Tanium Device Management User Guide

2026H2 Semiannual Release

Version 1.4

November 17, 2026



The information in this document is subject to change without notice. Further, the information provided in this document is provided "as is" and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium's customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://help.tanium.com for the most current Tanium product documentation.

This documentation may provide access to or information about content, products (including hardware and software), and servicesprovided by third parties ("Third Party Items"). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium.

Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S.Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years. We certify against the WCAG 2.2 / VPAT 2.5 standards for all major product modules. Tanium performs ongoing reassessments as appropriate, given the scope and type of changes to the UI and product features from release to release. In the most recent testing, the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.2 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making commercially reasonable efforts to address any gaps as quickly as is feasible, given the severity of the issue and scope of the changes. Tanium factors these objectives into the ongoing delivery schedule of features and releases with our existing resources.

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are

©2026 Tanium Inc. All Rights Reserved

committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, Tanium Support atsupport@tanium.com, or email accessibility@tanium.com to make further inquiries.

Tanium is a trademark of Tanium, Inc. in the U.S. and other countries. Third-party trademarks mentioned are the property of the irrespective owners.

Kubernetes®, K8s®, and the Kubernetes logo are registered trademarks of The Linux Foundation®.

Android, ChromeOS, and Google are trademarks of Google LLC.

iOS, iPad, iPadOS, iPhone, Mac, and macOS are trademarks of Apple Inc., and registered in the U.S. and other countries and regions.

Patents: https://www.tanium.com/patents

Tanium Open Source Disclosure : https://tanium.github.io/opensource/

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview 9
- Apple architecture 9
- Google architecture 10
- Entities and devices 11
- Entity providers 11
- Tanium Cloud MDM Service 12
- Interoperability with other Tanium products 12

Getting started 14

Requirements 17
- Core platform dependencies 17
- Computer group dependencies 17
- Solution dependencies 17
  - Tanium recommended installation 18
  - Import specific solutions 18
  - Required dependencies 18
- Tanium™ Module Server 18
- Endpoints 18
  - Supported internet protocols 19
  - Supported operating systems 19
- Third-party software 19
- Host and network security requirements 22
  - Ports 22
  - Security exclusions 23
  - Hosts and ports for Apple devices 23
- User role requirements 23
- Endpoint information collection 29

Installing 33

©2026 Tanium Inc. All Rights Reserved

Before you begin 33
Import Device Management 33
Upgrade Device Management 34
Verify Device Management version 34
Troubleshoot issues 34

Configuring 35
Set up Device Management users 35
(Apple) Configure an Apple Push Certificate to use with Device Management 37
(Apple Automated device enrollment) Configure an identity provider 39
(Apple, Optional) Configure automated enrollment using an Apple enrollment system 41
(Apple, Optional) Configure Apps & Books organizational units 44
Add an organizational unit 44
Manage organizational units 45
(Google) Configure a Google Workspace 45
(Optional) Configure custom tags for devices 45

Installing the Tanium Client 48
Select a Tanium Client deployment template 49
Upgrading the Tanium Client 50

(Apple) Enrolling devices 51
Automated device enrollment 51
Manual enrollment 52

(Apple) Managing settings 53
Add a custom setting 53
Add a curated setting 53
Delete a setting 54
Review settings 55
Use device variables in settings 57
What to do next 59

(Apple) Configuring Software Update Settings and Software Enforcement settings 60
Create a Software Update Settings setting 60
Create a Software Update Enforcement setting 60
What to do next 61

©2026 Tanium Inc. All Rights Reserved

(Apple) Managing web clips, applications, and Apps & Books 62
(macOS) Add an enterprise application 62
(iOS) Add a web clip 63
(Apple) Add an App Store application 64
Delete a web clip or application 64
Review web clips and applications 65
What to do next 67

(Apple) Managing collections 68
Create a collection 68
Delete a collection 70
Review collections 70

(Google) Configuring a Google Workspace 73
Set up a Google service account 73
Step 1: Enable the required Google Cloud APIs 74
Step 2: Create a service account 74
Step 3: Create a JSON key for the service account 74
Step 4: Enable domain-wide delegation in Google Cloud 75
Step 5: Authorize the service account in Google Workspace 76
Step 6: Prepare credentials for Device Management 77
Create a Google Workspace 77
Edit a Google Workspace 78
Perform a manual sync 78
Delete a Google Workspace 79

(Google) Managing Chrome policies 80
Policy states 80
View Chrome policies 80
Set a Chrome policy 81
Reset a policy to inherited 82

(Google) Managing Android Enterprise policies 83
Set up Android Enterprise 83
View and manage Android Enterprise registration 84
Edit Android Enterprise settings 85
Unbind an Android Enterprise 85

©2026 Tanium Inc. All Rights Reserved

Create an Android policy 86
Reorder Android policy priority 88
Edit an Android policy 89
Duplicate an Android policy 89
Delete an Android policy 89
Create an enrollment token 90
Enroll a device with a token 91
Link a zero-touch account for Android devices 92
Clone an enrollment token 93
Delete an enrollment token 93

Working with devices and device data 95
View the details for a device 97
General Info 98
Endpoint Overview 98
Deploy actions on a device 101
Issue questions to target devices enrolled with Device Management 105
Include devices enrolled with Device Management in a report 106
Use Tanium Connect to export data about devices enrolled with Device Management 107

Maintaining 108
Perform annual maintenance 108
Renew an Apple MDM Push Certificate 108
Update server tokens 109

Troubleshooting Device Management 111
Collect logs 111
Observed issues with specific settings 111
Password and Screen Unlock settings 111
FileVault settings 112
Wi-Fi Settings 113
Observed issues setting up Android Enterprise 113
Observed issues with Android Enterprise device actions and policies 114
Observed issues with Web Clips and Enterprise Applications 114
Issues with Apps & Books 115
Contact Tanium Support 116

©2026 Tanium Inc. All Rights Reserved

Reference: (Apple) Configuring Identity Providers to use with Device Management 117
Before you begin 117
OIDC requirements 118
auth0 119
Microsoft Entra ID 123
Okta 130
OneLogin 136
Troubleshooting 141

Reference: Filter operators 143

Tanium Client PPPC profile 145

©2026 Tanium Inc. All Rights Reserved

Overview

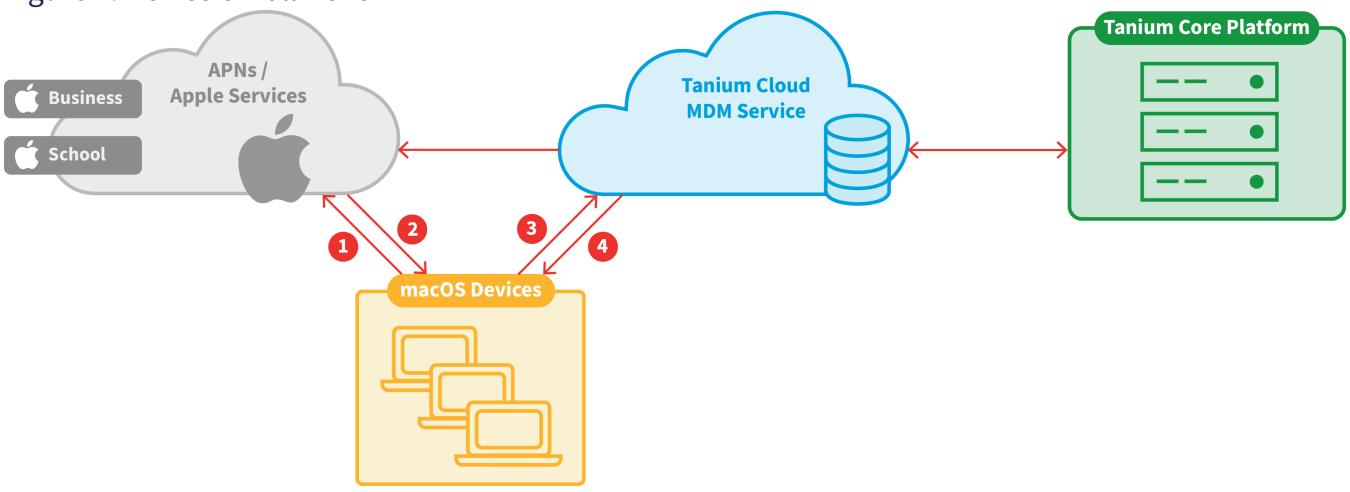
Note: Tanium Device Management is part of the Tanium™ Endpoint Management for Mobile solution.

Tanium Device Management extends your visibility and management of mobile and laptop devices. You can manage Apple devices (macOS, iOS, and iPadOS) through the Tanium Cloud MDM Service, and Google Workspace devices (ChromeOS laptops) through integrations with the Google Admin SDK and Chrome Policy API.

Apple architecture

Device Management connects the Tanium™ Server to the Tanium Cloud MDM Service, which then communicates with enrolled Apple devices through the Apple Push Notification Service (APNs). This architecture allows you to configure device settings in Device Management and push them to enrolled devices.

Figure 1. Device enrollment



1	The device enrolls with your Apple enrollment system (Apple Business Manager or Apple School Manager) using automated or manual enrollment.
2	The device retrieves instructions from Apple, depending on where the device is enrolled:

©2026 Tanium Inc. All Rights Reserved

	• If the device is enrolled in Apple Business Manager or Apple School Manager, devices are directed to the MDM provider. • If the device is not enrolled in Apple Business Manager or Apple School Manager, setup continues. Users can enroll with the MDM provider after installation.
3	The device reaches out to the Tanium Cloud MDM Service.
4	The configured settings push down to the device.

Note:

- Only one MDM can manage each device.
- To manage software updates on Apple devices using Tanium, devices must be enrolled with Device Management. For more information about managing software updates, see (Apple) Configuring Software Update Settings and Software Enforcement settings on page 60.
- Data sent to Apple is managed by the Apple Privacy Policy. For more information, see Apple: Apple Privacy Policy.
- Tanium Device Management is a new solution and is completely independent from the legacy Tanium™ Mac Device Enrollment solution. Devices that are currently enrolled with the legacy solution will not be affected if you configure Tanium Device Management on the same Tanium Server.

Google architecture

Device Management connects to the Google Admin SDK to inventory and manage Google Workspace devices. Unlike Apple device management, Google integration does not use the Tanium Cloud MDM Service. Device data syncs directly from Google to the Tanium module service on a periodic schedule.

The following Google APIs provide the integration:

©2026 Tanium Inc. All Rights Reserved

- Google Admin SDK Directory API: Provides device inventory, metadata, and remote actions for ChromeOS devices.
- Chrome Policy API: Provides policy schema discovery and Organizational Unit (OU)-based policy configuration for ChromeOS devices.

Device Management authenticates with Google using OAuth 2.0 through a Google Cloud Platform service account with domain-wide delegation. For more information about configuring credentials, see (Google) Configuring a Google Workspace on page 73.

Entities and endpoints

An *entity* is any discrete unit or node on a computer network that can be tracked, such as an endpoint, compute instance, cloud service, or identity object such as a user or group.

An *endpoint* is a computing device or node that connects to a computer network, through which data can enter or exit the network. Endpoints are a subset of entities; all endpoints are entities, but not all entities are endpoints. Endpoints include physical or virtual workstations that run Windows, macOS, or Linux, mobile devices that run Android or iOS, and other similar devices. In contrast, routers and switches are entities, but not endpoints, because routers and switches direct network traffic through the network, but do not provide a direct entry or exit point for data.

Entity providers

You can ingest data from endpoints managed using Tanium Client or an entity provider into the same Tanium instance to gain broader visibility into your entire network.

An *entity provider* is an adapter that ingests entity data into Tanium Core Platform. Tanium Core Platform uses this data to manage the entity. Entity providers collect entity data without installing Tanium Client on the endpoint. For example, you cannot install Tanium Client on mobile devices that run Android or iOS. You can configure the Tanium Connector for Microsoft Intune to integrate with a Microsoft Intune instance to ingest mobile device data or enroll Apple devices with Device Management.

- Management using Tanium Client: Tanium Client runs on endpoints that run a compatible operating system (OS), such as computers or virtual machines that run Linux, macOS, or Windows. These endpoints are generally part of the linear chain. Tanium Client reports information back to Tanium Core Platform through the linear chain.

©2026 Tanium Inc. All Rights Reserved

- Management using entity providers, which collect device information in different ways:
    - Through integrations, such as the Tanium Connector for Microsoft Intune that ingests Microsoft Intune mobile device data

  Management of these devices does not rely on Tanium Client being installed directly on an entity. The entity provider might report endpoint information that is different from the information that a Tanium Client reports, due to the difference in entity type. For example, mobile devices are assigned an International Mobile Equipment Identity (IMEI) serial number, which are not assigned to other types of devices, such as an endpoint that runs Windows Server.

Each entity is associated with a **Provider Type**, **Provider Name**, and **Entity Type**, which identify how Tanium Core Platform manages the entity.

Entity providers and related sensor values

Entity Provider	Provider Type value	Provider Name value	Entity Type value
Tanium Client	Tanium Client	Tanium	Computer
Tanium Endpoint Management for Mobile	Device Management	• Device Management Computer (for macOS) • Device Management Mobile Device (for iOS and iPadOS)	• Computer (for macOS) • Mobile Device (for iOS and iPadOS)

Tanium Cloud MDM Service

Tanium Cloud MDM Service is a cloud-based service that enables the Tanium Server to communicate with enrolled Apple devices through the Apple Push Notification Service.

Interoperability with other Tanium products

Reporting

The Device Management **Overview** page uses charts to visualize data that Tanium™ Reporting provides through reports. The overview includes metrics for Apple, and ChromeOS devices, including

©2026 Tanium Inc. All Rights Reserved

the health of connected Apps & Books organizational units. For more information, see Tanium Reporting User Guide: Working with reports.

Device Management provides access to the Endpoint Details page in Tanium™ Reporting, where you can view comprehensive information about a single device and manage the device. Apple and ChromeOS devices all appear in Reporting. To access the page, see Working with devices and device data on page 95. For more information about device details, see Tanium Reporting User Guide: Viewing and managing a single endpoint.

Interact

Google-managed devices are available in Tanium™ Interact alongside Apple MDM-enrolled devices. Use standard sensor queries to target and filter devices by platform. For more information, see Tanium Interact User Guide: Overview.

©2026 Tanium Inc. All Rights Reserved

Getting started with Device Management

Follow these steps to configure and use Device Management.

