
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 Webex App

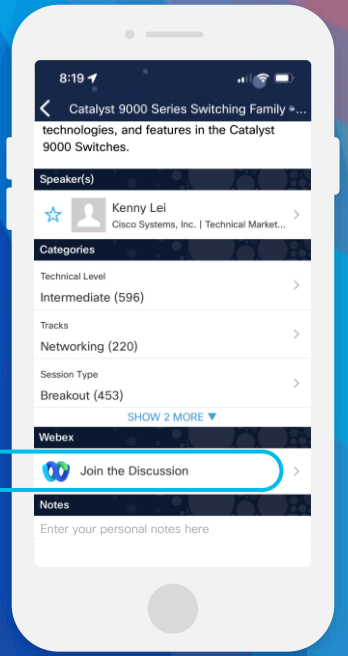
Questions?

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://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2105

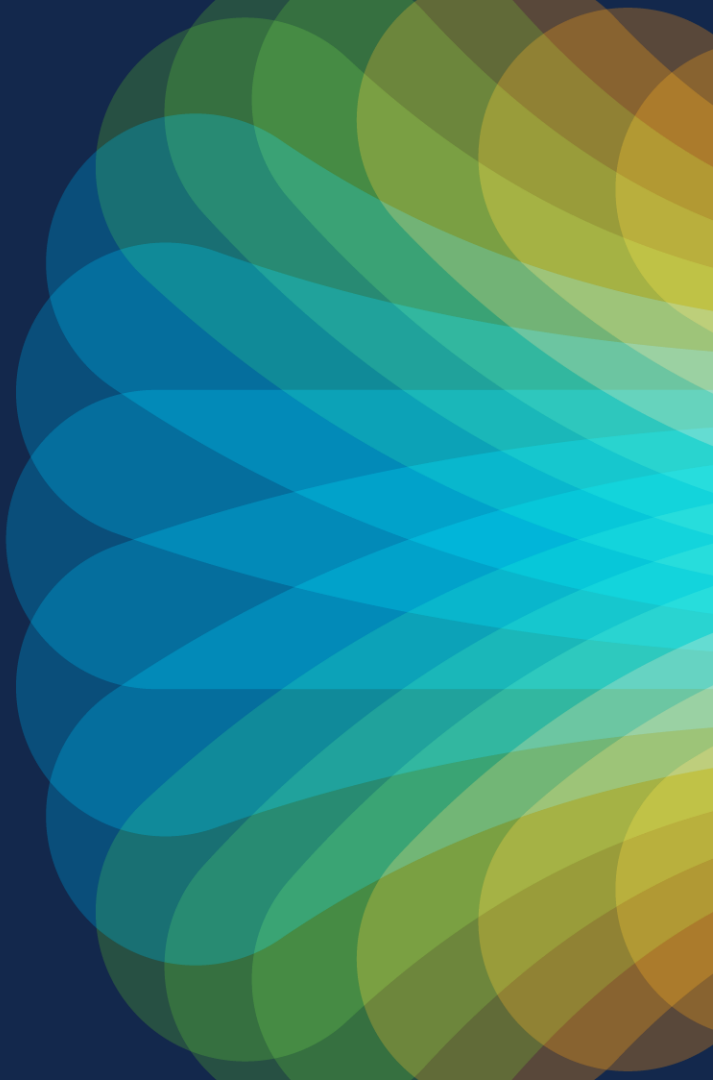
Agenda

- 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

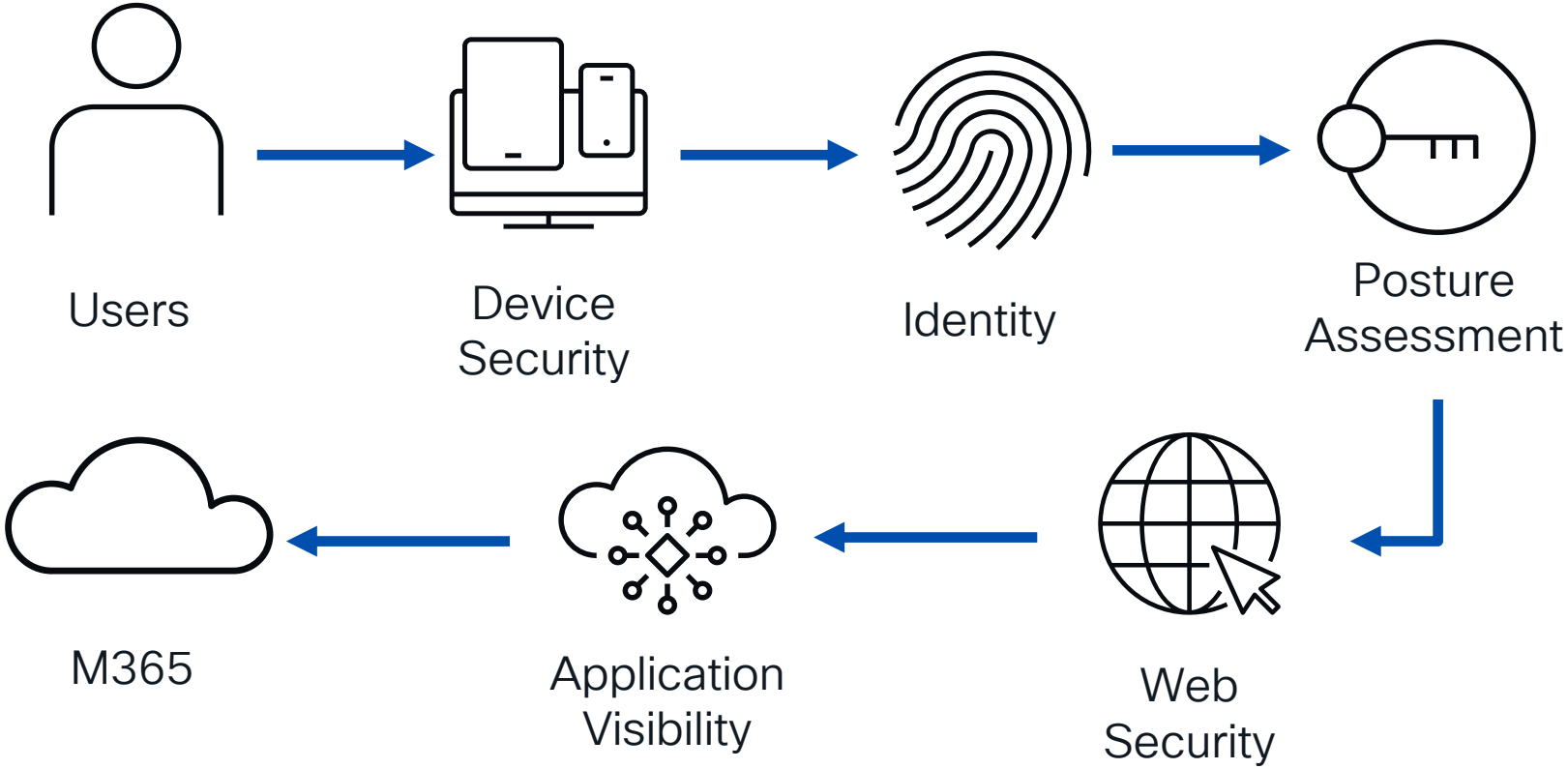
- **Identity Management**
  - Identity Governance
  - Password Abuse
  - Cloud and On Premise
- **Endpoint Protection**
  - Windows Defender
  - Intune
  - Group Policy

Cisco

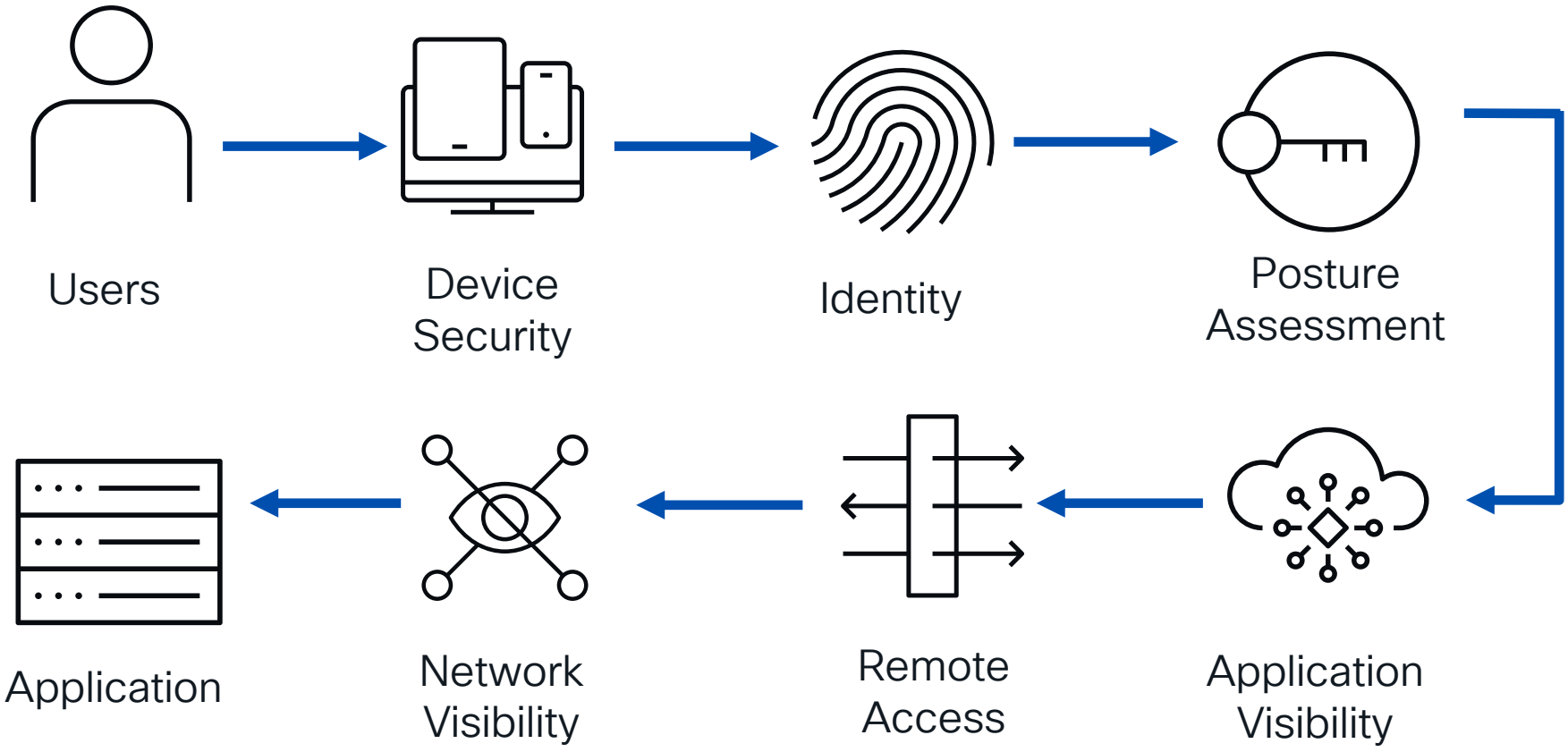
- **Flexible**
  - Simplify zero trust policy
  - Non-Microsoft Applications
  - Multi Platform
- **Protecting the Network**
  - Content Filtering
  - Segmentation
  - Multi Cloud

Practical Examples

Hybrid Employee Accessing M365



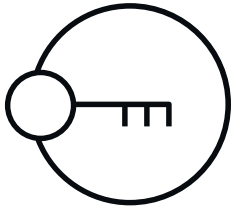
Remote User Accessing On Prem



Identity

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

Posture Assessment

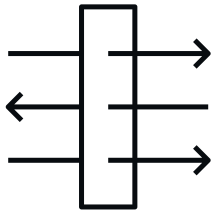


- **Device Management**
  - Duo Device Health Application
  - Microsoft Intune
- **Posture Verification**
  - Duo Device Health Application

Web Security

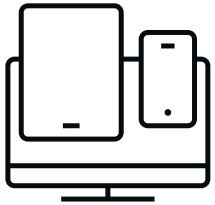
- **M365 Tenant Control**
  - Cisco Umbrella
- **Malicious Websites/Redirect Links**
  - Microsoft Defender/ Cisco Umbrella

Remote Access



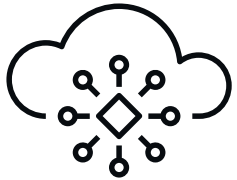
- **VPN Access**
  - Cisco Secure Client w/ Anyconnect
- **VPN-less Access**
  - Duo Network Gateway

