

The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, radiating from a bright white center on the right side.

CISCO *Live!*

Let's go

#CiscoLive



The bridge to possible

Deploying Cisco and Microsoft Zero Trust

Kevin Patrick – Technical Solutions Architect
LinkedIn @thatshouldbefine
BRKSEC-2105

CISCO *Live!*

#CiscoLive



Cisco Webex App

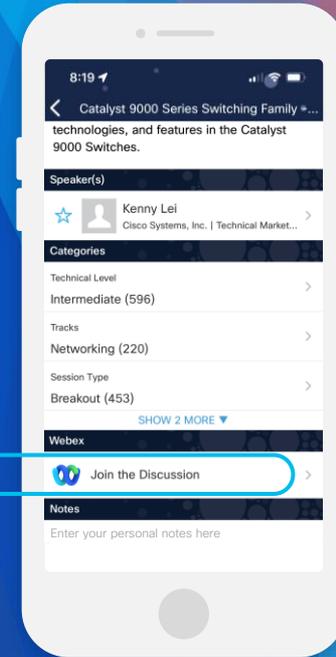
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 9, 2023.



<https://cislive.ciscoevents.com/cislivebot/#BRKSEC-2105>

Agenda

- All of the trusts that are Zero
- Practical Examples
- Duo and Microsoft
- Umbrella and Microsoft
- Enabling Off Prem Access
- Reference Architectures

Introduction



- 4 Years with Cisco
- 14 Years in Security
- Technical Solutions Architect – Incubation SaaS
- Napa Tour Guide



All Of The Trusts That Are Zero



Microsoft and Cisco Zero Trust Principles

Microsoft

- Verify explicitly
- Use least privilege access
- Assume breach

Cisco

- Always verify
- Enforce least privilege
- Never assume trust

Five Pillars Of Zero Trust

1. Identity
2. Devices
3. Network
4. Applications & Workloads
5. Data

[US Cybersecurity and Infrastructure Security Agency \(CISA\) Zero Trust Pillars](#)

Microsoft and Cisco Strengths

Microsoft

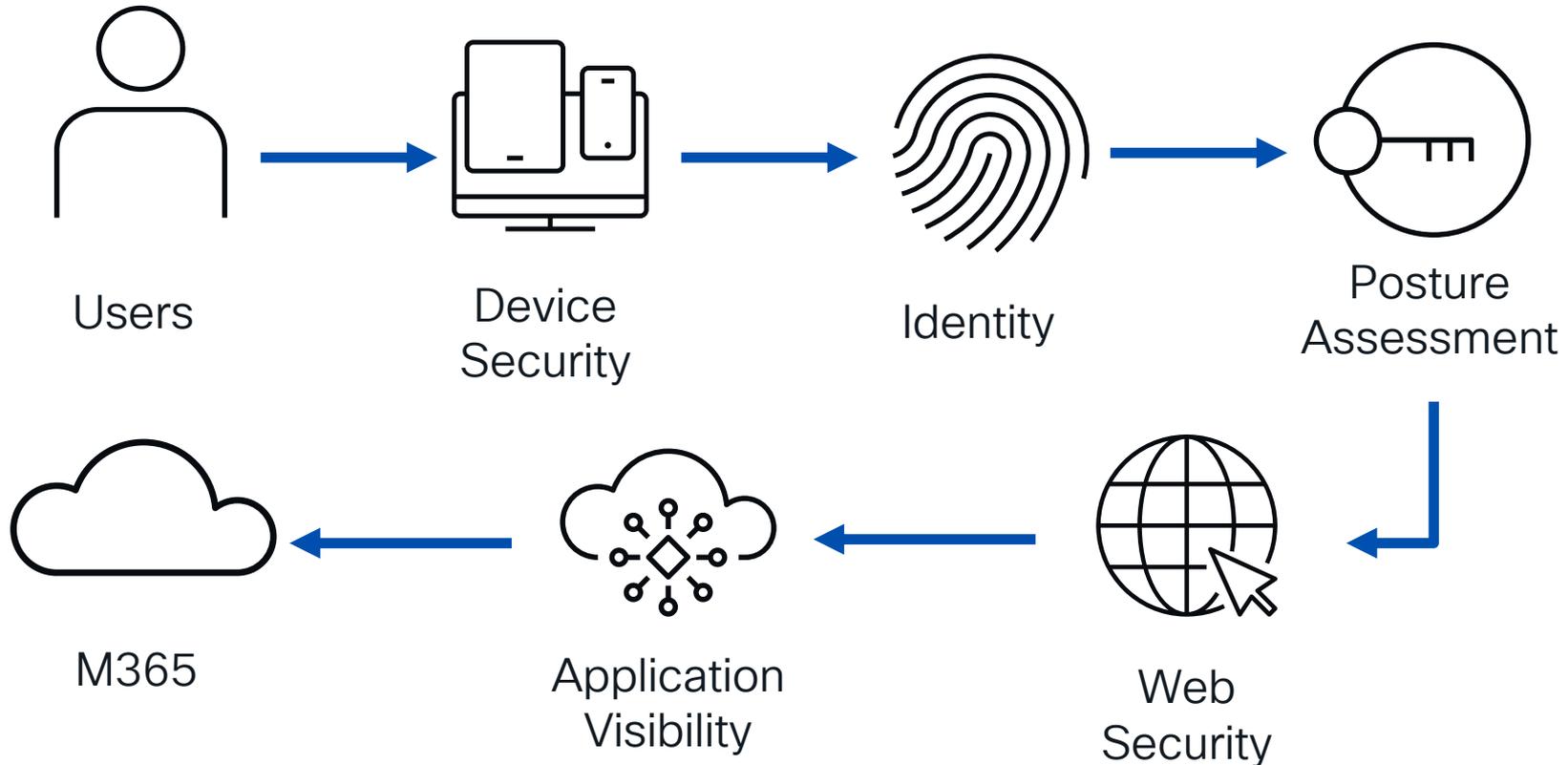
- **Identity Management**
 - Identity Governance
 - Password Abuse
 - Cloud and On Premise
- **Endpoint Protection**
 - Windows Defender
 - Intune
 - Group Policy

Cisco

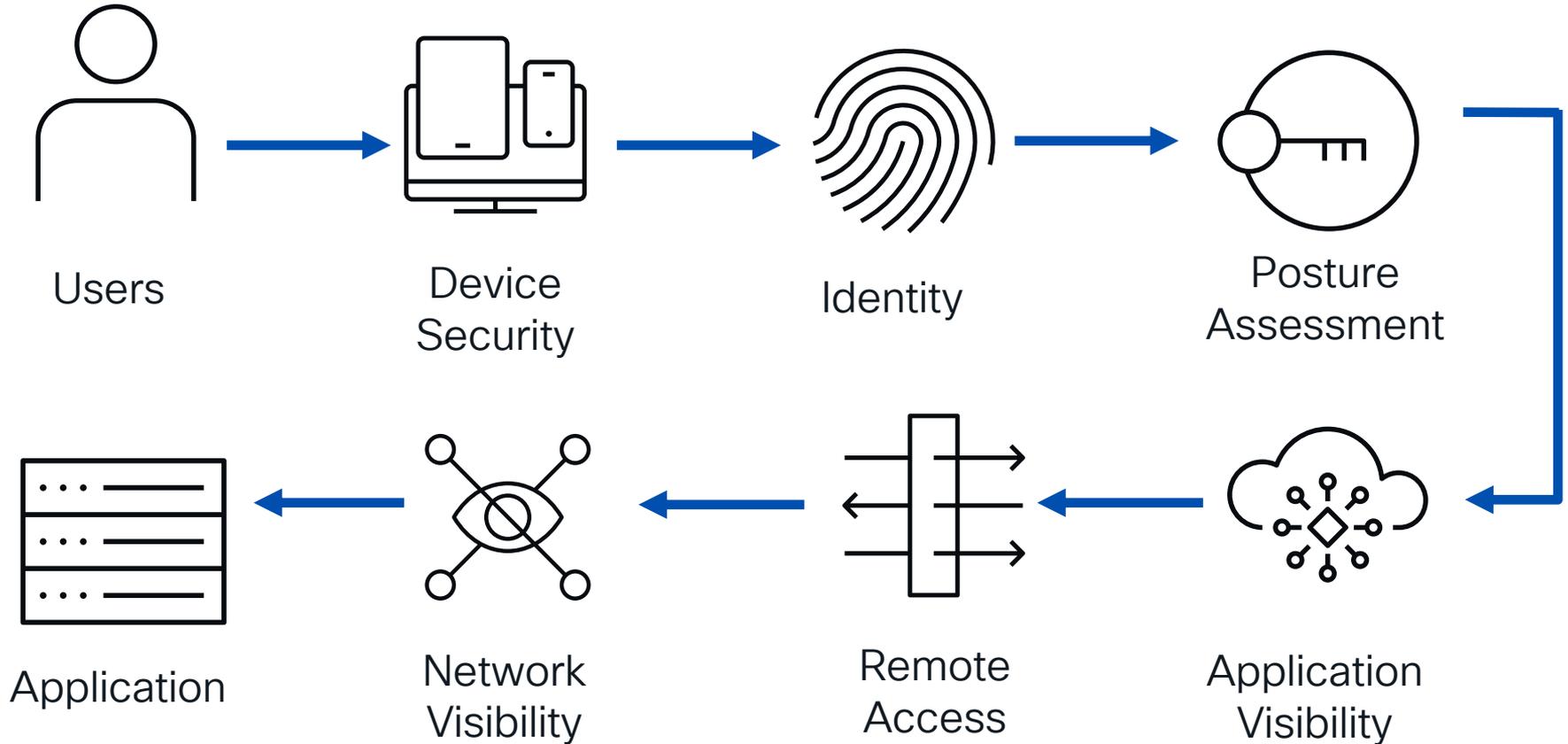
- **Flexible**
 - Simplify zero trust policy
 - Non-Microsoft Applications
 - Multi Platform
- **Protecting the Network**
 - Content Filtering
 - Segmentation
 - Multi Cloud

