



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**

About this Document	3
Introduction 4	
Technical Details	5
Cisco Identity Service Engine (ISE) Settings	6
Enabling TC-NAC Service in ISE	6
Configuring ISE TC-NAC AMP Connector	7
Cisco AMP for Endpoints in the Cloud	11
Configuring TC-NAC AMP Connector	11
Triggering a Threat Detection	13
Context Visibility Reports	14
ANC Policies	16
Troubleshooting	18
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 realtime 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

dentity Services Engine Home	Context Visibility	License Warning 🔺 🔍 🕘 ᆂ C
▼System ► Identity Management ► Network R	ources	Threat Centric NAC
Deployment Licensing + Certificates + Log	ng + Maintenance Upgrade Backup & Restore + Admin Access + Settings	
Deployment	Deployment Nodes	
↓		Selected 1   Total 1  🍪 🤪 🖕
<ul> <li>Deployment</li> </ul>	🖊 Edit 🔯 Register 😓 Syncup	Show All
💑 PAN Failover	Hostname A Node Type Personas Rol	e(s) Services Node Status
	✓ ise21ca ISE Administration, Monitoring, Policy Service, ST.	ANDALONE IDENTIT 🔽

#### Step 3 Enable Threat Centric-NAC

-the Identity Services Engine Home	Context Visibility      Operations      Policy      Administration      Work Centers
▼System → Identity Management → Network R	sources
Deployment Licensing + Certificates + Log	ng ► Maintenance Upgrade Backup & Restore ► Admin Access ► Settings
	Administration Role STANDALONE Make Primary
	Monitoring Role PRIMARY * Other Monitoring Node
	Policy Service
	Enable Session Services D Include Node in Node Group None v D
	Enable Profiling Service
	Enable Threat Centric NAC Service     ()
	Enable SVP Service (i) Use Interface GigabitEthemet 0 *
	Litatio SAF Service
	Enable Device Admin Service
	Enable Passive Identity Service     (i)
	🖾 pxGrid 🕖
	Save

#### 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
		2/0/
Database Listener	running	3684
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
CVD Engine Convice	dicabled	
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
VA Database	running	8245
VA Service	running	8446
pxoria intrastructure service	running	0136
		0000

### **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:

identity Services Engine	Home   Context	Visibility	Policy      Administration	Work Centers	
System Identity Management	Network Resources	Device Portal Management	t pxGrid Services + Feed S	Service   PassiveID	Threat Centric NAC     ■
Third Party Vendors					
Vendor Instances					
C Refresh + Add	sh 🕶 🕑 Edit			<b>T</b> Filter	- 0-
C Refresh + Add	sh • C Edit Vendor Name	Type Hostname	Conne	Filter ectivity Status	· o-



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

Note: This can	be any name
----------------	-------------

System Identity Mana	gement 🕨 N	Network Resou	rces Devi	ce Portal Management	pxGrid Services	Feed Service	PassiveID	- Threat Centric NAC
hird Party Vendors								
Vendor Instances > New	actorials (1) arrest	a required						
THE REAL PROPERTY AND A RE	asterisk (*) are	e required.						
Vendor*	AMP : THR	EAT			Ŧ			

#### Step 4 Select Save

**Step 5** You should see the following:

Note: The state of "Not Reachable" will change to "Ready to Configure"

cisco	Ident	lity Services Engine	Home • Context	Visibility • O	perations Pol	icy - Admin	istration 🔹 🕨	Nork Centers	
System	stem	Identity Management	Network Resources	Device Portal	Management px	Grid Services	Feed Service	PassiveID	Threat Centric
Third	Party	Vendors							
Ver	ndor l	nstances							
								_	
0	Refre	sh 🕂 Add 💼 Trash 🕇	<b>G</b> Edit					<b>▼</b> Filter	• ••
2	Refre	sh <b>+</b> Add <b>ڨ</b> Trash <b>-</b> stance Name	C Edit Vendor Name	Туре	Hostname		Connectivity	<b>▼</b> Filter	- 0-
	Refre	sh ∔Add 會Trash• stance Name ualys-Lab	C Edit     Vendor Name     Qualys	Type VA	Hostname qualysguard.qg2.	apps.qualys.c	Connectivity	Filter Status Active	- 0-

