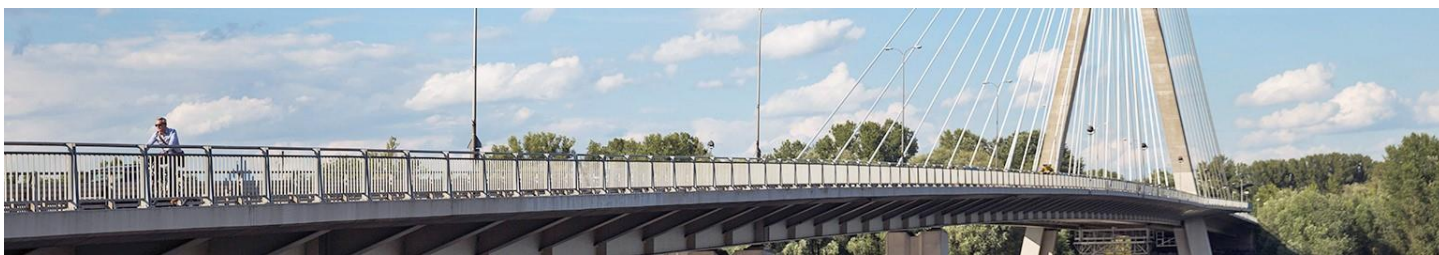


# Duo Admin Panel v1 - Instant Demo



마지막 업데이트: 2019 년 6 월 19 일

## 본 인스턴트 데모에 대하여

미리 구성되어 있는 본 인스턴트 데모는 아래 내용을 포함합니다:

[요구 사항](#)

[솔루션에 대하여](#)

[시작하기](#)

[시나리오 1. 대시보드 보기](#)

[시나리오 2. Device Insight 보기](#)

[시나리오 3. 정책 관리](#)

[What's Next?](#)

## 요구 사항

필수	선택 사항
노트북	Cisco AnyConnect®

## 솔루션에 대하여

**Duo Admin Panel** 인스턴트 데모는 Duo의 관리 경험을 안내합니다. Duo Admin Panel은 관리자가 새 애플리케이션 통합, 사용자 등록 및 기타 계정별 설정 추가와 같은 Duo 계정의 대부분의 측면을 구성할 수 있는 위치입니다. 또한 관리자는 회사 리소스에 접근하는 장치에 대한 정책을 보고 설정하여 보안 상태를 보다 잘 이해할 수 있습니다. Duo는 데이터를 캡처하고 모바일 및 데스크톱의 모든 주요 장치 플랫폼에 대한 통찰력을 제공합니다.

일반적으로 MDM 및 EMM과 같은 솔루션은 사용자가 중요한 장치 데이터를 캡처하기 위해 장치에 에이전트를 설치해야 합니다. 이러한 에이전트는 종종 사용자가 고용주에게 여러 권한을 부여하도록 요구하는데, 이는 사용자가 불편할 수 있습니다.

**Duo Admin Panel** 제공하는 몇 가지 장점은 다음과 같습니다:

- Duo는 에이전트 없이도 이 데이터를 캡처할 수 있으며 사용자가 Duoprotected 애플리케이션에 로그인할 때마다 캡처합니다.
- Duo는 최종 사용자에게 완전히 투명합니다.
- Duo는 관리자의 추가 설정이나 구성 없이 기본적으로 이 데이터를 캡처합니다.

또한 **Duo Admin Panel**을 통해 관리자는 최신 보안 장치만 애플리케이션에 접근하도록 장치 정책을 설정할 수 있습니다.

## 시작하기

### 시작하기에 앞서

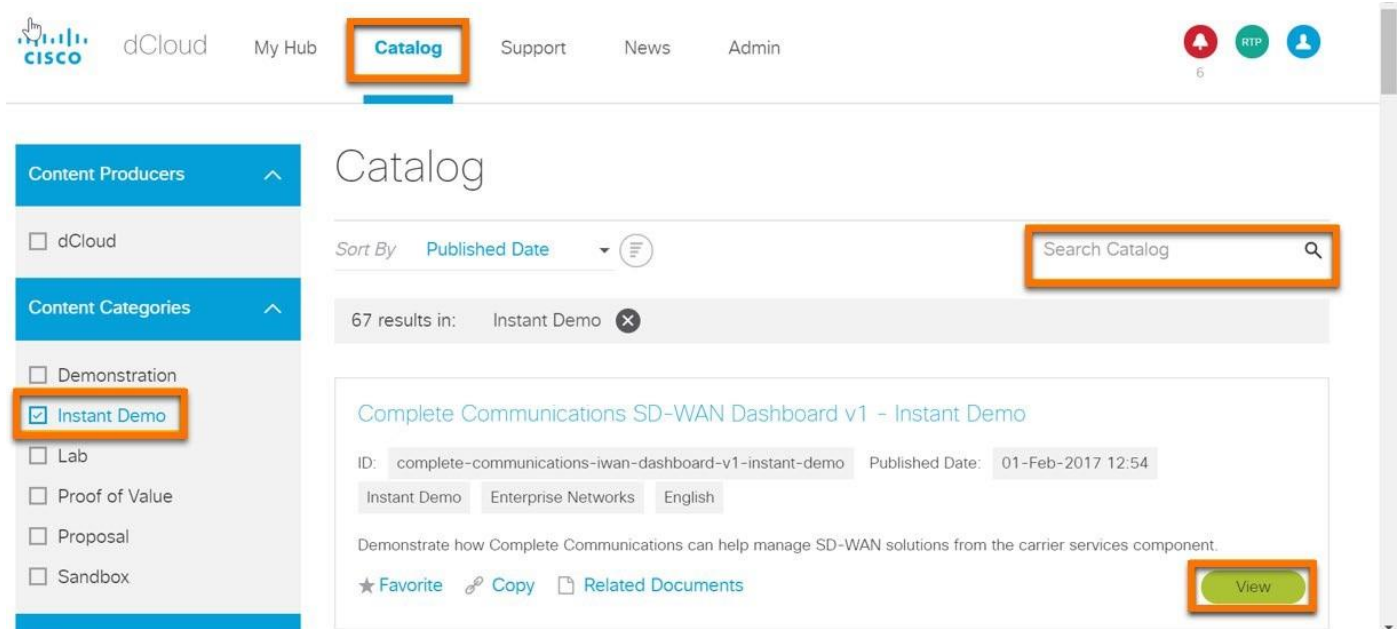
고객 및 파트너를 대상으로 데모 시연을 할 경우 원활한 진행을 위해 본 자료를 가지고 사전에 충분한 연습을 하시기를 권장합니다. 데모 완료 후 새롭게 구성을 해야 하는 경우는 세션을 다시 예약하십시오.

