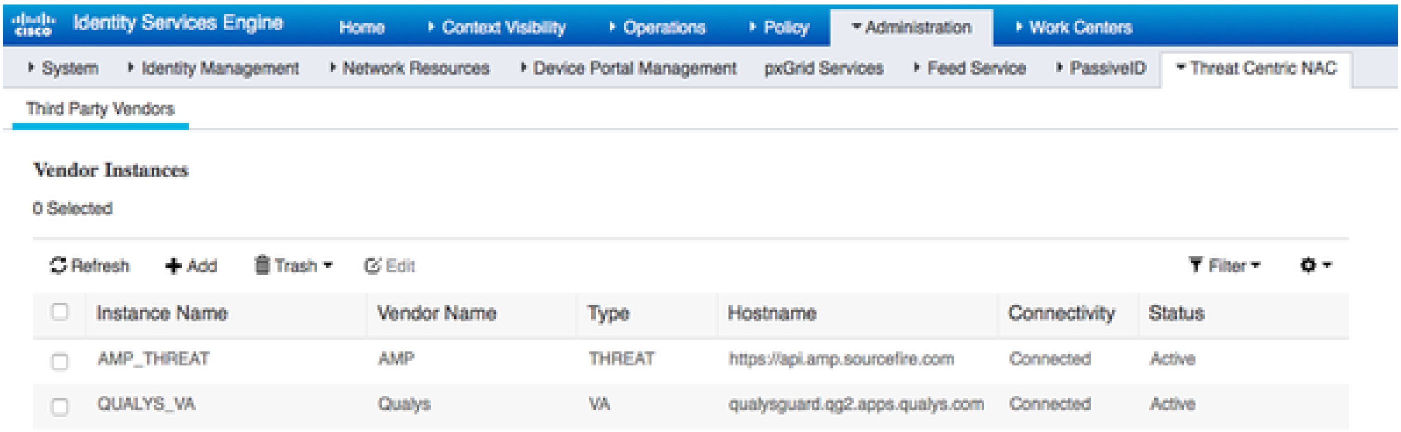
Domain Controller
Domain Controller Group for Cisco - ekorneyc

Protect
Protect Group for Cisco - ekorneyc

Server
Server Group for Cisco - ekorneyc

Triage

选择该的事件(例如，可疑下载、连接与可疑域，被执行的malware， Java妥协)您希望监控。适配器实例配置的汇总在配置汇总页显示。适配器实例过渡了到被连接的/激活状态。