Practical Examples

Hybrid Employee Accessing M365



Remote User Accessing On Prem

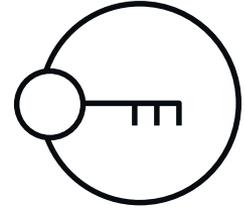


Identity



- **Identity Store**
 - Active Directory
 - Azure Active Directory
- **MFA**
 - Secure Access by Duo
- **Device Identity**
 - Duo Trusted Endpoint

Posture Assessment



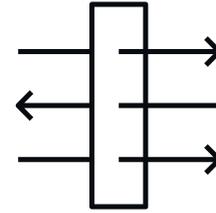
- **Device Management**
 - Duo Device Health Application
 - Microsoft Intune
- **Posture Verification**
 - Duo Device Health Application

Web Security



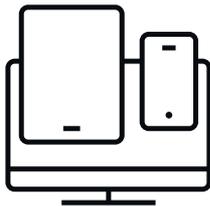
- **M365 Tenant Control**
 - Cisco Umbrella
- **Malicious Websites/Redirect Links**
 - Microsoft Defender/ Cisco Umbrella

Remote Access



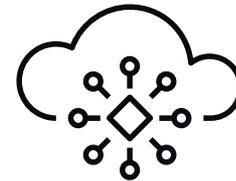
- **VPN Access**
 - Cisco Secure Client w/ Anyconnect
- **VPN-less Access**
 - Duo Network Gateway

Device Security



- **Endpoint Detection and Response**
 - Windows Defender
 - Cisco Secure
- **Firewall**
 - OS Firewall
- **Web Security**
 - Cisco Umbrella
- **Encryption**
 - OS Encryption

Application Visibility



- **Least Privilege Access**
 - Conditional Access
 - Identity Governance & Administration
- **Federation**
 - Azure Active Directory

Duo + Microsoft

Environment Assumptions

1. Configured Active Directory
2. Azure Active Directory Sync (AAD Connect)
3. Devices Managed in Intune
4. Administrator access to Duo

Configuration Roadmap

Step 1 Identity

Step 2 Device Trust

Step 3 Policy Configuration

Step 1

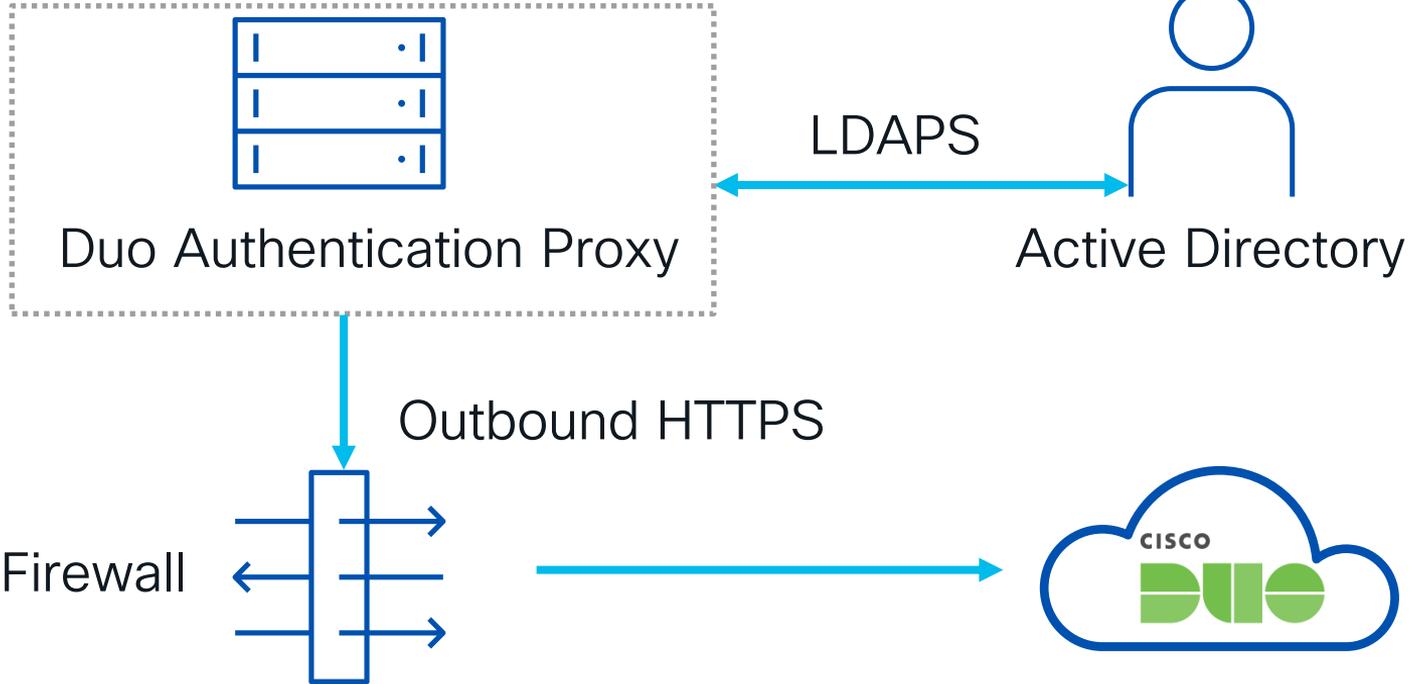
Identity

1. Active Directory Sync
2. Azure Active Directory Sync
3. Protecting Azure
4. Conditional Access Policy
5. Duo Enrollment

On-Prem Active Directory

On Prem Active Directory

On-premises Windows or Linux



On Prem Active Directory

1. Users > Directory Sync > Add New Sync > Active Directory
2. Add New Connection
3. Download the pre-configured file

Configuration metadata

1. To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#) 
2. Configure your Authentication Proxy. Update the `ik`, `sk`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).

On Prem Active Directory

1. Install Duo Authentication Proxy on Windows Server
2. Place the pre-configured file in C:\Program Files\Duo Security Authentication Proxy\conf
3. Add domain controller information

```
authproxy - Notepad
File Edit Format View Help
[cloud]
ikey=DIIFYXXXXXXXXXXXXX
skey=XXXXXXXXXXXXX
api_host=api-de93ff2b.duosecurity.com
```

|

On Prem Active Directory

1. Select groups to sync for users that do not sync into Azure
2. Create any aliases needed
3. Save and Sync Now

Groups

These groups and their users will be imported from your on-premises Active Directory

Synced Attributes

Username *

samaccountname

This attribute is in use and may not be changed.

Username aliases

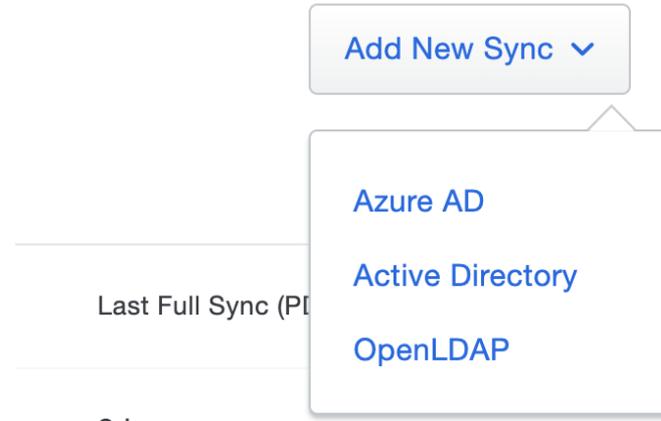
Username alias 1

mail

Azure Active Directory

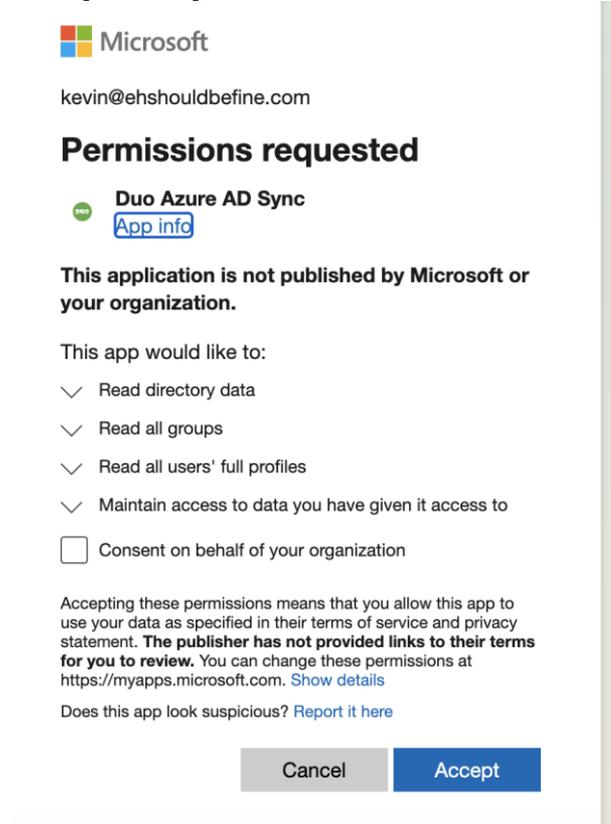
Azure Directory Sync

1. Create a temporary global administrator if possible
2. Add new sync for Azure AD under Users in Duo
3. Login with a global administrator account



Azure Directory Sync

1. Grant permissions
2. Global administrator access role can be changed to normal user



The screenshot shows a Microsoft app permissions dialog. At the top is the Microsoft logo and the email kevin@ehshouldbefine.com. The title is 'Permissions requested'. Below that is the app name 'Duo Azure AD Sync' with a link to 'App info'. A warning message states: 'This application is not published by Microsoft or your organization.' Underneath, it says 'This app would like to:' followed by a list of permissions: 'Read directory data', 'Read all groups', 'Read all users' full profiles', and 'Maintain access to data you have given it access to'. There is an unchecked checkbox for 'Consent on behalf of your organization'. A paragraph explains that accepting these permissions allows the app to use user data as specified in its terms of service and privacy statement, and notes that the publisher has not provided links to their terms for review. It provides a link to 'https://myapps.microsoft.com' and a 'Show details' link. At the bottom, it asks 'Does this app look suspicious?' with a 'Report it here' link. Two buttons are at the bottom right: 'Cancel' and 'Accept'.

