How-To Threat Centric NAC (Cognitive Threat Analysis (CTA) and Cisco Identity Services Engine (ISE) using STIX Technology

Authors: John Eppich, Karel Simek

Table of Contents

About this Document

This document is intended for Cisco Engineers and customers integrating CTA (Cognitive Threat Analytics) with Cisco Identity Services Engine (ISE 2.2+) using Cisco Web Security Appliance (WSA). Supported WSA Async images are: WSA8.5.1 GD, WSA 8.0.8, WSA 7.7.5 and 9.1.1-074 and supported WSA hardware: WSA-S100V, WSA S160, and WSA 5300V and Virtual WSA. ISE requires an APEX license for the ability to subscribe to CTA cloud instance.

The readers should have some familiarity with ISE and WSA and it is assumed that all the licenses have been installed and the reader has accounts on the Cisco CTA cloud instance.

CTA leverages WSA telemetry to identify security breaches or identity infected devices leveraging web traffic behavior analysis, machine learning and anomaly detection. These incidents are then reported to ISE using MITRE's Trusted Automated eXchange of Indicator Information (TAXII) as the transport protocol and reported incidents are in Structured Threat Information eXpression (STIX) language format and integrates with ISE via the Incident Response Feed (IRF) CTA adapter.

This provides visibility into the compromised endpoints in ISE. The ISE admin can take Adaptive Network Control (ANC) mitigation actions to automatically quarantine these compromised endpoints by configuring ISE CTA Course of Action authorization policies limiting network access or assigned Security Group Tags (SGT) or manually quarantining the endpoint by assigning the compromised endpoint to an ISE ANC quarantine policy.

This document covers the following:

- Introduction
  - Value proposition of the integration
  - Definition of the individual technologies
- Architecture and configuration procedure
  - Configuring CTA cloud instance to setup WSA
  - Configuring WSA to upload CTA log information to CTA Cloud instance
  - Configuring CTA to add ISE TAXII Account
  - Enabling ISE TC-NAC
  - Configuring ISE IRF CTA Adapter
  - Configuring ISE CTA Course of Action policies based on an organization's security policy.
- Use cases
  - Analyzing CTA events
  - Analyzing CTA events from ISE

Introduction

Value of the integration – Our data confirms that breaches are not a domain of a particular company type or size and to some extent cannot be avoided. In a situation where preventative measures fail, a breach happens. Dealing with breaches requires a specific process that is similar to incident response - with few exceptions. It needs to be executed much faster and has to be able to detect the breaches in the first place.

The integration between CTA and ISE covers a use-case where detection of a breached machine in the corporate environment is made by CTA and risk of data leak is determined as imminent. In such cases, being able to automatically disconnect and quarantine the endpoint is critical.

In later stages of the breach detection and mitigation process, more information is gathered in order to fully understand the scope and root cause of the breach by utilizing AMP for Endpoints, ThreatGrid and other technologies. Finally breached machines tend to get reimaged before they are used again.

Cisco® Cognitive Threat Analytics (CTA) is a cloud-based service that analyzes WSA telemetry data in order to detect breached devices on the network where prevention failed and attackers managed to establish their presence. Once inside, the malicious activity tends to become difficult to detect resulting in large windows of opportunity for further escalations and extractions. CTA automatically detects command and control channels and other evidence of an active infection and is able to track individual campaigns and attackers. CTA does not rely on existing security intelligence and is therefore effective against unknown variants of known threats as well as unique threats never seen before.

Cisco Web Security Appliance (WSA) is a web-based threat protection solution providing protection against malware, includes application and visibility controls which provides more visibility into web-based transactions for monitoring or blocking these transactions based on the organization’s web security policy. Identity profiles determine the authentication profiles and web access policies determine the organization’s web security policy. The WSA will send the telemetry data to the CTA account for behavior analysis.

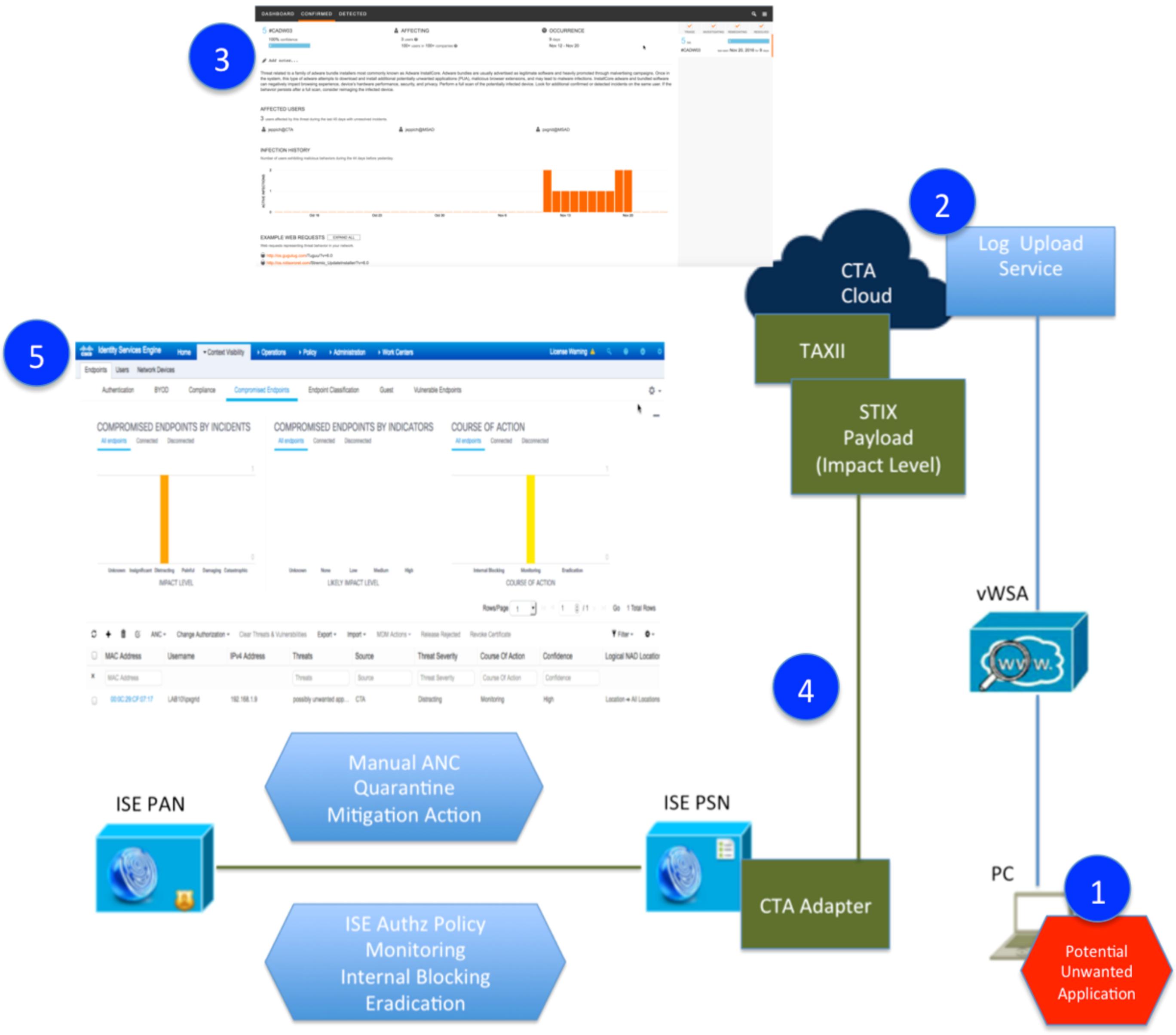
Cisco Identity Services Engine (ISE) is an identity software solution providing IEEE 802.1X authentication for wired, wireless, and virtual environments. In addition, ISE can perform additional functions such as Guest, Posture, and incorporate SGT (Security Group Tags), which is a component for the Cisco Trustsec Solution. When a user or device authenticates to the network, there is rich contextual information that is available from these authenticated sessions. With CTA integration, ISE can now detect if the host is infected or has been compromised and automated Adaptive Network Control (ANC) mitigation actions can be taken to limit network access until the endpoint has been remediated.

Trusted Automated Exchange of Indicator Information (TAXII) is a standard for exchanging information represented using the Structured Threat Information Expression (STIX) language, enabling organizations to share structured cyber threat information in a secure and automated manner. CTA supports TAXII through the CTA Cloud instance. The ISE CTA adapter is configured to poll the CTA Cloud instance for threat incident information. This threat incident information is defined in the STIX format.

Technical Details

Architecture

The following illustrates the solution architecture and process of analysis by web access log collection by WSA, analysis by CTA and quarantine action instructed by ISE towards other network and security devices.


3
2
CTA Cloud
Log Upload Service
TAXII
STIX Payload (Impact Level)
5
vWSA
4
Manual ANC Quarantine Mitigation Action
ISE PAN
ISE PSN
CTA Adapter
PC
1
Potential Unwanted Application
ISE Authz Policy Monitoring Internal Blocking Eradication

1. Endpoint requests a HTTP/HTTPs resource, or accesses a potential malware site, this activity is logged to the WSA.

2. After a certain interval, the WSA sends all new proxy logs to CTA cloud service using SCP for behavioral analysis and breach detection.

3. With enough evidence, CTA determines the endpoint as breached and creates all incidents describing the risk and other details.

4. ISE receives new CTA incidents: Unknown, Insignificant, Unknown, Distracting, Painful, Damaging, Catastrophic using Structured Threat Information expression (STIX) language format over MITRE's Trusted Automated Exchange of Indicator Information (TAXII) communication transport. These incidents are received by the ISE CTA Adapter (enabled on a PSN node) and contain pre-defined risk factor scores as determined by the CTA development engineers. These incidents are also tied to the ISE Authorization Course of Action condition rules such as eradication, monitoring and internal blocking for taking automated ANC mitigation actions on the compromised endpoint. Manual ANC mitigation and manual network actions can be taken by assigning the compromised endpoint to ANC policy (not legacy EPS).

5. Incident is passed on to the PAN node and is visible in ISE under Context Visibility view under compromised hosts.

Configuring CTA Analysis of WSA Telemetry Data

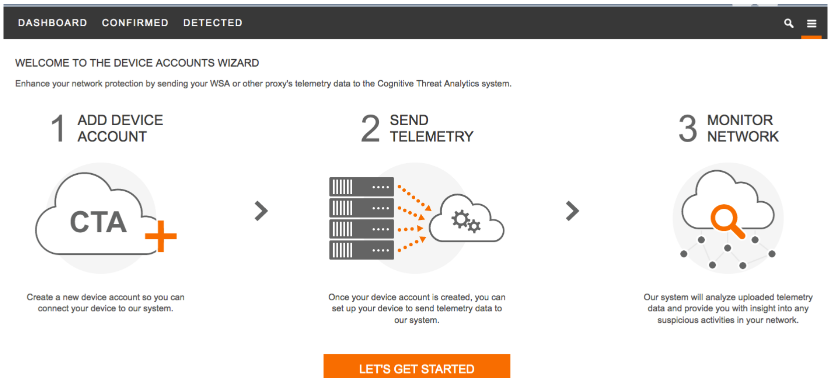
The CTA Portal is where you configure the WSA as a device for uploading the subscription logs or behavior analysis. This is also where you define an ISE TAXII account for the ISE CTA Adapter. You may log into the CTA portal via https://cognitive.cisco.com/login .

CTA can accept proxy logs from several sources, such as Bluecoat SG or Cisco Cloud Web Security. In this document we will focus on the Cisco WSA.

Adding WSA as a Device Account

In this section, CTA is configured to allow for receiving telemetry data from the WSA.

Step 1 Select **Threats->Device Accounts**
You should see the following:



WELCOME TO THE DEVICE ACCOUNTS WIZARD

Enhance your network protection by sending your WSA or other proxy's telemetry data to the Cognitive Threat Analytics system.

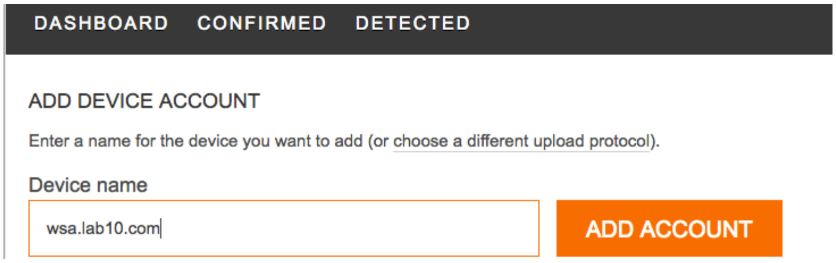
Create a new device account so you can connect your device to our system.

Once your device account is created, you can set up your device to send telemetry data to our system.

Our system will analyze uploaded telemetry data and provide you with insight into any suspicious activities in your network.

Step 2 Select **Lets Get Started**

Step 3 Select **Automatic->SCP->Add device account**

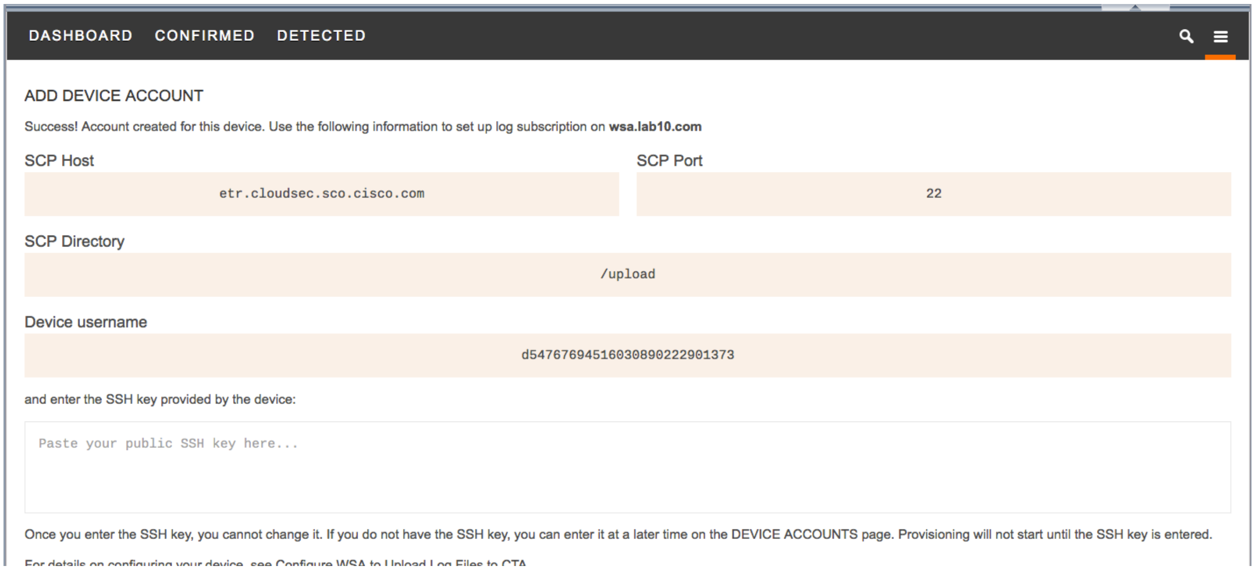


ADD DEVICE ACCOUNT

Enter a name for the device you want to add (or choose a different upload protocol).

Device name: wsa.lab10.com

Step 4 Select **Add Account**
You should see the following:



ADD DEVICE ACCOUNT

Success! Account created for this device. Use the following information to set up log subscription on **wsa.lab10.com**

SCP Host: `etr.cloudsec.sco.cisco.com`

SCP Port: `22`

SCP Directory: `/upload`

Device username: `d5476769451603089022901373`

and enter the SSH key provided by the device:

Paste your public SSH key here...

Once you enter the SSH key, you cannot change it. If you do not have the SSH key, you can enter it at a later time on the DEVICE ACCOUNTS page. Provisioning will not start until the SSH key is entered.

For details on configuring your device, see Configure WSA to Upload Log Files to CTA

Step 5 Leave this window open as you will need the account details when **Configuring WSA**. You will also need to paste the SSH key obtained from the WSA in later steps. Alternatively the same information can be viewed later by going to the sandwich menu in top right hand corner, selecting Device Accounts and expanding the account name. There you can either view the account info again or provide the SSH key.

Note**: If this screen times out, you can refresh and login. Select **Threats->Devices** and provide **SSH Key

Configuring the WSA to Send Telemetry Data

In this section, the WSA is configured for CTA integration. This includes creating the CTA log file for sending the telemetry events to the CTA Cloud instance and also for configuring the communication parameters between the WSA and the CTA Cloud instance.

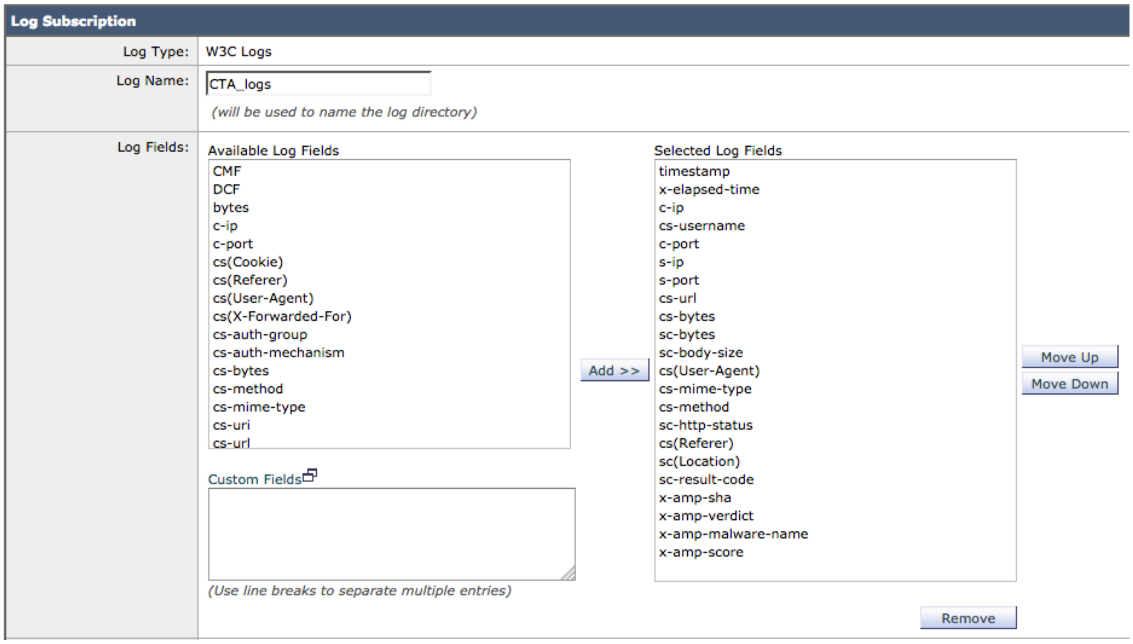
Step 1 Point your web browser to your WSA: http://wsa_*hostname*:8080/
Step 2 Log in as admin.
Step 3 Navigate to **System Administration > Log Subscriptions**.
Step 4 Click **Add Log Subscription**.
Step 5 In the **Log Type** pull-down, select **W3C Logs**.
Step 6 In the **Log Name** field, enter a descriptive name for the log directory. (i.e. **CTA logs**)
Step 7 Remove the pre-selected Log Fields by selecting all items in the **Selected Log Fields** box and clicking **Remove**
Step 8 In the **Custom Fields** box, enter the following items, using line breaks to separate them:

```
timestamp
x-elapsed-time
c-ip
cs-username
c-port
```

```
s-ip
s-port
cs-url
cs-bytes
sc-bytes
sc-body-size
cs(User-Agent)
cs-mime-type
cs-method
sc-http-status
cs(Referer)
sc(Location)
sc-result-code
x-amp-sha
x-amp-verdict
x-amp-malware-name
x-amp-score
```

Note: On WSA version 7.7.5, AMP is not supported; so do not add the four “x-amp” fields.

You should see the following:



Log Subscription

Log Type: W3C Logs

Log Name: CTA_logs

(will be used to name the log directory)

Log Fields:

Available Log Fields

```
CMF
DCF
bytes
c-ip
c-port
cs(Cookie)
cs(Referer)
cs(User-Agent)
cs(X-Forwarded-For)
cs-auth-group
cs-auth-mechanism
cs-bytes
cs-method
cs-mime-type
cs-uri
cs-url
```

Custom Fields

(Use line breaks to separate multiple entries)

Selected Log Fields

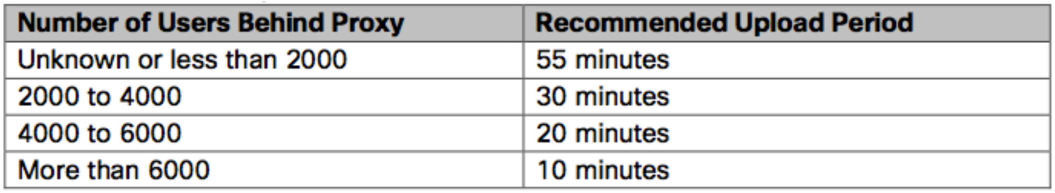
```
timestamp
x-elapsed-time
c-ip
cs-username
c-port
s-ip
s-port
cs-url
cs-bytes
sc-bytes
sc-body-size
cs(User-Agent)
cs-mime-type
cs-method
sc-http-status
cs(Referer)
sc(Location)
sc-result-code
x-amp-sha
x-amp-verdict
x-amp-malware-name
x-amp-score
```

Step 9 Once all items are entered, click **Add >>**.

