

The background is a vibrant, abstract composition of numerous colorful rays and shapes radiating from a central point. The colors include dark blue, light blue, green, yellow, orange, and red. Some shapes are solid, while others have white circular cutouts. The overall effect is dynamic and energetic.

TURN IT UP

CISCO *Live!*

#CiscoLive

Abstract

Today's threat landscape is rapidly changing. Attackers are constantly thinking of new and creative ways to infiltrate a network. Threat response and network security needs to be just as fast and adaptive which is why companies invest millions in security products to protect their domain.

This session will include products such as Cisco Secure Endpoint (Previously Advanced Malware Protection for Endpoints), Identity Services Engine (ISE), and Duo. These products will be integrated together to show how a Malware event detected by Secure Endpoint can be shared with ISE and Duo to block access to network resources as well as cloud applications, respectively.

After this session, participants will be able to understand the basic capabilities of the products, how they are integrated and what information can be shared between them. Afterwards, some demos will be provided to show the integration and rapid threat response in action.



The bridge to possible

Threat Centric Access Control with Cisco Secure Endpoint, Duo and ISE

Zaid Al-Kurdi, Security Consulting Engineer
BRKSEC-2108

CISCO *Live!*

#CiscoLive



Your Speakers For Today



Zaid Al-Kurdi

zalkurdi@cisco.com

Security Consulting Engineer





Agenda

- Introduction
- Cisco Secure Endpoint, Duo and ISE
- Threat Centric Network Access Control
- Threat Centric Application Access Control
- Key Takeaways

Introduction





Shift in IT Landscape

Users, devices and apps are everywhere

Remote Users



Personal &
Mobile Devices



Evolving
Perimeter

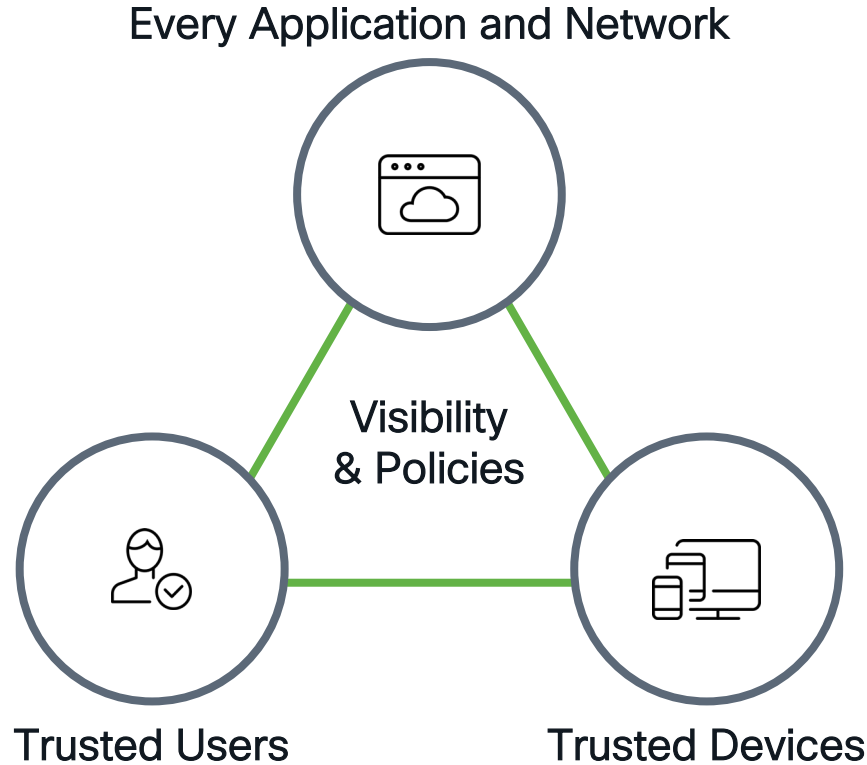


Cloud
Infrastructure



Hybrid
Infrastructure

Delivering Zero Trust





Threat Centric Network Access Control (TC-NAC)