Microsoft
kevin@ehshouldbefine.com

Permissions requested

Duo Azure AD Sync
[App info](#)

This application is not published by Microsoft or your organization.

This app would like to:

- ✓ Read directory data
- ✓ Read all groups
- ✓ Read all users' full profiles
- ✓ Maintain access to data you have given it access to

Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel Accept

Azure Directory Sync

1. Select Azure groups to sync
2. Do NOT select normalize
3. Create aliases
4. Sync Now

Synced Attributes

Username *

userPrincipalName

Default: userPrincipalName

This attribute may not be changed once the sync imports users into Duo. Username values must be unique.

Normalize usernames

Normalize usernames before importing them

"username@example.com" is imported as "username"

Username aliases

Username alias 1



onpremisesamaccountname

Protecting Azure

Protecting Azure

1. In Duo Admin Panel select applications
2. Search for Azure and select Protect next to Microsoft Azure Active Directory

[Dashboard](#) > [Applications](#) > Protect an Application

Protect an Application

Application	Protection Type		
 Microsoft 365	2FA with SSO hosted by Duo (Single Sign-On)	Documentation 	<button>Protect</button>
 Microsoft Azure Active Directory	2FA	Documentation 	<button>Protect</button>

Protecting Azure

1. Authorize and consent similarly to when we added Azure Active Directory for users
2. Create a second Azure Application and name it differently if you would like to have multiple Conditional Access policies for Duo
3. Remove Global Administrator rights

Microsoft Azure Active Directory -
MFA Only

Microsoft Azure Active Directory

Microsoft Azure Active Directory -
Trusted Only

Microsoft Azure Active Directory

Conditional Access Policy

Conditional Access Policy

1. In Azure Active Directory go to Security > Conditional Access >Custom Controls
2. In Duo Admin Panel go to Applications and the Azure Active Directory Application we created
3. Copy and paste the text into your favorite text editor
4. Rename ID and both Name fields to something unique. Like MFAOnly access and/or DuoTrustedEndpoints

```
{
  "AppId": " ",
  "ClientId": " ",
  "Controls": [
    {
      "ClaimsRequested": [
        {
          "Type": "DuoMfa",
          "Value": "MfaDone",
          "Values": null
        }
      ],
      "Id": "RequireDuoMfaTrusted",
      "Name": "RequireDuoMfaTrusted"
    }
  ],
  "DiscoveryUrl": "https://us.azureauth.duosecurity.com/.well-known/openid-configuration",
  "Name": "Duo Security - Trusted Only"
}
```

```
{
  "AppId": " ",
  "ClientId": " ",
  "Controls": [
    {
      "ClaimsRequested": [
        {
          "Type": "DuoMfa",
          "Value": "MfaDone",
          "Values": null
        }
      ],
      "Id": "RequireDuoMfaTrusted",
      "Name": "RequireDuoMfaTrusted"
    }
  ],
  "DiscoveryUrl": "https://us.azureauth.duosecurity.com/.well-known/openid-configuration",
  "Name": "Duo Security - Trusted Only"
}
```

Protecting Azure

1. Create a New Custom Control in Azure
2. Replace with the text that we edited previously
3. Repeat for second custom control

+ New custom control

🔍 Search controls.

Name

DuoTrustedEndpoint



MFAOnly



Protecting Azure

1. Under Policies in Conditional Access either create a new policy or modify an existing one
2. You can apply this policy to single users, groups, specific applications or all cloud apps.

Name ^{*}

Duo Trusted Endpoint

Assignments

Users ⓘ

[Specific users included](#)

Cloud apps or actions ⓘ

[All cloud apps](#)

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant ⓘ

Protecting Azure

1. Under Grant select the custom control
2. When you are ready to enable the Conditional Access policy select On under Enable Policy.

Grant



- Block access
- Grant access
 - Require multifactor authentication ⓘ
 - Require authentication strength (Preview) ⓘ
 - Require device to be marked as compliant ⓘ
 - Require Hybrid Azure AD joined device ⓘ
 - Require approved client app ⓘ
[See list of approved client apps](#)
 - Require app protection policy ⓘ
[See list of policy protected client apps](#)
 - Require password change ⓘ
 - MFAOnly
 - DuoTrustedEndpoint

Select

End State

- [Active Directory](#) users with aliases in Duo
- [Azure Active Directory](#) users with aliases in Duo
- Users that have multiple aliases count as one license
- Logins for Azure are protected with Duo MFA (Including M365)

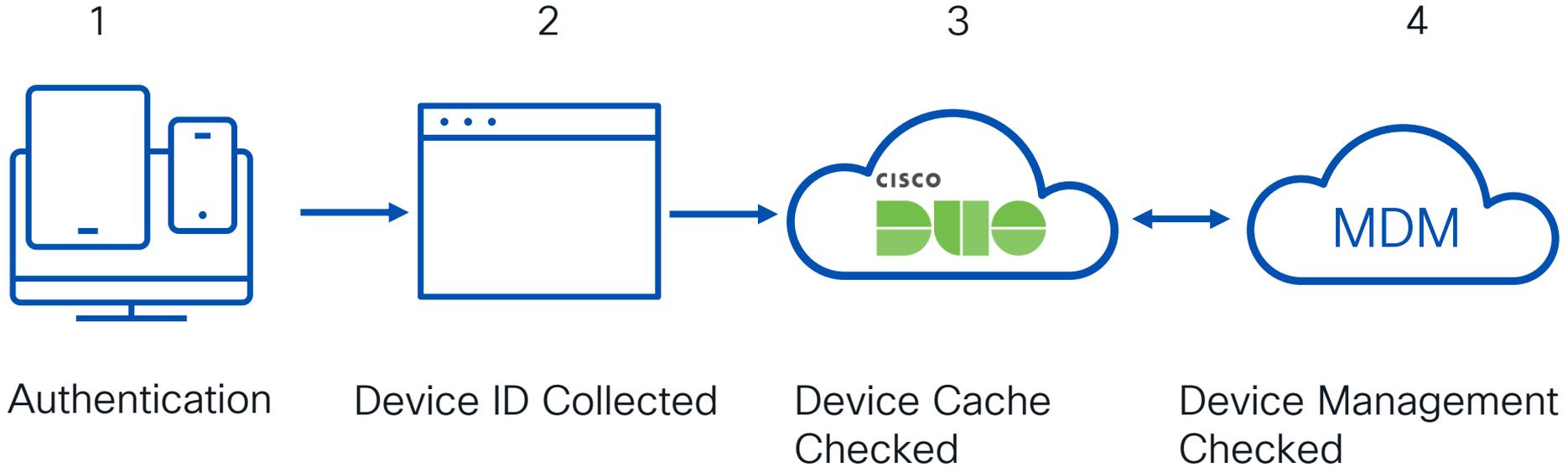
Step 2

Device Trust

1. Windows/Android/iOS – Intune and Domain Joined
2. Non Intune MDMs
3. Generic Trust

Establishing Managed Status

Trust Through Device Health Application



What is the Device Health Application?

Enforce Posturing for Managed and Non Managed Devices



OS

Mac OS X 13.2.1 ! out-of-date

Trusted Endpoint

No
Endpoint is not enrolled in your management system, via device health



Browser

Chrome
112.0.5615.49 ✓ up-to-date

Plugins

Flash ✓ uninstalled
Java ✓ uninstalled

🕒 **Last Seen**
1 minute ago



Browser

Safari 16.3 ! out-of-date

Plugins

Flash ✓ uninstalled
Java ✓ uninstalled

🕒 **Last Seen**
1 week ago

Device Health

Last Collected: Today



Device Health Application

Installed 4.3.0.0



Firewall

On



Disk Encryption

On



Password

Set

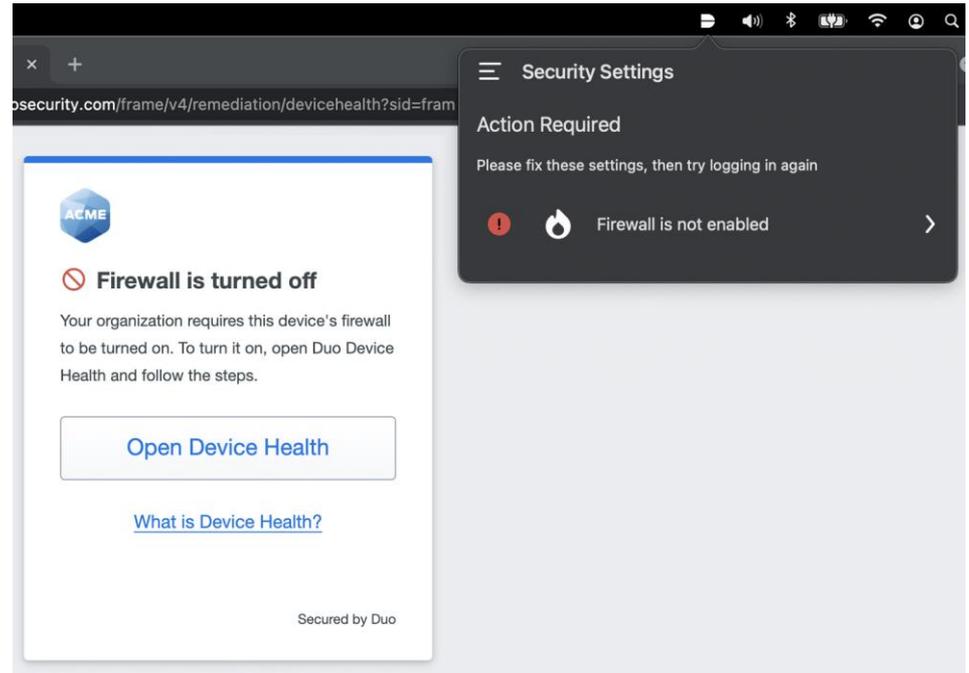
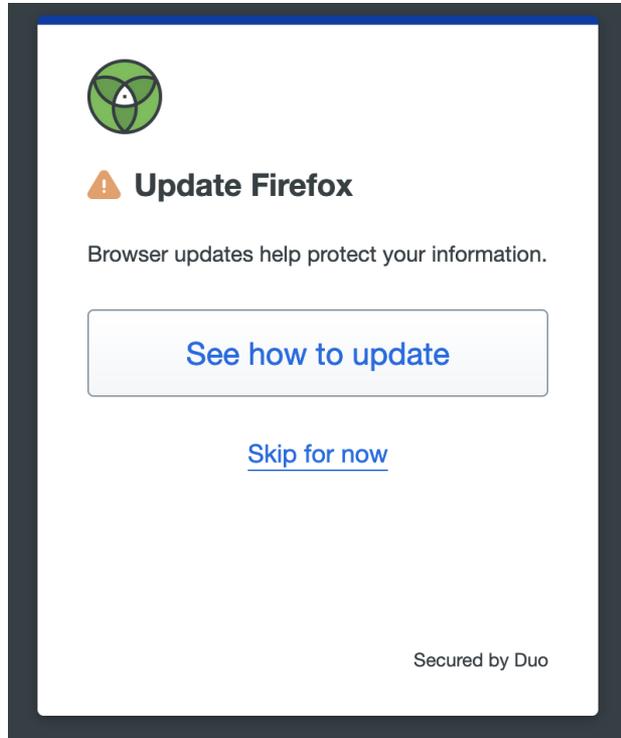


Endpoint Security Agent

Running Cisco Secure Endpoint 1.21.2.894

What is the Device Health Application?