#### Step 6 Select Ready to Configure

**Step 7** Configure proxy settings if applicable

Identity Services Engine	Home Contex	t Visibility	Policy →Adm	inistration 🔹 🕨	Work Centers	
System Identity Management	<ul> <li>Network Resources</li> </ul>	Device Portal Management	t pxGrid Services	Feed Service	PassiveID	Threat Centric NAC     ■
Third Party Vendors						
Vendor Instances > AMP-Lab Enter Socks Proxy Configura	ation (Optional)					
Socks proxy host						
Optional socks proxy host. Requires	socks proxy port also t	o be set. Leave blank if not usir	g a proxy.			
Socks proxy port						
Optional socks proxy port. Requires	socks proxy host also t	o be set. Leave blank if not usir	g a proxy.			
		Can	cel Next			



#### Step 8 Select Next

#### **Step 9** Select the Public Cloud to connect to

dentity S	Services Engine	Home	Context Visibil	ity	Policy	- Administration	Work Centers	
	dentity Management	Network	Resources + D	evice Portal Manageme	nt pxGrid Ser	vices Feed Se	ervice PassiveID	
Third Party Vend	lors							
Vendor Instanc	es > AMP-Lab							
Terraor motarie								
Cloud								
US Cloud					*			
Which public	cloud would you like to	o connect to	)					
				Car	Next			

#### Step 10 Select Next

#### Step 11 Select below link to connect to AMP for Endpoints



#### **Step 12** Login with your credentials

	▶
cisco	
AMP for	
 jeppich@cisco.com	
•••••	
Log In	

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



#### Step 14 You should see finished connection

dentity Services Engine	Home   Context	Visibility	Policy → Adm	ninistration	Work Centers
System Identity Management	<ul> <li>Network Resources</li> </ul>	Device Portal Management	pxGrid Services	Feed Serv	ice PassiveID
Third Party Vendors					
Vendor Instances > AMP-Lab					
Configuration Successful					
Cloud					
US Cloud					
Cloud Type					
Public Cloud					
		Advanced Settings	Finish		

#### Step 15 Select Finished

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

Note: The state will changed from Configured to Active

isco Id	lentity Services Engine	Home • Context	Visibility > O	perations + Policy - Admin	istration 🔹 W	ork Centers	
<ul> <li>Syster</li> </ul>	m Identity Management	Network Resources	Device Portal	Management pxGrid Services	Feed Service	PassiveID	
Third Pa	arty Vendors						
Vendo	or Instances efresh ∔Add तिTrash ◄	<b>€</b> Edit				<b>▼</b> Filter	• ••
	Instance Name	Vendor Name	Туре	Hostname	Connectivity	Status	
	Qualys-Lab	Qualys	VA	qualysguard.qg2.apps.qualys.c	Connected	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 <u>http://api.amp.sourcefire.com</u>
- Step 2 Select Management->Download Connector->select Group->Audit->Download

ashb	oard Analysis - Outbreak Cont	rol • Reports Management • Ac	counts - S	earch
i	New FireAMP for Mac Cor Version 1.2.2.407 is now available.	nnector Learn more in the <u>Official Release Notes</u>	×	
Dov	wnload Connector			
roup	Audit			
Group	Audit Windows	Audit Policy	🗯 Mac	C Audit Policy for FireAMP Mac
iroup	Audit Windows 21 computers need to update 18 must reboot to update	Audit Policy     Aidit Policy     Flash Scan on Install     Redistributable	🗯 Mac	Audit Policy for FireAMP Mac     Illian Scan on Install
Group	Audit Windows 21 computers need to update 18 must reboot to update Details	Audit Policy     Audit Policy     Flash Scan on Install     Redistributable     Show URL     Download	🗯 Mac	Audit Policy for FireAMP Mac     Flash Scan on Install     Show URL     Download
iroup	Audit Windows 21 computers need to update 18 must reboot to update Details	Audit Policy Audit Policy Audit Policy Audit Policy Audit Policy for FireAMP Linux	Mac	Audit Policy for FireAMP Mac     Audit Policy for FireAMP Mac     Show URL     Download     Default FireAMP Android

#### **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: <u>www.google.com</u>

Step 2 Type in: download netcat

Google	download netcat								
	All Videos Images News Shopping More - Search tools								
	About 234,000 results (0.36 seconds)								
	netcat 1.11 for Win32/Win64 https://eternallybored.org/misc/netcat/ Here's netcat 1.11 compiled for both 32 and 64-bit Windows (but note that 64-bit I never seem to be able to find a working netcat download when I need it.								