Step 1: Configure Device Management users

Assign required roles and permissions to users that will work with Device Management. For more information, see Set up Device Management users on page 35.

> **Note:** Only users with the Device Management Administrator role can access the configuration settings in the Device Management workbench.

Step 2: (Apple) Configure an Apple Push Certificate

Request and upload an Apple Push certificate to allow Tanium to communicate with Apple endpoints.

For more information, see (Apple) Configure an Apple Push Certificate to use with Device Management on page 37.

Step 3: (Optional, Apple) Configure an Apple enrollment system

Enable Device Management to interact with an Apple enrollment system, either Apple Business Manager or Apple School Manager, to automatically enroll endpoints. For more information, see (Apple, Optional) Configure automated enrollment using an Apple enrollment system on page 41.

©2026 Tanium Inc. All Rights Reserved

Step 4: (Optional, Apple) Enroll endpoints

Enroll endpoints in Device Management using one of these methods:

Automated enrollment

Automated device enrollment allows for devices purchased directly from Apple or authorized resellers to be preconfigured. With Apple Business Manager or Apple School Manager, endpoints automatically enroll into Tanium and receive the initial settings that you configure in Device Management.

Manual enrollment

With this method, an enrollment profile is provided by Device Management to install on the endpoint manually.

For more information, see (Apple) Enrolling devices on page 51.

Step 5: (Optional, Apple) Configure Apps & Books

Connect an Apple Business Manager or Apple School Manager Apps & Books content token to assign app licenses to enrolled devices.



Note: The Apps & Books feature replaced the Apple Volume Purchase Program (VPP) service.

For more information, see Configure Apps & Books organizational units on page 44.

Step 6: (Apple) Create settings

Add settings to configure how users connect to and access enterprise resources.

Settings are configuration rules that administrators push to managed endpoints to control how they work; for example, wireless network, VPN, and passcode settings. For more information, see (Apple) Managing settings on page 53.

©2026 Tanium Inc. All Rights Reserved

Step 7: (Apple) Create a collection

Create collections to specify which settings are configured on endpoints.

A collection is a group of settings. Collections can only contain settings, not other collections. For more information, see (Apple) Managing collections on page 68.

Step 8: (Google) Configure a Google Workspace

Connect Device Management to a Google Workspace tenant to inventory and manage ChromeOS devices.

For more information, see (Google) Configuring a Google Workspace on page 73.

Step 9: (Google) Manage Chrome policies

After a Google Workspace with ChromeOS enabled is configured, view and apply Chrome policies to Organizational Units (OUs) or Groups in Device Management.

For more information, see (Google) Managing Chrome policies on page 80.

Step 10: (Google) Manage Android Enterprise policies

Complete Android Enterprise registration, then create policies to manage Android Enterprise devices. Android Enterprise registration does not require a Google Workspace.

For more information, see (Google) Managing Android Enterprise policies on page 83.

©2026 Tanium Inc. All Rights Reserved

Device Management requirements

Review the requirements before you install and use Device Management.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Tanium Enforce. For more information about how to get Tanium Enforce, see Tanium Solutions & Bundles.
- Tanium™ Core Platform servers
- Tanium™ Client: No client requirements
- Tanium™ Console

Computer group dependencies

When you first sign in to Tanium Console after a fresh installation of Tanium Server, the server automatically imports the computer groups that Device Management requires:

- All Mobile Devices

Solution dependencies

Other Tanium solutions are required for Device Management to function (required dependencies) or for specific Device Management features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.

©2026 Tanium Inc. All Rights Reserved

Note: Some Device Management dependencies have their own dependencies, which you can see in the lists of required and feature-specific dependencies below. Where a dependency links to its own user guide, that link opens the guide for the latest version of the solution, not necessarily the minimum version that Device Management requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Device Management, the Tanium Server automatically imports all your licensed solutions at the same time. For more information, see Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Device Management to import, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Device Management, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Device Management has the following required dependencies:

- Tanium™ Account
- Tanium™ RDB Service
- Tanium™ Reporting

Tanium™ Module Server

Device Management is installed and runs as a service on the Module Server host computer. The impact on the Module Server is minimal and depends on usage.

For information about Module Server sizing in a Windows deployment, see Tanium Core Platform User Guide for Windows Deployments: Host system sizing guidelines.

Endpoints

©2026 Tanium Inc. All Rights Reserved

Supported internet protocols

Device Management supports IPv4 and IPv6 addresses.

Supported operating systems

The following endpoint operating systems are supported with Device Management.

Apple

- iOS 17 and later
- iPadOS 17 and later
- macOS Sonoma (version 14) and later

Google

- ChromeOS devices that receive automatic updates. For more information, see Chrome Enterprise and Education Help: Auto Update policy.
- Android Enterprise devices managed through the Android Management API. Minimum Android version depends on the enrollment type used: Android 6.0 for **Fully managed** and **Dedicated device (kiosk)**, Android 7.0 for **Work profile (BYOD)**, and Android 11.0 for **Work profile (company-owned)**. For more information, see Create an enrollment token on page 90.
- ChromeOS Flex Devices supported by Google. For more information, see ChromeOS Flex Help: Certified models list.



Note: Tanium Device Management supports Android devices that are eligible for Google Mobile Services (GMS) and enrolled through the Android Management API (AMAPI). Tanium Device Management does not support Android Open Source Project (AOSP) or other non-GMS Android devices.

Third-party software

©2026 Tanium Inc. All Rights Reserved

Tanium Device Management is supported for use with the following third-party software and requirements:

Apple

- Apple Business Manager or Apple School Manager

  You must be assigned the Administrator or Device Enrollment Manager role or equivalent permissions.

- Apple Push Notification Service

  Apple Push Notification Service requires you to upload a certificate signing request (CSR) in the Apple Push Certificates Portal, which then generates a certificate. For the portal credentials, use an Apple ID to which multiple users have access so that the certificate can be renewed. If you lose access to the Apple ID, the certificate expires, or you lose the ability to renew the certificate, all endpoints must re-enroll with Device Management.

    - OpenID Connect (OIDC) compliant identity provider:

      - auth0
      - Entra ID
      - Okta
      - OneLogin

©2026 Tanium Inc. All Rights Reserved

> **Note:**
>
> The identity provider administrator must have access to manage user roles, user permissions, user mappings, and user attributes; configure applications; and assign users to applications. Refer to your identity provider documentation to understand the required roles and permissions.
>
> For example, the Okta App Admin role provides the needed permissions: Manage Profile Editor, Manage Profile Mappings, View applications or application instances, Add and configure applications, Assign user access to applications, and Create and modify an OIDC App.
>
> The IdP must have the application configured as a Single Page Application (SPA) using Proof Key for Code Exchange (PKCE).

- (Optional) Apps & Books content token

  To assign app licenses to enrolled devices, you need a content token from Apple Business Manager or Apple School Manager. The Apple Business Manager or Apple School Manager Administrator who creates an organizational unit can assign the Content Manager role for that organizational unit to another team member, allowing that team member to download the content token. For more information, see Configure Apps & Books organizational units on page 44.

Google

- Google Workspace for Education or Enterprise
- Google Cloud Platform project with a service account

  Create a service account in Google Cloud Platform and configure domain-wide delegation in the Google Workspace Admin Console. The service account requires the following OAuth 2.0 scopes:

  - ChromeOS devices: `https://www.googleapis.com/auth/admin.directory.device.chromeos`
  - Groups: `https://www.googleapis.com/auth/`

©2026 Tanium Inc. All Rights Reserved

`admin.directory.group.readonly`

- Organizational Units: `https://www.googleapis.com/auth/admin.directory.orgunit.readonly`
- Chrome Policy: `https://www.googleapis.com/auth/chrome.management.policy`

Important: The admin email address that you provide must have sufficient Google Workspace admin privileges to use the configured OAuth scopes.

- Android Enterprise EMM registration

  Android Enterprise device management does not use a Google Workspace or domain-wide delegation. You need a Google Workspace Super Admin account to complete Android Enterprise registration. For more information, see View and manage Android Enterprise registration on page 84.

Host and network security requirements

Specific ports and processes are needed to run Device Management.

Ports

The following ports are required for Device Management communication.

Required ports for Device Management communication

Source	Destination	Port	Protocol	Purpose
Tanium Module Server	*.cloud.tanium.com	443	TCP (HTTPS)	Allows communication with Tanium Cloud MDM Service
Enrolled devices	*.cloud.tanium.com	443	TCP (HTTPS)	Allows communication with Tanium Cloud MDM Service

©2026 Tanium Inc. All Rights Reserved

Note: Exclude port 443 traffic to the listed domains from SSL inspection or interception if it is configured in your environment. The *.cloud.tanium.com domain does not support intercepting proxies.

Best Practice: Configure firewall policies to open ports for Tanium traffic with TCP-based rules instead of application identity-based rules. For example, on a Palo Alto Networks firewall, configure the rules with service objects or service groups instead of application objects or application groups.

For more information about Tanium Cloud ports, see Host and network security requirements.

Security exclusions

Device Management requires no specific security exclusions.

For more information about security exclusions to define across Tanium, see Reference: Endpoint security exclusions. For Windows-based Tanium Core Platform deployments, see Tanium Core Platform Server security exclusions.

Hosts and ports for Apple devices

For more information about the Apple hosts and ports that managed Apple devices must be able to access, see Use Apple products on enterprise networks.

User role requirements

Predefined roles grant the following permissions, which are required to use Device Management functionality:

- Table 3. Device Management solution permissions on page 25
- Device Management administration, platform content, and global permissions on page 29: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Device Management users on page 35.

©2026 Tanium Inc. All Rights Reserved

Note:

- In addition to the Administrator, Operator, and Read Only User roles covered in the tables below, Device Management also provides an **Device Management Action User** role and a **Device Management High Impact Action User** role, scoped to pushing actions only. For more information, see Set up Device Management users on page 35.
- Management rights: the Computer Groups assigned to a user, user group, or Persona do not limit which devices a collection targets. A collection targets every Device Management device that matches its targeting criteria, regardless of the management rights of the user who created or deployed the collection.

  Device views and actions, such as the actions available from the Endpoint Details, follow the management rights of the active session. If a user switches to a Persona, that user can view and act on only the devices within the scope for that Persona.

  Assigning **All Computers** and enabling **Unrestricted Management Rights** on a Persona grant the same access to Device Management devices.

Some Device Management solution permissions provide permissions that are associated with other solutions. Furthermore, all the platform content permissions and some solution permissions apply to content sets that might contain content for other solutions in addition to Device Management. If you create custom roles for Device Management users, be sure to assign all the solution permissions and content set permissions that are required for Device Management functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined roles. For more information, see the following sections of the Tanium Console User Guide:

- RBAC overview (provides an overview of roles, permissions, and content sets)
- Provided role permissions
- View effective role permissions
- Configure a custom role

©2026 Tanium Inc. All Rights Reserved

Note: Do not assign the following roles to users. These roles are for internal purposes only.

- **Device Management Service Account**
- **Device Management Service Account - All Content Sets**
- **Device Management Google Service Account**
- **Device Management Google Service Account - All Content Sets**

For more information about role permissions and associated content sets, see Tanium Console User Guide: Managing RBAC.

Note: The **Device Management Action User** and **Device Management High Impact Action User** roles do not grant the Push permission shown below. These roles deploy actions through a content-set-scoped action privilege rather than the command queue that the Push permission gates, so Push is not required. Assign one of these roles together with another Device Management role, such as Read Only User or Operator, for workbench and API visibility - the action roles alone grant only the permissions needed to deploy action packages.

Device Management solution permissions

Permission	Device Management Administrator	Device Management Operator	Device Management Read Only	Device Management Action User	Device Management High Impact Action User
Device Management View the Device Management workbench	✓ SHOW	✓ SHOW	✓ SHOW	✗	✗
Device Management Activation Lock Disable the activation lock for Device Management devices in Single Endpoint View	✓ DISABLE	✓ DISABLE	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Device Management Administrator	Device Management Operator	Device Management Read Only	Device Management Action User	Device Management High Impact Action User
Device Management Administrator Allows full control of Device Management	✓ ADMINISTER	✗	✗	✗	✗
Device Management API Read data from Device Management	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE
Device Management Apps & Books View and modify Apps & Books organizational units, applications, and assets for Device Management	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✗
Device Management Collections View, edit, and deploy collections to devices from Device Management	✓ DEPLOY READ WRITE	✓ DEPLOY READ WRITE	✓ READ	✗	✗
Device Management Enterprise Apps View and modify enterprise apps for Device Management	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✗
Device Management FileVault Keys Rotate the FileVault keys for devices enrolled with Device Management	✓ ROTATE READ	✓ ROTATE READ	✗	✗	✗
Device Management Get	✓	✓	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Device Management Administrator	Device Management Operator	Device Management Read Only	Device Management Action User	Device Management High Impact Action User
Activation Lock Bypass View activation lock bypass codes for devices enrolled with Device Management	CODES	CODES			
Device Management Get Available OS View the available operating system updates for devices enrolled with Device Management	✓ UPDATES	✓ UPDATES	✓ UPDATES	✗	✗
Device Management List ABM View devices enrolled with Device Management using Apple Business Manager (ABM) or Apple School Manager (ASM)	✓ DEVICES	✓ DEVICES	✗	✗	✗
Device Management Metrics View and edit the metrics in Device Management	✓ READ WRITE	✓ READ	✓ READ	✗	✗
Device Management Profile Download the enrollment profile to manually onboard devices to Device Management	✓ DOWNLOAD	✗	✗	✗	✗
Device Management Push Push a command to the command queue, which is	✓ COMMAND	✓ COMMAND	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Device Management Administrator	Device Management Operator	Device Management Read Only	Device Management Action User	Device Management High Impact Action User
required to take actions on Device Management devices from the Endpoint Details page					
Device Management Settings View and edit settings for Device Management	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✗
Device Management Single Endpoint View Device Management data on the Endpoint Details page	✓ VIEW	✓ VIEW	✓ VIEW	✓ VIEW	✓ VIEW
Device Management Unenroll Configure unenrollment settings and unenroll devices from Device Management	✓ DEVICE	✓ DEVICE	✗	✗	✗
The permissions for these roles provide solution permissions for other solutions. To view the provided permissions, see View effective role permissions .					

Note: The **Wipe** and **Relinquish Ownership** actions for Android Enterprise devices additionally require permissions to the **Device Management - High Impact** content set, on top of the Device Management Push permission or, for the Action User roles, the underlying action-execution privilege scoped to that content set.