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

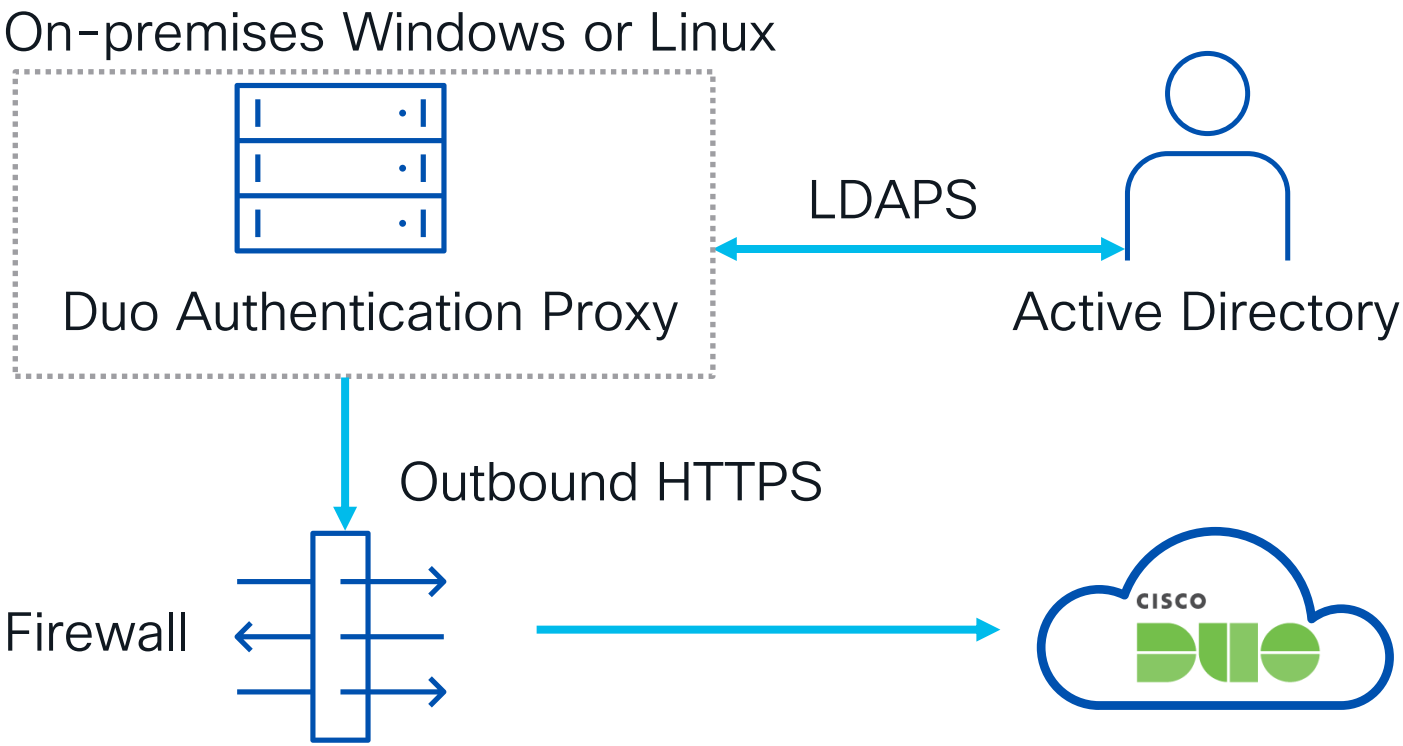
Step 1

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 Prem Active Directory

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

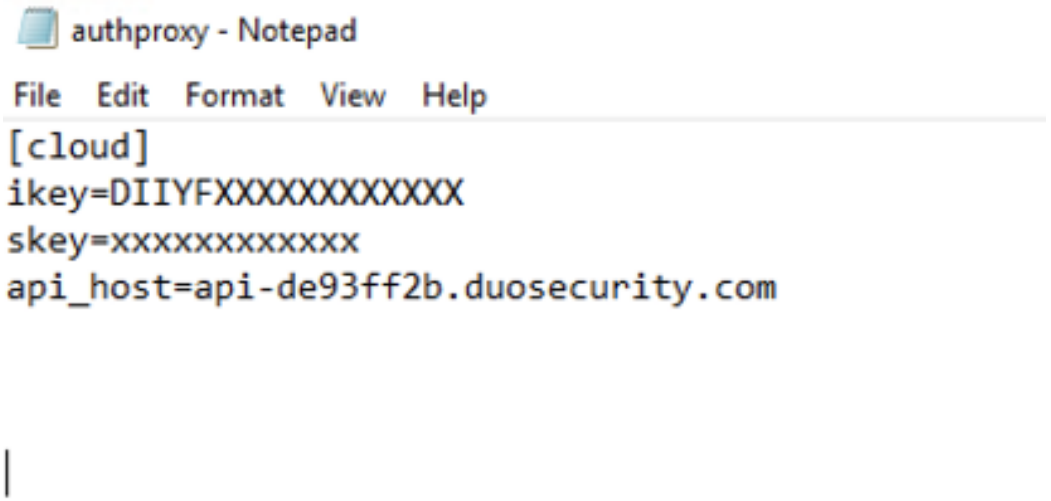
Configuration metadata

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 `ikey`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or download a pre-configured file.

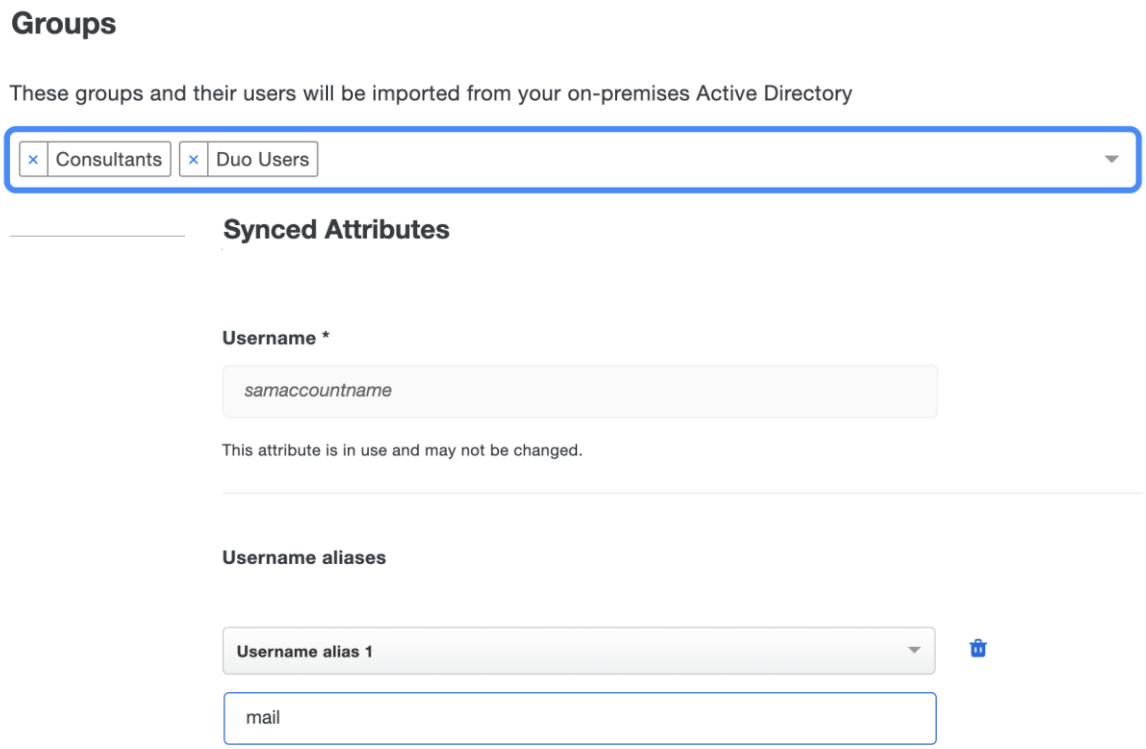
On Prem Active Directory

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



On Prem Active Directory

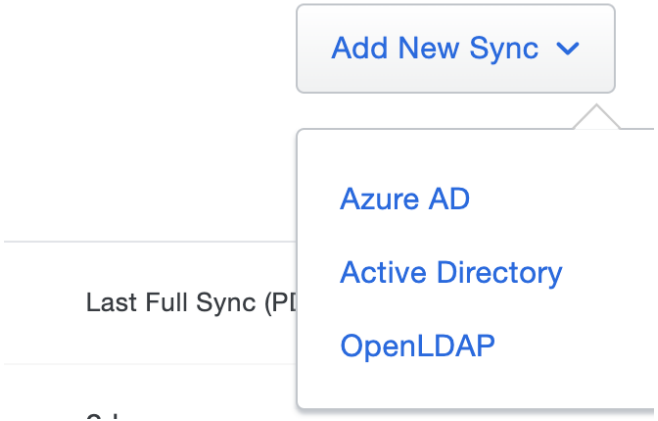
1. Select groups to sync for users that do not sync into Azure
2. Create any aliases needed
3. Save and Sync Now



Azure Active Directory

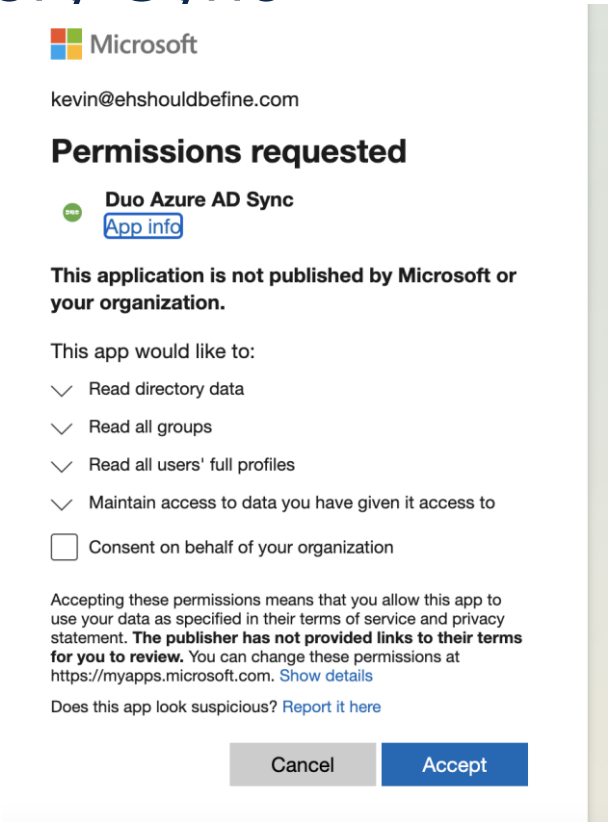
Azure Directory Sync

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



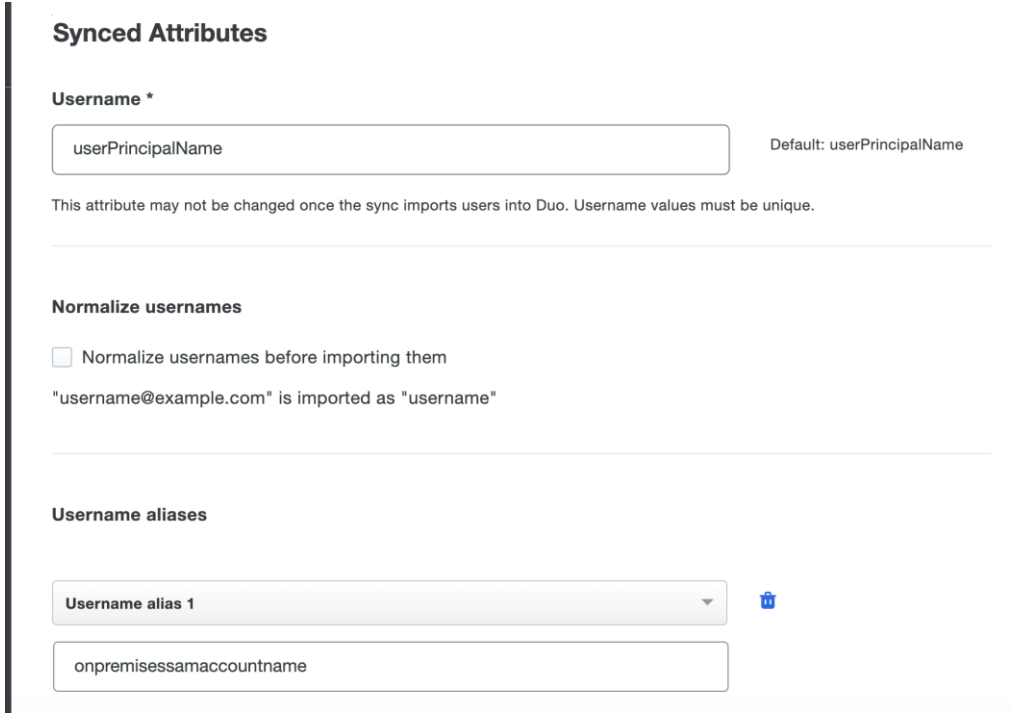
Azure Directory Sync

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



Azure Directory Sync

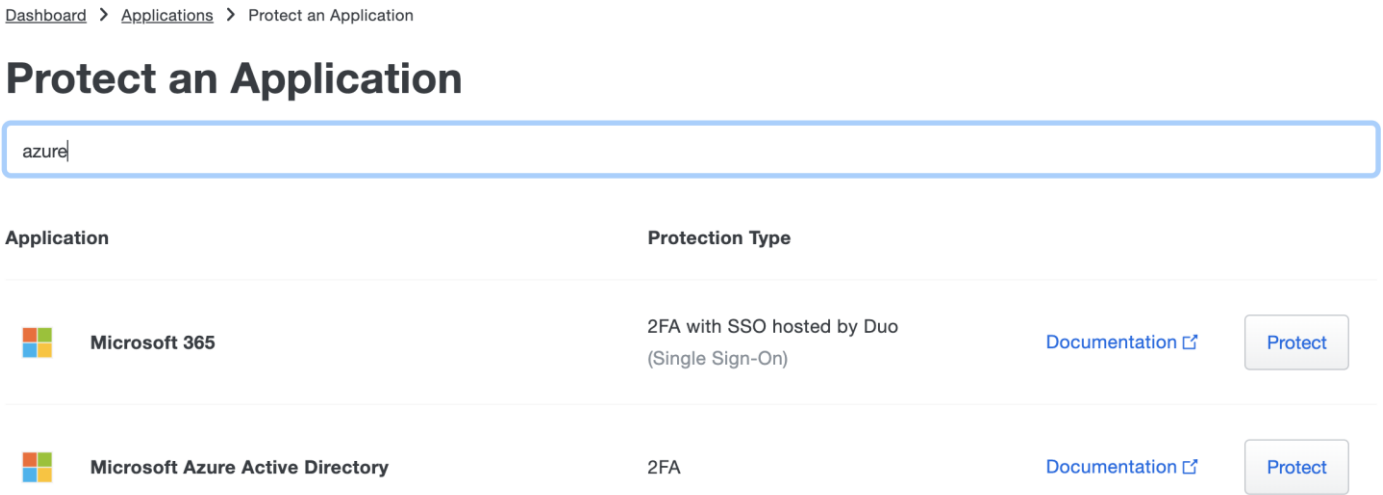
1. Select Azure groups to sync
2. Do NOT select normalize
3. Create aliases
4. Sync Now



