

# Duo 管理者パネル v1 : インスタント デモ



最終更新日 : 08-July-2019

## インスタント デモについて

この事前設定済みデモ ガイドの内容は次のとおりです。

[インスタント デモについて](#)

[このソリューションについて](#)

[はじめに](#)

シナリオ 1 : [ダッシュボードの表示](#)

シナリオ 2 : [デバイスの分析情報の表示](#)

シナリオ 3 : [ポリシーの管理](#)

[次に必要な作業](#)

## 要件

必須	オプション
ラップトップ	Cisco AnyConnect®

## このソリューションについて

この **Duo 管理者パネル (Duo Admin Panel)** インスタント デモでは Duo の管理作業について説明します。Duo アカウントに関するほとんどの設定は Duo 管理者パネルで行います。管理者は新しいアプリケーションの統合やユーザ登録などの設定を実行できます。また、企業リソースにアクセスしているデバイスに対するポリシーを表示して設定し、セキュリティ態勢をより深く理解できます。Duo はモバイルとデスクトップの両カテゴリの主要なデバイスプラットフォームでデータをキャプチャし、詳しい分析情報を提供します。

通常、MDM や EMM などのソリューションでは、重要なデバイス データをキャプチャするためにデバイスにエージェントをインストールする必要があります。これらエージェントでは、デバイスのユーザが複数の権限を管理者に与える必要があることが多く、ユーザが不安を感じる場合があります。

以下は **Duo 管理者パネル**が提供する利点の一部です。

- Duo はエージェントを必要とせずにデータをキャプチャ可能。Duo で保護されたアプリケーションにユーザがログインするたびにキャプチャを実行。
- エンド ユーザに Duo の存在を意識させない透過性。
- 管理者が追加のセットアップや設定を行うことなく、そのままデータをキャプチャ可能。

さらに、**Duo 管理者パネル**では、最新でセキュアなデバイスだけがアプリケーションにアクセス可能なようにデバイス ポリシーを設定できます。

## はじめに

### プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

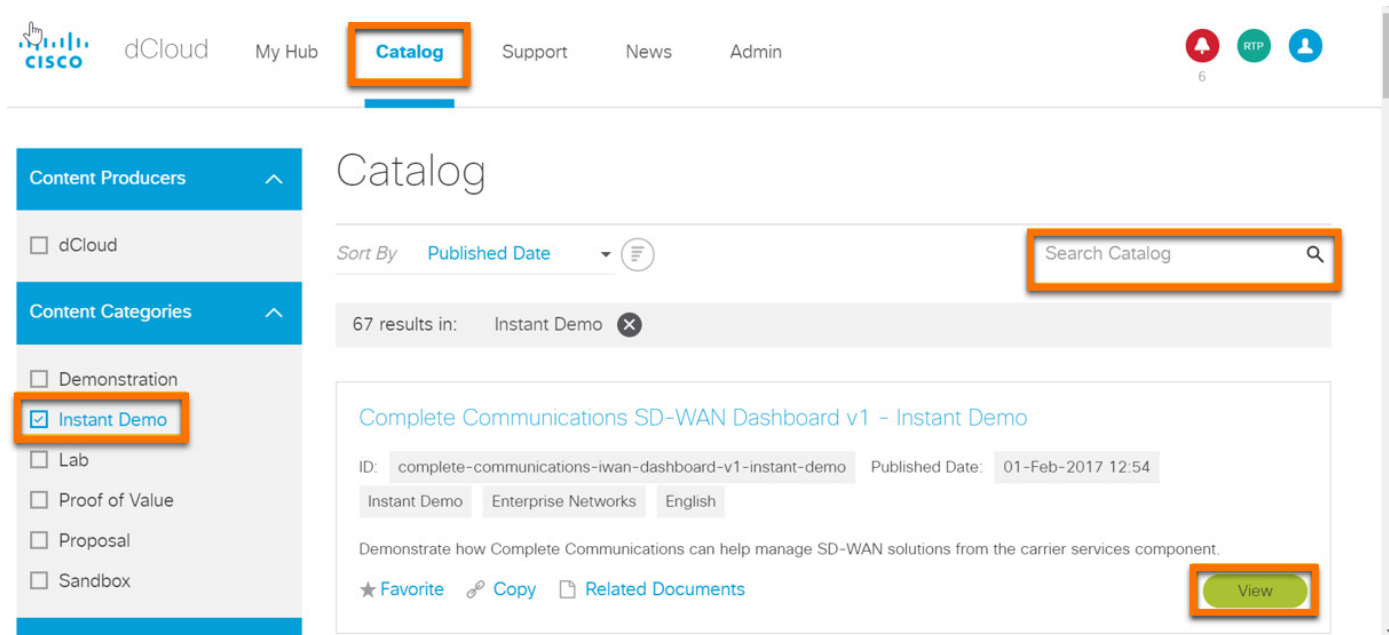
場合によっては、環境を元の構成にリセットするため、このガイドのシナリオを完了した後に新しいセッションをスケジュールする必要があります。

**プレゼンテーションを成功させるには入念な準備が不可欠です。**

次の手順に従ってインスタント アクセス コンテンツのセッションを開始し、プレゼンテーション環境を設定します。

1. [カタログ (Catalog) ]をクリックして、サイド バーから [インスタントデモ (Instant Demo) ]を選択します。  
これで、すべての dCloud インスタント デモが一覧表示されます。
2. [表示 (View) ]をクリックします。

**注 :** [カタログ検索 (Search Catalog) ] ボックスを使用して**インスタント デモ (Instant Demo)** の名前を検索することもできます。



The screenshot shows the Cisco dCloud interface. At the top, the navigation bar includes 'dCloud', 'My Hub', 'Catalog' (highlighted with an orange box), 'Support', 'News', and 'Admin'. On the right, there are notification and user icons. The left sidebar has 'Content Producers' and 'Content Categories' sections. Under 'Content Categories', 'Instant Demo' is selected (highlighted with an orange box). The main area is titled 'Catalog' and shows search results. A search box labeled 'Search Catalog' is highlighted with an orange box. Below it, 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', the published date '01-Feb-2017 12:54', and tags 'Instant Demo', 'Enterprise Networks', and 'English'. 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).