CISCO *Live!*



Reduce Vulnerabilities, contain Threats

Problem

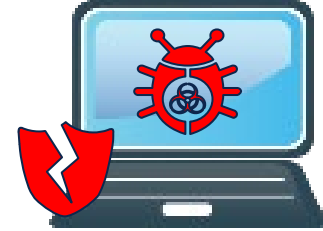
1 Malware Infection



2 Malware scans for
Vulnerable endpoints

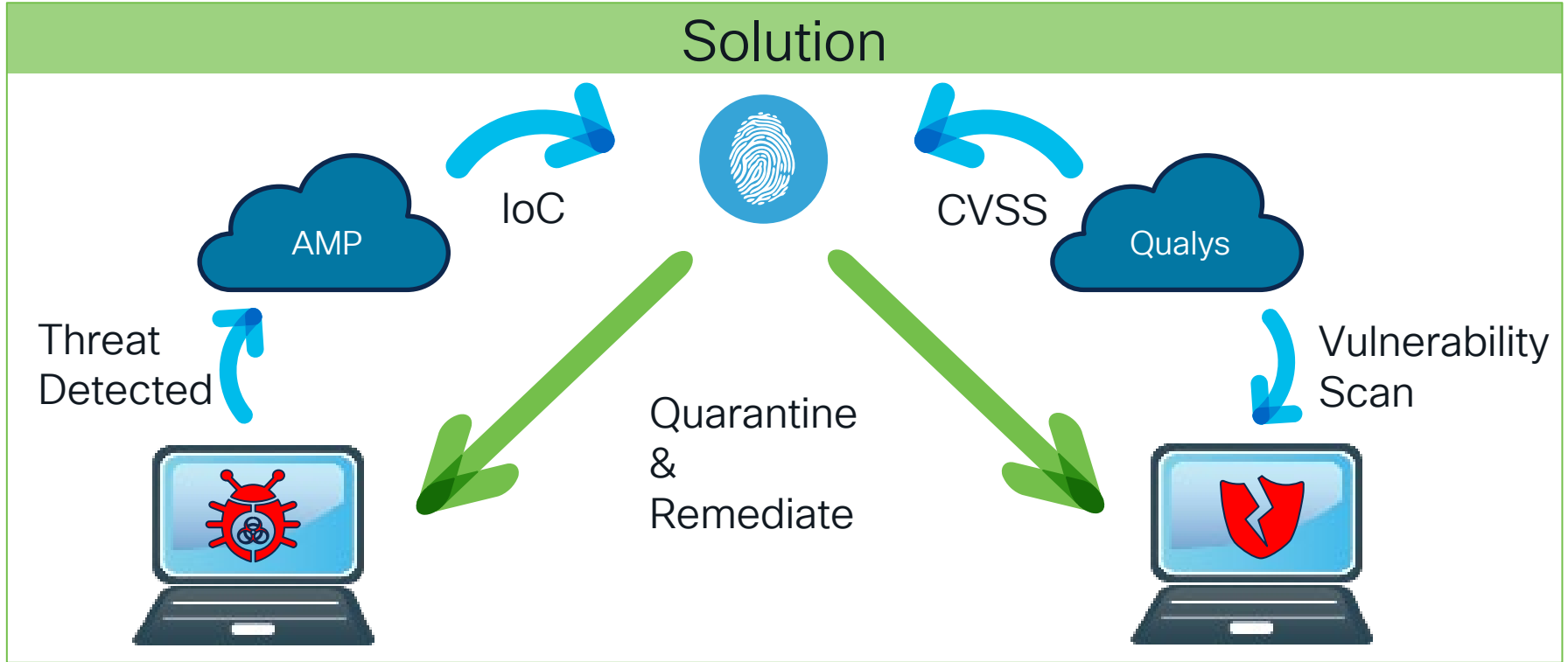


4 Infection spread



3 Vulnerability detected

Reduce Vulnerabilities, contain Threats



Threat Centric NAC

- Vulnerability assessment
- Detected Malware



TC-NAC vendor of your choice

- Detected Malware
- Vulnerability Scores



Endpoints

Access
Policy
Decision

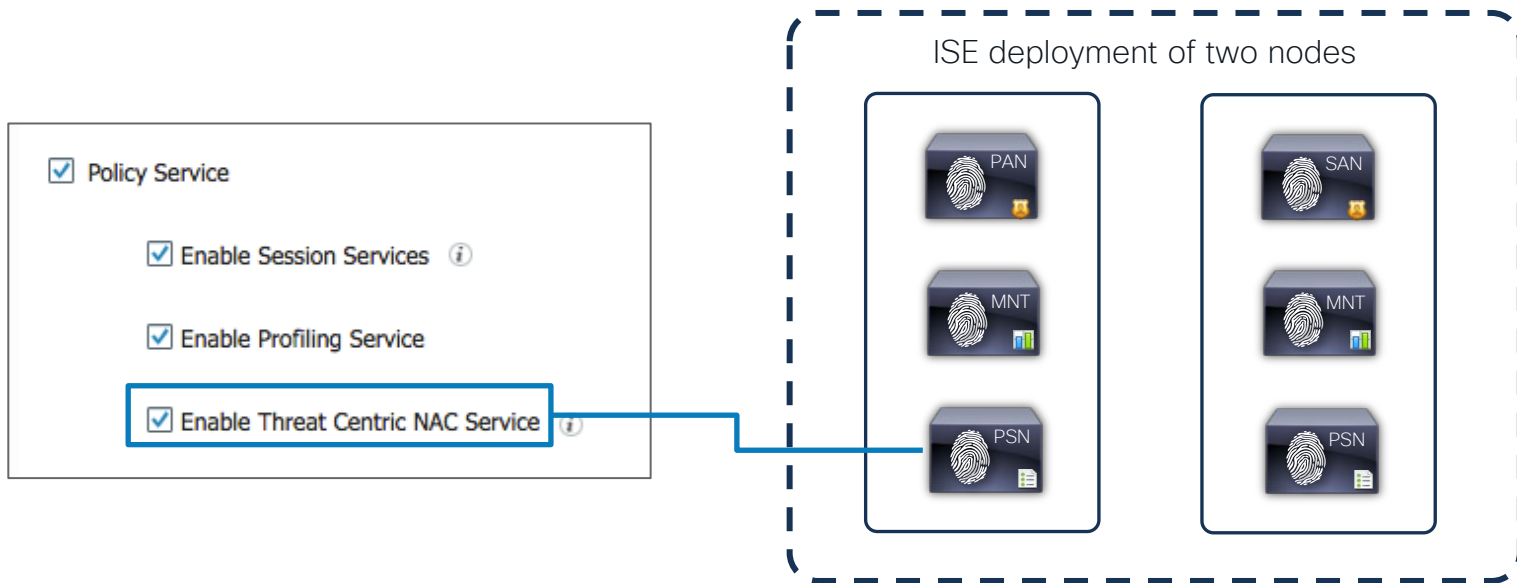


Cisco
ISE

Why ISE?