Protecting Azure

Protecting Azure

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



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

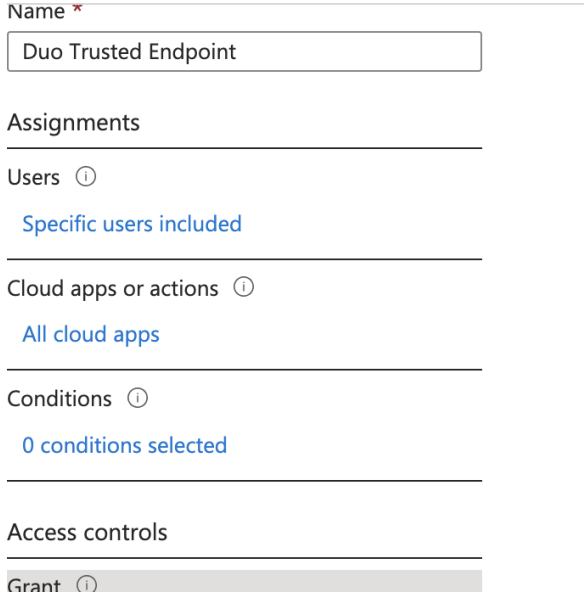
```
{
    "AppId": "[redacted]",
    "ClientId": "[redacted]",
    "Controls": [
        {
            "ClaimsRequested": [
                {
                    "Type": "DuoMfa",
                    "Value": "MfaDone",
                    "Values": null
                }
            ],
            "Id": "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

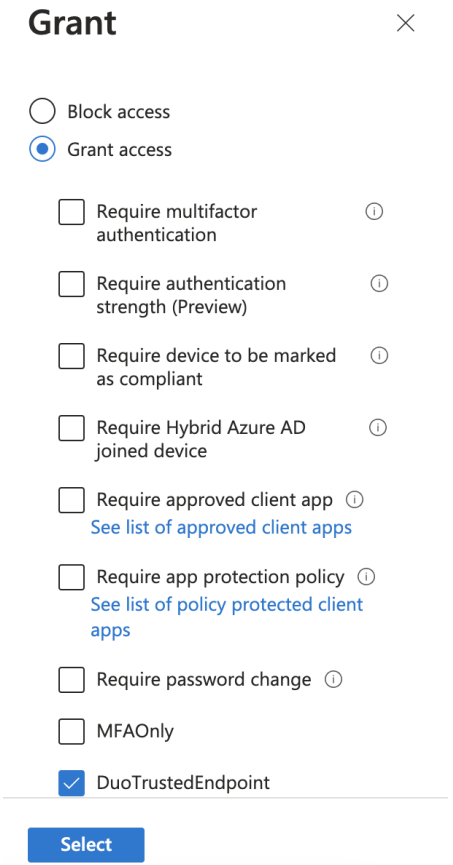
Protecting Azure

1. Under Polices 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.



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.



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)

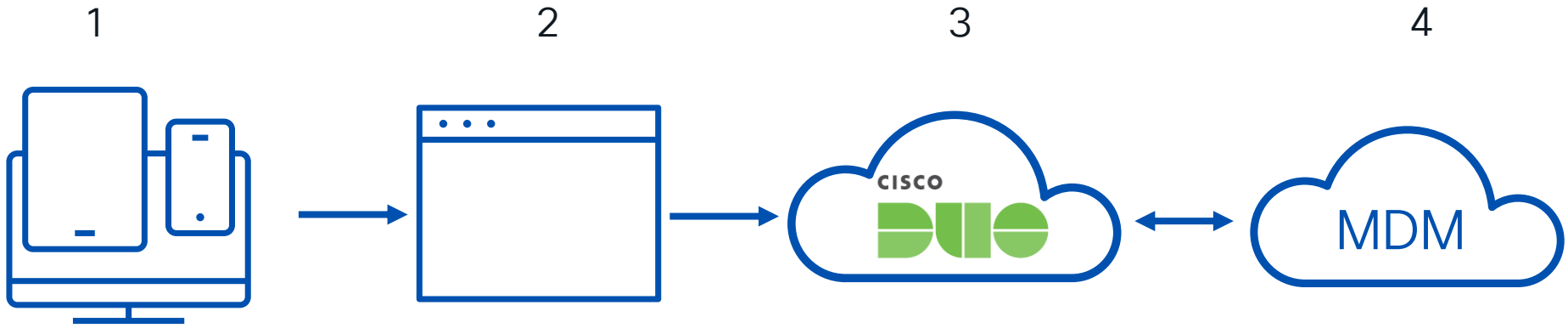
Step 2

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



Authentication

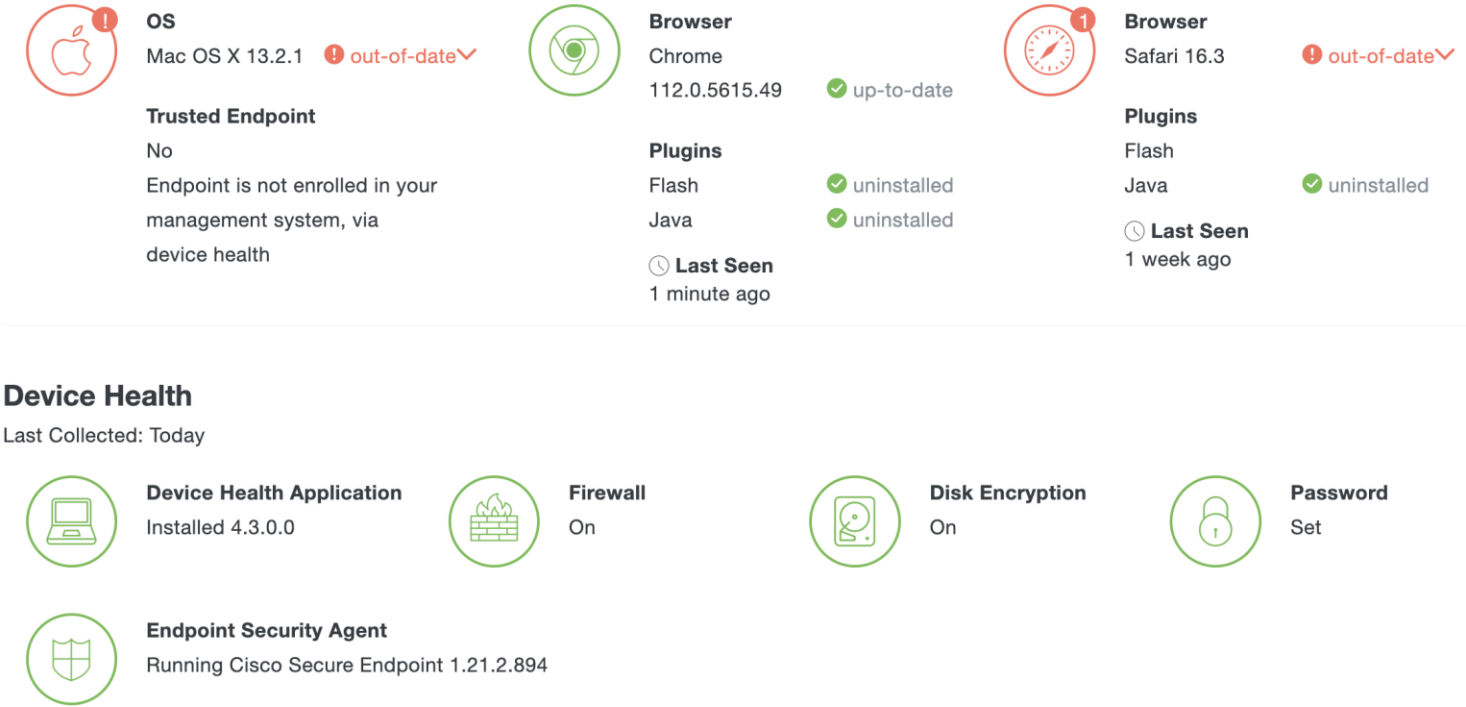
Device ID Collected

Device Cache Checked

Device Management Checked

