GUIDE

SECURE ACCESS WITH CISCO DUO

Portal User Guide

Spectrum ENTERPRISE™

Table of contents

Table of contents

Getting started

About Secure Access with Cisco Duo Portal

The Duo Admin Portal allows administrators to view and configure most aspects of their Secure Access with Cisco Duo service, including:

- Dashboard view of user activity and Duo account health assessment
- View and manage user enrollment and activity
- View and set policies for the devices that are accessing corporate resources

Quick links

Duo Knowledge Base

Knowledge Base | Duo Security

Resources for Administrators

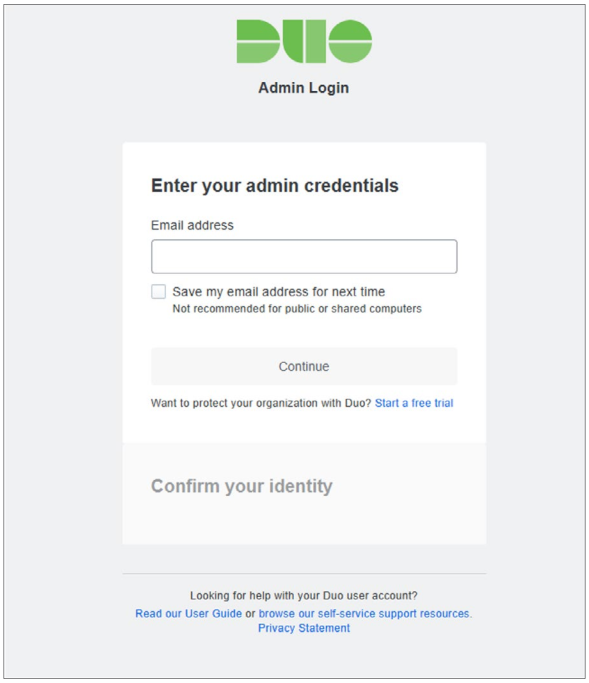
Duo Customer Support | Duo Security

Resources for End Users

Duo Customer Support | Duo Security

Logging in

Log into Duo Admin Portal with the credentials provided during the service activation process.



Admin Login

Enter your admin credentials

Email address

□ Save my email address for next time
Not recommended for public or shared computers

Continue

Want to protect your organization with Duo? Start a free trial

Confirm your identity

Looking for help with your Duo user account?
Read our User Guide or browse our self-service support resources.
Privacy Statement

Upon login, the Duo **Dashboard** is displayed.

Duo Dashboard

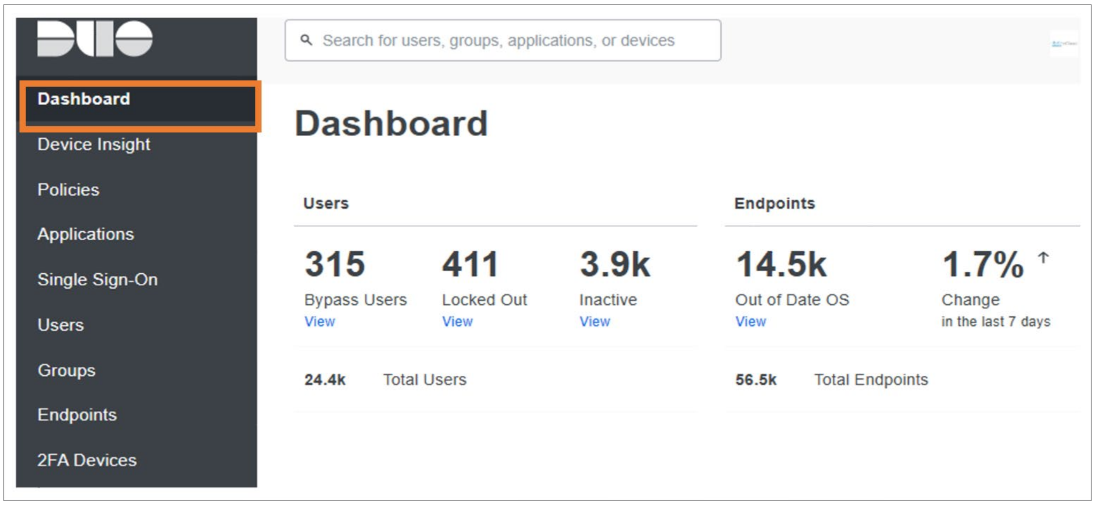
The dashboard provides visibility into the users and devices that are accessing corporate resources.

Using the Duo Dashboard

The Duo Dashboard is the landing page of the portal upon login.

1. The **User** section of the dashboard is a summary view of user activity.
Click View to see an inventory of users and their last log in.

- **Bypass Users** — count of users that are currently authenticated and actively using an application integrated with Cisco Duo.
- **Locked Out** — count of users that were locked out during the authentication process and may require immediate attention.
- **Inactive** — count of licensed users not using the application.
- **Total Users** — count of all licensed users



Dashboard

Users

315 Bypass Users View

411 Locked Out View

3.9k Inactive View

24.4k Total Users

Endpoints

14.5k Out of Date OS View

1.7% ↑ Change in the last 7 days

56.5k Total Endpoints

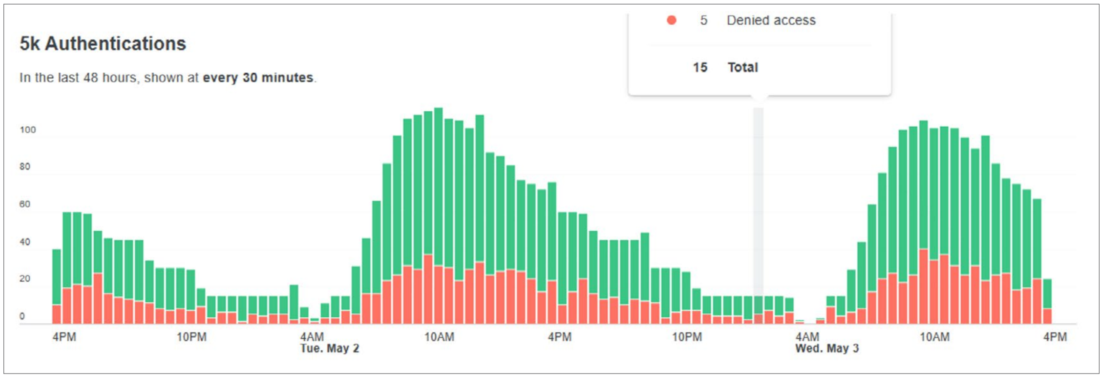
2. The **Endpoints** section is a summary view of endpoint device health.
Click View to see a detailed inventory of operating systems by platform.

- **Out of date OS** — count of endpoints that have an outdated OS.
- **Total endpoints** — count of all devices Number of devices (endpoints) enrolled.

3. The **Authentication** section is a summary of authentications for a given period of time.
Use the mouse to hover over a bar in the histogram to see authentication details for a specific time period.

The graph displays the following information:

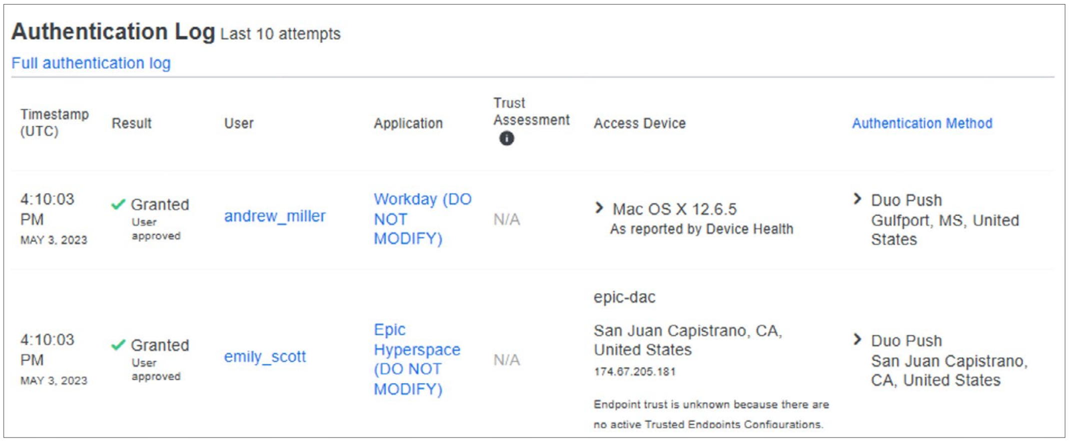
- Total number of authentications
- Time period (represented by selected bar).
- Number of users **Granted Access**.
- Number of users **Denied Access**



4. The **Authentication Log** section provides details on the log in attempts including:

- Time of log in
- Log in result
- User
- The application the user was logging into
- Whether the device is trusted (managed)
- Device used to access the application
- Authentication method and location

5. **Click** on any of the **blue** text for detailed information.