©2026 Tanium Inc. All Rights Reserved

Device Management administration and platform content permissions

Permission	Permission Type	Device Management Administrator	Device Management Operator	Device Management Read Only User [1]	Device Management Action User	Device Management High Impact Action User
Computer Group	Administration	READ	READ			
Filter Group	Platform Content	READ	READ	READ	READ	READ
Package	Platform Content	READ	READ	READ		
Plugin	Platform Content	READ EXECUTE	READ EXECUTE	READ EXECUTE	READ EXECUTE	READ EXECUTE
Sensor	Platform Content	READ	READ	READ	READ	READ

To view the content sets to which the platform content permissions apply, see View effective role permissions .

Endpoint information collection

Device Management uses sensors to collect information about enrolled and synced devices. The information collected enables identification and auditing of devices and enables Tanium to target actions to specific endpoints or groups of endpoints.

Apple sensors

- **Device Management - Device ID**
- **Device Management - Enrollment Type**

©2026 Tanium Inc. All Rights Reserved

- **Device Management - Is Supervised**

Google sensors

Shared

- **Device Management - Active Time Ranges**
- **Device Management - Bluetooth Number of Connected Devices**
- **Device Management - Collections Installation Status**
- **Device Management - Device ID**
- **Device Management - Device Serial Number**
- **Device Management - Dock MAC Address**
- **Device Management - Google ID**
- **Device Management - Last Check-In Time**
- **Device Management - MEID**
- **Device Management - Settings Installation Status**
- **Device Management - Status**
- **Device Management - TPM Details**

ChromeOS

- **Device Management - ChromeOS Annotated Asset ID**
- **Device Management - ChromeOS Annotated Location**
- **Device Management - ChromeOS Annotated User**
- **Device Management - ChromeOS Auto Update Through**
- **Device Management - ChromeOS Backlight Info**
- **Device Management - ChromeOS Boot Mode**

©2026 Tanium Inc. All Rights Reserved

- **Device Management - ChromeOS Deprovision Reason**
- **Device Management - ChromeOS Device Files**
- **Device Management - ChromeOS Device License Type**
- **Device Management - ChromeOS Disk Space Usage**
- **Device Management - ChromeOS Disk Volumes**
- **Device Management - ChromeOS Extended Support Eligible**
- **Device Management - ChromeOS Extended Support Enabled**
- **Device Management - ChromeOS Extended Support Start Date**
- **Device Management - ChromeOS Fan Speed**
- **Device Management - ChromeOS First Enrollment Time**
- **Device Management - ChromeOS Last Deprovision Time**
- **Device Management - ChromeOS Last Enrollment Time**
- **Device Management - ChromeOS Last Provision Timestamp**
- **Device Management - ChromeOS Manufacture Date**
- **Device Management - ChromeOS Notes**
- **Device Management - ChromeOS Order Number**
- **Device Management - ChromeOS Org Unit ID**
- **Device Management - ChromeOS Org Unit Path**
- **Device Management - ChromeOS OS Version Compliance**
- **Device Management - ChromeOS Platform Version**
- **Device Management - ChromeOS Recent Users**
- **Device Management - ChromeOS Screenshot Files**

©2026 Tanium Inc. All Rights Reserved

- **Device Management - ChromeOS Support End Date**
- **Device Management - ChromeOS Update Status Details**
- **Device Management - ChromeOS WAN IP Address**
- **Device Management - ChromeOS Will Auto Renew**

Android Enterprise

- **Device Management - Android API Level**
- **Device Management - Android Display Info**
- **Device Management - Android Enrollment Time**
- **Device Management - Android Enterprise**
- **Device Management - Android Hardware Info**
- **Device Management - Android Management Mode**
- **Device Management - Android Network Info**
- **Device Management - Android Non-Compliance Details**
- **Device Management - Android Ownership**
- **Device Management - Android Policy Compliant**
- **Device Management - Android Policy Name**
- **Device Management - Android Security Posture**

©2026 Tanium Inc. All Rights Reserved

Installing Device Management

About this task

Use Tanium Console **Solutions** page to install Device Management.

Before you begin

- Read the release notes.
- Review the Device Management requirements on page 17.
- If you are upgrading from a previous version, see Upgrade Device Management on page 34
- Assign the correct roles to users for Device Management. Review the User role requirements on page 23.
    - To import the Device Management solution, you must be assigned the Administrator reserved role.

Import Device Management

About this task

Perform the following steps to install the Device Management solution on the Tanium Server.

Note: If you have multiple Tanium Servers in an active-active configuration, you only need to perform these steps on one Tanium Server.

1. Sign in to Tanium Console with an account that has the **Administrator** reserved role.
2. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.
3. In the **Content** section, select **Device Management** and click **Import**.

©2026 Tanium Inc. All Rights Reserved

> **Tip:** If you need to install any prerequisite Tanium solutions, select those solutions as well.

4. Review the content to import and click **Start Import**.

Result

Upgrade Device Management

For the steps to upgrade Device Management, see Tanium Console User Guide: Install a Tanium release update. After the upgrade, verify that the correct version is installed: see Verify Device Management version on page 34.

Verify Device Management version

After you import or upgrade Device Management, verify that the correct version is installed.

1. Refresh your browser.
2. From the Main menu, go to **Shared Services** > **Device Management**.
3. To display version information, click Info .

Troubleshoot issues

About this task

If you experience issues with installing Device Management, see Troubleshooting Device Management on page 111.

©2026 Tanium Inc. All Rights Reserved

Configuring Device Management

About this task

No default settings are configured for Device Management.

Set up Device Management users

About this task

You can use the following set of predefined user roles to set up Device Management users.

For more information about the specific permissions for each role, see User role requirements on page 23.

Important: On installation, Device Management creates a Device Management user to automatically manage the Device Management service account. Do not edit or delete the Device Management user.

For more information about assigning user roles, see Tanium Console User Guide: Manage role assignments for a user.

Tip: To provide just-in-time access or scalable standing access to Device Management functionality, you can use SCIM provisioning combined with Tanium user groups. This approach lets you manage user access at scale or ad hoc through your identity provider, without creating users individually in Tanium. For more information, see Provision users into Tanium user groups with SCIM.

Device Management Administrator

Assign the **Device Management Administrator** role to users who manage the configuration and deployment of Device Management functionality to devices. This role can perform the following tasks:

- Configure Device Management.

©2026 Tanium Inc. All Rights Reserved

- Disable activation locks for Device Management devices in Single Endpoint View.
- View data from Device Management.
- View, modify, and deploy Device Management collections.
- View and modify Device Management enterprise apps.
- View and modify metrics for Device Management.
- Download enrollment profiles to manually enroll devices in Device Management.
- Push a command to the command queue, which is required to take actions on Device Management in Single Endpoint View.

Device Management Operator

Assign the **Device Management Operator** role to users who manage the configuration and deployment of Device Management functionality to devices. This role can perform the following tasks:

- Disable activation locks for Device Management devices in Single Endpoint View.
- View data from Device Management.
- View, modify, and deploy Device Management collections.
- View and modify Device Management enterprise apps.
- View metrics for Device Management.
- Push a command to the command queue, which is required to take actions on Device Management in Single Endpoint View.

Device Management Read Only User

Assign the **Device Management Read Only User** role to users who need visibility into Device Management data. This role can perform the following tasks:

- View Device Management settings.
- View data from Device Management.

©2026 Tanium Inc. All Rights Reserved

- View Device Management collections.
- View Device Management enterprise apps.
- View metrics for Device Management.

Device Management Action User

Assign the **Device Management Action User** role to users who need to deploy non-destructive Device Management actions to devices, without broader configuration access. This role is narrow by design: assign it together with another Device Management role, such as Read Only User or Operator, to also grant workbench and API visibility. This role can perform the following tasks:

- View Device Management data in Single Endpoint View.
- Deploy non-destructive Device Management action packages to devices.

This role cannot deploy high-impact actions, such as Wipe, Powerwash, and Deprovision.

Device Management High Impact Action User

Assign the **Device Management High Impact Action User** role to users who need to deploy both non-destructive and high-impact Device Management actions to devices, without broader configuration access. This role is narrow by design: assign it together with another Device Management role, such as Read Only User or Operator, to also grant workbench and API visibility. This role can perform the following tasks:

- View Device Management data in Single Endpoint View.
- Deploy Device Management action packages to devices, including high-impact actions such as Wipe, Powerwash, and Deprovision.



Note: Do not assign the **Device Management Service Account** and **Device Management Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

(Apple) Configure an Apple Push Certificate to use with Device Management

©2026 Tanium Inc. All Rights Reserved

About this task

Request and upload an Apple Push Certificate, also referred to as an APNs certificate, to allow Tanium to communicate with Apple devices.

Note: Tanium Device Management is a new solution and is completely independent from the legacy Tanium™ Mac Device Enrollment solution.

Before you begin

Create or identify an Apple ID to use for the Apple Push Certificate.

Important: Apple MDM Push Certificates are valid for one year. You must renew the certificate each year using the same Apple ID that you used to create the certificate. Otherwise, you must request a new certificate. If a new certificate is issued, Device Management loses the ability to communicate with enrolled devices, and all users are forced to re-enroll their devices. For more information, see Maintaining Device Management on page 108.

Best Practice: Use a role-based or managed Apple ID with Manager or Administrator rights that multiple users in your organization can access. The certificate must be renewed yearly using the same Apple ID that was used to create the certificate.

1. From the Main menu, go to **Shared Services** > **Device Management**.
2. In the **Configuration** section, click **Configure Apple Push Certificate**.
3. Select **Allow Tanium to send user and device information to Apple** to grant access to send data outside of Tanium.

©2026 Tanium Inc. All Rights Reserved

> **Note:**
> By checking this box, you acknowledge and allow that user and device information is sent from Tanium to Apple servers. For more information about this process, see Apple architecture on page 9.
>
> Data sent to Apple is managed by the Apple Privacy Policy. For more information, see Apple: Apple Privacy Policy.

4. In the **Certificate Signing Request** section, click **Download** to download the Tanium-signed certificate signing request, which is required when you request an Apple Push Certificate.
5. Go to the Apple website and create an Apple Push Certificate: `https://identity.apple.com/pushcert/`.
    a. Click **Choose File** and browse to the file that you downloaded in the previous step when you are prompted to choose the file with the Vendor-Signed Certificate Signing Request.
    b. Click **Upload**.
6. In the **Apple ID** field, specify the Apple ID that you used to request the Apple Push Certificate.
7. In the **Company Name** field, specify the name of your organization.
8. In the **Email Addresses** field, provide a comma-separated list of email addresses to notify when the Apple Push Certificate is nearing expiration.
9. In the **Apple MDM Push Certificate Upload** section, either browse to or drag and drop the PEM file for the Apple Push Certificate that you generated.
10. Click **Apply**.

(Apple Automated device enrollment) Configure an identity provider

About this task

Configure an OpenID Connect (OIDC) identity provider (IdP) to allow automated enrollment.

©2026 Tanium Inc. All Rights Reserved

Note:

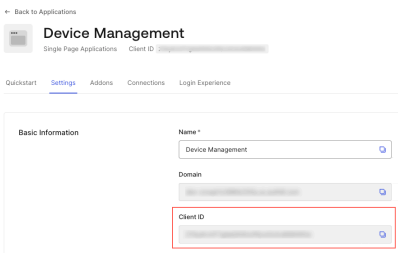
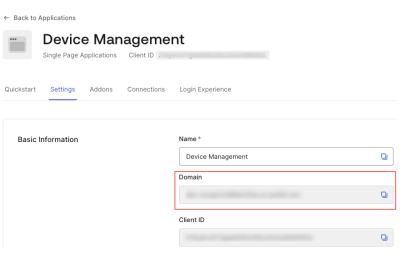
- This task is required only if you use automated device enrollment.
- The IdP must have the application configured as a Single Page Application (SPA) using Proof Key for Code Exchange (PKCE).
- For specific steps for a particular IdP, see Reference: (Apple) Configuring Identity Providers to use with Device Management on page 117.

1. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click **IDP Configuration**.
2. Update your IdP with the **Redirect URI**. Your IdP redirects users to this URI. The redirect URI is required for your IdP to integrate with Device Management.
3. Enter the **Client ID** (a unique, public identifier from the IdP) and **Issuer** for your IdP.

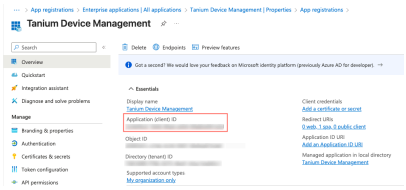
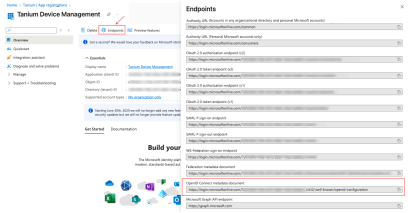
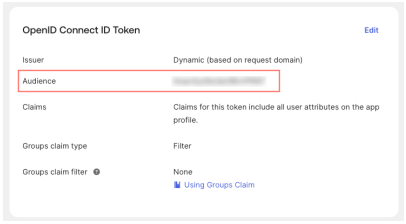
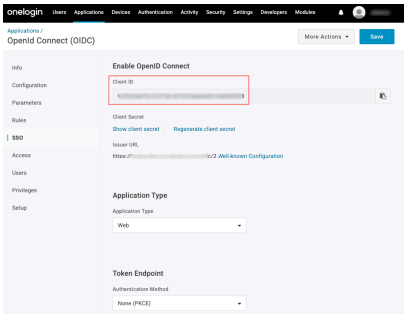
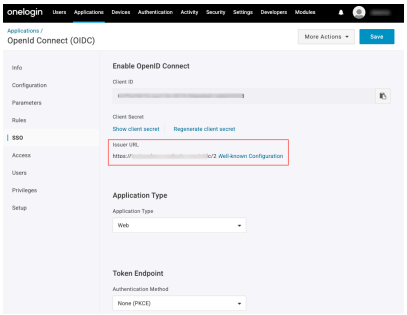
   Important: The **Issuer** is the URL of the IdP that allows the API server to find the public signing keys for the IdP. This value must begin with https://. Specify the URL exactly as your IdP requires, including or omitting characters such as trailing slashes. If this value does not exactly match the requirements of the IdP, errors can occur during enrollment which might prevent the **Welcome** page from loading.

