



# How-To Threat Centric NAC Cisco AMP for Endpoints in Cloud and Cisco Identity Service Engine (ISE) Integration using STIX Technology

Author: John Eppich

## Table of Contents

<b>About this Document</b> .....	<b>3</b>
<b>Introduction</b>	<b>4</b>
<b>Technical Details</b> .....	<b>5</b>
<b>Cisco Identity Service Engine (ISE) Settings</b> .....	<b>6</b>
Enabling TC-NAC Service in ISE.....	6
Configuring ISE TC-NAC AMP Connector.....	7
<b>Cisco AMP for Endpoints in the Cloud</b> .....	<b>11</b>
Configuring TC-NAC AMP Connector.....	11
<b>Triggering a Threat Detection</b> .....	<b>13</b>
Context Visibility Reports .....	14
ANC Policies .....	16
<b>Troubleshooting</b> .....	<b>18</b>
AMP Rejects Cisco Cloud AMP for Endpoints Approval.....	18
De-Register Rejects Cisco Cloud AMP for Endpoints Approval .....	18
Error Status trying to Configure Adaptor.....	18

## About this Document

---

This document is for Cisco Engineers and customers deploying Cisco Threat Centric NAC using Cisco Advanced Malware Protection (AMP) for Endpoints in the Cloud (FireAMP v5.3.2016072523 or greater) with Cisco Identity Services Engine (ISE) 2.1. ISE needs an APEX license for the ability to subscribe to the Cloud AMP for Endpoints.

Cisco AMP for Endpoint integration does not use Cisco platform Exchange Grid (pxGrid) for ISE integration, instead it uses Structured Threat Information Expression (STIX). STIX is an information exchange language and used to exchange cyber threat intelligence with organizations. It allows a common framework for organizations to share cyber threat information and adapt quicker to computer-based attacks.

Cisco Threat Centric NAC using Cisco AMP for Endpoints in the Cloud also falls into the Rapid Threat Containment category. Cisco Security Solutions and Ecosystem and CSTA partner solutions that fall into this category use Adaptive Network Control (ANC) mitigation actions to respond to or contain threats by issuing mitigation actions either from pxGrid, ISE EPS RESTful API or STIX.

Cisco Threat Centric NAC using Cisco AMP for Endpoints perform threat detection and malware analysis. The ISE STIX integration provides visibility into compromised hosts and provides manual ANC mitigation or Change of Authorization (CoA) actions the security administrator can take with regards to an organization's security policy.

This document covers the following:

- Enabling TC-NAC
- Configuring the ISE TC-NAC AMP Connector
- Assigning AMP Group Policy to TC-NAC AMP Connector
- Threat Detection
- AMP Analysis

## Introduction

---

Cisco AMP for Endpoints in the Cloud provides threat detection and malware analysis on the endpoints. In addition, malware analysis is provided by Talos. The lightweight AMP connector provides centralized Cisco AMP Cloud policy management and contains the scanned settings, blocked applications, file exceptions, and malware analysis methods.

Cisco ISE (Identity Services Engine) is an identity solution, providing ISE 802.1X authentication for wired, wireless and virtual environments. In addition, ISE can perform additional functions such as Guest, Posture, and incorporate SGT (Security Group Tags) which is a component for the Cisco TrustSec solution. When a user or device authenticates to the network, there is rich contextual information that is available from these authenticated session. This session information may include the username, IP address, MAC address, posture status, SGT, and endpoint profile information that provides more information around the IP event. Cisco platform exchange protocol (pxGrid) allows the sharing of this contextual information ecosystem and CSTA partners.

Currently ISE cannot consume information from ecosystem and CSTA partners, this is where STIX technology comes in. STIX is a framework for sharing cyber threat information among security solutions. ISE consumes the Cisco AMP for Endpoints in the Cloud threat and Indications of Compromise (IOC) detection and provides visibility into the endpoints, where the security administrator can enforce an organization's security policy by issuing an Adaptive Network Control (ANC) mitigation policies or by issuing Change of Authorization network actions on the endpoints reducing risks stemming from computer-based attacks.