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

#### **Step 4** You should see the following

Here's <u>netcat 1.11</u> compiled for both 32 and 64-bit Windows (but note that 64-bit version hasn't been tested much - use at your own risk).

I'm providing it here because I never seem to be able to find a working netcat download when I need it.

Small update: <u>netcat 1.12</u> - adds -c command-line option to send CRLF line endings instead of just CR (eg. to talk to Exchange SMTP)

Warning: a bunch of antiviruses think that netcat (nc.exe) is harmful for some reason, and may block or delete the file when you try to download it. I could get around this by recompiling the binary every now and then (without doing any other changes at all, which should give you an idea about the level of protection these products offer), but I really can't be bothered.



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

	Opening netcat-win32-1.11.zip		
Here's netcat 1.11 compile nuch - use at your own ris	You have chosen to open:	sion hasn't been tested	Windows ports Gifsicle
'm providing it here becaus	which is: Compressed (zipped) Folder (107 KB) from: https://eternallybored.org	ad when I need it.	PCI Utilities GNU Wget
Small update: netcat 1.12 alk to Exchange SMTP)	What should Firefox do with this file?	stead of just CR (eg. to	Scripts AutoHotKey for pfSense
Varning: a bunch of antiviruses ry to download it. I could get ar	Open with Windows Explorer (default)     Save File	<ul> <li>pr delete the file when you ig any other changes at all,</li> </ul>	for (he)xchat for VMWare ESXi
vhich should give you an idea a	Do this gutomatically for files like this from now on.	bothered.	Other things GIMP-related stuff
			Provided by <u>Jernei Simon</u>
	OK	Cancel	
		SOURCE	
		- 🚱	Warnin
			I hreat Detec

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

ore i fill, select Context visionity->Enapoints->Compromised Enapoints, you she	iouiu see
---	-----------

de lde	ntity Services Eng	ine Home 🔫	context Visibility Operation	ns + Policy + Adr	ninistration + Work Ce	enters	License Wan	ning 🔺 🤇	× 0	1 0
ndpoints	Network Device	S					N.			
Aut	hentication B'	YOD Compliance	Compromised Endpoints	Endpoint Classification	Guest Vulne	erable Endpoints				¢
CC All or	MPROMISED	ENDPOINTS BY	INCIDENTS		COMPRO All endpoints		S BY INDICATORS			-
	Unknown In	isignificant Distractir IMF	ng Painful Damag ACT LEVEL	ing Catastrophic	Un	known None	Low Med	llum	High	
						Rows/Pa	ige 1 💌 💷 1 🗟	/1 > >	Go 1 Tol	tal Rows
C Ref	esh 🕂 Add	🗂 Trash 👻 🕑 Edit	ANC - Change Authorizate	Clear Threats & Vu	Inerabilities Export -	Import - MDM Actions	Revoke Certificate		₹ Filter -	<b>Q</b> ~
	MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivi	ty	Hostna
×	MAC Address			Threats	Source	Threat Severity		Connectivit	y .	