   The names for these values in the IdP user interface vary based on the IdP:

Client IDs and Issuers for IdPs

Identity Provider	Use this value for Client ID	Use this value for Issuer
auth0	**Client ID** Figure 2. Client ID field in auth0 	**Domain** (add `https://` to the beginning) Figure 3. Domain field in auth0 

©2026 Tanium Inc. All Rights Reserved

Identity Provider	Use this value for Client ID	Use this value for Issuer
Entra ID	**Application (client) ID** Figure 4. Application (client) ID field in Entra ID 	**OpenID Connect metadata document** (omit the /.well-known/openid-configuration from the end) Figure 5. OpenID Connect metadata document value in Entra ID 
Okta	**Audience** Figure 6. Audience field in Okta 	Okta instance URL
OneLogin	**Client ID** Figure 7. Client ID field in OneLogin 	**Issuer URL** Figure 8. Issuer URL value in OneLogin 

4. Click **Apply**.

(Apple, Optional) Configure automated enrollment using an Apple enrollment system

About this task

©2026 Tanium Inc. All Rights Reserved

Enable Device Management to interact with an Apple enrollment system, either Apple Business Manager or Apple School Manager, to automatically enroll devices.

Before you begin

- Create or identify an Apple ID to use for the Apple Push Certificate.

  > **Best Practice:** Use a role-based or managed Apple ID with Manager or Administrator rights that multiple users in your organization can access. The certificate must be renewed yearly using the same Apple ID that was used to create the certificate.

- Configure the Apple Push Certificate with Device Management. For more information, see (Apple) Configure an Apple Push Certificate to use with Device Management on page 37.

- Configure an identity provider. For more information, see (Apple Automated device enrollment) Configure an identity provider on page 39.

1. From the Main menu, go to **Shared Services** > **Device Management**.
2. In the **Configuration** section, click **Configure Automated Device Enrollment**.

   > **Note:**
   > This section changes to **Summary** after the initial configuration. If you want to return to this configuration page, click **Configured** in the **Automated Enrollment** section of the **Summary** section or click Settings and then click **Automated Enrollment**.

3. In the **Download the Public Key Certificate** section, click **Download** to download the Tanium-signed public key certificate, which is required when you configure an Apple enrollment system.
4. Go to the Apple website and upload the Tanium-signed public key certificate to associate it with your organization. Then download the service token for this configuration. For more information, see Apple Business Manager User Guide: Link to an external device management service in Apple Business Manager or Apple School Manager User Guide: Link to an external device management service in Apple School Manager.
5. Return to the Automated Enrollment tab of the Device Management settings. In the **Upload the Token file from Apple Business Manager** section, either browse to or drag and drop the P7M file from Apple Business Manager or Apple School Manager.

©2026 Tanium Inc. All Rights Reserved

6. Click **Next**.
7. (Optional) Configure the welcome screen that users see when they are enrolling a device:
    a. In the **Upload corporate logo or other image** section, browse to or drag and drop a graphic file to show on the welcome screen.
    Supported file formats are JPG, JPEG, PNG, SVG, and GIF. The maximum file size is 1 MB.

    b. In the **Header** field, specify the heading to show on the Welcome screen.
    c. In the **Body** field, specify the text to show under the heading on the Welcome screen.
    d. In the **Button Text** field, specify the text for the button that users click to proceed with the enrollment process.

    > **Note:** If you skip this step during the initial configuration, you can return later and add a welcome screen.

8. Click **Next**.
9. (Optional) On the **Skip Keys for iOS**, configure the setup pages that iOS users see during device setup. Click **Skip** or **Show** for each setting, or, to configure the selection for all settings, click **Skip All** or **Show All**.

    > **Note:** If a skip key that was previously selected in your configuration is removed from a later release, saving this configuration again removes that skip key from your saved selections. Review your Skip Keys for iOS selections after upgrading to confirm they are still what you expect. For example, the Tips and Tap to Setup skip keys were removed in 1.4.944.

10. Click **Next**.
11. (Optional) On the **Skip Keys for macOS**, configure the setup pages that macOS users see during device setup. Click **Skip** or **Show** for each setting, or, to configure the selection for all settings, click **Skip All** or **Show All**.

    > **Note:** If a skip key that was previously selected in your configuration is removed from a later release, saving this configuration again removes that skip key from your saved selections. Review your Skip Keys for macOS selections after upgrading to confirm they are still what you expect. For example, the Tips and Tap to Setup skip keys were removed in 1.4.944.

12. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

(Apple, Optional) Configure Apps & Books organizational units

About this task

Connect an Apple Business Manager or Apple School Manager Apps & Books content token to allow Device Management to sync app license inventory and assign licenses to enrolled devices. Each content token represents one organizational unit (formerly called a location) in Apple Business Manager or Apple School Manager.

Note: The Apps & Books feature replaced the Apple Volume Purchase Program (VPP) service.

Before you begin

- Create or identify an Apple ID to use for the Apps & Books content token.

  Best Practice: Use a dedicated Managed Apple Account that multiple administrators in your organization can access. The content token expires after one year, and is invalidated if the password changes for the account that downloaded it.

- Sign in to Apple Business Manager or Apple School Manager with an account that can download an Apps & Books content token. By default, only the Administrator who creates an organizational unit can download its content token. To allow another team member to download the token, the Administrator must assign that team member the Content Manager role for the organizational unit: in Apple Business Manager or Apple School Manager, go to the **People** tab, search for and select the team member, click Edit, and assign the **Content Manager** role along with the organizational unit.

Add an organizational unit

1. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings.
2. On the **Apps & Books** tab, click **Add Organizational Unit**.
3. Sign in to Apple Business Manager or Apple School Manager and download the content token from Apple. For more information, see Apple Business User Guide: Manage content tokens in Apple Business or Apple School Manager User Guide: Manage content tokens in Apple School Manager.

©2026 Tanium Inc. All Rights Reserved

4. In the **Organizational Unit Name** field, specify a name for the organizational unit.
5. (Optional) In the **Description** field, specify a description for the organizational unit.
6. In the **Content Token** section, browse to or drag and drop the content token file that you downloaded from Apple Business Manager or Apple School Manager.
7. Click **Save**.

Manage organizational units

About this task

The organizational units list shows the Apple Portal Type (Apple Business Manager or Apple School Manager) for each organizational unit, along with its status. A status of **Expiring soon** means the content token for an otherwise active organizational unit expires within 30 days.

1. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click the **Apps & Books** tab.
2. For the organizational unit that you want to manage, click Organizational Unit actions , and then select **Edit details**, **Sync now**, or **Remove organizational unit**.

Result

Important: Removing an organizational unit removes its assigned applications from enrolled devices, and then permanently deletes the organizational unit and its license assignment records.

(Google) Configure a Google Workspace

Connect Device Management to a Google Workspace tenant to inventory and manage ChromeOS devices.

For more information, see (Google) Configuring a Google Workspace on page 73.

(Optional) Configure custom tags for devices

About this task

A custom tag is a user-defined label that you can assign to, or unassign from, endpoints. Tags are

©2026 Tanium Inc. All Rights Reserved

useful for defining computer group membership if you sometimes want to change which endpoints are members. For more information, see Tanium Console User Guide: Manage custom tags for computer groups. You can also use custom tags when targeting collections by referencing the **Custom Tags** sensor.

You can add or remove custom tags from devices enrolled with Device Management from the Device Management settings.

> **Note:** You cannot use custom tags as a parameter when asking questions with the **Custom Tag Exists** sensor, but you can view this data in reports.

1. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click the **Custom Tags** tab.
2. In the **Operation** section, select whether you want to **Add Tags** or **Remove Tags**.
3. Depending on the selected operation, either enter each tag on a new line in the **Tags** field or remove tags as needed.
4. In the **Device Targeting** section, configure the targeting for the addition or removal of the specified tags:
    a. Click **Add Row** or **Add Group**.
    b. (Group filter only) Select whether to apply a Boolean **AND** or **OR** to all the filters in the group.
    c. Select an option for the first or only targeting filter:

    Computer Group:

    The dropdown lists all the computer management groups and filter groups that you have permissions to access. You can type a string in the typeaheads field to filter the list if it is long. Select a computer group.

    Sensor:

    i. Perform one of the following sub-steps to specify each sensor:
    - Start typing the sensor name in the **Filter by Name** text field. The typeaheads dropdown list below the field shows a list of sensors that match your entry. Select a sensor and click Apply .

    Substring matching: To match only part of a result string, select

©2026 Tanium Inc. All Rights Reserved

the **Substring** checkbox, enter the **Start** position (where `0` is the first position), and enter the number of characters (**Length**). The following example matches results from the **Installed Applications** sensor where the first two characters match the string `ts`. For a multi-column sensor, you cannot apply the **Substring** filter to a specific column, only across all the columns (**Row Filter**).

- Click **Browse All Sensors** to open the **Browse Sensors** dialog and select a sensor. The bottom of the dialog displays the **Sensor Description**.

ii. Specify the filter operator and value. For more information about filter operators, see Reference: Filter operators on page 143.

iii. (Optional) Click **Advanced Sensor Options** below the filter to configure additional settings. For more information, see Advanced sensor settings.

d. Click Apply ✓.

e. (Optional) Click **Add Row** or **Add Group** to specify additional targeting filters.

5. Click **Add Custom Tags** or **Remove Custom Tags**, depending on the selected operation.

©2026 Tanium Inc. All Rights Reserved

Installing the Tanium Client

After you select a Tanium Client deployment template and the **Tanium Client Installer Status** is **Available**, the Tanium Client installs automatically when devices running an operating system that supports the Tanium Client enroll with Device Management. For a list of supported operating systems for the Tanium Client, see Tanium Client User Guide: Client version and operating system requirements.

Overview

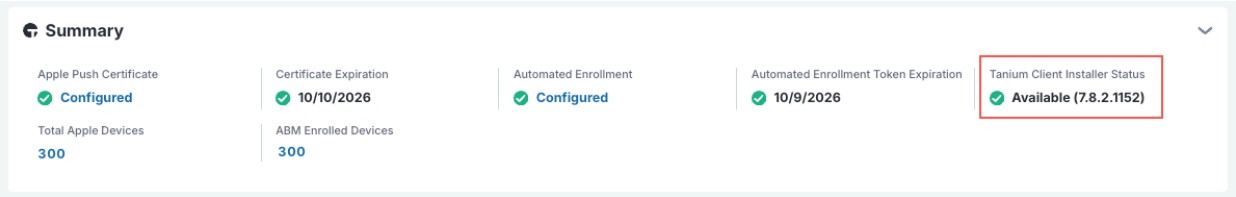
Device Management starts a process to create the Tanium Client Installer after you configure the following prerequisites:

- An Apple Push Notification service (APNs) certificate in Device Management. For more information, see (Apple) Configure an Apple Push Certificate to use with Device Management on page 37
- A Tanium Client deployment template selected in Device Management. The template must already exist in Tanium Client Management. For more information, see Tanium Client Management User Guide: (Optional) Create a Client deployment template and Select a Tanium Client deployment template on page 49

This process can take some time to complete after these requirements are met. The **Tanium Client Installer Status** section of the **Summary** panel on the **Device Management Overview** page shows one of the following statuses:

- **Available**: The Tanium Client installer is ready. When a version is available, the version number appears in parentheses (for example, **Available (7.8.2.1152)**).

  Figure 9. Tanium Client Installer Status: Available



©2026 Tanium Inc. All Rights Reserved

- **In Progress**: Device Management is preparing the Tanium Client installer.
- **No Installer**: No Tanium Client deployment template is selected. Click **No Installer** to go to the **Tanium Client** settings tab and select a template.

After the installer is available, Device Management pushes the Tanium Client to enrolled devices. Device Management also deploys the Tanium Client Privacy Preferences Policy Control (PPPC) profile to enrolled Macs, which grants the Tanium Client the macOS permissions that it requires. For more information about the PPPC profile, see Tanium Client PPPC profile on page 145. Enrolled devices are periodically checked for the presence of the Tanium Client and the Client is reinstalled if a user uninstalls it.

Note: This action changes the version only for new Tanium Client installations on newly enrolled devices. It does not initiate an upgrade for enrolled devices with an existing installation of an earlier version of the Tanium Client. For more information about upgrading the Tanium Client on enrolled devices, see Upgrading the Tanium Client on page 50.

Select a Tanium Client deployment template

About this task

Select the deployment template that Device Management uses to install the Tanium Client on enrolled Mac devices. The list of templates comes from Tanium Client Management.

Before you begin

- Configure the Apple Push Certificate with Device Management. For more information, see (Apple) Configure an Apple Push Certificate to use with Device Management on page 37.
- Create a Client deployment template in Tanium Client Management. For more information, see Tanium Client Management User Guide: Create a Client deployment template.

1. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click the **Tanium Client** tab.
2. From the **Tanium Client Template** list, select the deployment template to use when installing the Tanium Client on enrolled Mac devices.
3. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

Result

Device Management submits a signing request for the Tanium Client package from the selected template. The signing process can take several days. When the signed installer is ready, the **Tanium Client Installer Status** on the **Overview** page changes to **Available**.

Upgrading the Tanium Client

The Tanium Client Installer in Device Management only handles initial installations. Use Tanium Client Management to upgrade the Tanium Client on enrolled devices. For more information, see Tanium Client Management User Guide: Upgrading Tanium Clients.

©2026 Tanium Inc. All Rights Reserved

(Apple) Enrolling devices

Enroll devices in Device Management so that you can see information about the device in Tanium and manage settings.

Overview

Enroll endpoints in Device Management using one of these methods:

Automated enrollment

Automated device enrollment allows for devices purchased directly from Apple or authorized resellers to be preconfigured. With Apple Business Manager or Apple School Manager, endpoints automatically enroll into Tanium and receive the initial settings that you configure in Device Management.

Manual enrollment

With this method, an enrollment profile is provided by Device Management to install on the endpoint manually.

Automated device enrollment

1. Import a server token from your Apple enrollment system. When devices enroll in an Apple enrollment system, they are assigned to a server token. When you import a server token into Device Management, the list of devices assigned to the server token is identified to Tanium. For more information, see (Apple, Optional) Configure automated enrollment using an Apple enrollment system on page 41.
2. Create settings. Settings include custom settings uploaded to Device Management from a configuration profile and password and screen unlock settings that you create in Device Management. For information, see (Apple) Managing settings on page 53.
3. Create collections to target settings to these devices. For more information, see (Apple) Managing collections on page 68.