Vendor Instances

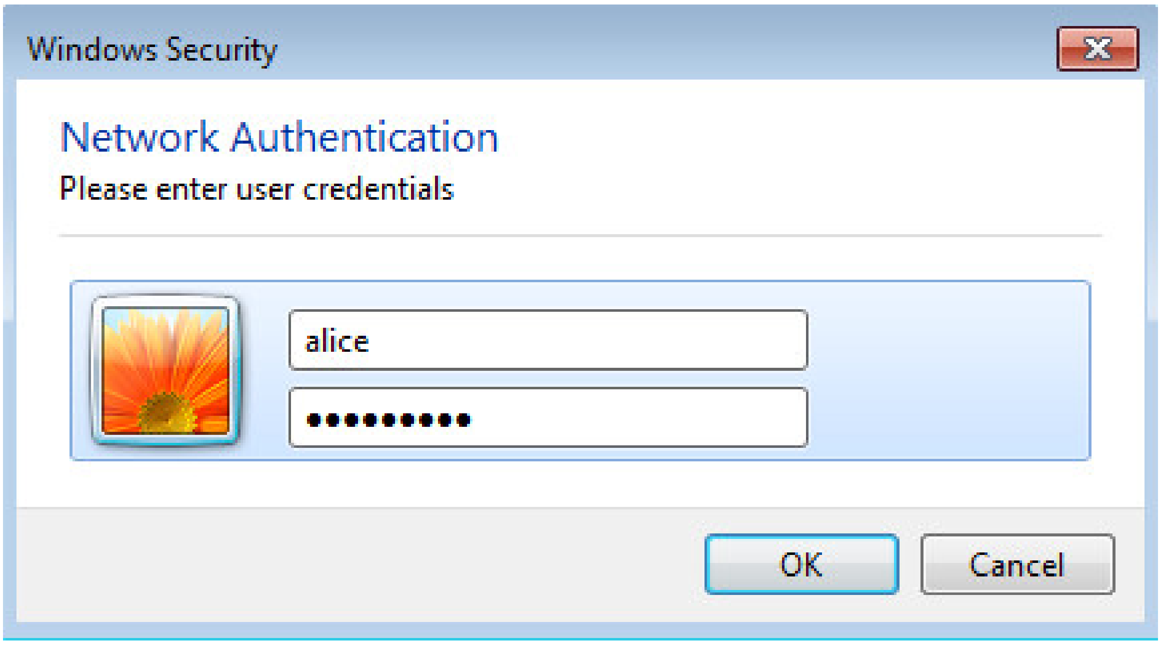
0 Selected

□	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

Verify

终端

连接到无线网络通过PEAP (MSCHAPv2)。


Windows Security

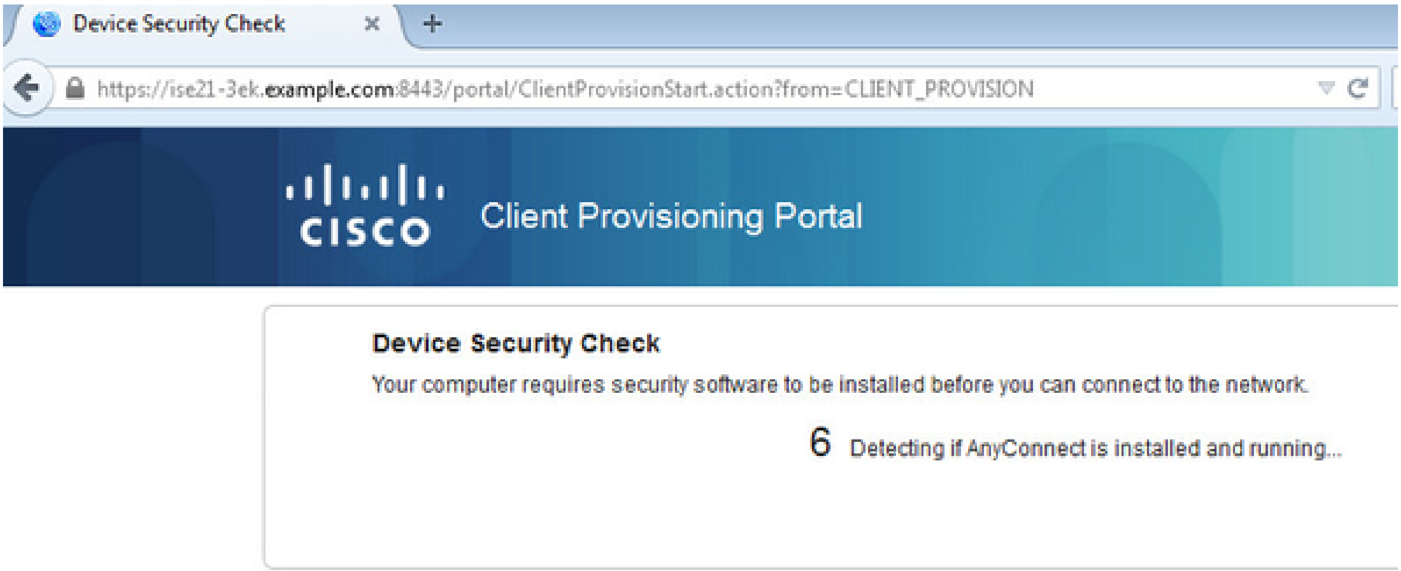
Network Authentication

Please enter user credentials

alice

●●●●●●●●●●

一旦连接重定向到客户端设置的门户发生。



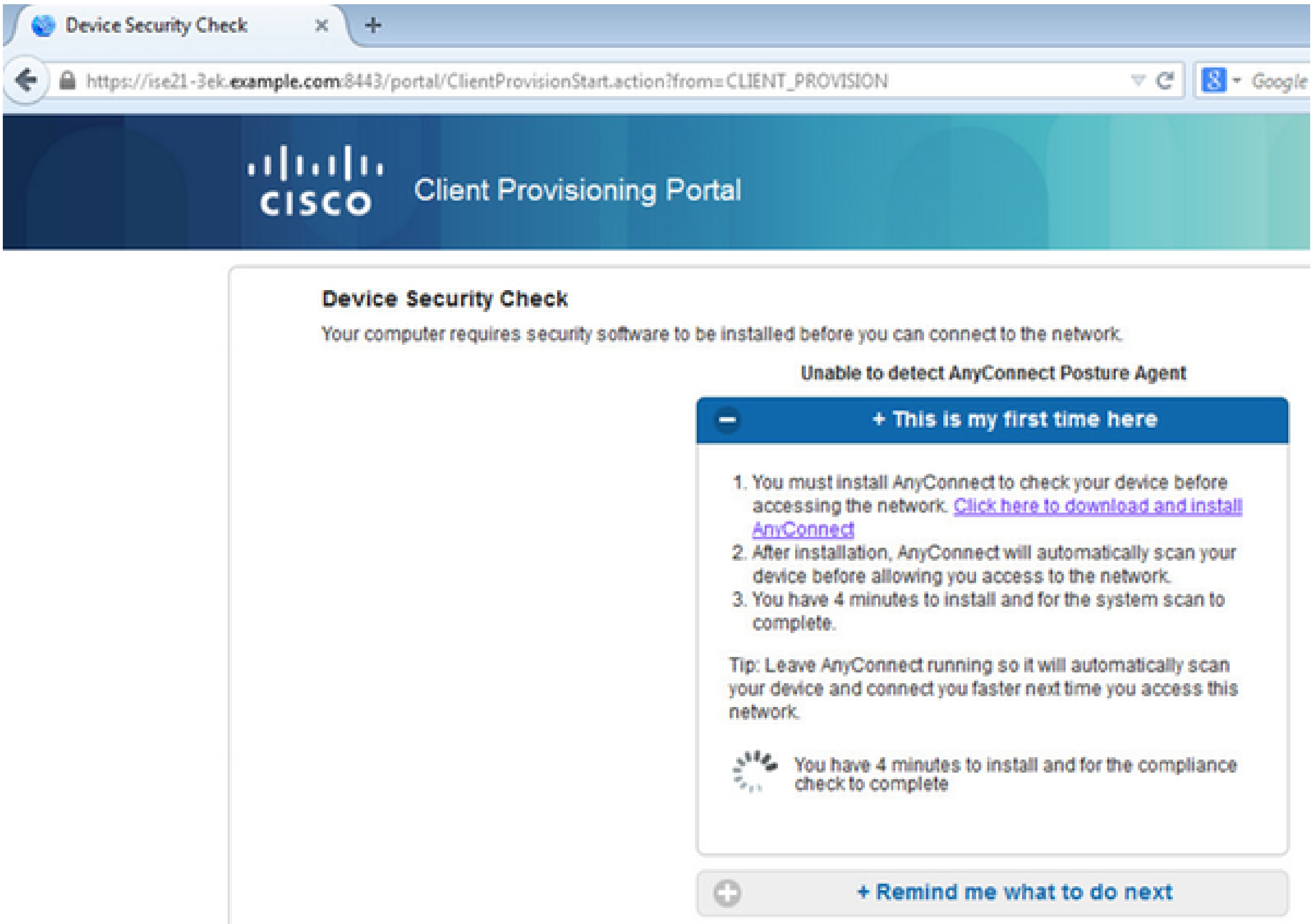
Device Security Check
https://ise21-3ek.example.com:8443/portal/ClientProvisionStart.action?from=CLIENT_PROVISION
cisco
Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

6 Detecting if AnyConnect is installed and running...

因为在客户端机器上安装的没什么， ISE提示输入AnyConnect客户端安装。



Device Security Check
https://ise21-3ek.example.com:8443/portal/ClientProvisionStart.action?from=CLIENT_PROVISION
Google
cisco
Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect AnyConnect Posture Agent

+ This is my first time here

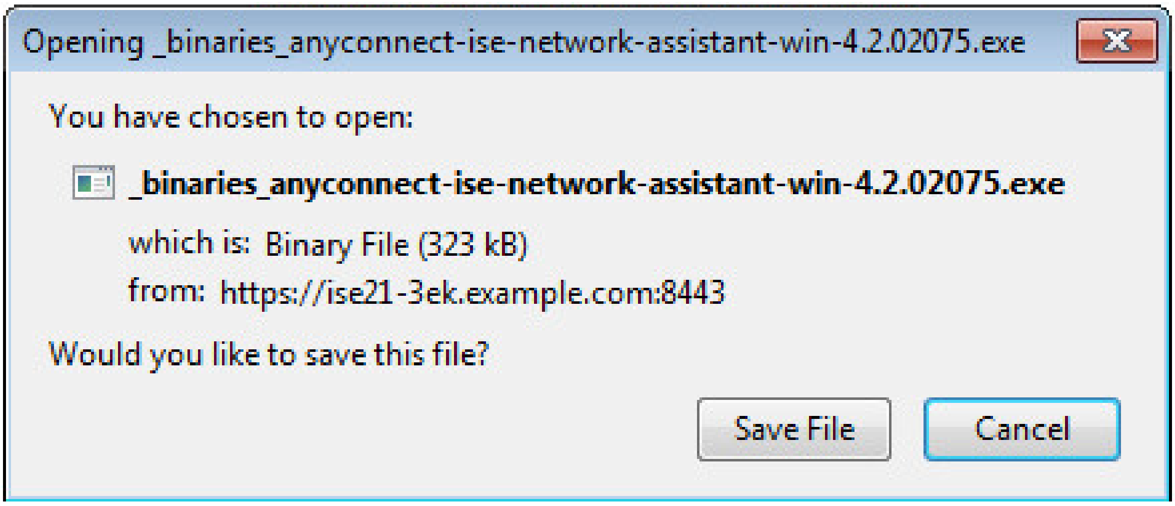
1. You must install AnyConnect to check your device before accessing the network. Click here to download and install AnyConnect
2. After installation, AnyConnect will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave AnyConnect running so it will automatically scan your device and connect you faster next time you access this network.

You have 4 minutes to install and for the compliance check to complete

+ Remind me what to do next

应该从客户端机器下载网络建立辅助(NSA)应用程序和运行。



Opening _binaries_anyconnect-ise-network-assistant-win-4.2.02075.exe

You have chosen to open:

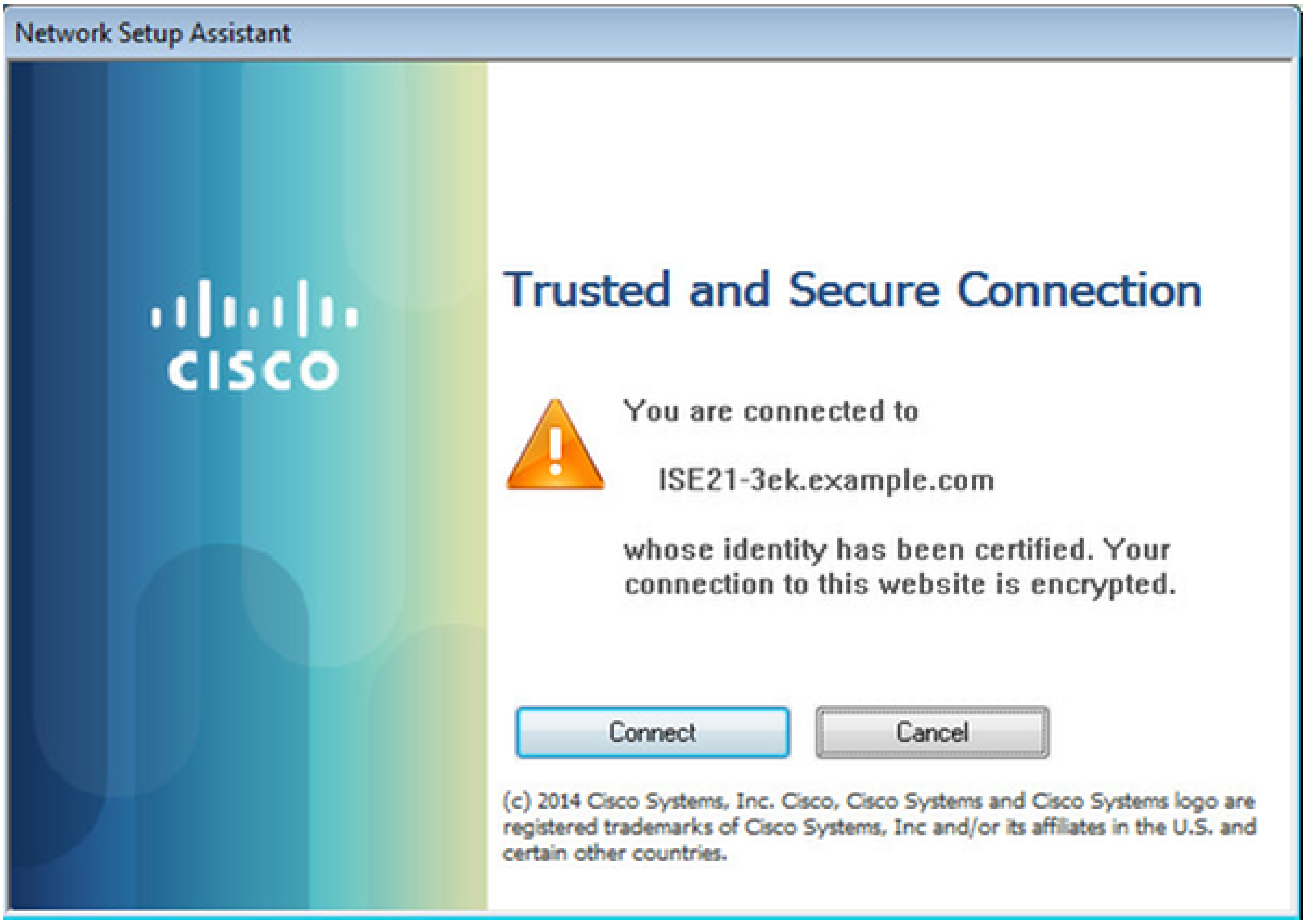
_binaries_anyconnect-ise-network-assistant-win-4.2.02075.exe

which is: Binary File (323 kB)

from: https://ise21-3ek.example.com:8443

Would you like to save this file?