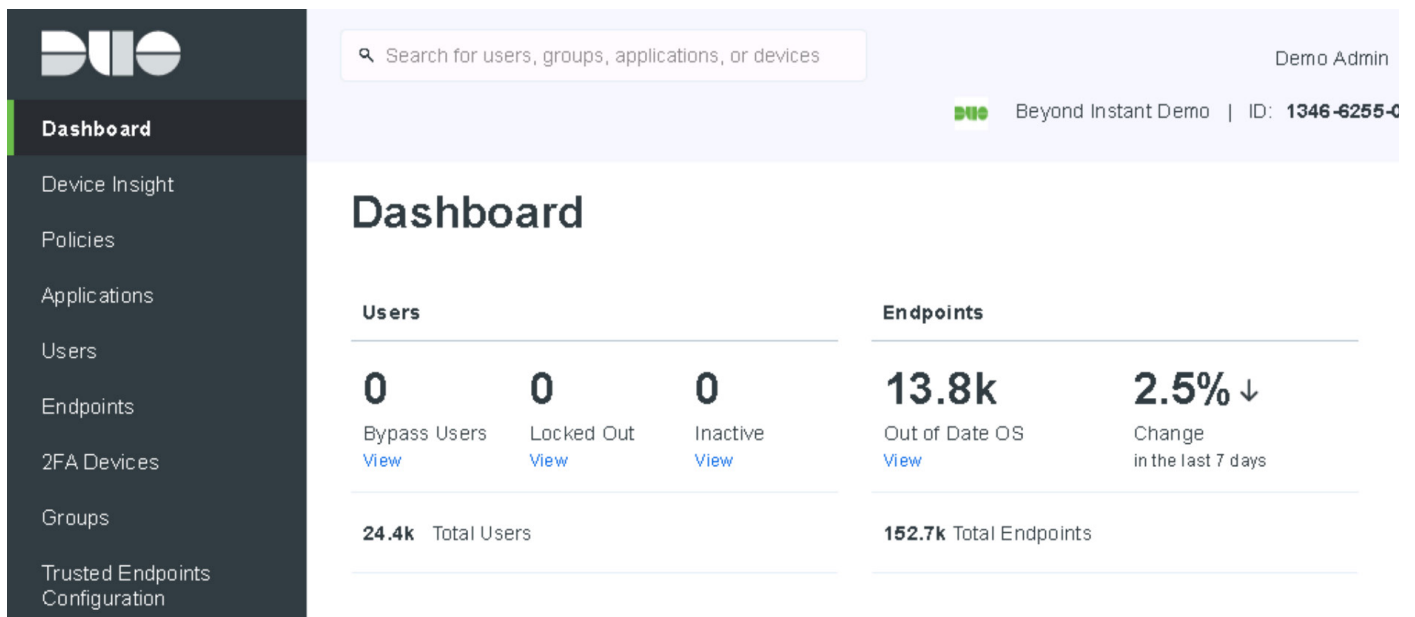
## シナリオ 1： ダッシュボードの表示

**価値提案：**ダッシュボードでは、組織内にある Duo インスタンスを管理できるほか、Duo 全体の稼働状況を表示できます。

### 手順

1. **Duo 管理者パネル**にログインすると、Duo **ダッシュボード**画面になり、企業リソースにアクセスしているユーザとデバイスの詳細が表示されます。

**注：**デモの Duo **管理者パネル**には、一般的なお客様のデータが例として入力されています。



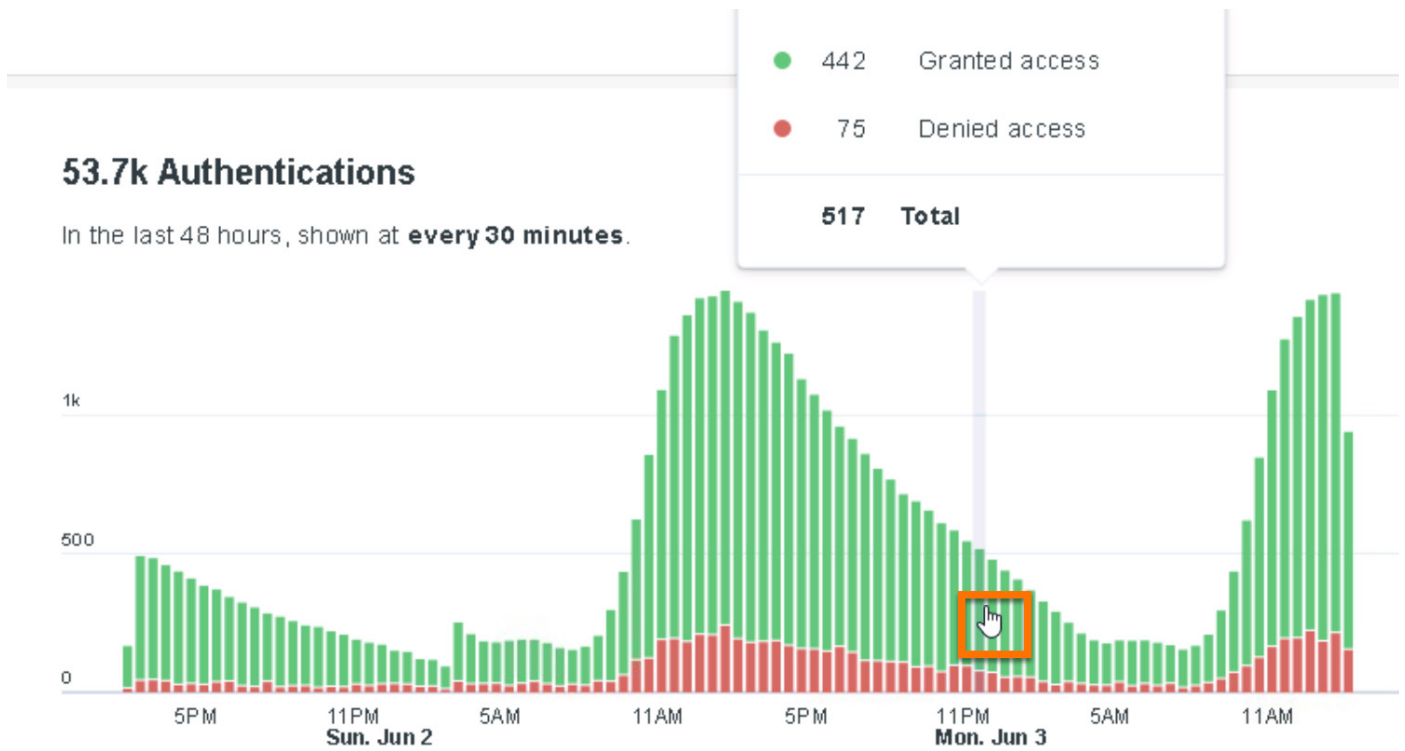
Users			Endpoints	
0	0	0	13.8k	2.5% ↓
Bypass Users <a href="#">View</a>	Locked Out <a href="#">View</a>	Inactive <a href="#">View</a>	Out of Date OS <a href="#">View</a>	Change in the last 7 days
24.4k Total Users			152.7k Total Endpoints	