Result

©2026 Tanium Inc. All Rights Reserved

Important: A device fails to enroll if an unmanaged Activation Lock is already enabled on the device, such as a User-linked Activation Lock tied to a personal Apple Account. An Activation Lock prevents Device Management from establishing a managed Activation Lock during enrollment. Before you enroll the device with Device Management, release the Activation Lock. For example, remove the device from Find My, or if the device has already been erased, release the Activation Lock at the activation prompt. For more information, see Apple Platform Deployment: Activation Lock on Apple devices and Apple Support: Remove a device from Find Devices on iCloud.com.

Manual enrollment

Use an enrollment profile that you download from Device Management to manually install on the endpoint for enrollment.

Best Practice: Manual enrollment is typically used only for testing.

1. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click **Device Enrollment**.
2. In the **Manual Enrollment** section, click **Download** and select the enrollment file for the endpoint operating system.
3. When the download finishes, copy the enrollment file to the endpoint.
4. Install the profile on the endpoint. For more information about installing profiles on a macOS device, see Mac User Guide: Use configuration profiles to standardize settings on Mac computers.

©2026 Tanium Inc. All Rights Reserved

(Apple) Managing settings

About this task

Create setting configurations that you can group with web clips and enterprise applications into *collections* and push out to enrolled endpoints.

Add a custom setting

About this task

You can use a configuration profile that you generate outside of Device Management to create custom settings. For more information about these profiles, see Apple Platform Deployment documentation: Configuration profiles.

1. From the Main menu, go to **Shared Services** > **Device Management Apple** > **Settings**.
2. In the **Custom Setting** section, click +.
3. Specify the name for the setting configuration and click ✓ to save your change.
4. In the **Choose a platform** section, select the operating systems for which the setting applies.
5. In the **Upload your profile** section, browse to or drag and drop the MOBILECONFIG file for the setting.
6. Click **Open**.
7. (Optional) In the **Notes** section, add notes to identify the setting configuration.
8. Click **Save**.

Add a curated setting

About this task

If you do not have a configuration profile, use the curated settings to configure settings for endpoints.

1. From the Main menu, go to **Shared Services** > **Device Management Apple** > **Settings**.

©2026 Tanium Inc. All Rights Reserved

2. In the tile for the setting that you want to add, click +.
3. Specify the name for the setting configuration and click ✓ to save your change.
4. In the **Choose a platform** section, select the operating systems for which the setting applies.
5. Configure the options for the setting.
   For more information, see:

   - Apple Platform Deployment documentation: Device management payload list for Mac computers
   - Apple Platform Deployment documentation: Device management payload list for iPhone and iPad devices

   Note:

   - If you configure a setting that is not compatible with a targeted device, such as a Software Update Enforcement setting configured with an OS version that is not compatible with the hardware on the targeted device, the device might return an error or silently ignore the enforcement. This behavior is by Apple design. In this scenario, the enforcement shows in the MDM profile and no errors or notifications are shown on the device.
   - If you enable FileVault for a device, the recovery key is available in Enforce. From the Main menu, go to **Modules** > **Enforce** > **Endpoint Encryption** > **Recovery Keys**. Recovery keys escrowed using Device Management are not available through the encryption key recovery portal.

6. Click **Save**.

Delete a setting

About this task

Important: You can delete settings that are used in collections. Confirm the usage and deployment before you delete a setting.

©2026 Tanium Inc. All Rights Reserved

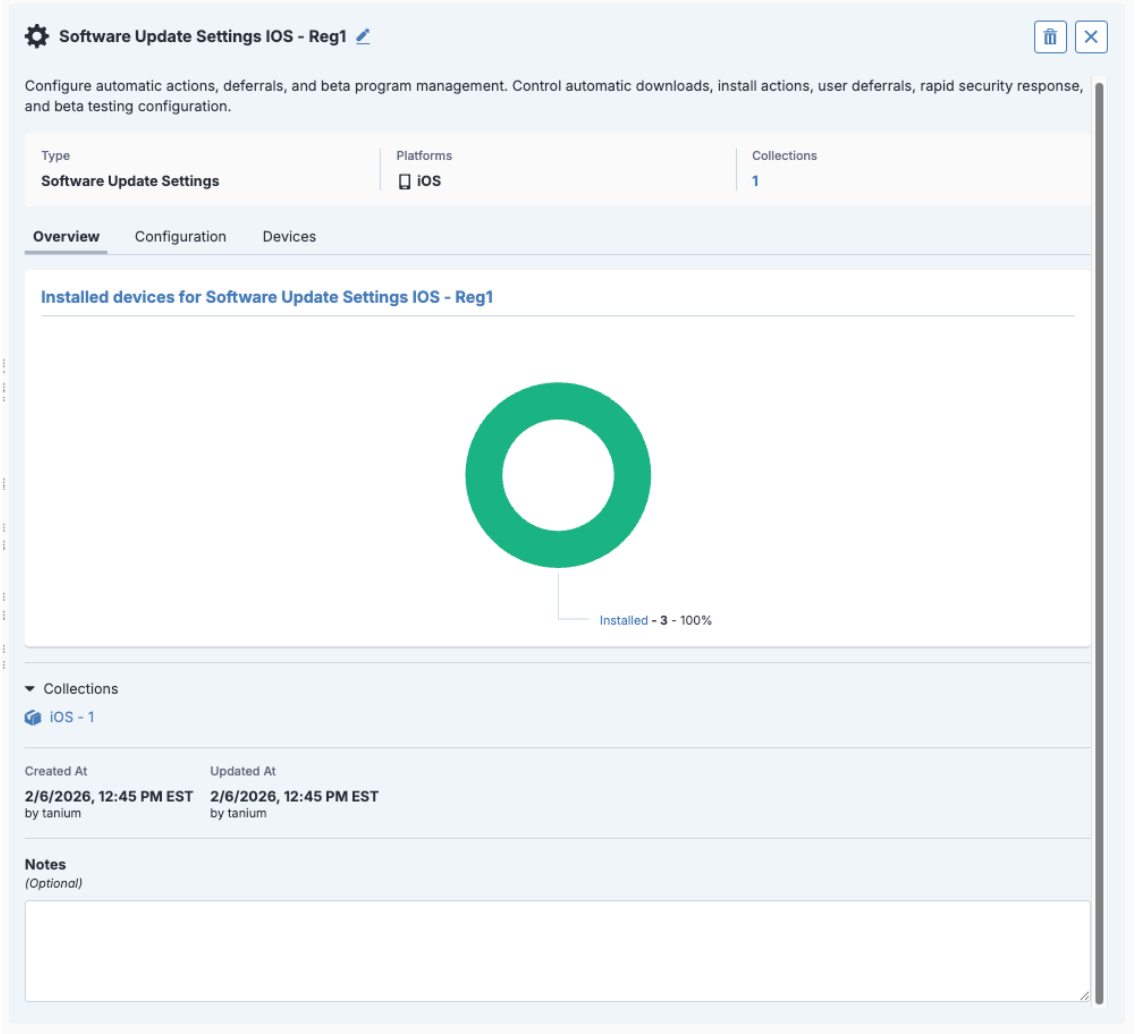
1. From the Main menu, go to **Shared Services** > **Device Management Apple** > **Settings**.
2. In the **Settings Configurations** list, click the name of the setting that you want to delete.
3. Click Delete .
4. Click **Confirm**.

Review settings

1. From the Main menu, go to **Shared Services** > **Device Management Apple** > **Settings**.
2. In the **Settings Configurations** list, click the name of the setting that you want to review.
    - On the **Overview** tab, you can see the status of the setting application, the collections to which the settings belong, who created the settings, when the settings were created, and notes. Click a status in the donut chart to see a list of the endpoints.

      Figure 10. Overview tab

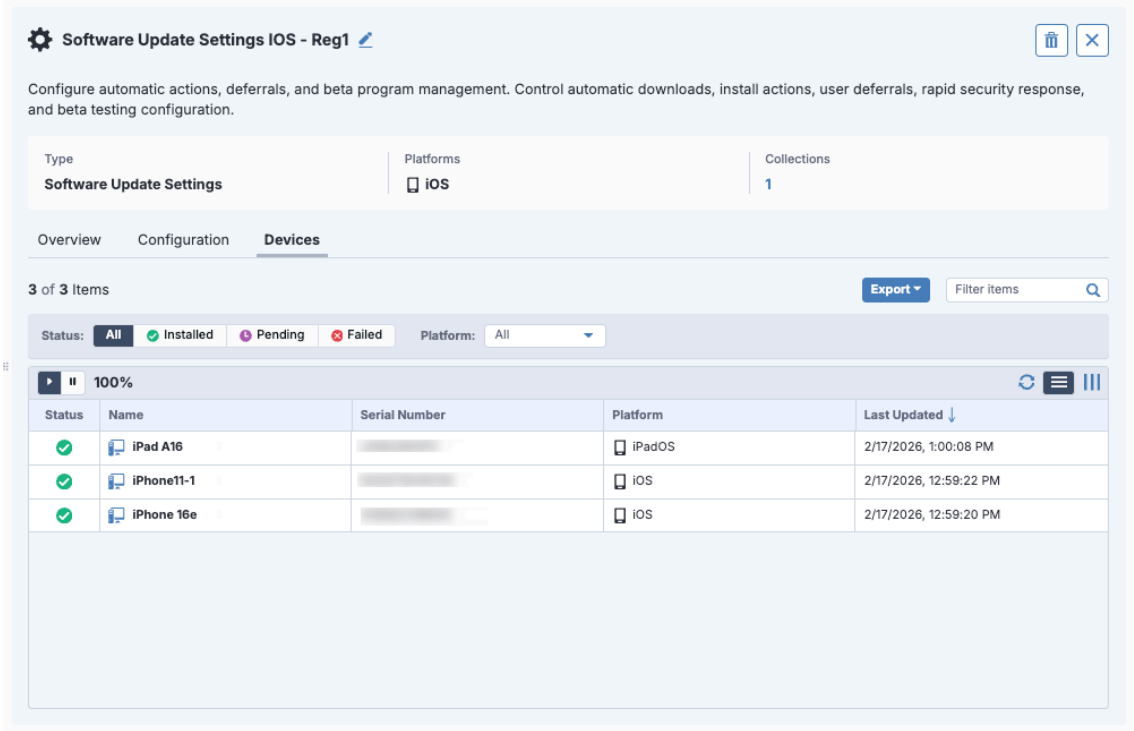
©2026 Tanium Inc. All Rights Reserved



- (Custom settings) The **Configuration** tab shows the platforms for the setting and the profile used for the setting. Click **View XML** to review the profile details. Click **Replace** and browse or drag and drop a MOBILECONFIG file to use a different profile.
- The **Devices** tab shows details about the endpoints where the settings are applied.

Figure 11. Devices tab

©2026 Tanium Inc. All Rights Reserved



Use device variables in settings

When you create or edit a setting, you can include *device variables*, which are placeholders that Device Management automatically replaces with the actual information for the device when the setting is delivered. Device variables let you build one setting that applies correctly to every targeted device, instead of creating a separate setting for each device.

Syntax

Wrap a variable name in double curly braces: `{{VariableName}}`. Place the variable inside a text field where you would normally type a literal value.

Examples:

- In the proxy username field in a Wi-Fi setting: `{{SerialNumber}}`
- In the Subject field of a Certificates setting: `CN={{SerialNumber}},O=Example Corp`

Variable names are case-sensitive. `{{SerialNumber}}` resolves correctly; `{{serialnumber}}` or `{{SERIALNUMBER}}` does not. Use the exact spelling and capitalization shown in the following table.

©2026 Tanium Inc. All Rights Reserved

Available device variables

Device variables

Variable	Description
SerialNumber	The device serial number.
UDID	The device UDID.
DeviceName	The device name, as shown in Device Management .
ModelIdentifier	The device model identifier, for example, iPhone13,3.
ModelMarketingName	The device model marketing name, for example, iPhone 13 Pro.
ModelFamily	The device model family, for example, iPhone.
OSVersion	The device operating system version.
OSMarketingName	The operating system marketing name.
WiFiMAC	The device Wi-Fi MAC address.
EthernetMAC	The device Ethernet MAC address.
BluetoothMAC	The device Bluetooth MAC address.
Hostname	The device network host name.
UserEmail	The email address of the enrolled user. Available only for ADE-enrolled devices. See UserEmail and UserName require ADE enrollment on page 59 .
UserName	The name of the enrolled user. Available only for ADE-enrolled devices. See UserEmail and UserName require ADE enrollment on page 59 .

Limitations

Device variables only replace text inside an existing value. You cannot use a device variable to build a list, add conditional logic, or generate new fields. If you type a variable name that is not in the preceding table, or misspell one, Device Management rejects the setting when you try to save it, so

©2026 Tanium Inc. All Rights Reserved

you find out immediately instead of after the setting is delivered.

UserEmail and UserName require ADE enrollment

UserEmail and **UserName** are populated only for devices that enrolled through Automated Device Enrollment (ADE) with an identity provider configured for authenticated enrollment. Devices enrolled any other way, including ADE enrollments that did not use an identity provider, have blank values for these two variables. A blank value does not cause an error: the setting still saves and delivers successfully, with an empty value where the variable was. Use **UserEmail** or **UserName** only if every device that the setting is assigned to is known to have enrolled through ADE with identity provider authentication.

Using device variables in a Wi-Fi setting

In a **Wi-Fi** setting, you can use a device variable in the proxy username field. **SerialNumber**, **UDID**, **DeviceName**, **Hostname**, **UserEmail**, and **UserName** are all appropriate here, depending on how your proxy server identifies devices or users.

Using device variables in a Certificates setting

If you use a device variable in a **Certificates** setting (SCEP or ACME), use **SerialNumber**, **UDID**, or **ModelIdentifier** since these values never change for a device. Avoid **UserEmail**, **Hostname**, or **DeviceName** if the value might change after you assign the setting: if the value changes between assignment and when the device requests a certificate, the request can fail. If this happens, resend the setting to the affected devices; the setting regenerates correctly using current information from the device.

What to do next

To apply these settings to devices, create a collection and target the collection to a group of devices. For more information, see (Apple) Managing collections on page 68.

©2026 Tanium Inc. All Rights Reserved

(Apple) Configuring Software Update Settings and Software Enforcement settings

Create software update settings, which can consist of software update options and software restrictions, to manage software updates for iOS and macOS devices. For example, you can create a restriction to delay user visibility of major software updates, and then enforce those settings across different devices. On macOS devices, users can see the settings in **System Settings** > **General** > **Device Management**. On iOS devices, users can see the settings in **System Settings** > **General** > **VPN & Device Management**.