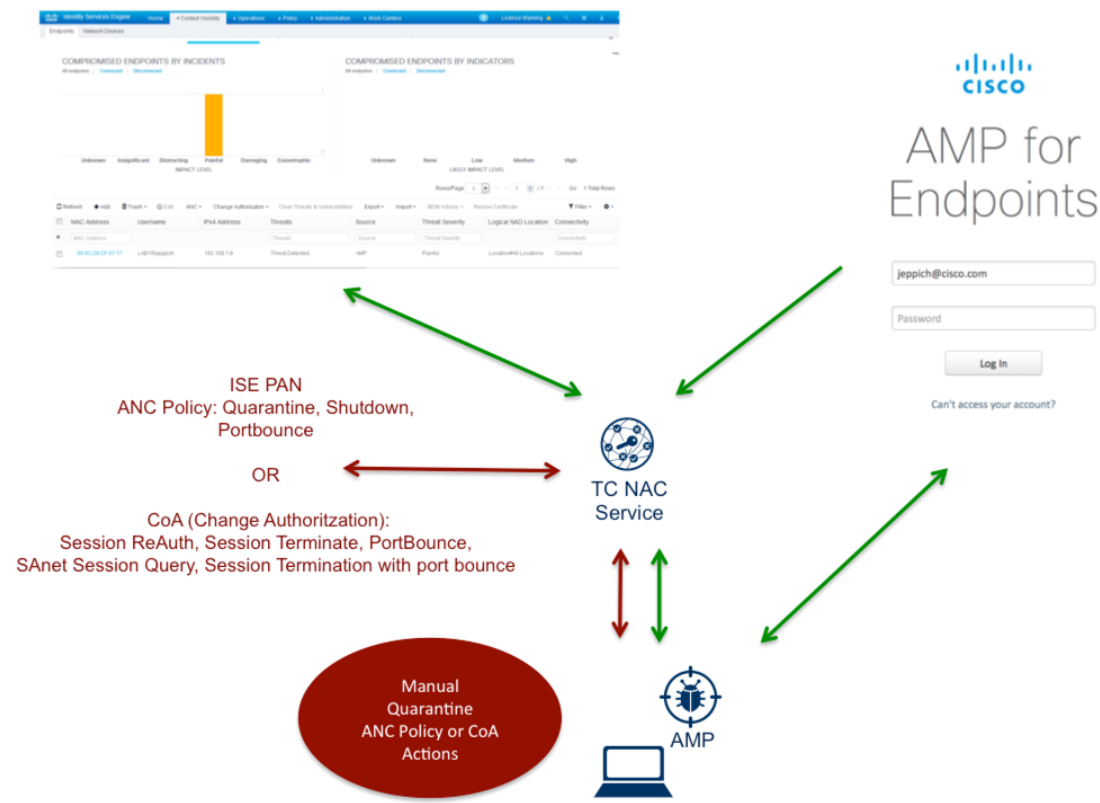
# Technical Details

Cisco AMP for Endpoints in the Cloud provides threat detection and malware analysis to ISE in real-time. Cisco AMP for Endpoints in the Cloud publishes scan information to cloud based topics, and ISE AMP subscribes to this topic and receives the threat-based information in real-time using STIX technology.

The TC-NAC service enables Incidents Response Framework (IRF), which contains the configuration data and ISE AMP connector. The ISE AMP connector obtains and receives Cisco AMP for Endpoints threat information in real-time and sends this information over to the ISE (Policy Administration Node) PAN node for context visibility reporting. The security administrator can enforce an organization’s security policy taking manual Adaptive Network Control (ANC) mitigation actions on compromised hosts and quarantining them. Additionally (Change of Authorization (CoA) network actions such as session re-auth. Session terminate, portbounce can take place instead of assigning compromised hosts to an ANC quarantine policy.

The TC-NAC service should be enabled on an ISE Policy Service Node (PSN) in a productional deployment. There can be only 1 TC-NAC enabled service per ISE deployment. If the PSN with the TC-NAC enabled service goes down, TC-NAC can be enabled another PSN.

The PSN node on which TC-NAC role is enabled acts as consumer of threat data. The adapter or TC NAC connector consumes this data from Cisco AMP for Endpoints in the Cloud and is sent to ISE engine for further processing (i.e. aggregating threats, triggering CoA etc.). Once a threat is received for a given endpoint on this Policy Service Node (PSN) node, this TC-NAC code on node PSN1 would find out which PSN say node PSN2 had authenticated the endpoint. It then triggers CoA to that PSN2 node and tracks whether the operation is successful or a failure.



# Cisco Identity Service Engine (ISE) Settings

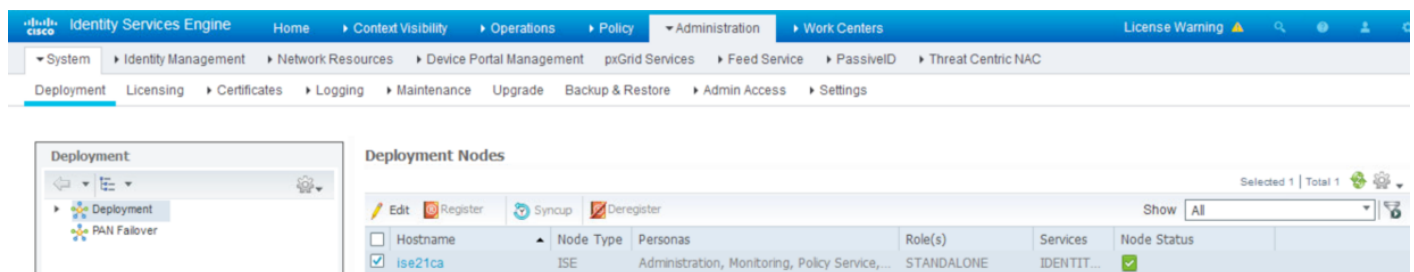
This section details the procedure for enabling the TC-NAC service and the ISE TC-NAC AMP Connector.

## Enabling TC-NAC Service in ISE

Enable the TC-NAC service and verify the Docker, Rabbit MQ services and IRF core engine started.