Authentication Log Last 10 attempts

Full authentication log

Timestamp (UTC)	Result	User	Application	Trust Assessment	Access Device	Authentication Method
4:10:03 PM MAY 3, 2023	✓ Granted User approved	andrew_miller	Workday (DO NOT MODIFY)	N/A	› Mac OS X 12.6.5 As reported by Device Health	› Duo Push Gulfport, MS, United States
4:10:03 PM MAY 3, 2023	✓ Granted User approved	emily_scott	Epic Hyperspace (DO NOT MODIFY)	N/A	epic-dac San Juan Capistrano, CA, United States 174.67.205.181 Endpoint trust is unknown because there are no active Trusted Endpoints Configurations.	› Duo Push San Juan Capistrano, CA, United States

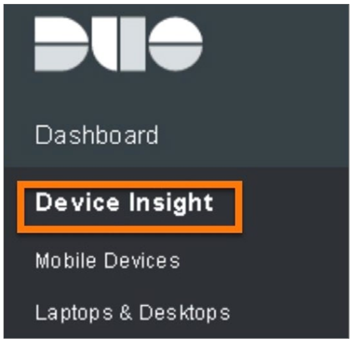
Device Insights

The Device Insight section of the Duo Admin portal provides IT Administrators with a view of the devices accessing the network.

There are 3 views within the Device Insight section:

- Device Insight (overview)
- Mobile devices
- Laptops and desktops

1. From the **Admin Panel**, select **Device Insight** to display the **Device Insight** screen.



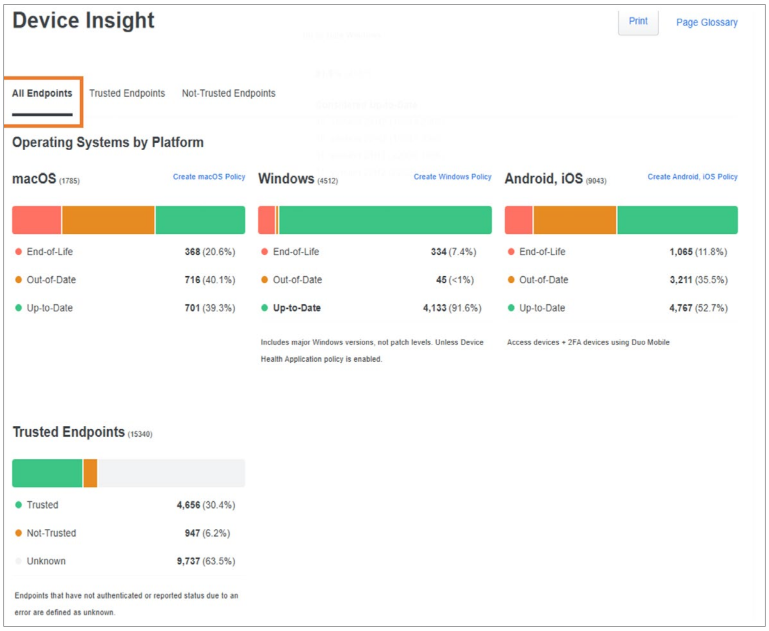
Device Insight (overview)

The Devices Insight Overview section is a high level overview of all devices and operating systems accessing their corporate applications such as laptops and desktops as well as mobile devices, including those used to perform multi-factor authentication.

Click on **Page Glossary** in the upper right hand corner to see the Cisco definition of End of Life, Out of Date and Trusted Endpoints

1. The Operating System by Platform section is a summary of Operating System (OS) status for **All Endpoints** by default.

NOTE: This view can also be filtered to see only data pertaining to Trusted or Non-trusted Endpoints by clicking on **Trusted Endpoints** or **Non-Trusted Endpoints**.



Device Insight

Operating Systems by Platform

macOS (1785)

● End-of-Life	**368** (20.6%)
● Out-of-Date	**716** (40.1%)
● Up-to-Date	**701** (39.3%)

Windows (4512)

● End-of-Life	**334** (7.4%)
● Out-of-Date	**45** (<1%)
● **Up-to-Date**	**4,133** (91.6%)

Includes major Windows versions, not patch levels. Unless Device Health Application policy is enabled.

Android, iOS (9043)

● End-of-Life	**1,065** (11.8%)
● Out-of-Date	**3,211** (35.5%)
● Up-to-Date	**4,767** (52.7%)

Access devices + 2FA devices using Duo Mobile

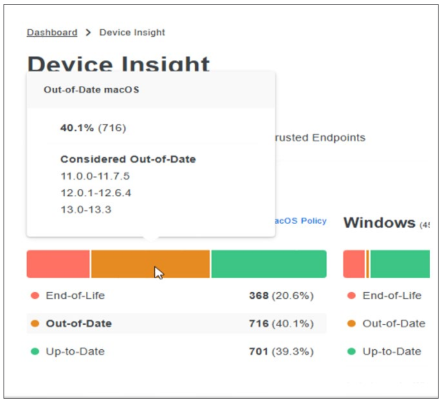
Trusted Endpoints (15340)

● Trusted	**4,656** (30.4%)
● Not-Trusted	**947** (6.2%)
● Unknown	**9,737** (63.5%)

Endpoints that have not authenticated or reported status due to an error are defined as unknown.

2. **Click** on **Print** button in the upper right hand corner to print device insight data just as it is displayed on this page.

3. Hover over the bar graph to see more granular details for the End-Of Life, Out-of-Date and Up-to Date devices.



Dashboard > Device Insight

Device Insight

Out-of-Date macOS

40.1% (716)

Considered Out-of-Date
11.0.0-11.7.5
12.0.1-12.6.4
13.0-13.3

rusted Endpoints

acOS Policy

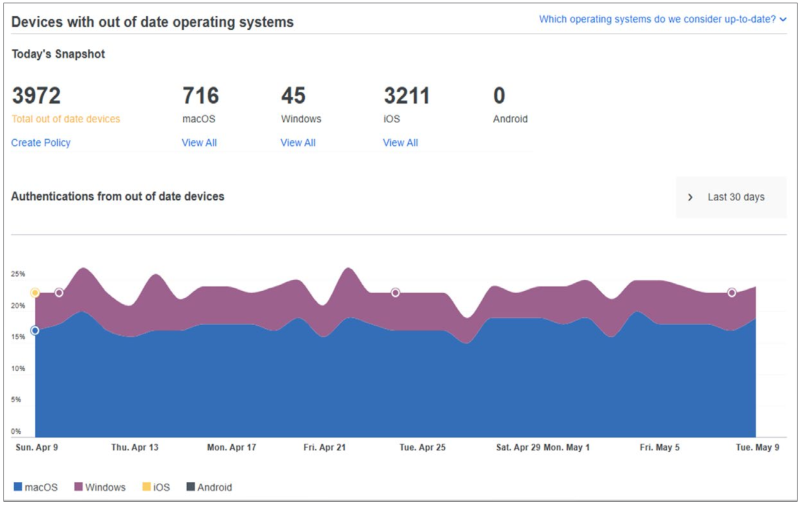
Windows (4!

● End-of-Life	**368** (20.6%)
● **Out-of-Date**	**716** (40.1%)
● Up-to-Date	**701** (39.3%)

● End-of-Life
● Out-of-Date
● Up-to-Date

4. Scroll down to see graphs that show how devices with out of date operating systems, browsers and plug ins have been trending over a specific time period.

NOTE: A recent software release corresponds to an uptick in out-of-date devices.



Devices with out of date operating systems

Which operating systems do we consider up-to-date?

Today's Snapshot

3972	716	45	3211	0
Total out of date devices	macOS	Windows	iOS	Android
Create Policy	View All	View All	View All	

Authentications from out of date devices

> Last 30 days

5. **Click** on **Which Operating systems do we consider up-to-date?** to see a list of OS versions by device that Cisco defines as current.

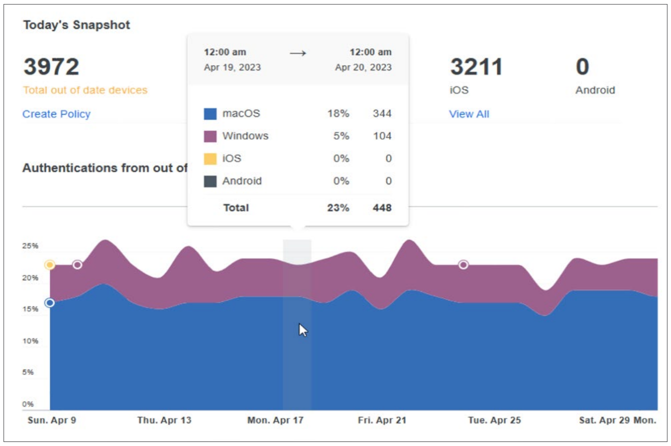
6. Toggle the **> Last 30 days** button to view a different time period (last 7 days or last 90 days).