Step 10 In the **Rollover by File Size** field, enter `500M`.

Step 11 In the Rollover by Time pull-down, select Custom Time Interval.

Step 12 In the **Rollover every** field, enter for example `55m`.



Number of Users Behind Proxy	Recommended Upload Period
Unknown or less than 2000	55 minutes
2000 to 4000	30 minutes
4000 to 6000	20 minutes
More than 6000	10 minutes

Step 13 In the **File Name** field, enter `w3c_log`.

Step 14 Enable compression by checking **Log Compression**.

Step 15 For Retrieval Method, select SCP on Remote Server.

Step 16 In the **SCP Host** field, enter the SCP host provided in Cisco CTA Cloud instance, e.g. `etr.cloudsec.sco.cisco.com`

Step 17 In the **SCP Port** field, enter `22`.

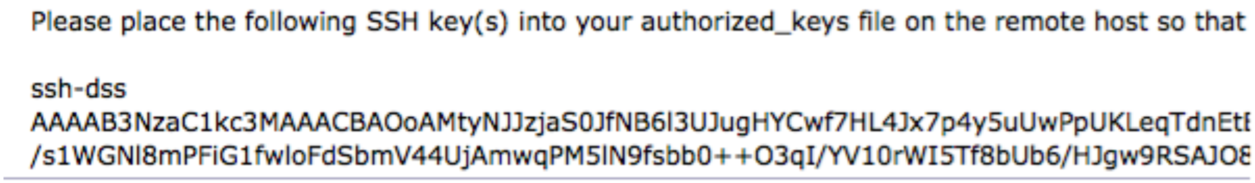
Step 18 In the **Directory** field, enter `/upload`.

Step 19 In the **Username** field, enter the username generated for your device in the CTA portal. The device username is case sensitive and different for each proxy device.

Step 20 Select the **Enable Host Key Checking** check box, and select the **Automatically Scan** radio button.

Step 21 Click **Submit**.

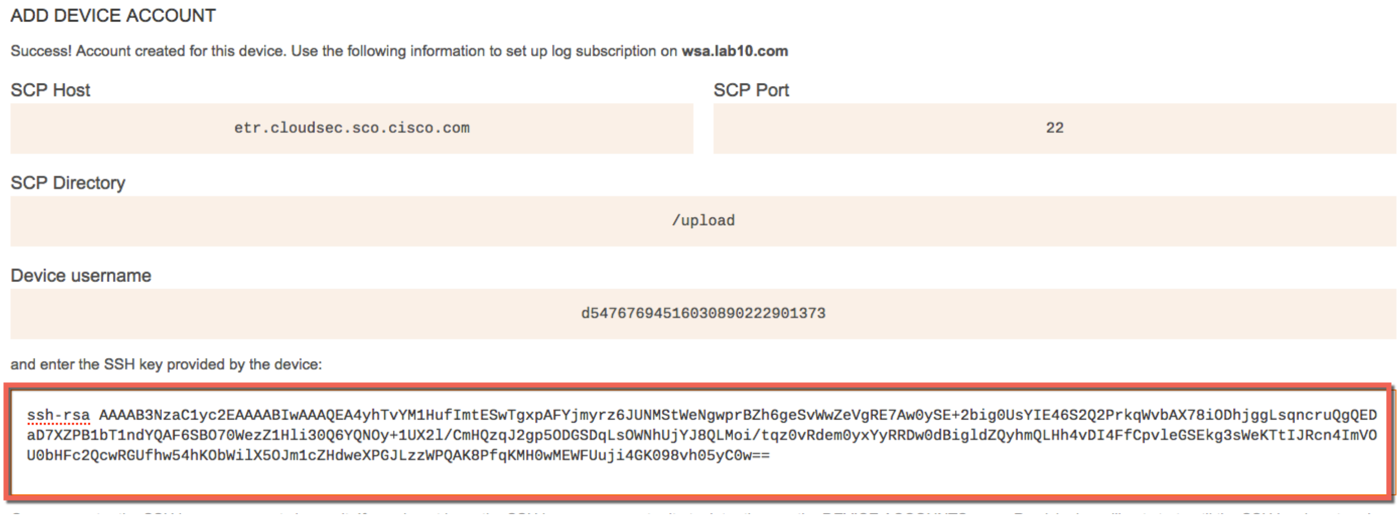
Step 22 The WSA Management Console displays a public SSH key. Copy and paste the whole key, including the "ssh-dss" at the beginning, into the device account in Cisco CTA Cloud Instance. Successful authentication between your proxy device and CTA system will allow log files from your proxy device to be uploaded to the CTA system for analysis.



Please place the following SSH key(s) into your authorized_keys file on the remote host so that