**Step 1** Enable TC-NAC

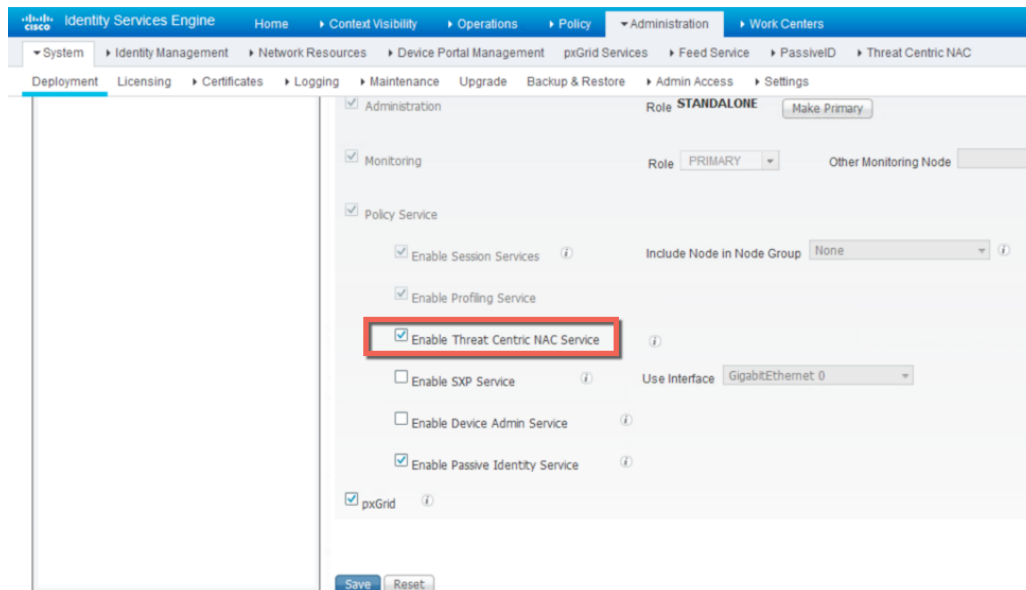
**Step 2** Select **Administration->System->Deployment->Select the node->Edit**



The screenshot shows the ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation tree with 'Deployment' selected. The main content area displays 'Deployment Nodes' with a table of nodes. The 'ise21ca' node is selected, and the 'Edit' button is highlighted.

Hostname	Node Type	Personas	Role(s)	Services	Node Status
ise21ca	ISE	Administration, Monitoring, Policy Service,...	STANDALONE	IDENTIT...	✓

**Step 3** Enable Threat Centric-NAC



The screenshot shows the ISE Administration console configuration page for the 'ise21ca' node. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation tree with 'Deployment' selected. The main content area displays the configuration for the 'ise21ca' node. The 'Enable Threat Centric NAC Service' checkbox is checked and highlighted with a red box.

Service	Role	Other Monitoring Node	Include Node in Node Group	Use Interface
Administration	STANDALONE		None	GigabitEthernet 0
Monitoring	PRIMARY			
Policy Service			None	
Enable Session Services				
Enable Profiling Service				
<b>Enable Threat Centric NAC Service</b>				
Enable SXP Service				
Enable Device Admin Service				
Enable Passive Identity Service				
pxGrid				

**Step 4** Select **Save**

**Step 5** Run “application status ise’ to view the Threat Centric NAC services have started.

```
application status ise
```

You should see the TC-NAC services initialize and then in a running state

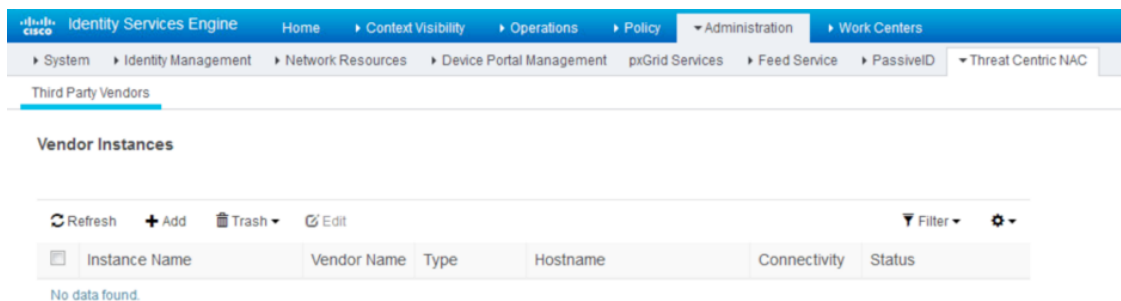
```
ise21ca/admin# sh application status ise
ISE PROCESS NAME          STATE          PROCESS ID
-----
Database Listener         running        3604
Database Server           running        69 PROCESSES
Application Server        running        7261
Profiler Database         running        4994
ISE Indexing Engine       running        7672
AD Connector              running        8681
M&T Session Database     running        3061
M&T Log Collector        running        8272
M&T Log Processor        running        8185
Certificate Authority Service running        8019
EST Service               running        16202
TCP Engine Service       disabled
TC-NAC Docker Service    running        3335
TC-NAC MongoDB Container running        6049
TC-NAC RabbitMQ Container running        6854
TC-NAC Core Engine Container running        7685
UA Database               running        8245
UA Service                running        8446
pxGrid Infrastructure Service running        9752
pxGrid Publisher-Subscriber Service running        9892
```

## Configuring ISE TC-NAC AMP Connector

The ISE TC-NC AMP Connector contains the Cisco AMP cloud configuration. It receives Cisco AMP threat information and provides endpoint threat information to the ISE REST API and the ISE Policy Administration Node (PAN) node for context visibility.