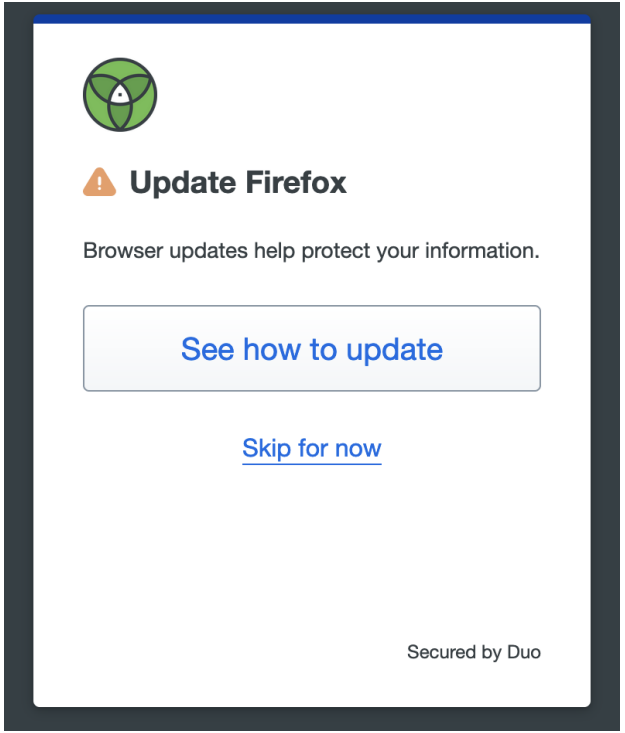
What is the Device Health Application?

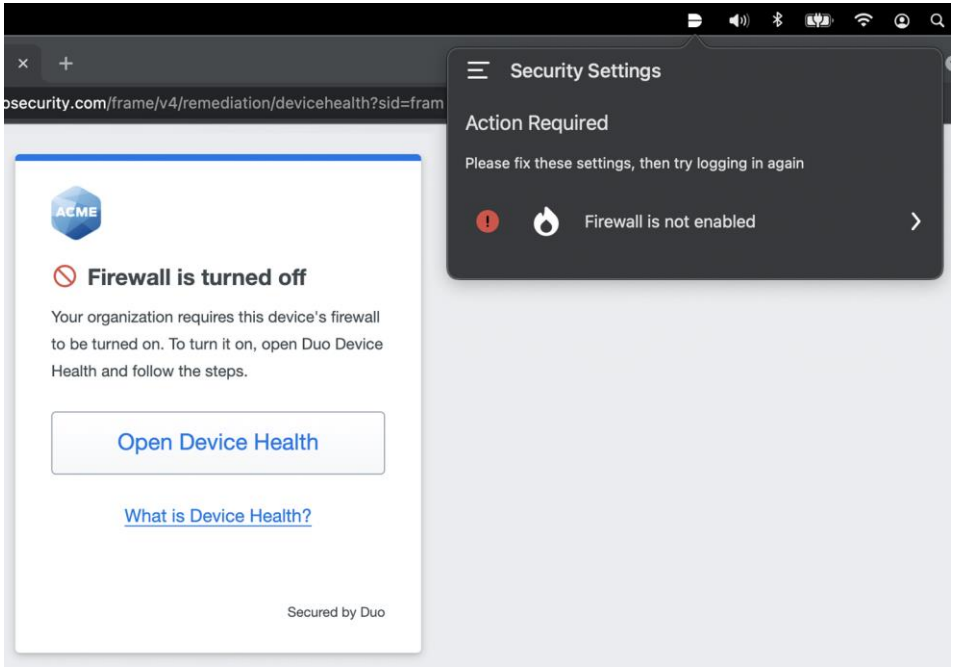
Enforce Posturing for Managed and Non Managed Devices



What is the Device Health Application?

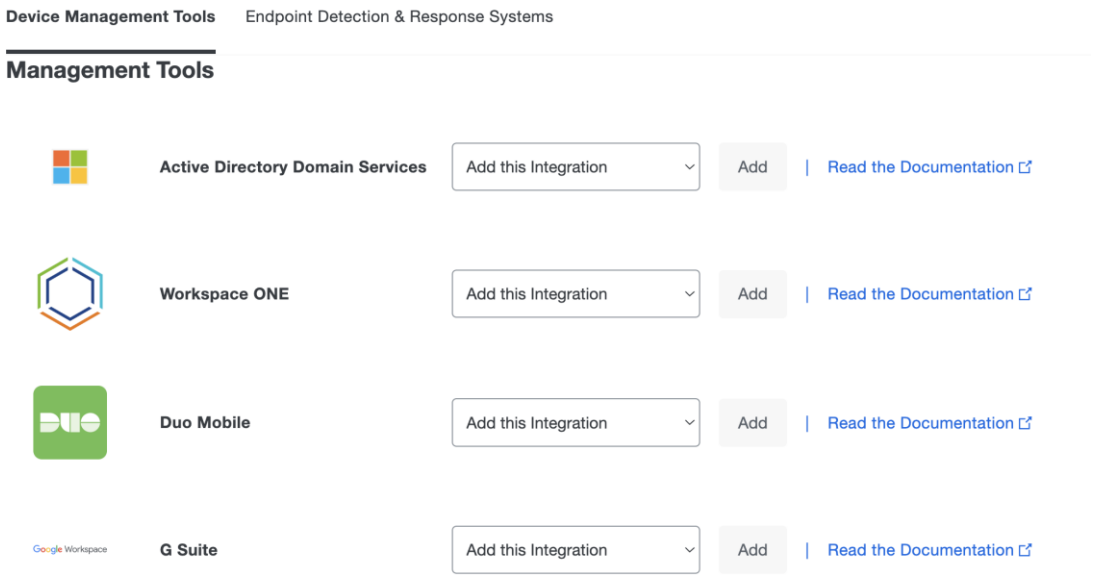
Verify at the point of authentication





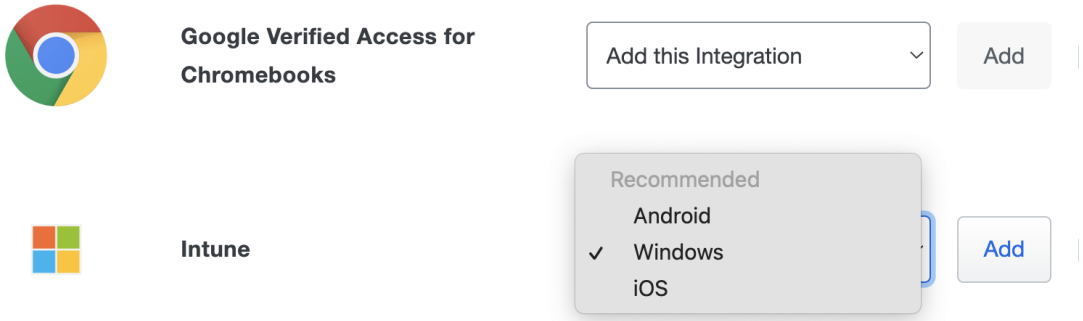
Configuring Duo MDM and Device Management

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



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



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

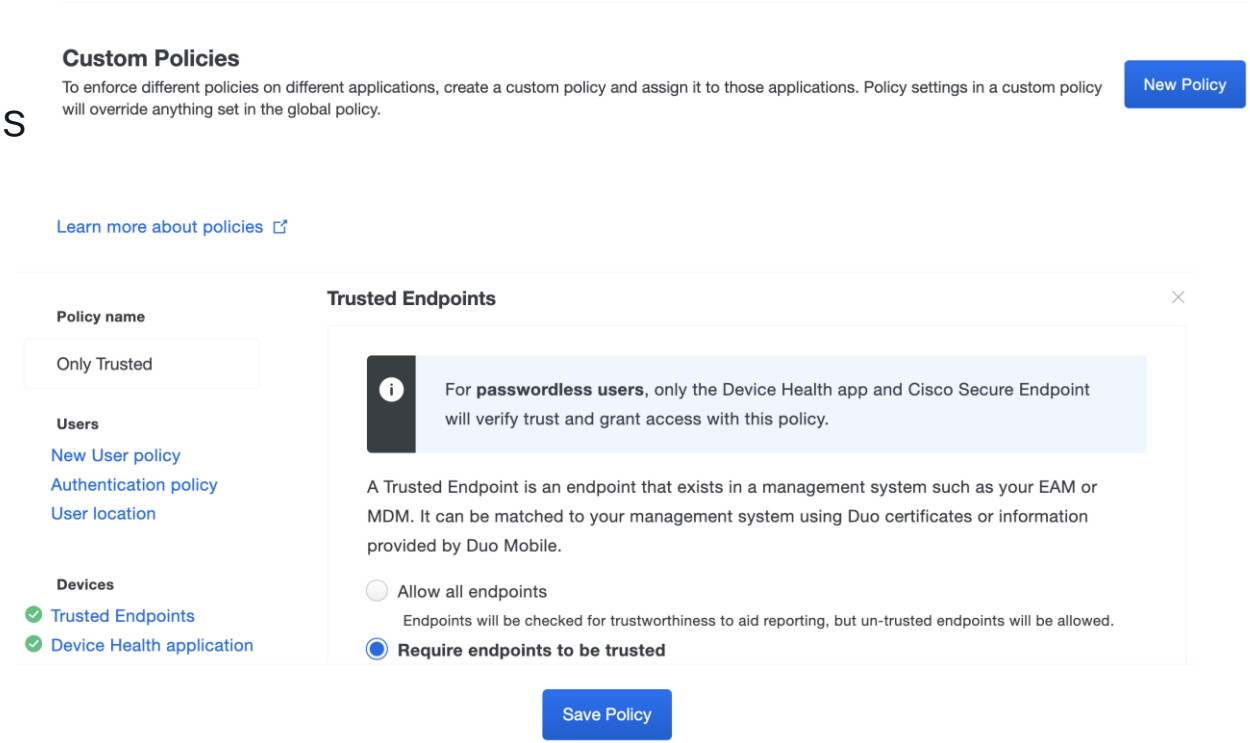
Duo Policy

Duo Policies

Highest Takes Precedence

Duo Policy Configuration

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



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

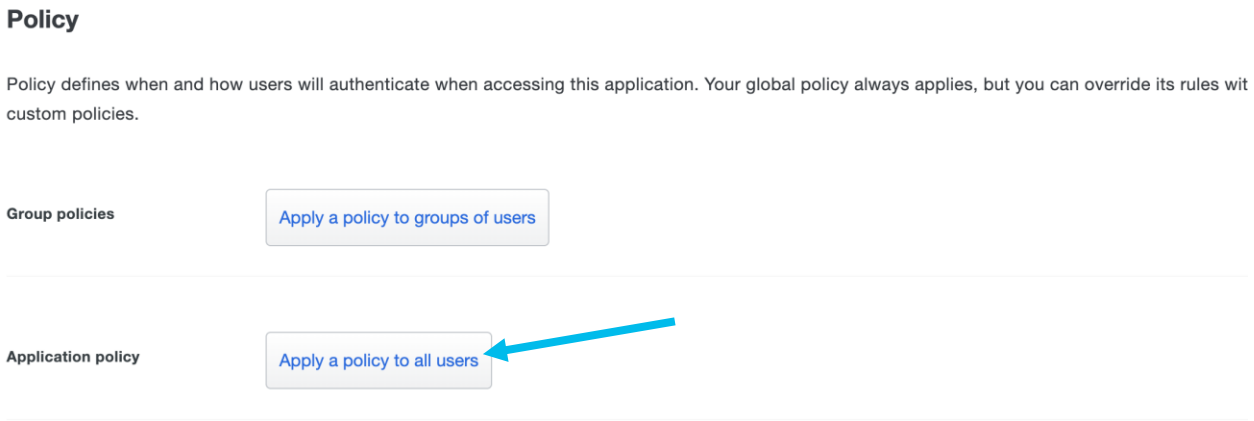
Duo Policy Configuration

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

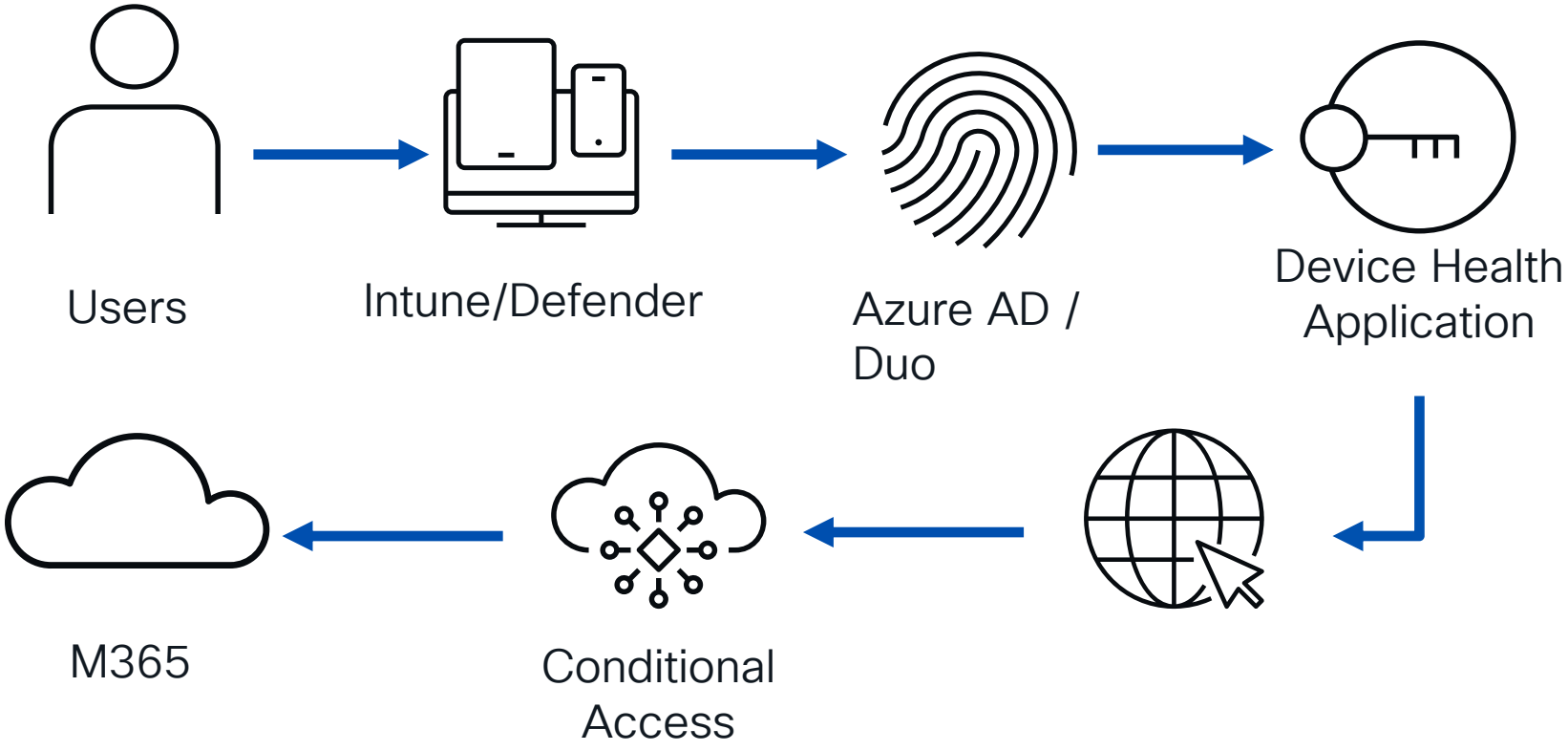
1. Go to Applications and find your Azure application