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAOoAMtyNJJzjaS0JfNB6l3UJugHYCwf7HL4Jx7p4y5uUwPpUKLeqTdnEtE
/s1WGNl8mPFiG1fwloFdSbmV44UjAmwqPM5lN9fsbb0++O3qI/YV10rWI5Tf8bUb6/HJgw9RSAJO8
```

Step 23 Copy/paste the **Device username** ssh key into the device account



ADD DEVICE ACCOUNT

Success! Account created for this device. Use the following information to set up log subscription on **wsa.lab10.com**

SCP Host	SCP Port
etr.cloudsec.sco.cisco.com	22

SCP Directory: `/upload`

Device username: `d547676945160308902229O1373`

and enter the SSH key provided by the device:

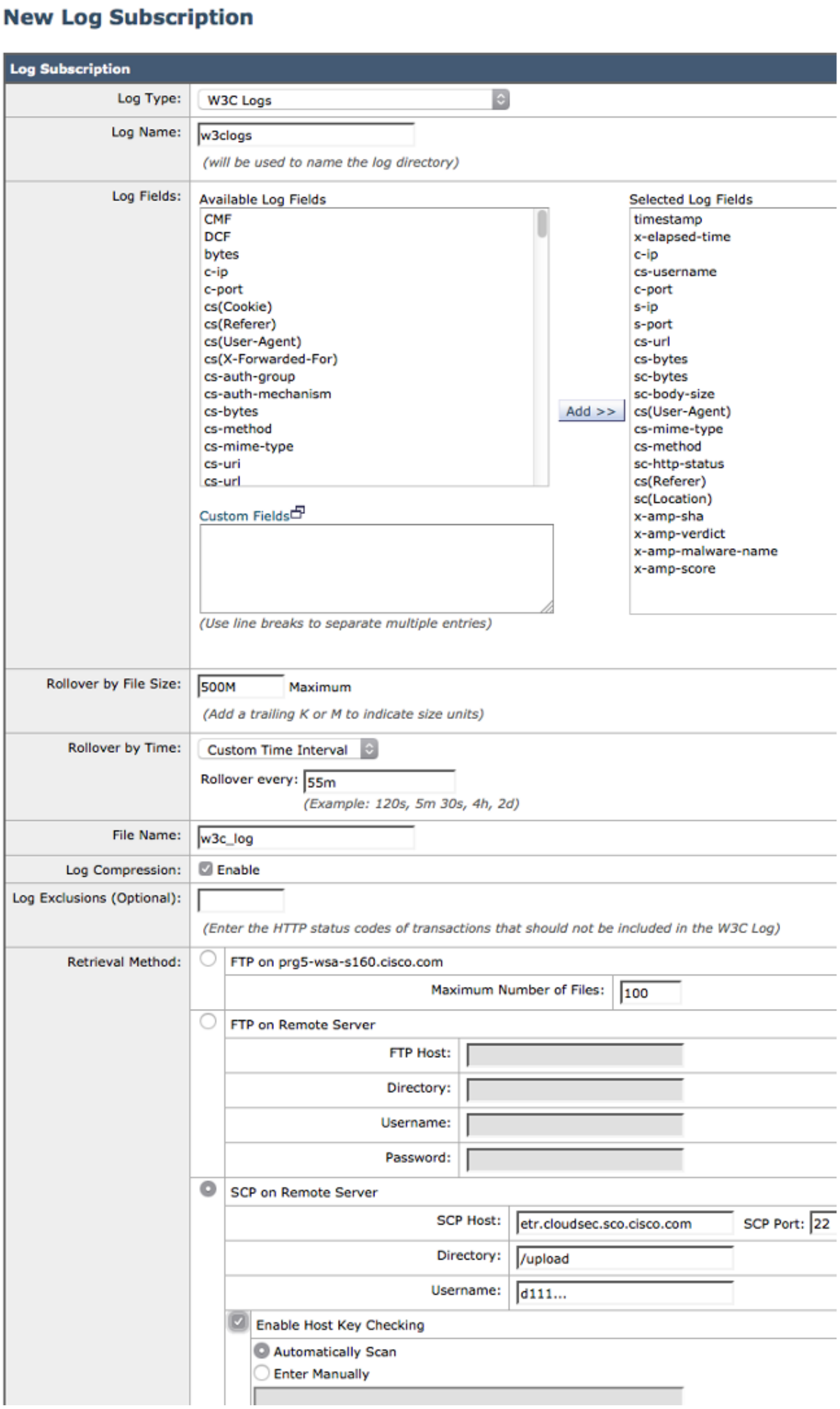
```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA4yhTvYM1HufImtESwTgxpAFYjmyrz6JUNMStWeNgwprBZh6geSvWwZeVgRE7Aw0ySE+2big0UsYIE46S2Q2PrkqWvbAX78iODhjggLsqncruQgQED
aD7XZPB1bT1ndYQAF6SBO70WezZ1Hli30Q6YQNOy+1UX2l/CmHQzqJ2gp5ODGSDqLsOWNhUjYJ8QLMoi/tqz0vRdem0yxYyRRDw0dBigldZQyhmQLHh4vDI4FfCpvleGSEkg3sWeKTtIJRcn4ImVO
U0bHFc2QcwRGUfhw54hKObWilX5OJm1cZHdweXPGJLzzWPQAK8PfqKMH0wMEWFUuji4GK098vh05yC0w==
```

Step 24 Select **Finish**

Step 25 Click **Commit Changes**

Note: In order to process these changes, the proxy process will restart after you commit changes. This will cause a brief interruption in service. Additionally, the authentication cache will be cleared, which might require some users to authenticate again. We recommended you configure the WSA during an off-hour maintenance window to avoid impacting users during production hours.

You should see the following:



New Log Subscription

Log Subscription

Log Type: W3C Logs

Log Name: w3clogs
(will be used to name the log directory)

Log Fields:

Available Log Fields: CMF, DCF, bytes, c-ip, c-port, cs(Cookie), cs(Referer), cs(User-Agent), cs(X-Forwarded-For), cs-auth-group, cs-auth-mechanism, cs-bytes, cs-method, cs-mime-type, cs-uri, cs-url

Add >>

Selected Log Fields: timestamp, x-elapsed-time, c-ip, cs-username, c-port, s-ip, s-port, cs-url, cs-bytes, sc-bytes, sc-body-size, cs(User-Agent), cs-mime-type, cs-method, sc-http-status, cs(Referer), sc(Location), x-amp-sha, x-amp-verdict, x-amp-malware-name, x-amp-score

Custom Fields
(Use line breaks to separate multiple entries)

Rollover by File Size: 500M Maximum
(Add a trailing K or M to indicate size units)

Rollover by Time: Custom Time Interval
Rollover every: 55m
(Example: 120s, 5m 30s, 4h, 2d)

File Name: w3c_log

Log Compression: ☑ Enable

Log Exclusions (Optional):
(Enter the HTTP status codes of transactions that should not be included in the W3C Log)

Retrieval Method:

○ FTP on prg5-wsa-s160.cisco.com
Maximum Number of Files: 100

○ FTP on Remote Server
FTP Host:
Directory:
Username:
Password:

● SCP on Remote Server
SCP Host: etr.cloudsec.sco.cisco.com SCP Port: 22
Directory: /upload
Username: d111...
☑ Enable Host Key Checking
● Automatically Scan
○ Enter Manually

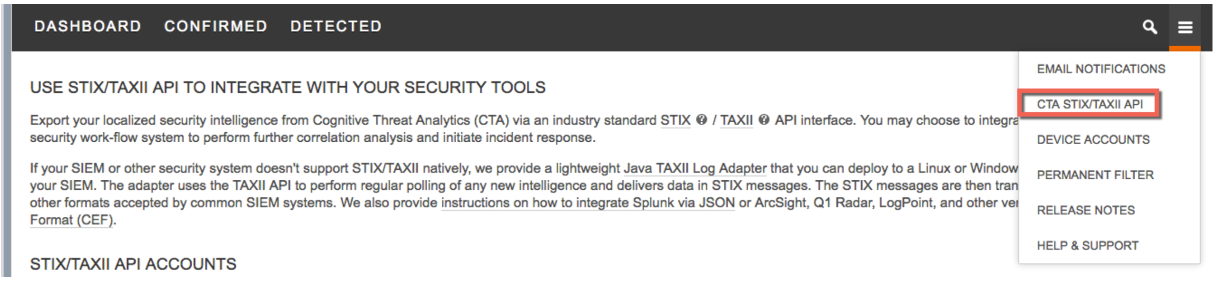
Configuring Incidents Export from CTA to ISE

Creating ISE STIX/TAXII Account

In this section, new STIX/TAXII Account is created in CTA cloud instance to be later used by ISE to poll the incident data.

Step 1 Add ISE Account in Scansafe

Select **Threats->≡->CTA STIX/TAXII API**



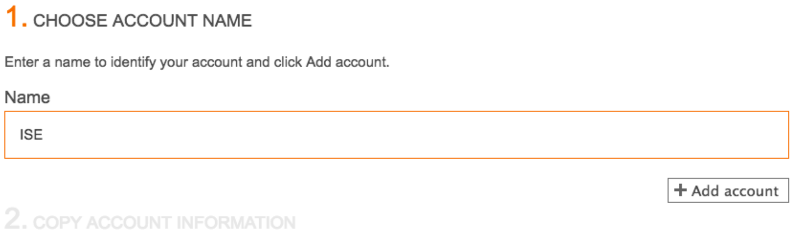
USE STIX/TAXII API TO INTEGRATE WITH YOUR SECURITY TOOLS

Export your localized security intelligence from Cognitive Threat Analytics (CTA) via an industry standard STIX / TAXII API interface. You may choose to integra security work-flow system to perform further correlation analysis and initiate incident response.

If your SIEM or other security system doesn't support STIX/TAXII natively, we provide a lightweight Java TAXII Log Adapter that you can deploy to a Linux or Window your SIEM. The adapter uses the TAXII API to perform regular polling of any new intelligence and delivers data in STIX messages. The STIX messages are then tran other formats accepted by common SIEM systems. We also provide instructions on how to integrate Splunk via JSON or ArcSight, Q1 Radar, LogPoint, and other ver Format (CEF).

STIX/TAXII API ACCOUNTS

Step 2 Select **Add Account** add ACCOUNT NAME



1. CHOOSE ACCOUNT NAME

Enter a name to identify your account and click Add account.

Name: ISE

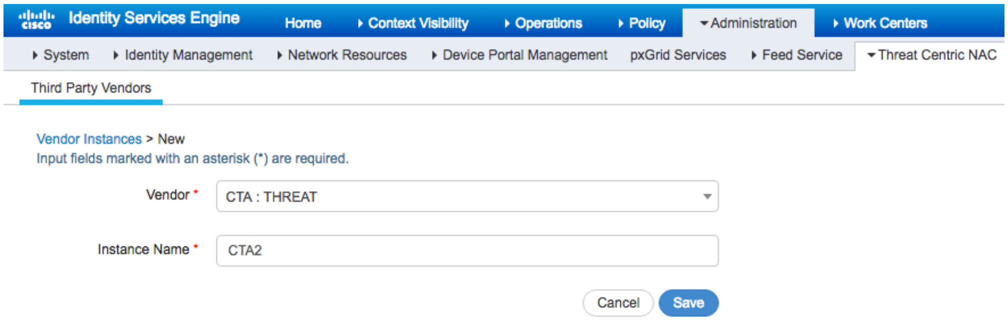
2. COPY ACCOUNT INFORMATION

Step 3 Select **Add Account**

Step 4 Copy Account Information and paste into ISE CTA Adapter Configuration in **Configuring ISE CTA Adapter**

Configuring ISE CTA Adapter

Step 1 Select **Administration->Threat Centric NAC->Third Party Vendors->CTA** from Vendor Drop down and enter instance name (i.e. CTA2)



Vendor Instances > New

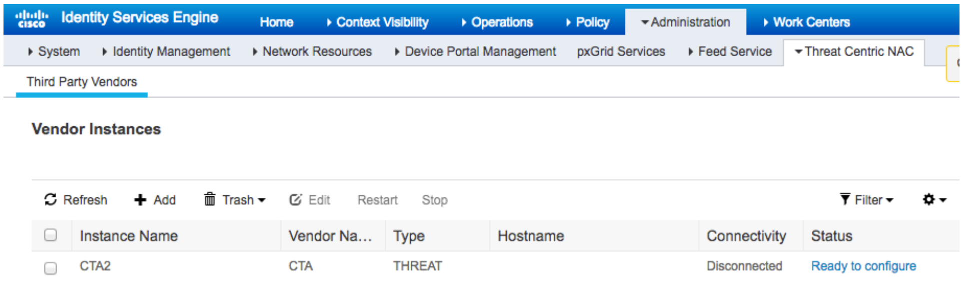
Input fields marked with an asterisk (*) are required.

Vendor * CTA : THREAT

Instance Name * CTA2

Step 2 Select **Save**

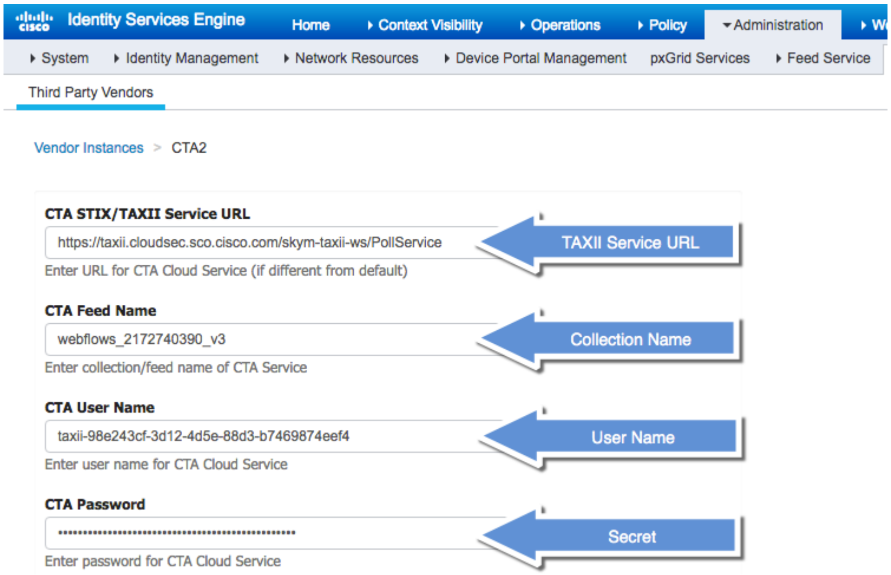
Step 3 Select **Ready to Configure**



Vendor Instances

	Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
□	CTA2	CTA	THREAT		Disconnected	Ready to configure

Step 4 Paste in CTA STIX information



Vendor Instances > CTA2

CTA STIX/TAXII Service URL

https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService

Enter URL for CTA Cloud Service (if different from default)

CTA Feed Name

webflows_2172740390_v3

Enter collection/feed name of CTA Service

CTA User Name

taxii-98e243cf-3d12-4d5e-88d3-b7469874eef4

Enter user name for CTA Cloud Service

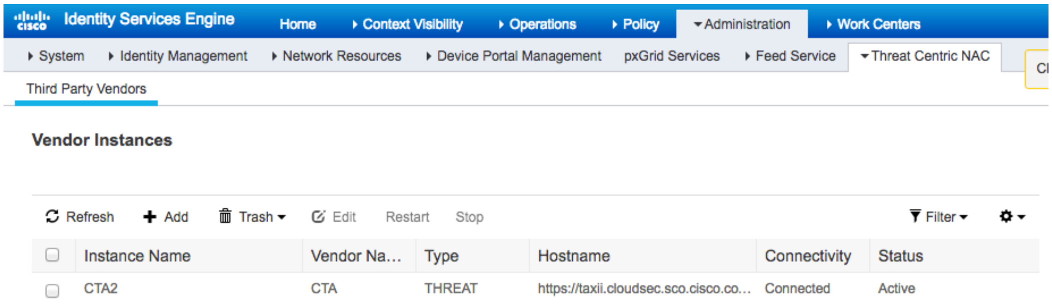
CTA Password

••

Enter password for CTA Cloud Service

Step 5 Select **Next->Finish**

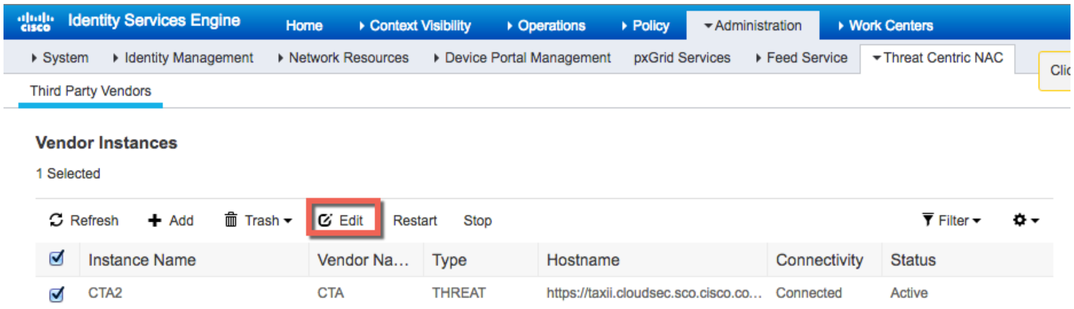
Step 6 You should see an **Active Status**



Vendor Instances

☐	Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
☐	CTA2	CTA	THREAT	https://taxii.cloudsec.sco.cisco.co...	Connected	Active

Step 7 Change the Impact Qualification Settings to 1-Significant
Select **Administration->Threat Centric NAC->Third Party Vendors-Edit the Instance (i.e. CTA2)**

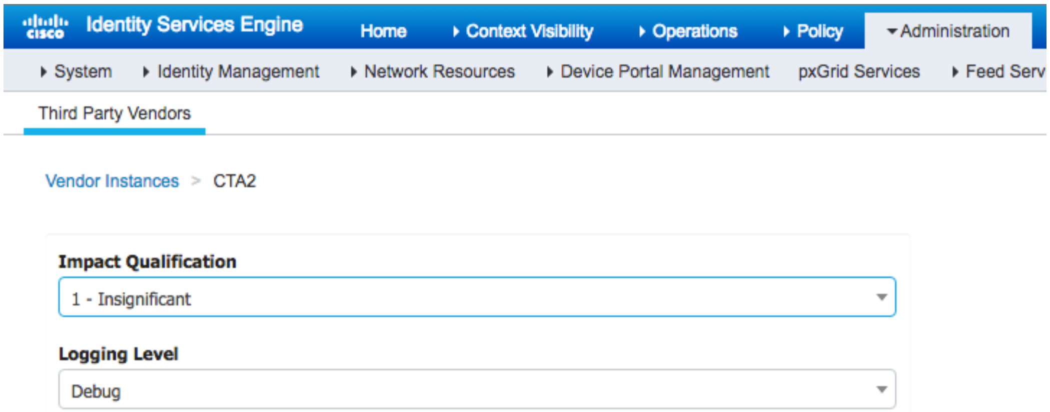


Vendor Instances

1 Selected

☑	Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
☑	CTA2	CTA	THREAT	https://taxii.cloudsec.sco.cisco.co...	Connected	Active

Step 8 Under **Advanced Settings**, select **Change,** and from the drop-down menu select **Insignificant** also change the **Logging Level** to Debug



Impact Qualification: 1 - Insignificant

Logging Level: Debug

Note: Changing the Impact Qualification to Insignificant you will receive more CTA telemetry information

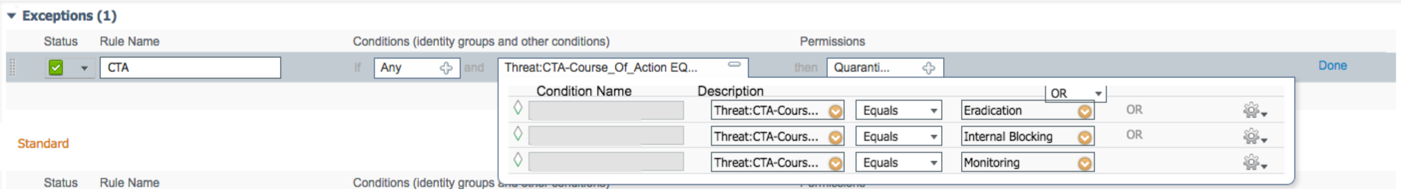
Step 9 Select **Next->Finish**

Configuring ISE Adaptive Network Control (ANC) Mitigation Policies

This section describes creating automated and manual ANC mitigations policies on endpoint once the endpoint has been compromised. There can be an automated ANC mitigation action based on the ISE Course of Action authorization policies. These mitigation actions can result in a Quarantine SGT and given limited network access.

Configuring ISE CTA Authorization Policy

Step 1 Select **Policy->Authorization->Exceptions->Create new exception**, create the following rule:



▾ Exceptions (1)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
☑	CTA	if Any and Threat:CTA-Course_Of_Action EQ...	then Quaranti...

Done

Condition Name	Description			OR
	Threat:CTA-Cours...	Equals	Eradication	OR
	Threat:CTA-Cours...	Equals	Internal Blocking	OR
	Threat:CTA-Cours...	Equals	Monitoring	

Standard

Status Rule Name Conditions (identity groups and other conditions) Permissions

Step 2 For the rule name, enter: **CTA**

Step 3 Select the **Condition(s) "+" ->Create new Condition->Description->Threat:CTACourseofAction->Equals->Eradication->** Click on gear to Add attribute value

Step 4 Select **OR** instead of AND

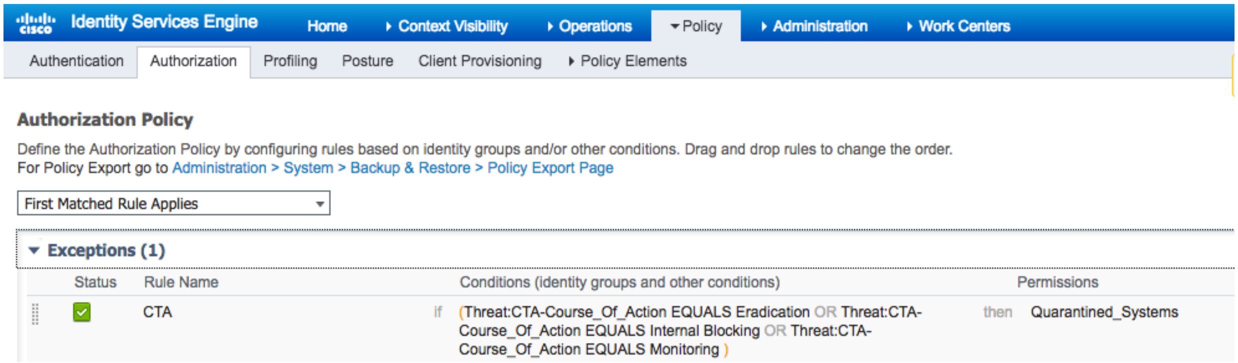
Step 5 **Create new Condition->Description->Threat:CTACourseofAction->Equals->Internal Blocking->** Click on gear to Add attribute value

Step 6 **Create new Condition->Description->Threat:CTACourseofAction->Equals->Monitoring->** Click on gear to **Add attribute value**

Step 7 Under Permissions, select **Authz Pr… + ->Security Group->Quarantined Systems**

Step 8 Select **Done->Save**

You should see the following:



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

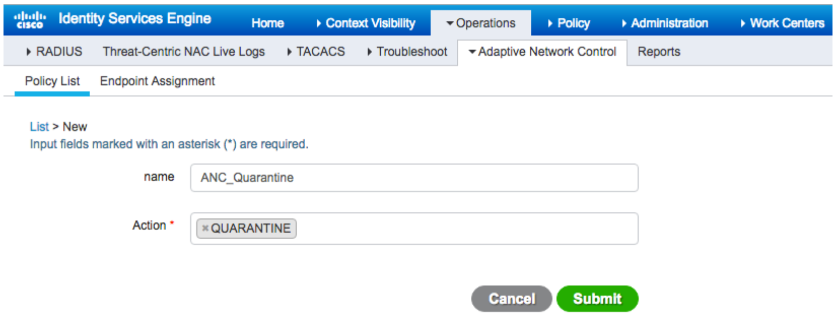
▾ Exceptions (1)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
☑	CTA	if (Threat:CTA-Course_Of_Action EQUALS Eradication OR Threat:CTA-Course_Of_Action EQUALS Internal Blocking OR Threat:CTA-Course_Of_Action EQUALS Monitoring)	then Quarantined_Systems

Configuring ISE Adaptive Network Control (ANC) Policy

Step 1 Select **Operations->Adaptive Network Control->Policy List->Add, enter name: ANC_Quarantine**

Step 2 Select **Quarantine** from the Drop-Down menu under **Action**



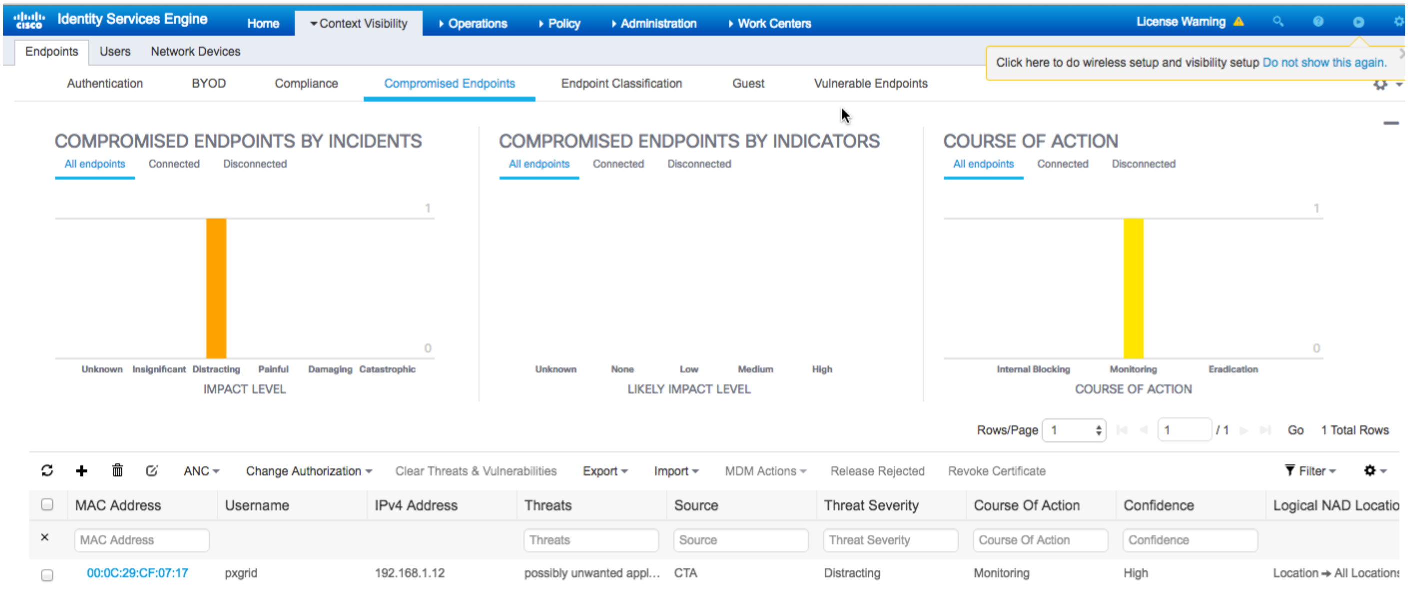
Input fields marked with an asterisk (*) are required.

name: ANC_Quarantine

Action *: QUARANTINE

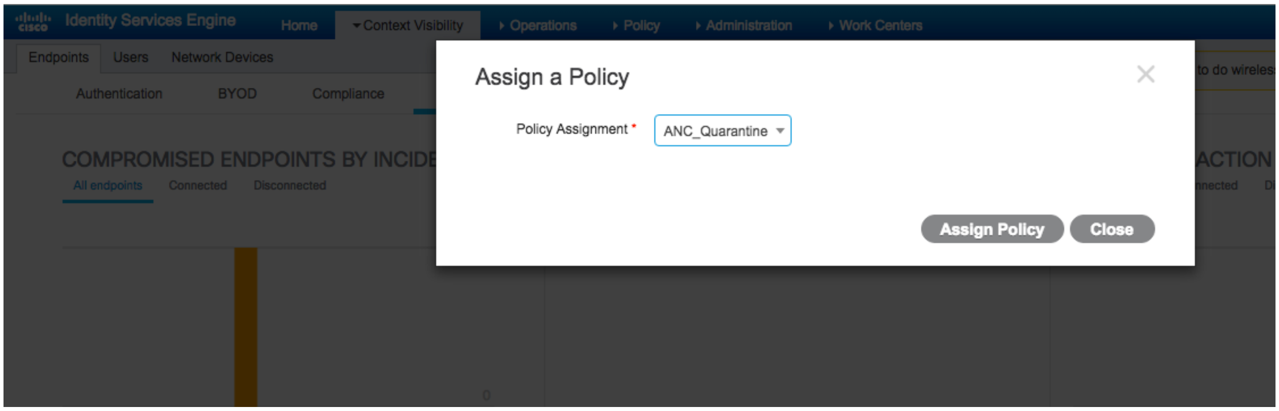
Step 3 Select **Submit**

Step 4 Select **Context Visibility->Endpoints->Compromised Endpoints**



MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Course Of Action	Confidence	Logical NAD Locatio
00:0C:29:CF:07:17	pxgrid	192.168.1.12	possibly unwanted appl...	CTA	Distracting	Monitoring	High	Location → All Locations

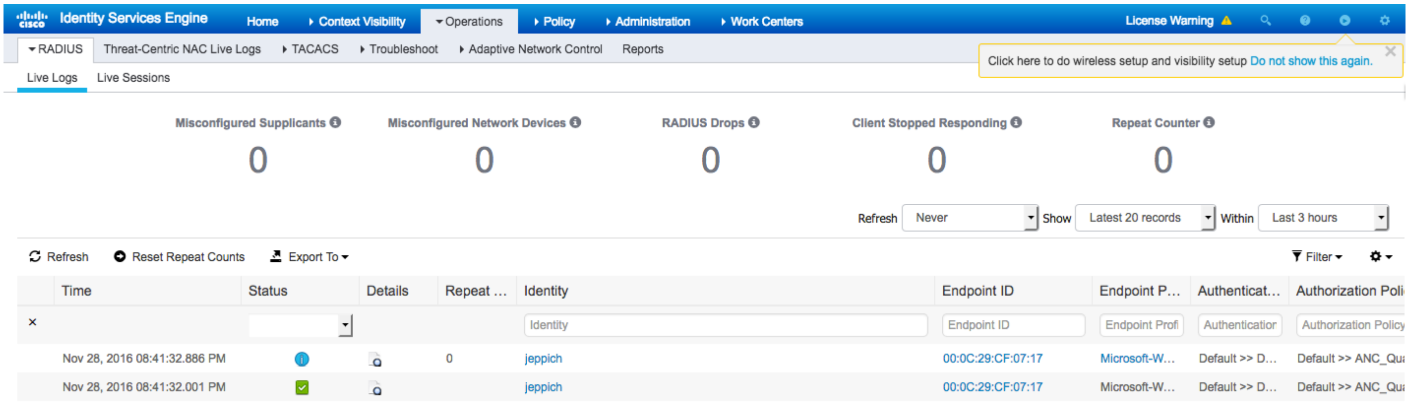
Step 5 Select the desired **MAC address->ANC->Assign a Policy->Policy Assignment->ANC_Quarantine**



Policy Assignment *: ANC_Quarantine

Step 6 Select **Assign Policy**

Step 7 You should see the following:



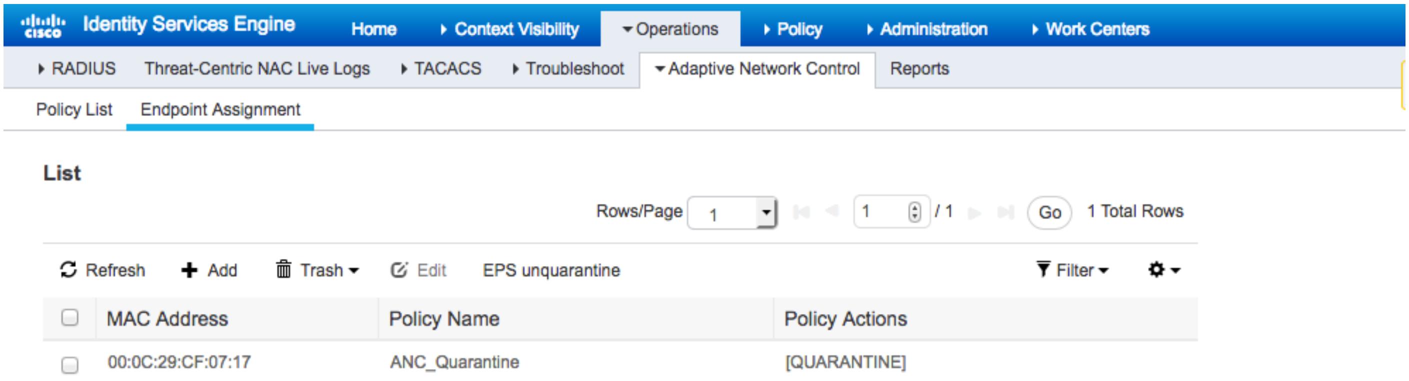
Click here to do wireless setup and visibility setup Do not show this again.

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

Refresh: Never Show: Latest 20 records Within: Last 3 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Poli
Nov 28, 2016 08:41:32.886 PM	●		0	jeppich	00:0C:29:CF:07:17	Microsoft-W...	Default >> D...	Default >> ANC_Qua
Nov 28, 2016 08:41:32.001 PM	✓			jeppich	00:0C:29:CF:07:17	Microsoft-W...	Default >> D...	Default >> ANC_Qua

Step 8 To Unquarantine, Select **Operations->Adaptive Network Control->Endpoint Assignment**



List

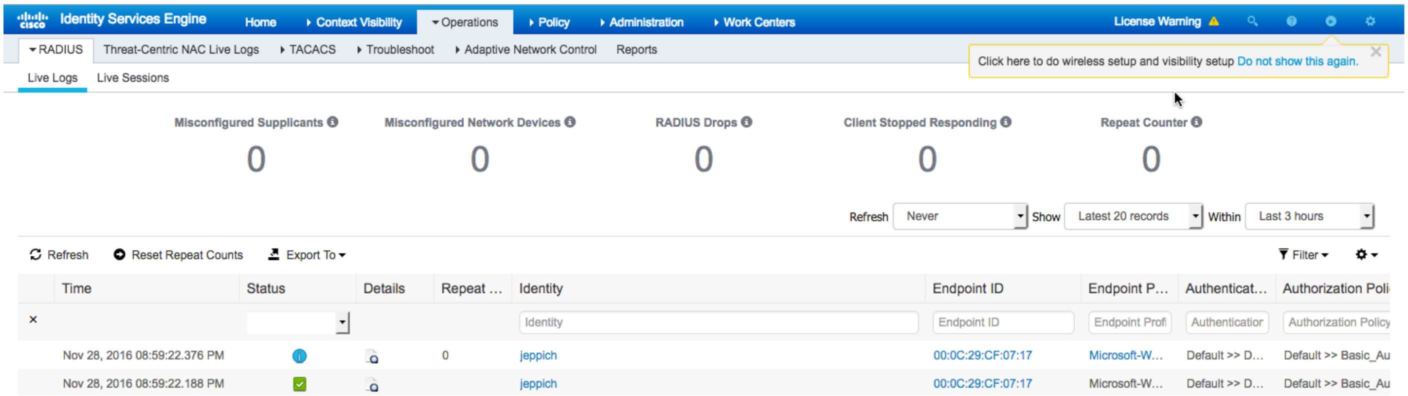
Rows/Page 1 1 / 1 Go 1 Total Rows

☐	MAC Address	Policy Name	Policy Actions
☐	00:0C:29:CF:07:17	ANC_Quarantine	[QUARANTINE]

Step 9 Select the **MAC Address->Trash**

Step 10 Select **Operations->RADIUS-Live Logs**

You should see the endpoint has been unquarantined



Click here to do wireless setup and visibility setup Do not show this again.

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

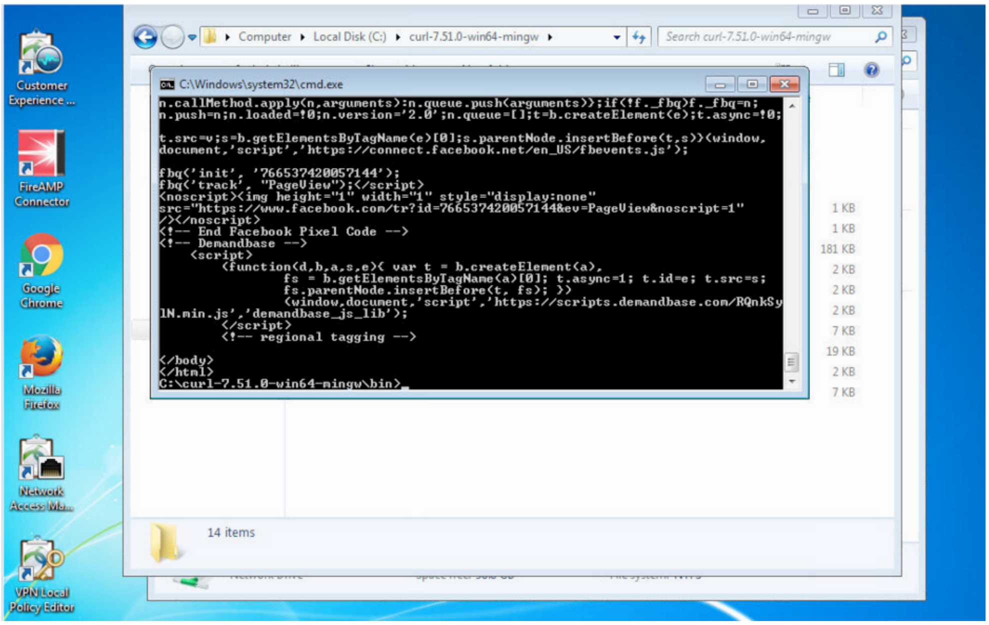
Refresh: Never Show: Latest 20 records Within: Last 3 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Poli
Nov 28, 2016 08:59:22.376 PM	●		0	jeppich	00:0C:29:CF:07:17	Microsoft-W...	Default >> D...	Default >> Basic_Au
Nov 28, 2016 08:59:22.188 PM	✓			jeppich	00:0C:29:CF:07:17	Microsoft-W...	Default >> D...	Default >> Basic_Au

Testing

Two Windows 7 PC’s were used for testing.   A test.bat file was run on both PC’s. This file contains known malware sites and legitimates sites, using curl script to send all traffic through the WSA. The WSA will upload the logs to the CTA cloud instance for analysis.   ISE will receive CTA incidents and can be will be viewed under Compromised hosts under the Context and Visibility View in ISE.

The end user logs in and test.bat was run in the curl-7.51.0-win64-mingw\bin folder



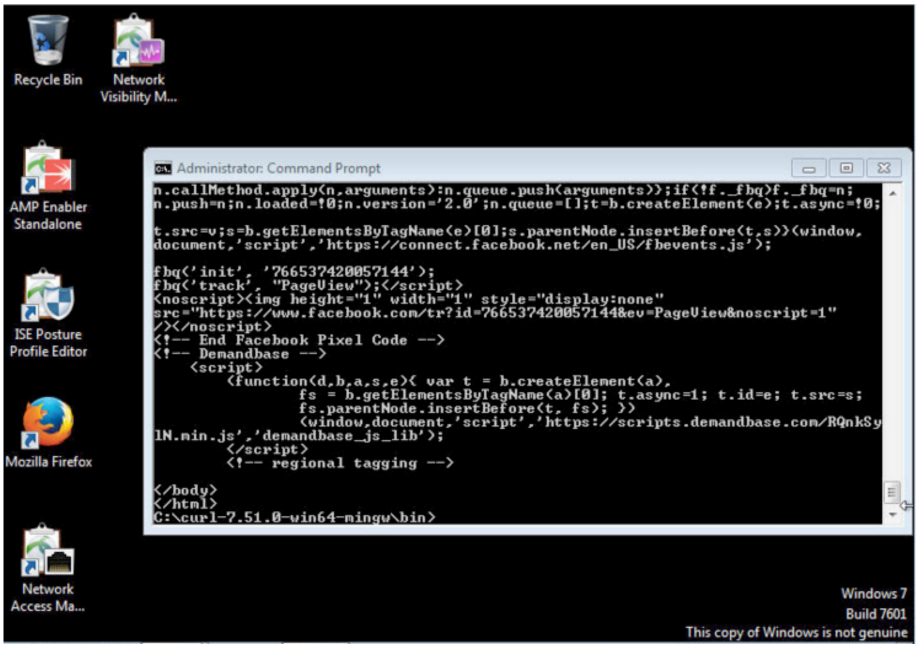
```
n.callMethod.apply(n,arguments):n.queue.push(arguments)};if(!f._fbq)f._fbq=n;
n.push=n;n.loaded=!0;n.version='2.0';n.queue=[];t=b.createElement(e);t.async=!0;