NSA照料安装必需的组件和配置文件。



Network Setup Assistant

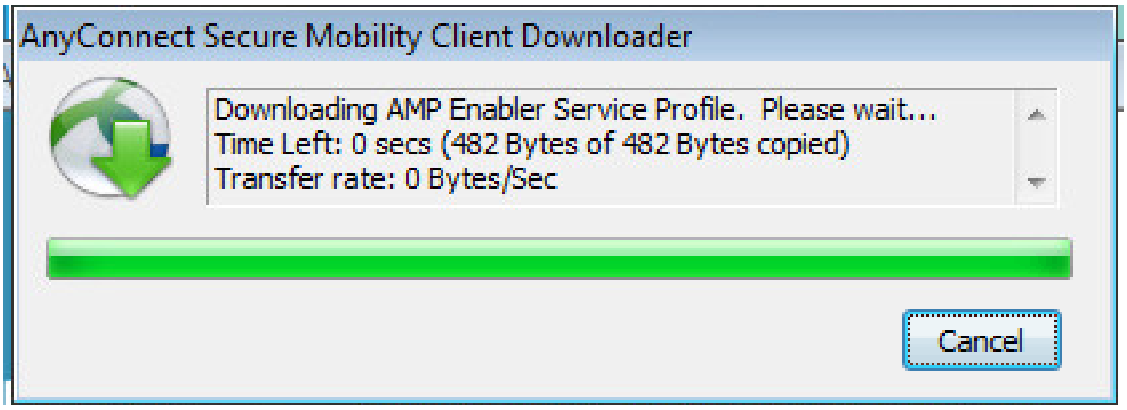
Trusted and Secure Connection

You are connected to

ISE21-3ek.example.com

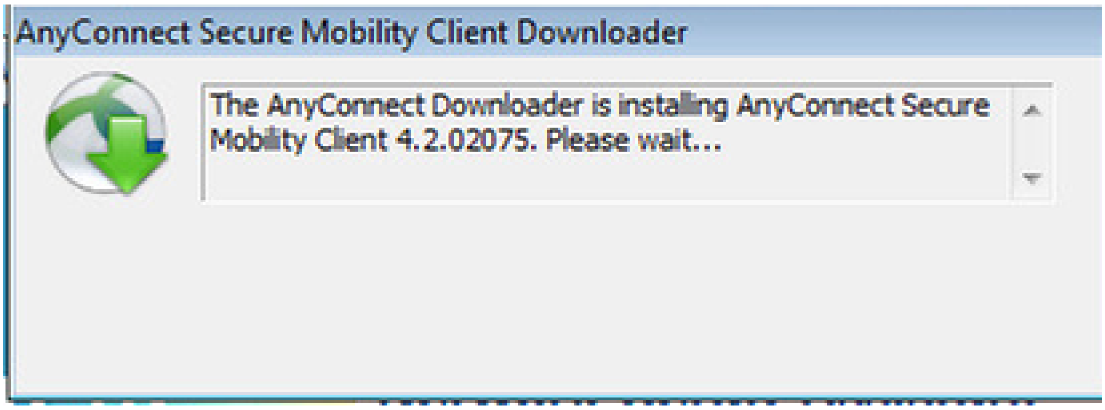
whose identity has been certified. Your connection to this website is encrypted.

(c) 2014 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.



AnyConnect Secure Mobility Client Downloader

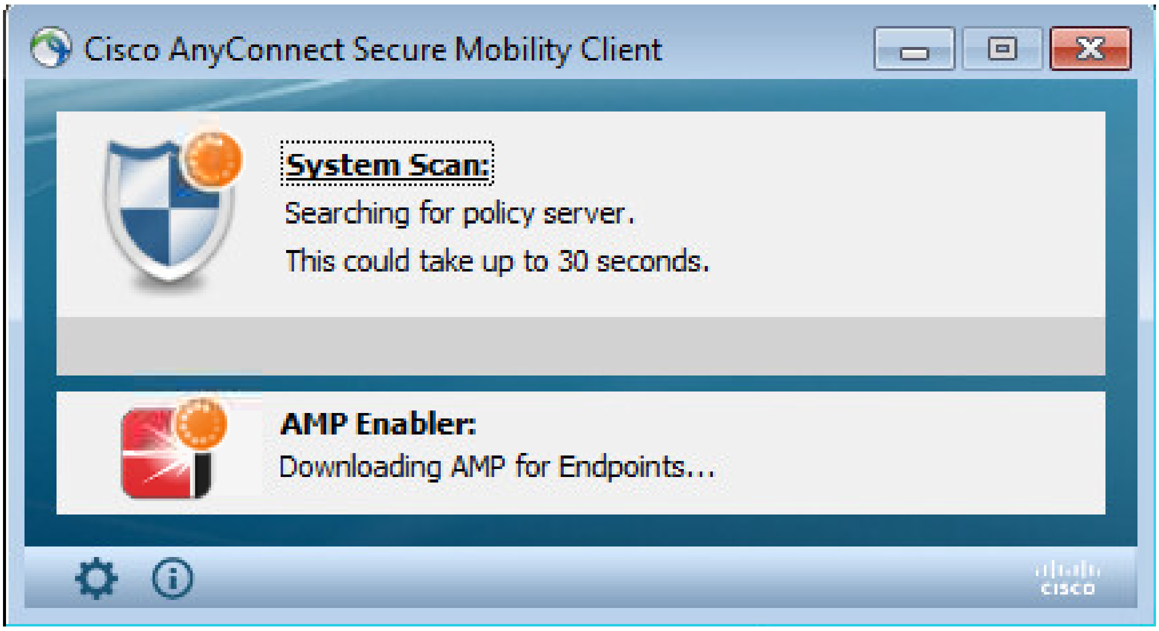
```
Downloading AMP Enabler Service Profile.  Please wait...
Time Left: 0 secs (482 Bytes of 482 Bytes copied)
Transfer rate: 0 Bytes/Sec
```



AnyConnect Secure Mobility Client Downloader

The AnyConnect Downloader is installing AnyConnect Secure Mobility Client 4.2.02075. Please wait...

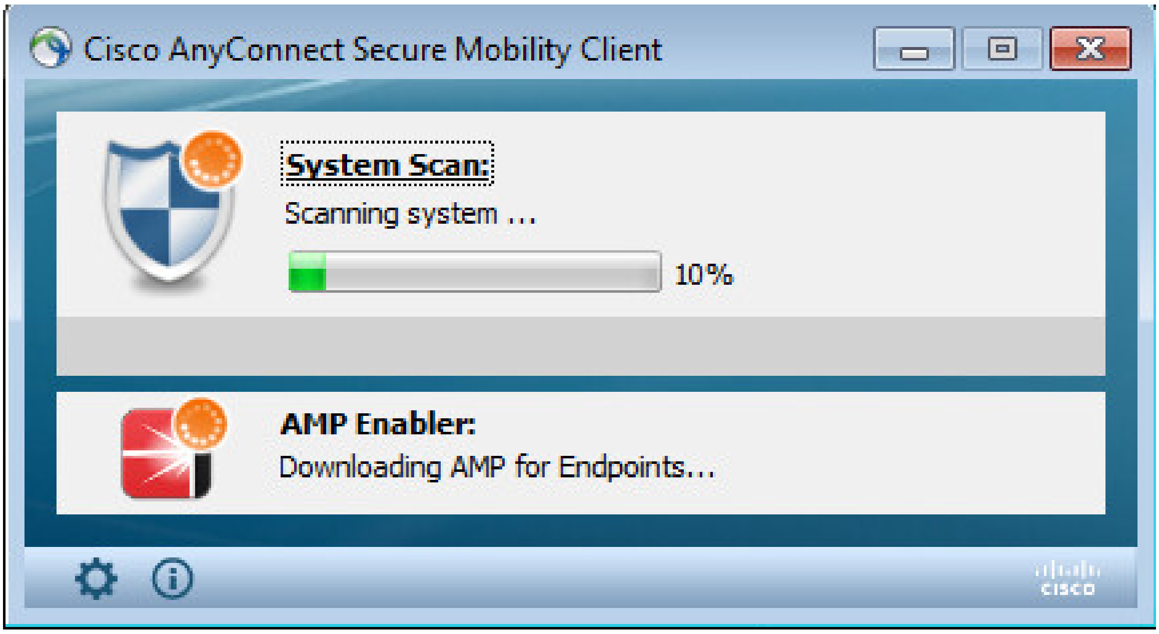
一旦安装完成， AnyConnect状态模块执行标准检查。



Cisco AnyConnect Secure Mobility Client

System Scan:
Searching for policy server.
This could take up to 30 seconds.

AMP Enabler:
Downloading AMP for Endpoints...

