



You make **possible**



Duo+Cisco: All Integration Together!

Better together

Ruoting Sun, Head Tech Partnerships and International Expansion
Leya Leykider, Tech Partnership Manager

DEVLIT-4041

CISCO *Live!*

Barcelona | January 27-31, 2020



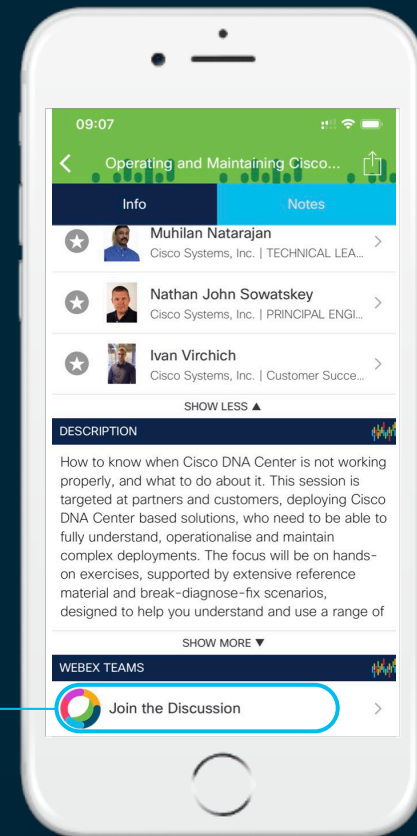
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events Mobile App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space



Agenda

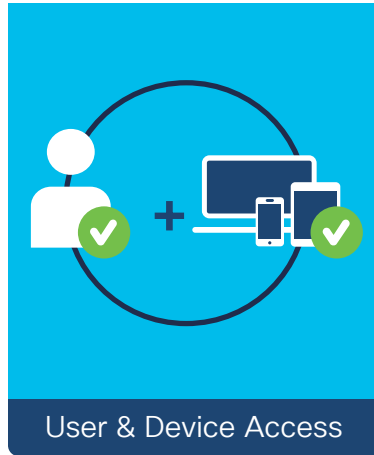
- Introduction
- Quick re-cap: Cisco Zero Trust Strategy
- Duo + Cisco Integration Strategy
- Currently Supported Integrations
- Demo: Duo + AMP4E
- Conclusion

Cisco's Zero Trust Framework

It is all about access: Secure access for the workforce, workloads, and workplace

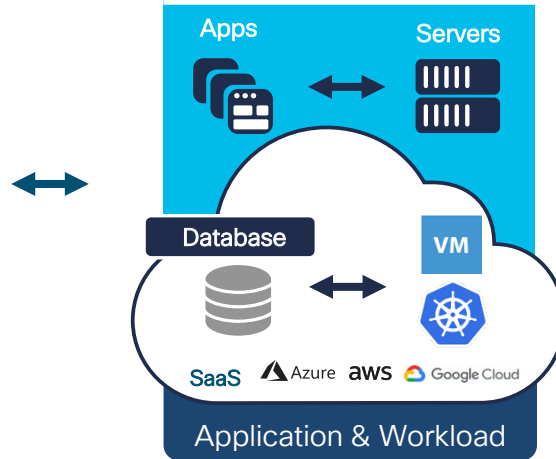
Workforce

All Corp IT



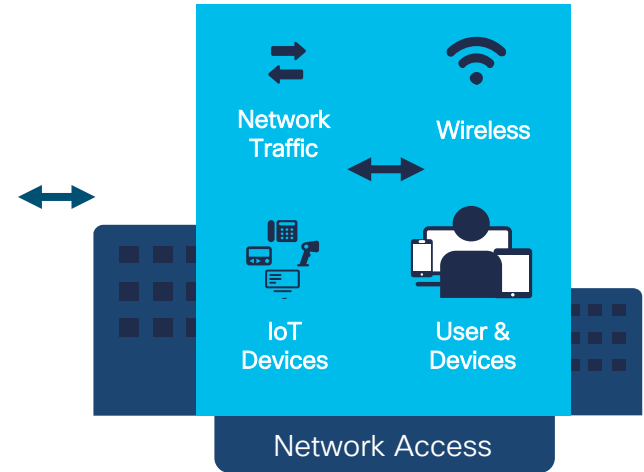
Workload

Data Center



Workplace

Corporate Network



Zero Trust for Workforce

Duo For Workforce Access Management

Secure Access to **all user**
connecting to **any application** from
any device

Workforce

How to Verify Trust



Verify users' identities

WITH

Multi-factor authentication (MFA)