t.src=v;s=b.getElementsByTagName(e)[0];s.parentNode.insertBefore(t,s)}(window,
document,'script','https://connect.facebook.net/en_US/fbevents.js');

fbq('init', '766537420057144');
fbq('track', "PageView");</script>
<noscript><img height="1" width="1" style="display:none"
src="https://www.facebook.com/tr?id=766537420057144&ev=PageView&noscript=1"
/></noscript>
<!-- End Facebook Pixel Code -->
<!-- Demandbase -->
    <script>
        (function(d,b,a,s,e){ var t = b.createElement(a),
                fs = b.getElementsByTagName(a)[0]; t.async=1; t.id=e; t.src=s;
                fs.parentNode.insertBefore(t, fs); })
                (window,document,'script','https://scripts.demandbase.com/RQnkSy
lN.min.js','demandbase_js_lib');
        </script>
        <!-- regional tagging -->

</body>
</html>
C:\curl-7.51.0-win64-mingw\bin>_
```

Simultaneously, another end-user logs in on the second PC.



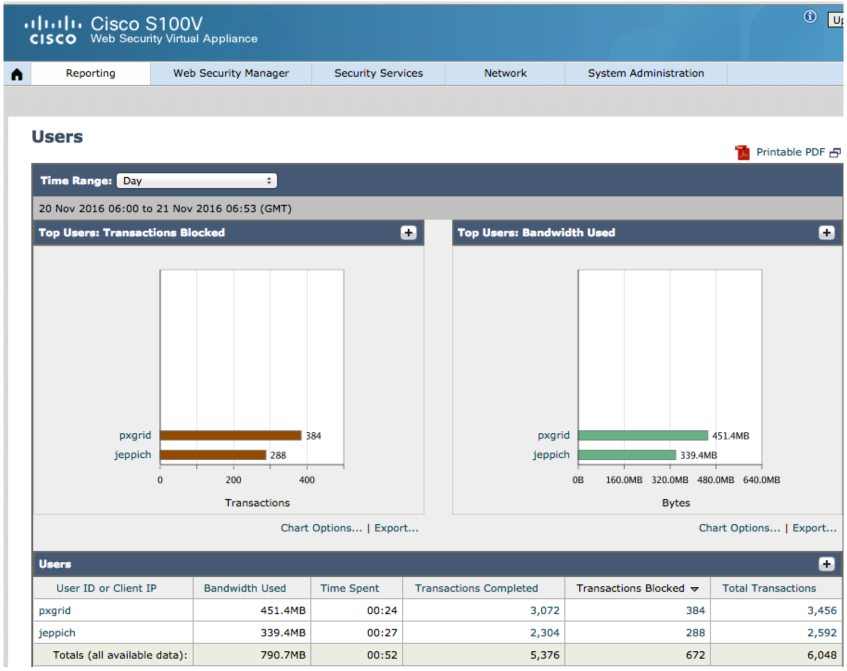
```
n.callMethod.apply(n,arguments):n.queue.push(arguments)};if(!f._fbq)f._fbq=n;
n.push=n;n.loaded=!0;n.version='2.0';n.queue=[];t=b.createElement(e);t.async=!0;

t.src=v;s=b.getElementsByTagName(e)[0];s.parentNode.insertBefore(t,s)}(window,
document,'script','https://connect.facebook.net/en_US/fbevents.js');

fbq('init', '766537420057144');
fbq('track', "PageView");</script>
<noscript><img height="1" width="1" style="display:none"
src="https://www.facebook.com/tr?id=766537420057144&ev=PageView&noscript=1"
/></noscript>
<!-- End Facebook Pixel Code -->
<!-- Demandbase -->
    <script>
        (function(d,b,a,s,e){ var t = b.createElement(a),
                fs = b.getElementsByTagName(a)[0]; t.async=1; t.id=e; t.src=s;
                fs.parentNode.insertBefore(t, fs); })
                (window,document,'script','https://scripts.demandbase.com/RQnkSy
lN.min.js','demandbase_js_lib');
        </script>
        <!-- regional tagging -->