**사전에 충분한 연습은 성공적 진행을 위한 필수 조건입니다.**

다음 스텝에 따라 인스턴트 액세스 콘텐츠의 세션을 시작하고 프리젠테이션 환경을 구성합니다.

1. **Catalog** 를 클릭하고 사이드 바에서 **Instant Demo** 를 선택하십시오. 여기에는 모든 dCloud Instant 데모가 나열됩니다.
2. **View** 를 클릭합니다.

**참고:** 또는 **Search Catalog** 상자를 사용하여 **Instant Demo** 이름을 검색할 수 있습니다.



The screenshot shows the Cisco dCloud Catalog page. The top navigation bar includes 'dCloud', 'My Hub', 'Catalog' (highlighted with an orange box), 'Support', 'News', and 'Admin'. On the right, there are notification, RTP, and user icons. The left sidebar has 'Content Producers' (dCloud) and 'Content Categories' (Demonstration, Instant Demo (checked and highlighted with an orange box), Lab, Proof of Value, Proposal, Sandbox). The main content area is titled 'Catalog' and shows search results for 'Instant Demo'. A search bar at the top right contains 'Search Catalog' (highlighted with an orange box). Below the search bar, it says '67 results in: Instant Demo'. The first result is 'Complete Communications SD-WAN Dashboard v1 - Instant Demo'. Below the title, it shows the ID 'complete-communications-iwan-dashboard-v1-instant-demo', Published Date '01-Feb-2017 12:54', and tags 'Instant Demo', 'Enterprise Networks', and 'English'. A description follows: 'Demonstrate how Complete Communications can help manage SD-WAN solutions from the carrier services component.' At the bottom of the result card, there are links for 'Favorite', 'Copy', and 'Related Documents', and a 'View' button (highlighted with an orange box).

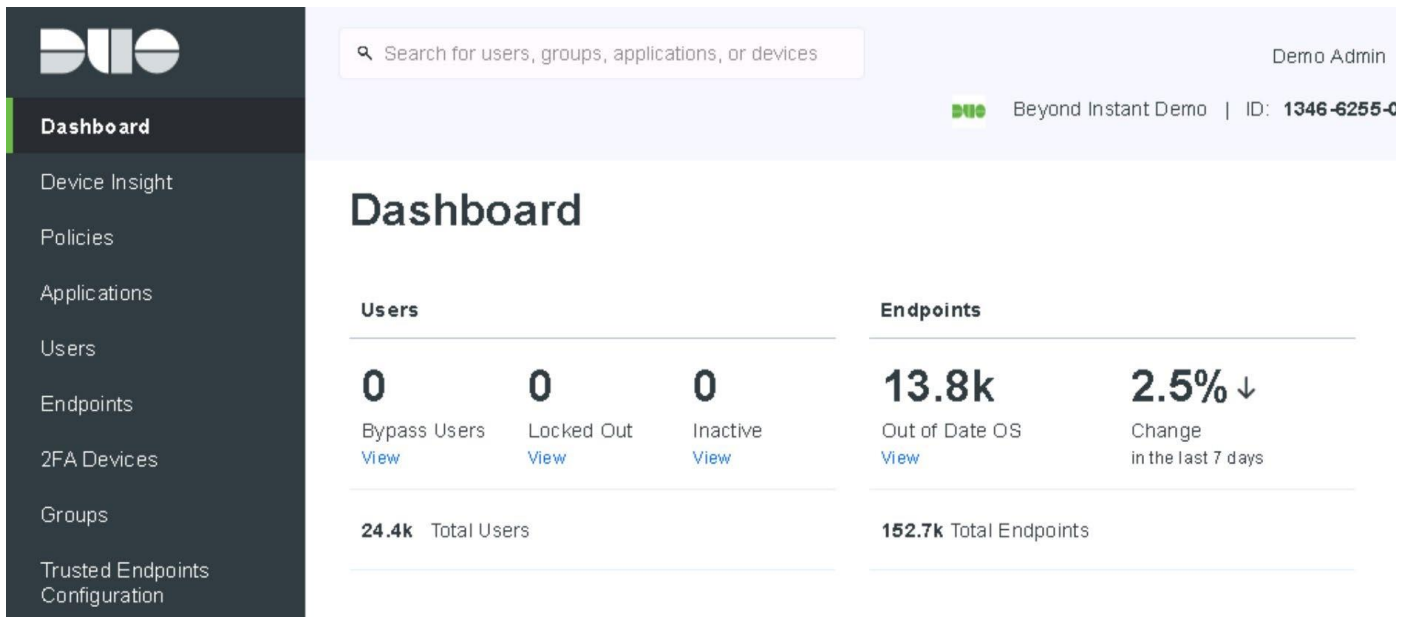
## 시나리오 1. 대시보드 보기

**가치 제안:** **Dashboard** 를 통해 Duo instance 를 관리할 수 있을 뿐만 아니라 조직 내 Duo 의 전반적인 상태를 확인할 수 있습니다.

### 스텝

1. **Duo Admin Panel** 에 로그인하면 **Dashboard** 가 표시되므로 기업 리소스에 접근하는 사용자와 장치를 볼 수 있습니다.