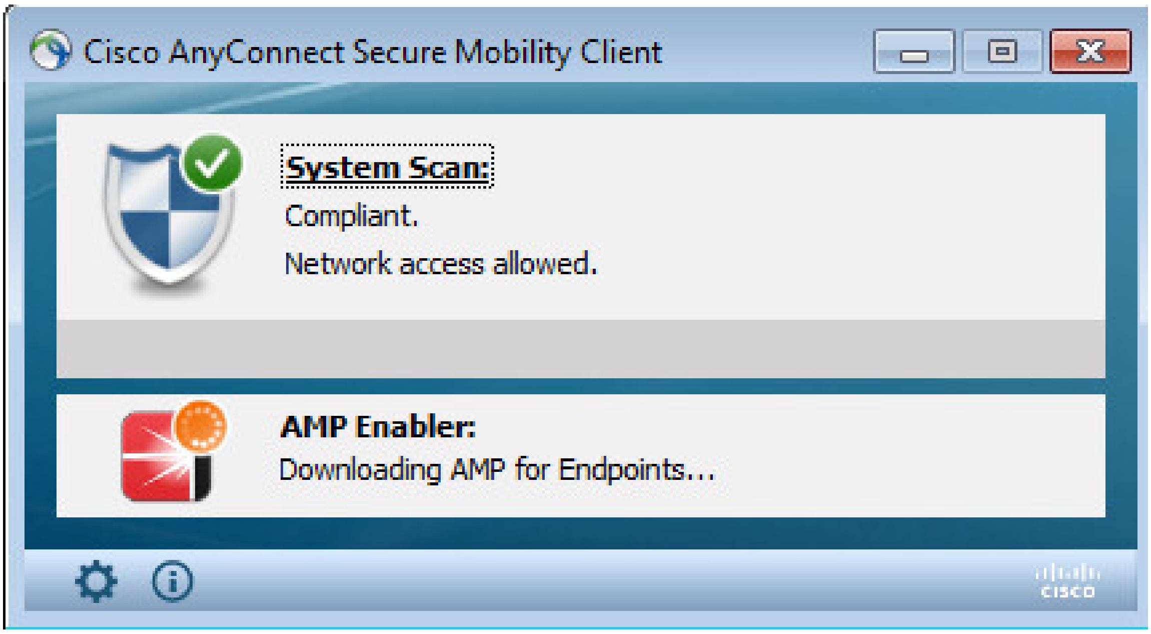


Cisco AnyConnect Secure Mobility Client

System Scan:
Scanning system ...
10%

AMP Enabler:
Downloading AMP for Endpoints...

当全部存取产生，如果终端是兼容的， AMP从在AMP配置文件指定的前网络服务器下载并且安装
。



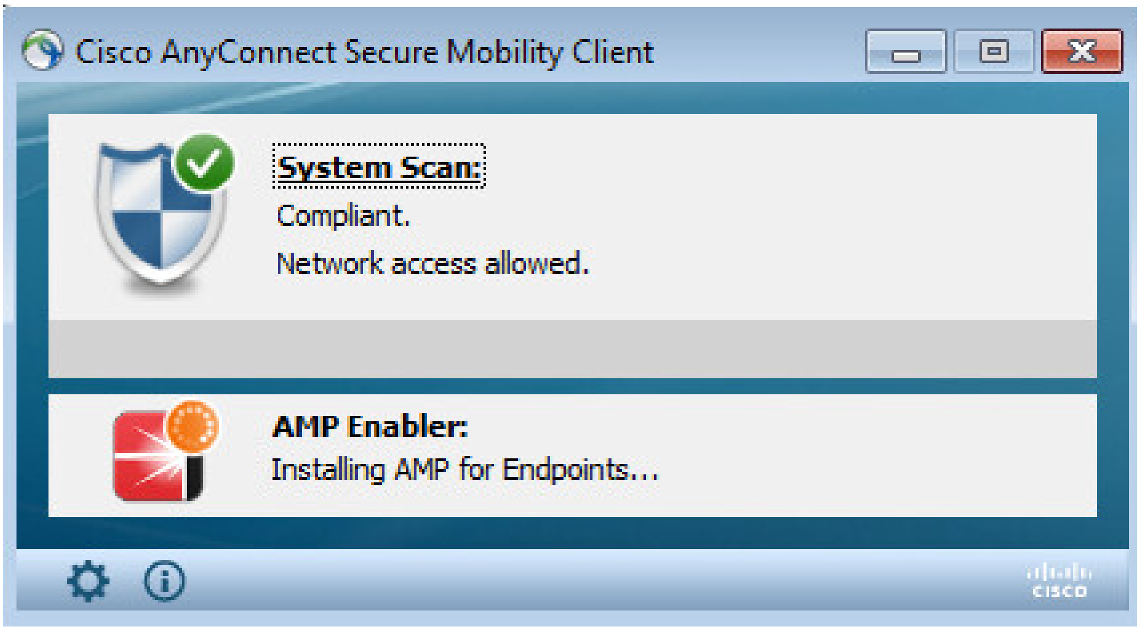
System Scan:

Compliant.

Network access allowed.

AMP Enabler:

Downloading AMP for Endpoints...



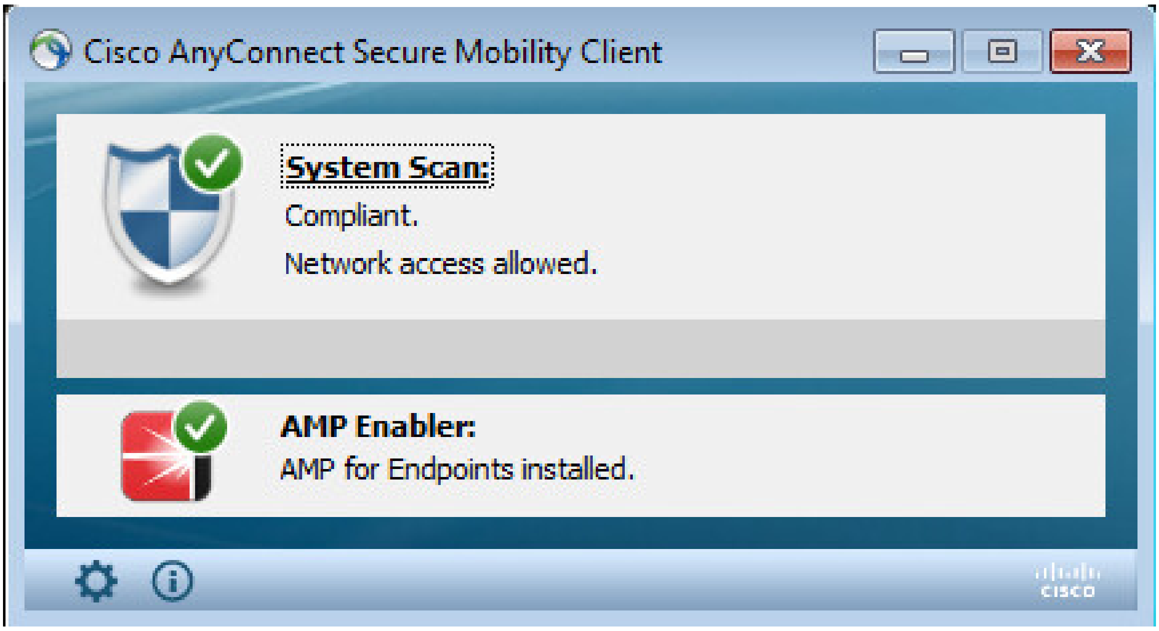
System Scan:

Compliant.

Network access allowed.

AMP Enabler:

Installing AMP for Endpoints...



System Scan:

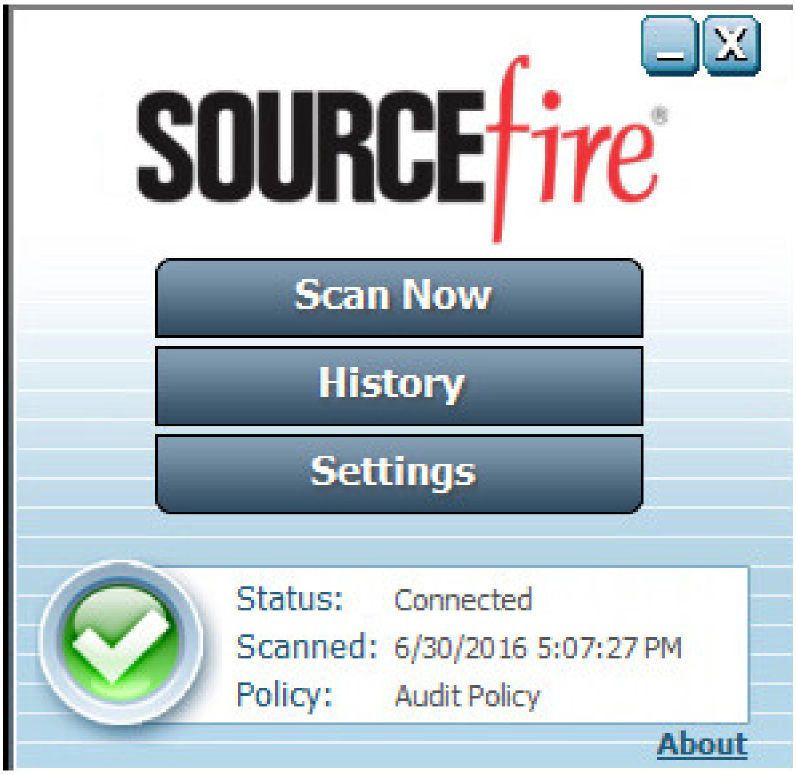
Compliant.