2. **ダッシュボード**を確認します。以下の情報が表示されています。

- 登録済みユーザの数。
- 登録済みデバイスの数。
- 認証データ履歴。
- 緊急性が高い可能性のある状況（現在ロックアウトされているユーザの数など）。

3. [認証 (Authentications) ] セクションでヒストグラムの棒グラフにマウス ポインタを合わせると、その期間の認証の詳細を確認できます。

- 期間 (選択した棒グラフが示す)。
- アクセスを許可 (Granted Access) されたユーザの数。
- アクセスを拒否 (Denied Access) されたユーザの数。



4. [認証ログ (Authentication Log) ] セクションまで下にスクロールすると、認証に関するさらに詳しい情報が表示されます (ユーザ名、アプリケーションなど)。

## Authentication Log Last 10 attempts

### Full authentication log

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

## シナリオ 2： デバイスの分析情報の表示

**価値提案：**このシナリオでは、環境内のデバイスについて Duo で表示されるデータを示します。このデータには多くの価値があります。組織の多くでは、会社のラップトップを使うよう従業員に求めています。その方針を守る技術的な方法がありません。何も対策を取らないと、エンド ユーザが各自の個人デバイスから Outlook Web App などのリソースにアクセスする可能性があります。企業リソースに個人デバイスでアクセスされると、脆弱なバージョンの Windows (Vista など) を実行していても把握できないため、これはかなり危険です。

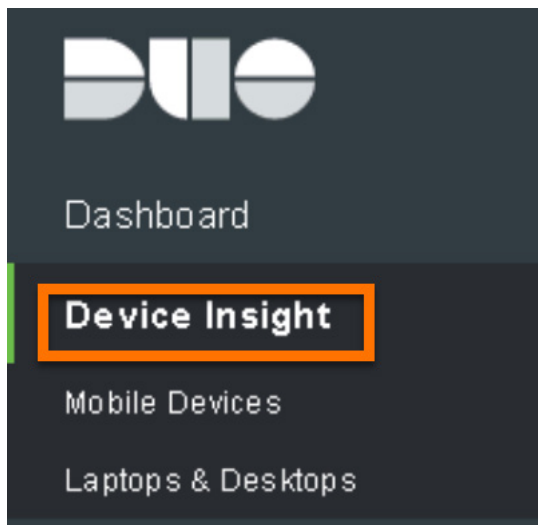
このデモでは、Duo **管理者**パネルの 3 つの領域に焦点を当てます。

- デバイス インサイト (概要)
- モバイル デバイス
- ラップトップおよびデスクトップ

### 手順

#### 概要

1. 管理者パネル (Admin Panel) で [デバイスインサイト (Device Insight) ] を選択し、[デバイスインサイト (Device Insight) ] 画面を表示します。



2. [デバイスインサイト (Device Insight) ] 画面を詳しく確認します。
  - 企業アプリケーションにアクセスするラップトップやデスクトップなどのデバイスすべて、およびモバイルデバイス (多要素認証に使うデバイスも含む) の概要を確認します。
  - 最新デバイスと旧型デバイスの割合など、オペレーティング システムの分布を確認します。管理者は、管理対象デバイスと管理対象外デバイスの数を比較することもできます。



[Dashboard](#) > Device Insight

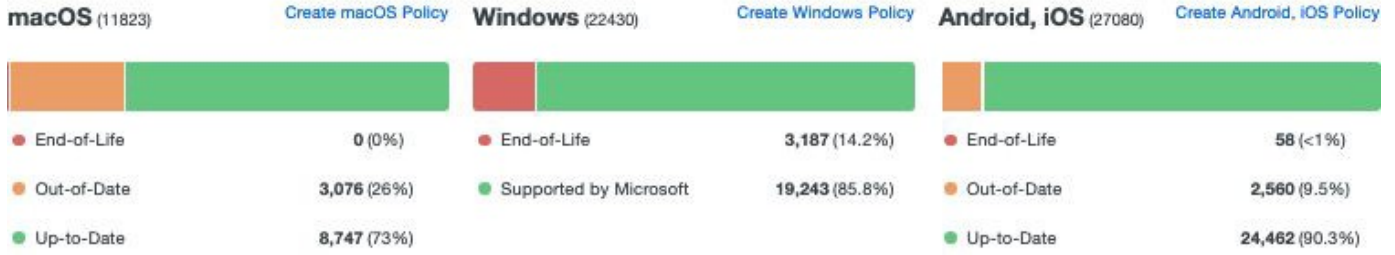
## Device Insight

Print

Page Glossary

All Endpoints Trusted Endpoints Not-Trusted Endpoints

### Operating Systems by Platform



Includes major Windows versions, not patch levels.