Verify at the point of authentication



Configuring Duo MDM and Device Management

1. In Duo Admin Panel go to Trusted Endpoints
2. Select Add Integration
3. You will see a list of integrations

Device Management Tools Endpoint Detection & Response Systems

Management Tools

	Active Directory Domain Services	<input type="text" value="Add this Integration"/>	<input type="button" value="Add"/>	Read the Documentation
	Workspace ONE	<input type="text" value="Add this Integration"/>	<input type="button" value="Add"/>	Read the Documentation
	Duo Mobile	<input type="text" value="Add this Integration"/>	<input type="button" value="Add"/>	Read the Documentation
	G Suite	<input type="text" value="Add this Integration"/>	<input type="button" value="Add"/>	Read the Documentation

Configuring Duo MDM and Device Management

- Instructions for each supported device in [Intune](#)
- Domain joined devices [without Intune](#)
- Other MDMs such as [JAMF](#)
- No MDM is present we need to use [Generic Trust](#)



Google Verified Access for
Chromebooks

Add this Integration

Add



Intune

Recommended

Android

✓ Windows

iOS

Add

Microsoft Integration Highlights

Intune

- Support for mobile devices
- Verification of active management
- No long-lived certificates

Domain Joined

- Quick deployment
- Verify management of devices that cannot join Intune
- No extra Microsoft licenses required

End State

- Verification of devices that are being actively managed
- Non managed devices will be denied access
- Device Health Application checks that Windows Defender and Windows Firewall are both active

Step 3

Policy Enforcement

1. Duo Policy
2. Demo Videos

Duo Policy

Duo Policies



Highest Takes Precedence

Duo Policy Configuration

1. Go to Policies
2. Next to Custom Policies
Select New Policy
3. Name the policy

Custom Policies

To enforce different policies on different applications, create a custom policy and assign it to those applications. Policy settings in a custom policy will override anything set in the global policy.

[Learn more about policies](#)

[New Policy](#)

Policy name

Only Trusted

Users

[New User policy](#)
[Authentication policy](#)
[User location](#)

Devices

[Trusted Endpoints](#)
 [Device Health application](#)

Trusted Endpoints

i For **passwordless users**, only the Device Health app and Cisco Secure Endpoint will verify trust and grant access with this policy.

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

[Save Policy](#)

Duo Policy Configuration

1. Trusted Endpoints

- Select **Allow all endpoints** to verify prior to enforcement
- For Deployment **Require endpoints to be trusted**

2. Device Health Application

- When **Requiring users to have the app** end users must download prior to access
- Alternatively, **Don't require users to have the app** allows collection of data without Enforcement

Duo Policy Configuration

General Guidance

- Set policy for minimum allowed operating system versions
- Encourage users to update their browsers
- Limit MFA methods
- Block countries where you do not do business
- Enforce screen lock, firewall, drive encryption
- Require Enrollment when testing Deny Access in production

Duo Policy Configuration

1. Go to Applications and find your Azure application
2. Select and apply your newly created policy at the application level

Policy

Policy defines when and how users will authenticate when accessing this application. Your global policy always applies, but you can override its rules with custom policies.

Group policies

[Apply a policy to groups of users](#)

Application policy

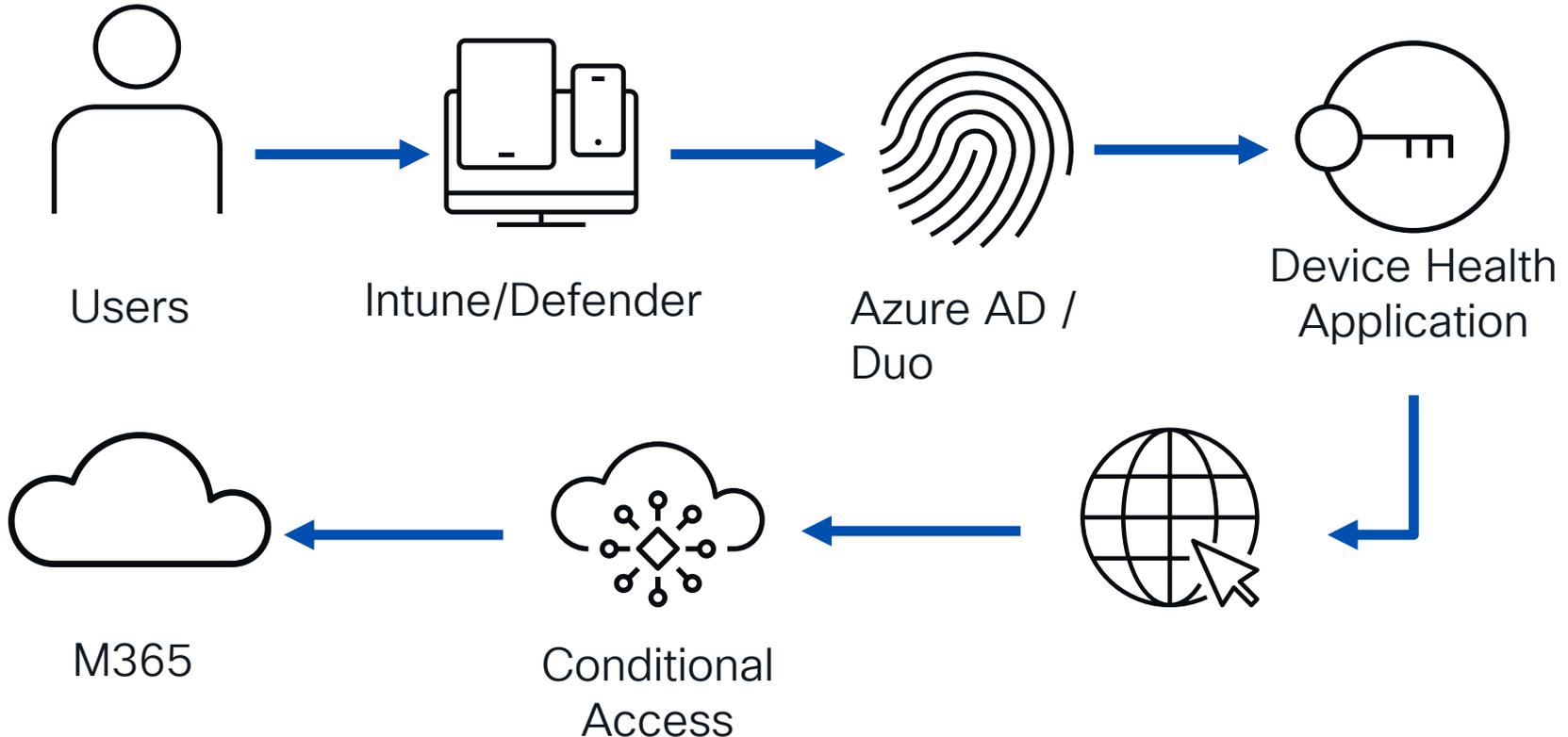
[Apply a policy to all users](#)



End State

- M365 protected with Duo MFA to enforce trusted endpoints
- Nonemployee posturing for M365
- Device Health Application checks that Windows Defender and Windows Firewall are both active

Hybrid Employee Accessing M365



Untrusted Access Attempt – M365

Introducing Microsoft 365 Copilot—your copilot for work. Learn more >



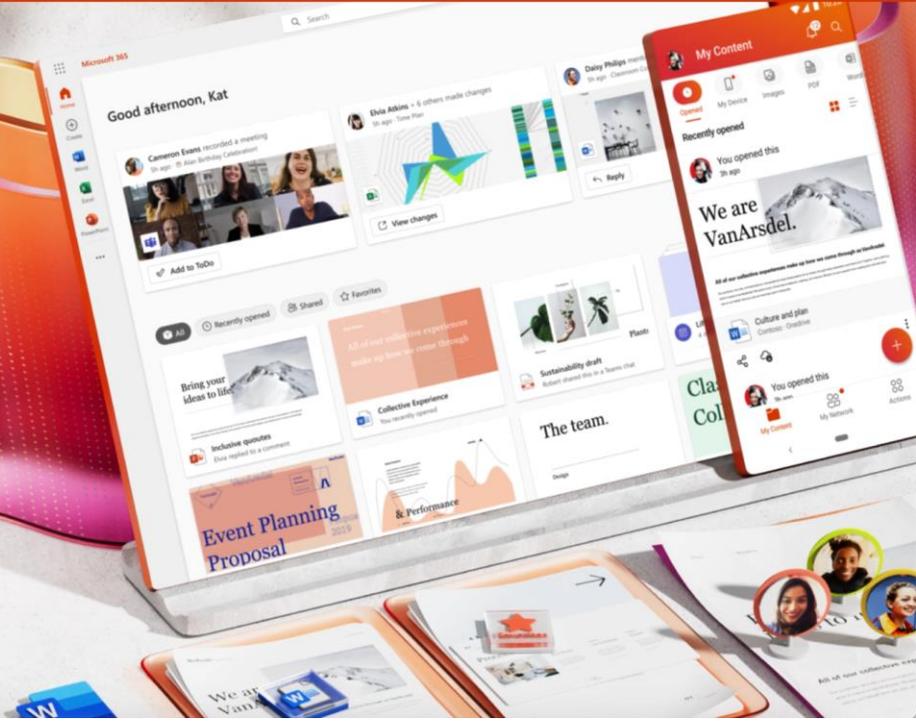
Hello, Welcome back.