Network access allowed.

AMP Enabler:

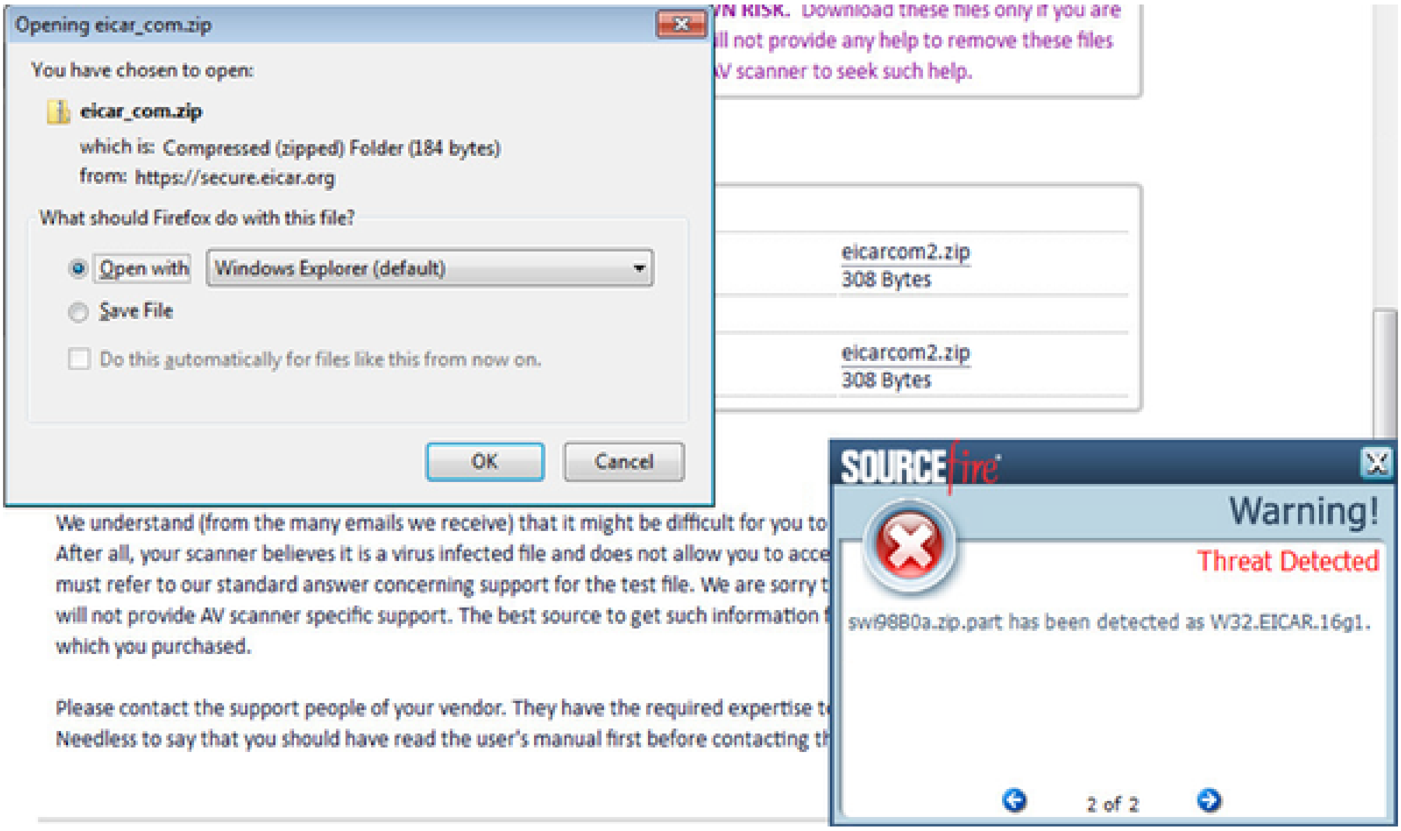
AMP for Endpoints installed.

AMP连接器出现。



Status: Connected
Scanned: 6/30/2016 5:07:27 PM
Policy: Audit Policy

要测试在动作的AMP下载在压缩文件包含的Eicar字符串。威胁被发现，并且向AMP Cloud报告。



You have chosen to open:

eicar_com.zip

which is: Compressed (zipped) Folder (184 bytes)

from: https://secure.eicar.org

What should Firefox do with this file?

● Open with Windows Explorer (default)

○ Save File

□ Do this automatically for files like this from now on.

WN RISK. Download these files only if you are
ill not provide any help to remove these files
V scanner to seek such help.

eicarcom2.zip
308 Bytes

eicarcom2.zip
308 Bytes

We understand (from the many emails we receive) that it might be difficult for you to
After all, your scanner believes it is a virus infected file and does not allow you to acce
must refer to our standard answer concerning support for the test file. We are sorry t
will not provide AV scanner specific support. The best source to get such information f
which you purchased.

Please contact the support people of your vendor. They have the required expertise t
Needless to say that you should have read the user's manual first before contacting th

Warning!

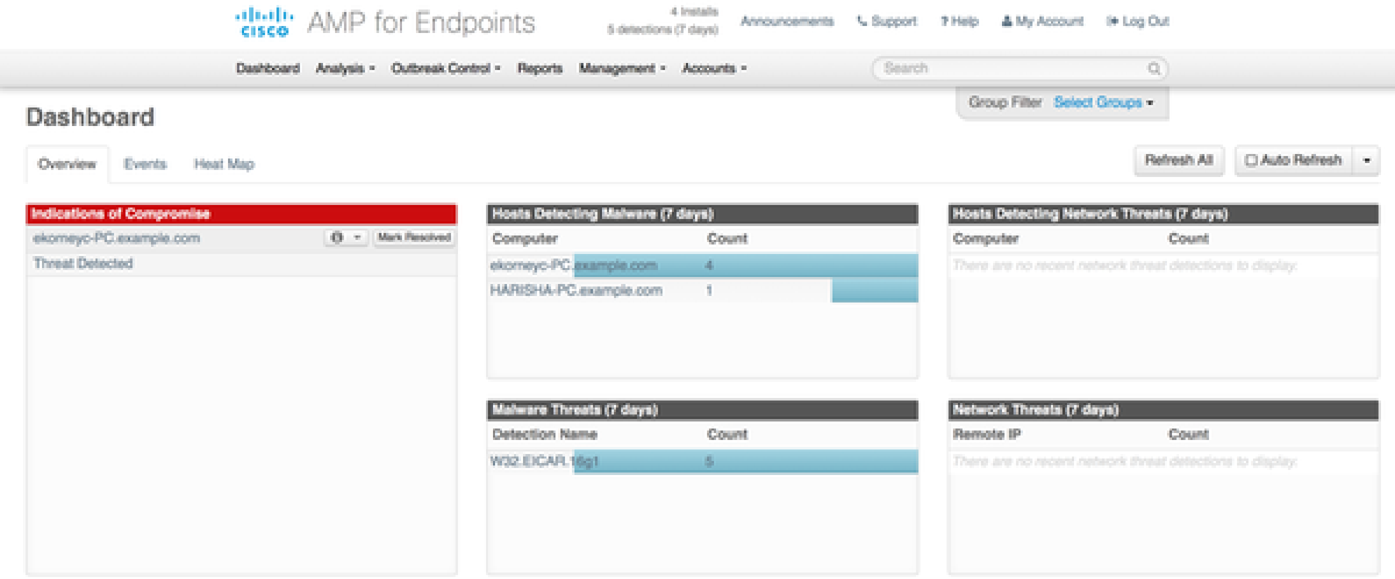
Threat Detected

swi9880a.zip.part has been detected as W32.EICAR.16g1.

2 of 2

AMP Cloud

可以使用要验证AMP网云威胁显示板的详细资料。



Dashboard

Indications of Compromise

ekorneyc-PC.example.com

Threat Detected

Hosts Detecting Malware (7 days)

Computer	Count
ekorneyc-PC.example.com	4
HARISHA-PC.example.com	1

Hosts Detecting Network Threats (7 days)

Computer	Count

There are no recent network threat detections to display.