2. Select and apply your newly created policy at the application level



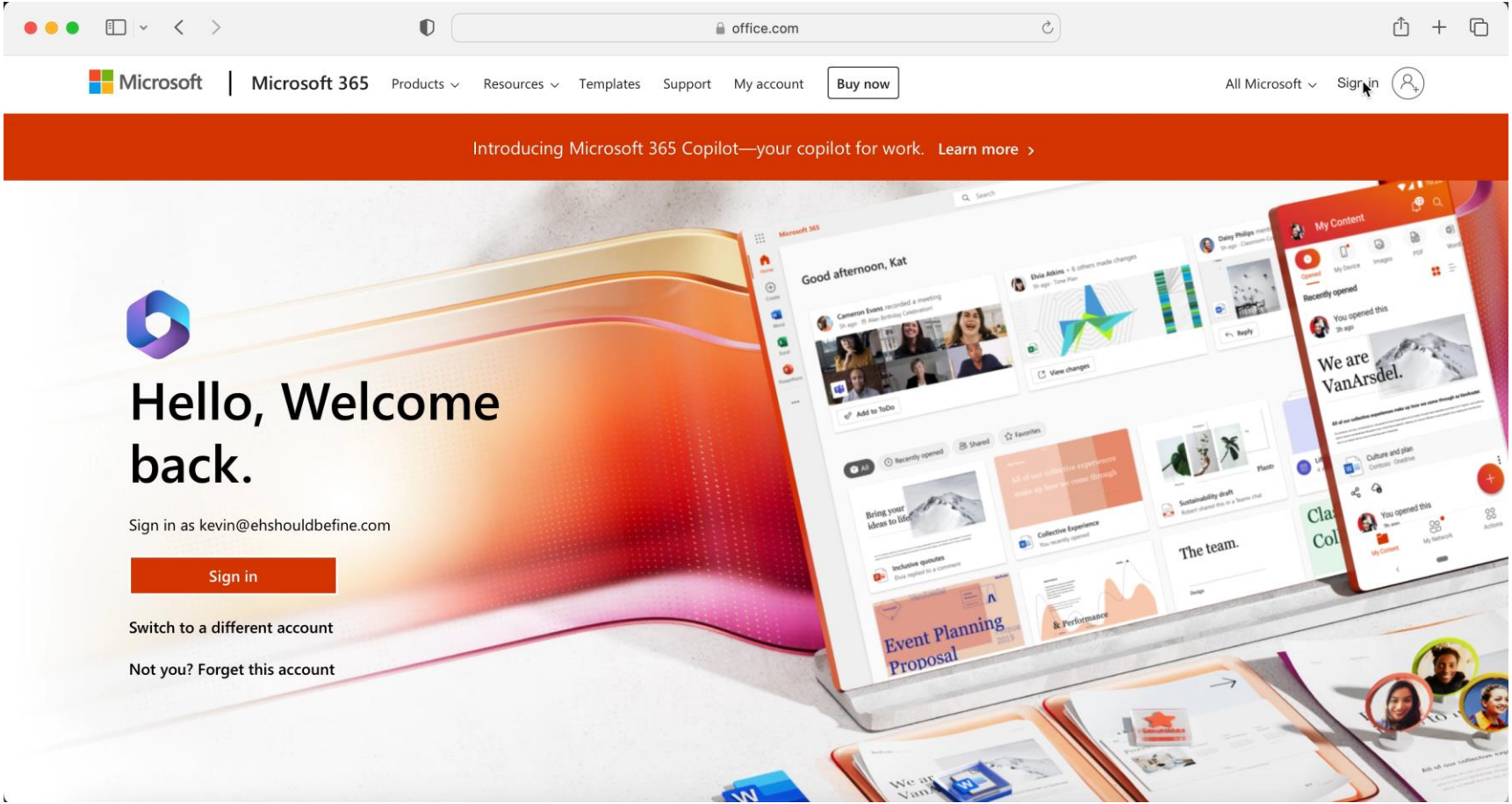
End State

- 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



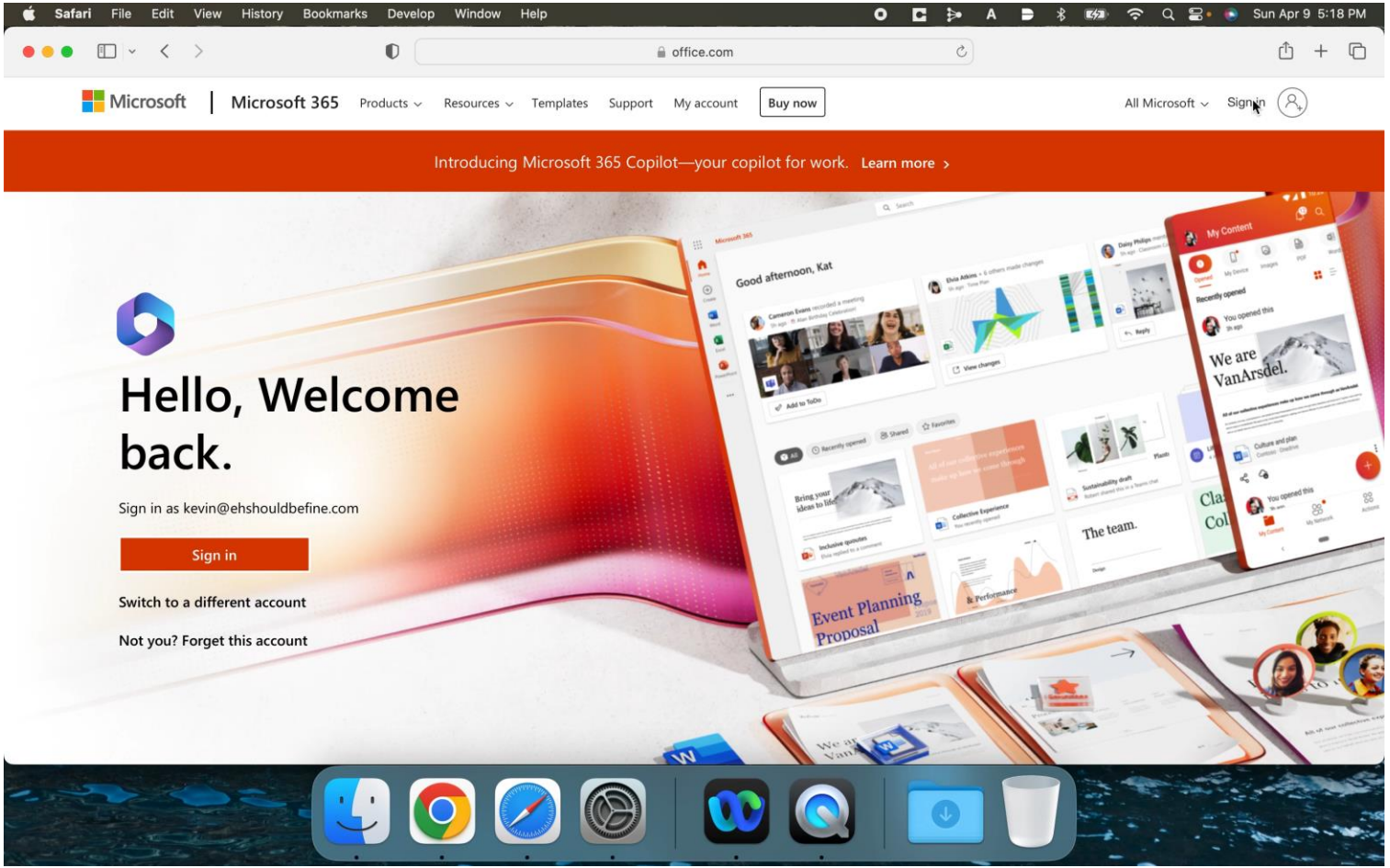
Untrusted Access Attempt – M365



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	Normal	Mac OS X 13.3.1 (22E261) As reported by Device Health Hostname KEVPATRI-M-70HW Safari 16.4 Flash Not installed Java Not installed Device Health Application Installed Firewall On Encryption On Password Set Security Agents Running: Cisco Secure Endpoint Napa, CA, United States 75.10.1.159 Not a Trusted Endpoint determined by Device Health

Firewall Disabled Attempt Trusted Device – M365

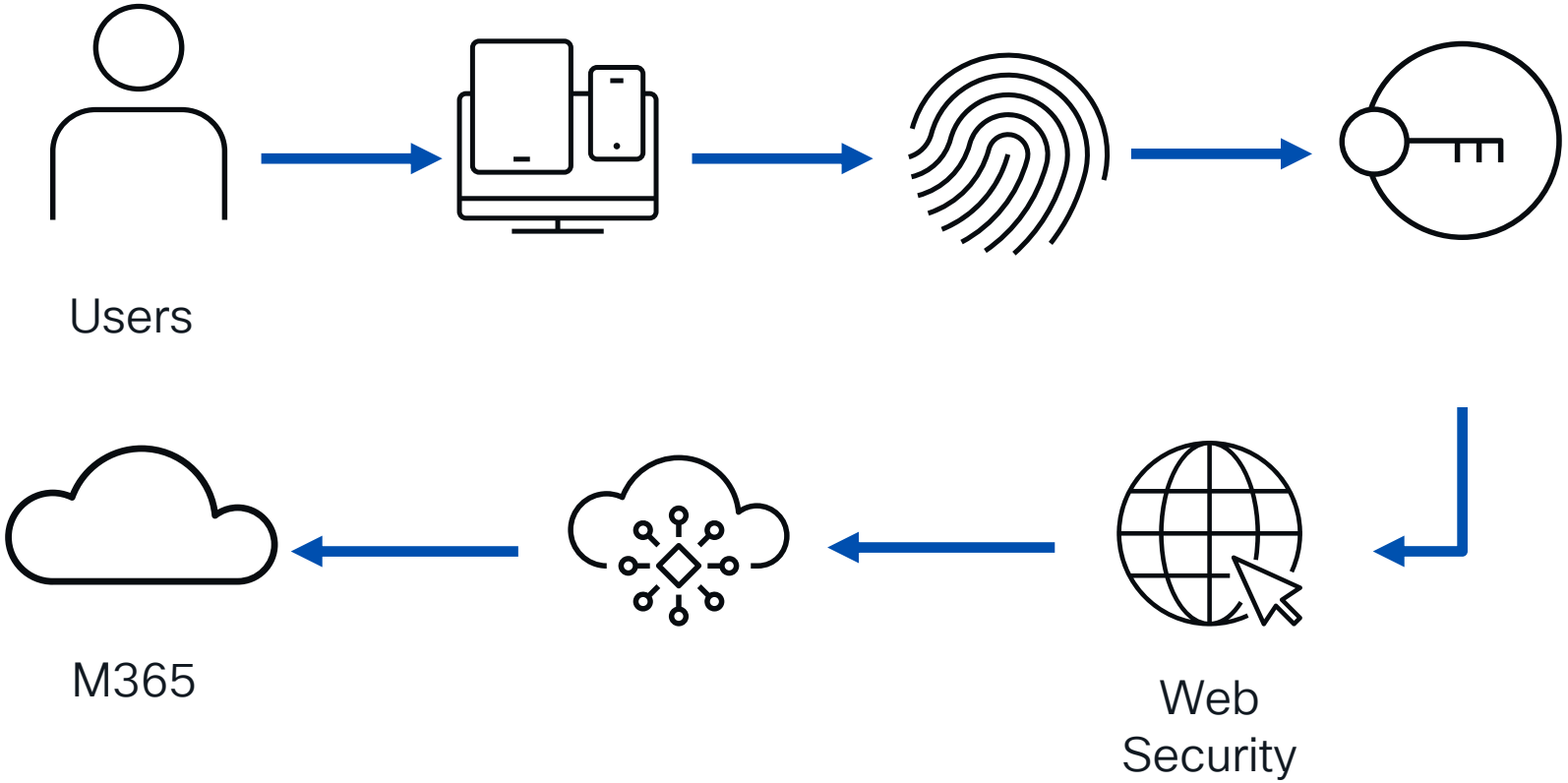


Duo And Microsoft

- 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

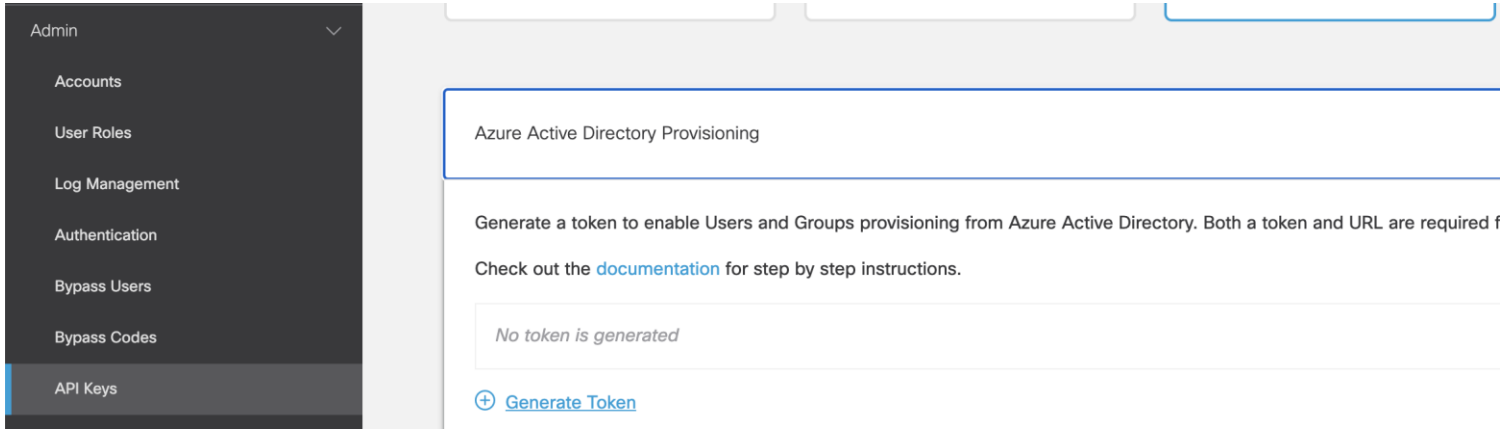
Identity

1. Provision Azure AD Users

Azure AD Users

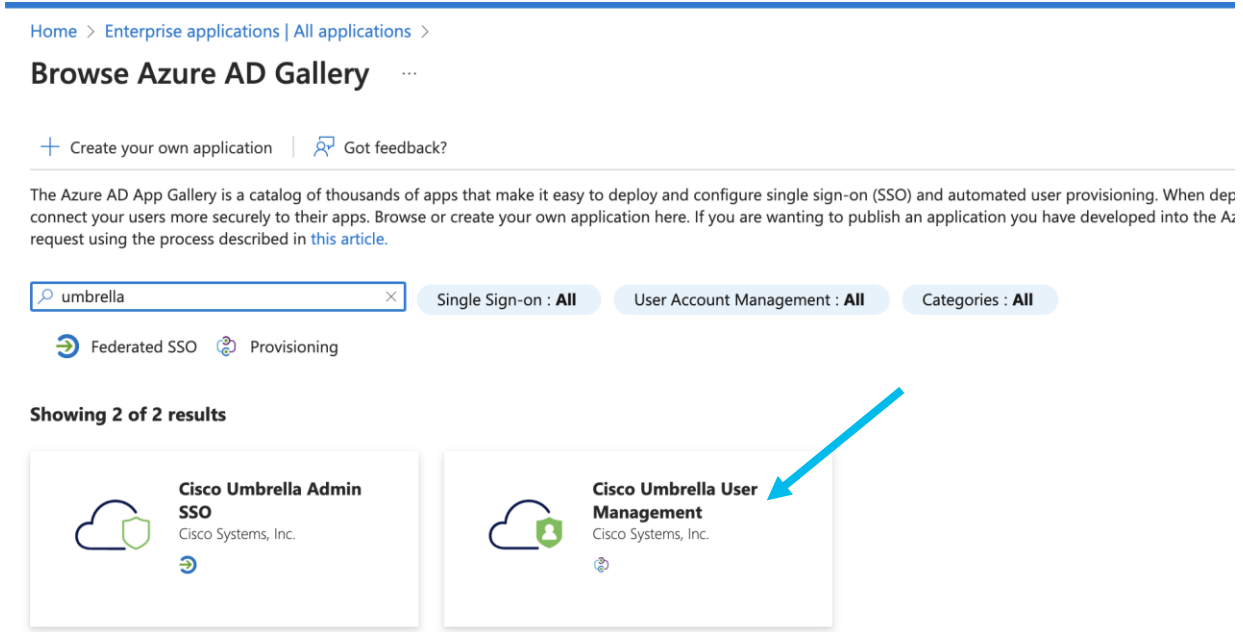
Azure AD Provisioning

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