Sign in as kevin@ehshouldbefine.com

Sign in

Switch to a different account

Not you? Forget this account



Duo Report

Timestamp (PDT) 	Result	User	Application	Trust Assessment 	Access Device
4:54:37 PM APR 9, 2023	 Denied Endpoint is not trusted	kevinpatrick	Microsoft Azure Active Directory - Trusted Only	<u>Normal</u>	<p>▼ Mac OS X 13.3.1 (22E261) As reported by Device Health</p> <p>Hostname KEVPATRI-M-70HW</p> <p>Safari 16.4 Flash Not installed Java Not installed</p> <p>Device Health Application Installed</p> <p>Firewall On Encryption On Password Set Security Agents Running: Cisco Secure Endpoint</p> <p>Napa, CA, United States 75.10.1.159</p> <p>Not a Trusted Endpoint determined by Device Health</p>

Firewall Disabled Attempt Trusted Device – M365

Introducing Microsoft 365 Copilot—your copilot for work. Learn more >



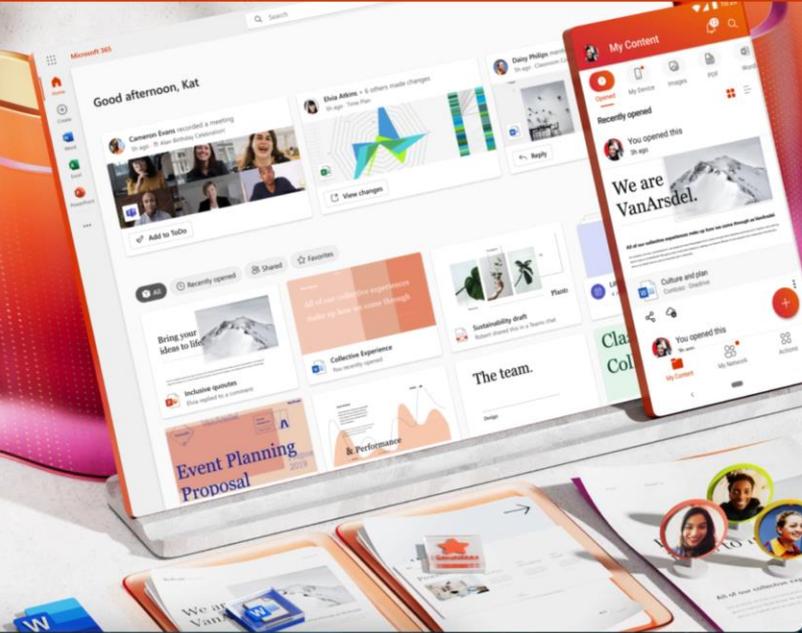
Hello, Welcome back.

Sign in as kevin@ehshouldbefine.com

Sign in

Switch to a different account

Not you? Forget this account



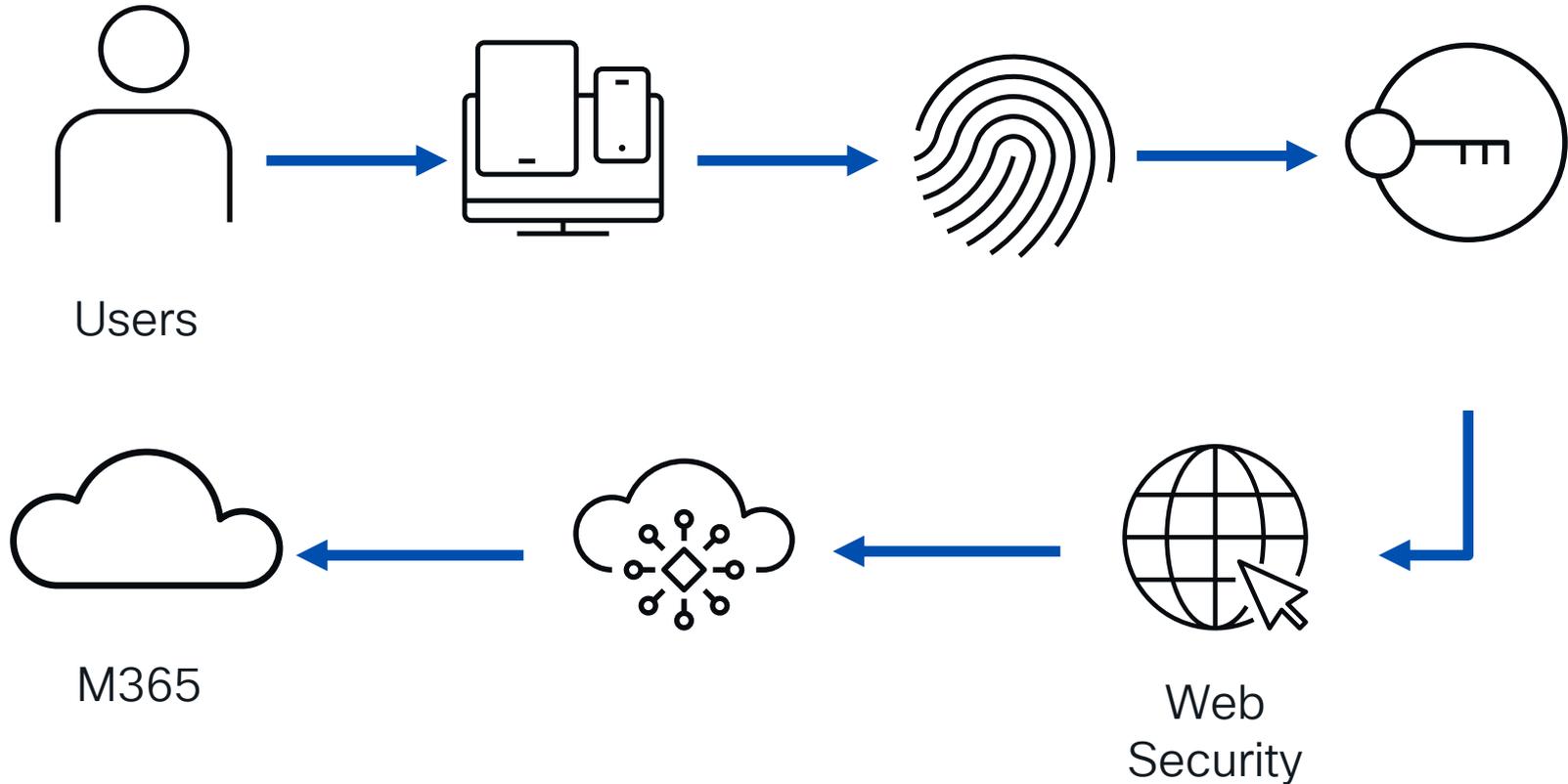
Duo And Microsoft

- Central Zero Trust device enforcement in Duo
- Identity management and least privilege access in Microsoft
- Device Health Application checks that Windows Defender and Windows Firewall are both active
- Posturing checks for non managed devices accessing Azure protected resources

Umbrella + Microsoft



Hybrid Employee Accessing M365



Configuration Roadmap

Step 1 Identity

Step 2 HTTPS Filtering

Step 3 Application Protection

Environment Assumptions

1. Configured Azure Active Directory
2. Azure Active Directory Sync
3. Azure AD joined machine
4. Basic filtering policies setup in Umbrella (web policy)
5. Administrator access to Umbrella
6. Roaming Computer configuration on endpoints (secure endpoint)

Steps for Deployment

1. Azure Active Directory sync with Umbrella
2. Add Umbrella Cert (both DNS & Web) Add customer signed certificate to Umbrella (if not using Umbrella Root Certificate)
3. Deploy/Install AnyConnect
4. Configure AnyConnect with Umbrella Secure Client profile (org.json)
5. Set up Web Policy in Umbrella
6. Set up Tenant Controls in Umbrella

Step 1

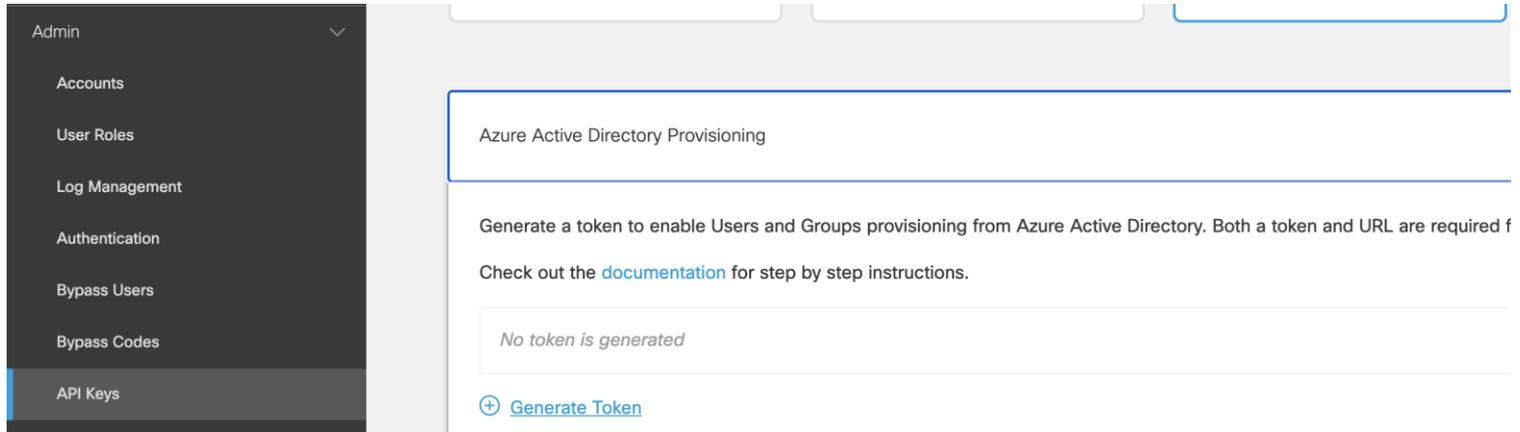
Identity

1. Provision Azure AD Users

Azure AD Users

Azure AD Provisioning

1. Login to your Umbrella admin panel
2. Go to Admin > Keys
3. Generate a new key
4. Copy your key and the SCIM URL *key is only shown once



The screenshot shows the Umbrella admin panel interface. On the left is a dark sidebar menu with the following items: Admin (with a dropdown arrow), Accounts, User Roles, Log Management, Authentication, Bypass Users, Bypass Codes, and API Keys (highlighted with a blue bar). The main content area is titled 'Azure Active Directory Provisioning'. Below the title, there is a text block: 'Generate a token to enable Users and Groups provisioning from Azure Active Directory. Both a token and URL are required for provisioning. Check out the [documentation](#) for step by step instructions.' Below this text is a light gray box containing the message 'No token is generated'. At the bottom of the page, there is a blue button with a plus sign and the text 'Generate Token'.