Gain device visibility & establish trust

WITH

Endpoint health & management status

Enforce access policies for every app

WITH

Adaptive & role-based access controls

Duo + Cisco Integration Strategy

Integration Across Zero Trust Products

- Sharing endpoint posture data (Duo, AMP4E, ISE, AnyConnect)
- Sharing user identity data across all products
- Share event information (ex: failed access request)
- Long-Term: Share policy objects

Duo + Cisco: Current Supported Integration



Duo + AnyConnect VPN

The Majority of Networking is 'On-Premises'!

- Secure the **workplace**
- The industry leading VPN client
- Connects to ASA and Firepower Threat Defense
- Integrations with Duo, Cisco ISE and Umbrella



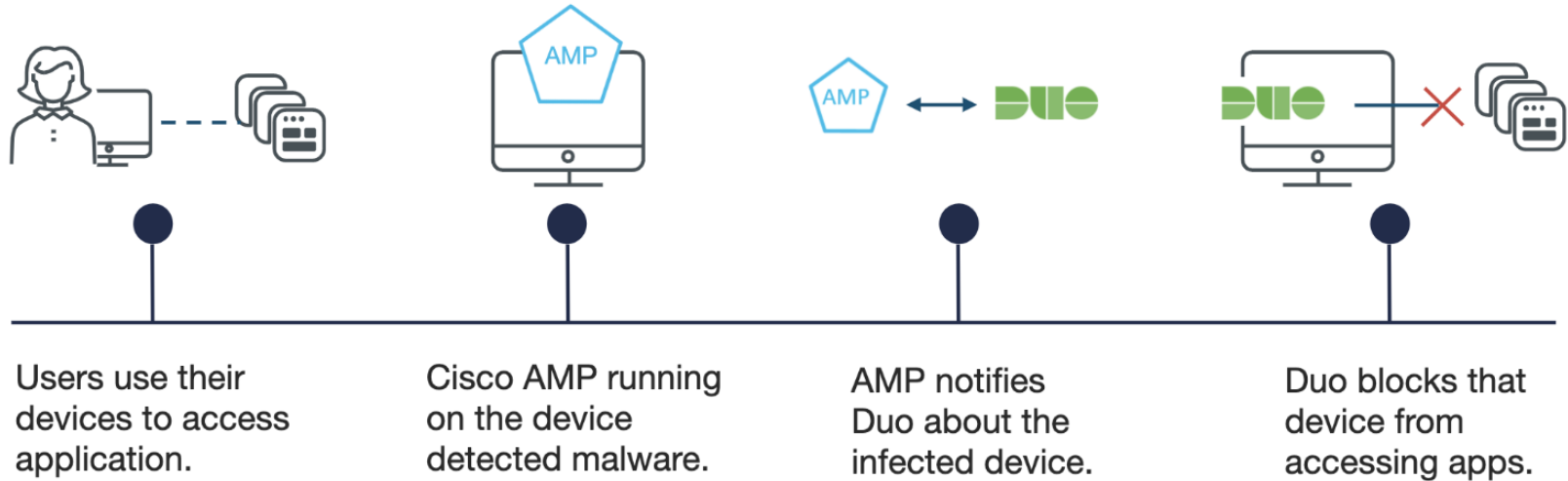
Secure the **workforce**

- Users accessing the network
- Verify the identity of the user
- Check the hygiene of devices
- Check for device trust



Duo + AMP4E

- It is all about access: Secure access for the workforce, workloads, and workplace





Demo: Duo + AMP4E

<https://demo.duo.com/cisco-amp>

What Next?