</body>
</html>
C:\curl-7.51.0-win64-mingw\bin>
```

From the WSA, Select **Reporting->Users** to ensure that user traffic is flowing through the WSA



Users

Time Range: Day

20 Nov 2016 06:00 to 21 Nov 2016 06:53 (GMT)

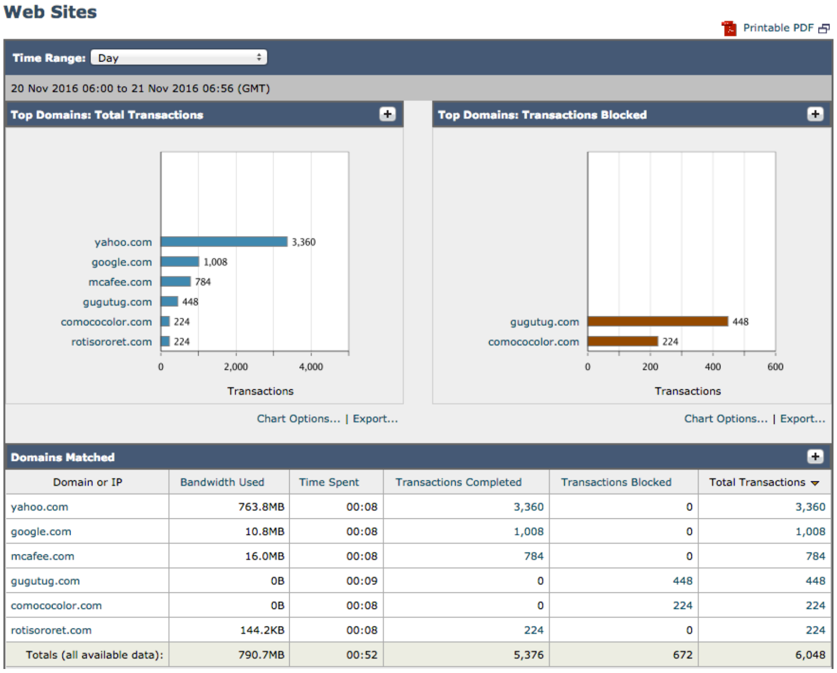
Top Users: Transactions Blocked

Top Users: Bandwidth Used

Users

User ID or Client IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked ▼	Total Transactions
pxgrid	451.4MB	00:24	3,072	384	3,456
jeppich	339.4MB	00:27	2,304	288	2,592
Totals (all available data):	790.7MB	00:52	5,376	672	6,048

Select **Reporting->Web Sites** to see a list of web sites visited by end-users, notice comocolor that is one of the malware sites.



Web Sites

Time Range: Day

20 Nov 2016 06:00 to 21 Nov 2016 06:56 (GMT)

Top Domains: Total Transactions

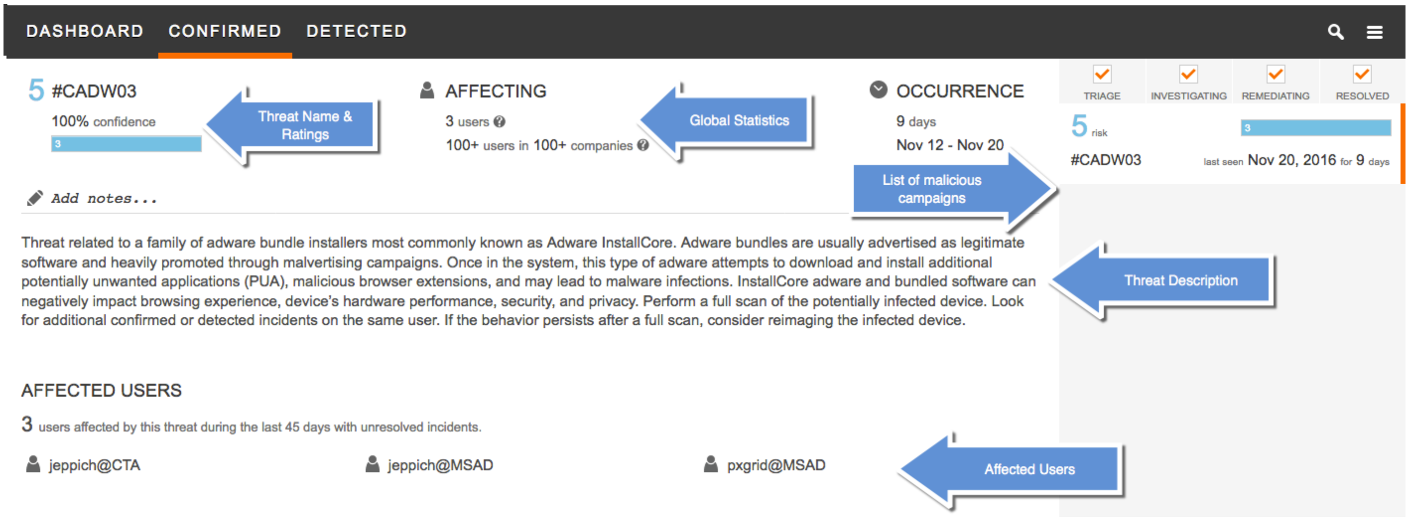
Top Domains: Transactions Blocked

Domains Matched

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions ▼
yahoo.com	763.8MB	00:08	3,360	0	3,360
google.com	10.8MB	00:08	1,008	0	1,008
mcafee.com	16.0MB	00:08	784	0	784
gugutug.com	0B	00:09	0	448	448
comococolor.com	0B	00:08	0	224	224
rotisororet.com	144.2KB	00:08	224	0	224
Totals (all available data):	790.7MB	00:52	5,376	672	6,048

CTA Analysis

Below is a sample incident report with detailed descriptions of the CTA incident.



5 #CADW03

100% confidence

3

Threat Name & Ratings

AFFECTING

3 users

100+ users in 100+ companies

Global Statistics

OCCURRENCE

9 days

Nov 12 - Nov 20

List of malicious campaigns

5 risk

3

#CADW03

last seen Nov 20, 2016 for 9 days

Add notes...

Threat related to a family of adware bundle installers most commonly known as Adware InstallCore. Adware bundles are usually advertised as legitimate software and heavily promoted through malvertising campaigns. Once in the system, this type of adware attempts to download and install additional potentially unwanted applications (PUA), malicious browser extensions, and may lead to malware infections. InstallCore adware and bundled software can negatively impact browsing experience, device's hardware performance, security, and privacy. Perform a full scan of the potentially infected device. Look for additional confirmed or detected incidents on the same user. If the behavior persists after a full scan, consider reimaging the infected device.

Threat Description

AFFECTED USERS

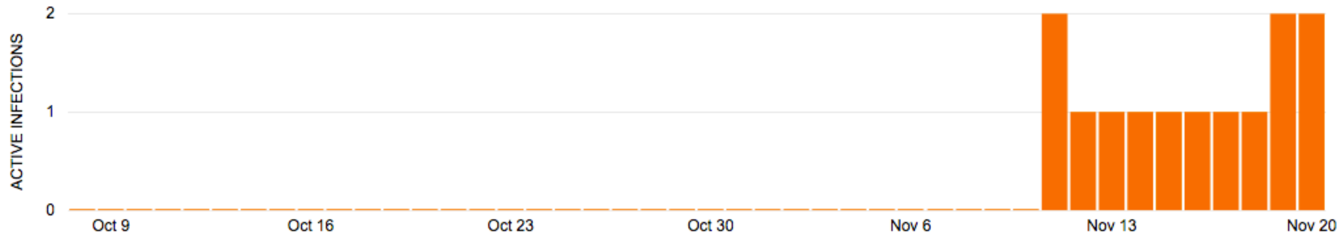
3 users affected by this threat during the last 45 days with unresolved incidents.

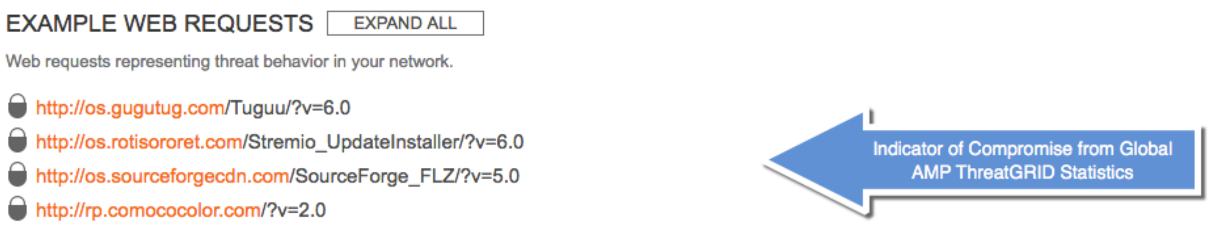
jeppich@CTA jeppich@MSAD pxgrid@MSAD

Affected Users

INFECTION HISTORY

Number of users exhibiting malicious behaviors during the 44 days before yesterday.





EXAMPLE WEB REQUESTS

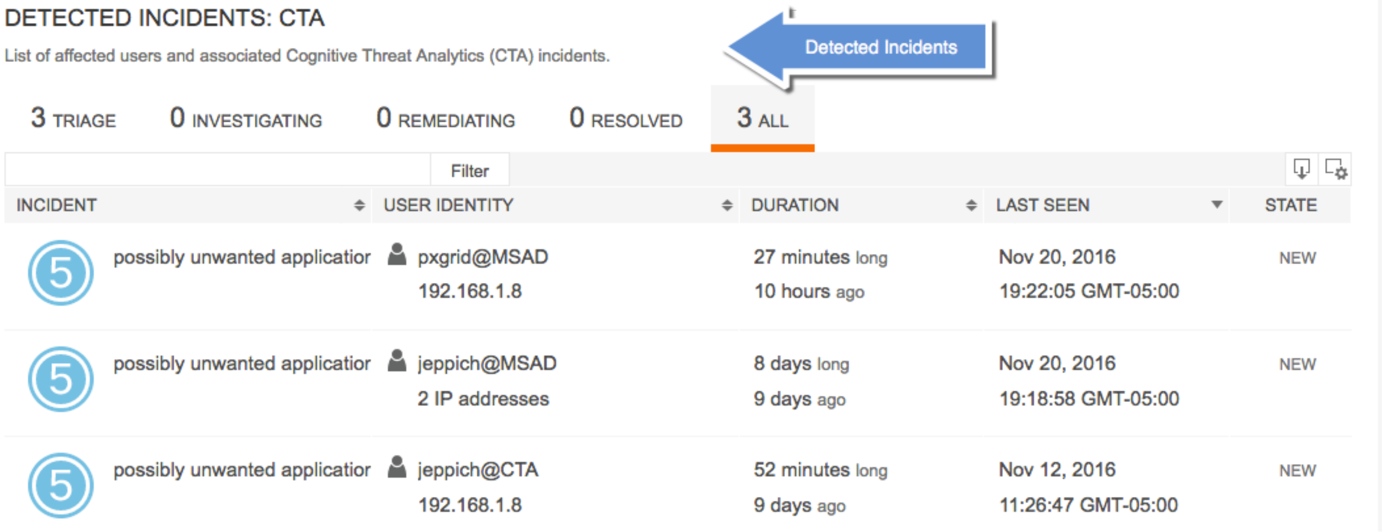
Web requests representing threat behavior in your network.

- http://os.gugutug.com/Tuguu/?v=6.0
- http://os.rotisororet.com/Stremio_UpdateInstaller/?v=6.0
- http://os.sourceforgecdn.com/SourceForge_FLZ/?v=5.0
- http://rp.comococolor.com/?v=2.0

Indicator of Compromise from Global AMP ThreatGRID Statistics

GLOBAL INTELLIGENCE: AMP THREAT GRID

The following statistics are based on 2 samples of threat artifacts from AMP Threat Grid that show network behaviors related to this CONFIRMED CTA threat category.



DETECTED INCIDENTS: CTA

List of affected users and associated Cognitive Threat Analytics (CTA) incidents.

Detected Incidents

3 TRIAGE | 0 INVESTIGATING | 0 REMEDIATING | 0 RESOLVED | 3 ALL

	INCIDENT	USER IDENTITY	DURATION	LAST SEEN	STATE
5	possibly unwanted applicatior	pxgrid@MSAD 192.168.1.8	27 minutes long 10 hours ago	Nov 20, 2016 19:22:05 GMT-05:00	NEW
5	possibly unwanted applicatior	jeppich@MSAD 2 IP addresses	8 days long 9 days ago	Nov 20, 2016 19:18:58 GMT-05:00	NEW
5	possibly unwanted applicatior	jeppich@CTA 192.168.1.8	52 minutes long 9 days ago	Nov 12, 2016 11:26:47 GMT-05:00	NEW

List of Malicious Campaigns –

Defines the malicious campaigns and risk, threat name, number of infected users and time of last malicious activity

Threat Description –

Describes the infection

Affected Users –

If one infection targeted three hosts, the information is aggregated into one incident. This is performed by looking at similarities between hosts or shared malware infrastructure. Such information helps to diagnose the spread of malware over time and reduces costs by focusing on the infection as a whole. Knowing the size of the infection is essential for prioritization.

In the above example, the affected user graph displays the number of infected user on a daily basis. As an example, on Nov 20, 2016, there are 2 affected users.

Global Statistics–

The global statistics of the threat represent behavior similarity across the shared information and across the whole customer base. Such information is more anonymized and presented in aggregate form. The goal of such information is to be able to differentiate between targeted and emerging threats (low numbers) and infections that operate on a global scale (high numbers).

Threat Name-

These names are internal to CTA and allow tracking of larger campaigns where the malicious actor might change, underlying malware or technique. Due to the behavioral similarity evolving threats are tracked. A particular common name of the threat associated with the current infected user is found in the description. The common name is especially useful when looking into other sources of intelligence.

Risk-

This score represents the overall potential of the malware and how high it should be on the list for remediation. High numbers, 7 to 9 are generally reserved to malware with highly destructive missions while lower numbers could indicate various botnets performing click-fraud operations and unwanted applications such as adware or TOR

Confidence-

This number represents how certain the system is that this incident belongs to the assigned category. In some cases we were able to correlate the behavior with existing campaign and achieve 100% confidence. In other cases, the number is lower- usually above 80%. This number does not indicate false positive rates, as these detections are 100% confirmed breaches.

In-line Blocking-

This percentage represents the statistics gathered from CWS that represent how much of the detected traffic was blocked inline by AMP inline blocking, outbreak intelligence, antivirus, and other inline technologies running on CWS (available only when CWS is used as a proxy). Low numbers indicate that the attackers are extremely well prepared as no part of their infrastructure or traffic going over that infrastructure to the infected endpoint is detectable. On the other hand, even if those numbers indicate that 100% of the traffic detected by CTA is blocked inline, we still have an active threat in out network that needs to be remediated. Blocking in this case does not solve the problem.

Indicator of Compromise from Global AMP ThreatGRID Statistics

This section applies to all confirmed incidents. When CTA detects a command and control channel, a query to AMP ThreatGRID API is made to get context of other files that utilized the same command and control infrastructure. While the latest samples might be impossible to sandbox, if the attackers have reused part of the infrastructure and there were other malicious files uploaded to AMP ThreatGRID., we can pivot from that and reveal the nature of the malicious campaign. Also by having visibility into many sandboxed files, we can derive statistics that give us probability of various artifacts to be on the infected endpoint. This gives us endpoint-level details without having to deploy an agent.

The report gives precise confidence, such as which files are to be likely found on the target system. Due to various missions that one infection can lead to, this gives good insight into what the malicious groups as a whole does.

ISE Context Visibility

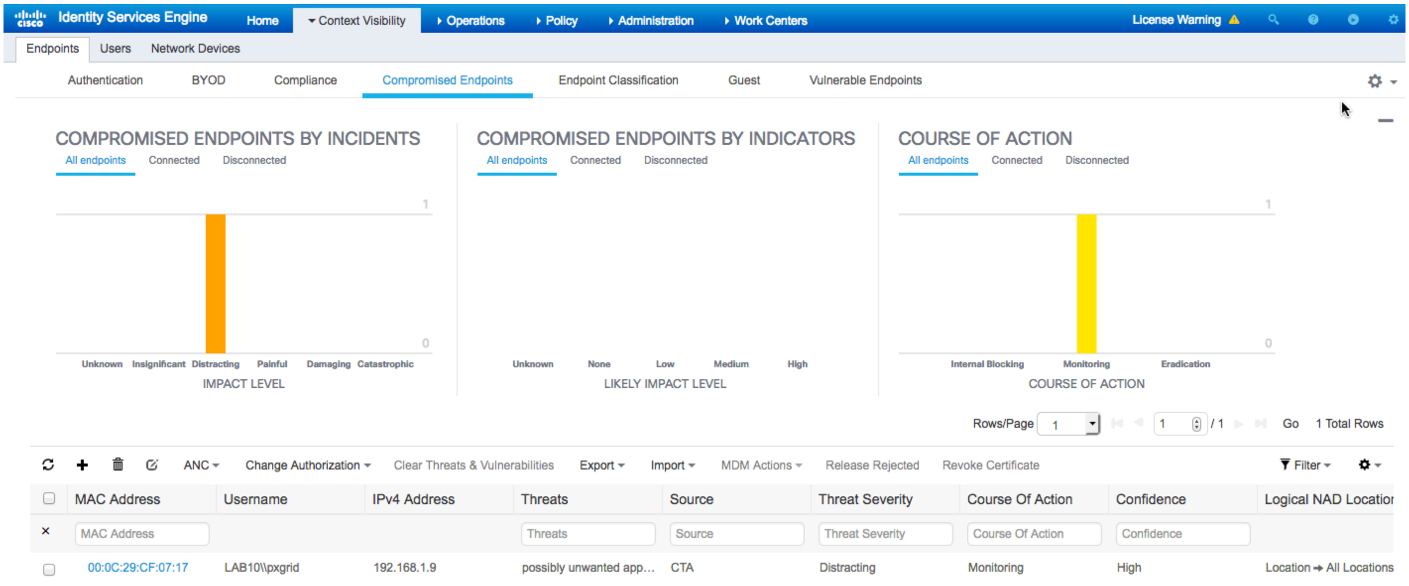
This section illustrates the graphic view of compromised hosts in ISE.

Each incident indicated by CTA has the following attributes:

- Impact Level: Impact assessment for this cyber threat incident
- Likely Impact Level: Confidence held in the characterization of the incident
- Recommended Course of Action: Recommended type of incident response action

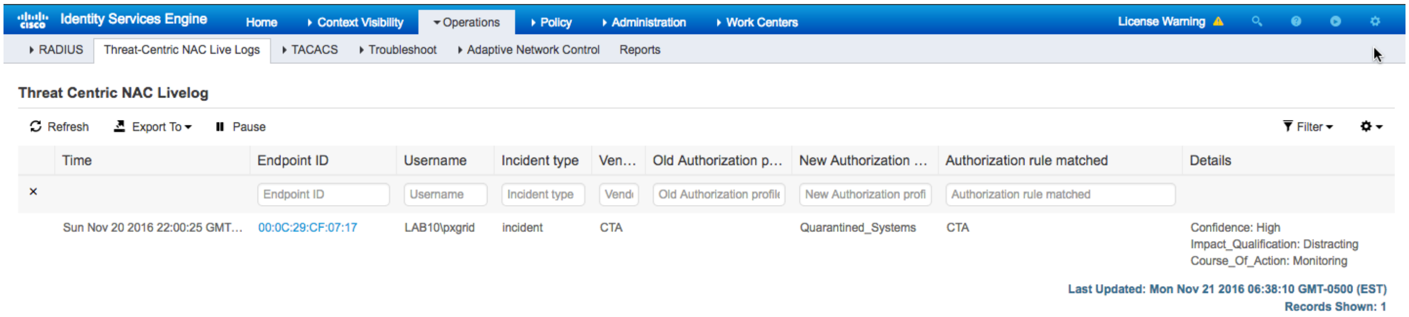
Select **Context Visibility->Endpoints->Compromised Hosts**

You will see the reported incident(s) from the CTA instance and the ISE Course of Action response as determined by the ISE Authorization Course of Action policy.



MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Course Of Action	Confidence	Logical NAD Locatior
00:0C:29:CF:07:17	LAB10\\pxgrid	192.168.1.9	possibly unwanted app…	CTA	Distracting	Monitoring	High	Location → All Locations

Select **Operations->Threat Centric NAC Live Logs** you should also see the incidents.

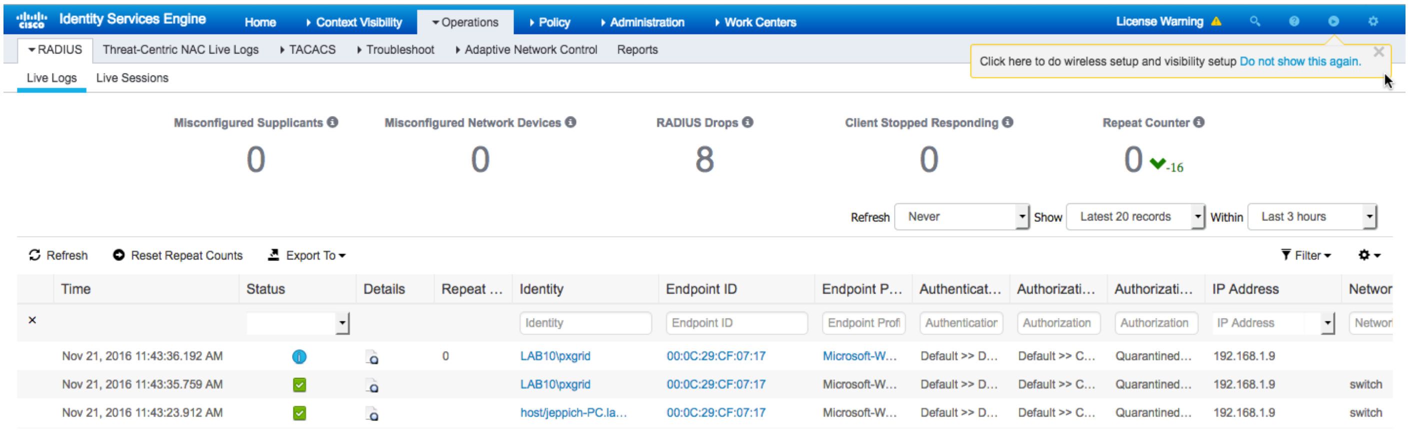


Threat Centric NAC Livelog

Time	Endpoint ID	Username	Incident type	Ven…	Old Authorization p…	New Authorization …	Authorization rule matched	Details
Sun Nov 20 2016 22:00:25 GMT…	00:0C:29:CF:07:17	LAB10\pxgrid	incident	CTA		Quarantined_Systems	CTA	Confidence: High Impact_Qualification: Distracting Course_Of_Action: Monitoring

Last Updated: Mon Nov 21 2016 06:38:10 GMT-0500 (EST)
Records Shown: 1

Select Operations**->RADIUS->Radius Live Logs,** you should see the endpoints assigned a Security Group Tag (SGT) of Quarantined Systems



Click here to do wireless setup and visibility setup Do not show this again.

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	8	0	0 -16

Refresh: Never Show: Latest 20 records Within: Last 3 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address	Networ
Nov 21, 2016 11:43:36.192 AM	●		0	LAB10\pxgrid	00:0C:29:CF:07:17	Microsoft-W...	Default >> D...	Default >> C...	Quarantined...	192.168.1.9	
Nov 21, 2016 11:43:35.759 AM	✓			LAB10\pxgrid	00:0C:29:CF:07:17	Microsoft-W...	Default >> D...	Default >> C...	Quarantined...	192.168.1.9	switch
Nov 21, 2016 11:43:23.912 AM	✓			host/jeppich-PC.la...	00:0C:29:CF:07:17	Microsoft-W...	Default >> D...	Default >> C...	Quarantined...	192.168.1.9	switch

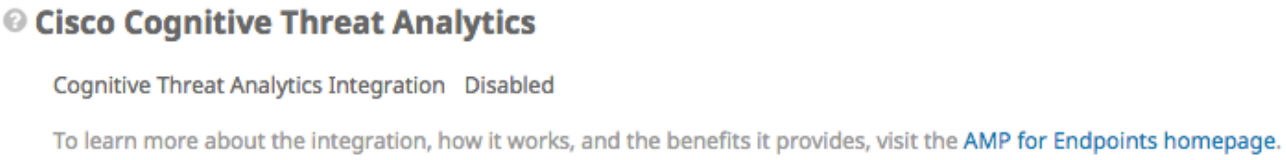
Provisioning CTA through AMP (Optional)

Internal CTA accounts, please reach out to ipss-salesoperations@cisco.com, you can provision a CTA account from your AMP console.

Logins to both instances are defined below:

- CTA for cloud instance: https://scancenter.scansafe.com/portal/admin/login.jsp
- AMP for endpoints cloud instance: https://api.amp.sourcefire.com

Step 1 Select **Accounts-Business**
You should see CTA as being disabled

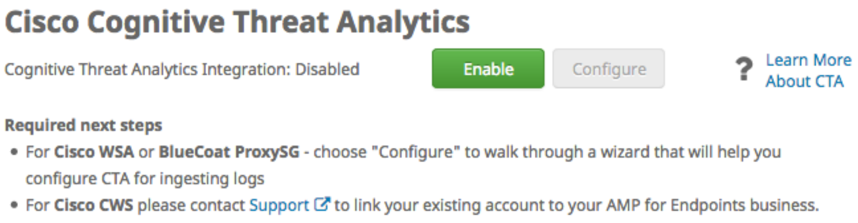


Cisco Cognitive Threat Analytics

Cognitive Threat Analytics Integration Disabled

To learn more about the integration, how it works, and the benefits it provides, visit the AMP for Endpoints homepage.

Step 2 Select **Edit**
You should see the following



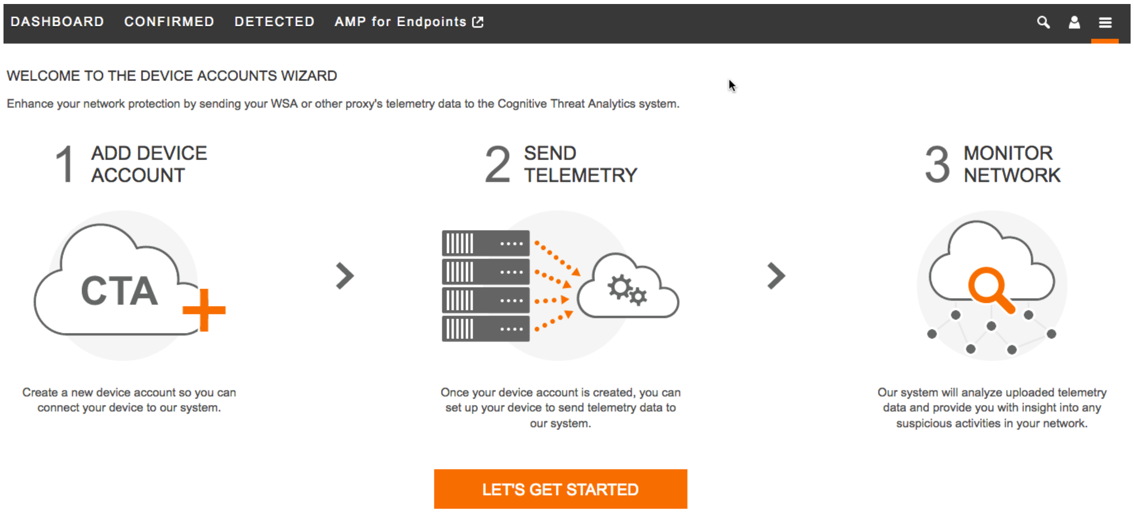
Cisco Cognitive Threat Analytics

Cognitive Threat Analytics Integration: Disabled

Required next steps

- For **Cisco WSA** or **BlueCoat ProxySG** - choose "Configure" to walk through a wizard that will help you configure CTA for ingesting logs
- For **Cisco CWS** please contact Support to link your existing account to your AMP for Endpoints business.

Step 3 Select **Enable->Configure**
Step 4 You should see the following:



WELCOME TO THE DEVICE ACCOUNTS WIZARD

Enhance your network protection by sending your WSA or other proxy's telemetry data to the Cognitive Threat Analytics system.

1 ADD DEVICE ACCOUNT

Create a new device account so you can connect your device to our system.

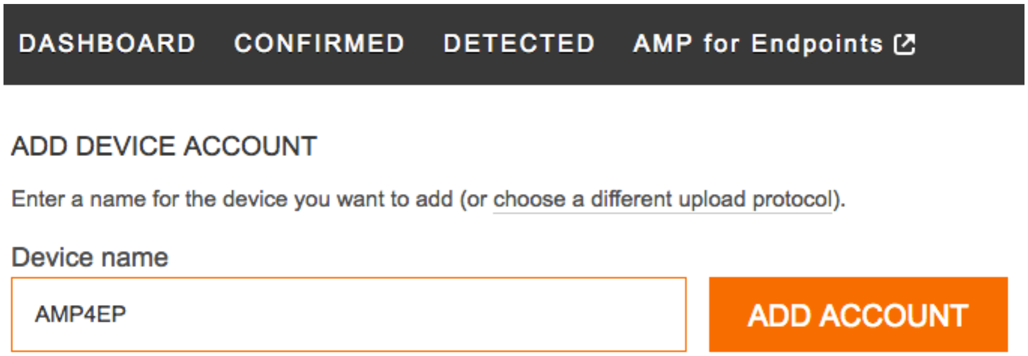
2 SEND TELEMETRY

Once your device account is created, you can set up your device to send telemetry data to our system.

3 MONITOR NETWORK

Our system will analyze uploaded telemetry data and provide you with insight into any suspicious activities in your network.

Step 5 Select **Lets Get Started**
Step 6 Select **SCP**
Step 7 Add **Device Account**

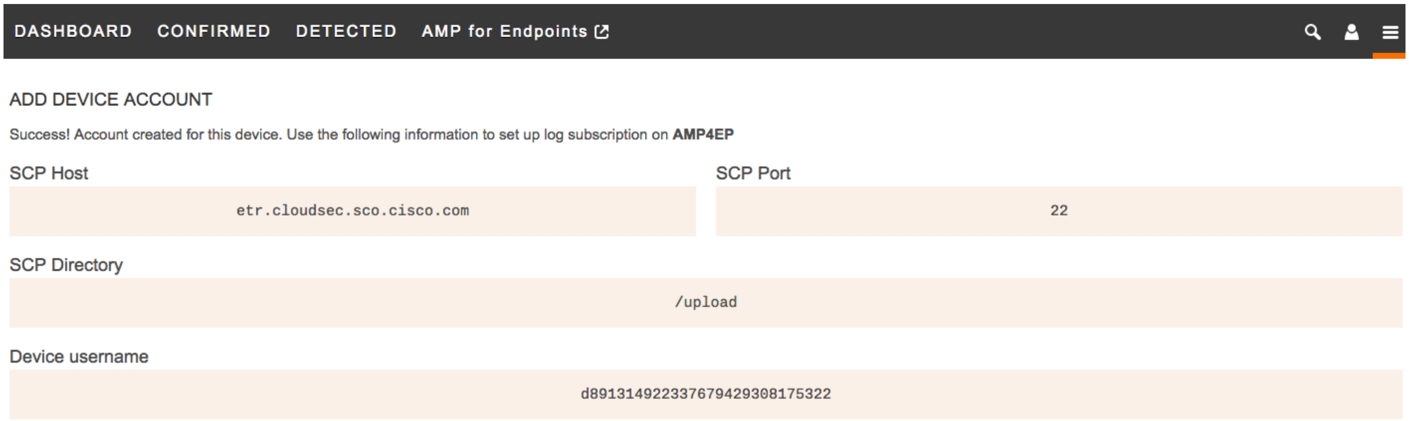


ADD DEVICE ACCOUNT

Enter a name for the device you want to add (or choose a different upload protocol).

Device name: AMP4EP

Step 8 On the WSA, select System Administration->Log Subscriptions->CTALogs, scroll down to **Retrieval Method** and enter the following under **SCP on remote server**



ADD DEVICE ACCOUNT

Success! Account created for this device. Use the following information to set up log subscription on **AMP4EP**

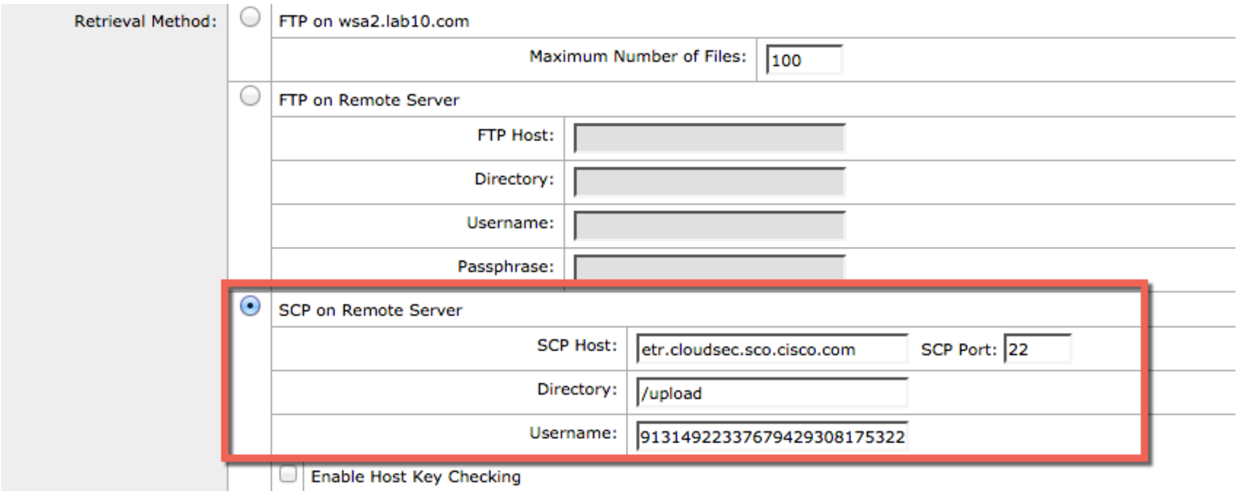
SCP Host: etr.cloudsec.sco.cisco.com

SCP Port: 22

SCP Directory: /upload

Device username: d8913149223376794293O8175322

Step 9 On the WSA, you should see the following:


Retrieval Method:

○ FTP on wsa2.lab10.com

Maximum Number of Files: 100

○ FTP on Remote Server

FTP Host:

Directory:

Username:

Passphrase:

● SCP on Remote Server

SCP Host: etr.cloudsec.sco.cisco.com SCP Port: 22

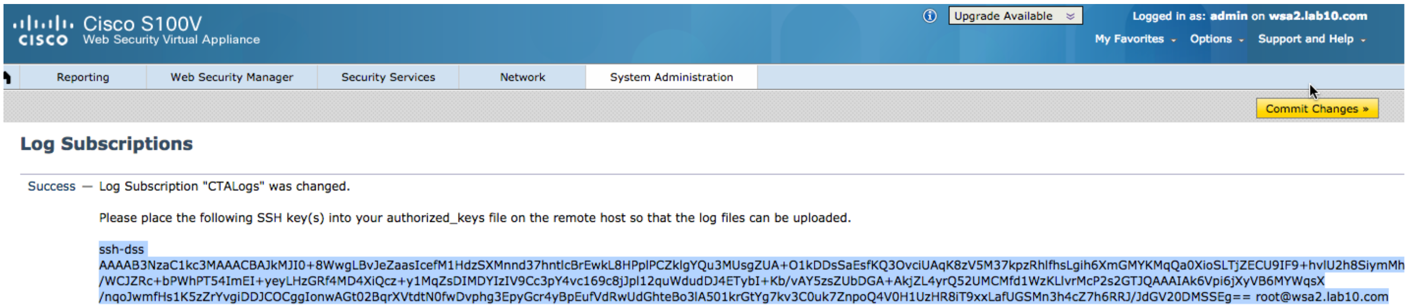
Directory: /upload

Username: 913149223376794293O8175322

□ Enable Host Key Checking

Step 10 Enable **Host Key Checking->Automatically Scan->Submit**

Step 11 Copy the ssh-dss key



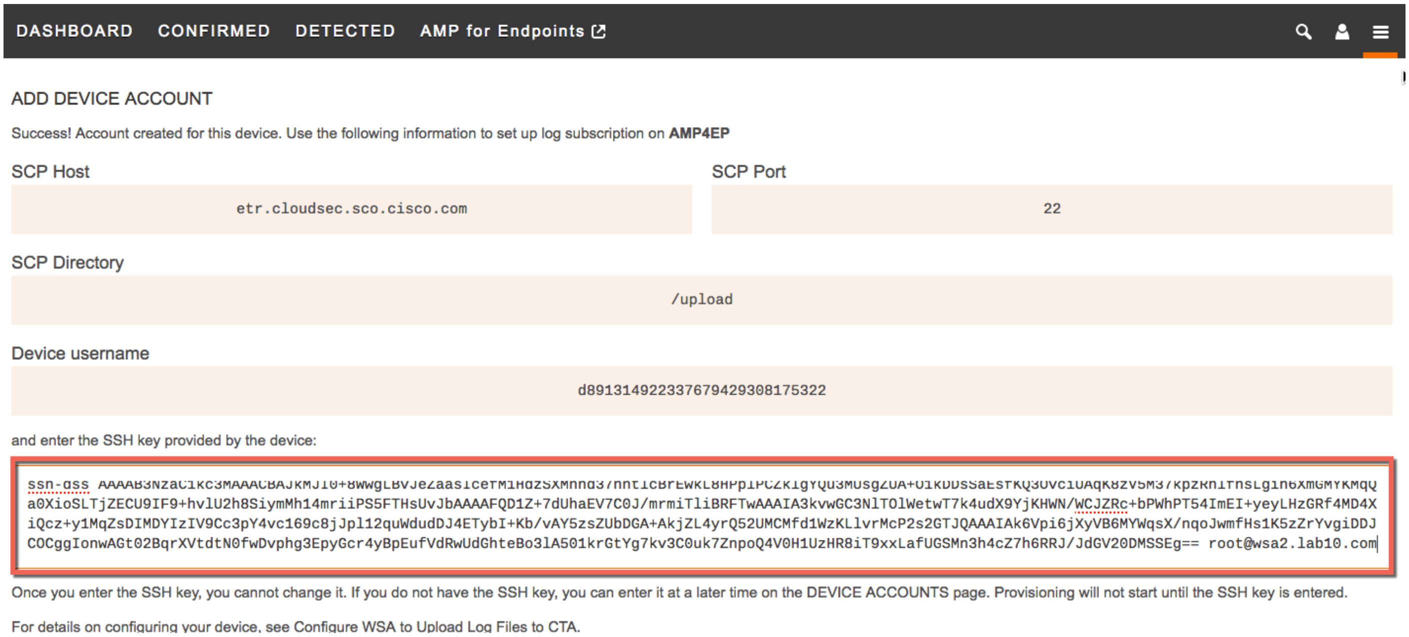
Log Subscriptions

Success — Log Subscription "CTALogs" was changed.

Please place the following SSH key(s) into your authorized_keys file on the remote host so that the log files can be uploaded.

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAJkMJI0+8WwgLBvJeZaasIcefM1HdzSXMnnd37hntlcBrEwkL8HPplPCZklgYQu3MUsgZUA+O1kDDsSaEsfKQ3OvciUAqK8zV5M37kpzRhlfhsLgih6XmGMYKMqQa0XioSLTjZECU9IF9+hvlU2h8SiymMh
/WCJZRc+bPWhPT54ImEI+yeyLHzGRf4MD4XiQcz+y1MqZsDIMDYIzIV9Cc3pY4vc169c8jJpl12quWdudDJ4ETybI+Kb/vAY5zsZUbDGA+AkjZL4yrQ52UMCMfd1WzKLlvrMcP2s2GTJQAAAIAk6Vpi6jXyVB6MYWqsX
/nqoJwmfHs1K5zZrYvgiDDJCOCggIonwAGt02BqrXVtdtN0fwDvphg3EpyGcr4yBpEufVdRwUdGhteBo3lA501krGtYg7kv3C0uk7ZnpoQ4V0H1UzHR8iT9xxLafUGSMn3h4cZ7h6RRJ/JdGV20DMSSEg== root@wsa2.lab10.com
```