**참고:** 데모 Duo **Admin Panel** 은 이미 일반 고객의 데이터 담당자로 채워져 있습니다.



**Users**

0	0	0
Bypass Users <a href="#">View</a>	Locked Out <a href="#">View</a>	Inactive <a href="#">View</a>
<b>24.4k</b> Total Users		

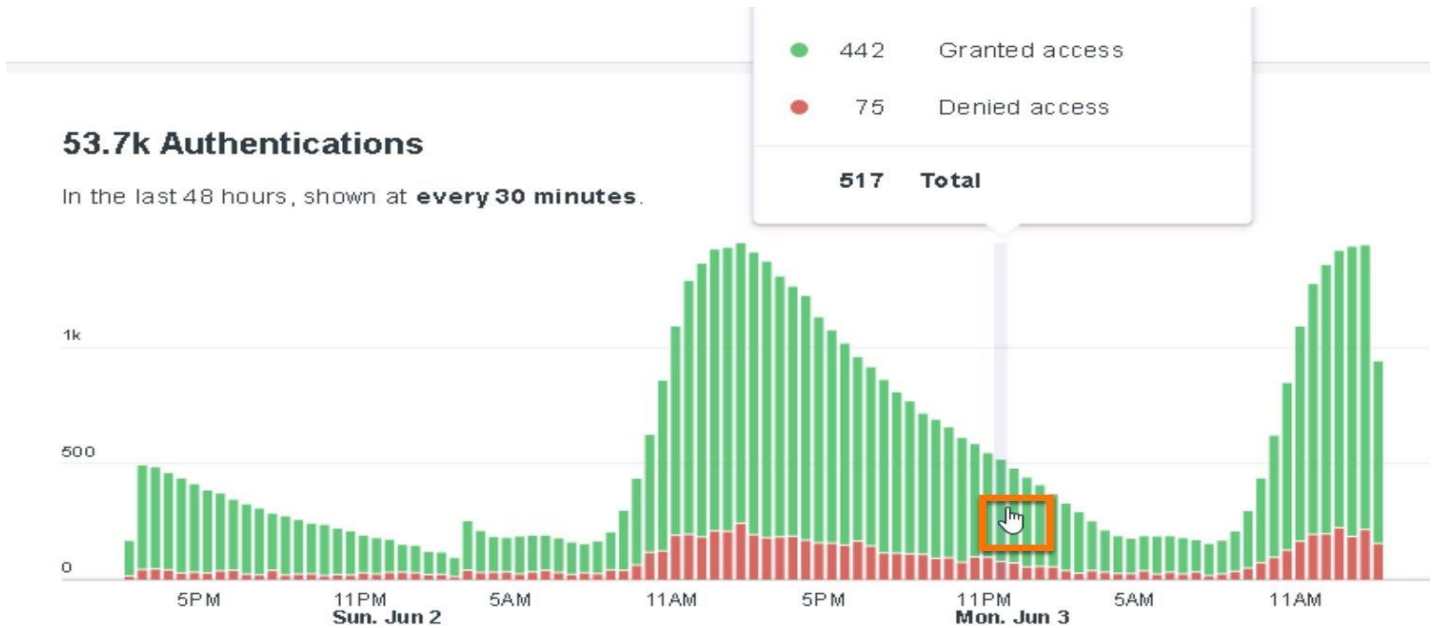
**Endpoints**

<b>13.8k</b>	<b>2.5% ↓</b>
Out of Date OS <a href="#">View</a>	Change in the last 7 days
<b>152.7k</b> Total Endpoints	

2. 다음을 표시하는 **Dashboard** 를 검토하십시오.
  - 등록된 사용자 수
  - 등록된 장치 수
  - 기록 인증 데이터
  - 즉각적인 주의가 필요할 수 있는 조건 (현재 잠겨 있는 사용자 수 등)

3. **Authentications** 섹션에서 히스토그램의 막대 위에 마우스 포인터를 올려 놓으면 지정된 기간 동안의 인증 세부 정보를 볼 수 있습니다.

- 기간 (선택한 막대로 표시됨)
- **Granted Access** 접근 권한 허용된 사용자 수
- **Denied Access** 접근 권한 거부된 사용자 수



4. 더 자세한 인증 세부 정보(예: 사용자 이름, 애플리케이션 등)을 보려면 **Authentication Log** 섹션으로 스크롤하십시오.

### Authentication Log Last 10 attempts

[Full authentication log](#)

Timestamp (UTC)	Result	User	Application	Access Device	Second Factor
3: 19 PM JUN 4, 2019	✔ Granted User approved	edward_hu...	Duo Access Gateway Launcher	> Windows 10	> Duo Push Chicago, IL
3: 19 PM JUN 4, 2019	✔ Granted User approved	jacob_cornis	Splunk Admin	> Windows 10	> Duo Push United States
3: 19 PM JUN 4, 2019	✘ Denied User mistake	andrew_gill	SAML - Salesforce	> Mac OS X 10.14.5	> Duo Push Fresno,

## 시나리오 2. 디바이스 인사이트 보기 (Viewing Device Insight)

**가치 제안:** 이 시나리오는 Duo 가 환경의 장치에 제공하는 가시성을 보여줍니다. 고객은 종종 이 데이터가 매우 공개된다고 생각합니다. 많은 조직에서 직원이 회사 노트북을 사용하도록 요구하는 정책을 시행하고 있지만, 궁극적으로 이를 시행하는 데 필요한 기술적 통제는 없다고 말합니다. 이러한 제어 기능이 마련되지 않은 최종 사용자는 자신의 개인 장치에서 Outlook Web App 과 같은 리소스에 접근할 수 밖에 없습니다. 회사 리소스에 접근하는 이러한 개인 장치가 Vista 와 같이 잠재적으로 안전하지 않은 Windows 버전을 실행할 수 있기 때문에 위험합니다.

이 데모에서는 Duo **Admin** panel 의 세 가지 특정 영역에 초점을 맞춥니다:

- Device Insight (개요)
- 모바일 장치(Mobile Devices)
- 노트북 및 데스크탑 (Laptops and Desktops)

### 스텝

#### 개요

1. **Admin Panel** 에서 **Device Insight** 를 선택하여 **Device Insight** 화면을 표시하십시오.