**Step 1** Select **Administration->Threat Centric NAC->Third Party Vendors->**

You should see the following:



- Step 2** From the Vendor drop-down menu, select **AMP-Threat**
- Step 3** Create Instance Name, **AMP-Lab**

**Note:** This can be any name

- Step 4** Select **Save**
- Step 5** You should see the following:

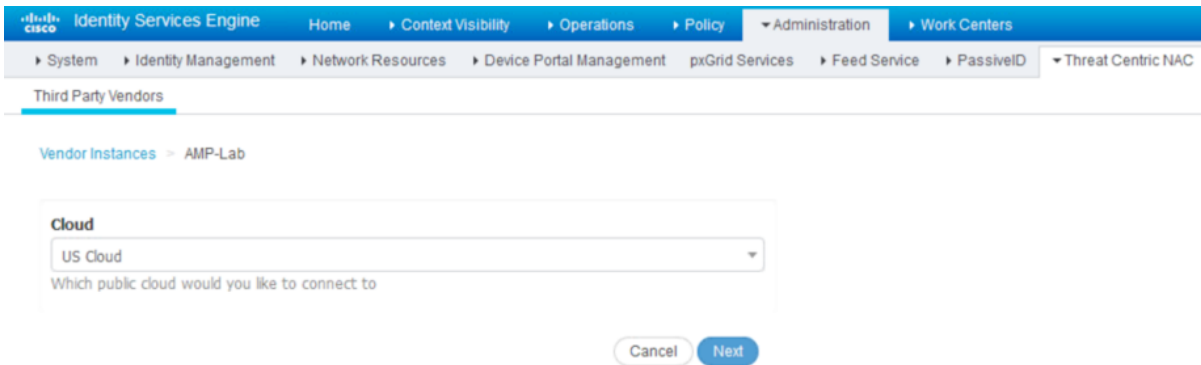
**Note:** The state of “Not Reachable” will change to “Ready to Configure”

Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
Qualys-Lab	Qualys	VA	qualysguard.qg2.apps.qualys.c...	Connected	Active
AMP-Lab	AMP	THREAT		Disconnected	Ready to configure

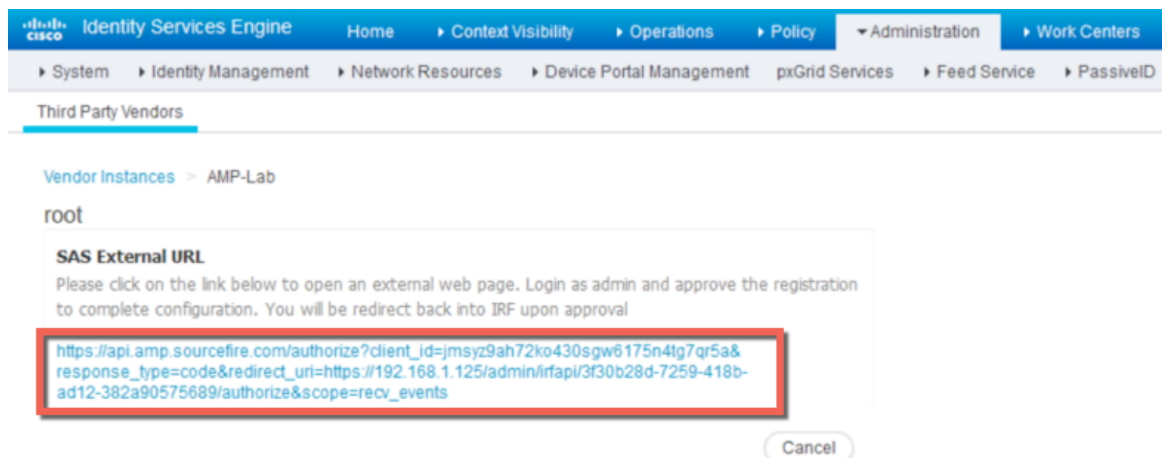
- Step 6** Select **Ready to Configure**
- Step 7** Configure proxy settings if applicable



- Step 8 Select **Next**
- Step 9 Select the Public Cloud to connect to



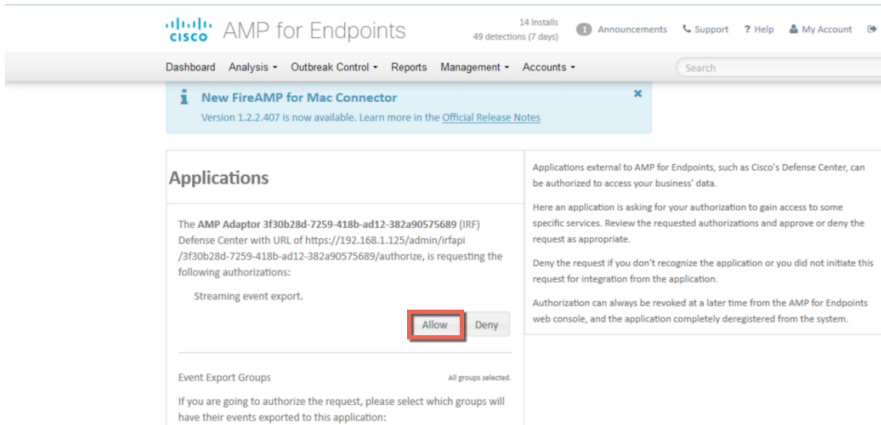
- Step 10 Select **Next**
- Step 11 Select below link to connect to **AMP for Endpoints**