Malware Threats (7 days)

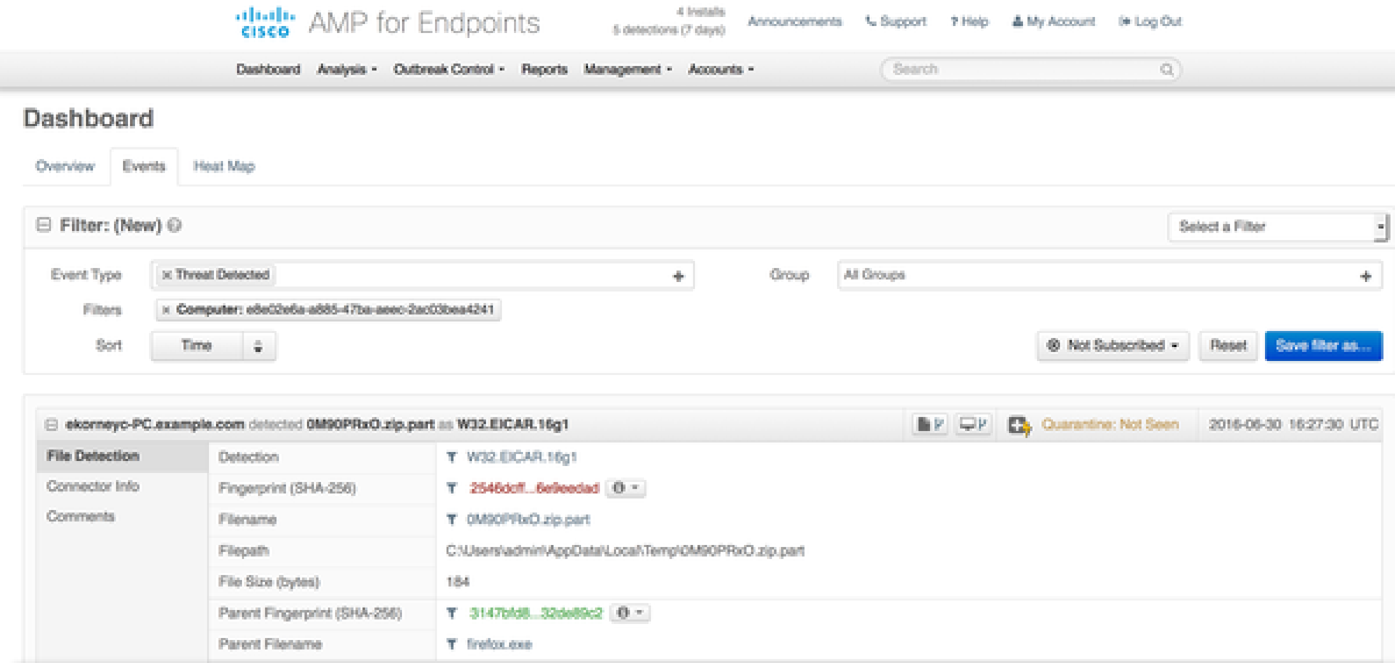
Detection Name	Count
W32.EICAR.16g1	5

Network Threats (7 days)

Remote IP	Count

There are no recent network threat detections to display.

为了获得关于威胁的更多详细资料，文件路径和fingerpints，您能点击主机，发现malware。



Dashboard

Filter: (New)

Event Type: × Threat Detected

Group: All Groups

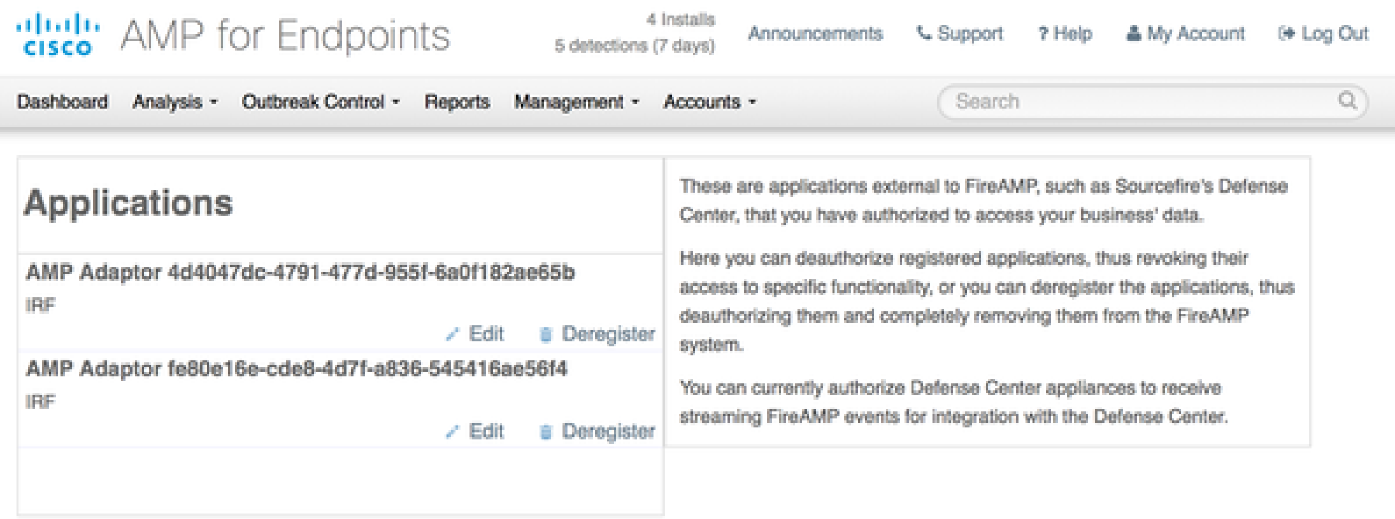
Filters: × Computer: e8e02e6a-a885-47ba-aeec-2ac03bea4241

Sort: Time

ekorneyc-PC.example.com detected **0M90PRxO.zip.part** as **W32.EICAR.16g1** 2016-06-30 16:27:30 UTC

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)	3147bfd8...32de89c2
Parent Filename	firefox.exe

查看或注销登记您能连接到帐户>应用程序ISE的实例



Applications

AMP Adaptor 4d4047dc-4791-477d-955f-6a0f182ae65b

IRF

AMP Adaptor fe80e16e-cde8-4d7f-a836-545416ae56f4

IRF

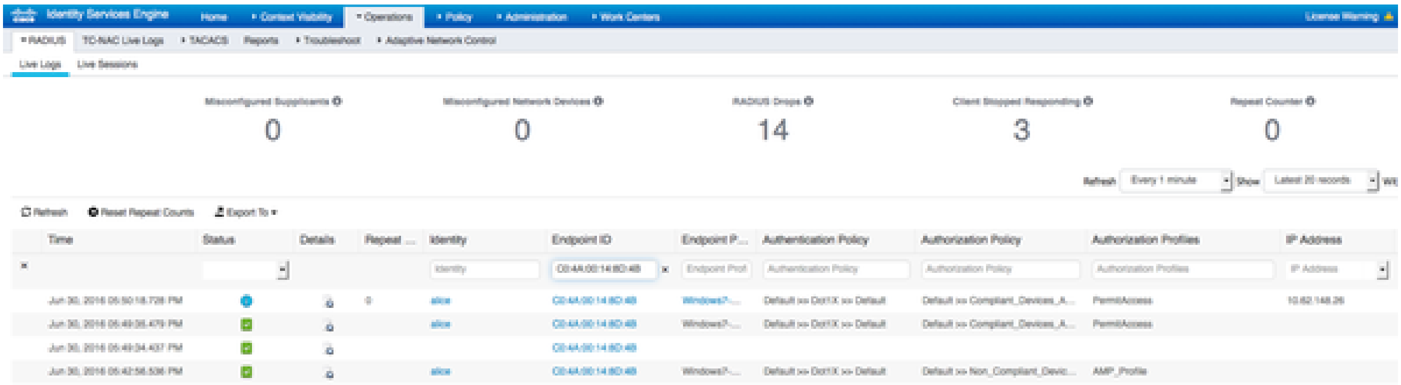
These are applications external to FireAMP, such as Sourcefire's Defense Center, that you have authorized to access your business' data.