#### Step 2 Select the MAC address

alialia cisco	Identity Services Engine	Home Context	t Visibility • Operations	Policy ► Admir	istration	rs	License War	ning 🔺 🔍
End	points Network Devices							
	All endpoints Connected	Disconnected		1	All endpoints Conne	cted Disconnected	k	
	Unknown Insig	nificant Distracting IMPACT L	Painful Damaging EVEL	0 Catastrophic	Unknown	None LIKEL Rows/Page	Low Medium Y IMPACT LEVEL	н
\$	Refresh 🕂 Add 📋 T	'rash <del>▼</del> 🕑 Edit ANC	<ul> <li>Change Authorizaton</li> </ul>	<ul> <li>Clear Threats &amp; Vuln</li> </ul>	erabilities Export -	Import - MDM Actions -	Revoke Certificate	1
E	MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivity
×	MAC Address			Threats	Source	Threat Severity		Connectivity
E	00:0C:29:CF:07:17	LAB10\\jeppich	192.168.1.19	Threat Detected	AMP	Painful	Location#All Locations	Connected
*			m					

You should see the attribute details

dentity Services Eng	ine Home	← Context Visibility	Operations	Policy	Adminis
Endpoints Network Devices	3				
Endpoints > 00:0C:29:CF:07	7:17				
00:0C:29:CF:07:17	QG	8			
MAC Addres Username: Endpoint Pr Current IP A Location:	s: 00:0C:29:CF:07:1 LAB10\\jeppich ofile: Microsoft-Wo ddress: 192.168.1.1	17 rkstation 19			
Attributes Authe	ntication Thre	eats Vulnerabilitie	s		
General Attributes					
Description					
Static Assignment	false				
Endpoint Policy	Microsoft-Worksta	tion			
Static Group Assignment	false				
Identity Group Assignment	Workstation				
Custom Attributes					
				▼ Filter ▼	۰ ټ

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



### **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

dentity Services En	gine Home	Context Visibility		Policy	Administration
RADIUS TC-NAC Live L	ogs + TACACS	Reports + Troublesh	-Adaptive	Network Control	
Policy List Endpoint Assig	nment				
List > New Input fields marked with an	asterisk (*) are requi	ired.			
Name	ANC_Quarantine	1			
Action *	×QUARANTINE	] [			
			Ca	ncel 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

dialla cisco	lde	ntity Services	Engine	Home	▼Context Visibility	Operations	Policy	Administration	• Work Centers		License Wa	ming 🔺 🔍
End	points	s Network De	vices									
	Aut	hentication	BYOD	Complia	nce Compromise	d Endpoints	Endpoint Class	ification Guest	Vulnerable	Endpoints		
	CC All er	MPROMIS	ED EN	DPOINTS Disconnected	BY INCIDENTS			CO All en		D ENDPOINTS BY	(INDICATORS	
		Unknown	Insigni	ificant Distr	racting Painful	Damaging	g Catastroph	0 NC	Unknown	None	Low Mediur Y IMPACT LEVEL	n High
1 Se	electe	ed			HIT FOF SAFELA					Rows/Page		/1 ⊨ ⊨ Go
0	Ref	resh 🕂 Add	💼 Tra	ash 👻 🗹 Edi	it ANC - Char	nge Authorizaton	<ul> <li>Clear Threa</li> </ul>	ats & Vulnerabilities	Export - Im	port - MDM Actions -	Revoke Certificate	<b>▼</b> F
	1	MAC Address		Username	IPv4 Ad	dress	Threats	Source		Threat Severity	Logical NAD Location	Connectivity
×		MAC Address					Threats	Source		Threat Severity		Connectivity
	7	00:0C:29:CF:0	07:17	LAB10\\jeppic	h 192.168.	1.19	Threat Detecte	d AMP		Painful	Location#All Locations	Connected

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

dentity Services Engine	Home: Context \	isibility • Operations	Policy      ► Admini	stration	lers
Endpoints Network Devices		Assign a Policy			
Authentication BYOD	Compliance Co				
COMPROMISED END	POINTS BY INCI	Policy Assignment *	ANC_Qu *	Ass	sign Policy Close
		_			
Unknown Insignific	ant Distracting	Painful Damaging	Catastrophic	Unknow	n None LIKELY IN
1 Selected					Rows/Page
CRefresh 🕂 Add 🖀 Trast	- 🕑 Edit ANC -	Change Authorizaton -	Clear Threats & Vulne	rabilities Export <del>-</del>	Import - MDM Actions -
MAC Address U	sername	IPv4 Address	Threats	Source	Threat Severity L
× MAC Address					
00:0C:29:CF:07:17 L					

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