2. **Device Insight** 화면을 탐색하십시오.

- 멀티팩터 인증을 수행하는 데 사용되는 장치를 포함하여 laptops, desktops 및 Mobile Devices 와 같은 회사 애플리케이션에 접근하는 모든 장치의 개괄적인 개요를 검토.
- 최신 장치 대 구식 장치의 비율을 포함하여 운영 체제의 배포를 검토. 관리자는 관리 대상 장치 대 관리되지 않는 장치 수를 평가 가능.



Dashboard > Device Insight

# Device Insight

Print

Page Glossary

All Endpoints Trusted Endpoints Not-Trusted Endpoints

## Operating Systems by Platform



- 스크롤하여 지난 7 일, 30 일 또는 90 일 동안 이 데이터의 추세를 보여주는 그래프를 볼 수 있습니다.
  - 소프트웨어 릴리스가 구식 장치의 증가에 어떻게 대응하는지 확인할 수 있습니다.

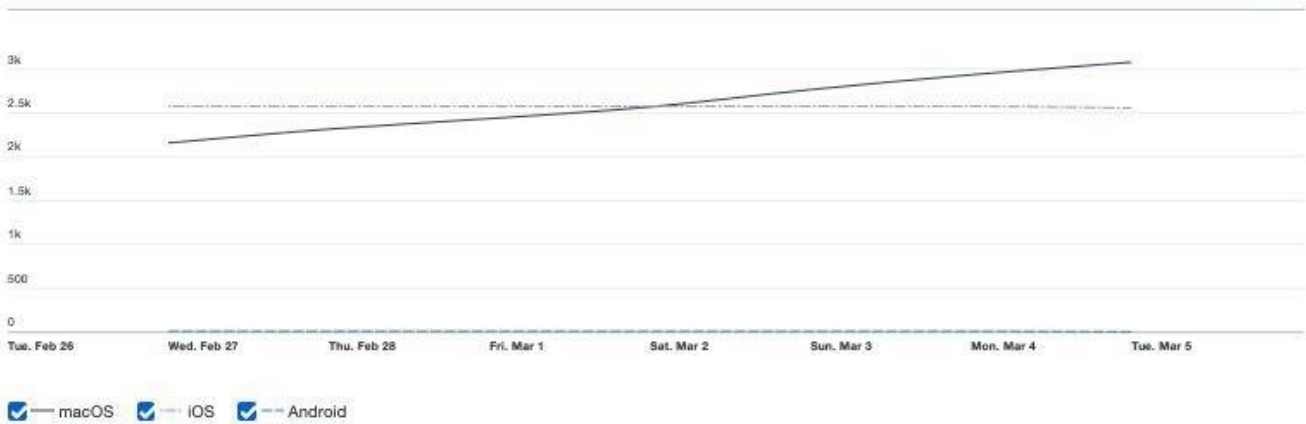
## Endpoints With Out-of-Date Operating Systems

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



## Historical Data

> Last 7 days



**참고:** 공격에 취약한 또 다른 영역인 브라우저(및 브라우저 플러그인)에서도 동일한 추세 데이터를 사용할 수 있습니다.

### Endpoints With Out-of-Date Browsers

Which browsers do we consider up-to-date? ▾

**17744**

Total Out-of-Date Endpoints

[Create policies for these endpoints](#)

**0**

Internet Explorer

**1533**

Firefox

[View All](#)

**821**

Edge

[View All](#)

**196**

Safari

[View All](#)

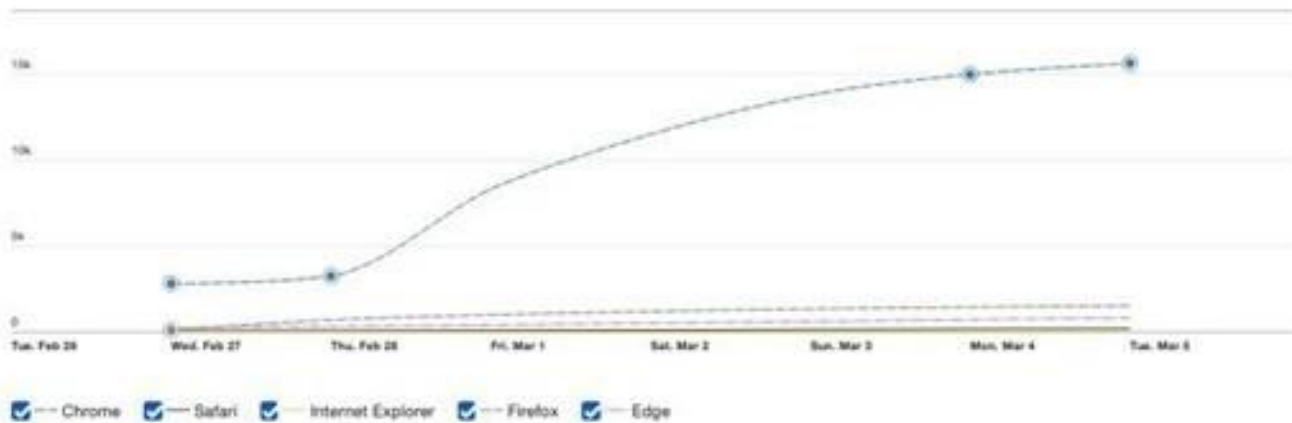
**15636**

Chrome

[View All](#)

### Historical Data

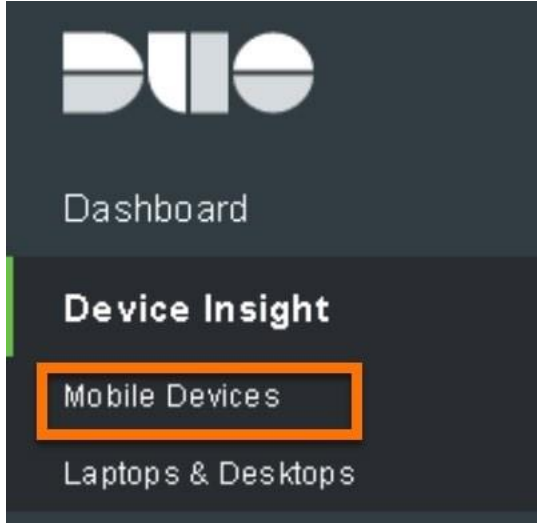
[Last 7 days](#)





### Mobile Devices

1. **Admin Panel** 에서 **Device Insight > Mobile Devices** 선택하십시오.