7. **Click Create Policy** to set policies for device operating systems.

8. **Click View All** to see details for a specific device including:

- OS
- Browser
- Security Warnings
- User
- Time and date of log in attempt
- Whether the device is a managed (trusted) device

9. Hover over the graph to see detail on the % of devices detected during a specific time period.



Today's Snapshot

3972
Total out of date devices
Create Policy

3211
iOS
View All

0
Android

Authentications from out of

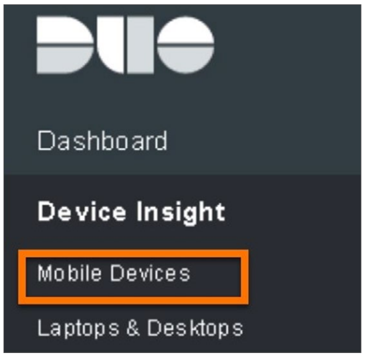
12:00 am Apr 19, 2023	→	12:00 am Apr 20, 2023
■ macOS	18%	344
■ Windows	5%	104
■ iOS	0%	0
■ Android	0%	0
Total	23%	448

10. The graphs for out-of-date browsers and out-of-date plug ins show the same data.

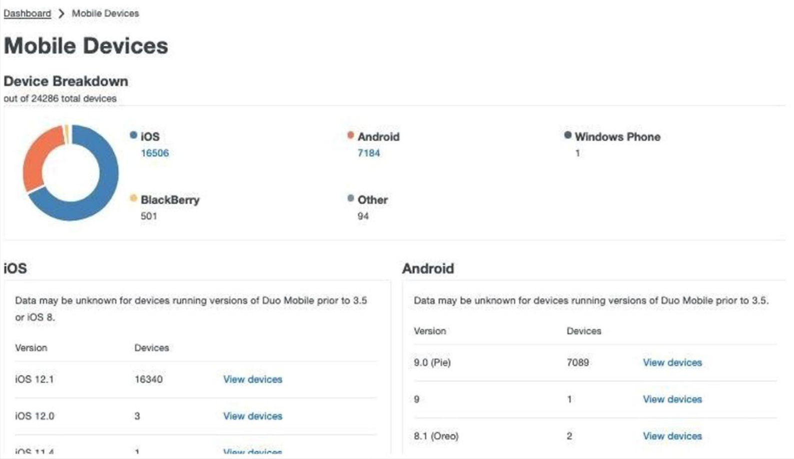
Mobile Devices

The Mobile Device section of the Duo Admin portal provides visibility to the types of mobile devices that are in use. This includes both devices that have the Duo Mobile application installed as well a devices accessing browser-based corporate resources that have been protected with Duo.

1. From the **Admin Panel**, select **Device Insight > Mobile Devices**.



2. View the **Device Breakdown** section of the page for a breakdown of the different OS platforms and granular detail with regards to the specific versions of both iOS and Android.



Dashboard > Mobile Devices

Mobile Devices

Device Breakdown
out of 24286 total devices

● iOS	16506
● Android	7184
● Windows Phone	1
● BlackBerry	501
● Other	94

iOS

Data may be unknown for devices running versions of Duo Mobile prior to 3.5 or iOS 8.

Version	Devices	
iOS 12.1	16340	View devices
iOS 12.0	3	View devices
iOS 11.4	1	View devices

Android

Data may be unknown for devices running versions of Duo Mobile prior to 3.5.

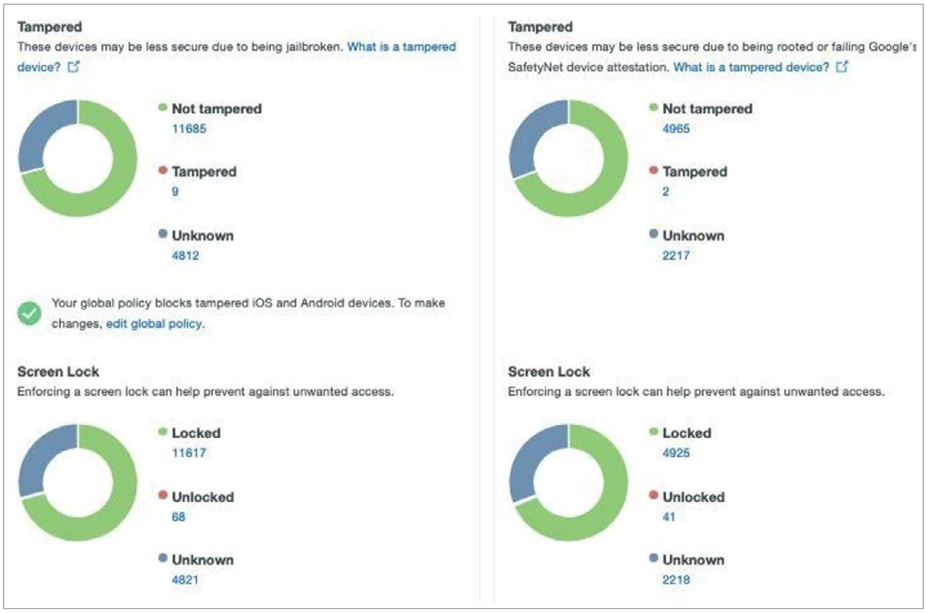
Version	Devices	
9.0 (Pie)	7089	View devices
9	1	View devices
8.1 (Oreo)	2	View devices

3. **Click** on the **number** below the device version to see detailed information related to the mobile device including:

- OS
- Browser
- Security Warnings
- Duo Mobile Version (field is blank if not using Duo Mobile for authentication)
- Security Warnings
- User (click to see user details)

4. **Click** on **View Devices** to see specific iOS or Android devices using a listed OS version

5. Scroll down to see whether these devices are **tampered** (i.e., jailbroken or rooted) whether screen lock is enabled, whether or not biometrics are enabled and if disk encryption is enabled on Android devices as it is enabled by default on all iOS devices. The data in this section is captured natively from devices using the Duo Mobile application.



Tampered

These devices may be less secure due to being jailbroken. What is a tampered device?

● Not tampered
11685

● Tampered
9

● Unknown
4812

✓ Your global policy blocks tampered iOS and Android devices. To make changes, edit global policy.

Screen Lock

Enforcing a screen lock can help prevent against unwanted access.

● Locked
11617

● Unlocked
68

● Unknown
4821

Tampered

These devices may be less secure due to being rooted or failing Google's SafetyNet device attestation. What is a tampered device?

● Not tampered
4965

● Tampered
2

● Unknown
2217

Screen Lock

Enforcing a screen lock can help prevent against unwanted access.

● Locked
4925

● Unlocked
41

● Unknown
2218

NOTE: This insight, along with the corresponding policies can help with compliance regulations that may require encryption and screen lock on devices accessing company data.

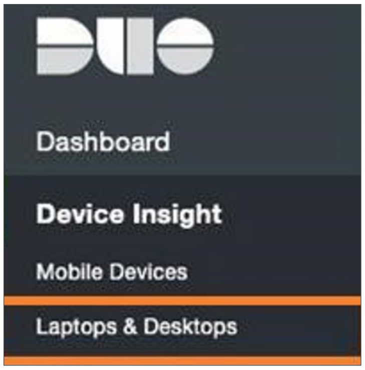
6. **Click** on **What is a tampered device?** to see how Cisco defines tampered device.

7. **Click** on the **number** below the Tampered / Screen Lock status to see detailed records for the affected devices.

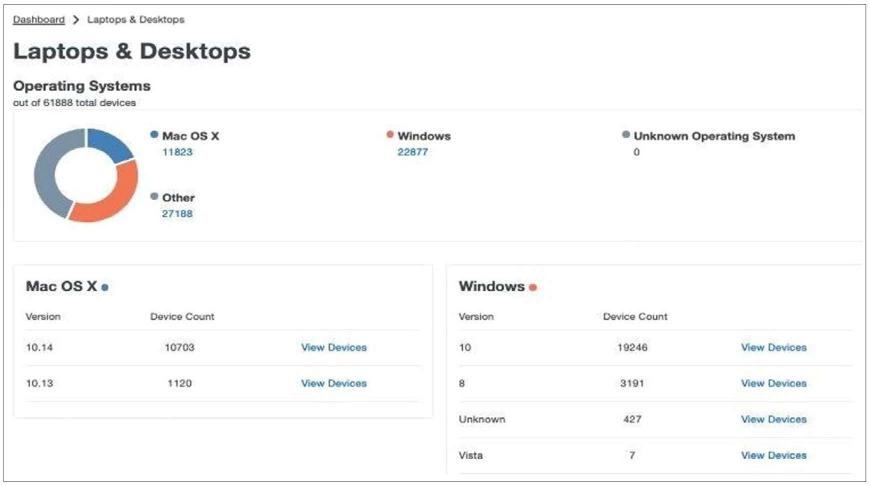
Laptops and desktops

Similar to the Mobile Device section, the Laptops and Desktops section of the Duo Admin portal provides visibility to the types of laptop and desktop devices that are in use. Data is captured by Duo each time a devices logs into a browser-based corporate resources that have been protected with Duo.