The **Device Management Overview** page includes reports for **Mac Devices by Version** and **iOS Devices by Version**. For more information about Apple software updates, see Apple Platform Deployment Documentation: About software updates for Apple devices.

Create a Software Update Settings setting

About this task

Define the device software update settings and restrictions.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Apple** > **Settings**.
2. In the **Software Update Settings** tile, click +.
3. Specify the name for the setting configuration and click ✓ to save your change.
4. In the **Choose a platform** section, select the operating systems for which the setting applies.
5. Configure the options for the setting and click **Save**.
   For more information about the options, see Apple Platform Deployment documentation: SoftwareUpdateSettings (and child objects).

Create a Software Update Enforcement setting

©2026 Tanium Inc. All Rights Reserved

About this task

Define the update deadlines and target build versions.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Apple** > **Settings**.
2. In the **Software Update Enforcement** tile, click +.
3. Specify the name for the setting configuration and click ✓ to save your change.
4. In the **Choose a platform** section, select the operating systems for which the setting applies.
5. Configure the options for the setting and click **Save**.
   For more information about the options, see Apple Platform Deployment documentation: SoftwareUpdateEnforcementSpecific.

   > **Note:** If you configure a setting that is not compatible with a targeted device, such as a Software Update Enforcement setting configured with an OS version that is not compatible with the hardware on the targeted device, the device might return an error or silently ignore the enforcement. This behavior is by Apple design. In this scenario, the enforcement shows in the MDM profile and no errors or notifications are shown on the device.

What to do next

- For more information about managing settings, see (Apple) Managing settings on page 53.
- To target these settings to devices, create a collection and target the collection to a group of devices. For more information, see (Apple) Managing collections on page 68.

©2026 Tanium Inc. All Rights Reserved

(Apple) Managing web clips, applications, and Apps & Books

Create web clip, application, and Apps & Books configurations that you can group with *settings* into *collections* and push out to enrolled devices.

You can create configurations for enterprise applications, web clips (which add a shortcut to a website on the Home Screen), and licensed applications from a connected Apps & Books organizational unit. For more information about web clips, see Apple documentation: Web Clips device management payload settings for Apple devices. For more information about Apps & Books, see Apple documentation: Intro to apps and books licenses in Apple Business.

Note: The Apps & Books feature replaced the Apple Volume Purchase Program (VPP) service.

(macOS) Add an enterprise application

1. From the Main menu, go to **Shared Services** > **Device Management** > **Apple** > **Applications**.
2. In the **Enterprise Application** tile, click +.
3. Specify the name for the application configuration and click ✓ to save your change.
4. In the **Application Package** section, browse to or drag and drop the PKG file for the application.

   Note: Only distribution packages are supported for installation. Component packages are not supported.
5. Select whether you want to **Install as Managed**.
6. (Optional) Provide the **App Configuration**.

©2026 Tanium Inc. All Rights Reserved

> **Note:**
>
> - Most apps do not require this additional information. Specify these details only when required by the app publisher.
> - This file is a dictionary with the application configuration. For more information about this file, see Apple Developer documentation: Configuring managed apps and extensions and Apple Developer Documentation: AppManagedAppConfigDictionaryObject.

7. (Optional) Specify **Notes** for the application.
8. Click **Save**.

(iOS) Add a web clip

1. From the Main menu, go to **Shared Services** > **Device Management** > **Apple** > **Applications**.
2. In the **Web Clip** tile, click +.
3. Specify the name for the web clip configuration and click ✓ to save your change.
4. In the **Application Name** field, specify the name for the web clip as you want it shown on the Home Screen.
5. In the **URL** field, provide the URL for the web clip.
6. For the **Is Removable** field, select **Yes** if you want to allow the user to remove the web clip from the Home Screen or **No** to not allow removal.
7. For the **Full Screen** field, select whether you want to open the web clip as a full-screen web app.
8. In the **Icon Upload** section, browse to and update a PNG file to use for the web clip icon on the Home Screen.
9. For the **Precomposed Icon** field, select **Yes** if you want the operating system to apply default styling to the icon or **No** to show the icon as-is.
10. (Optional) Specify **Notes** for the web clip.
11. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

(Apple) Add an App Store application

About this task

Add an application from a connected Apps & Books organizational unit to make the license available for assignment to enrolled devices. For more information about connecting an organizational unit, see Configure Apps & Books organizational units on page 44.

> **Note:** Device Management supports app licenses only. Book licenses are not supported.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Apple** > **Applications**.
2. In the **App Store** tile, click +.
3. Select the organizational unit that has the license that you want to assign.
4. Select the application that you want to add. The library shows the available license count for each application.

   > **Note:**
   >
   > - An application that is removed from Apple Business Manager or Apple School Manager shows a status of **Removed from store**. You can view existing assignments for a removed application, but you cannot make new assignments.
   > - Applications are installed as managed applications that Device Management can update and remove.

5. Click **Save**.

Delete a web clip or application

About this task

©2026 Tanium Inc. All Rights Reserved

Important: You can delete web clips and applications that are used in collections. Confirm the usage and deployment before you delete them.

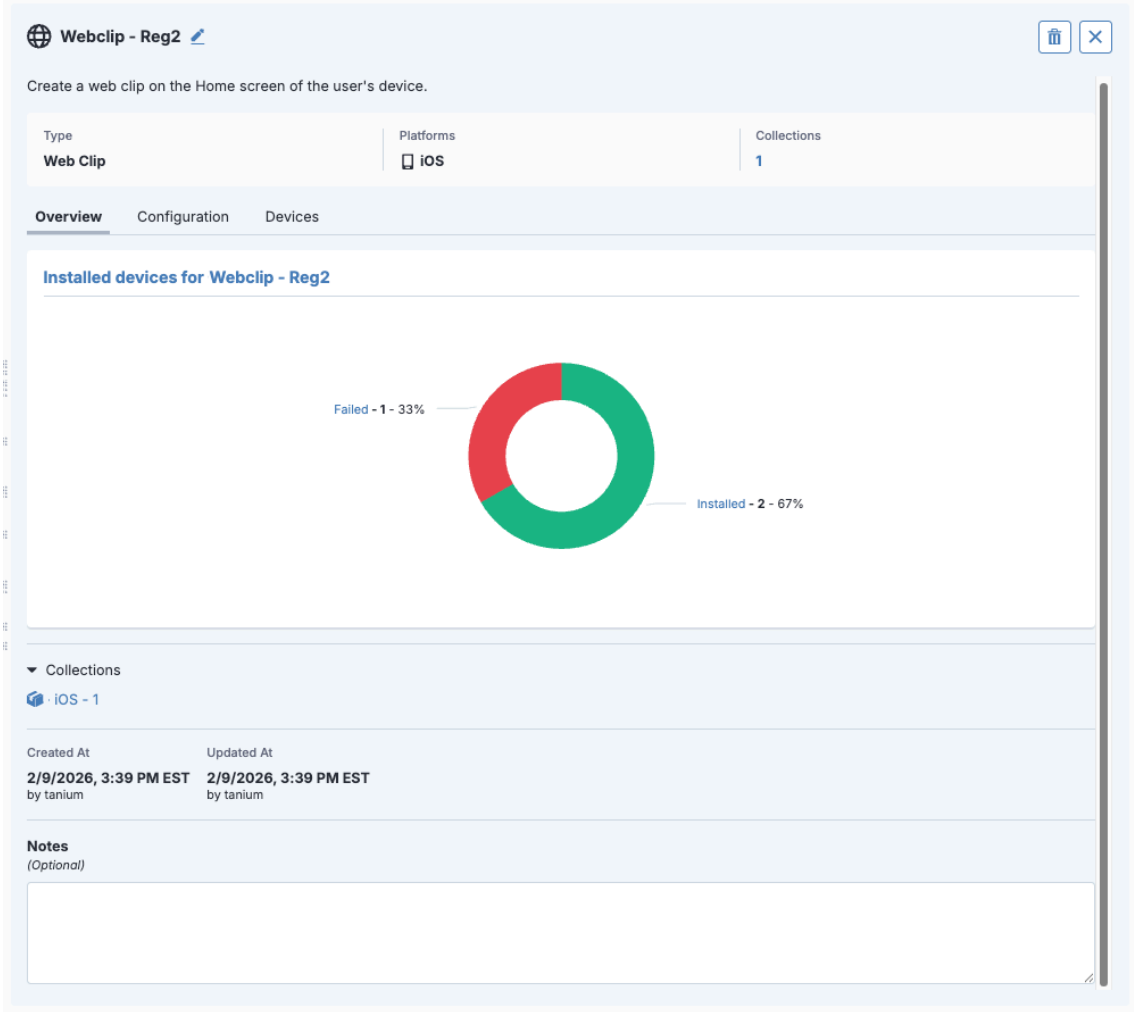
1. From the Main menu, go to **Shared Services** > **Device Management** > **Apple** > **Applications**.
2. In the **Applications** list, click the name of the web clip or application that you want to delete.
3. Click Delete .
4. Click **Confirm**.

Review web clips and applications

1. From the Main menu, go to **Shared Services** > **Device Management** > **Apple** > **Applications**.
2. In the **Applications** list, click the name of the web clip or application that you want to review.
    - On the **Overview** tab, you can see the status of the setting application, the collections to which the application or web clip belongs, who created the settings, when the settings were created and updated, and notes. Click a status in the donut chart to see a list of the endpoints with that status.

      Figure 12. Overview tab

©2026 Tanium Inc. All Rights Reserved



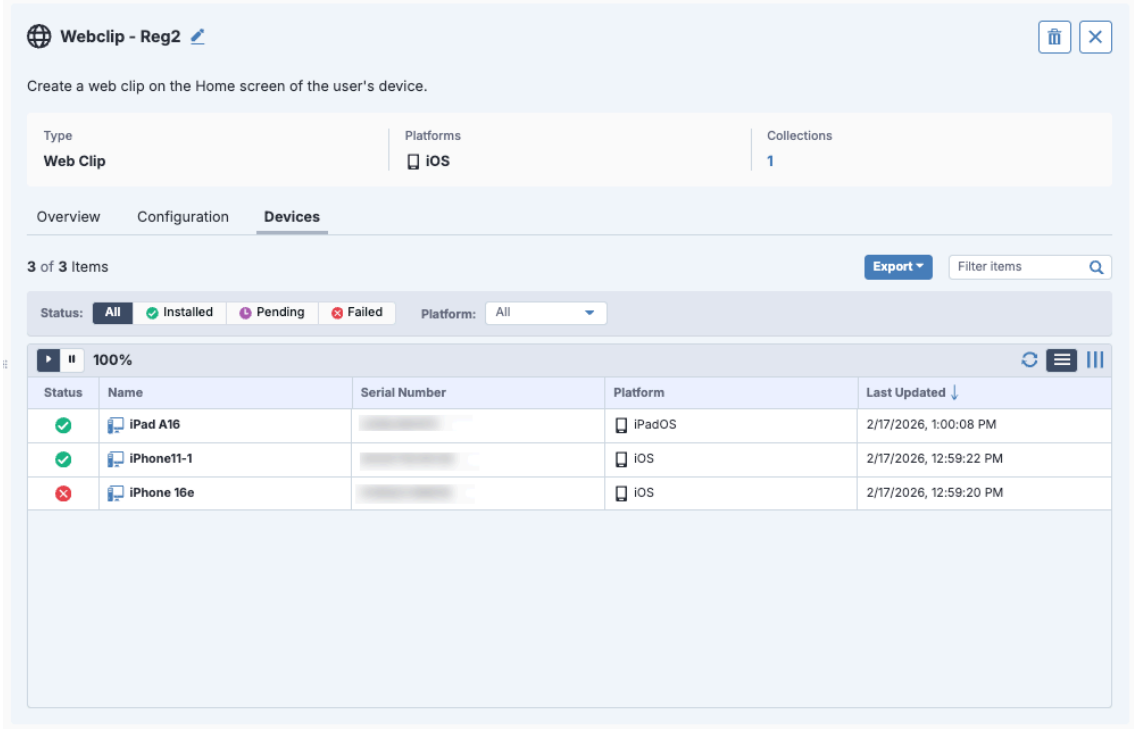
- The **Configuration** tab shows the configuration for the application or web clip.

> **Note:** The version shown on this tab for enterprise applications is derived from the file metadata. If the publisher does not specify the correct version information in the metadata, the version shown on this tab might not correspond to the actual version of the file. The version installed on devices is determined by the version embedded in the file.

- The **Devices** tab shows details about the endpoints where the application or web clip is applied.

Figure 13. Devices tab

©2026 Tanium Inc. All Rights Reserved



What to do next

To install enterprise applications, configure web clips, and assign App Store application licenses on devices, create a collection and target the collection to a group of devices. For more information, see (Apple) Managing collections on page 68.

©2026 Tanium Inc. All Rights Reserved

(Apple) Managing collections

Create collections and target enrolled devices to apply settings, configure web clips, and install applications.

Create a collection

Before you begin

Create the settings, web clips, and applications that you want to include in a collection to apply on enrolled devices. For more information, see (Apple) Managing settings on page 53 and (Apple) Managing web clips, applications, and Apps & Books on page 62.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Apple** > **Collections**.
2. Click Add Collection +.
3. Specify the name for the collection and click ✓ to save.
4. (Optional) In the **Notes** section, add notes with details about the collection.
5. Click **Next**.
6. Click **Add** for each setting that you want to add to the collection and click **Next**.
7. Click **Add** for each enterprise application, App Store application, or web clip that you want to add to the collection and click **Next**.

   > **Note:** If the number of devices targeted by the collection exceeds the available license count for an App Store application, Device Management still creates the collection and assigns the license to devices up to the available count. The remaining devices show a status of **Pending license**. To resolve this, purchase additional licenses in Apple Business Manager or Apple School Manager or reduce the number of targeted devices, and then sync the organizational unit.

8. Configure the targeting filter for the collection:
   a. Click **Add Row** or **Add Group**.
   b. (Group filter only) Select whether to apply a Boolean **AND** or **OR** to all the filters in

©2026 Tanium Inc. All Rights Reserved

the group.

c. Select an option for the first or only targeting filter:

Computer Group:

The dropdown lists all the computer management groups and filter groups that you have permissions to access. You can type a string in the typeaheads field to filter the list if it is long. Select a computer group.

Sensor:

i. Perform one of the following sub-steps to specify each sensor:

- Start typing the sensor name in the **Filter by Name** text field. The typeaheads dropdown list below the field shows a list of sensors that match your entry. Select a sensor and click Apply ✓.