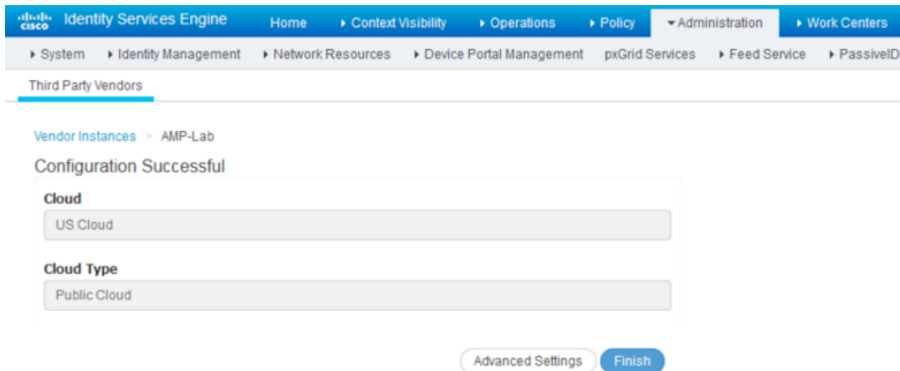
- Step 12 Login with your credentials



**Step 13** Select **Allow** for the streaming event



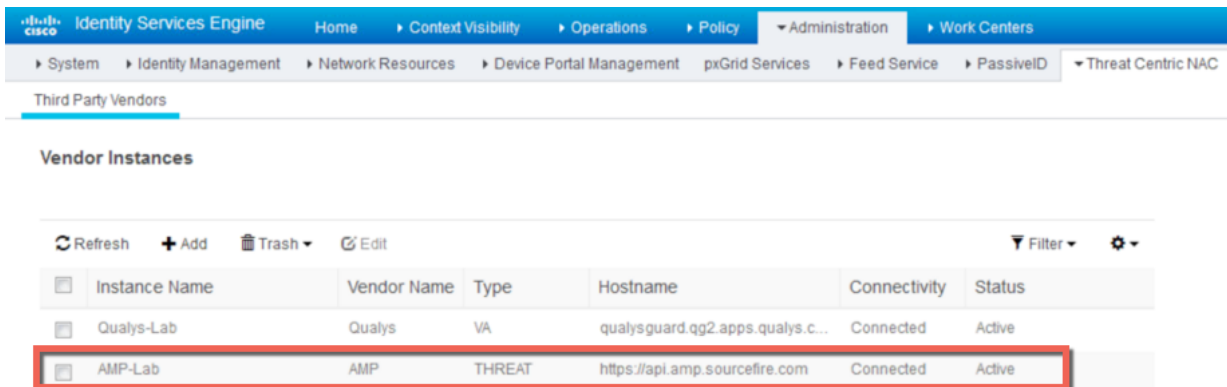
**Step 14** You should see finished connection