1. From the **Admin Panel**, select **Device Insight > Laptops & Desktops**.



2. View the **Laptops & Desktops** screen for a high-level breakdown of the operating systems used in the environment, for both corporate managed and BYO devices.



Dashboard > Laptops & Desktops

Laptops & Desktops

Operating Systems
out of 61888 total devices

● Mac OS X
11823

● Windows
22877

● Unknown Operating System
0

● Other
27188

Mac OS X ●

Version	Device Count	
10.14	10703	View Devices
10.13	1120	View Devices

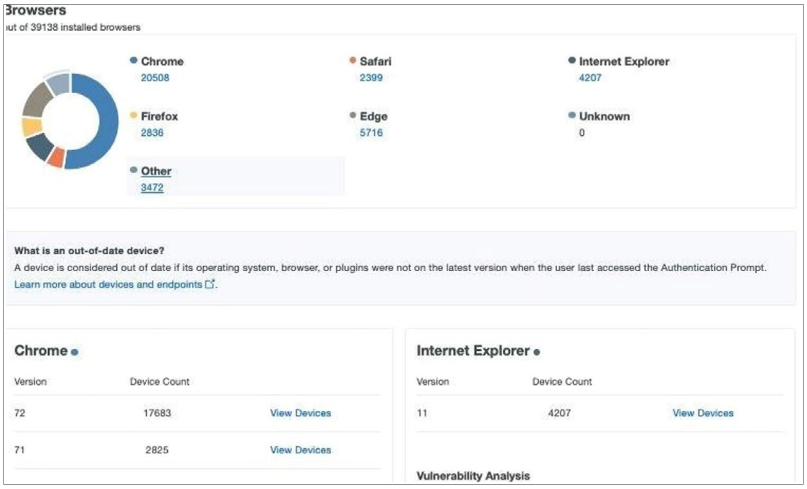
Windows ●

Version	Device Count	
10	19246	View Devices
8	3191	View Devices
Unknown	427	View Devices
Vista	7	View Devices

3. **Click** on the **number** below the OS version to get details.

4. **Click** on **View Devices** in the tables below the summary to see devices at a specific OS versions.

5. Scroll down to see a similar breakdown of browser platforms and specific versions including vulnerability analysis.



Browsers

ut of 39138 installed browsers

● Chrome 20508	● Safari 2399	● Internet Explorer 4207
● Firefox 2836	● Edge 5716	● Unknown 0
● Other 3472		

What is an out-of-date device?
A device is considered out of date if its operating system, browser, or plugins were not on the latest version when the user last accessed the Authentication Prompt.
Learn more about devices and endpoints.

Chrome ●

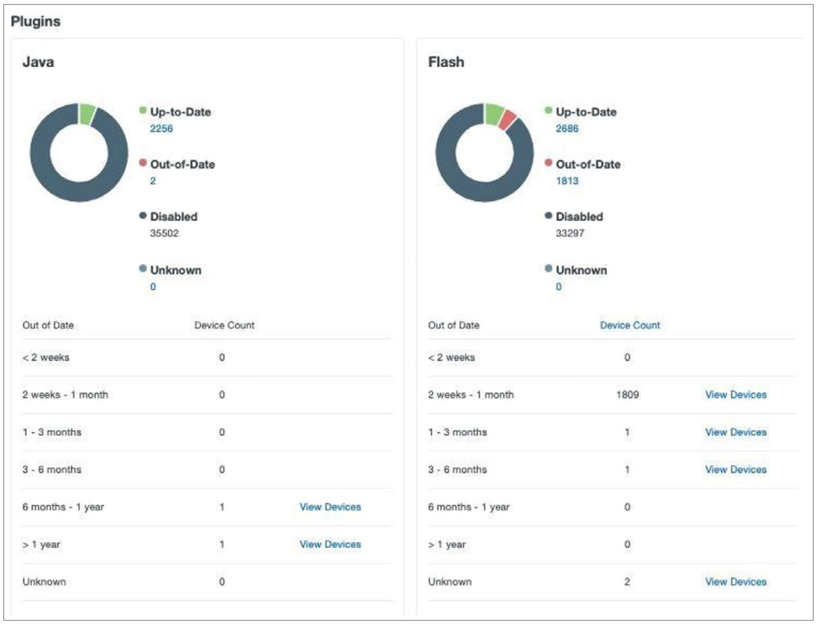
Version	Device Count	
72	17683	View Devices
71	2825	View Devices

Internet Explorer ●

Version	Device Count	
11	4207	View Devices

Vulnerability Analysis

6. Scroll down further to view the status of Java and Flash plugins to determine if the plugins are enabled and, if so, whether they are up-to-date.



Plugins

Java

● Up-to-Date 2256
● Out-of-Date 2
● Disabled 35502
● Unknown 0

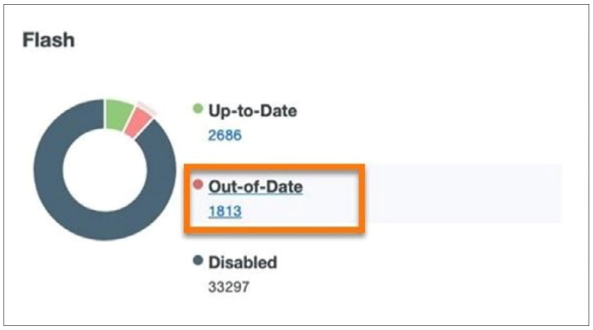
Out of Date	Device Count	
< 2 weeks	0	
2 weeks - 1 month	0	
1 - 3 months	0	
3 - 6 months	0	
6 months - 1 year	1	View Devices
> 1 year	1	View Devices
Unknown	0	

Flash

● Up-to-Date 2686
● Out-of-Date 1813
● Disabled 33297
● Unknown 0

Out of Date	Device Count	
< 2 weeks	0	
2 weeks - 1 month	1809	View Devices
1 - 3 months	1	View Devices
3 - 6 months	1	View Devices
6 months - 1 year	0	
> 1 year	0	
Unknown	2	View Devices

7. Click any of these **Plugins** options to drill down and view the specific devices and their associated users.



Flash

● Up-to-Date 2686
● Out-of-Date 1813
● Disabled 33297

Policies

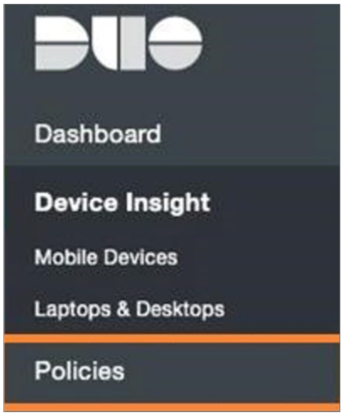
The Policy section of the Duo Administration portal allows Administrators to control how users authenticate, from where, and using which types of devices.

Policies can be defined at three different levels:

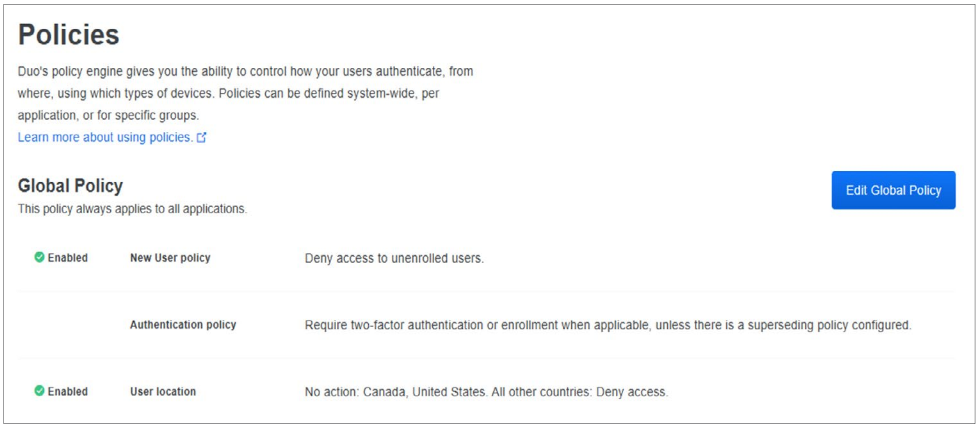
- **Global** — Policies that apply to all users and applications.
- **Application** — Policies that apply to the specific application to which it is assigned.
- **Group** — Policies that apply to a specific group of users connecting to a specific application(s).

Viewing policies

1. From the **Admin Panel,** select **Policies**.



2. From the policy page, Administrators can view the current Global, Application, and Group policies.



Policies

Duo's policy engine gives you the ability to control how your users authenticate, from where, using which types of devices. Policies can be defined system-wide, per application, or for specific groups.