ISE has the knowledge of endpoints across the network. ISE can change the privilege and context of an endpoint dynamically, notifying the network and other applications of the change so that access to resources can be restricted



ISE TC-NAC configuration with AMP

Step 1: Create Instance



Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | PassiveID | Threat Centric NAC

Third Party Vendors

Vendor Instances > New

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

Vendor * AMP : THREAT

Instance Name * AMP_THREAT|

Cancel Save

ISE TC-NAC configuration with AMP

Step 2: Configure Instance



Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Third Party Vendors

Vendor Instances

0 Selected

Refresh Add Trash Edit Filter Settings

<input type="checkbox"/>	Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
<input type="checkbox"/>	QualysVA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active
<input type="checkbox"/>	AMP_THREAT	AMP	THREAT		Disconnected	Ready to configure

ISE TC-NAC configuration with AMP

Step 3: Choose Cloud



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes tabs for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The 'Administration' tab is selected, and the 'Threat Centric NAC' sub-tab is active. The main content area is titled 'Third Party Vendors' and shows a breadcrumb path 'Vendor Instances > AMP'. Below this, there is a 'Cloud' section with a dropdown menu currently set to 'US Cloud'. A text prompt asks, 'Which public cloud would you like to connect to'. At the bottom of the form are 'Cancel' and 'Next' buttons.

ISE TC-NAC configuration with AMP

Step 4: Login to AMP




The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes tabs for Home, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. Under the Administration tab, there are sub-tabs for System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, PassiveID, and Threat Centric NAC (selected). The main content area is titled 'Third Party Vendors' and shows a list of 'Vendor Instances' with one instance named 'AMP'. The 'AMP' instance is expanded, showing a 'root' section with a 'SAS External URL' field. The URL is: https://api.amp.sourcefire.com/authorize?client_id=mbga79xvh3tq7aafywt7yh9sb90ktz5p&response_type=code&redirect_uri=https://ise21-3ek.example.com/admin/irfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize&scope=recv_events. A 'Cancel' button is located at the bottom right of the configuration area.

ISE TC-NAC configuration with AMP

Step 5: Allow event streaming



 AMP for Endpoints Premier

Dashboard

Analysis

Outbreak Control

Management

Accounts

Search

Q

Zaid Al-Kurdi

< Authorize AMP Adaptor b6980603-505b-4ec6-8ba3-a209cffd5620

The AMP Adaptor b6980603-505b-4ec6-8ba3-a209cffd5620 (IRF) with URL of https://10.48.26.244/admin/irfapi/b6980603-505b-4ec6-8ba3-a209cffd5620/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

Deny

Allow

Applications external to AMP for Endpoints, such as Cisco's Firepower Management Center, can be authorized to access your business' data.

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

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

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

Search Groups

Audit

Domain Controller

Protect

Server

Triage

cisco Live!

#CiscoLive

BRKSEC-2108

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

20

ISE TC-NAC configuration with AMP

Step 6: Verify Status



Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Third Party Vendors

Vendor Instances

0 Selected

Refresh + Add Trash Edit Filter Settings

<input type="checkbox"/>	Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
<input type="checkbox"/>	AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
<input type="checkbox"/>	QUALYS_VA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active