Azure AD Provisioning

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



Azure AD Provisioning

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

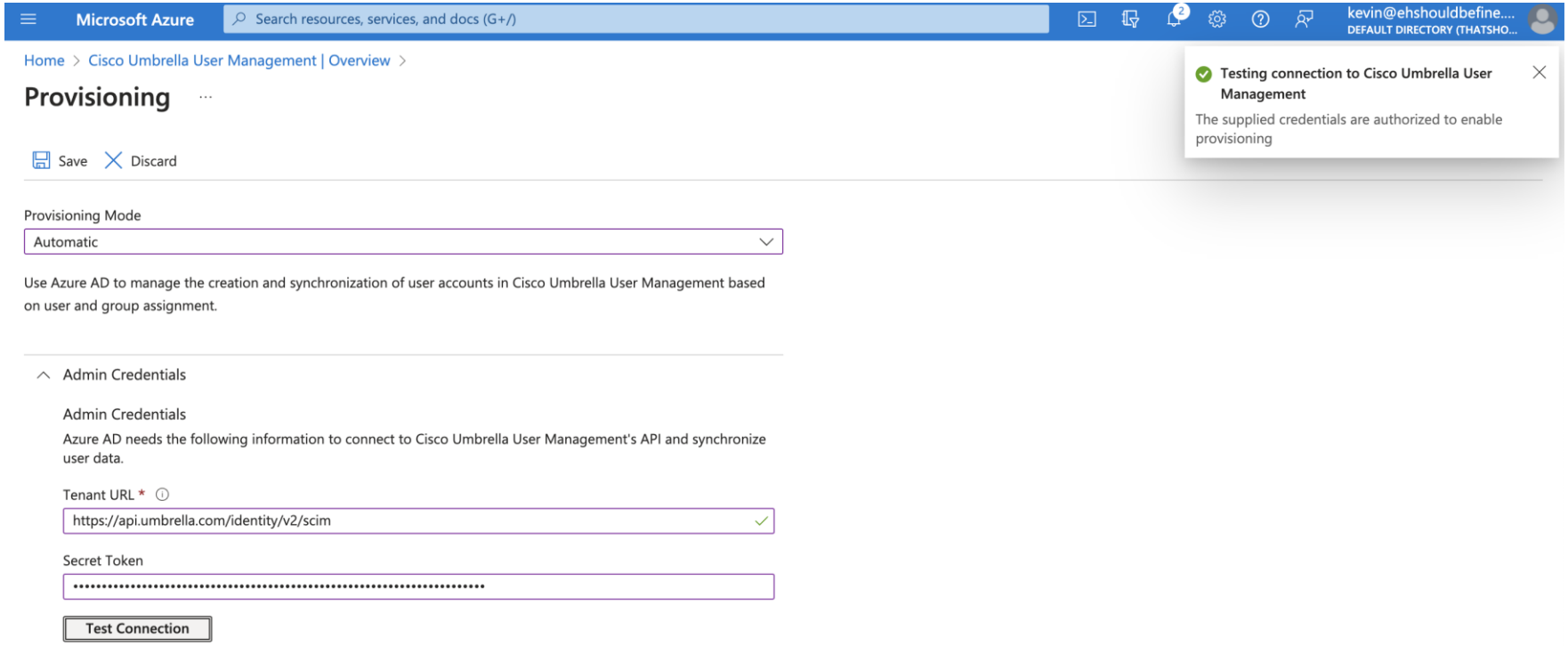
Automate identity lifecycle management with Azure Active Directory

Automatically create, update, and delete accounts when users join, leave, and move within your organization. Learn more.

Get started

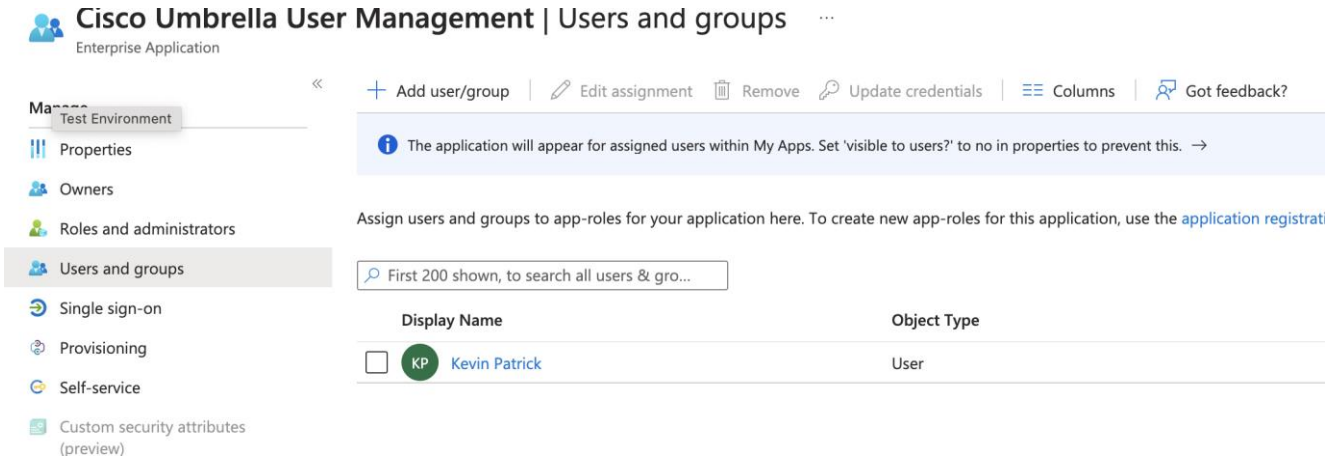
Azure AD Provisioning

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



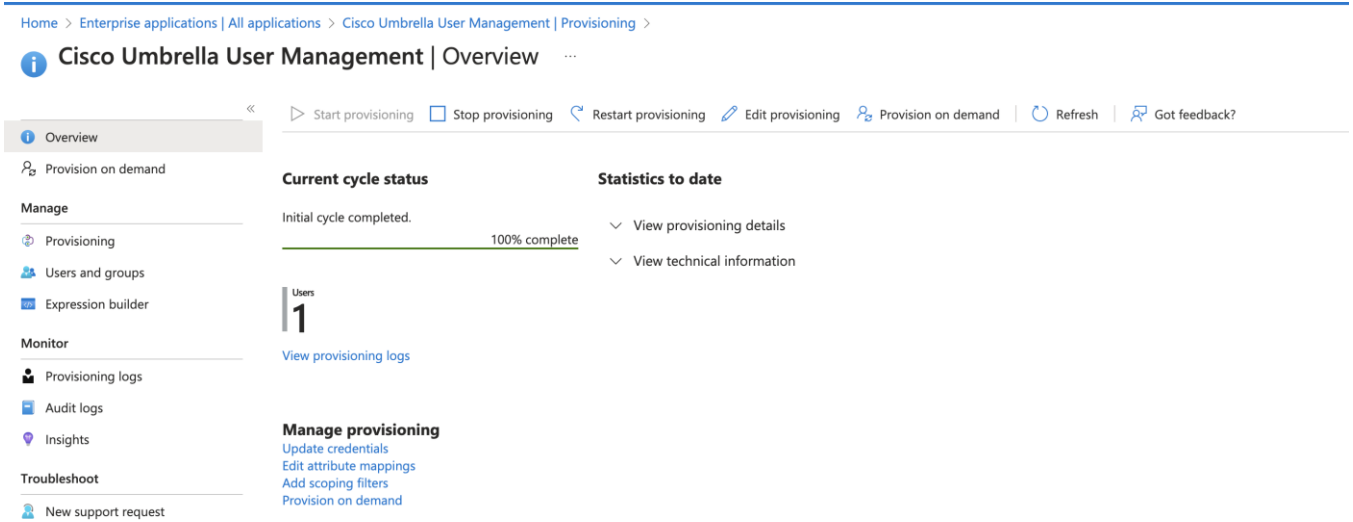
Azure AD Provisioning

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



Azure AD Provisioning

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



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)

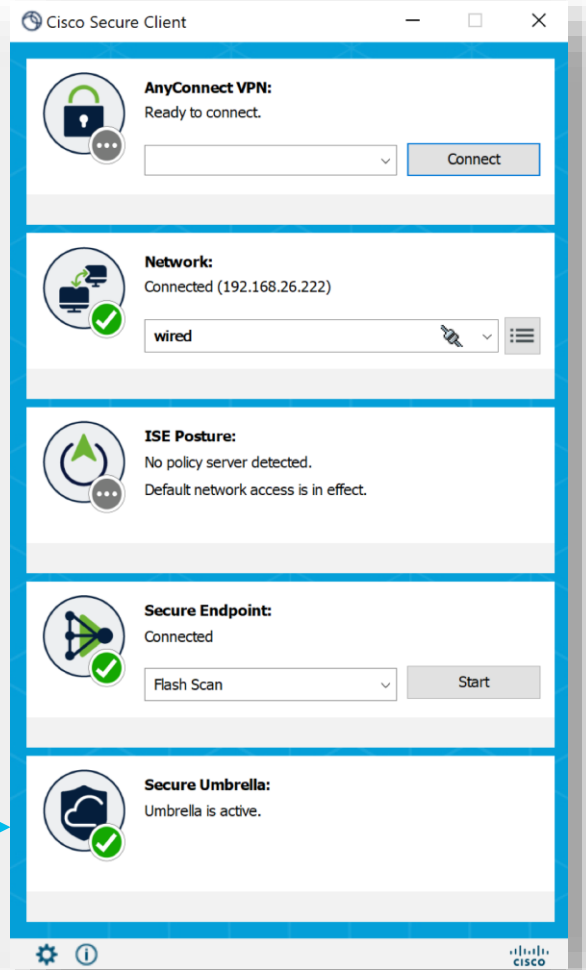
SIG Web Policy – Prerequisites

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

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

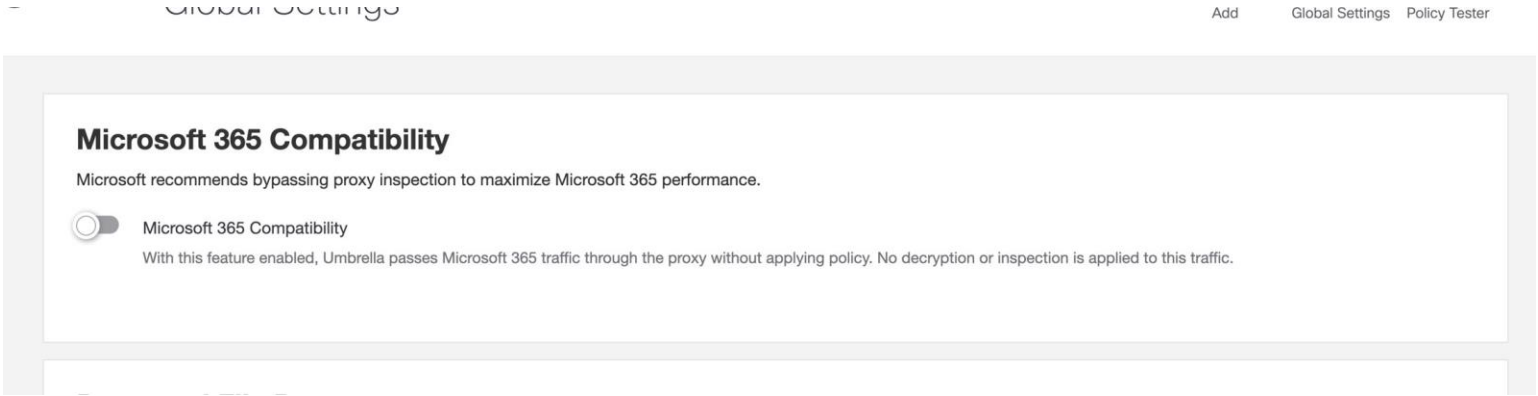
Step 3

Application Protection