Learn more about using policies.

Global Policy

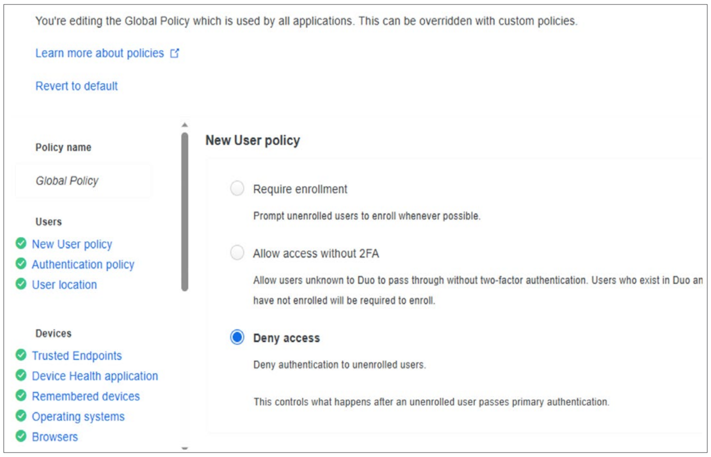
This policy always applies to all applications.

✓ Enabled	New User policy	Deny access to unenrolled users.
	Authentication policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.
✓ Enabled	User location	No action: Canada, United States. All other countries: Deny access.

3. Global policies apply to all users but can be overridden by a custom policy. Policies for a specific application or user group are considered custom policies.

Modifying a policy

1. To edit a Global policy, **click** the **Edit Global Policy** button.



You're editing the Global Policy which is used by all applications. This can be overridden with custom policies.

Policy name: Global Policy

New User policy

○ Require enrollment
Prompt unenrolled users to enroll whenever possible.

○ Allow access without 2FA
Allow users unknown to Duo to pass through without two-factor authentication. Users who exist in Duo an have not enrolled will be required to enroll.

● Deny access
Deny authentication to unenrolled users.

This controls what happens after an unenrolled user passes primary authentication.

On the left side of the page, you will see the name of the policy you are editing and the **4 policy categories:**

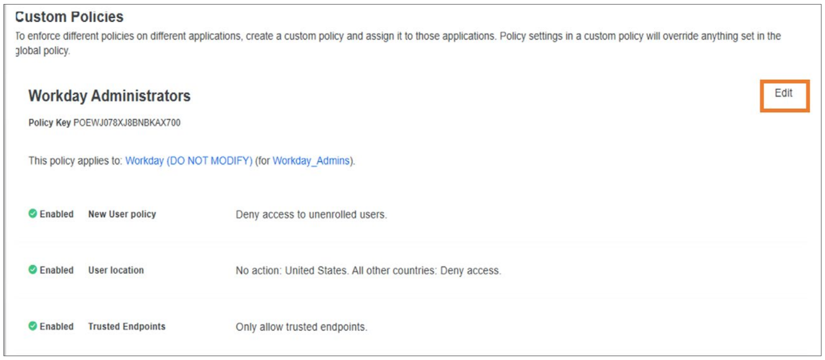
- Users
- Devices
- Networks
- Authenticators

2. **Click** on the policy you want to change.

3. Toggle on the policy option you want to enforce, then **click** the **Save Policy** button at the bottom of the page.

4. To **edit** a **Custom Policy**, scroll down to find the custom policy you want to edit.

5. **Click** on **EDIT** to the right of the policy name.



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.

Workday Administrators

Policy Key POEWJ078XJ8BNBKAX700

This policy applies to: Workday (DO NOT MODIFY) (for Workday_Admins).

✓ Enabled	New User policy	Deny access to unenrolled users.
✓ Enabled	User location	No action: United States. All other countries: Deny access.
✓ Enabled	Trusted Endpoints	Only allow trusted endpoints.

6. Follow steps 4 and 5 to change a custom policy.

7. To revert all policies back to Cisco default policies, **click** **Revert to Default** at the top of the page.

Other policy administration options

Administrators with the Owner and Administrator role can create, assign / unassign, reorder and delete custom policies for an application or user group from an application's properties page.

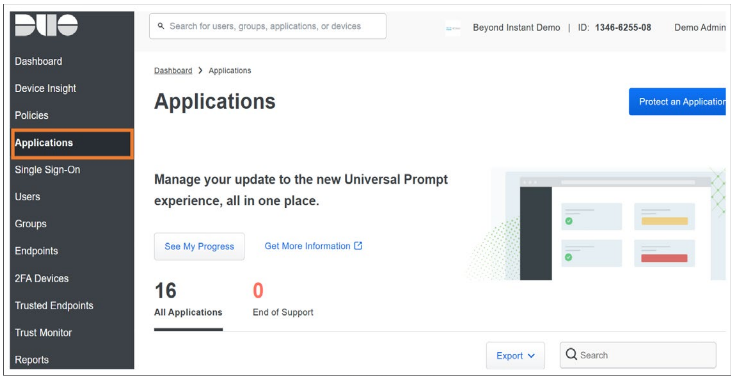
See the **Cisco Policy** guide for step by step instructions: [Duo Administration — Policy & Control | Duo Security]

Applications

This page allows Administrators to add protection to new applications as well as view the applications that are integrated (protected) with DUO and any Application or Group policies that have been defined for a specific application.

Viewing applications

1. From the **Admin Panel**, select **Applications.**



Manage your update to the new Universal Prompt experience, all in one place.

2. On this page, Administrators can see all integrated applications (listed alphabetically) or filter to just see applications that are End of Support. Use the search field to find a specific application.

3. **Click** on the **Application Name** to see specific details about the application including:

- Integration Key
- API hostname
- **Settings** — Application Type, Application Name. Permissions, and Networks for API access.

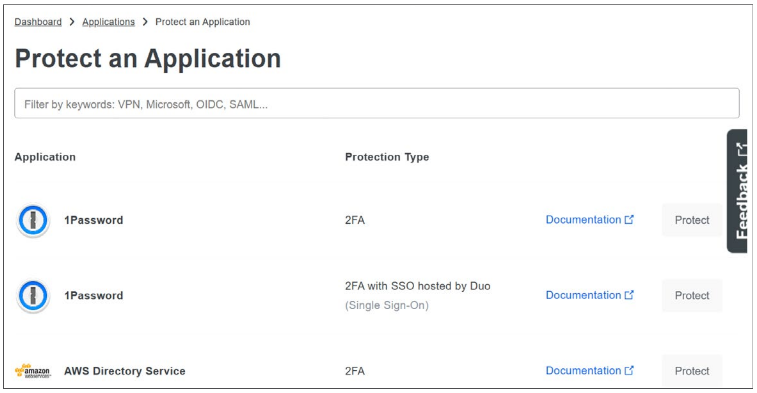
4. **Click** on the **Application Policy name** or **Group Policy name** to see / edit policy details. [See Policies]. Applications without an application policy or group policy listed do not have a custom policy. Only Global policies would apply to these applications.

5. **Click** on the **Export** button to export a CSV file of Applications.

Protect an application

IT administrators can protect an application by integrating it with Duo for 2 Factor Authentication (2FA).

1. From the Application page, **click** the **Protect an Application** button to see a list of the different types of services you can protect with Duo. The **Protection Type** column indicates how Duo protects that specific application.



Dashboard > Applications > Protect an Application

Protect an Application

Filter by keywords: VPN, Microsoft, OIDC, SAML...

Application	Protection Type		
1Password	2FA	Documentation	Protect
1Password	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect
AWS Directory Service	2FA	Documentation	Protect

2. **Click** the **Documentation** for an application to review the requirements and configuration steps for integrating Duo into your service before adding the new application. If you don't see a "Documentation" link that means it's a partner application for which Duo doesn't host configuration instructions. You'll see a link for more information later once you create the application.

See the **Cisco documentation** for step by step instructions for configuring (protecting) an application: Duo Administration — Protecting Applications | Duo Security

Universal prompt

The Universal prompt provides a simplified and accessible Duo login experience for web-based applications, offering a redesigned visual interface with security and usability enhancements.

1. **Click Get More Information** at the top of the Application section for detailed instructions on setting up Universal Prompt.

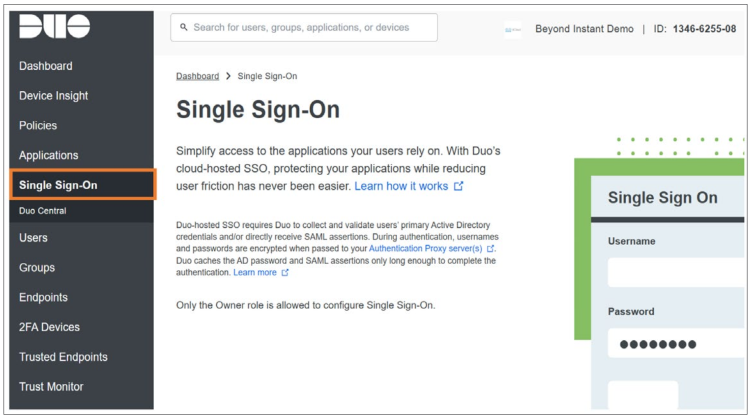
2. **Click** the **See My Progress** button at the top the top of the Application section to see the activation status of each applications updated with the Universal Prompt.