Partner of your choice – what is supported

Vulnerability Assessment



CISCO *Live!*

Threat Detection



Threat Centric NAC with Secure Endpoint – Simplified Flow



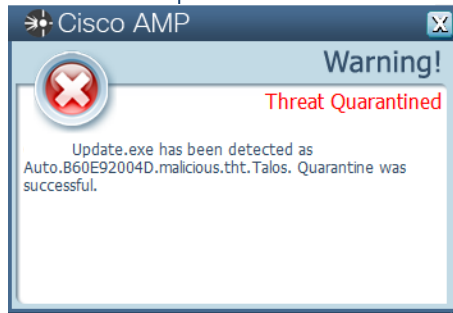
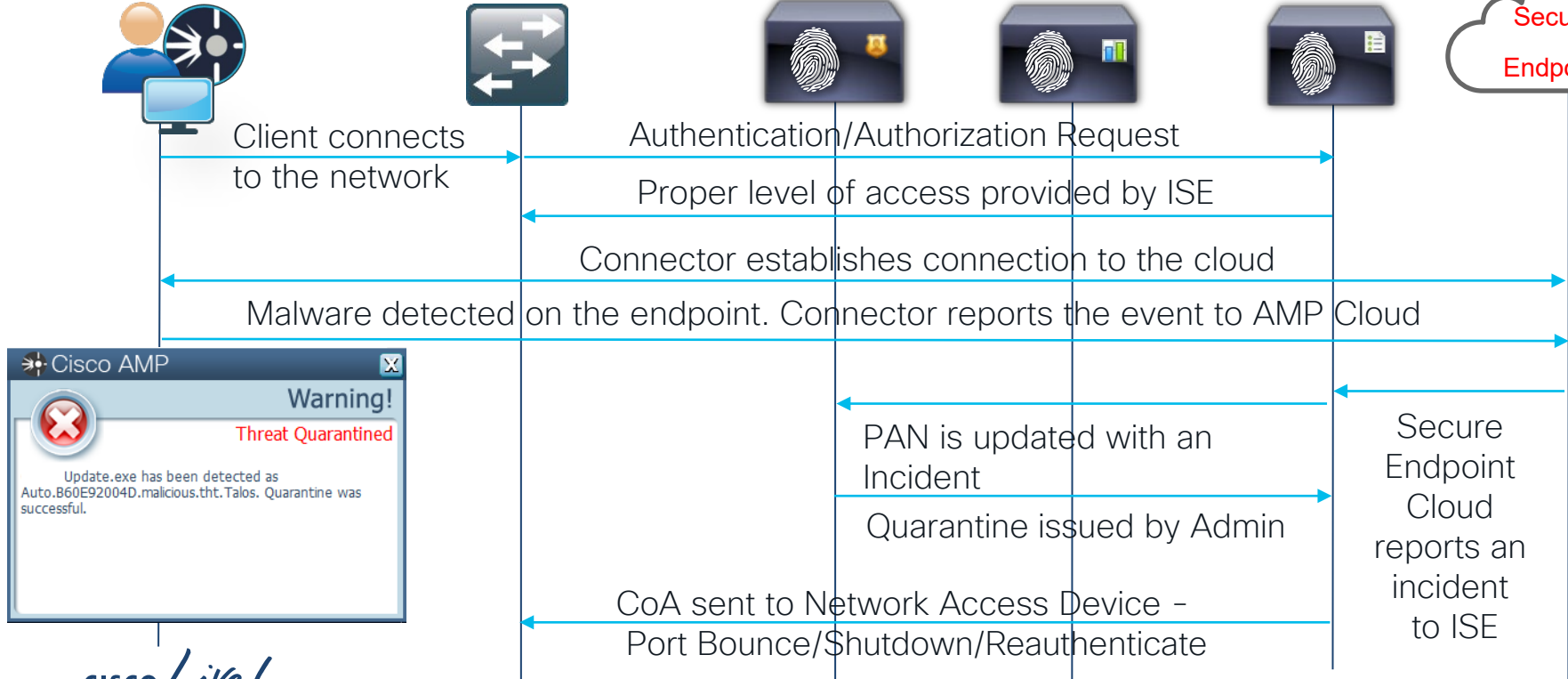
Endpoint with Secure Endpoint Connector