1. Tenant Controls
2. Web Policy

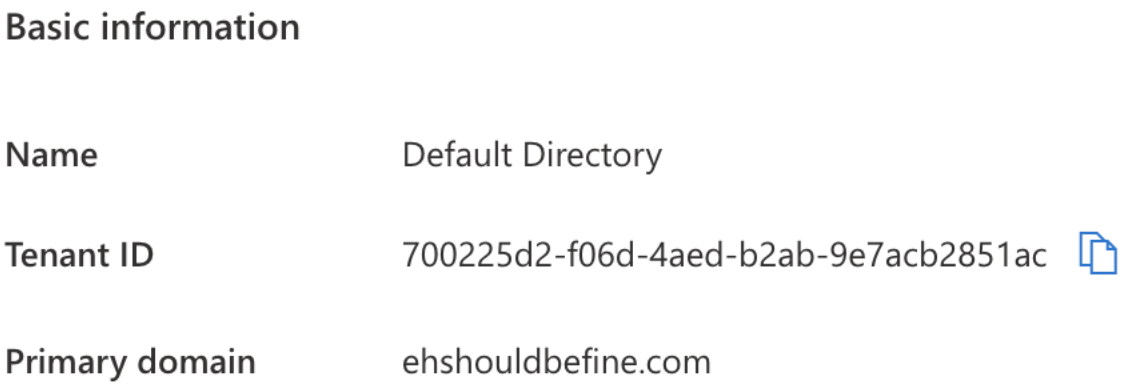
Tenant Controls

Microsoft Compatibility



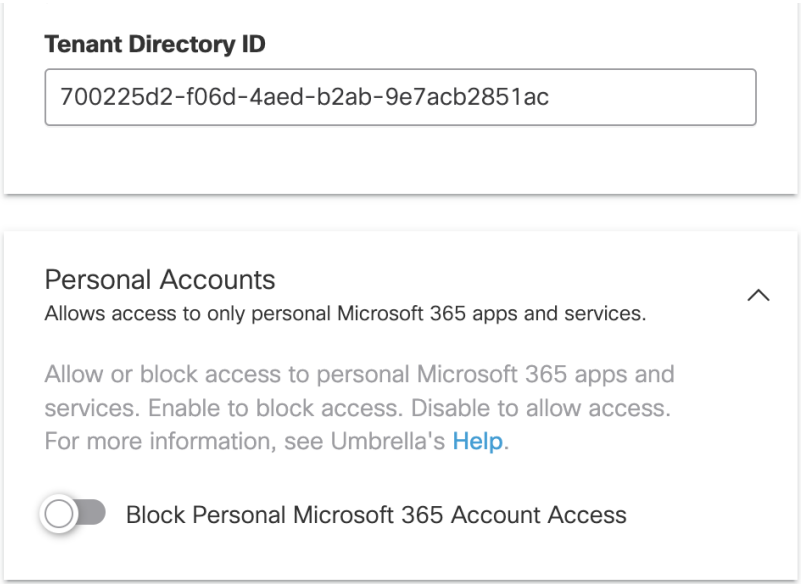
Microsoft Tenant Controls

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



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



Configure Web Policy

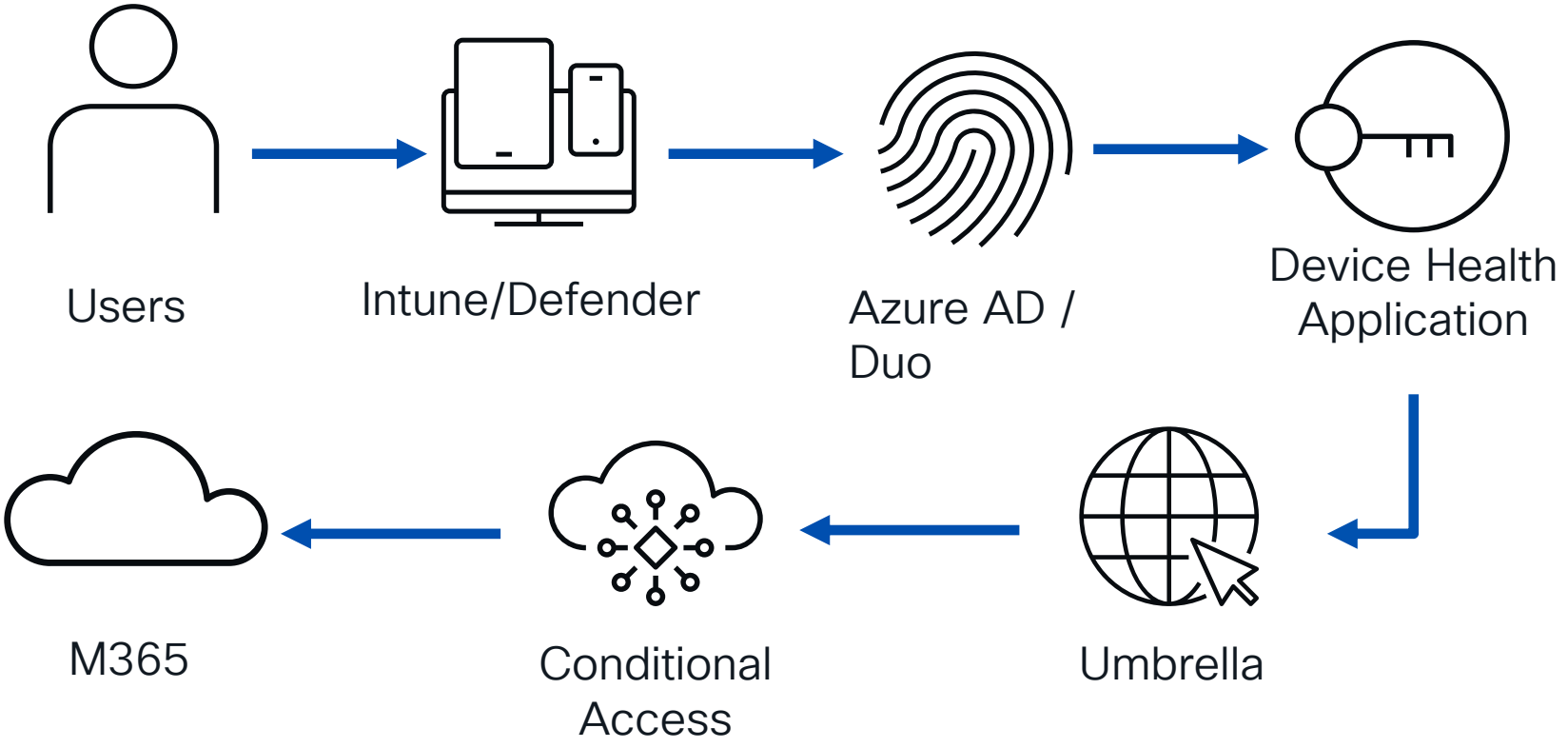
1. Go to Policies > Web Policy
2. Enable HTTPS Inspection
3. Add rule sets for custom identities

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

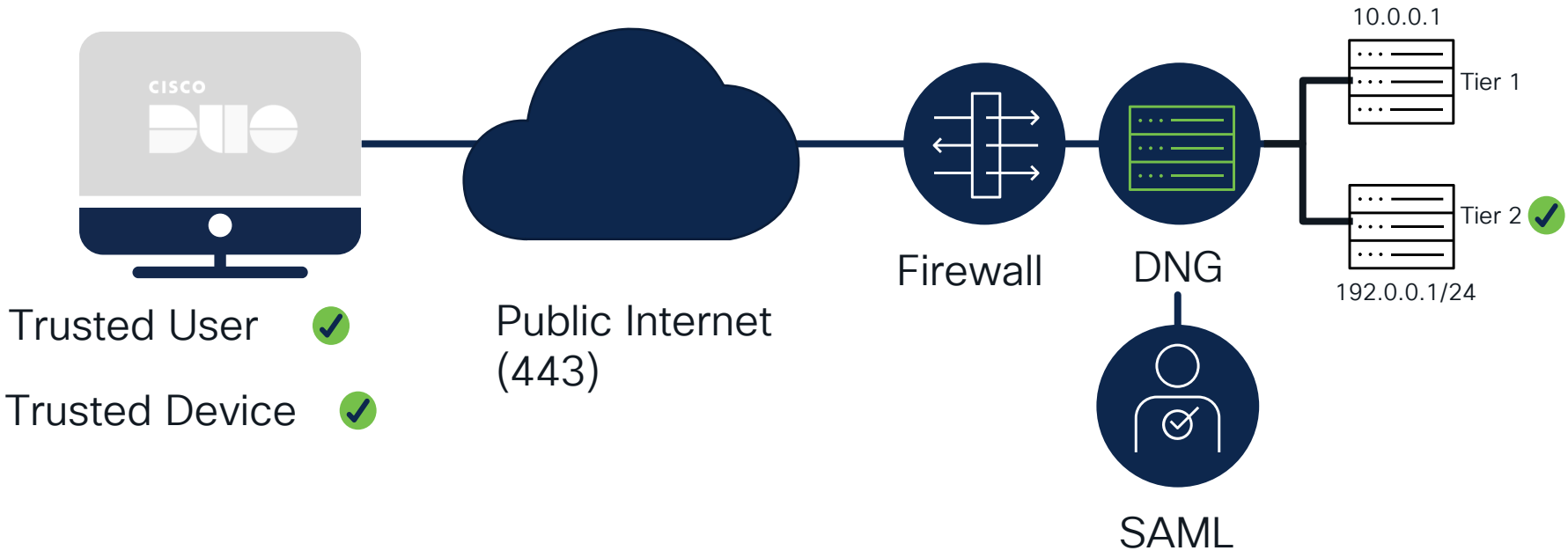
VPNless

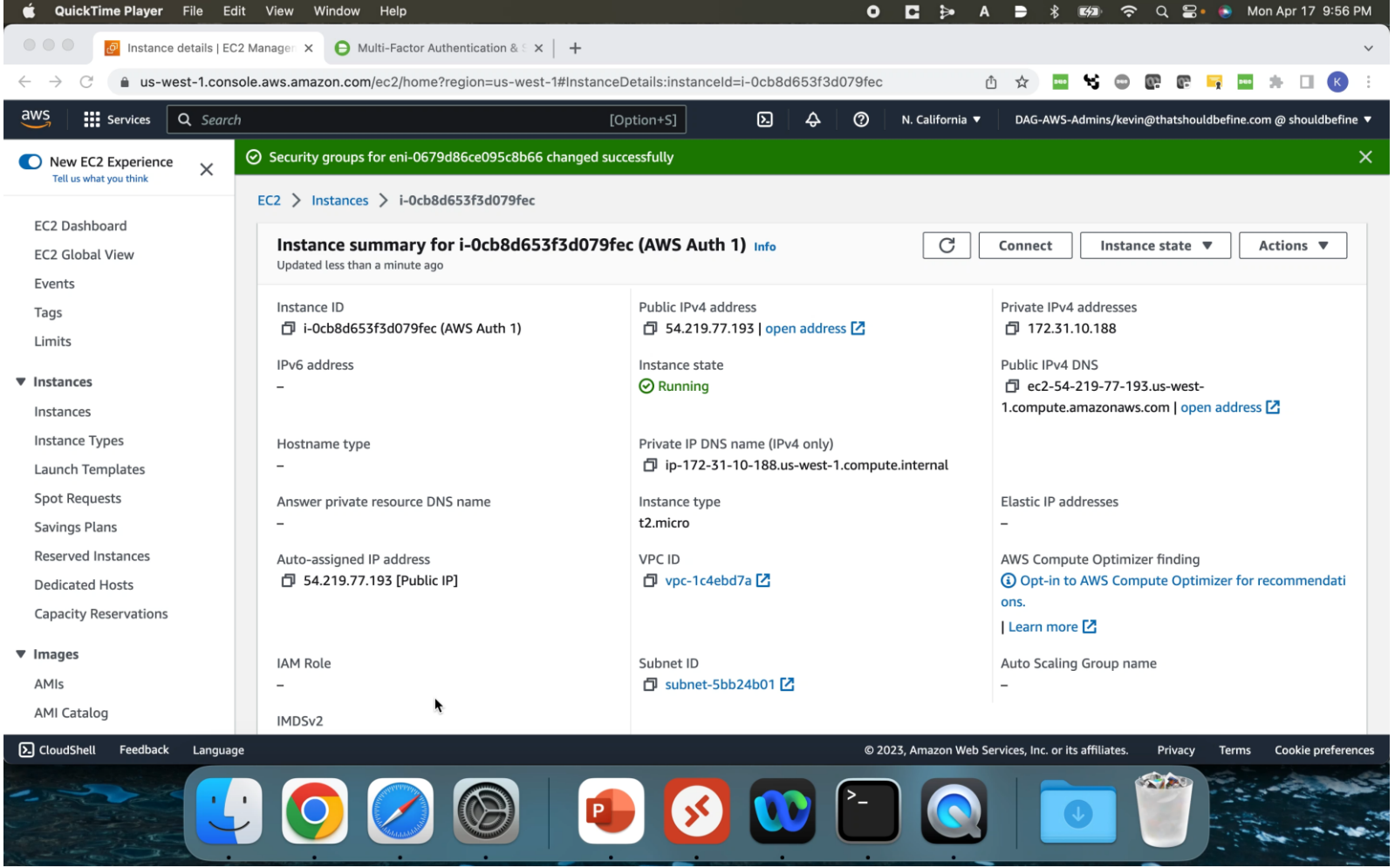
- Duo Network Gateway
- HTTPS applications
- No tunneling required

VPN Required

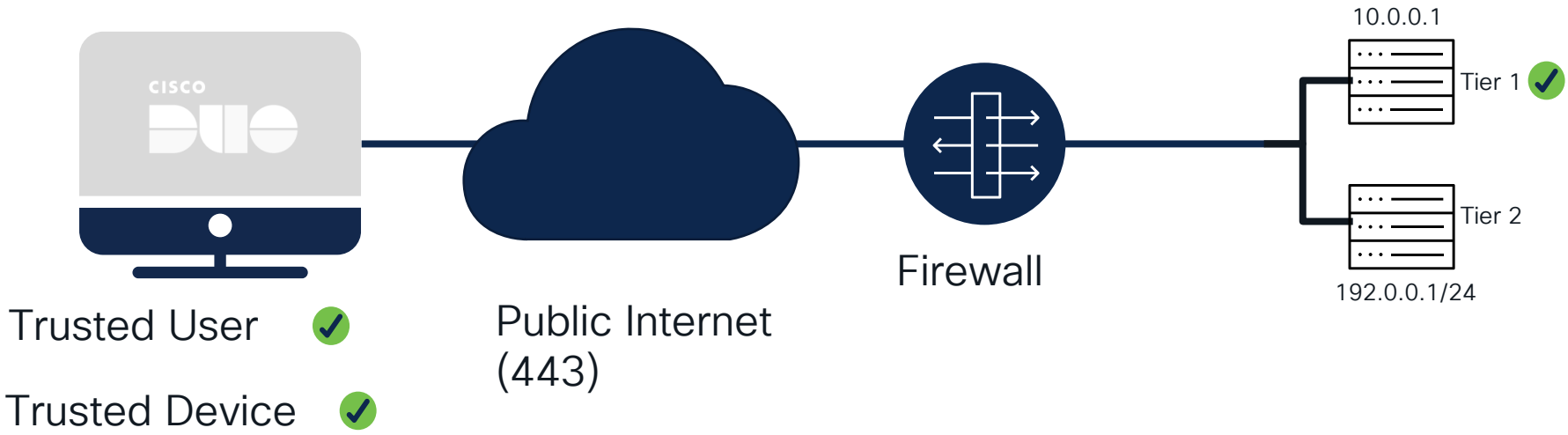
- Secure Client w/ Anyconnect and Firepower
- Legacy applications
- Pending application onboarding

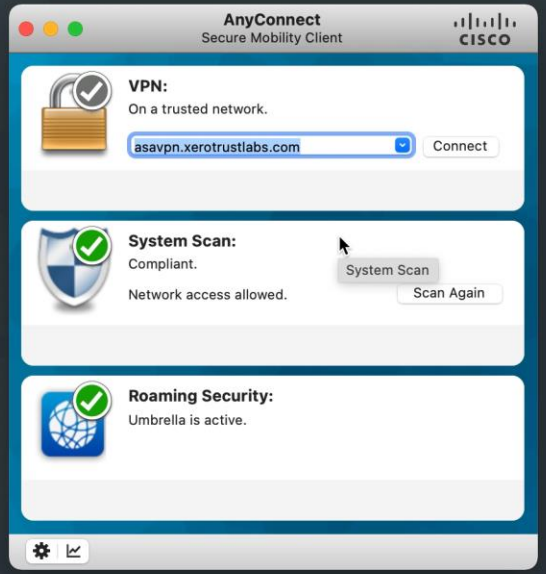
Duo Network Gateway



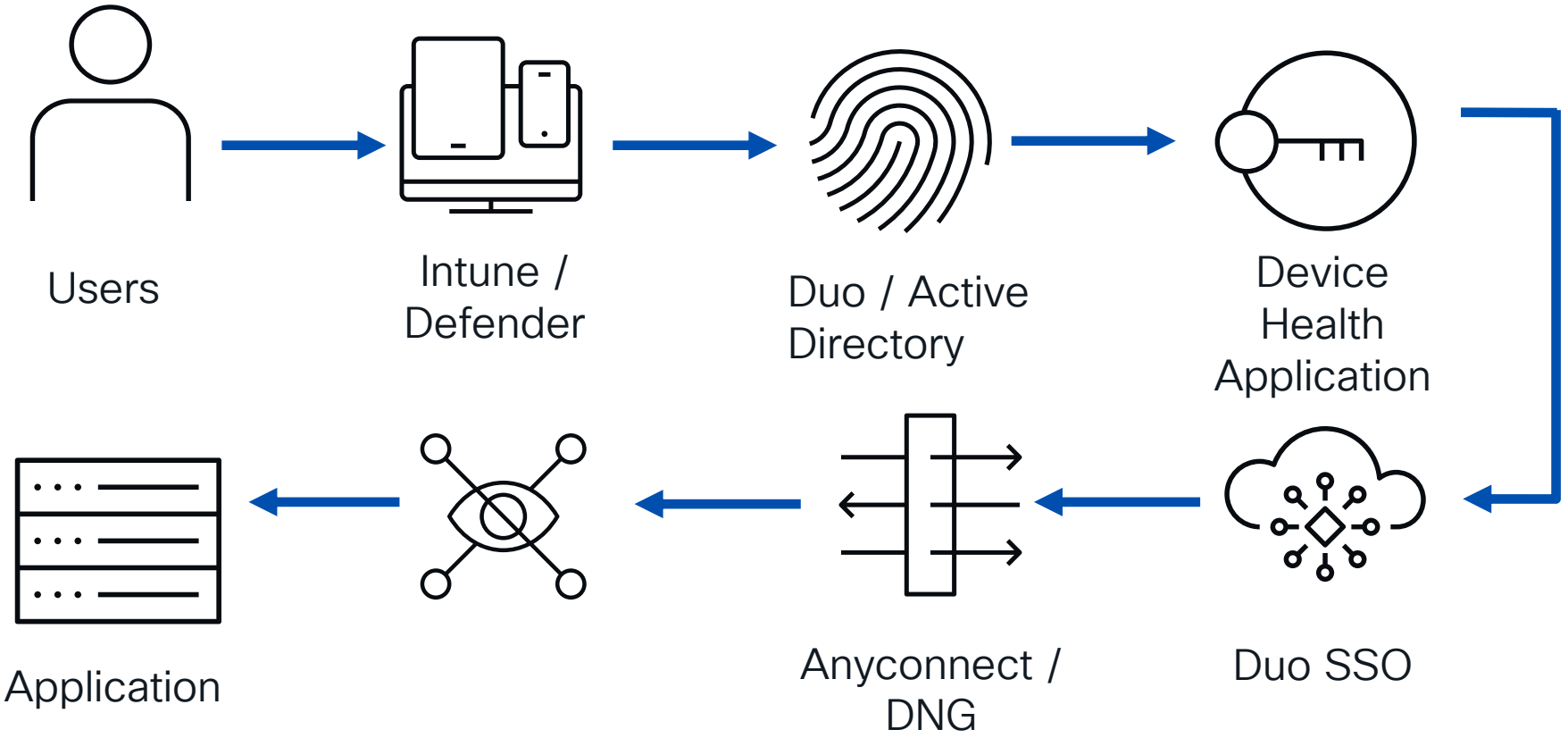


Secure Client





Remote User Accessing On Prem



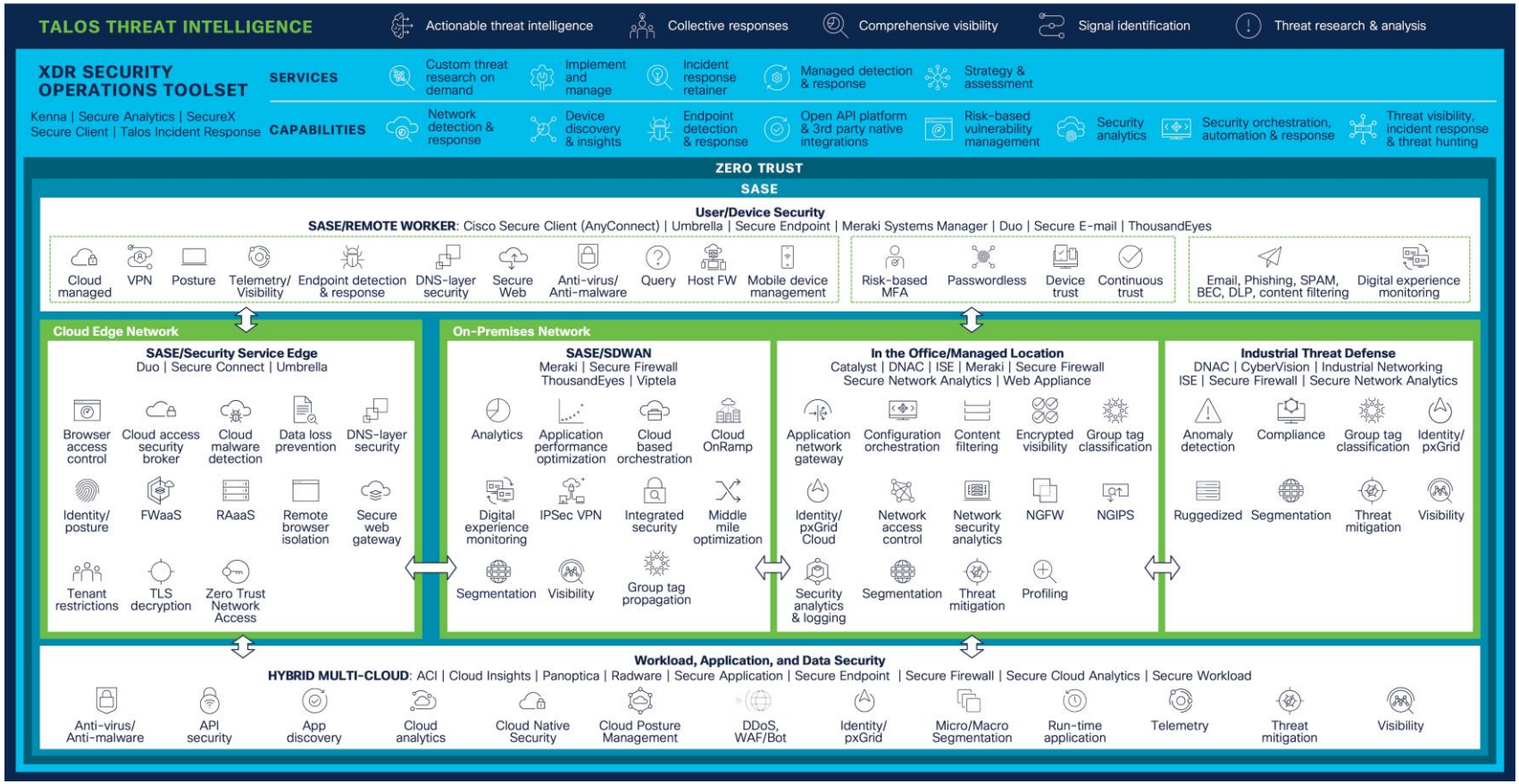