Access devices + 2FA devices using Duo Mobile

3. 下にスクロールすると、このデータの直近 7 日、30 日、90 日のトレンドを示すグラフを確認できます。

- 最近のソフトウェア リリースと旧型デバイスの上昇が対応していることに注目してください。

### Endpoints With Out-of-Date Operating Systems

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

**5636**

Total Out-of-Date Endpoints

[Create policies for these endpoints](#)

**3076**

macOS

[View All](#)

**2555**

iOS

[View All](#)

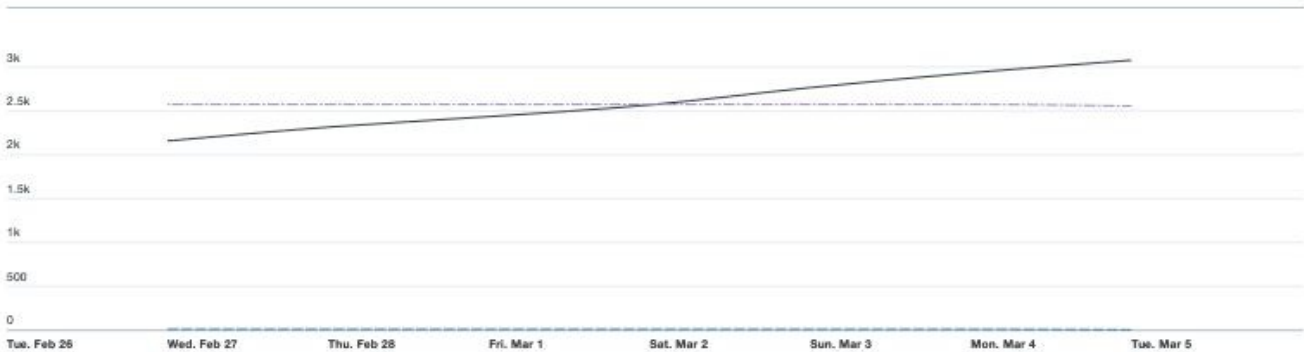
**5**

Android

[View All](#)