**Step 15** Select **Finished**

**Step 16** You should see the action as Active

**Note:** The state will be changed from Configured to Active

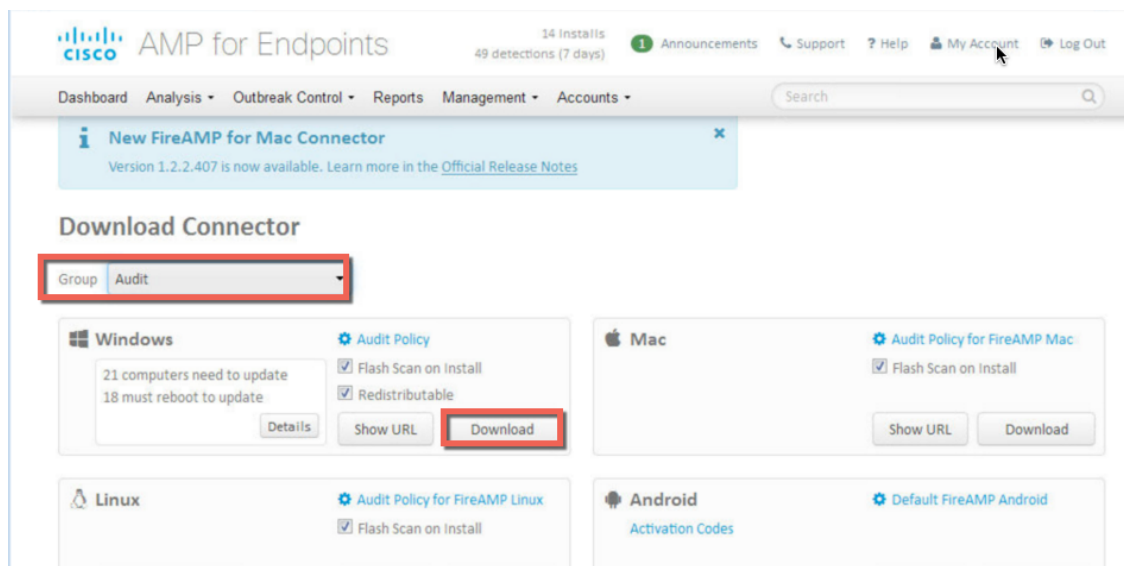


## Cisco AMP for Endpoints in the Cloud

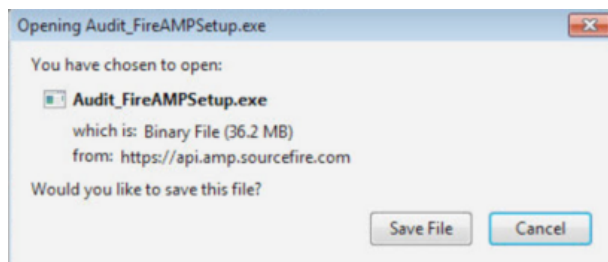
The Cisco TC-NAC AMP connector is a lightweight connector used for metadata and malware analysis and gets installed on the endpoint. The Cisco TC-NAC AMP Connector is assigned to a Cisco AMP policy that will have additional configuration settings such as: blocking applications, scanning detection methods, file exclusions and IP blacklists and whitelists.

### Configuring TC-NAC AMP Connector

- Step 1** Open browser on PC client connect to <http://api.amp.sourcefire.com>  
**Step 2** Select **Management->Download Connector->select Group->Audit->Download**



- Step 3** Save the file locally



- Step 4** Install the TC-NAC AMP Connector, after the install you should see the Scan Settings appear



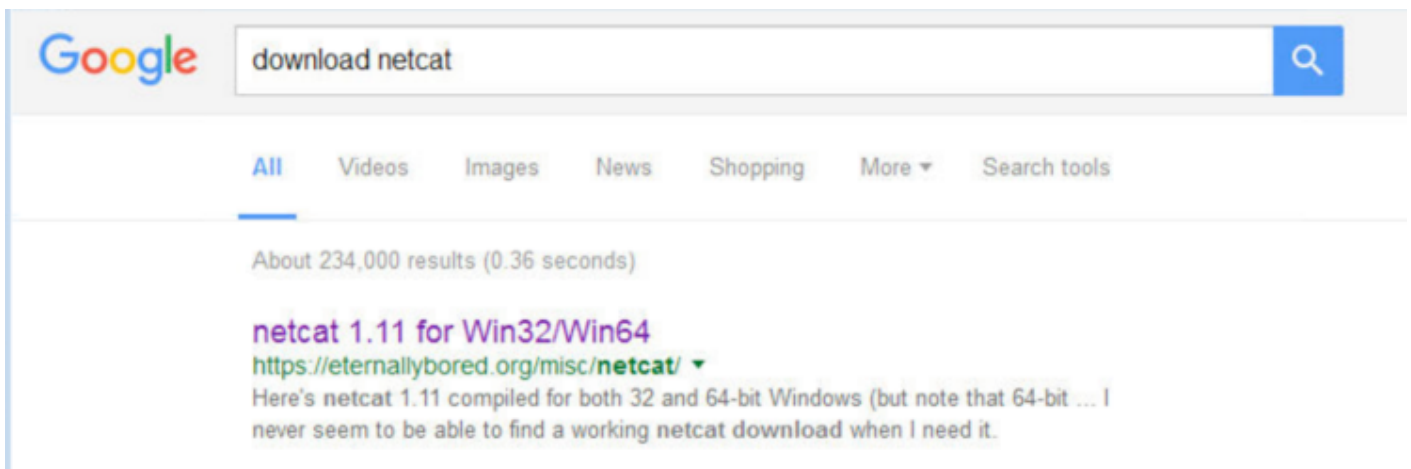
- Step 5** You can select “Scan Now” for to begin scanning the endpoint based on the Cisco AMP for Endpoints in the Cloud policy that has been assigned to the ISE TC-NAC AMP connector.

## Triggering a Threat Detection

In this section, netcat is downloaded and the threat is detected by the Cisco AMP connector. We will view the compromised endpoint in the ISE Context visibility screen and manually quarantine the endpoint by assigning an ANC Quarantine mitigation policy to the endpoint.

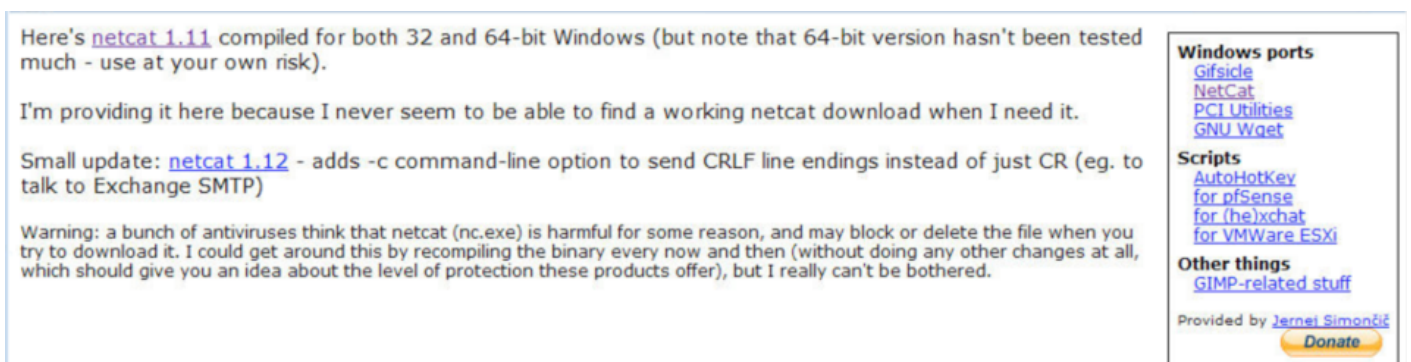
**Step 1** Open your browser: [www.google.com](http://www.google.com)