Azure AD Provisioning

1. In Azure go to Enterprise Applications
2. Search for Umbrella
3. Select Cisco Umbrella User Management

The screenshot shows the Azure AD App Gallery interface. At the top, there is a breadcrumb trail: Home > Enterprise applications | All applications >. Below this is the heading 'Browse Azure AD Gallery' with a three-dot menu icon. There are two links: '+ Create your own application' and 'Got feedback?'. A descriptive paragraph follows: 'The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When dep connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the A: request using the process described in [this article](#).' Below the text is a search bar containing 'umbrella' with a clear button. To the right of the search bar are three filter buttons: 'Single Sign-on : All', 'User Account Management : All', and 'Categories : All'. Below the filters are two toggle buttons: 'Federated SSO' (selected) and 'Provisioning'. The results section is titled 'Showing 2 of 2 results'. There are two application cards. The first card is for 'Cisco Umbrella Admin SSO' by Cisco Systems, Inc., featuring a cloud and shield icon. The second card is for 'Cisco Umbrella User Management' by Cisco Systems, Inc., featuring a cloud and person icon. A blue arrow points to the 'Cisco Umbrella User Management' card.

Azure AD Provisioning

1. Go to the Umbrella Application in Enterprise Applications
2. Select Provisioning and then Get Started



Automate identity lifecycle management with Azure Active Directory

Automatically create, update, and delete accounts when users join, leave, and move within your organization. [Learn more.](#)

Get started

Azure AD Provisioning

1. Enter the information you copied earlier and test the connection. Click Save

Microsoft Azure Search resources, services, and docs (G+)

Home > Cisco Umbrella User Management | Overview >

Provisioning

Save Discard

Provisioning Mode
Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Cisco Umbrella User Management based on user and group assignment.

Admin Credentials

Admin Credentials
Azure AD needs the following information to connect to Cisco Umbrella User Management's API and synchronize user data.

Tenant URL * ⓘ
https://api.umbrella.com/identity/v2/scim ✓

Secret Token
.....

Test Connection

Testing connection to Cisco Umbrella User Management
The supplied credentials are authorized to enable provisioning

Azure AD Provisioning

1. Go to Users and Groups
2. Select whom you would like to provision

The screenshot shows the Cisco Umbrella User Management interface for an application named "Test Environment". The left sidebar contains a navigation menu with the following items: Properties, Owners, Roles and administrators, Users and groups (highlighted), Single sign-on, Provisioning, Self-service, and Custom security attributes (preview). The main content area has a header "Cisco Umbrella User Management | Users and groups" and a sub-header "Enterprise Application". Below the header are action buttons: Add user/group, Edit assignment, Remove, Update credentials, Columns, and Got feedback?. A blue information banner states: "The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this." Below this is a search bar with the text "First 200 shown, to search all users & gro...". A table below the search bar has two columns: "Display Name" and "Object Type". The table contains one row with a checkbox, a circular profile icon with "KP", the name "Kevin Patrick", and the object type "User".

Display Name	Object Type
<input type="checkbox"/>  Kevin Patrick	User

Azure AD Provisioning

1. Provisioning has a fixed interval
2. You can start this manually by selecting Provisioning

The screenshot shows the 'Cisco Umbrella User Management | Overview' page. The breadcrumb trail is 'Home > Enterprise applications | All applications > Cisco Umbrella User Management | Provisioning >'. The page title is 'Cisco Umbrella User Management | Overview'. The navigation bar includes links for 'Start provisioning', 'Stop provisioning', 'Restart provisioning', 'Edit provisioning', 'Provision on demand', 'Refresh', and 'Got feedback?'. The left sidebar has sections for 'Manage' (Overview, Provision on demand, Users and groups, Expression builder) and 'Monitor' (Provisioning logs, Audit logs, Insights). The main content area shows 'Current cycle status' as 'Initial cycle completed.' with a '100% complete' progress bar. Below this is a 'Users' count of '1' and a link to 'View provisioning logs'. The 'Statistics to date' section has links for 'View provisioning details' and 'View technical information'. The 'Manage provisioning' section includes links for 'Update credentials', 'Edit attribute mappings', 'Add scoping filters', and 'Provision on demand'.

End State

- Azure identities synced into Umbrella
- Able to provision user and group information during SAML authentication
- Identity support in Anyconnect SWG module

Step 2

HTTPS Filtering

1. Web Policy Secure Web Gateway (SWG)

SIG Web Policy - Prerequisites

1. [HTTPS inspection](#) must be enabled for endpoints.
 1. Deploying [Umbrella root certificate](#)
 2. OR deploy [your own certificate](#)
 3. Deploy [Secure Client profile](#) Remote Employees - AnyConnect + Roaming Computers config

SIG



IPsec
tunnel*

CDFW & Web



HQ & Branch



Proxy chain or
Cloud PAC File

Web only



HQ & Branch



Cisco Secure Client
(AnyConnect)

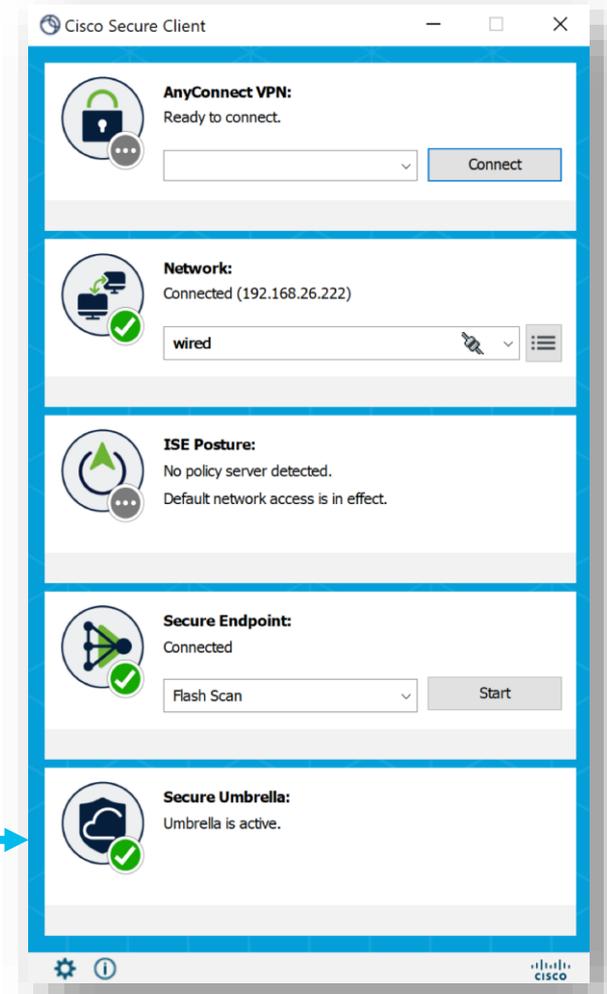
Web & DNS



Roaming

Cisco Secure Client Suite of Security Service Enablement Modules

- AnyConnect VPN (Core)
- Network Access Manager (NAM)
- ISE Posture
- HostScan (aka: ASA posture) (No UI)
- Secure Endpoint (AMP)
- Umbrella Module
- Cloud Management Module (No UI)
- Network Visibility Module (NVM) (No UI)
- Diagnostics and Reporting Tool (DART)



End State

- Trusted certificate deployed to device
- Secure Client deployed across device types
- Umbrella configuration sending traffic to your Umbrella tenant

Step 3

Application Protection

1. Tenant Controls
2. Web Policy

Tenant Controls

Microsoft Compatibility

Global Settings

Add Global Settings Policy Tester

Microsoft 365 Compatibility

Microsoft recommends bypassing proxy inspection to maximize Microsoft 365 performance.

Microsoft 365 Compatibility

With this feature enabled, Umbrella passes Microsoft 365 traffic through the proxy without applying policy. No decryption or inspection is applied to this traffic.

Microsoft Tenant Controls

1. Go to Azure Active Directory > Properties. Copy your tenant ID
2. Copy your domain you will be using

Basic information

Name	Default Directory
Tenant ID	700225d2-f06d-4aed-b2ab-9e7acb2851ac 
Primary domain	ehshouldbefine.com

Microsoft Tenant Controls

1. Go to Umbrella Policy > Policy Components > Tenant Controls
2. Enter your information under Microsoft 365
3. Optionally you can block using Personal Accounts

Tenant Directory ID

700225d2-f06d-4aed-b2ab-9e7acb2851ac

Personal Accounts

Allows access to only personal Microsoft 365 apps and services.

Allow or block access to personal Microsoft 365 apps and services. Enable to block access. Disable to allow access. For more information, see Umbrella's [Help](#).