Single Sign On

Single Sign On improves security and productivity by enabling Users to access all applications using only one username and password.

Configuring Single Sign On

1. From the **Admin Panel**, select **Single Sign On**.



Single Sign-On

Simplify access to the applications your users rely on. With Duo's cloud-hosted SSO, protecting your applications while reducing user friction has never been easier. Learn how it works

Duo-hosted SSO requires Duo to collect and validate users' primary Active Directory credentials and/or directly receive SAML assertions. During authentication, usernames and passwords are encrypted when passed to your Authentication Proxy server(s). Duo caches the AD password and SAML assertions only long enough to complete the authentication. Learn more

Only the Owner role is allowed to configure Single Sign-On.

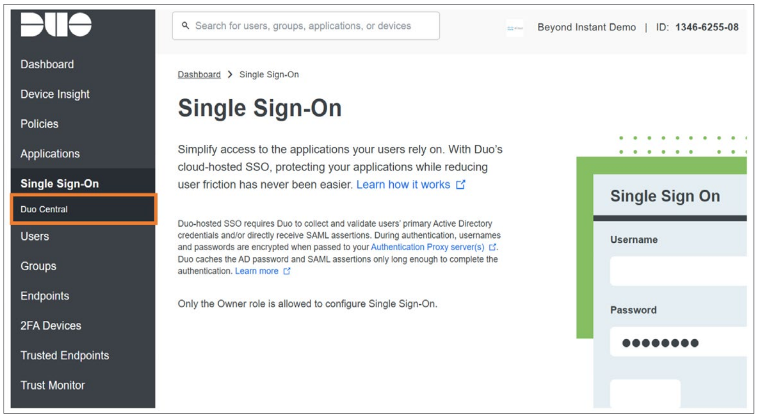
2. Single Sign on can only be configured by the Owner.
See **Cisco link** to learn how it works: [How to Use Duo Single Sign-On (SSO) | Duo Security]

Duo Central

Duo Central is a customizable one-stop access point for users and the software they need to do their jobs securely.

NOTE: Single Sign on is required for Duo Central.

1. From the **Admin Panel**, select **Single Sign On** then select **Duo Central**.



Single Sign-On

Simplify access to the applications your users rely on. With Duo's cloud-hosted SSO, protecting your applications while reducing user friction has never been easier. Learn how it works

Duo-hosted SSO requires Duo to collect and validate users' primary Active Directory credentials and/or directly receive SAML assertions. During authentication, usernames and passwords are encrypted when passed to your Authentication Proxy server(s). Duo caches the AD password and SAML assertions only long enough to complete the authentication. Learn more

Only the Owner role is allowed to configure Single Sign-On.

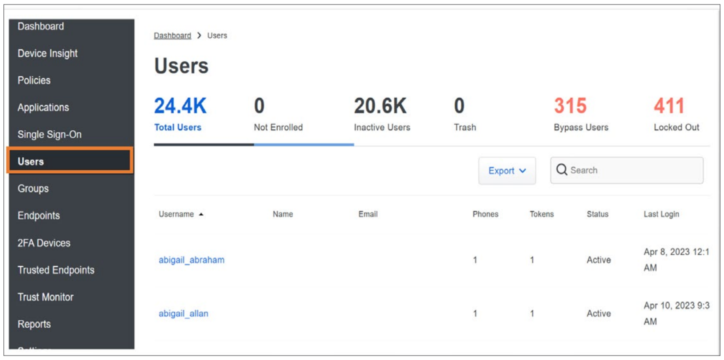
2. See **Cisco link** to learn how it works: [Duo Central | Duo Security]

Users

The Users section of the section of the Duo Administration portal allows Administrators to view, search and export log data related to users.

Viewing users

1. From the **Admin Panel**, select **Users**.



Username ▲	Name	Email	Phones	Tokens	Status	Last Login
abigail_abraham			1	1	Active	Apr 8, 2023 12:1 AM
abigail_allan			1	1	Active	Apr 10, 2023 9:3 AM

2. From this page, you can see the total number of users and user status.

3. **Click** on the **Export** button to download a list of users.

Users can be exported to:

- CSV
- JSON
- Printer

4. **Click** on a specific **username** to see user details.

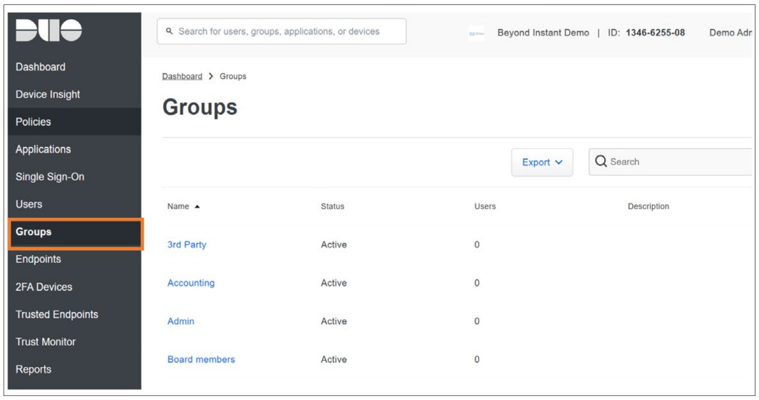
Groups

A group is a set of users with custom policies. The Groups section of the section of the Duo Administration portal allows Administrators to search for and view detailed information about a user group.

NOTE: See the Policy section for creating / modifying groups

Viewing groups

1. From the **Admin Panel**, select **Groups**.



Name ▲	Status	Users	Description
3rd Party	Active	0	
Accounting	Active	0	
Admin	Active	0	
Board members	Active	0	

2. From this page, you can see the total number of group, group status and number of users in each group.

3. **Click** on the **Export** button to download a list of groups

Groups can be exported to:

- CSV

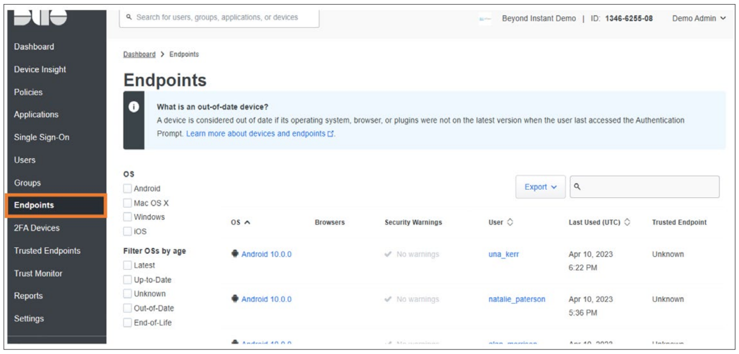
4. **Click** on a specific **Name** to see group details including 2FA authentication status (Active / Bypass / Disabled) as defined by the group policy and the users within a group.

Endpoints

The Endpoints section of the Duo Administration portal allows Administrators to view, search and export log data related to Endpoints.

Viewing Endpoints

1. From the **Admin Panel**, select **Endpoints.**



Endpoints

What is an out-of-date device?

A device is considered out of date if its operating system, browser, or plugins were not on the latest version when the user last accessed the Authentication Prompt. Learn more about devices and endpoints.

OS	Browsers	Security Warnings	User	Last Used (UTC)	Trusted Endpoint
Android 10.0.0		✓ No warnings	una_kerr	Apr 10, 2023 6:22 PM	Unknown
Android 10.0.0		✓ No warnings	natalie_paterson	Apr 10, 2023 5:36 PM	Unknown

2. Toggle the boxes on / off to apply or remove a filer.

3. Use the Search field to find a specific user.

4. **Click** on **OS Version** or **User** to see details for the endpoint device / user.

5. **Click** on the **Export** button to export log data.

Data can be exported in the following formats:

- CSV
- JSON
- URL
- PDF

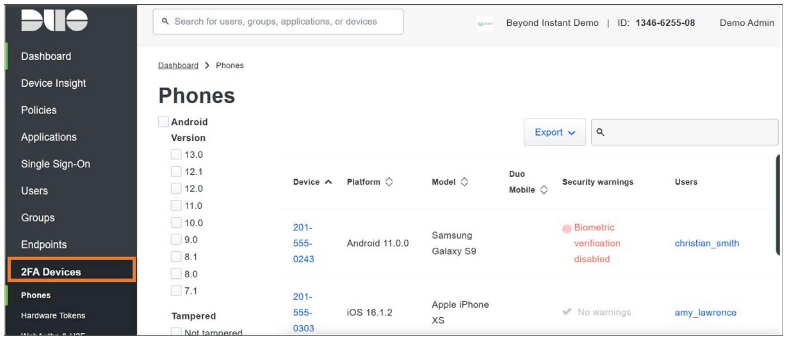
Data is retained on the Duo platform for 180 days.