2. 사용 중인 모바일 장치에 대한 자세한 내용을 보려면 **Mobile Devices** 화면을 보십시오. 여기에는 Duo Mobile 애플리케이션이 설치된 장치와 Duo 로 보호되어 있는 브라우저 기반 회사 리소스에 접근하는 장치가 모두 포함됩니다.

[Dashboard](#) > [Mobile Devices](#)

## Mobile Devices

### Device Breakdown

out of 24286 total devices



### 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	<a href="#">View devices</a>
iOS 12.0	3	<a href="#">View devices</a>
iOS 11.4	1	<a href="#">View devices</a>

### Android

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

Version	Devices	
9.0 (Pie)	7089	<a href="#">View devices</a>
9	1	<a href="#">View devices</a>
8.1 (Oreo)	2	<a href="#">View devices</a>

- 화면의 **Device Breakdown** 섹션에서 다양한 OS 플랫폼에 대한 세부 정보를 확인한 다음 iOS 와 Android 의 특정 버전을 보다 세분화하십시오.

**참고:** 이러한 통찰력은 관리자가 Spectre 및 Meltdown 과 같은 취약성과 관련된 위험 프로파일을 이해하는 데 매우 중요합니다.

- 아래로 스크롤하여 장치가 **변조되었는지(tampered)** (즉, 탈옥 또는 루팅, 화면 잠금 활성화 여부, 생체 인식 활성화 여부, 모든 iOS 장치에서 기본적으로 활성화되는 대로 Android 장치에서 디스크 암호화가 활성화되는지 여부) 확인하십시오.

**Tampered**  
 These devices may be less secure due to being jailbroken. [What is a tampered device?](#)

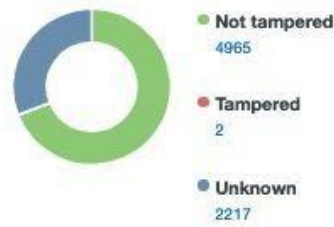


Your global policy blocks tampered iOS and Android devices. To make changes, [edit global policy.](#)

**Screen Lock**  
 Enforcing a screen lock can help prevent against unwanted access.



**Tampered**  
 These devices may be less secure due to being rooted or failing Google's SafetyNet device attestation. [What is a tampered device?](#)



**Screen Lock**  
 Enforcing a screen lock can help prevent against unwanted access.



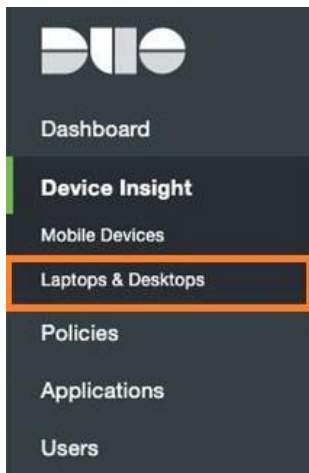
**참고:** 이러한 통찰력과 해당 정책( 시나리오 3 에서 설명됨)을 통해 회사 데이터에 접근하는 장치의 암호화 및 화면 잠금이 필요할 수 있는 컴플라이언스 규정을 해결할 수 있습니다.

**참고:** 이 모든 데이터는 기본적으로 Duo Mobile 애플리케이션을 사용하여 캡처됩니다. 따라서 에이전트가 필요하지 않습니다.

## Laptops &amp; Desktops

**가치 제안:** 최근 3 월 초 Google Chrome 제로 데이에서 이러한 심각한 취약성을 발견했습니다. Duo 고객은 사용자가 사용중인 Chrome 버전을 확인할 수 있을 뿐만 아니라 사용자가 업데이트할 때까지 Chrome 에서 접근을 제한하는 다음 스텝을 수행할 수 있었습니다.

1. **Admin Panel** 에서 **Device Insight > Laptops & Desktops** 선택합니다.



**참고:** 이 모든 데이터는 사용자가 Duo 로 보호되는 브라우저 기반 리소스에 로그인할 때마다 Duo 에 의해 캡처되며, 에이전트도 필요하지 않습니다.

2. **Laptops & Desktops** 화면에서 기업 관리 및 BYO 장치 모두에 대해 환경에서 사용되는 운영 체제에 대한 높은 수준의 분석을 확인할 수 있습니다.

[Dashboard](#) > [Laptops & Desktops](#)

## Laptops & Desktops

### Operating Systems

out of 61888 total devices



Mac OS X		
Version	Device Count	
10.14	10703	<a href="#">View Devices</a>
10.13	1120	<a href="#">View Devices</a>

Windows		
Version	Device Count	
10	19246	<a href="#">View Devices</a>
8	3191	<a href="#">View Devices</a>
Unknown	427	<a href="#">View Devices</a>
Vista	7	<a href="#">View Devices</a>

3. 높은 수준의 OS 정보 다음에 특정 OS 버전이 뒤따른다는 점에 유의하십시오.
4. 브라우저 플랫폼과 특정 버전에 대한 유사한 분석을 보려면 아래로 스크롤하십시오.