Block Personal Microsoft 365 Account Access

Configure Web Policy

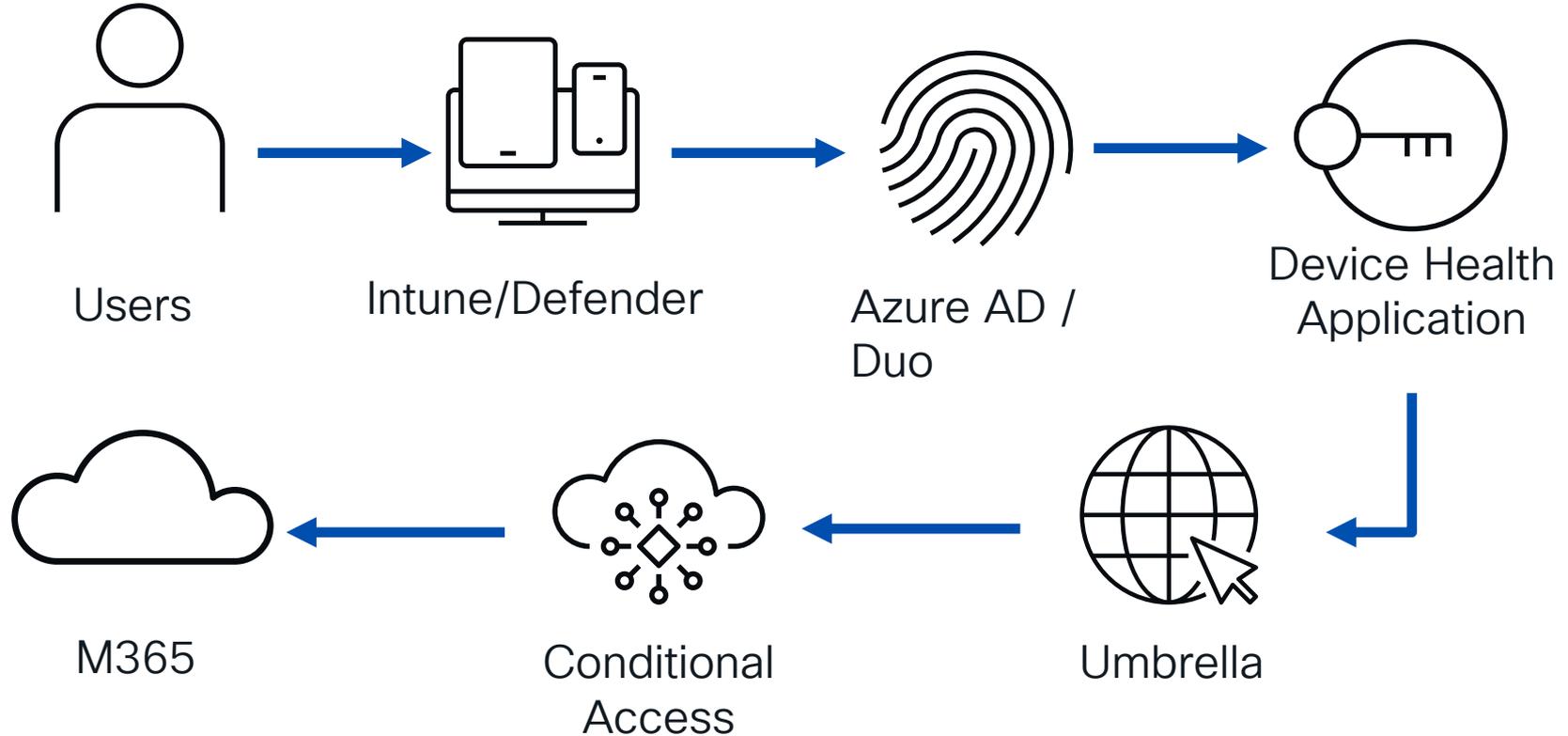
1. Go to Policies > Web Policy
2. Enable HTTPS Inspection
3. Add rule sets for custom identities

Tenant Controls	Global Tenant Controls	Edit
File Analysis	1 Setting Enabled	Edit
File Type Control	Disabled	Edit
HTTPS Inspection	Enabled	Edit
PAC File	https://proxy.prod.pac.swg.umbrella.com/...	

End State

- M365 tenant enforcement enabled
- Off network devices are being protected with Umbrella

Hybrid Employee Accessing M365



Enabling Off Prem Access (ZTNA)

Remote Access at Cisco

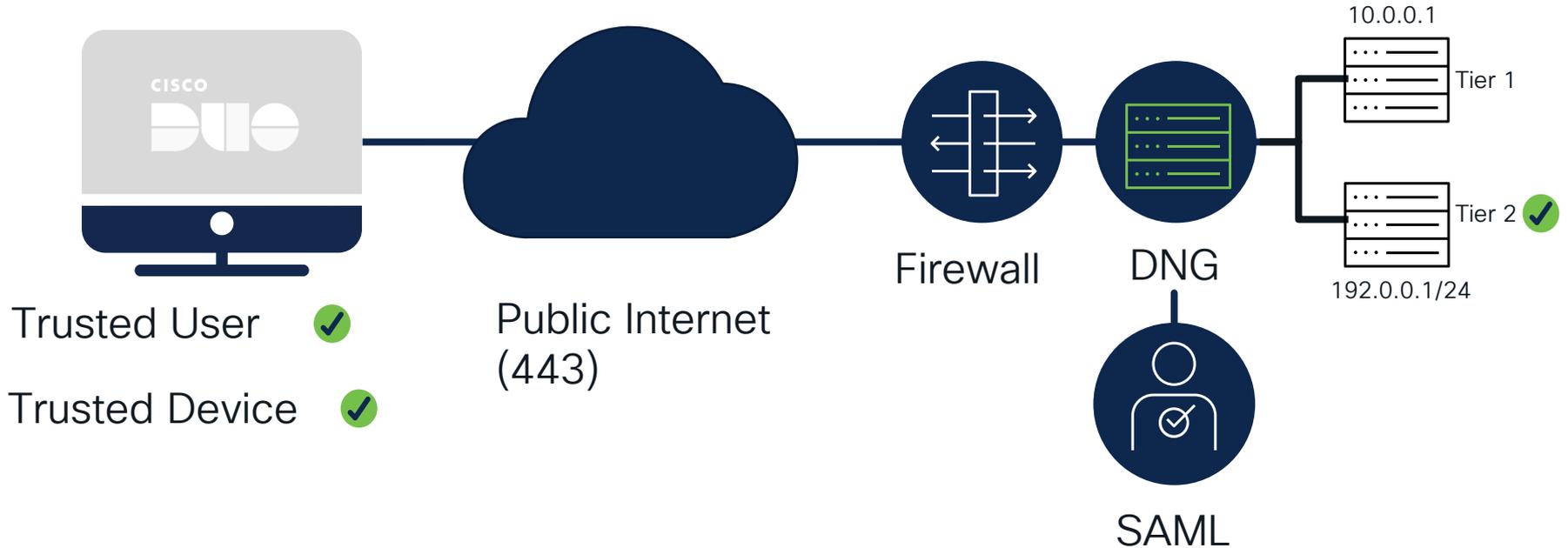
VPNless

- [Duo Network Gateway](#)
- HTTPS applications
- No tunneling required

VPN Required

- Secure Client w/ Anyconnect and Firepower
- Legacy applications
- Pending application onboarding

Duo Network Gateway



QuickTime Player File Edit View Window Help

Instance details | EC2 Manager X Multi-Factor Authentication & S X +

us-west-1.console.aws.amazon.com/ec2/home?region=us-west-1#InstanceDetails:instanceId=i-0cb8d653f3d079fec

aws Services Search [Option+S] N. California DAG-AWS-Admins/kevin@thatshouldbefine.com @ shouldbefine

New EC2 Experience Tell us what you think X

Security groups for eni-0679d86ce095c8b66 changed successfully X

EC2 > Instances > i-0cb8d653f3d079fec

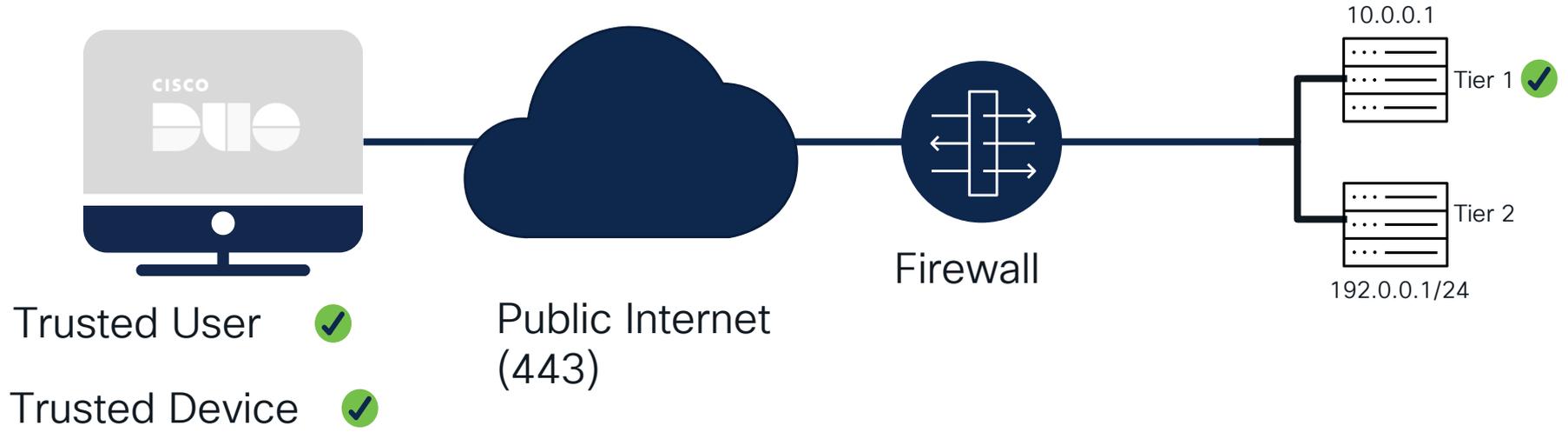
Instance summary for i-0cb8d653f3d079fec (AWS Auth 1) Info Refresh Connect Instance state Actions