2FA devices

The 2FA section of the Duo Administration portal allows Administrators to see the device used for 2 Factor Authentication (2FA).

Viewing phones

1. From the **Admin Panel**, select **2FA Devices.**



Device	Platform	Model	Duo Mobile	Security warnings	Users
201-555-0243	Android 11.0.0	Samsung Galaxy S9		Biometric verification disabled	christian_smith
201-555-0303	iOS 16.1.2	Apple iPhone XS		✓ No warnings	amy_lawrence

2. From this page, Administrators can see details pertaining to the device used for 2FA including:

- Phone Number
- Platform
- Model
- Duo Mobile version (blank means Duo Mobile was not used)
- Security Warnings
- User

3. **Click** on the **Export** button to export the device details.

Data can be exported in the following formats:

- CSV
- JSON
- URL
- PDF

4. Click on a **phone number** or **username** to see detailed information about the device or user.

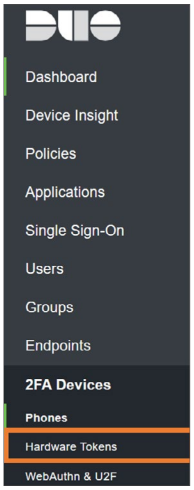
5. Toggle the buttons on the Right to filter devices based on:

- Phone Type / OS version
- Tampered status
- Screen Lock
- Biometrics
- Disc Encryption

6. Use the search bar to search for a specific phone number or user

Viewing Hardware Tokens

1. From the **Admin Panel**, select **2FA Devices** then **Hardware Tokens**.



2. From this page, Administrators can see details pertaining to the hardware token used for 2FA including:

- Serial number
- Token Type
- User

3. **Click** on the **Export** button to export the device details.

Data can be exported in the following formats:

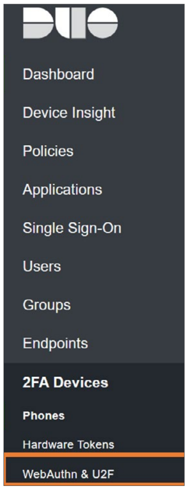
- CSV
- JSON
- Print

4. **Click** on a **serial number** or **username** to see detailed information about the token or user.

5. Use the search bar to search for a specific serial number or user.

Viewing WebAuthn and U2F

1. From the **Admin Panel**, select **2FA Devices** then **WebAuthn & U2F**



2. From this page, Administrators can see details pertaining to the security keys registered with the U2F standard as well as passkeys (security keys and biometric devices) registered with the WebAuthn standard:

- Name
- Web Authn ID
- U2F ID
- User

3. **Click** on the **Export** button to export the device details.

Data can be exported in the following formats:

- CSV
- JSON
- URL
- PDF

4. **Click** on a **username** to see detailed information about the token or user.

5. Use the search bar to search for a specific ID or user.

Trusted Endpoints

The Trusted Endpoints section of the Duo Administration portal allows Administrators to define and manage trusted endpoints and grant secure access to your organization's applications with policies that verify systems using device certificates, application verification, or management status.

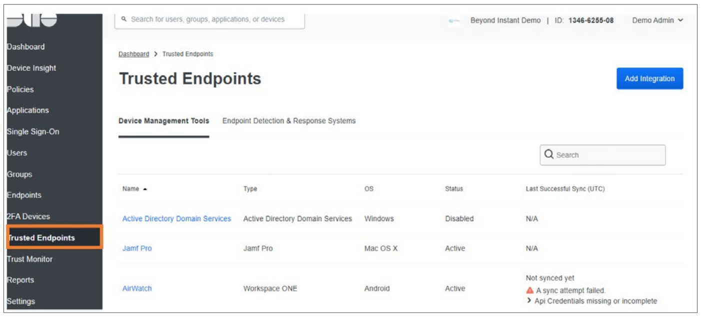
Duo helps you distinguish between unmanaged endpoints and managed endpoints that access your browser-based applications. The Trusted Endpoints policy tracks whether clients accessing the applications can be identified as managed or can block access to various applications from systems that aren't managed.

In order to set Policies for trusted devices, a **Mobile Device Management tool** will need to be integrated with Duo.

For more information about **Trusted Endpoints**, see the **Cisco documentation**: Duo Trusted Endpoints | Duo Security

Viewing Device Management Tools

1. From the **Admin Panel**, select **Trusted Endpoints**



Trusted Endpoints

Name ▲	Type	OS	Status	Last Successful Sync (UTC)
Active Directory Domain Services	Active Directory Domain Services	Windows	Disabled	N/A
Jamf Pro	Jamf Pro	Mac OS X	Active	N/A
AirWatch	Workspace ONE	Android	Active	Not synced yet ⚠ A sync attempt failed. › Api Credentials missing or incomplete

2. On this page, Administrators can see the Mobile Device Management (MDM).

Tools that have been integrated with Duo including:

- Tool Type
- Tool OS
- Tool Status
- Last successful sync

3. **Click** on a **name** to see details pertaining to a specific **Endpoint Management tool.**

4. **Click** on **Endpoint Detection & Response Systems** to see Tools that have been integrated with Duo including:

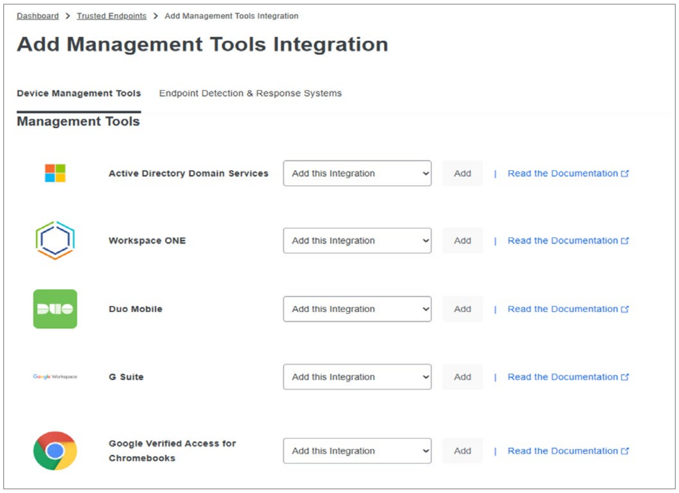
- Key
- Type
- Status

5. **Click** on a specific **Key** for details pertaining to the **Endpoint Detection and Response Systems**.

Integrating a Device Management Tool

1. From the Trusted Endpoint landing page, **click** the **Add Integration** button on the top right side of the page.

2. Scroll to find the **MDM tool** to be integrated.



Dashboard > Trusted Endpoints > Add Management Tools Integration

Add Management Tools Integration

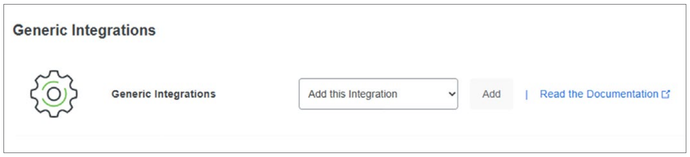
Device Management Tools   Endpoint Detection & Response Systems

Management Tools

Active Directory Domain Services	Add this Integration	Add	Read the Documentation
Workspace ONE	Add this Integration	Add	Read the Documentation
Duo Mobile	Add this Integration	Add	Read the Documentation
G Suite	Add this Integration	Add	Read the Documentation
Google Verified Access for Chromebooks	Add this Integration	Add	Read the Documentation

3. **Click Read the Documentation** for step by step process for integrating the MDM tool.

4. If your tool is not listed, scroll to the Generic Integrations section and **click Read the Documentation** for step by step instructions to complete the integration.



Generic Integrations

Generic Integrations	Add this Integration	Add	Read the Documentation

Trust Monitor

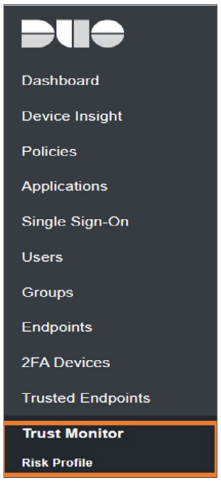
The Trust Monitor section of the Duo Administration portal provides Administrators with a dashboard view of actionable security events. A Security Event is an authentication or registration that surfaced due to its anomaly score, known attack patterns, or other heuristics (i.e. the Risk Profile designation, etc.). The top events represent the highest priority event at any given time, based on both anomalistic nature and Risk Profile weighting.