Upcoming integration

Duo + Meraki SM integration: April 2020

Your opinion matters!

- Consistent access policies between network and application access.
- Duo as access policy manager for wired, wireless, VPN access and SD WAN – light weight NAC.

You + Cisco: Better Together!

Need your suggestions on integrations you would like to see!

- <Email id>

Secure The Workforce + Workplace



AnyConnect VPN

Connects to ASA & FTD Firewalls

LDAPS

RADIUS

SAML



ASA or FTD Firewalls

IPsec VPN

SSL VPN

RADIUS

RADIUS / LDAPS

Verify user identities	Yes	Yes	Yes	Yes	Yes
Check device hygiene	No	No	Yes	No	No
Check device trust	No	No	Yes	No	No



Duo + Meraki



Meraki Client VPN

Secure access to the workplace

RADIUS

Meraki Admin Panel

Meraki SSO logins

SAML

Verify user identities	Yes	Admins
Check device hygiene	No	Yes
Check device trust	No	Yes



Duo + ISE

Secure The Workforce + Workplace



Cisco ISE

Secure access to the workplace


RADIUS

Verify user identities Regular user Device Admin (TACACS+)	Yes
Check device hygiene	No
Check device trust	No




1. SAML based integration with Umbrella admin console

CISCO *Live!*



Dashboard
Device Insight
Policies
Applications
Protect an Application
Single Sign-On
Users
Groups
Endpoints
2FA Devices
Administrators
Trusted Endpoints Configuration
Reports
Phishing
Settings
Support
Need help? [Email Support](#) or call 1-855-386-2884.
[Support Tickets](#)
Account ID
2969-9160-77
Deployment ID
DUOALPHA
Helpful Links
[Documentation](#)
[User Guide](#)
[Knowledge Base](#)
[Community](#)

Search for users, groups, applications, or devices

Batwave Cloud
ID: 2969-9160-77
canderson@duo.c

Application modified successfully.

Dashboard > Applications > Cisco Umbrella

Cisco Umbrella

Authentication Log
Remove Application

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<input type="text" value="https://sso-b10552ad.test.sso.duosecurity.com/saml2/sp/DIUGEV7301LN78LORG0X/met"/>	copy
Single Sign-On URL	<input type="text" value="https://sso-b10552ad.test.sso.duosecurity.com/saml2/sp/DIUGEV7301LN78LORG0X/sso"/>	copy
Single Log-Out URL	<input type="text" value="https://sso-b10552ad.test.sso.duosecurity.com/saml2/sp/DIUGEV7301LN78LORG0X/slo"/>	copy
Metadata URL	<input type="text" value="https://sso-b10552ad.test.sso.duosecurity.com/saml2/sp/DIUGEV7301LN78LORG0X/met"/>	copy

Certificate Fingerprints

SHA - 1 Fingerprint	<input type="text" value="0E:CF:DA:F7:BA:D5:C1:AF:FC:D8:DC:5C:20:CC:58:5B:63:4C:1F:61"/>	copy
SHA - 256 Fingerprint	<input type="text" value="D6:A3:FD:AF:BE:15:4E:44:B9:39:E2:B5:69:69:E2:3E:47:94:C5:95:D4:A0:CA:81:04:9F:1A:C"/>	copy

Downloads

Certificate	Download Certificate
SAML Metadata	Download XML

Service Provider

Service provider name *

The name of the service provider being configured.

Entity ID *

The unique identifier of the service provider.

Assertion Consumer Service *

The service provider endpoint that receives and processes SAML assertions.

Single Logout URL

Optional: The service provider endpoint that receives and processes SAML logout requests.

Complete your online session survey



- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education



Demos in the
Cisco Showcase



Walk-In Labs



Meet the Engineer
1:1 meetings



Related sessions



Thank you





You make **possible**