### Browsers

out of 39138 installed browsers



#### 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	<a href="#">View Devices</a>
71	2825	<a href="#">View Devices</a>

#### Internet Explorer

Version	Device Count	
11	4207	<a href="#">View Devices</a>

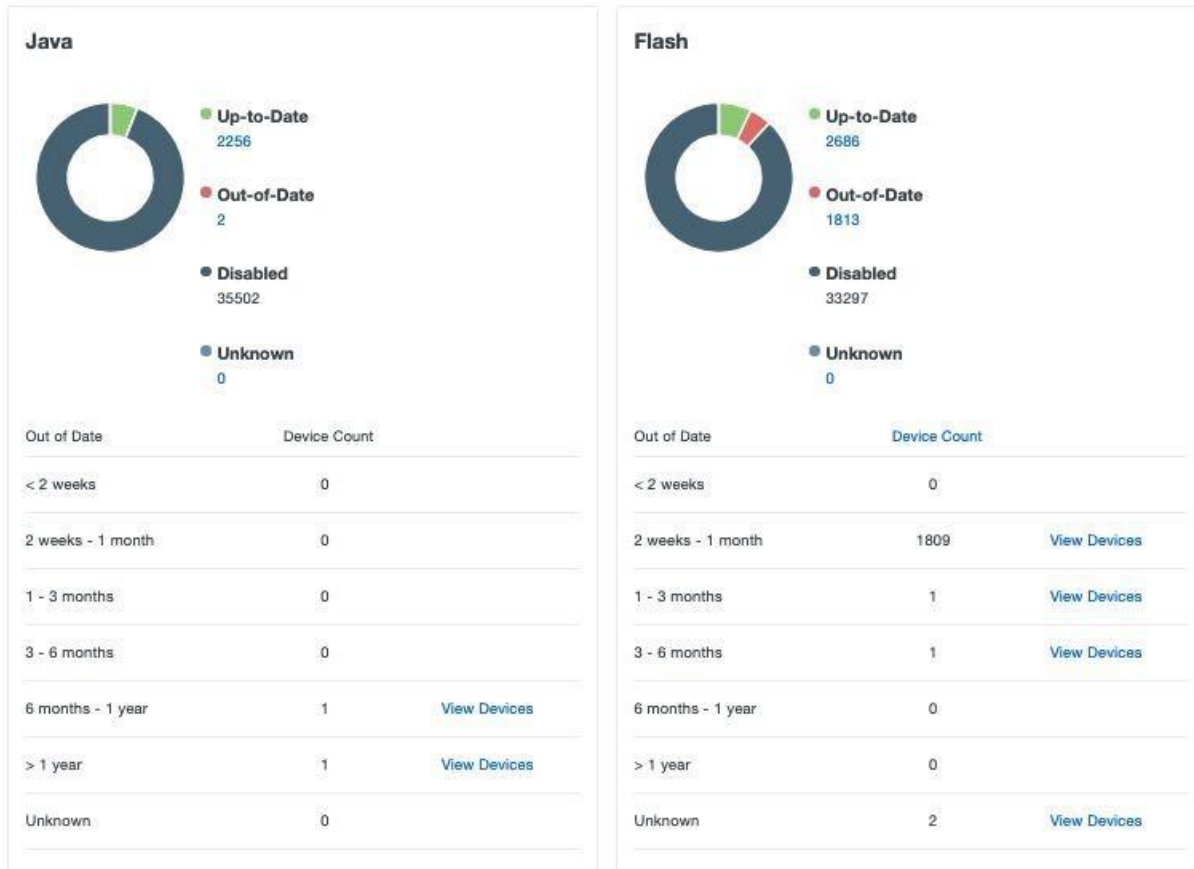
**Vulnerability Analysis**

**가치 제안:** 다른 소프트웨어와 마찬가지로 오래된 브라우저는 악용에 취약합니다. 또한 최종 사용자가 개인 및 잠재적으로 의심스러운 웹 사이트와 함께 점점 더 많은 기업 리소스에 접근하기 위해 브라우저를 매일 사용하기 때문에 브라우저의 공격 영역이 매우 넓습니다. 공격자는 오래된 브라우저를 취약하게 인식하여 공격을 시작하므로 브라우저가 최신 상태인지 확인하는 것이 많은 공격을 완화하는 중요한 방법이 됩니다.

- 더 아래로 스크롤하여 Java 및 Flash 플러그인의 상태를 확인하여 플러그인이 활성화되었는지 여부와 활성화된 경우 최신 상태인지 확인하십시오.

**참고:** Java 와 Flash 플러그인에 대한 릴리스 노트(특히 보안 업데이트)만 검토하여 이 두 가지 모두를 비활성화하거나 최신 상태로 유지하는 것이 얼마나 중요한지 파악할 수 있습니다.

**Plugins**



- 다음 플러그인 옵션 중 하나를 클릭하여 특정 장치와 관련 사용자를 드릴다운하고 확인하십시오.





- Dashboard
- Device Insight
- Policies
- Applications
- Users
- Endpoints
- 2FA Devices
- Groups
- Administrators
- Trusted Endpoints Configuration
- Reports
- Phishing
- Accounts
- Settings
- Billing

Dashboard > 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**

- Android
- Chrome OS
- Linux
- Mac OS X
- Windows
- iOS

**Filter OSs by age**

- Latest
- Up-to-Date
- Unknown
- Out-of-Date
- End-of-Life

**Browsers**

- Chrome

Export

OS	Browsers	Security Warnings	User	Last Used (CST)	Trusted Endpoint
Chrome OS 6783.1.0	<ul style="list-style-type: none"> <li>Chrome 71.0.3578.127</li> <li>Flash 32.0.0.114</li> <li>Java 1.8.0.201</li> </ul>	Flash out-of-date	amanda_fisher	Feb 26, 2019 12:16 AM	Unknown
Chrome OS 6783.1.0	<ul style="list-style-type: none"> <li>Chrome 71.0.3578.127</li> <li>Flash 32.0.0.114</li> </ul>	Flash out-of-date	pullman_karen	Feb 26, 2019 12:16 AM	Unknown

**참고:** 이 모든 데이터는 Duo 의 플랫폼에 180 일 동안 유지되며 다른 플랫폼(예: Splunk, Rapid7 및 기타 SIEM)으로 내보낼 수 있습니다.

© 2019 Cisco and/or its affiliates. All rights reserved. 해당 문서는 Cisco 공개용 문서입니다.