Step 12 Paste into ssh-key for AMP4EP configuration



ADD DEVICE ACCOUNT

Success! Account created for this device. Use the following information to set up log subscription on **AMP4EP**

SCP Host: etr.cloudsec.sco.cisco.com

SCP Port: 22

SCP Directory: /upload

Device username: d891314922337679429308175322

and enter the SSH key provided by the device:

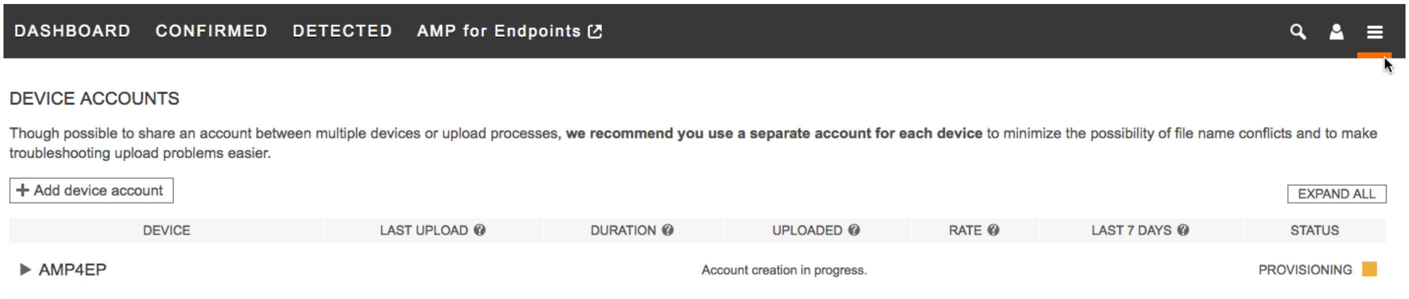
```
ssh-dss AAAAB3NzaC1kc3MAAACBAJkMJI0+8WwgLBvJeZaasIcefM1HdzSXMnnd37hntIcBrEwkL8HPplPCZklgYQu3MUsgZUA+O1kDDsSaEsfKQ3OvciUAqK8zV5M37kpzRhlfhsLgih6XmGMYKMqQ
a0XioSLTjZECU9IF9+hvlU2h8SiymMh14mriiPS5FTHsUvJbAAAAFQD1Z+7dUhaEV7C0J/mrmiTliBRFTwAAAIA3kvwGC3NlTOlWetwT7k4udX9YjKHWN/WCJZRc+bPWhPT54ImEI+yeyLHzGRf4MD4X
iQcz+y1MqZsDIMDYIzIV9Cc3pY4vc169c8jJpl12quWdudDJ4ETybI+Kb/vAY5zsZUbDGA+AkjZL4yrQ52UMCMfd1WzKLlvrMcP2s2GTJQAAAIAk6Vpi6jXyVB6MYWqsX/nqoJwmfHs1K5zZrYvgiDDJ
COCggIonwAGt02BqrXVtdtN0fwDvphg3EpyGcr4yBpEufVdRwUdGhteBo3lA501krGtYg7kv3C0uk7ZnpoQ4V0H1UzHR8iT9xxLafUGSMn3h4cZ7h6RRJ/JdGV20DMSSEg== root@wsa2.lab10.com
```

Once you enter the SSH key, you cannot change it. If you do not have the SSH key, you can enter it at a later time on the DEVICE ACCOUNTS page. Provisioning will not start until the SSH key is entered.

For details on configuring your device, see Configure WSA to Upload Log Files to CTA.

Step 13 Select **Finish**

Step 14 You should see the following

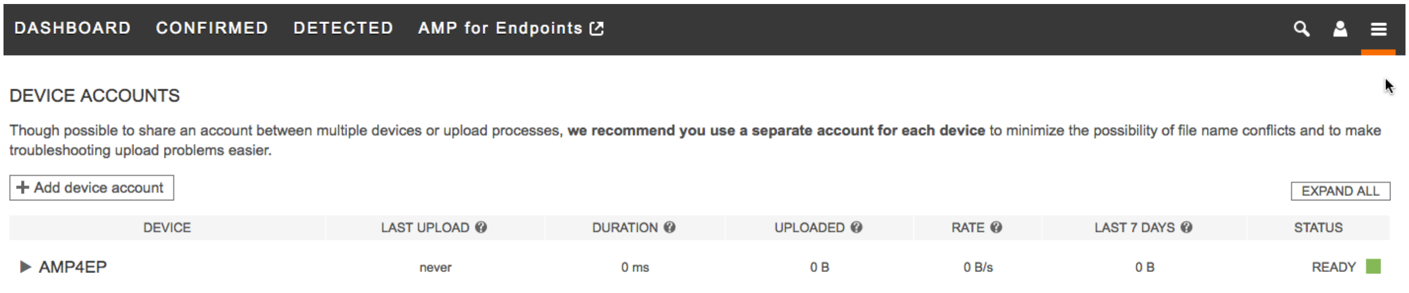


DEVICE ACCOUNTS

Though possible to share an account between multiple devices or upload processes, **we recommend you use a separate account for each device** to minimize the possibility of file name conflicts and to make troubleshooting upload problems easier.

DEVICE	LAST UPLOAD	DURATION	UPLOADED	RATE	LAST 7 DAYS	STATUS
▶ AMP4EP			Account creation in progress.			PROVISIONING 🟧

Step 15 You can refresh the refresh the screen to see a READY state

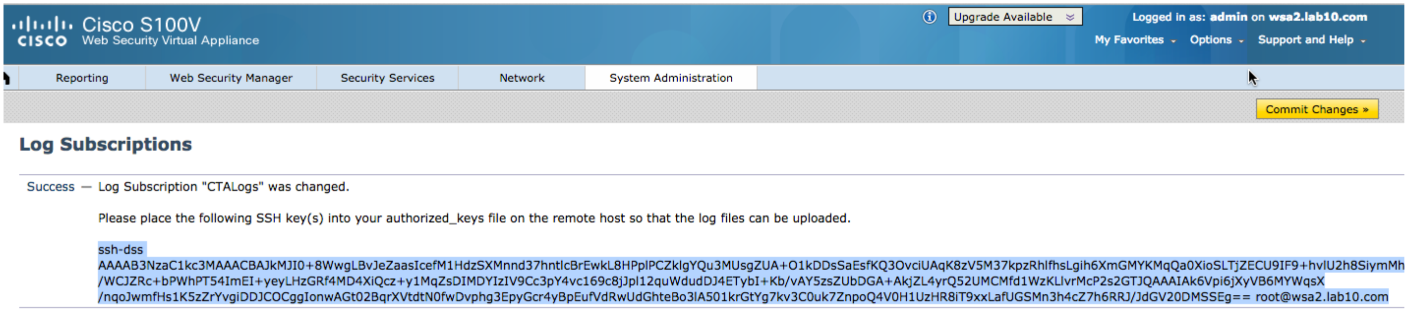


DEVICE ACCOUNTS

Though possible to share an account between multiple devices or upload processes, **we recommend you use a separate account for each device** to minimize the possibility of file name conflicts and to make troubleshooting upload problems easier.

DEVICE	LAST UPLOAD	DURATION	UPLOADED	RATE	LAST 7 DAYS	STATUS
▶ AMP4EP	never	0 ms	0 B	0 B/s	0 B	READY 🟩

Step 16 Go back to the WSA and commit the changes



Log Subscriptions

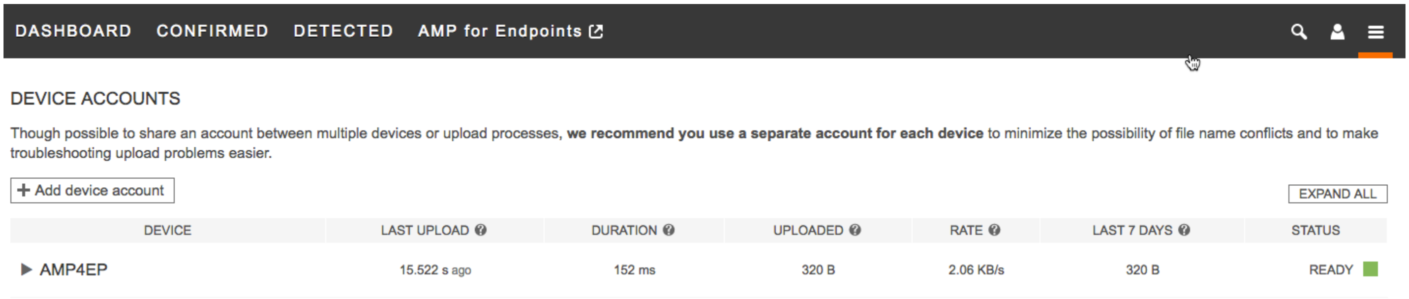
Success — Log Subscription "CTALogs" was changed.

Please place the following SSH key(s) into your authorized_keys file on the remote host so that the log files can be uploaded.