For detailed information on this threat detection feature see the **Cisco documentation** on **Trust Monitor**: Duo Trust Monitor | Duo Security

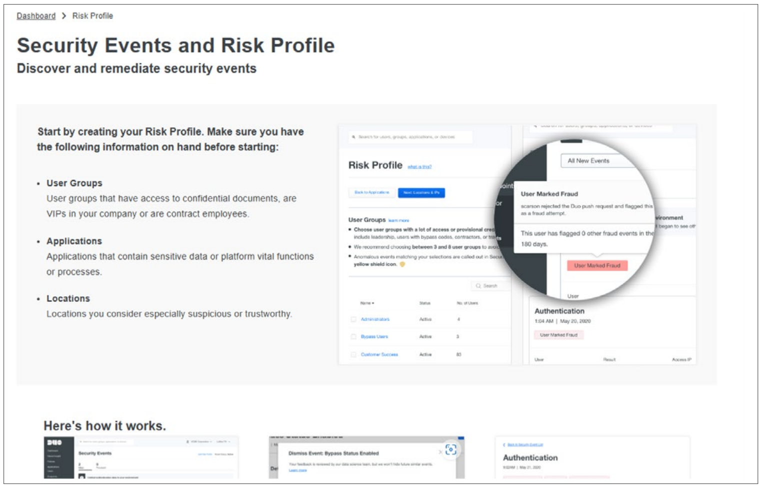
NOTE: The Trust Monitor feature is only available to clients with the Advantage or Premier licenses.

Creating a risk profile

1. From the **Admin Panel**, select **Trust Monitor** then select **Risk Profile**.



2. The **Risk Profile landing page** provides detailed information about how to create a risk profile and how a risk profile works.



Dashboard > Risk Profile

Security Events and Risk Profile

Discover and remediate security events

Start by creating your Risk Profile. Make sure you have the following information on hand before starting:

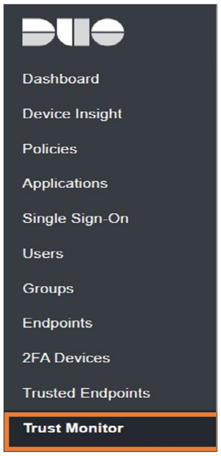
- **User Groups**
  User groups that have access to confidential documents, are VIPs in your company or are contract employees.
- **Applications**
  Applications that contain sensitive data or platform vital functions or processes.
- **Locations**
  Locations you consider especially suspicious or trustworthy.

Here's how it works.

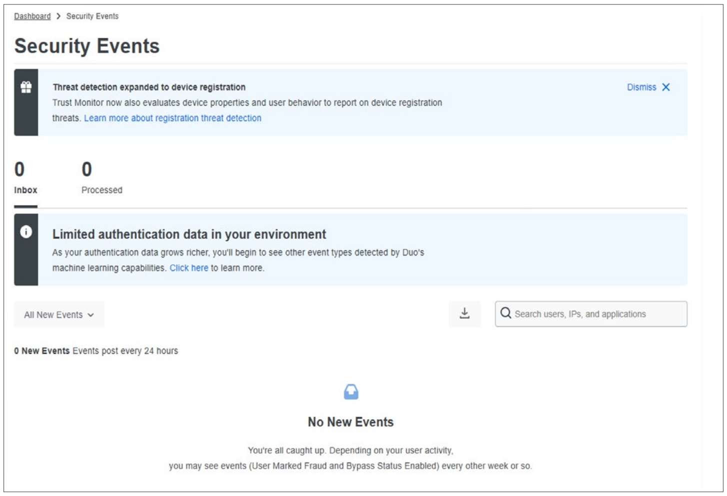
Risk Profile
User Groups
All New Events
User Marked Fraud
scarson rejected the Duo push request and flagged this as a fraud attempt.
This user has flagged 0 other fraud events in the 180 days.
User Marked Fraud
Authentication
1:04 AM | May 20, 2020
User Marked Fraud
Security Events
Dismiss Event: Bypass Status Enabled
Authentication

Viewing security events

1. From the **Admin Panel**, select **Trust Monitor**.



2. The landing page of the **Trust Monitor** section is the **Security Events page**.


Dashboard > Security Events
Dismiss ×
All New Events
Search users, IPs, and applications

Security Events

Threat detection expanded to device registration

Trust Monitor now also evaluates device properties and user behavior to report on device registration threats. Learn more about registration threat detection

0 Inbox

0 Processed

Limited authentication data in your environment

As your authentication data grows richer, you'll begin to see other event types detected by Duo's machine learning capabilities. Click here to learn more.

0 New Events Events post every 24 hours

No New Events

You're all caught up. Depending on your user activity, you may see events (User Marked Fraud and Bypass Status Enabled) every other week or so.

3. From the **Security Events page**, Administrators can see any announcements from Cisco and review security events surfaced by Duo Trust Monitor.

NOTE: Administrators may not see any security events in the table at first. That means that the majority of your users don't have enough authentications to build accurate modeling. As they continue to use Duo, the platform will automatically evaluate and begin providing events when the authentications increase.

If log retention is set to anything under 90 days, you will not be eligible for Machine Learning modeling and will only see security events for registration events, bypass status (if enabled in your Risk Profile) and user marked fraud. Duo recommends retaining at least 180 days of logs to build the most accurate Trust Monitor models.

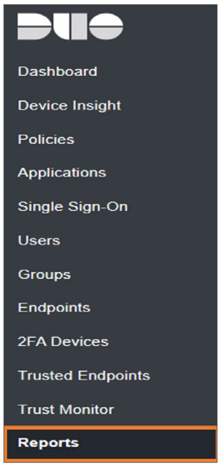
4. See the **Cisco documentation** on **Security Events** for detailed information about how to read and process security events: Duo Trust Monitor | Duo Security

Reports

The Report section of the Duo Administration Portal provides reports on log data.

Viewing reports

1. From the Duo **Admin Panel** select **Reports**.



2. The **Authentication Log report** is the landing page of the **Reports section**.

3. Select a specific report from the **Admin Panel**. The report name, description and **Cisco documentation** is listed below:

Report name	Description	Cisco documentation
Authentication Log	Log of Authentication attempts	Guide to reading the Authentication Log report in the Duo Admin Panel
Device Health Deployment	Report of all unique endpoints that have reached Duo and the current status of the Device Health app on those devices	Guide to reading the Device Health Deployment Progress report in the Duo Admin Panel
Single Sign-On Log	Summary of how and when users accessed which application, along with which device and which MFA method was used	Guide to reading the Duo Single Sign-On Log report in the Duo Admin Panel
Telephony Log	Summary of all telephony authentication attempts that have reached Duo	Guide to reading the Telephony Log report in the Duo Admin Panel
Administrator Actions	Report of all changes made by Duo administrators as well as any updates related to the Directory Sync events in the Duo Admin Panel	Guide to reading the Administrator Actions report in the Duo Admin Panel

Report name	Description	Cisco documentation
Authentication Summary	**Report of the following:** • Authentication success rate • Top Authentication methods • Top Applications being accessed • Changes in authentication method over time	Guide to reading the Authentication Summary report in the Duo Admin Panel
Denied Authentications	**Report of the following:** • Failed authentication rate • Breakdown of failed authentications by method and reason denied • Top denied users • Top denied applications	Guide to reading the Denied Authentications report in the Duo Admin Panel
Deployment Progress	Report of the deployment status of all users, including the number of licenses uses and unused.	Guide to reading the Deployment Progress report in the Duo Admin Panel
Policy Impact	Report of how policies are impacting users and how the are working together to secure access within your organization. **NOTE:** only available with Advantage and Premier license options	Guide to reading the Policy Impact report in the Duo Admin Panel
Universal Prompt Progress	Report of Universal prompt Progress in a new Universal prompt section including upgrade status and applications that need upgraded.	Guide to reading the Universal Prompt Update Progress report in the Duo Admin Panel

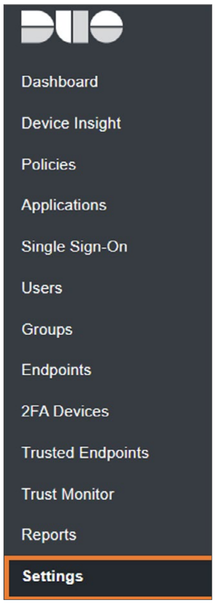
Settings

The Settings section of the Duo Admin portal includes general information specific to your Duo account including:

- Custom Branding
- User Communication
- Notifications
- Admin Role Permissions
- Phone Calls
- SMS Passcodes
- Lockout and Fraud
- User Deletion
- Duo Mobile App
- Logging
- Admin Password Policy

Viewing settings

1. From the **Duo Admin Panel**, select **Settings**.



2. Select the setting to view / update account configurations.

NOTE: Only Account Owners and Administrators can make changes to the account settings. See the **Cisco documentation** for details on **Administrative roles**:
Duo Administrative Roles | Duo Security

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary. Restrictions may apply.