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

在ISE正常状态流被看到，重定向首先发生检查网络标准。当终端是兼容的，发送CoA Reauth，并且与PermitAccess的新配置文件分配。

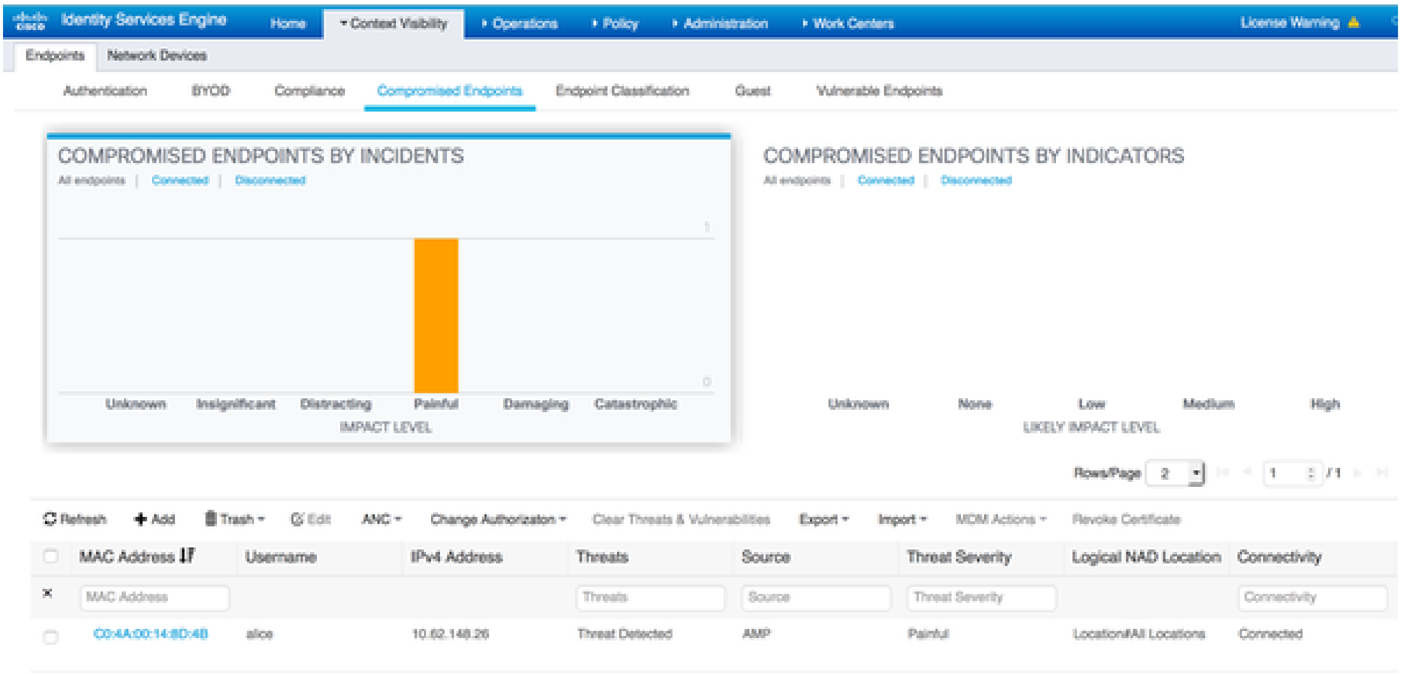


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	14	3	0

Refresh Every 1 minute Show Latest 20 records

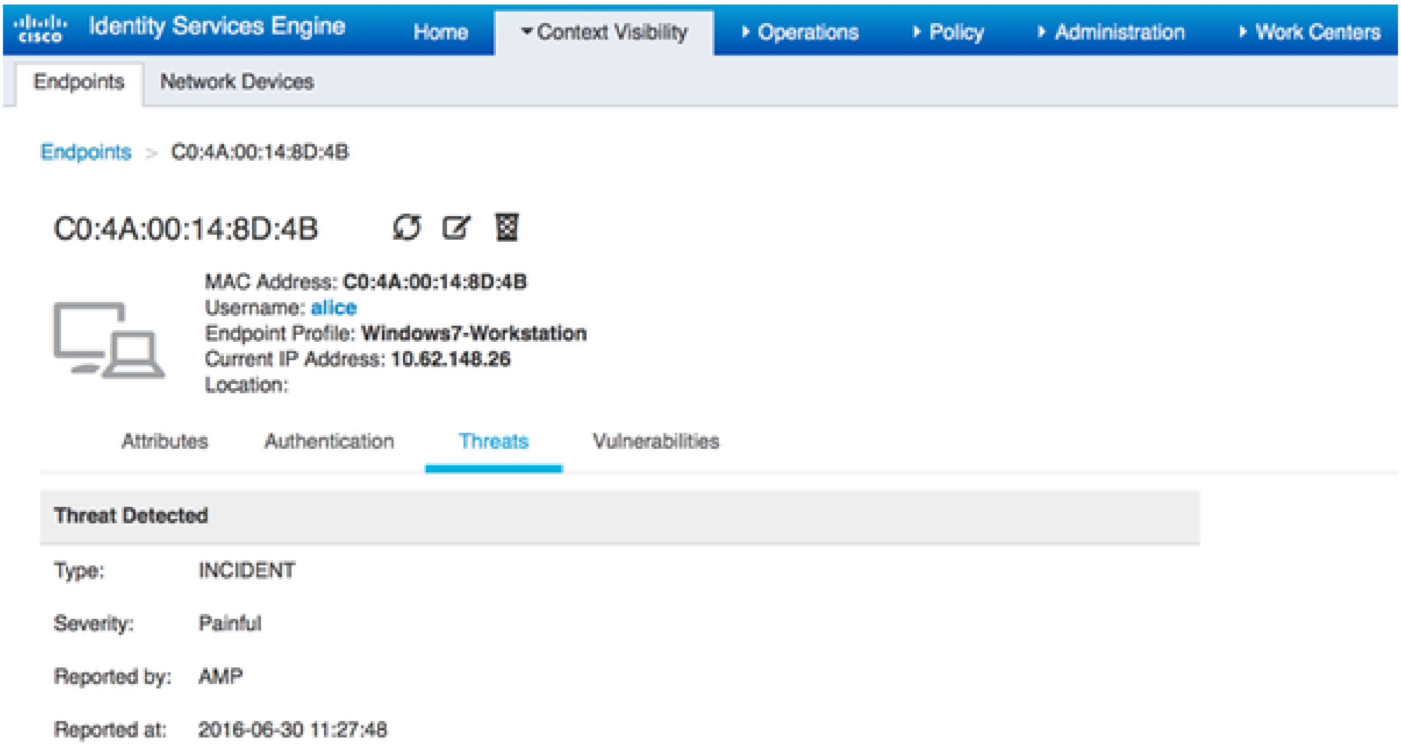
Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Jun 30, 2016 05:50:18.728 PM	●		0	alice	C0:4A:00:14:8D:4B	Windows7-...	Default >> Dot1X >> Default	Default >> Compliant_Devices_A...	PermitAccess	10.62.148.26
Jun 30, 2016 05:49:35.479 PM	✓			alice	C0:4A:00:14:8D:4B	Windows7-...	Default >> Dot1X >> Default	Default >> Compliant_Devices_A...	PermitAccess	
Jun 30, 2016 05:49:34.437 PM	✓				C0:4A:00:14:8D:4B					
Jun 30, 2016 05:42:56.536 PM	✓			alice	C0:4A:00:14:8D:4B	Windows7-...	Default >> Dot1X >> Default	Default >> Non_Compliant_Devic...	AMP_Profile	

查看您能连接到上下文公开性>终端>减弱的终端的被发现的威胁



□	MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivity
□	C0:4A:00:14:8D:4B	alice	10.62.148.26	Threat Detected	AMP	Painful	Location#All Locations	Connected