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAJkMJI0+8WwgLBvJeZaasIcefM1HdzSXMnnd37hntlcBrEwkL8HPplPCZklgYQu3MUsgZUA+O1kDDsSaEsfKQ3OvciUAqK8zV5M37kpzRhlfhsLgih6XmGMYKMqQa0XioSLTjZECU9IF9+hvlU2h8SiymMh
/WCJZRc+bPWhPT54ImEI+yeyLHzGRf4MD4XiQcz+y1MqZsDIMDYIzIV9Cc3pY4vc169c8jJpl12quWdudDJ4ETybI+Kb/vAY5zsZUbDGA+AkjZL4yrQ52UMCMfd1WzKLlvrMcP2s2GTJQAAAIAk6Vpi6jXyVB6MYWqsX
/nqoJwmfHs1K5zZrYvgiDDJCOCggIonwAGt02BqrXVtdtN0fwDvphg3EpyGcr4yBpEufVdRwUdGhteBo3lA501krGtYg7kv3C0uk7ZnpoQ4V0H1UzHR8iT9xxLafUGSMn3h4cZ7h6RRJ/JdGV20DMSSEg== root@wsa2.lab10.com
```

Step 17 Select **Commit Changes->Commit Changes**

Step 18 On the AMP4EP device account screen you should see the following after a couple of minutes



DEVICE ACCOUNTS

Though possible to share an account between multiple devices or upload processes, **we recommend you use a separate account for each device** to minimize the possibility of file name conflicts and to make troubleshooting upload problems easier.

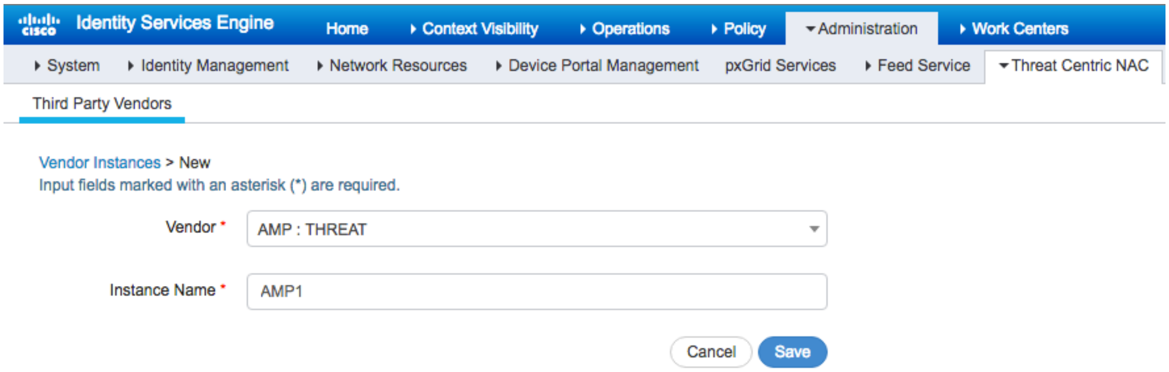
DEVICE	LAST UPLOAD	DURATION	UPLOADED	RATE	LAST 7 DAYS	STATUS
▶ AMP4EP	15.522 s ago	152 ms	320 B	2.06 KB/s	320 B	READY 🟩

Configuring ISE AMP Adapter

Step 1 Select **Administration->Threat Centric NAC->Add->AMP:Threat** from the menu drop-down menu

Step 2 Provide an Instance Name **AMP1**

You should see the following:



Vendor Instances > New

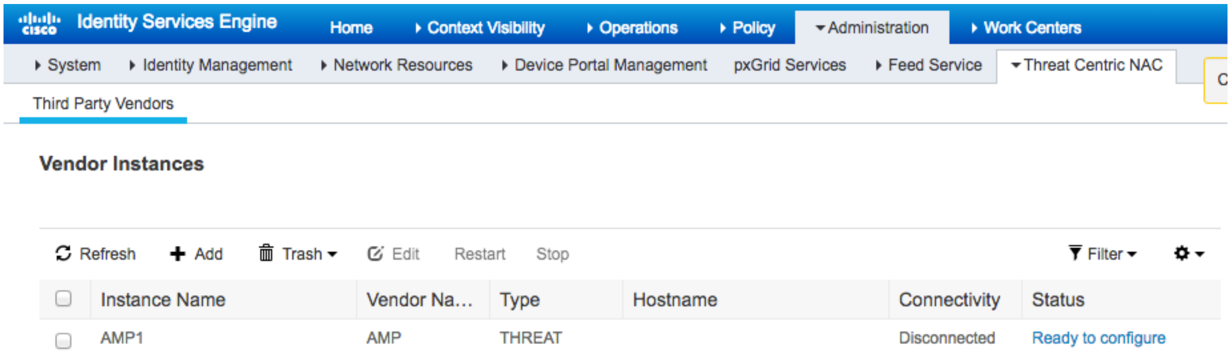
Input fields marked with an asterisk (*) are required.

Vendor * AMP : THREAT

Instance Name * AMP1

Step 3 Select **Save**

You should see: **Ready to Configure**



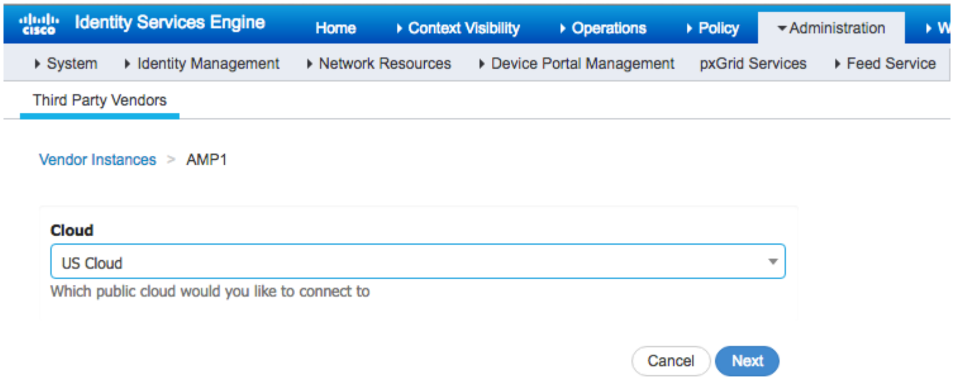
Vendor Instances

☐	Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
☐	AMP1	AMP	THREAT		Disconnected	Ready to configure

Step 4 Select **Ready to Configure**

Step 5 Enter proxy information if applicable select **Next**

Step 6 Select **US Cloud** from the menu drop-down



Vendor Instances > AMP1

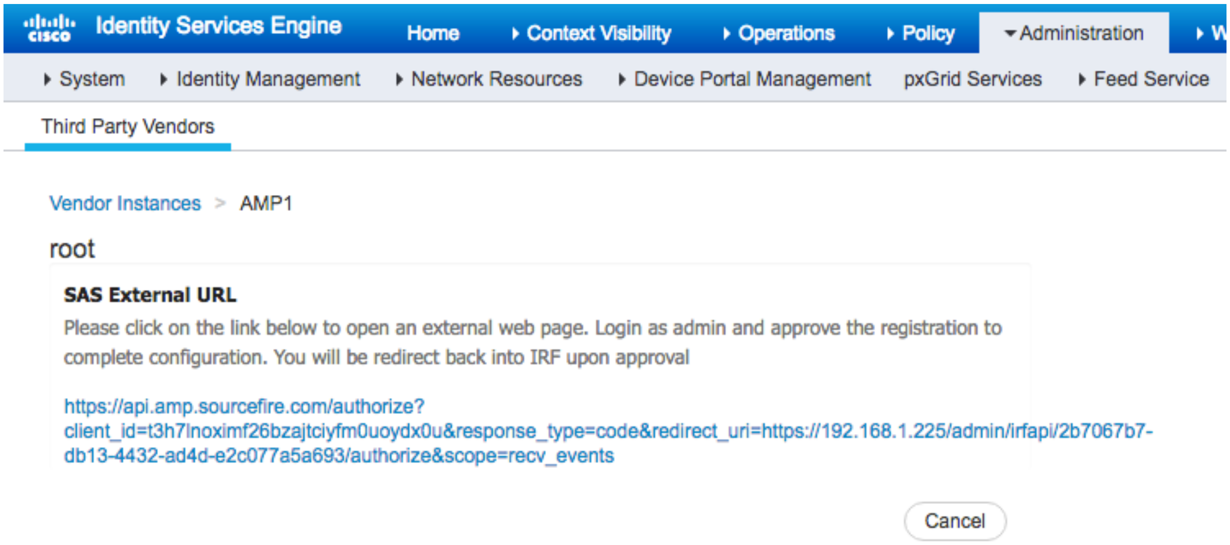
Cloud

US Cloud

Which public cloud would you like to connect to

Step 7 Select **Next**

Step 8 Click on the registration link



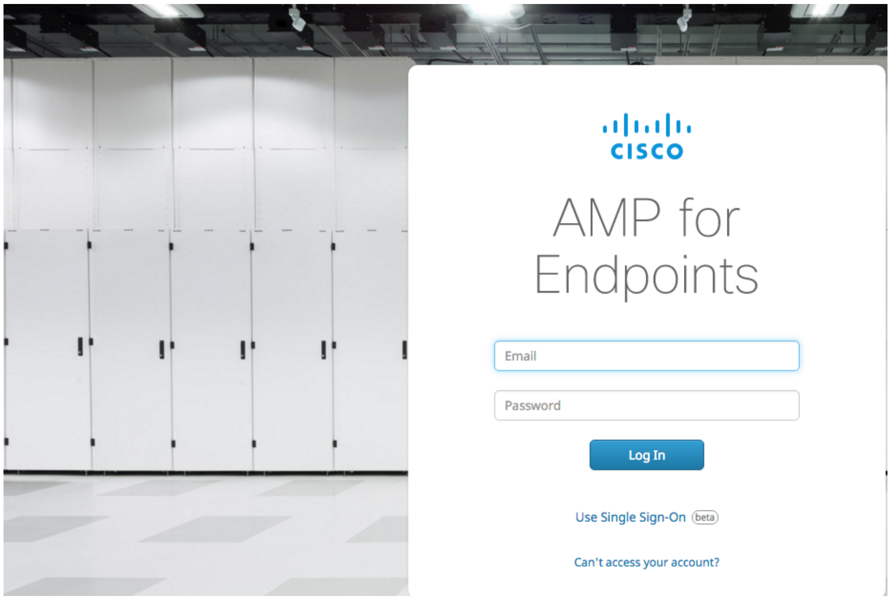
root

SAS External URL

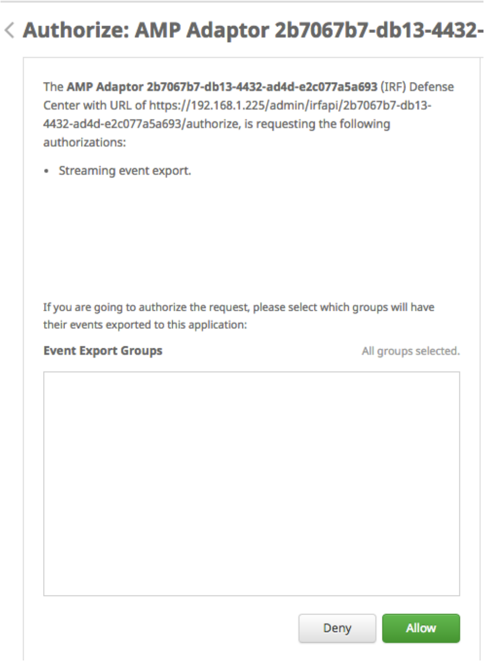
Please click on the link below to open an external web page. Login as admin and approve the registration to complete configuration. You will be redirect back into IRF upon approval

https://api.amp.sourcefire.com/authorize?client_id=t3h7lnoximf26bzajtciyfm0uoydx0u&response_type=code&redirect_uri=https://192.168.1.225/admin/irfapi/2b7067b7-db13-4432-ad4d-e2c077a5a693/authorize&scope=recv_events

Step 9 Login as admin



Step 10 Select **Allow**



Authorize: AMP Adaptor 2b7067b7-db13-4432-

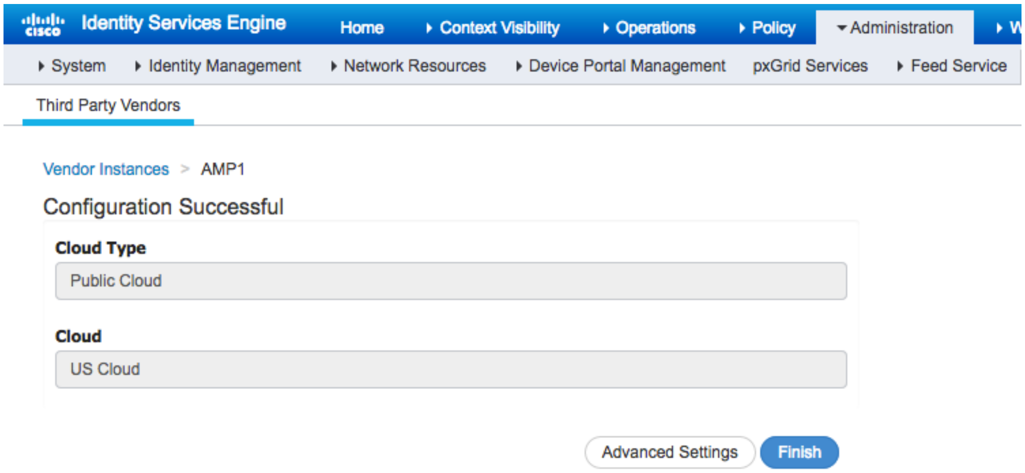
The **AMP Adaptor 2b7067b7-db13-4432-ad4d-e2c077a5a693** (IRF) Defense Center with URL of https://192.168.1.225/admin/irfapi/2b7067b7-db13-4432-ad4d-e2c077a5a693/authorize, is requesting the following authorizations:

- Streaming event export.

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

Event Export Groups All groups selected.

Step 11 You should see the following



Configuration Successful

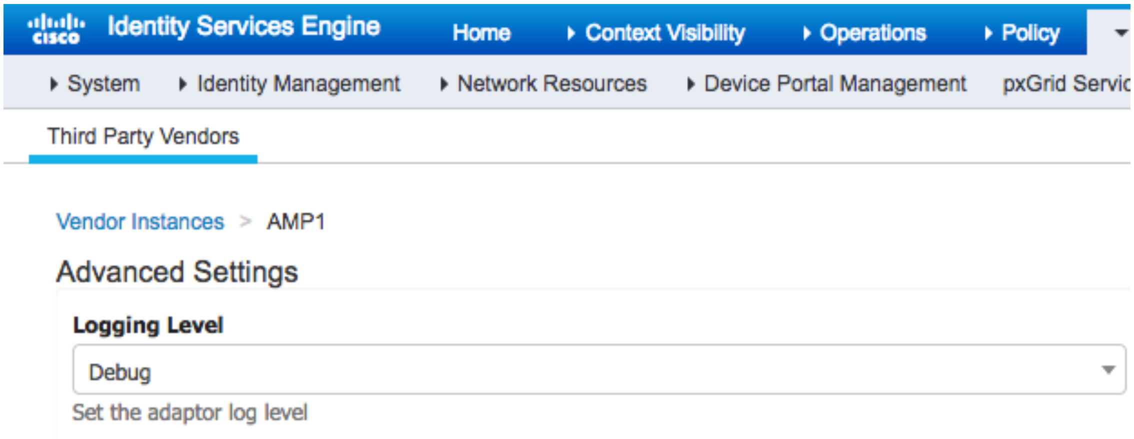
Cloud Type

Public Cloud

Cloud

US Cloud

Step 12 Select **Advanced Settings,** change Logging Level from Info to Debug



Advanced Settings

Logging Level

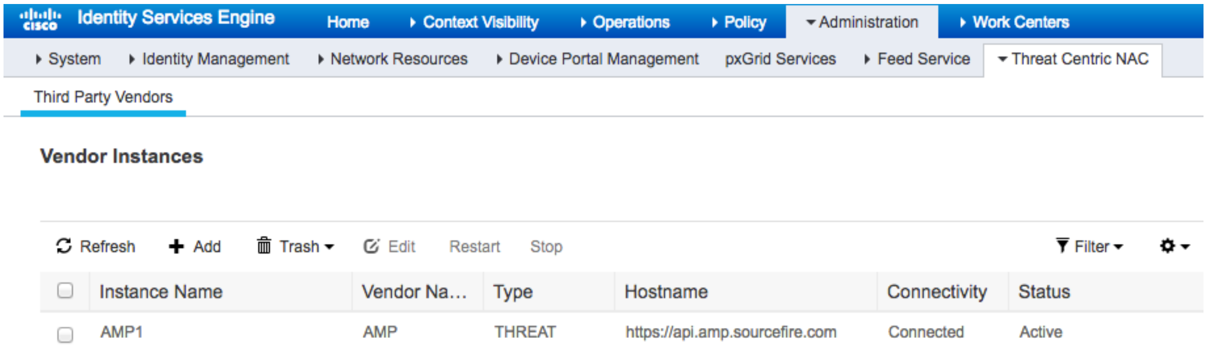
Debug

Set the adaptor log level

Step 13 Select **Next**

Step 14 Select **Finish**

You should see the following:

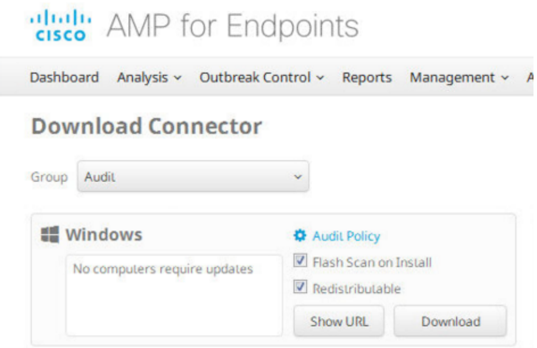


Vendor Instances

□	Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
□	AMP1	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active

Installing AMP Connector

Step 1 Select **Management->Download Connector->Select Group->Audit**



Download Connector

Group Audit

Windows

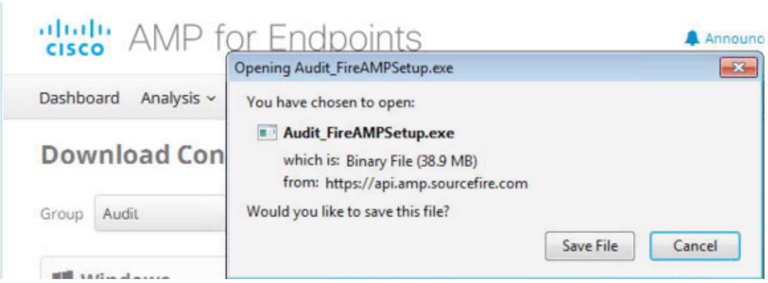
No computers require updates

Audit Policy

☑ Flash Scan on Install

☑ Redistributable

Step 2 Select **Download** and save the file locally



Opening Audit_FireAMPSetup.exe

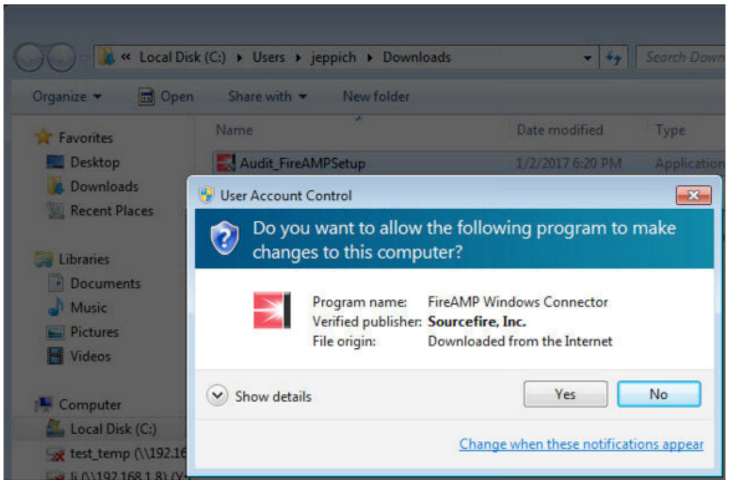
You have chosen to open:

Audit_FireAMPSetup.exe

which is: Binary File (38.9 MB)
from: https://api.amp.sourcefire.com

Would you like to save this file?

Step 3 Run the setup and install the connector application

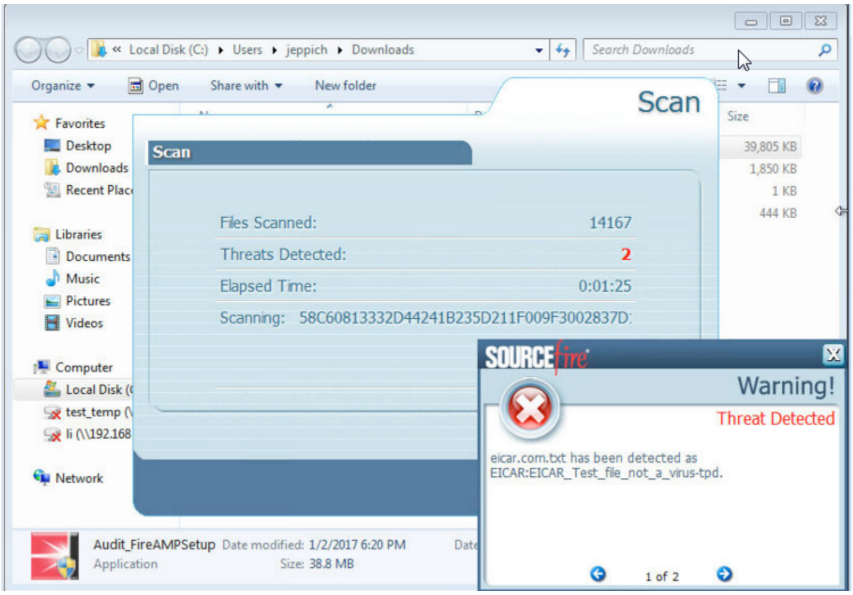


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: FireAMP Windows Connector
Verified publisher: **Sourcefire, Inc.**
File origin: Downloaded from the Internet

Step 4 Run a full scan



Scan

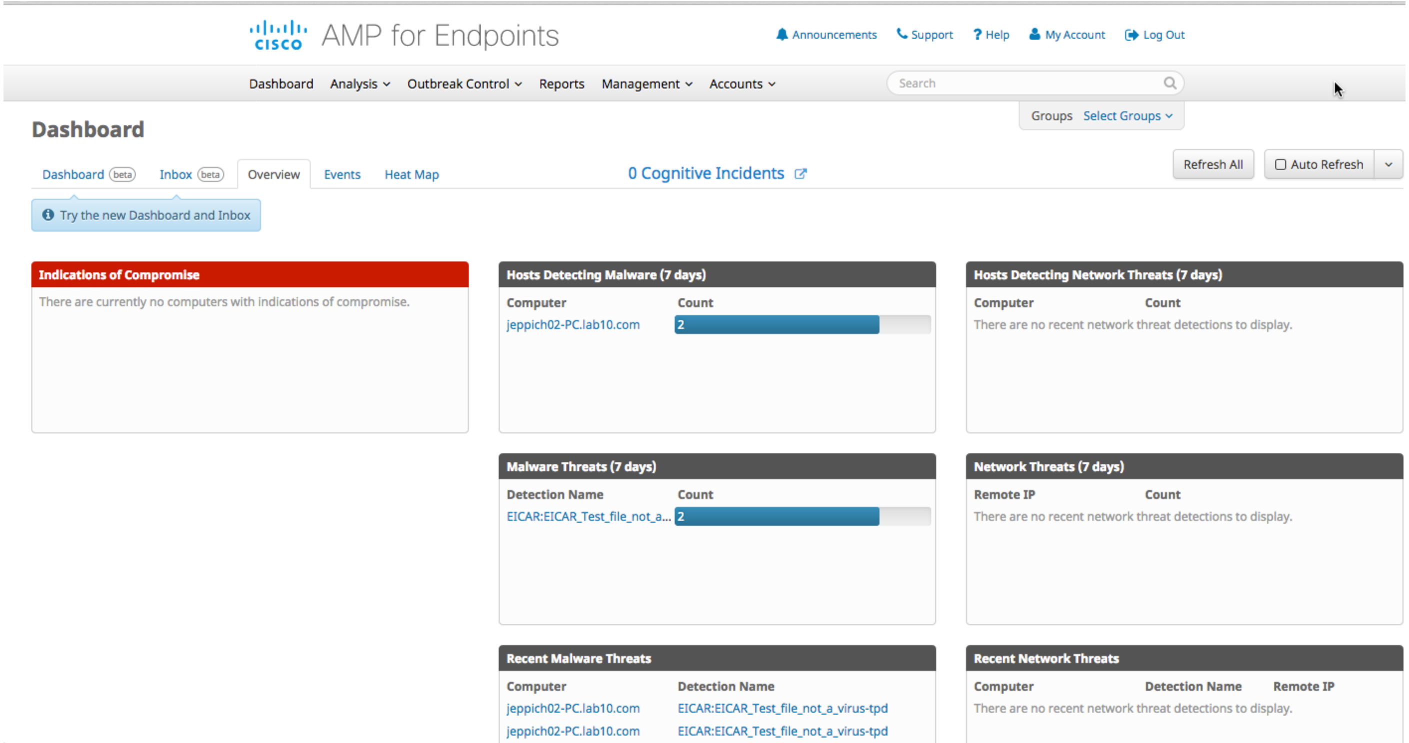
Files Scanned: 14167
Threats Detected: 2
Elapsed Time: 0:01:25
Scanning: 58C60813332D44241B235D211F009F3002837D

Warning!
Threat Detected

eicar.com.txt has been detected as EICAR:EICAR_Test_file_not_a_virus-tpd.

Audit_FireAMPSetup Date modified: 1/2/2017 6:20 PM
Application Size: 38.8 MB

Step 5 Login in to AMP for Endpoint instance



Indications of Compromise

There are currently no computers with indications of compromise.

Hosts Detecting Malware (7 days)

Computer	Count
jeppich02-PC.lab10.com	2

Hosts Detecting Network Threats (7 days)

Computer Count

There are no recent network threat detections to display.

Malware Threats (7 days)

Detection Name	Count
EICAR:EICAR_Test_file_not_a...	2

Network Threats (7 days)

Remote IP Count

There are no recent network threat detections to display.

Recent Malware Threats

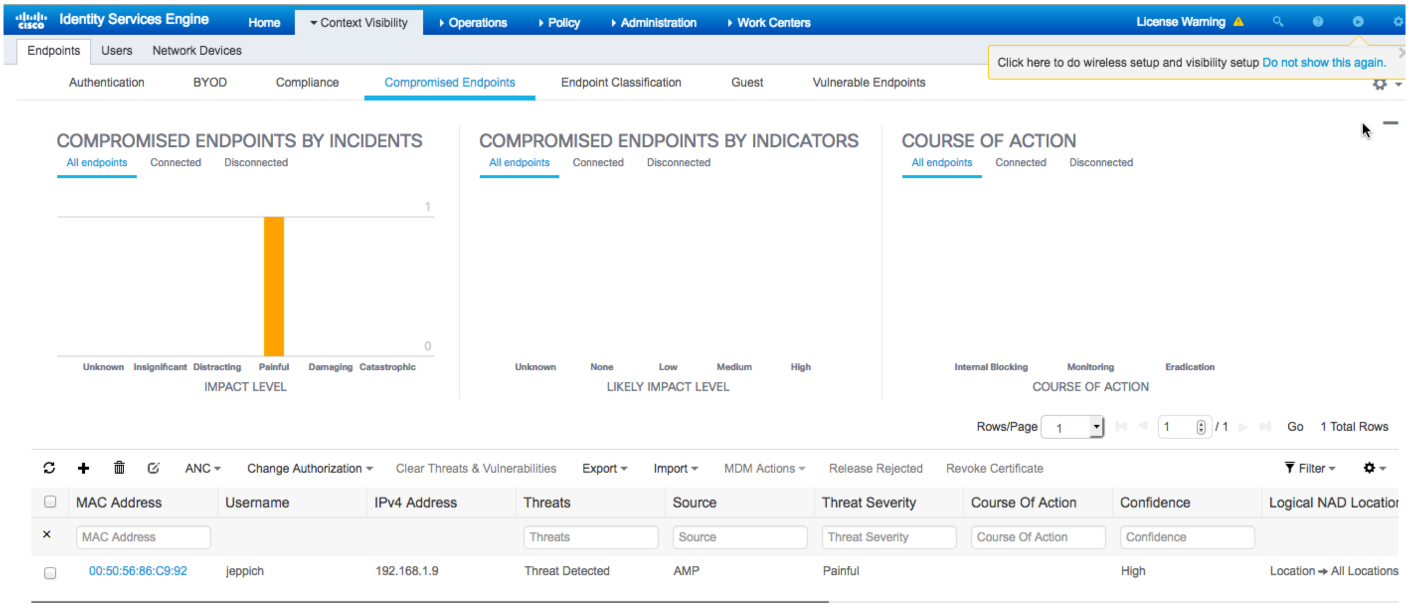
Computer	Detection Name
jeppich02-PC.lab10.com	EICAR:EICAR_Test_file_not_a_virus-tpd
jeppich02-PC.lab10.com	EICAR:EICAR_Test_file_not_a_virus-tpd

Recent Network Threats

Computer Detection Name Remote IP

There are no recent network threat detections to display.

Step 6 Select **Context Visibility->Endpoints->Compromised Endpoints**



Click here to do wireless setup and visibility setup Do not show this again.

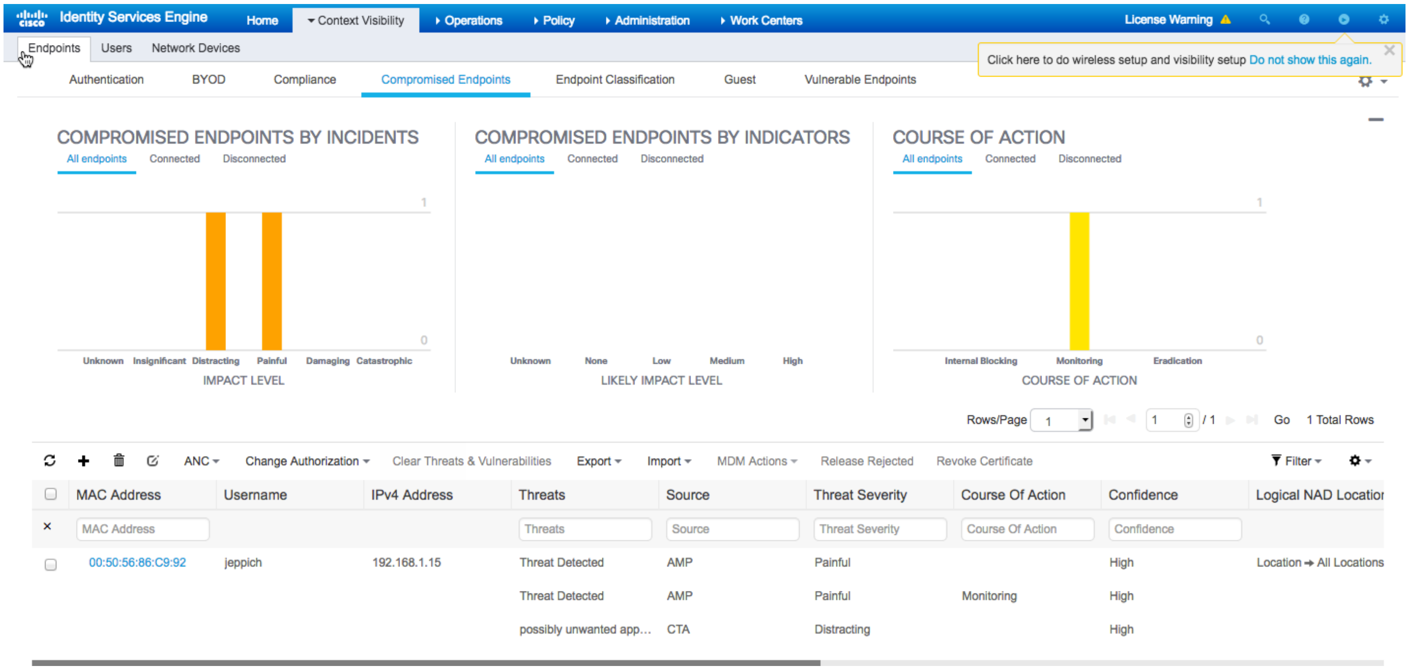
MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Course Of Action	Confidence	Logical NAD Locatior
00:50:56:86:C9:92	jeppich	192.168.1.9	Threat Detected	AMP	Painful		High	Location → All Locations

Step 7 To enable CTA events to appear in ISE, you need to create the CTA Adapter and add ISE to the TAXII/STIX CTA account. Please see: Configuring Incidents Export from CTA to ISE.

Testing

Select **Context Visibility->Endpoints->Compromised Endpoints**

Here we see the results with both the ISE AMP Adapter and ISE CTA Adapter installed.

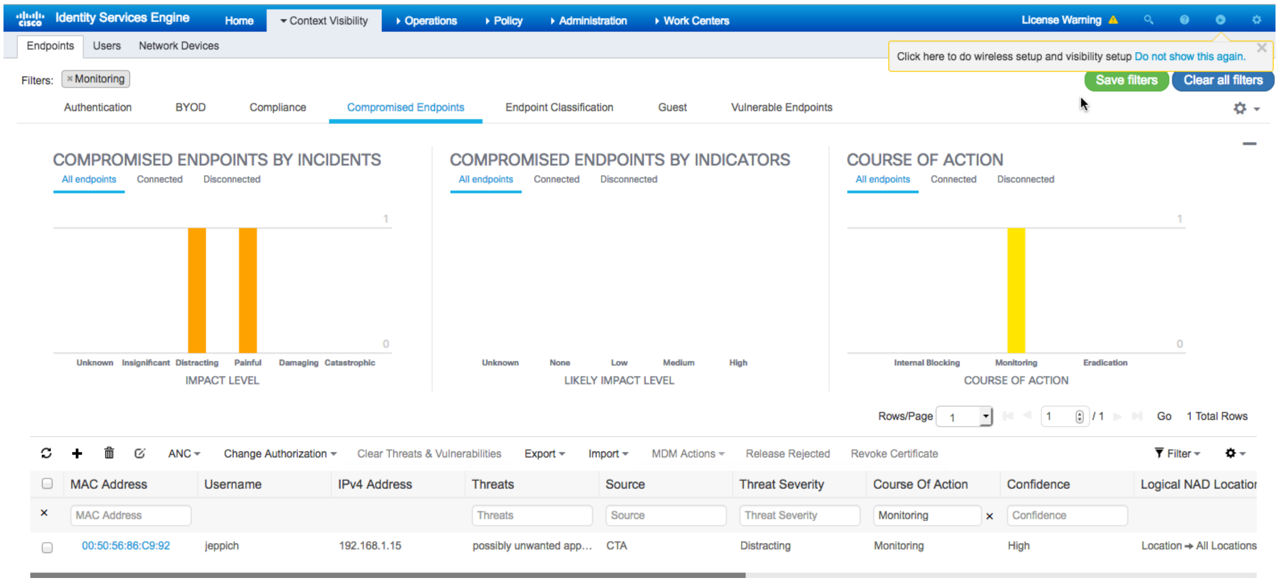


Click here to do wireless setup and visibility setup Do not show this again.

Rows/Page 1 | 1 / 1 Go 1 Total Rows

MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Course Of Action	Confidence	Logical NAD Locatior
00:50:56:86:C9:92	jeppich	192.168.1.15	Threat Detected	AMP	Painful		High	Location → All Locations
			Threat Detected	AMP	Painful	Monitoring	High	
			possibly unwanted app…	CTA	Distracting		High	

Note the CTA incident of “potentially unwanted application” under threat and the associated monitoring event and the associated Monitoring Course of action event.



Click here to do wireless setup and visibility setup Do not show this again.

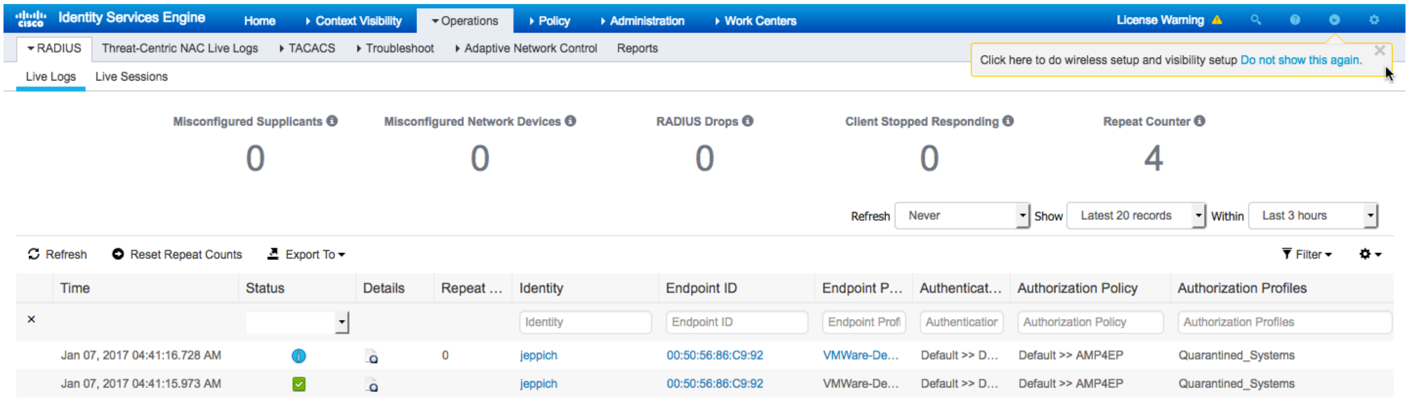
Filters: × Monitoring

Rows/Page 1 | 1 / 1 Go 1 Total Rows

MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Course Of Action	Confidence	Logical NAD Locatior
00:50:56:86:C9:92	jeppich	192.168.1.15	possibly unwanted app…	CTA	Distracting	Monitoring	High	Location → All Locations

Select **Operations->RADIUS->Live Logs**

Here the endpoint is successfully quarantined and assigned the Quarantine Security Group Tag of Quarantine.



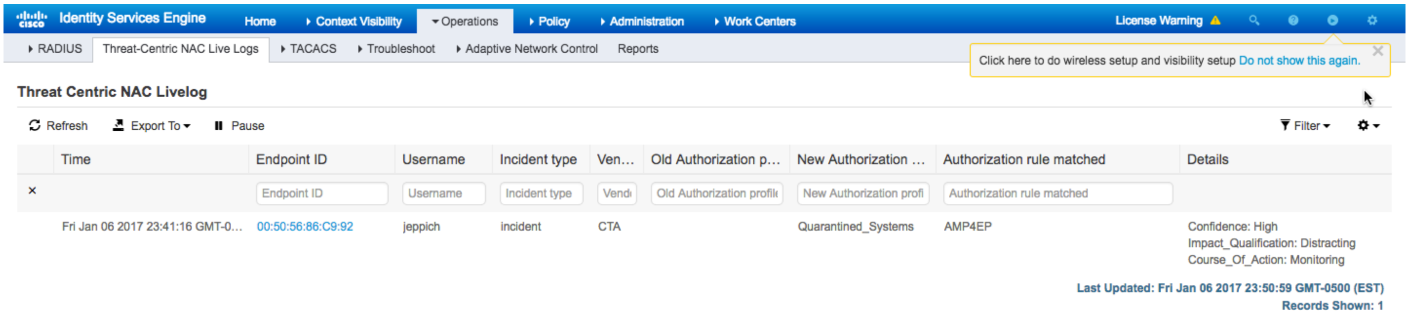
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	4

Refresh Never Show Latest 20 records Within Last 3 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Policy	Authorization Profiles
				Identity	Endpoint ID	Endpoint Profi	Authentication	Authorization Policy	Authorization Profiles
Jan 07, 2017 04:41:16.728 AM	●		0	jeppich	00:50:56:86:C9:92	VMWare-De...	Default >> D...	Default >> AMP4EP	Quarantined_Systems
Jan 07, 2017 04:41:15.973 AM	✓			jeppich	00:50:56:86:C9:92	VMWare-De...	Default >> D...	Default >> AMP4EP	Quarantined_Systems

Select **Operations->Threat Centric NAC Live Logs**

Here we see the ISE Course of Action Policy

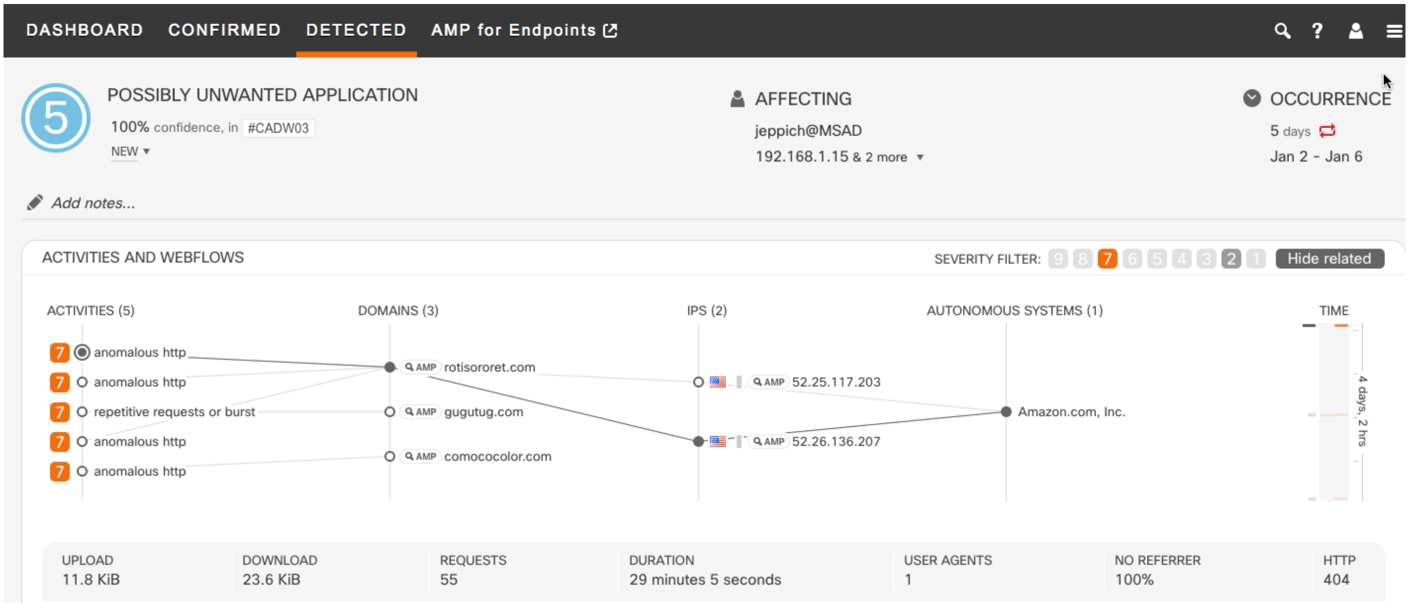


Threat Centric NAC Livelog

Time	Endpoint ID	Username	Incident type	Ven...	Old Authorization p...	New Authorization ...	Authorization rule matched	Details
	Endpoint ID	Username	Incident type	Vend	Old Authorization profile	New Authorization profi	Authorization rule matched	
Fri Jan 06 2017 23:41:16 GMT-0...	00:50:56:86:C9:92	jeppich	incident	CTA		Quarantined_Systems	AMP4EP	Confidence: High Impact_Qualification: Distracting Course_Of_Action: Monitoring

Last Updated: Fri Jan 06 2017 23:50:59 GMT-0500 (EST)
Records Shown: 1

On the CTA instance, we see the related CTA incident



POSSIBLY UNWANTED APPLICATION

100% confidence, in #CADW03

NEW

AFFECTING

jeppich@MSAD

192.168.1.15 & 2 more

OCCURRENCE

5 days

Jan 2 - Jan 6

ACTIVITIES AND WEBFLOWS

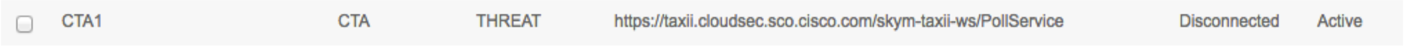
UPLOAD	DOWNLOAD	REQUESTS	DURATION	USER AGENTS	NO REFERRER	HTTP
11.8 KiB	23.6 KiB	55	29 minutes 5 seconds	1	100%	404

Troubleshooting

This section highlights some of the troubleshooting procedures between ISE and CTA communication:

Activity in Disconnected State

If the you see the CTA adapter in a disconnected state,



□	CTA1	CTA	THREAT	https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService	Disconnected	Active

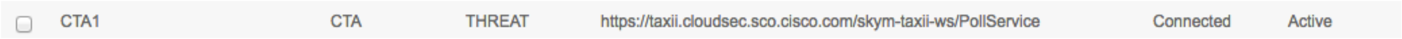
Select ISE->System->Deployment-> edit node and **disable** the **TC-NAC service**. Wait a few seconds and re-start the TC-NAC service

Run the below command to view the state of TC-NAC services