  Substring matching: To match only part of a result string, select the **Substring** checkbox, enter the **Start** position (where `0` is the first position), and enter the number of characters (**Length**). The following example matches results from the **Installed Applications** sensor where the first two characters match the string `ts`. For a multi-column sensor, you cannot apply the **Substring** filter to a specific column, only across all the columns (**Row Filter**).

- Click **Browse All Sensors** to open the **Browse Sensors** dialog and select a sensor. The bottom of the dialog displays the **Sensor Description**.

ii. Specify the filter operator and value. For more information about filter operators, see Reference: Filter operators on page 143.

iii. (Optional) Click **Advanced Sensor Options** below the filter to configure additional settings. For more information, see Advanced sensor settings.

> **Note:** This targeting filter is not limited by your management rights. The collection targets every device that matches the filter, regardless of the Computer Groups assigned to your user, user group, or active Persona. For more information, see User role requirements on page 23.

d. Click Apply ✓.

e. (Optional) Click **Add Row** or **Add Group** to specify additional targeting filters.

©2026 Tanium Inc. All Rights Reserved

9. Click **Add**.
10. Click **Preview Targeted Endpoints** to verify the devices that you are targeting with the collection. If the targeted devices are accurate, click **Save**. Click Edit to adjust the targeting filter.

Delete a collection

About this task

Important: You can delete collections that are applied to devices. Confirm the usage and deployment before you delete a collection.

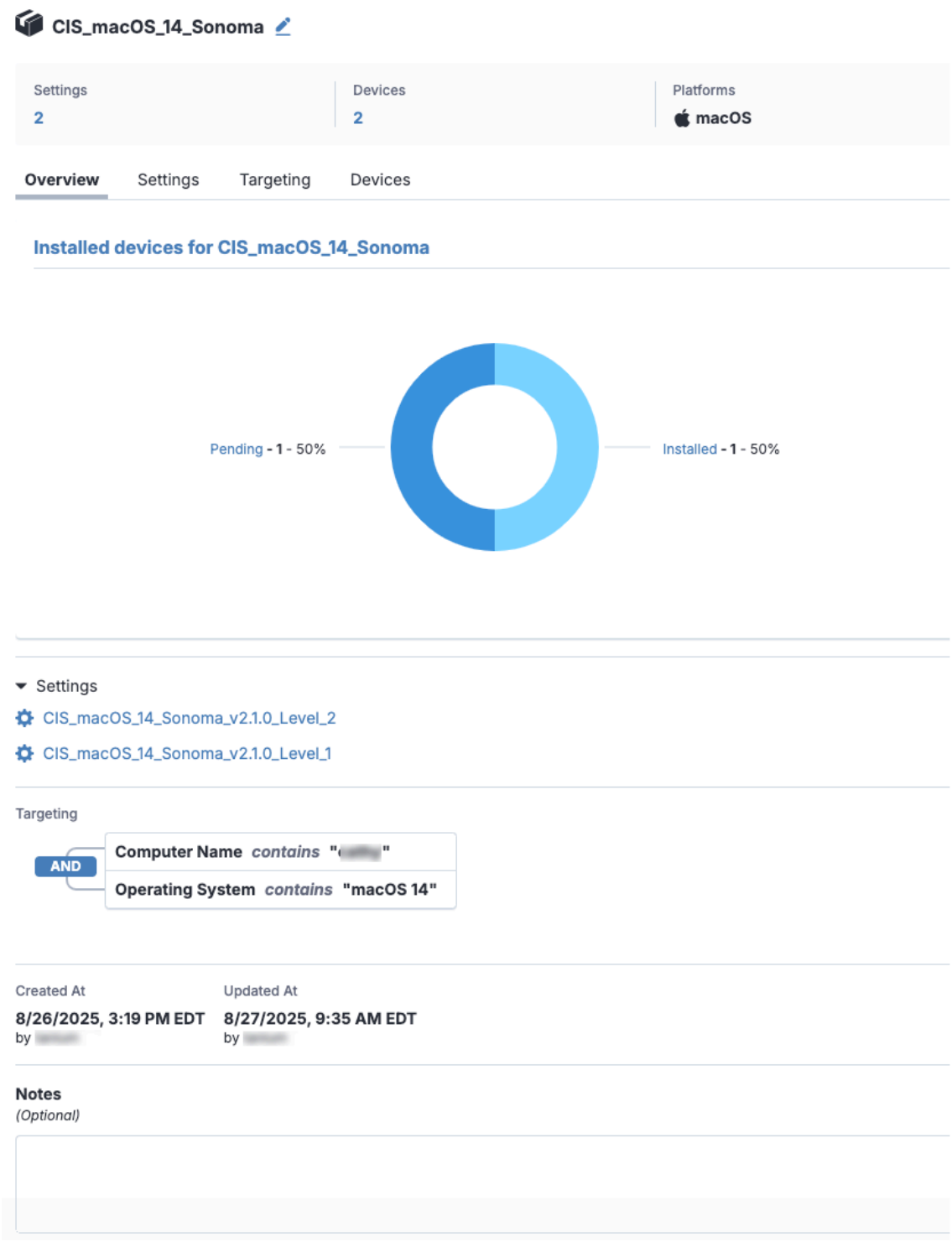
1. From the Main menu, go to **Shared Services** > **Device Management** > **Apple** > **Collections**.
2. In the **Collections** list, click the name of the collection that you want to delete.
3. Click Delete.
4. Click **Confirm**.

Review collections

1. From the Main menu, go to **Shared Services** > **Device Management** > **Apple** > **Collections**.
2. In the **Collections** list, click the name of the collection that you want to review.
    - On the **Overview** tab, you can see the devices where the collection is applied, the settings in the collection, the targeting for the collection, who created the collection, when the collection was created, and notes. Click a status in the donut chart to see a list of the devices with that status.

      Figure 14. Overview tab

©2026 Tanium Inc. All Rights Reserved

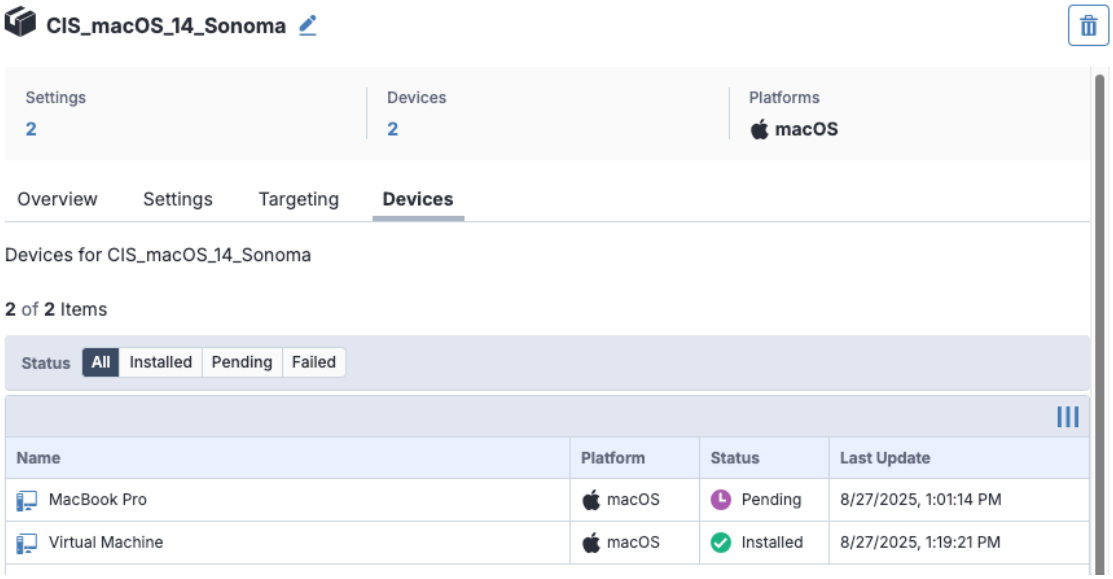


- The **Settings** tab shows the settings in the collection. Click the name of the setting to review the details. Click to add or remove settings from the collection.
- The **Applications** tab shows the applications and web clips in the collection. Click the name of an application or web clip to review the details. Click to add or remove an application or web clip from the collection.

©2026 Tanium Inc. All Rights Reserved

- The **Targeting** tab shows the targeting filter for the collection. From this tab, click **Preview Targeted Endpoints** to see the devices targeted by this collection. Click Edit to update the targeting filter. Click Remove to delete the targeting filter.
- The **Devices** tab shows details about the devices where the collection is applied.

Figure 15. Devices tab



©2026 Tanium Inc. All Rights Reserved

(Google) Configuring a Google Workspace

Configure a Google Workspace to connect Device Management to your Google Workspace tenant and begin syncing ChromeOS devices.

Note: You can configure up to 20 Google Workspaces. Each workspace connects to one Google Workspace tenant and syncs ChromeOS devices.

Note: Android Enterprise device management does not require a Google Workspace. Android Enterprise is a separate, standalone registration. For more information, see View and manage Android Enterprise registration on page 84.

Before you begin

Before you configure a Google Workspace in Device Management, ensure you have the following:

- Access to the Google Cloud Console with a project.
- Permissions in Google Cloud to enable APIs, create service accounts, and create service account keys.
- The **Organization Policy Administrator** and **Editor** roles in Google Cloud, if your organization blocks service account key creation by default.
- Access to the Google Workspace Admin Console with the **Super Admin** or **Device Admin** role.
- ChromeOS devices enrolled in your Google Workspace domain.

Set up a Google service account

©2026 Tanium Inc. All Rights Reserved

Set up a service account in Google Cloud and authorize it in Google Workspace so that Device Management can sync devices and manage policies.

Step 1: Enable the required Google Cloud APIs

Before you begin

Enable the APIs that match the device types and features you want to manage:

- **Admin SDK API**: Required to sync ChromeOS device inventory from Google Workspace.
- **Chrome Policy API**: Required to manage Chrome policies on organizational units (OUs) and groups.

1. Go to the Google Cloud Console and select your project.
2. Go to **APIs & Services** > **Library**.
3. Search for each API by name, select it from the search results, and then click **Enable**.

Step 2: Create a service account

About this task

Create a dedicated service account that Device Management uses to access Google Workspace device data.

1. In the Google Cloud Console, go to **IAM & Admin** > **Service Accounts**.
2. Click **Create Service Account**.
3. Enter a service account name (for example, `google-device-sync`) and a description that identifies the service account as the one that Device Management uses to sync Google devices.
4. Click **Create and Continue**.
5. Skip **Grant this service account access to project** and click **Continue**.
6. Skip **Grant users access to this service account** and click **Done**.

Step 3: Create a JSON key for the service account

©2026 Tanium Inc. All Rights Reserved

About this task

Generate a JSON key that Device Management uses to authenticate as the service account.

1. In the service accounts list, click the service account you created.
2. Click the **Keys** tab.
3. Click **Add Key** > **Create new key**.
4. Select **JSON** and then click **Create**. The JSON key file downloads automatically.

Next steps

Important: Store the JSON key file securely. The key provides access to your Google Workspace data and cannot be recovered if lost. Do not commit the key to version control.

Note: If you receive an error that service account key creation is disabled by organization policy, an organization administrator must override the policy for the project before you can create a key. For more information, see Google Cloud documentation: Restricting service account usage.

Step 4: Enable domain-wide delegation in Google Cloud

About this task

Domain-wide delegation allows the service account to impersonate users in your Google Workspace domain.

1. On the service account details page, expand **Advanced settings**.
2. In the **Domain-wide delegation** section, select **Enable Google Workspace Domain-wide Delegation**.
3. In **Product name for consent screen**, enter `Tanium Device Management`.
4. Click **Save**. Google Cloud generates a Client ID for the service account.
5. Copy the Client ID. You need it in the next step.

©2026 Tanium Inc. All Rights Reserved

Step 5: Authorize the service account in Google Workspace

About this task

Authorize the service account to access Google device data in your Google Workspace domain.

1. Go to the Google Workspace Admin Console and sign in with a **Super Admin** account.
2. Go to **Security** > **Access and data control** > **API Controls**.
3. In the **Domain-wide delegation** section, click **Manage Domain Wide Delegation**.
4. Click **Add new**.
5. In the **Client ID** field, paste the Client ID that you copied in Step 4.
6. In the **OAuth scopes** field, enter the scopes for your use case as a comma-separated list.
   For device management only

   ```
   https://www.googleapis.com/auth/admin.directory.device.chromeos
   ```

   For device management and Chrome policy management

   ```
   https://www.googleapis.com/auth/admin.directory.device.chromeos,
   https://www.googleapis.com/auth/chrome.management.policy,
   https://www.googleapis.com/auth/admin.directory.orgunit.readonly,
   https://www.googleapis.com/auth/admin.directory.group.readonly
   ```

   Important: Enter the OAuth scopes exactly as shown. Misspelled or extra characters cause validation errors when you save the workspace.

   Important: Chrome policy management requires all of the scopes in the second list, not just `chrome.management.policy`. Device Management uses the `admin.directory.orgunit.readonly` and `admin.directory.group.readonly` scopes to read the organizational units and groups that you target with Chrome policies.

   Note: These scopes grant both read (inventory) and write (action) permissions.
7. Click **Authorize**. The service account appears in the list of authorized API clients.

©2026 Tanium Inc. All Rights Reserved

Step 6: Prepare credentials for Device Management

You now have everything you need to create the Google Workspace in Device Management. When you create the workspace, you provide the following:

- **Service Account JSON**: The entire contents of the JSON key file that you downloaded in Step 3.
- **Admin Email**: A Google Workspace admin email address that the service account impersonates.

Service Account JSON

When you open the downloaded JSON key file in a text editor, the contents look like the following example:

```
{
  "type": "service_account",
  "project_id": "your-project-id",
  "private_key_id": "abc123...",
  "private_key": "-----BEGIN PRIVATE KEY-----\n...\n-----END PRIVATE KEY-----\n",
  "client_email": "google-device-sync@your-project.iam.gserviceaccount.com",
  "client_id": "106584026335185594283",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/..."
}
```

Admin Email

The admin email address must meet the following requirements:

- Be a valid Google Workspace user in your domain.
- Have the **Super Admin** or **Device Admin** role.
- Have permission to view devices in the Google Workspace Admin Console for the device types that you want to manage.

For example: `admin@yourdomain.com` or `device-admin@yourdomain.com`.