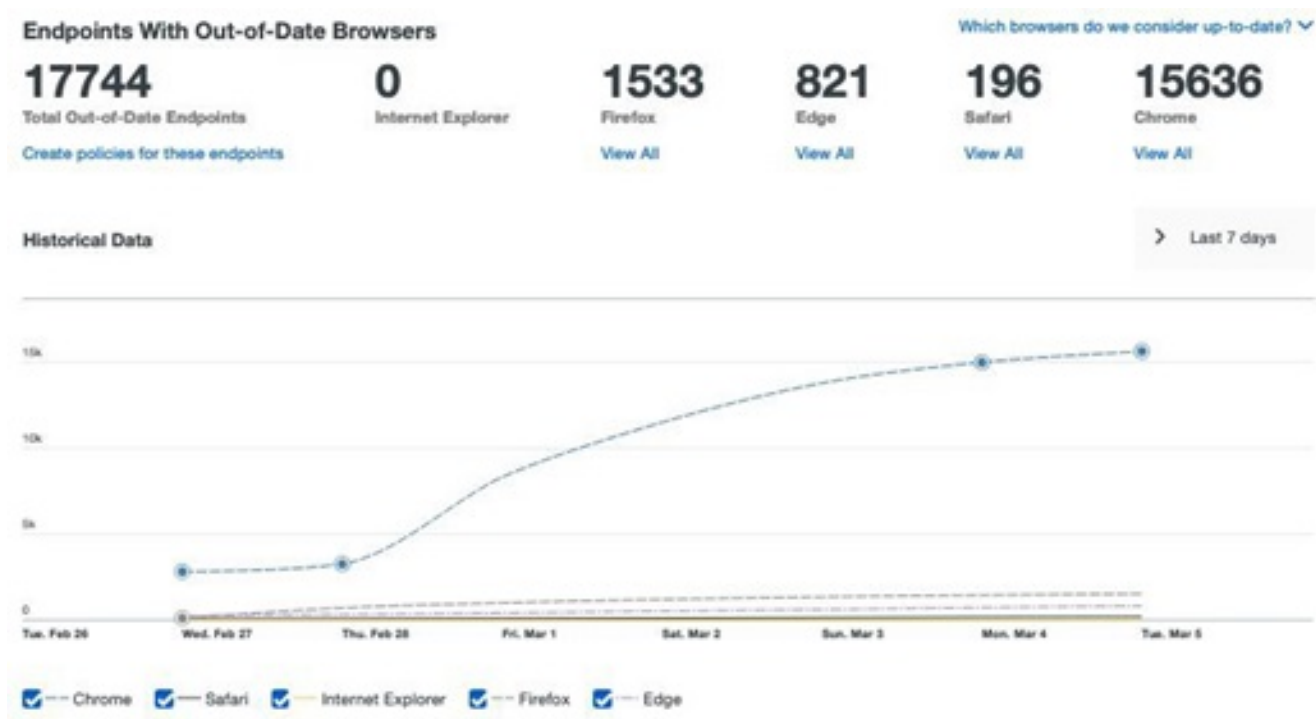
### Historical Data

> Last 7 days



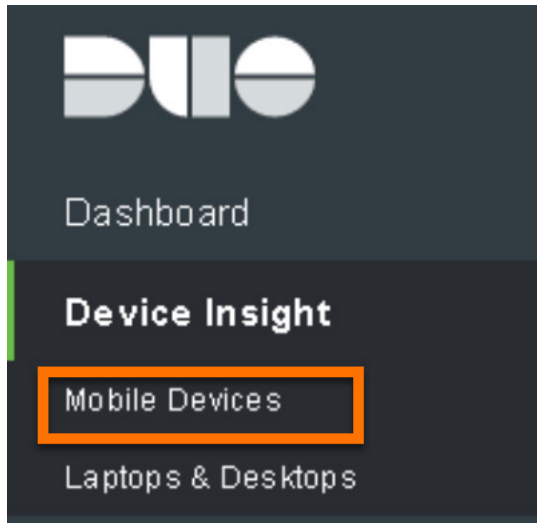
macOS  iOS  Android

注：ブラウザ（およびブラウザ プラグイン）も攻撃に対する脆弱性がよく見られますが、これらについても同様のトレンド データを利用できます。



## モバイル デバイス

1. 管理者パネルで、[デバイスインサイト (Device Insight) ] > [モバイルデバイス (Mobile Devices) ] を選択します。



2. [モバイルデバイス (Mobile Devices) ] 画面には、使用中のモバイル デバイスの詳細な内訳が表示されます。これには Duo モバイル アプリケーションをインストールしているデバイスと、Duo で保護されているブラウザベースの企業リソースにアクセスするデバイスの両方が含まれます。

[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

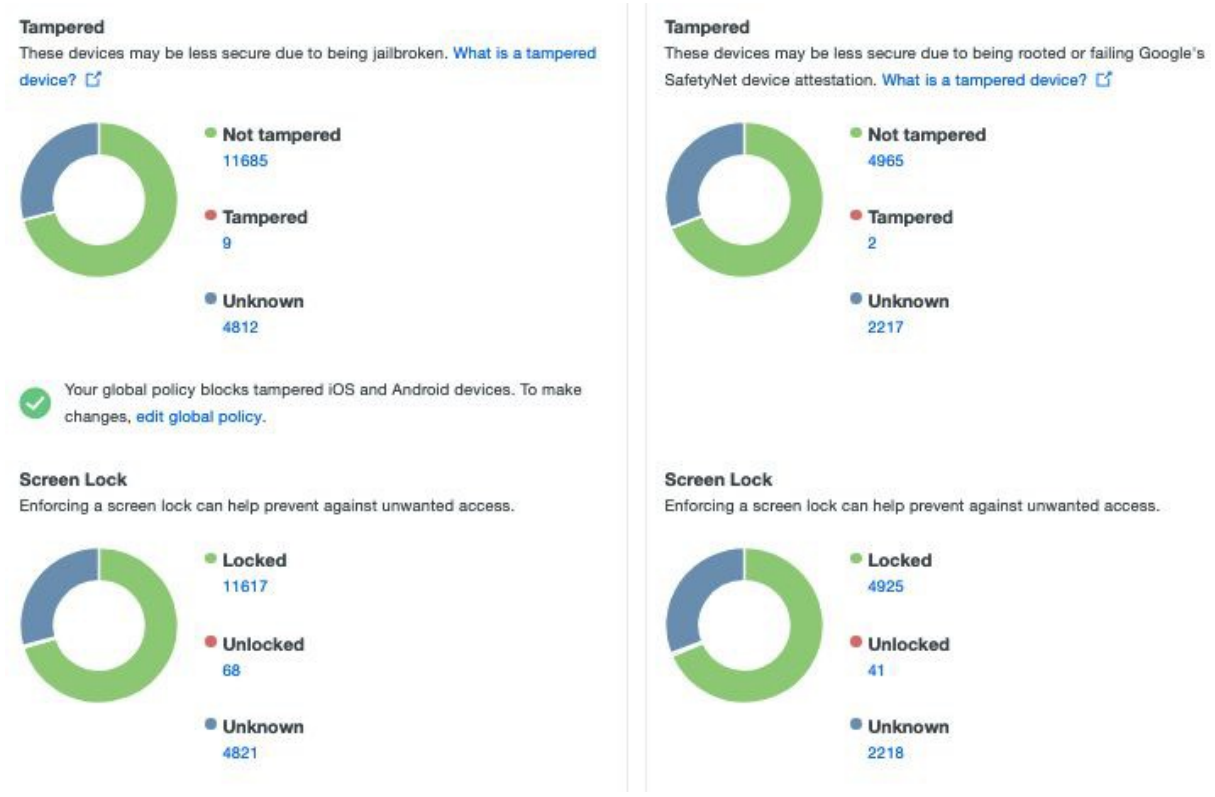
Data may be unknown for devices running versions of Duo Mobile prior to 3.5.