如果选择终端并且连接对威胁选项，更多详细资料显示。



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

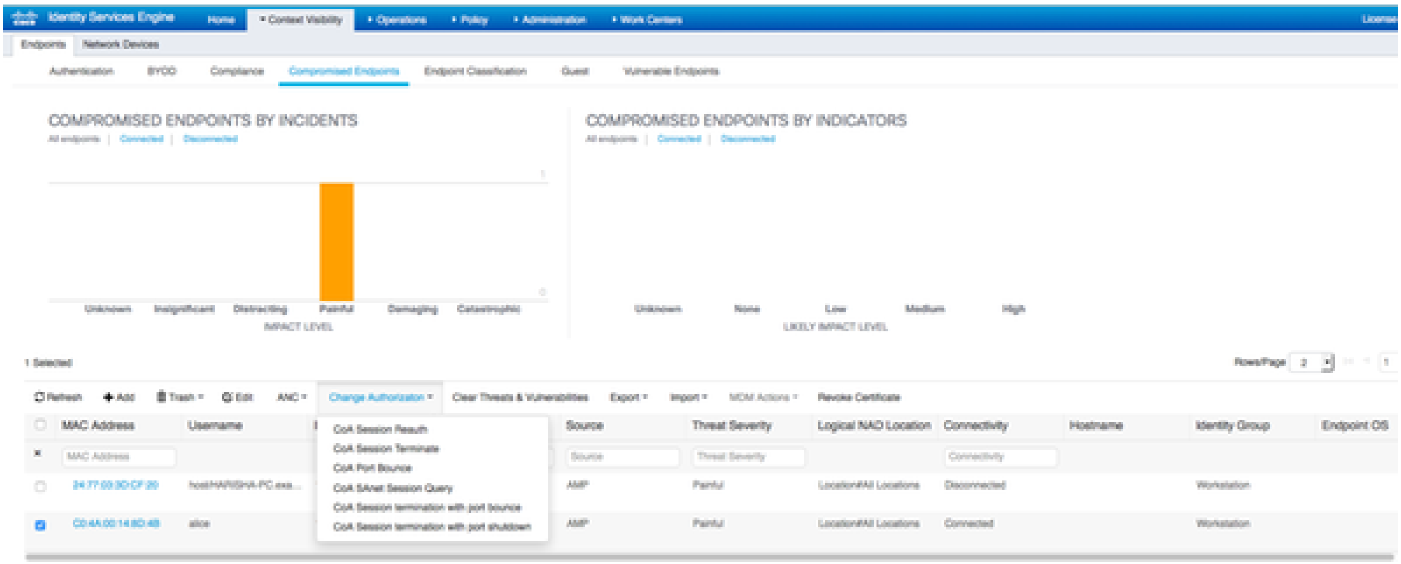
C0:4A:00:14:8D:4B

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

Threat Detected

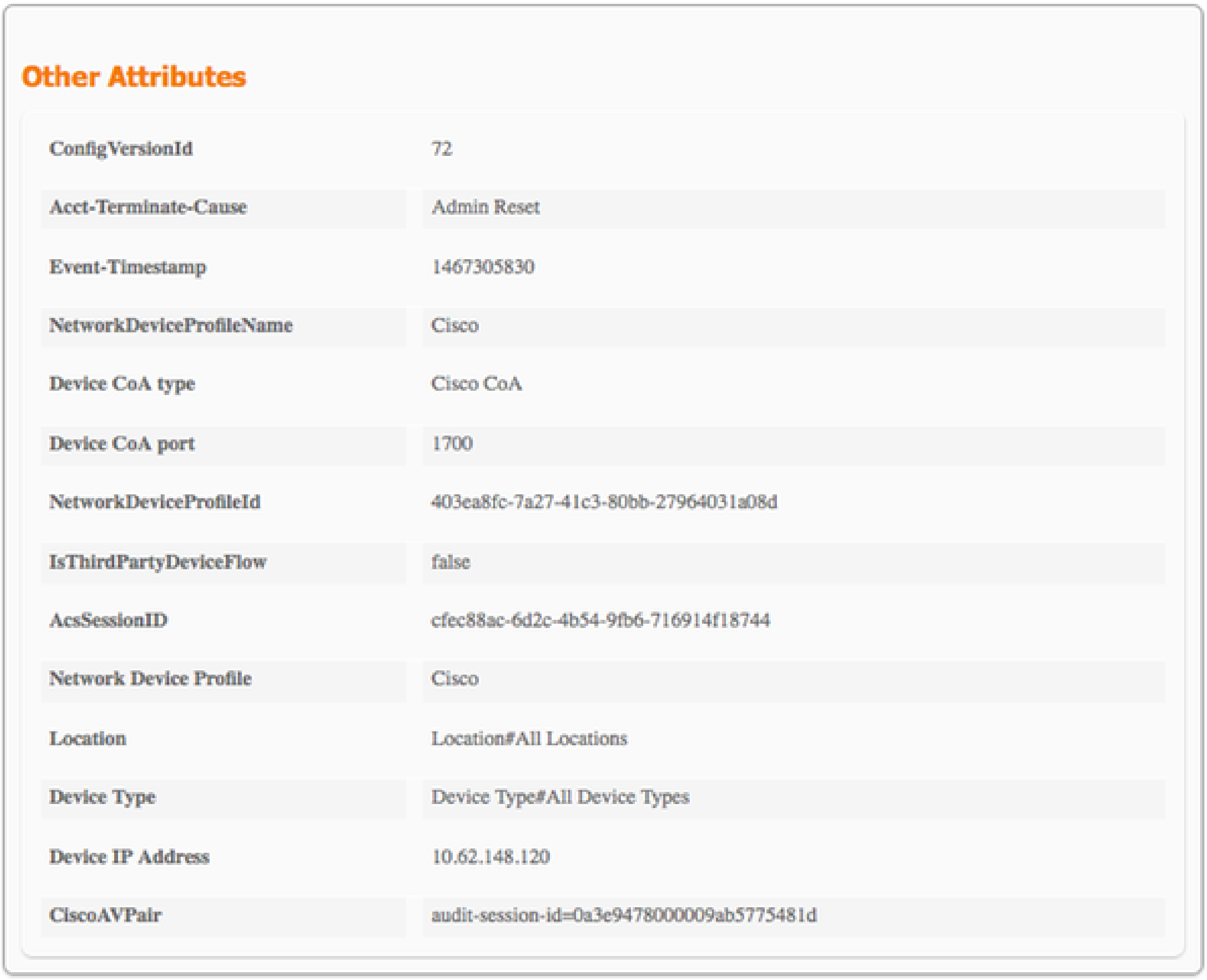
Type:	INCIDENT
Severity:	Painful
Reported by:	AMP
Reported at:	2016-06-30 11:27:48

当威胁事件为终端时被发现，您能选择终端的MAC地址在折衷的终端页的和运用ANC策略例如(若被设定，检疫)。或者您能发出授权的更改终止会话。



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

如果CoA会话Terminate选择， ISE发送CoA断开，并且客户端丢失对网络的访问。

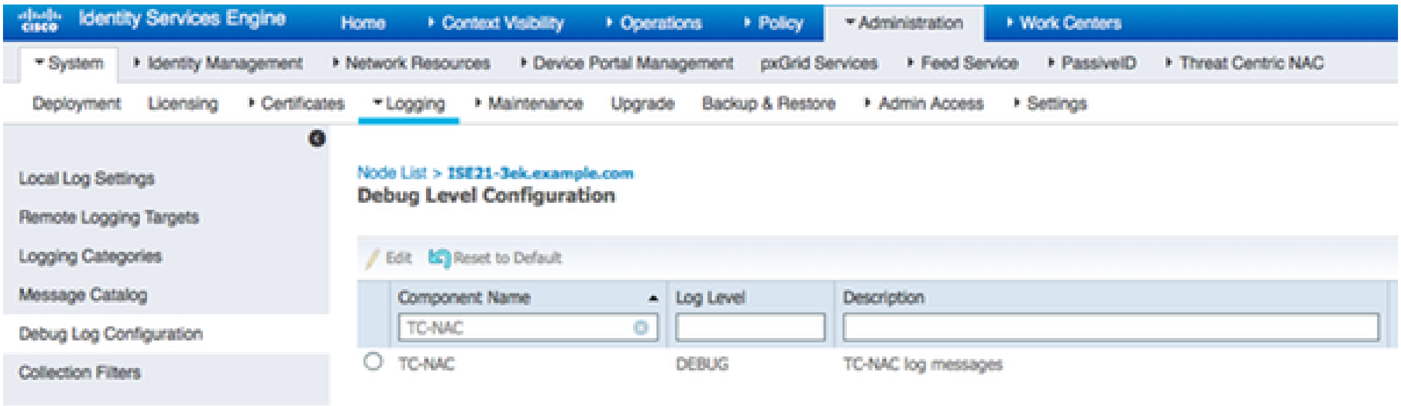


Other Attributes

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

Troubleshoot

为了在ISE的关闭调试连接对管理>System >记录>调试日志配置，挑选TC-NAC节点并且改变TC-NAC组件的**日志标准调试**



Node List > ISE21-3ek.example.com

Debug Level Configuration

Component Name	Log Level	Description
TC-NAC		
○ TC-NAC	DEBUG	TC-NAC log messages

将被检查的日志- irf.log。您能直接地从ISE CLI盯梢它：

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

威胁从AMP Cloud被遭受

```
2016-06-30 18:27:48,617[IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:53 -     -
com.cisco.cpm.irf.service.IrfNotificationHandler$MyNotificationHandler@3fac8043
{messageType=NOTIFICATION messageId=THREAT_EVENT content= {“c0:4a:00:14:8d:4b" [{“”
{“Impact_Qualification” “”} “” 1467304068599 “” “AMP” “” “”}]} ‘priority=0 timestamp=Thu Jun 30
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=nullheaders=null delivery-mode=null priority=0
correlation-id=nullreply-to=nullexpiration=nullmessage-id=THREAT_EVENTtimestamp=null
type=NOTIFICATION user-id=null app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4 cluster-id=null)}
2016-06-30 18:27:48,617[IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.service.IrfNotificationHandler:handle:140 -     -{messageType=NOTIFICATION
messageId=THREAT_EVENT content= {“c0:4a:00:14:8d:4b" [{“” {“Impact_Qualification” “”} “”
1467304068599 “” “AMP” “” “”}]} ‘priority=0 timestamp=Thu Jun 30 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=nullheaders=null delivery-mode=null priority=0
correlation-id=nullreply-to=nullexpiration=nullmessage-id=THREAT_EVENTtimestamp=null
type=NOTIFICATION user-id=null app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4 cluster-id=null)}
2016-06-30 18:27:48,617[IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:59 -     -Envelope(deliveryTag=79
redeliver=falseexchange=irf.topic.events routingKey=irf.events.threat) #contentHeader<basic>
(content-type=application/json content-encoding=nullheaders=null delivery-mode=null priority=0
correlation-id=nullreply-to=nullexpiration=nullmessage-id=THREAT_EVENTtimestamp=null
type=NOTIFICATION user-id=null app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4 cluster-id=null)
2016-06-30 18:27:48,706[IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:parseNotification:221 -     -{messageType=NOTIFICATION
messageId=THREAT_EVENT content='{"c0:4a:00:14:8d:4b" [{“” {“Impact_Qualification” “”} “”
1467304068599 “” “AMP” “” “”}]} ‘priority=0 timestamp=Thu Jun 30 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=nullheaders=null delivery-mode=null priority=0
correlation-id=nullreply-to=nullexpiration=nullmessage-id=THREAT_EVENTtimestamp=null
type=NOTIFICATION user-id=null app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4 cluster-id=null)}
```

关于威胁的信息被发送到PAN

```
2016-06-30 18:27:48,724[IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:storeEventsInES:366 -     -c0:4a:00:14:8d:4b {incident=
{Impact_Qualification=Painful} time-stamp=1467304068599vendor=AMP title=Threat}
```