Reference Architectures

cisco SECURE

Security Reference Architecture

cisco.com/go/sra

v3.1

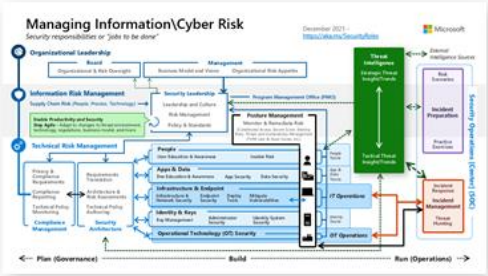


Microsoft Cybersecurity Reference Architectures (MCRA)

Capabilities
What cybersecurity capabilities does Microsoft have?

Build Slide

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



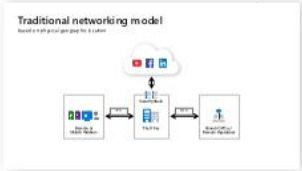
Zero Trust User Access
How to validate trust of user/devices for all resources?

Azure Native Controls
What native security is available?

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?



Attack Chain Coverage
How does this map to insider and external attacks?

Build Slide

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.

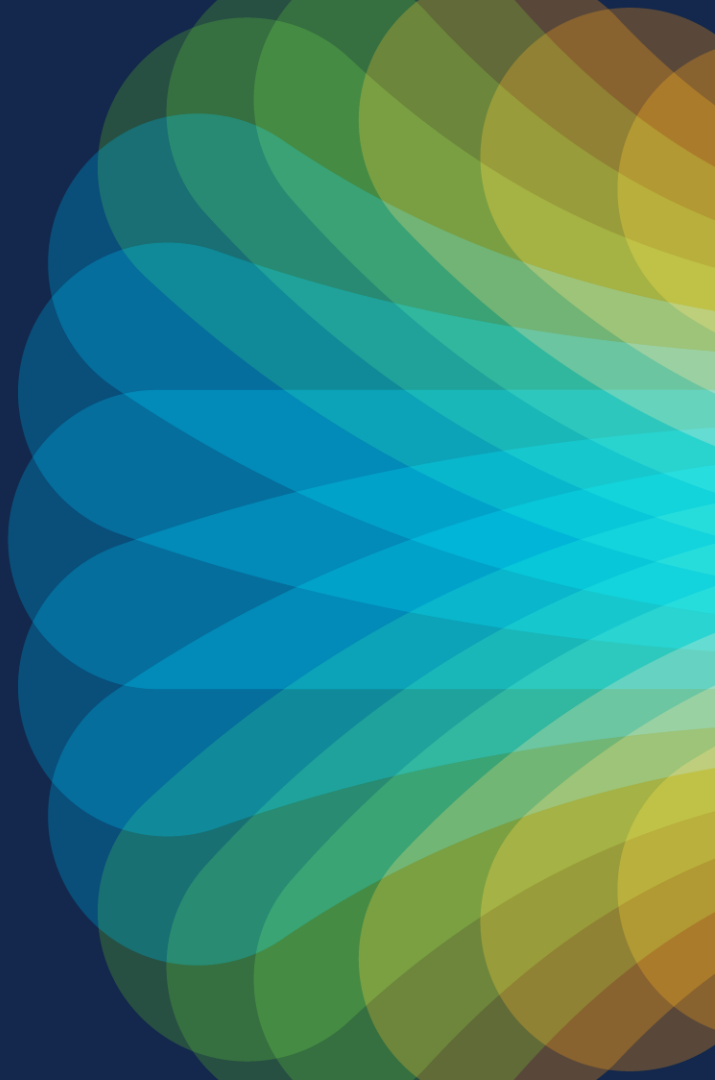
These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- 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



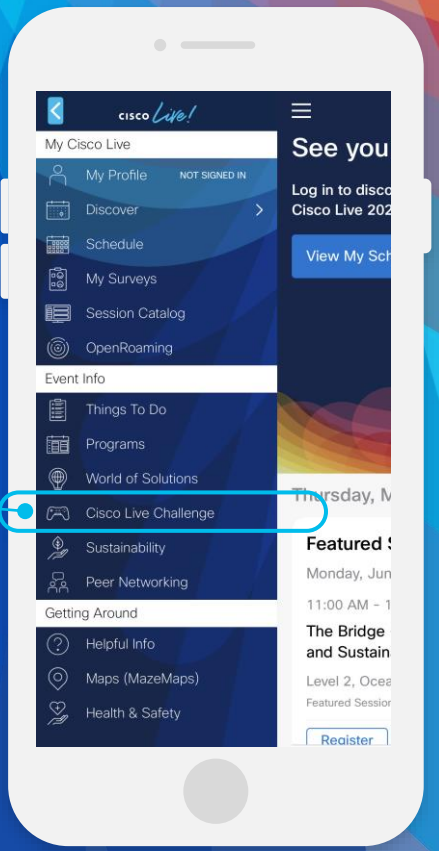
Cisco Live
Challenge

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:




cisco Live!
Let's go
#CiscoLive