Network Access Device

Admin Node

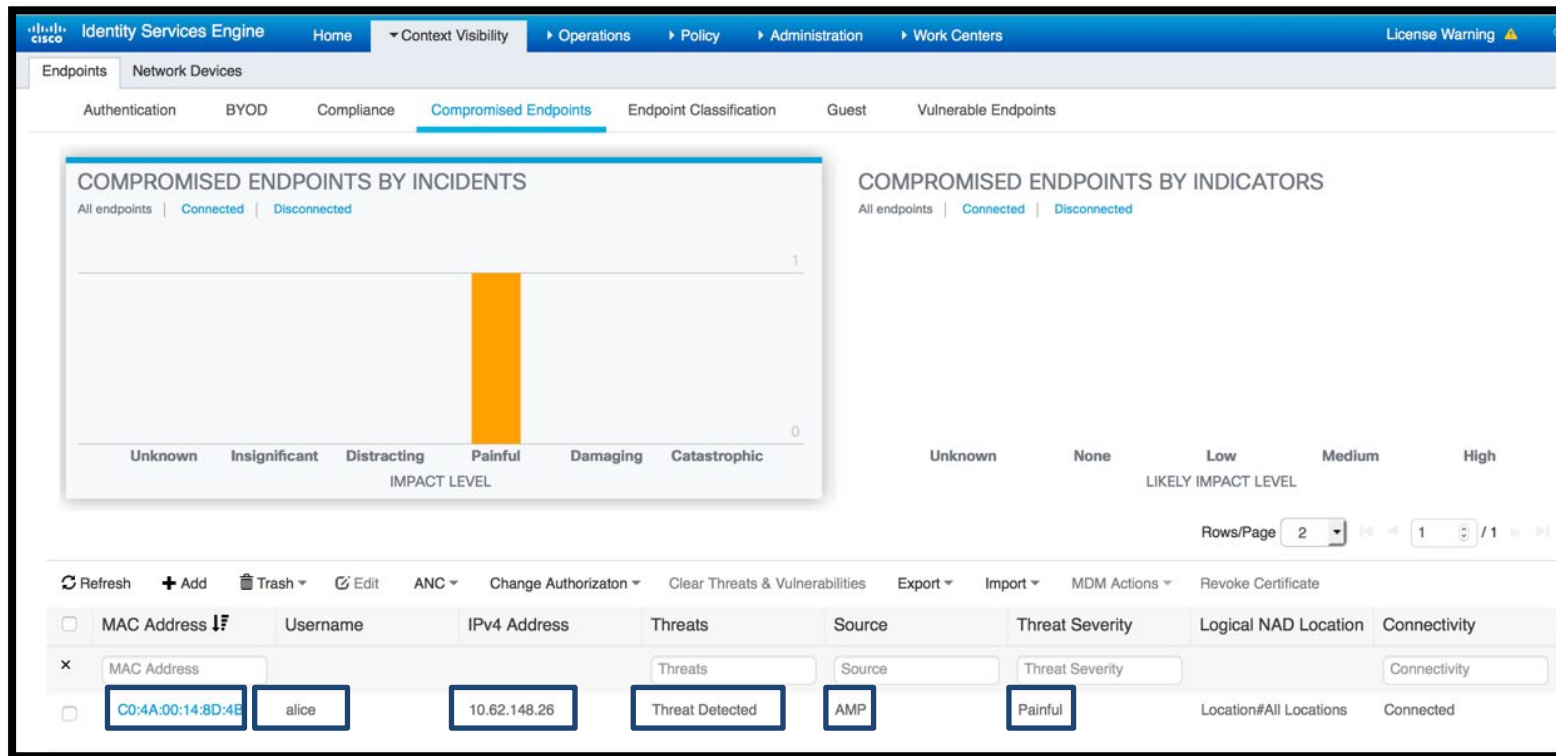
MNT Node

PSN with TC-NAC



CISCO Live!

Threat Centric NAC with AMP – Visibility



Mac Address
Username
IP Address
Threat Source
Threat Severity

Threat Centric Network Access Control Demo

Threat Centric Application Access Control

CISCO *Live!*

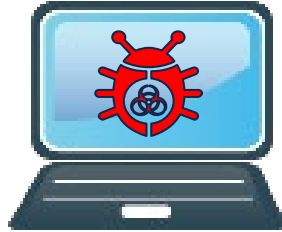


Cisco Secure Endpoint and Duo

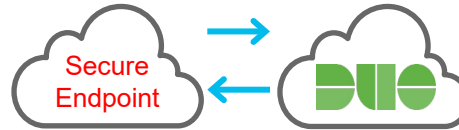
This integration allows for Threat Detection & Automated Policy Enforcement for protected Applications



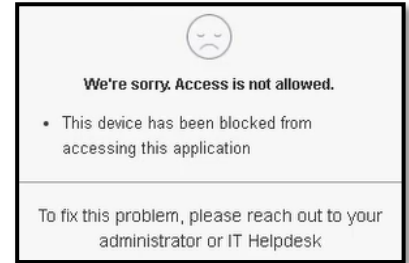
User access protected application from a trusted device



Connector on the machine detects a Malware



Secure Endpoint notifies Duo about the infected device



Duo blocks that device from accessing apps

Secure Endpoint and Duo User Interface

☐ ▼ Ghandi-Windows in group Protect

Definitions Up To Date

Hostname	Ghandi-Windows	Group	Protect
Operating System	Windows 10 Pro	Policy	Protect
Connector Version	7.2.13.11865	Internal IP	10.48.26.86, 192.168.10.89
Install Date	2020-09-14 21:22:26 UTC	External IP	
Connector GUID	dd785643-855d-4a04-9b45-349f630f8171	Last Seen	
Definition Version	TETRA 32 bit (daily version: 112107)	Definitions Last Updated	
Update Server	tetra-defs.amp.cisco.com		
Processor ID	0fabfbff000306e7		