Page 14 of 19

## 시나리오 3. 정책 관리

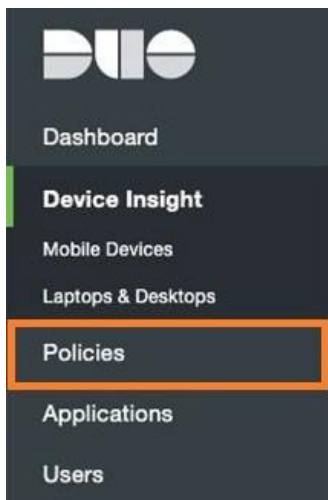
**가치 제안:** 이 시나리오에서는 관리자가 장치 데이터를 기반으로 설정할 수 있는 정책을 검토하고 최신 보안 장치만 애플리케이션에 액세스하도록 Duo 장치 정책을 사용하는 방법을 보여 줍니다.

일반적으로 이러한 정책은 관리자의 상호 작용이 거의 필요하지 않습니다. 그러나 올해 초 발견된 제로 데이 Chrome 취약성과 같은 새로운 위협이 발생할 경우 관리자는 로그인하여 몇 번의 클릭만으로 2 주 정책을 업데이트 즉시 정책으로 변경할 수 있으며, 지속적으로 변화하는 위협 환경에서도 조직의 보안 상태를 즉시 개선할 수 있습니다.

**참고:** Duo 는 소프트웨어 업데이트 목록을 유지 관리하므로 새 버전이 출시될 때마다 정책을 지속적으로 확인하고 업데이트할 필요가 없습니다.

### 스텝

1. **Admin Panel** 에서 **Policies** 을 선택하십시오.



2. 이미 구성된 정책을 검토하고 다음과 같은 세 가지 수준에서 Duo 정책이 시행될 수 있음을 확인합니다.
  - **글로벌.** 모든 사용자 및 애플리케이션에 적용되는 정책
  - **애플리케이션.** 할당된 특정 애플리케이션에 적용되는 정책
  - **그룹.** 특정 애플리케이션에 연결하는 특정 사용자 그룹에 적용되는 정책

**참고:** 이 3 가지 정책 수준을 사용하면 관리 부담을 최소화하면서 비즈니스 운영에 필요한 접근만 제공하는 포괄적인 보안 정책을 만들 수 있습니다.

3. 아래로 스크롤하여 **Workday Administrators** 정책을 확인하십시오.

- 이 클라우드 기반 엔터프라이즈 리소스 계획 솔루션의 관리자로서 이러한 사용자는 조직의 미션 크리티컬 애플리케이션으로 매우 높은 권한을 가지고 있습니다.

- **Workday Administrators** 는 보다 제한적인 접근 정책을 요구합니다.
- 그룹 수준 정책을 사용하므로 Workday administrators 만 영향을 받게 되며 표준 사용자 로그인에 대해 덜 제한적인 정책을 만들 수 있습니다.

### Workday Administrator Edit

**Policy Key** POC0V87BZS2D10303DTD

This policy applies to: [Workday](#).

✔ Enabled	<b>New User Policy</b>	Deny access to unenrolled users.
✔ Enabled	<b>User Location</b>	No action: United States. All other countries: Deny access.
✔ Enabled	<b>Trusted Endpoints</b>	Only allow trusted endpoints.
✔ Enabled	<b>Remembered Devices</b>	Users may choose to remember their device for 1 hour per application.

4. 위로 스크롤하여 **User Location** 정책이 미국에서의 Allow Access 및 다른 모든 국가의 Deny Access 로 구성되었음을 확인하십시오.

✔ Enabled	<b>User Location</b>	No action: United States. All other countries: Deny access.
-----------	----------------------	---

**가치 제안:** 이 경우, 모든 관리자가 미국에 있으며 절대 업무차 여행하지 않는다는 것을 알 수 있습니다. 다른 글로벌 위치 및/또는 직원이 이러한 지역 이외의 지역으로 자주 출장을 가는 경우 미국 이외의 지역에서 로그인할 수 있는 사용자를 위해 별도의 세분화된 그룹 정책을 만들 수 있습니다.

5. **Trusted Endpoints** 정책을 보십시오.
- 현재 이 설정은 관리자가 회사의 관리되고 신뢰할 수 있는 엔드포인트를 통해서만 **Workday** 에 로그인할 수 있도록 설정되어 있습니다. 이것은 EMM (예 : Jamf)에서 관리하는 노트북이거나 회사 MDM 에 등록된 모바일 장치 (예 : Airwatch) 일 수 있습니다.

✔ Enabled	<b>Trusted Endpoints</b>	Only allow trusted endpoints.
-----------	--------------------------	-------------------------------

**참고:** Workday 는 매우 민감한 데이터를 포함하는 중요한 애플리케이션이므로 관리되는 신뢰할 수 있는 장치의 필요성을 보장합니다. 조직 내에 중요도가 낮은 다른 애플리케이션이나 사용자 그룹이 있을 수 있으며 따라서 그 장치가 최신 상태로 유지되는 한 BYO 장치에서 액세스가 허용될 수 있습니다.



6. 아래로 스크롤하여 사용자가 Workday 에 로그인할 때 Chrome 을 사용해야 하는 **Browsers** 정책도 설정되었는지 확인하고 Chrome 이 2 주 이상 지난 상태일 수 없음을 지정하십시오.

- 브라우저가 최신 버전이 아닌 경우 Workday 에 로그인할 때 즉시 사용자가 알림을 받기 시작하지만 처음 2 주 동안은 업데이트 실행을 편리해질 때까지 연기할 수 있습니다.
- 그러나 2 주 이상 기다리면 차단되고 업데이트해야 들어갈 수 있습니다.

Notify users when their browser version is out of date.

Enabled **Browsers**

Block users when their browser version is more than 2 weeks out of date.

Only allow devices accessing applications using Chrome.