**Step 2** Type in: **download netcat**

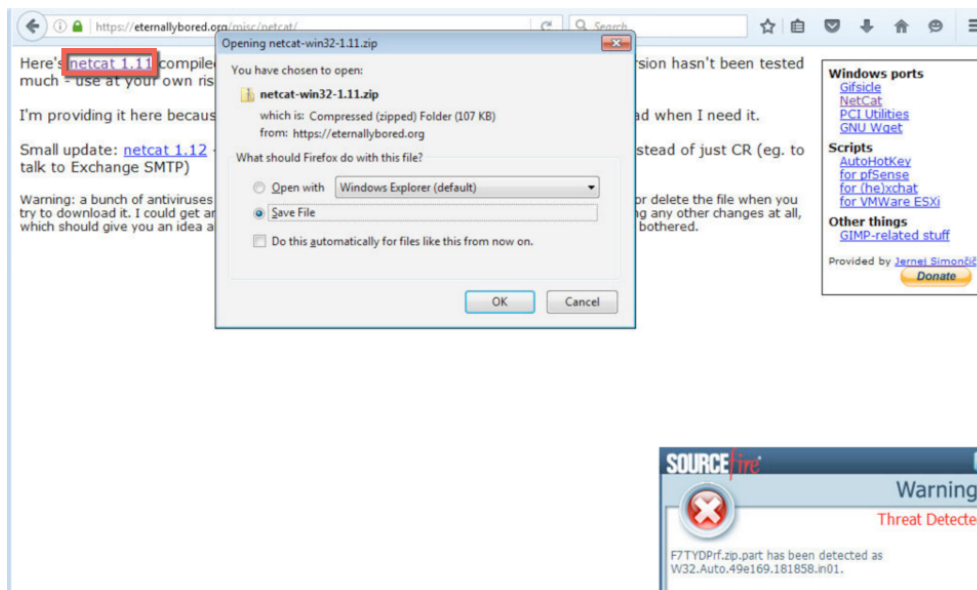


**Step 3** Select **netcat 1.11 for Win32/Win64**

**Step 4** You should see the following



**Step 5** Select netcat 1.11, you should see threat detected notification appear:



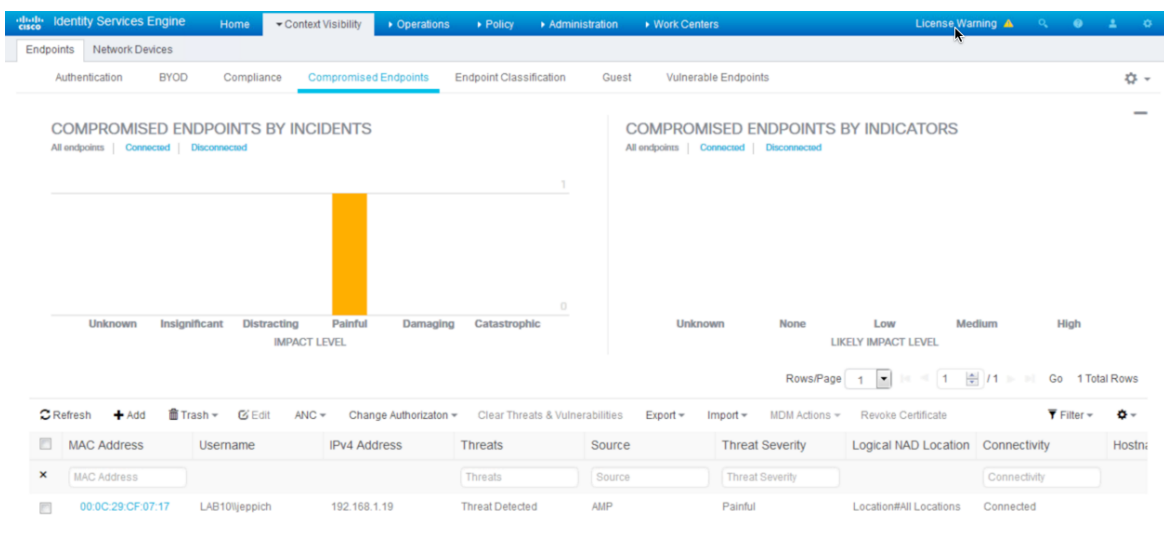
**Step 6** Select **OK** to save the file

## Context Visibility Reports

Context Visibility Reports provide visibility into detected threats as incidents on compromised endpoints or by executed threats as in Indications of Compromise (IOC). You can drill down into the MAC address for additional attribute details and manually assign endpoints to Adaptive Network Control (ANC) Policies such as quarantine.