Secure Endpoint UI

OS

Windows

10.0.18362.1016 latest

Trusted Endpoint

Yes

Valid certificate collected

Certificate

SourceWindows Enterprise Asset Management Tool

Serial11001c2907aa947534474b54250000001c2907

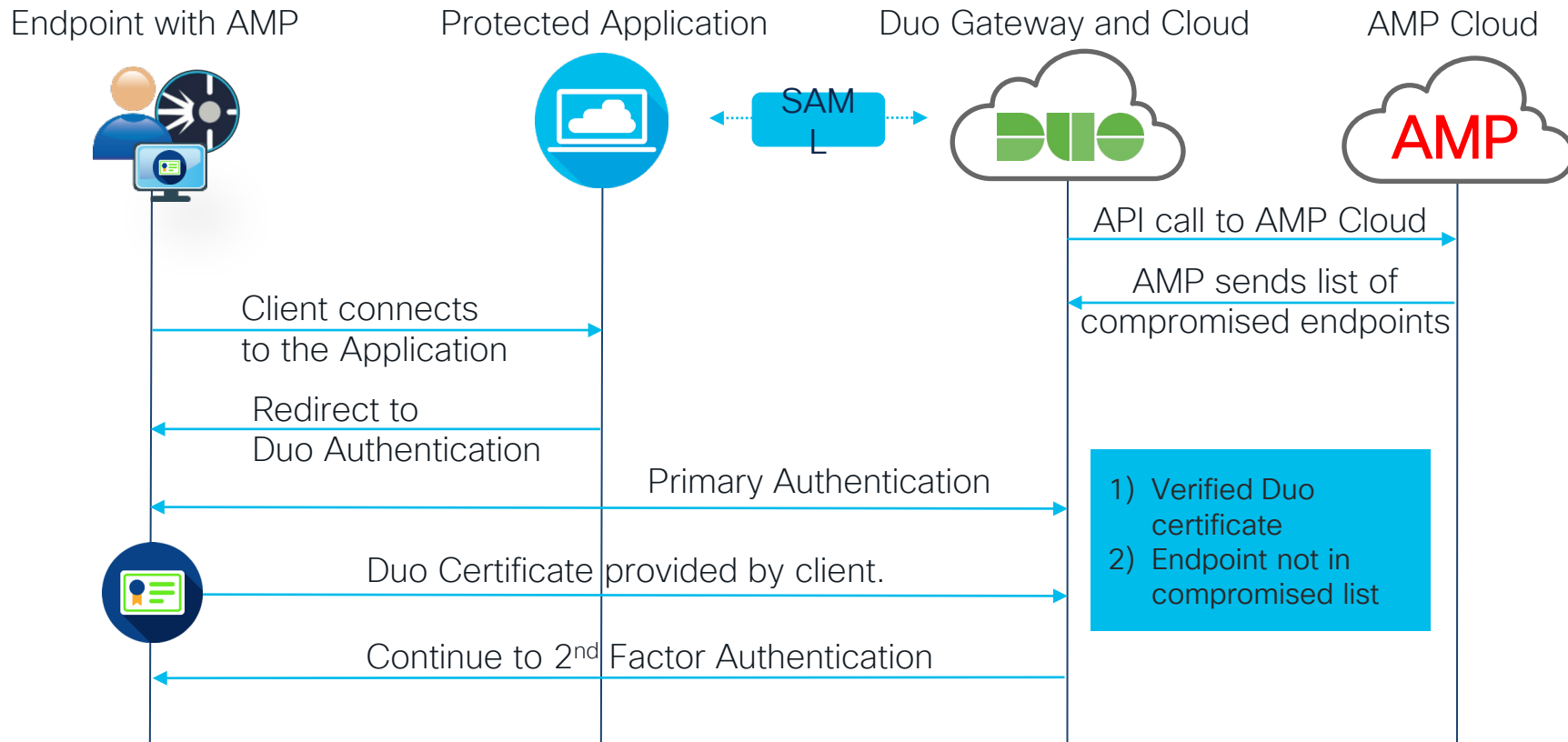
Device UserGHANDI-WINDOWS\cisco

Device Id0FABFBFF000306E7

ExpirationSep 14, 2021 9:12 PM UTC

Duo UI

AMP and Duo – Healthy Endpoint Flow



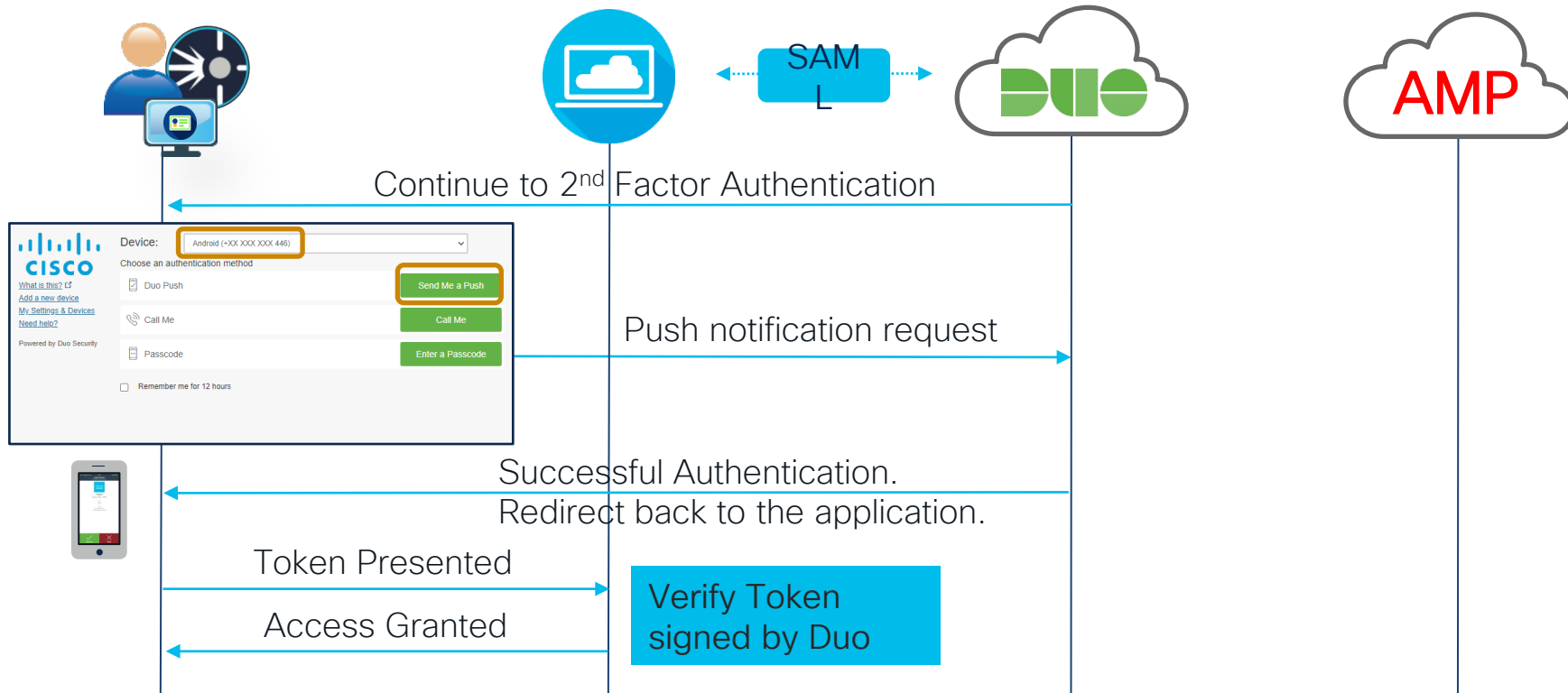
AMP and Duo – Healthy Endpoint Flow