**가치 제안:** Duo 는 사용자에게 차단된 이유뿐만 아니라 장치 업데이트 방법을 알려주기 때문에 IT 또는 관리자 지원 없이도 이 프로세스를 완료할 수 있으므로 헬프데스크 부담을 줄이고 솔루션 해결 방법에 대한 단계별 지침을 제공하여 비즈니스 사용자도 시간을 낭비하지 않습니다. 이 경우 이들은 관리자입니다. 따라서 로그인 보호뿐만 아니라 Duo 가 나머지 사용자에게 제공하는 가치를 인식할 수 있습니다.

화면 하단에 있는 **모바일** 정책에 유의하십시오.

Enabled **Tampered Devices**

Don't allow authentication from tampered devices.

Enabled **Screen Lock**

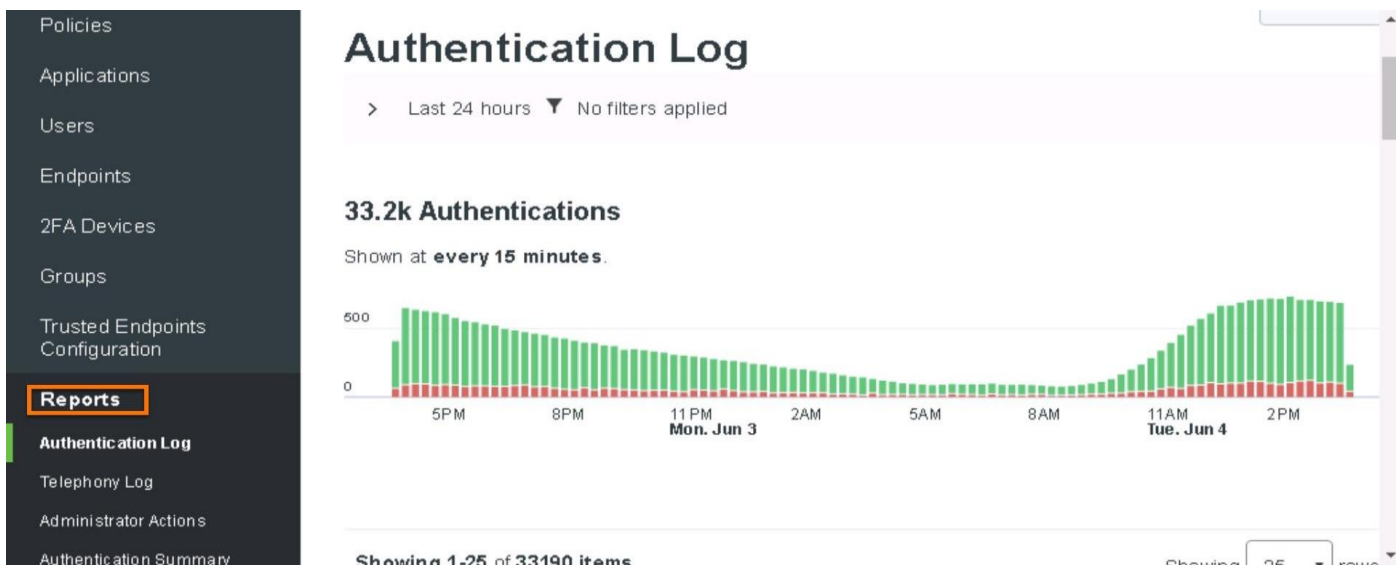
Don't allow authentication from devices without a screen lock.

Enabled **Full-Disk Encryption**

Don't allow authentication from Android devices without full-disk encryption.

**참고:** 이러한 각 기능은 관리자가 빠르고 쉽게 구성할 수 있도록 설계되었으며, 사용자가 화면 잠금을 활성화하도록 요구하거나 장치가 손상되지 않도록 하는 등 강력한 보안 모범 사례를 준수하고 있음을 보장합니다.

7. **Admin Panel** 에서 **Authentication Log** 를 볼 **Reports** 를 선택하여 Duo 정책으로 인해 애플리케이션에 로그인할 수 없는 사용자의 예를 확인하십시오.



8. 필터 아이콘을 클릭하여 필터 필드 및 필터 옵션을 표시하십시오. **Access Denied** 상자를 선택하십시오.

# Authentication Log

▼ Last 24 hours ⌵ **26 filters applied** (clear all)

Filter by user, application, or group

### Time Range

- Custom
- Last 24 hours
- Last 48 hours
- Last 7 days
- Last 30 days
- Last 60 days

### Authentication Result

- ✓ Access granted
- ✗ Access denied
- Enrolled

### Second factor

- Duo Push
- Phone Call
- Hardware Token
- WebAuthn & U2F [+]
- Passcode [+]
- Other [+]

9. 사용자의 로그인이 금지된 여러 인증 이벤트(위치 제한, 구식 장치 등)가 나타날 때까지 아래로 스크롤하십시오.

Showing 1-25 of 1824 items

Showing 25 rows

Timestamp (CDT) ▼	Result	User	Application	Access Device	Second Factor
1:16 PM APR 12, 2019	✗ Denied Location restricted	donna_grant	LastPass	Singapore 165.173.23.127	Unknown
1:15 PM APR 12, 2019	✗ Denied User mistake	nicola_clark	SAML - Box	› Windows 10	› Duo Push Brooklyn, NY
1:15 PM APR 12, 2019	✗ Denied Software restricted	carol_cornish	SAML - Office 365 2	› Mac OS X 10.13.5	Unknown
1:15 PM APR 12, 2019	✗ Denied Out of date	john_hughes	SAML - Salesforce	› Windows 8	Unknown



## What's Next?

[Duo Security Proposal](#) 을 통해 Duo Security 가 온프레미스 또는 클라우드의 모든 애플리케이션에 간편하고 안전하게 접근할 수 있는 방법을 알아보십시오.



---

### Americas Headquarters

Cisco Systems, Inc.  
San Jose, CA

### Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.  
Singapore

### Europe Headquarters

Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)