Updated less than a minute ago

Instance ID i-0cb8d653f3d079fec (AWS Auth 1)	Public IPv4 address 54.219.77.193 open address	Private IPv4 addresses 172.31.10.188
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-54-219-77-193.us-west-1.compute.amazonaws.com open address
Hostname type -	Private IP DNS name (IPv4 only) ip-172-31-10-188.us-west-1.compute.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 54.219.77.193 [Public IP]	VPC ID vpc-1c4ebd7a	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-5bb24b01	
IMDSv2		

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Secure Client





AnyConnect
Secure Mobility Client

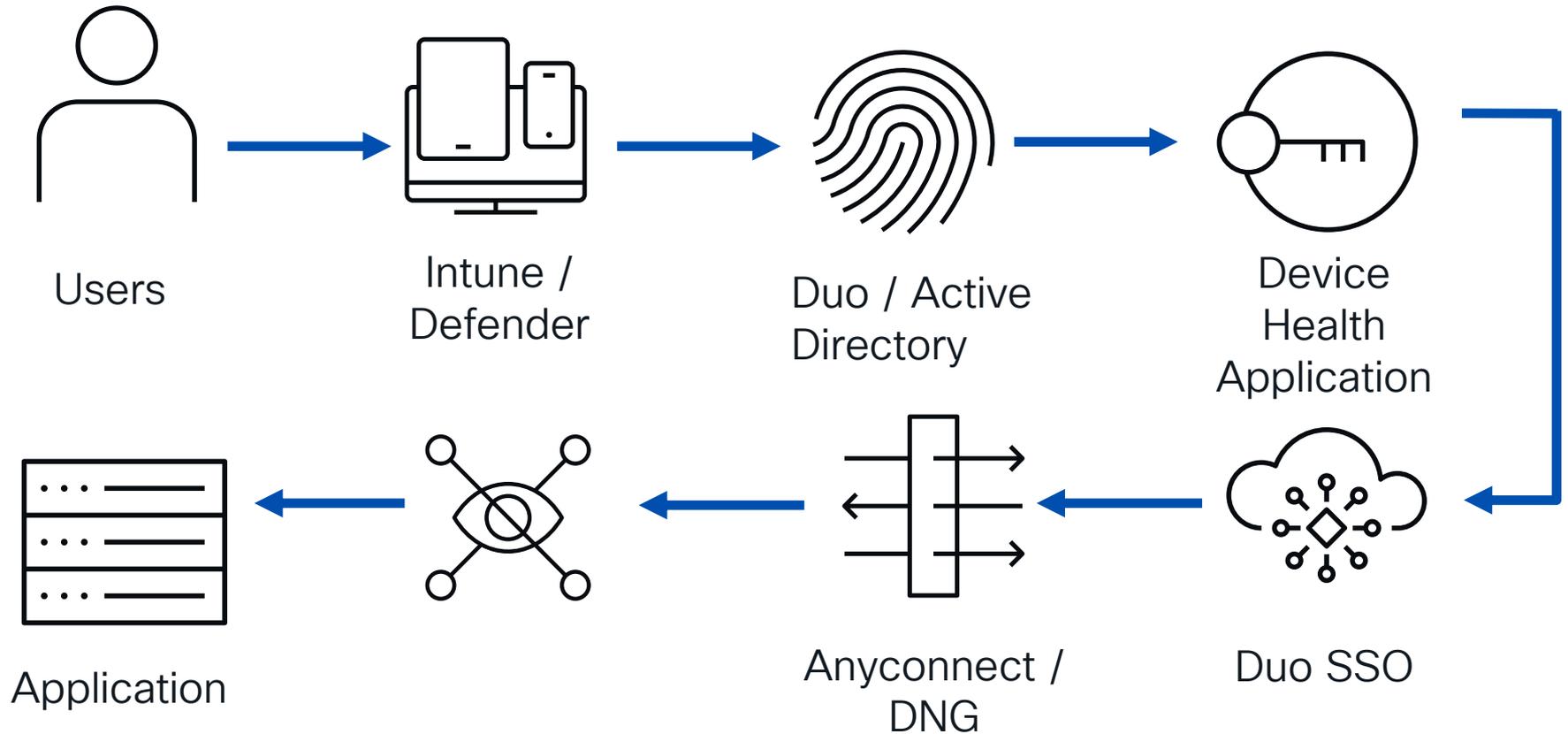
VPN:
On a trusted network.
asavpn.xerotrustlabs.com

System Scan:
Compliant.
Network access allowed.

Roaming Security:
Umbrella is active.



Remote User Accessing On Prem



Reference Architectures



TALOS THREAT INTELLIGENCE

- Actionable threat intelligence
- Collective responses
- Comprehensive visibility
- Signal identification
- Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

SERVICES

- Custom threat research on demand
- Implement and manage
- Incident response retainer
- Managed detection & response
- Strategy & assessment

Kenna | Secure Analytics | SecureX
Secure Client | Talos Incident Response

CAPABILITIES

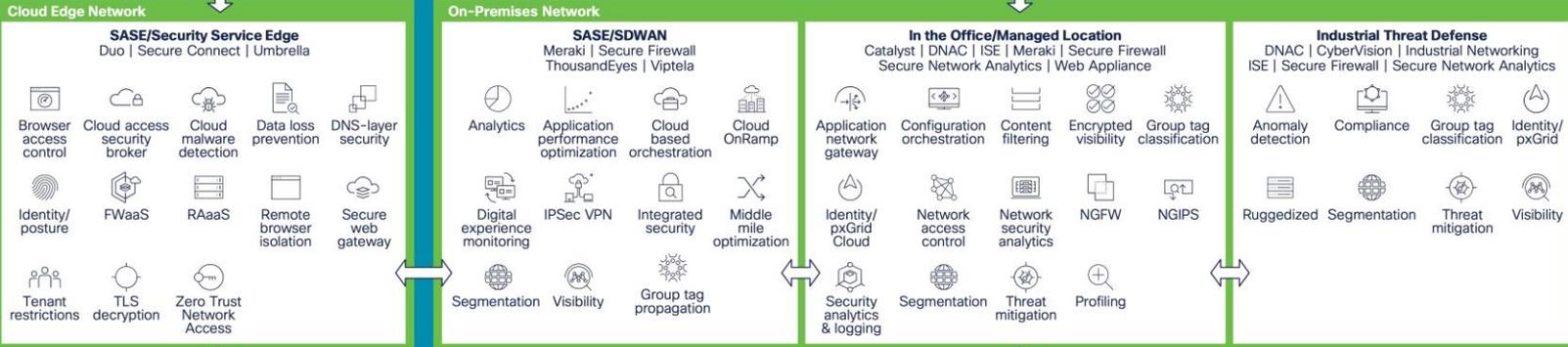
- Network detection & response
- Device discovery & insights
- Endpoint detection & response
- Open API platform & 3rd party native integrations
- Risk-based vulnerability management
- Security analytics
- Security orchestration, automation & response
- Threat visibility, incident response & threat hunting

ZERO TRUST

SASE

User/Device Security

SASE/REMOTE WORKER: Cisco Secure Client (AnyConnect) | Umbrella | Meraki Systems Manager | Duo | Secure E-mail | ThousandEyes



Workload, Application, and Data Security

HYBRID MULTI-CLOUD: ACI | Cloud Insights | Panoptica | Radware | Secure Application | Secure Endpoint | Secure Firewall | Secure Cloud Analytics | Secure Workload



Microsoft Cybersecurity Reference Architectures (MCRA)

Capabilities

What cybersecurity capabilities does Microsoft have?



Build Slide

Azure Native Controls

What native security is available?



Attack Chain Coverage

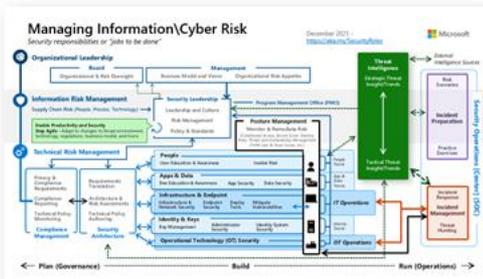
How does this map to insider and external attacks?



Build Slide

People

How are roles & responsibilities evolving with cloud and zero trust?



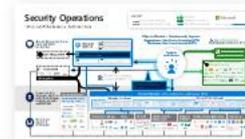
Zero Trust User Access

How to validate trust of user/devices for all resources?



Security Operations

How to enable rapid incident response?



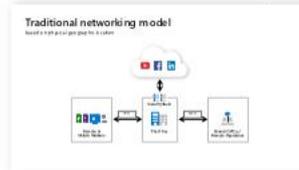
Multi-Cloud & Cross-Platform

What clouds & platforms does Microsoft protect?



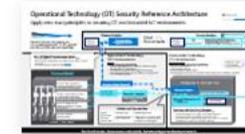
Secure Access Service Edge (SASE)

What is it? How does it compare to Zero Trust?



Operational Technology

How to enable Zero Trust Security for OT?



aka.ms/MCRA | December 2021 | Microsoft

Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

CISCO *Live!*

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

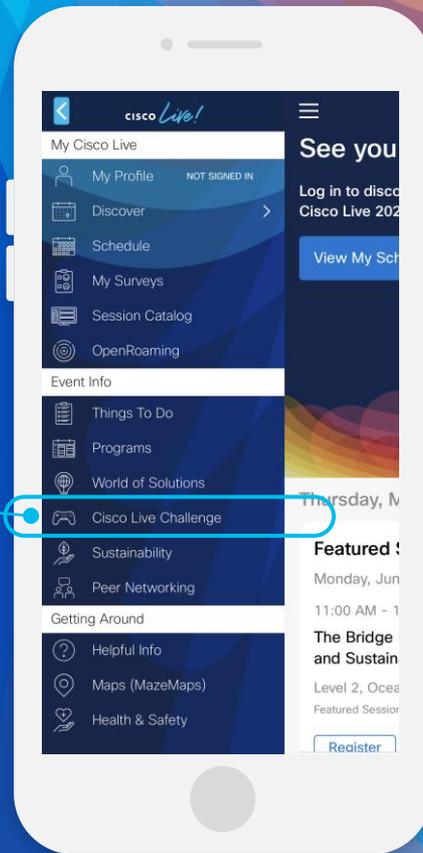


Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, radiating from a bright white point on the right side.

CISCO *Live!*

Let's go

#CiscoLive