Endpoint with AMP

Protected Application

Duo Gateway and Cloud

AMP Cloud



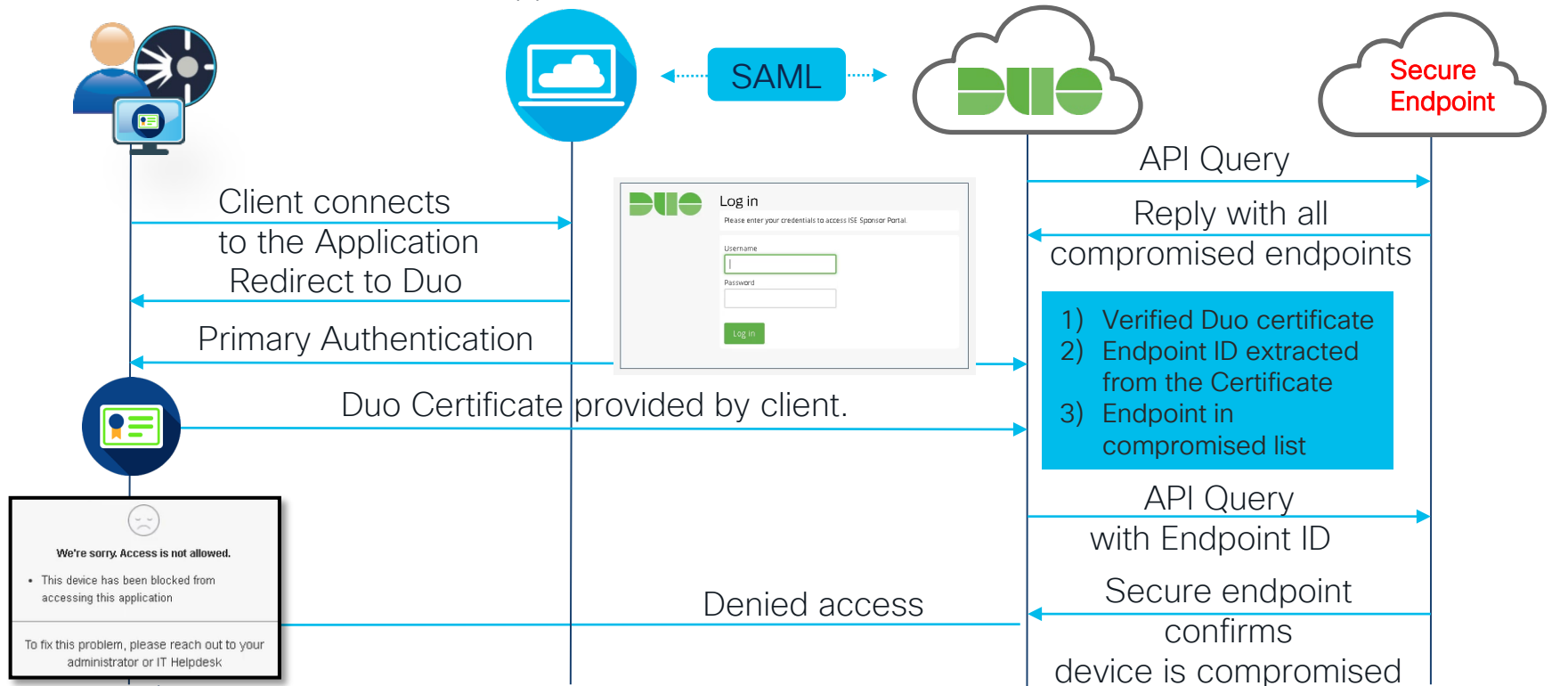
AMP and Duo – Compromised Endpoint Flow

Endpoint with connector
and certificate

Protected
Application

Duo Gateway
and Cloud

Secure Endpoint
Cloud



Configuration

- 1) Gather AMP credentials from your AMP admin panel.
- 2) Enter AMP credentials in Duo admin panel.
- 3) Set policies in Duo to protect against risky devices.