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>

3. 画面の [デバイスの内訳 (Device Breakdown) ] セクションには、プラットフォームのさまざまな OS の内訳が表示され、iOS と Android それぞれの詳しいバージョンも表示されます。

注：この分析情報は、管理者が Spectre や Meltdown などの脆弱性に関連するリスク プロファイルを把握するために重要です。

4. 下にスクロールして、これらのデバイスが改ざんされているかどうか（脱獄、または root 化されている）、画面ロックが有効かどうか、バイOMETリックが有効かどうか、Android デバイスでディスク暗号化が有効かどうか（すべての iOS デバイスではデフォルトで有効）を確認します。



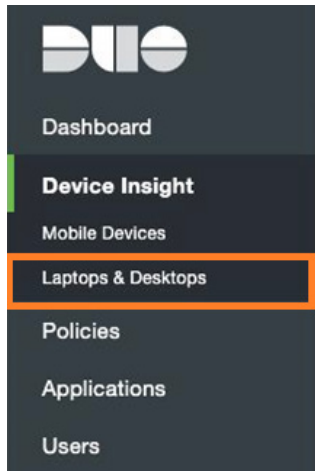
注：これらの分析情報は、対応するポリシー（シナリオ 3 で説明）と共に、企業データにアクセスするデバイスに暗号化と画面ロックを求めるコンプライアンス規制で役立ちます。

注：このデータはすべて、Duo モバイル アプリケーションを使用してネイティブにキャプチャされます。このためエージェントは必要ありません。

## ラップトップおよびデスクトップ

**価値提案**：3月初旬、Google Chrome に対してゼロデイ攻撃が発生し、重大な脆弱性があることが発覚しました。この時 Duo を利用する企業は、エンド ユーザが使用していた Chrome のバージョンを把握していただだけでなく、エンド ユーザの Chrome が更新されるまで Chrome からのアクセスを制限することもできました。

1. 管理者パネルで、[デバイスインサイト (Device Insight) ] > [ラップトップおよびデスクトップ (Laptops & Desktops) ] の順に選択します。



**注**：このすべてのデータは、Duo で保護されたブラウザベースのリソースにユーザがログインするたびに Duo でキャプチャされます。エージェントは必要ありません。

2. [ラップトップおよびデスクトップ (Laptops & Desktops) ] 画面で、環境で使われている企業の管理対象デバイスと BYO デバイスの両方についてオペレーティング システムの内訳の概要を確認します。

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

## Laptops & Desktops

### Operating Systems

out of 61888 total devices



#### Mac OS X

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

#### Windows

Version	Device Count	Action
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. 最初に OS 情報の概要が表示され、その後に OS バージョンごとのデータが表示されます。
4. 下にスクロールして、ブラウザ プラットフォームと各バージョンの同様の内訳を確認します。

### 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			Internet Explorer		
Version	Device Count		Version	Device Count	
72	17683	<a href="#">View Devices</a>	11	4207	<a href="#">View Devices</a>
71	2825	<a href="#">View Devices</a>			

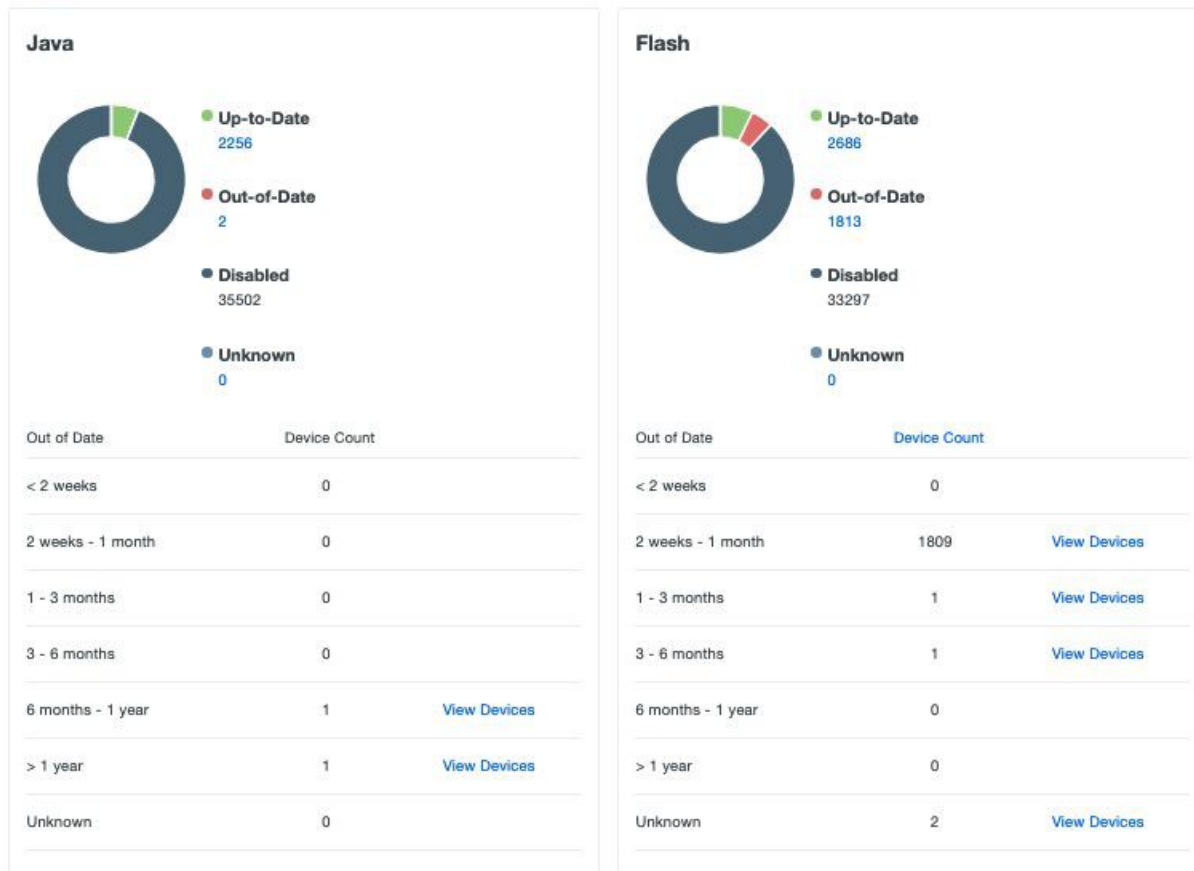
**Vulnerability Analysis**

**価値提案：**他のソフトウェアと同様に、古いブラウザはエクスプロイトに対して脆弱です。ブラウザはエンド ユーザーが日常的に（企業リソースだけでなく）個人の Web サイトや疑わしい Web サイトへのアクセスにも使っているため、かなり広い攻撃対象領域を抱えています。攻撃者はエクスプロイトしやすい古いブラウザを探して攻撃を仕掛けるため、ブラウザを最新の状態に維持することが、膨大な数の攻撃を少しでも減らす重要な手段となります。