```
sh application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          3774
Database Server                        running          69 PROCESSES
Application Server                     running          8024
Profiler Database                      running          5442
ISE Indexing Engine                    running          9466
AD Connector                           running          13243
M&T Session Database                   running          5349
M&T Log Collector                      running          8246
M&T Log Processor                      running          8071
Certificate Authority Service          running          13016
EST Service                            running          20577
SXP Engine Service                     disabled
Docker Daemon                          running          608
TC-NAC MongoDB Container               running          16184
TC-NAC RabbitMQ Container              running          16327
TC-NAC Core Engine Container           running          16957
VA Database                            running          17436
VA Service                             running          17629
Wifi Setup Helper Container            running          12604
 Wifi Setup Helper Vault               running          31
--More--
```

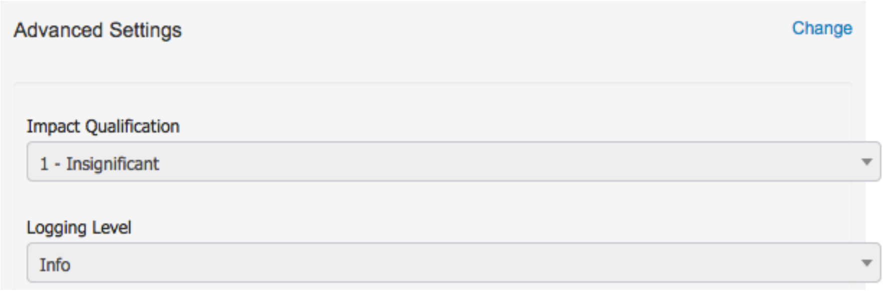
You should now see the CTA adapter in the "connected state"



□	CTA1	CTA	THREAT	https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService	Connected	Active

Not Seeing CTA Events in ISE

- Please make sure you have the Impact Qualification set to **Insignificant,** this will allow the CTA adapter to receive all incidents from the CTA cloud instance



Advanced Settings

Impact Qualification: 1 - Insignificant

Logging Level: Info

- Select **Admnistration->Threat Centric NAC->edit the CTA instance** and under **Advanced Settings**, **Change** the Impact Qualification to **Insignificant**, select **Next->Finish**

References

Integration Guides: https://communities.cisco.com/docs/DOC-64012