The categories on the **Impact Level** and **Likely Impact Level** of the Context Visibility Report are determined by Cisco AMP for Endpoints in the Cloud

**Step 1** On ISE, select **Context Visibility->Endpoints->Compromised Endpoints**, you should see:



**Step 2** Select the **MAC address**

MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivity
00:0C:29:CF:07:17	LAB10\jeppich	192.168.1.19	Threat Detected	AMP	Painful	Location#All Locations	Connected

You should see the attribute details

Attributes

General Attributes

Description

- Static Assignment: false
- Endpoint Policy: Microsoft-Workstation
- Static Group Assignment: false
- Identity Group Assignment: Workstation

**Step 3** Select **Threats**, to view the incident

Threat Detected

- Type: INCIDENT
- Severity: Painful
- Reported by: AMP
- Reported at: 2016-07-31 13:55:01

## ANC Policies

Adaptive Network Control (ANC) Policies determine the manual mitigation responses taken on the compromised endpoints. Quarantine, Shutdown, and PortBounce are the available mitigation responses.

- Step 1** Create ANC Policy and assign Endpoint to quarantine ANC policy
- Step 2** Select **Operations->Adaptive Network Control->Policy List->Add->enter name of ANC policy**

Identity Services Engine Home Context Visibility Operations Policy Administration

RADIUS TC-NAC Live Logs TACACS Reports Troubleshoot Adaptive Network Control

Policy List Endpoint Assignment

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

Name

Action \*

Cancel Submit

- Step 3** Select **Submit**
- Step 4** Assign Compromised host to ANC policy  
Select **Context Visibility->Endpoints->Compromised Endpoints->select the MAC address of compromised endpoint**

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Endpoints Network Devices

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

COMPROMISED ENDPOINTS BY INCIDENTS  
All endpoints | Connected | Disconnected

Unknown Insignificant Distracting Painful Damaging Catastrophic  
IMPACT LEVEL

COMPROMISED ENDPOINTS BY INDICATORS  
All endpoints | Connected | Disconnected

Unknown None Low Medium High  
LIKELY IMPACT LEVEL

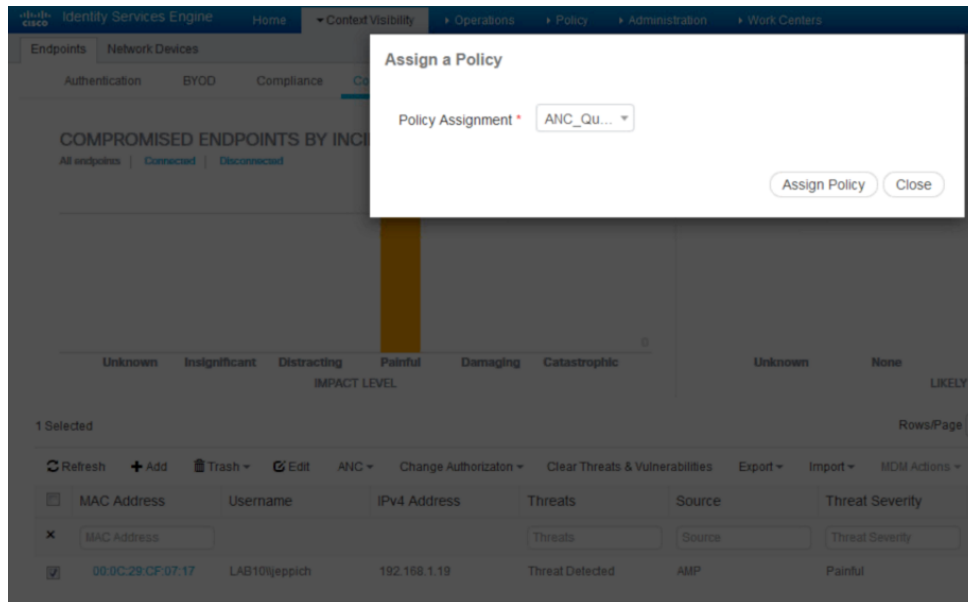
1 Selected Rows/Page 1 / 1 Go

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

MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivity
<input type="text" value="MAC Address"/>			<input type="text" value="Threats"/>	<input type="text" value="Source"/>	<input type="text" value="Threat Severity"/>		<input type="text" value="Connectivity"/>
<input checked="" type="checkbox"/>	00:0C:29:CF:07:17	LAB10\jpeppich	192.168.1.19	Threat Detected	AMP	Painful	Location#All Locations Connected



**Step 5** Select ANC->Assign Policy->ANC Quarantine



**Step 6** Select Assign Policy

## Troubleshooting

---

Listed are common issues when troubleshooting Threat Centric NAC-AMP

### AMP Rejects Cisco Cloud AMP for Endpoints Approval

Most likely cause: User is attempting to register an adaptor instance with the same MAC address as an already registered instance

Fix: Deregister old instance on AMP console

### De-Register Rejects Cisco Cloud AMP for Endpoints Approval

Select Accounts->Applications->Deregister

**AMP Adaptor 52249104-2002-4ca6-a69e-f9d0d5e90381**

IRF

 Edit  Deregister

### Error Status trying to Configure Adaptor

Most likely cause: HTTP error while making REST call to AMP (check log to verify)

Fix: Deregister instance on AMP console (if registered already) and attempt to configure adaptor again