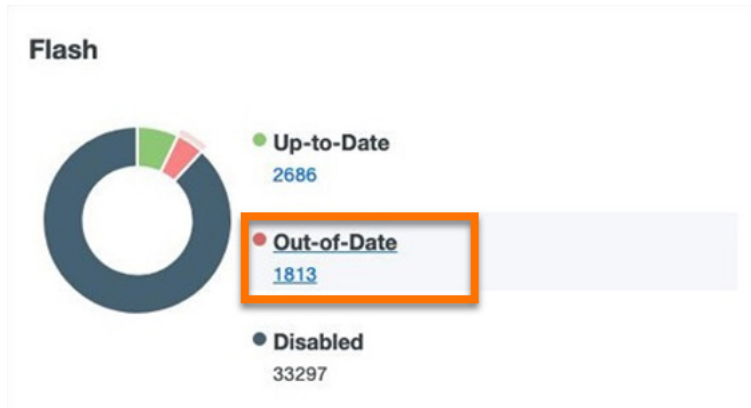
5. さらに下にスクロールして Java と Flash プラグインのステータスを表示し、プラグインが有効かどうかを確認します。有効な場合は最新のものかどうかを判断します。

注：Java と Flash プラグインのリリース ノート（特にセキュリティ更新について）を確認すれば、これらプラグインを無効にすべきか、少なくとも最新の状態に維持すべきかを判断できます。

Plugins



6. いずれかのプラグインをクリックすることで、特定のデバイスとその関連ユーザを詳しく表示できます。



- 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

注：このデータはすべて Duo プラットフォームに 180 日間保管され、その他のプラットフォーム (Splunk、Rapid7、その他の SIEM など) にエクスポートできます。



## シナリオ 3： ポリシーの管理

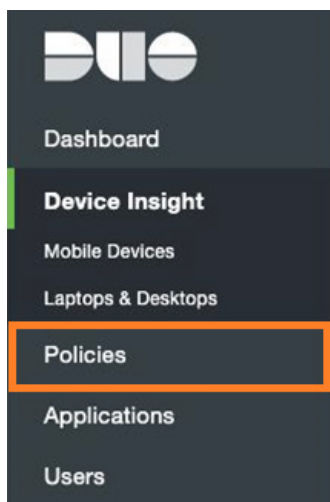
**価値提案：**このシナリオでは、管理者がデバイス データに基づいて設定できるポリシーを詳しく説明します。また、Duo デバイス ポリシーを使用して、最新かつセキュアなデバイスだけにアプリケーションへのアクセスを認める方法を紹介します。

通常、これらのポリシーで管理者の操作が必要になることはほとんどありません。しかし、今年初めに発覚した Chrome の脆弱性を突いたゼロデイ攻撃など新たな脅威が発生した場合は、管理者がログインして数回クリックするだけで、「直ちに更新を求めるポリシー」を 2 週間適用できます。これにより、絶えず変化する脅威の状況下でも組織のセキュリティ態勢をすぐに改善できます。

**注：**Duo でソフトウェア アップデートが管理されているため、新しいバージョンがリリースされるたびにポリシーのチェックと更新を心配する必要がありません。

### 手順

1. 管理者パネルで [ポリシー (Policies) ] を選択します。



2. すでに設定されているポリシーを確認します。Duo ポリシーの適用レベルは 3 つあります。
  - **グローバル：**すべてのユーザとアプリケーションに適用されるポリシー
  - **アプリケーション：**割り当てられている特定のアプリケーションに適用されるポリシー
  - **グループ：**特定のアプリケーションに接続する特定のユーザ グループに適用されるポリシー

**注：**この 3 つのポリシー レベルを使用すると、管理上の負担を最小限に抑えながら、ビジネスを実行するために必要なアクセスのみを提供する、包括的なセキュリティ ポリシーを作成できます。

3. 下にスクロールして、Workday 管理者 (Workday Administrators) ポリシーを表示します。

- ERP ソリューションである Workday の管理者は、組織のミッション クリティカルなアプリケーションに対してかなり高い権限を持ちます。
- **Workday 管理者**には、より制限されたアクセス ポリシーが必要です。
- グループ レベルのポリシーを使用しているため、Workday 管理者のみが影響を受けます。標準のログイン ユーザにはもう少し制限のないポリシーを作成できます。

## Workday Administrator Edit

**Policy Key** POC0VS7BZS2D10303DTD

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. 上にスクロールして戻り、**ユーザ ロケーション (User Location)** ポリシーで米国からのアクセスを許可し、それ以外の国からのアクセスは拒否するように設定されているのを確認します。

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

**価値提案**：これはすべての管理者が米国にいて、出張もないことがわかっている場合です。米国以外にも拠点がある場合や、従業員が国外に頻繁に出張する場合は、これらのユーザに対して米国以外からのログインを許可するきめ細かいグループ ポリシーを別に作成できます。

5. [信頼できるエンドポイント (Trusted Endpoints) ] ポリシーを表示します。

- 現在はこのポリシーが設定されているため、企業が管理して信頼できるエンドポイントでのみ **Workday** にログインできます。これには、EMM (Jamf など) が管理するラップトップや企業 MDM (Airwatch など) に登録されているモバイル デバイスなどがあります。

✔ Enabled Trusted Endpoints Only allow trusted endpoints.