Search for users, groups, applications, or devices

Duo First | ID: DAZ2JSJ2RBL9AHLAGRNL | Lee Brenner

Management tools integration added successfully.

[Dashboard](#) > [Trusted Endpoints Configuration](#) > AMP for Endpoints Integration 1

AMP for Endpoints Integration 1 [Rename](#)

Integration is disabled [Change](#) [Remove Integration](#)

This integration is currently disabled.

This integration is disabled by default. Once you complete all instructions, you can enable it here.

Part 1: Generate AMP Credentials

1. [Login to the AMP console.](#)
2. Navigate to "Accounts → API Credentials".
3. Click "New API Credential".
4. Give the credential a name and make it read-only.
5. Click "Create".
6. Copy the **Client ID**, **API Key**, and **Hostname** and return to this screen.

Part 2: Enter AMP Credentials

Client ID

API Key

Hostname

Part 3: Enable Integration

1. Click "Test Integration" to ensure everything is working.

Not Tested [Test Integration](#)

2. After a successful test, [enable](#) the integration.
3. [Update](#) the Trusted Endpoints rule in your Global or custom policy.

Edit Policy

You're editing the Global Policy which is used by all applications. This can be overridden with custom policies. [Revert to default](#)

Policy Name

Global Policy

Users

- ✓ New User Policy
- ✓ Group Access Policy
- ✓ User Location

Devices

- ✓ Trusted Endpoints
- ✓ Remembered Devices
- ✓ Operating Systems
- ✓ Browsers
- ✓ ...

Trusted Endpoints

A Trusted Endpoint is an endpoint that exists in a management system such as your EAM or MDM. It can be matched to your management system using Duo certificates or information provided by Duo Mobile.



Allow all endpoints

Endpoints will be checked for trustworthiness to aid reporting, but un-trusted endpoints will be allowed.



Require endpoints to be trusted

Only Trusted Endpoints will be able to access browser-based applications.



Allow AMP for Endpoints to block compromised endpoints

Endpoints that AMP deems to be compromised will be block from accessing browser-based applications.

Note: This option only applies to trusted endpoints.

Configure AMP policy in Duo to instantly block risky devices

Threat Centric Application Access Control Demo

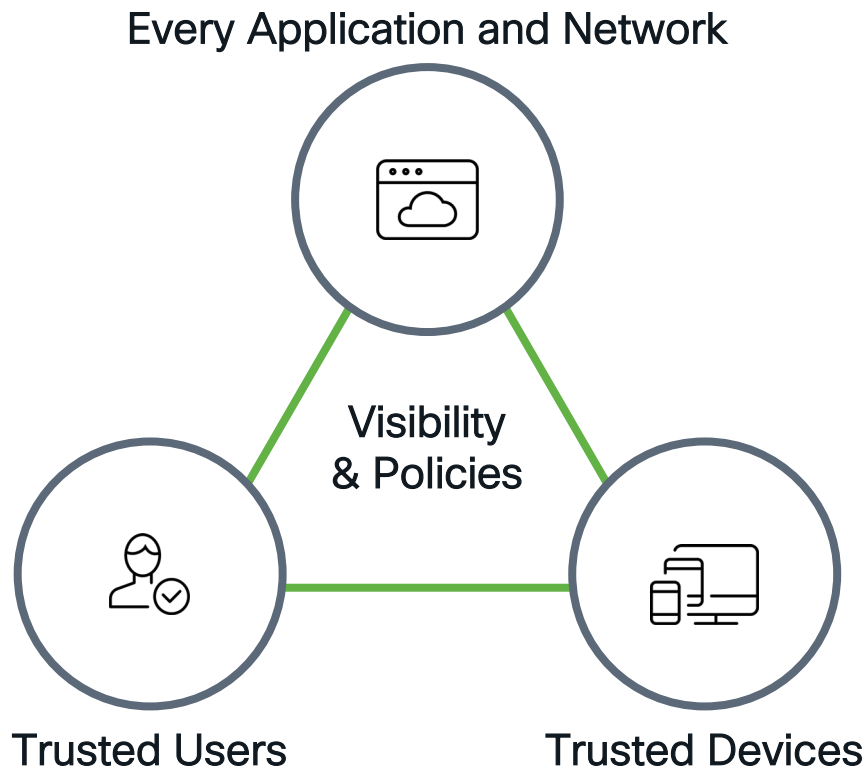
Key Takeaways

- Shifting IT Landscape means new challenges.
- Secure Endpoints can enrich both ISE and Duo with threat information.
- ISE controls access to network resources.
- Duo controls access to applications.

Resources

- [ISE TC-NAC Configuration Example](#)
- [ISE 2.7 Admin Guide Threat Containment](#)
- [Duo Trusted Endpoints](#)
- [Trusted Endpoints Certificate Installation](#)
- [Duo and AMP4E Integration](#)

Delivering Zero Trust





The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive



The background is a vibrant, abstract composition of numerous colorful rays and shapes radiating from a central point. The colors include dark blue, light blue, green, yellow, orange, and red. Some shapes are solid, while others have white circular cutouts. The overall effect is dynamic and energetic.

TURN IT UP

CISCO *Live!*

#CiscoLive