注：Workday は機密データを扱う極めて重要性の高いアプリケーションであるため、管理された信頼できるデバイスが必要とされるのは当然です。組織内には重要性が若干低いアプリケーションやユーザ グループが他にも存在するため、それらにはデバイスが最新の状態で保たれている限り、BYO デバイスを使ったアクセスを許可できます。

6. 下にスクロールし、Workday にログインする際は Chrome を使うこと、および Chrome の最新バージョンがリリースされた場合は 2 週間以内に更新する必要があることを規定した **Browsers** ポリシーが設定されていることを確認します。

- このポリシーでは、ブラウザが最新バージョンでなくなると、Workday にログインするたびに通知を受け取るようになりますが、最初の 2 週間は更新を延期できます。
- ただし、2 週間を超えるとログインはブロックされ、更新してからでないとログインできなくなります。

✔ Enabled Browsers Notify users when their browser version is out of date.  
Block users when their browser version is more than 2 weeks out of date.  
Only allow devices accessing applications using Chrome.

価値提案：Duo はユーザにブロックした理由だけでなく、デバイスの更新方法についても通知するため、IT 部門や管理者のサポートがなくてもユーザはこのプロセスを完了できます。これによりヘルプデスクの負担が減り、ステップバイステップで解決方法がわかるため、ビジネス ユーザの時間が無駄になりません。ここでのユーザは管理者です。Duo ではログインが保護されるだけでなく、その他のユーザにも役立つ価値が提供されます。

7. 画面下部の **Mobile** ポリシーに注目します。

✔ Enabled Tampered Devices Don't allow authentication from tampered devices.

---

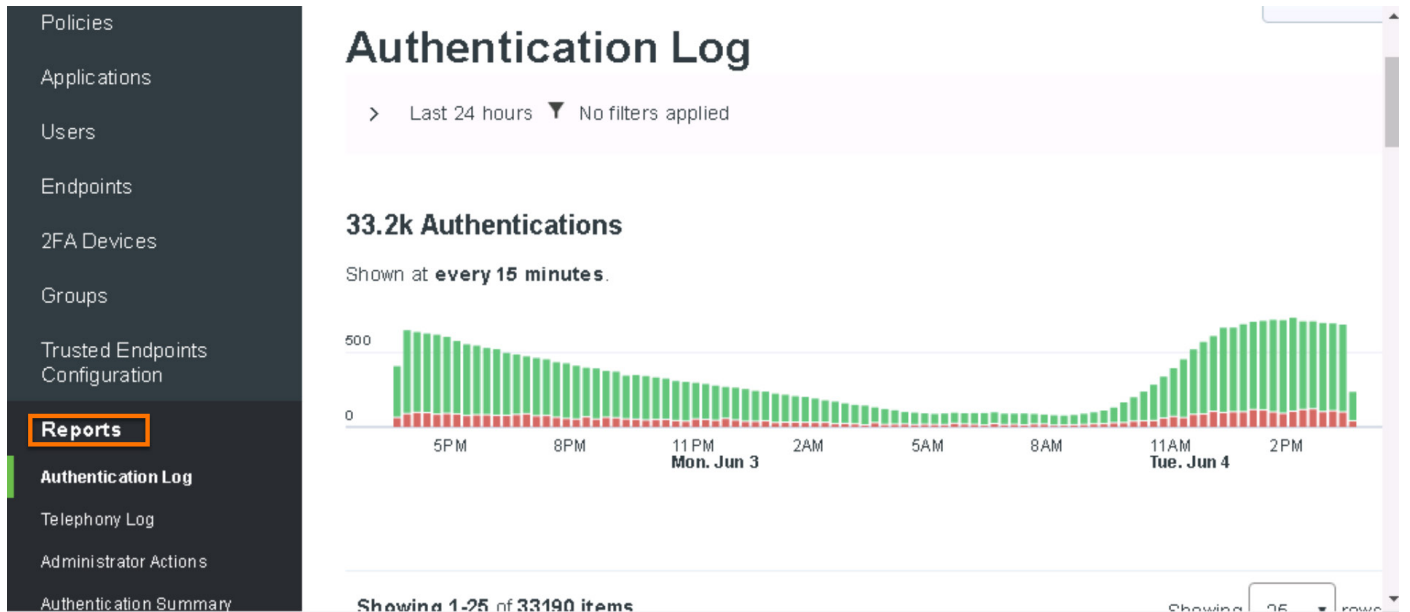
✔ Enabled Screen Lock Don't allow authentication from devices without a screen lock.

---

✔ Enabled Full-Disk Encryption Don't allow authentication from Android devices without full-disk encryption.

注：これらの各ポリシーは、ユーザが強力なセキュリティのベスト プラクティス（画面ロックを有効にすることを求める、デバイスが脱獄、または root 化（改ざん）されていないことを求める、など）に従うようにするアシユアランスを管理者がすばやく簡単に設定して提供できるように設計されています。

- 管理者パネルで [レポート (Reports) ] を選択して [認証ログ (Authentication Log) ] を表示し、Duo ポリシーによりアプリケーションへのログインが阻止されたユーザを確認します。



- フィルタ アイコンをクリックすると、フィルタ フィールドとフィルタ オプションが表示されます。[アクセス拒否 (Access denied) ] ボックスをオンにします。

## 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 [+]

10. ユーザがログインできなかった認証イベントがいくつか表示されるまで下にスクロールします（場所の制限、古いデバイスなどの理由）。

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



## 次に必要な作業

関連する [Duo Security プロポーザル](#)を確認し、Duo Security によって、オンプレミスとクラウドのすべてのアプリケーションへのユーザ、デバイス、場所を問わないシンプルで安全なアクセスがどのように実現されているのか理解してください。

©2019 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は2019年7月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



お問い合わせ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>