Create a Google Workspace

1. From the Main menu, go to **Shared Services** > **Device Management** > **Google** > **Workspaces**.

©2026 Tanium Inc. All Rights Reserved

2. Click **Create Google Workspace**.
3. In the **Instance Name** field, enter a unique name for this workspace.
4. In the **Service Account JSON** section, upload the JSON key file that you downloaded earlier from the Google Cloud Console.
5. Enter the administrator email address in the **Admin Email** field.

   Important: Device Management validates the service account credentials when you save. If a required OAuth scope is missing from the domain-wide delegation configuration, an error appears. Verify that all required scopes are granted in the Google Workspace Admin Console before saving.
6. Click **Save**.

Result

After saving, Device Management begins an initial ChromeOS device sync. The sync interval adjusts automatically based on the number of devices in the workspace.

Note: To apply Chrome policies by group, the groups must exist in your Google Workspace before you can target them in Device Management. Device Management does not create Google groups. Create groups in the Google Workspace Admin Console (**Directory** > **Groups**). For more information, see Google Workspace Admin Help: Create a group.

Edit a Google Workspace

1. From the Main menu, go to **Shared Services** > **Device Management** > **Google** > **Workspaces**.
2. Click the name of the workspace you want to edit.
3. Update the workspace name, service account JSON file, or administrator email address as needed.
4. Click **Save**.

Perform a manual sync

About this task

©2026 Tanium Inc. All Rights Reserved

Device data syncs automatically on a periodic schedule. To sync immediately, perform a manual sync.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Google** > **Workspaces**.
2. In the row for the workspace you want to sync, click Sync.

Delete a Google Workspace

About this task

Important: Deleting a workspace removes all device data synced from that workspace from Device Management. This action cannot be undone.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Google** > **Workspaces**.
2. In the row for the workspace you want to delete, click Delete.
3. Click **Confirm**.

Result

©2026 Tanium Inc. All Rights Reserved

(Google) Managing Chrome policies

View and manage Chrome policies for ChromeOS devices in your Google Workspace. Policies are applied at the Organizational Unit (OU) level and can be set locally on an OU or inherited from a parent OU. For more information about Chrome policies, see Google Chrome Enterprise Help: Set ChromeOS device policies and Google Chrome Enterprise Help: Set Chrome policies for users or browsers. For more information about organizational units, see Google Workspace Admin Help: Add an organizational unit.

Note: Chrome policy management requires a Google Workspace with ChromeOS enabled. For more information, see (Google) Configuring a Google Workspace on page 73.

Policy states

Each Chrome policy has one of the following states:

Google Default

The policy uses the default value that Google applies when no administrator has configured it.

Inherited

The policy value is set at a higher level in the OU hierarchy and cascades down to child OUs.

Locally Set

The policy value is configured specifically on this OU and does not inherit from a parent.

View Chrome policies

1. From the Main menu, go to **Shared Services** > **Device Management** > **Google** > **ChromeOS**.
2. If you have more than one Google Workspace configured, select the workspace from the **Workspace** list.

©2026 Tanium Inc. All Rights Reserved

3. Select whether to view policies by Organizational Unit (OU) or by Group:
    - OUs: Shows the OU hierarchy as a tree. Policies can be inherited from parent OUs.
    - Groups: Shows a flat list of groups that are defined in the Google Admin Console. Groups do not inherit policies from a hierarchy.

    > **Note:** Device Management does not create groups. To create or manage groups, go to the Google Workspace Admin Console (**Directory** > **Groups**). For more information, see Google Workspace Admin Help: Create a group.

4. Select the OU or group for which you want to view policies.
5. (Optional) Use the **Search policies** field to filter by policy name or description.

Set a Chrome policy

1. From the Main menu, go to **Shared Services** > **Device Management** > **Google** > **ChromeOS**.
2. If you have more than one Google Workspace configured, select the workspace from the **Workspace** list.
3. Select the OU or Group on which you want to set the policy.

    > **Note:** Device Management does not create groups. To create or manage groups, go to the Google Workspace Admin Console (**Directory** > **Groups**). For more information, see Google Workspace Admin Help: Create a group.

4. Locate the policy and click it to open the detail panel.
5. Configure the policy settings. The available options depend on the policy. For more information about a specific policy setting, see Google: Chrome Enterprise policy list.

    > **Note:** You can apply Managed Guest Session policies only to OUs, not to groups.

6. Click **Apply**.

Result

The policy state changes to **Locally Set** for the selected OU or group. Child OUs that do not have a locally set value for this policy inherit the new value.

©2026 Tanium Inc. All Rights Reserved

Reset a policy to inherited

About this task

Reset a locally set policy on an OU to inherit its value from the parent OU. This option applies only to OUs; groups do not inherit policies.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Google** > **ChromeOS**.
2. If you have more than one Google Workspace configured, select the workspace from the **Workspace** list.
3. Select the OU or group that has the locally set policy.
4. Locate the policy and click it to open the detail panel.
5. Click **Reset to Inherited**.

Result

Note: If the parent OU also has no locally set value for this policy, the policy reverts to the Google Default.

©2026 Tanium Inc. All Rights Reserved

(Google) Managing Android Enterprise policies

Use Android Enterprise management (EMM) to apply policies to Android devices and manage device enrollment in your organization. For more information about the Android Management API, see Google for Developers: Android Management API quickstart.

Note: Android Enterprise management does not require a Google Workspace. Android Enterprise registration is independent of Google Workspace configuration; complete registration before you manage Android policies or devices. For more information, see Set up Android Enterprise on page 83.

Note: Every Android Enterprise device is assigned to a system-owned **default** policy when it enrolls. The default policy reports device status only and applies no management restrictions. A device remains on the default policy until a targeting rule on another policy matches the device, and falls back to the default policy if no other policy matches. You cannot edit, target, or delete the default policy.

Set up Android Enterprise

About this task

Before you can manage Android Enterprise devices, register Device Management as the Enterprise Mobility Management (EMM) provider for your organization.

Important: Registering Device Management as an EMM provider replaces any existing EMM provider bound to your organization. If another EMM is currently registered, Android devices must re-enroll after the migration.

©2026 Tanium Inc. All Rights Reserved

Note:

- A Device Management deployment supports one Android Enterprise by default.

Before you begin

You must have a Google Workspace Super Admin account to complete registration.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Integrations** > **Android**.
2. Click **Begin Registration**. Device Management opens Google's signup page in a new tab.

   Note: The following steps occur the Google sign up page.

   a. Sign in with a Google Workspace Super Admin account.
   b. Review the consent screen and authorize Device Management as the EMM provider for your organization.
3. Return to the Device Management tab. Device Management detects the completed registration automatically and shows a confirmation message. This message confirms the completion of the setup process.

   Tip: If the Google signup tab closes before you finish, click **Reopen Google signup** to resume, or **Cancel** to stop registration.

View and manage Android Enterprise registration

View the registration details for your bound Android Enterprise, sync devices on demand, test the connection to Google, or unbind the enterprise. From the Main menu, go to **Shared Services** > **Device Management** > **Integrations** > **Android**.

The **Enterprise Registration** page shows an **Android EMM Registration** section with the following details:

- **Organization name** and **Organization ID**: The enterprise name and Google resource ID.
- **Enterprise type**: Managed Google domain or managed Google Play Accounts enterprise.

©2026 Tanium Inc. All Rights Reserved

Shows a dash if not yet available.

- **Google authentication**: Whether Google authentication is required to enroll devices. Applies only to managed Google Play Accounts enterprises, and this row does not show for managed Google domain enterprises or if the value is not yet available.
- **Registration date**, **Last device sync**, and **Synced devices**.
- **Status**: For example, Connected.

From this page, a Device Management Administrator can click **Sync devices** to trigger an immediate sync, or any user can click **Test connection** to verify connectivity to Google.



Note: If your Android Enterprise uses managed Google Play accounts, a notice on this page recommends upgrading to a managed Google domain for stronger security and simpler administration. Upgrading is a Google-side action performed outside Device Management; the notice is informational only.

Edit Android Enterprise settings

About this task

Update the branding and contact information that Google shows to users during Android Enterprise enrollment.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Integrations** > **Android**.
2. In the **Enterprise settings** section, update the **Display name**, **Brand color**, **Logo URL**, or **Contact email** fields as needed.
3. (Optional) Update the **Data protection officer** or **EU representative** name, email, and phone fields.
4. Click **Save**. To discard your changes instead, click **Discard changes**.

Unbind an Android Enterprise

About this task

©2026 Tanium Inc. All Rights Reserved

Important: Unbinding an Android Enterprise removes the enterprise from Device Management and stops managing its devices. This action cannot be undone.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Integrations** > **Android**.
2. Click **Unbind**.
3. In the **Unbind enterprise** confirmation dialog, click **Confirm**.

Create an Android policy

About this task

The Android policy editor is a single page made up of the sections described in the following steps. Click **View JSON** at any time to preview the full policy body that Device Management assembles from the form.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Android** > **Policies**.
2. If you have more than one Google Workspace configured, select the workspace from the **Workspace** list.
3. Click **Create Policy**.
4. In the **New policy** section, enter a **Name** and, optionally, a **Description**.
5. In the **Targeting** section, select the computer group whose devices are eligible for this policy from the **Limiting computer group** list.

   Note: When multiple policies could apply to the same device, Device Management assigns the device to the eligible policy with the highest priority. If no policy other than the default policy matches the device, the device remains on the default policy.
6. (Optional) Configure an **Additional filter** to further narrow which devices in the limiting computer group receive the policy.
   a. Click **Add Row** or **Add Group**.
   b. (Group filter only) Select whether to apply a Boolean **AND** or **OR** to all the filters in the group.

©2026 Tanium Inc. All Rights Reserved

c. Select an option for the first or only targeting filter:

Computer Group:

The dropdown lists all the computer management groups and filter groups that you have permissions to access. You can type a string in the typeaheads field to filter the list if it is long. Select a computer group.

Sensor:

i. Perform one of the following sub-steps to specify each sensor:

- Start typing the sensor name in the **Filter by Name** text field. The typeaheads dropdown list below the field shows a list of sensors that match your entry. Select a sensor and click Apply ✓.

  Substring matching: To match only part of a result string, select the **Substring** checkbox, enter the **Start** position (where `0` is the first position), and enter the number of characters (**Length**). The following example matches results from the **Installed Applications** sensor where the first two characters match the string `ts`. For a multi-column sensor, you cannot apply the **Substring** filter to a specific column, only across all the columns (**Row Filter**).

- Click **Browse All Sensors** to open the **Browse Sensors** dialog and select a sensor. The bottom of the dialog displays the **Sensor Description**.

ii. Specify the filter operator and value. For more information about filter operators, see Reference: Filter operators on page 143.

iii. (Optional) Click **Advanced Sensor Options** below the filter to configure additional settings. For more information, see Advanced sensor settings.

d. Click Apply ✓.

e. (Optional) Click **Add Row** or **Add Group** to specify additional targeting filters.

7. In the **Applications** section, click **Add apps from managed Google Play** to add apps to the policy. The managed Google Play interface opens; search for and select the app you want to add, then configure its install type, managed configuration, and, if applicable, allowed release tracks.

©2026 Tanium Inc. All Rights Reserved

> **Tip:** If you know an app's package name, you can add the app directly instead: enter the package name in the **Add by package name** field and click **Add**.

> **Note:** App metadata, including the release tracks available for an app, comes from the app's managed Google Play listing. Managed configuration values are set through the managed Google Play interface, not through the **Advanced settings** section.

8. In the **Password policies** section, turn on **Device password** or **Work profile password** and set the password requirements for that scope. A scope that is turned off, or that has no requirements set, is not configured, and devices fall back to the Android defaults.
9. In the **Settings** section, use the search field to match a setting by its friendly name, AMAPI key, or description, or expand a category (for example **Apps**, **Device**, **General**, **Network**, **Security**, or **Work Profile**) to browse and configure its settings. Categories and their settings are supplied by the Android Management API schema and can change as Google updates that schema.

   > **Note:** Turn off **Only show configured settings** to browse settings you have not yet configured.

10. (Optional) In the **Advanced settings** section, edit policy settings that the form does not surface, such as lists of objects, as raw JSON. These values are merged into the policy body alongside the settings you configure in the other sections.
11. Click **Create policy**. To discard your changes instead, click **Discard changes**.

Reorder Android policy priority

About this task

Reorder the priority of multiple Android policies at once by dragging them into the order you want, rather than editing each policy individually.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Android** > **Policies**.
2. Click **Prioritize policies**.

©2026 Tanium Inc. All Rights Reserved

> **Note:** **Prioritize policies** is available only when at least two policies in the group have targeting configured.

3. Drag policies into the order you want. The policy at the top has the highest priority.
4. Click **Save priorities**.

Edit an Android policy

About this task

For descriptions of the sections and fields in the policy editor, see Create an Android policy on page 86.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Android** > **Policies**.
2. If you have more than one Google Workspace configured, select the workspace from the **Workspace** list.
3. Click the policy name.
4. Update the policy settings and click **Save policy**. To discard your changes instead, click **Discard changes**.

Duplicate an Android policy

About this task

Duplicate an existing Android policy to use as the starting point for a new policy.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Android** > **Policies**.
2. In the row for the policy you want to duplicate, click Duplicate .
3. Update the policy name, settings, and targeting as needed, and then click **Save**.

Delete an Android policy

About this task

©2026 Tanium Inc. All Rights Reserved

Important: Deleting a policy removes it from all devices it is applied to. This action cannot be undone.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Android** > **Policies**.
2. Click the policy name.
3. Click Delete .
4. Click **Confirm**.

Create an enrollment token

About this task

Generate an enrollment token to enroll Android Enterprise devices. Every token enrolls devices onto the system default Android policy; use targeting to move a device onto a different policy after it enrolls. For more information, see Create an Android policy on page 86.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Android** > **Enrollments**.
2. Click **Create enrollment token**.
3. On the **Enrollment token** step, in the **Name & description** section, enter a **Name** and, optionally, a **Description**. These fields are for your reference only and are not shown to the end user.
4. In the **Enrollment type** section, select the ownership and management mode for devices that enroll with this token:
    - **Fully managed** (Android 6.0 or later): The entire device is managed with no personal profile. Use for rugged handhelds, field devices, and standard corporate phones.
    - **Dedicated device (kiosk)** (Android 6.0 or later): Single- or limited-use devices with no user account, such as point-of-sale terminals, checkout tablets, digital signage, and warehouse scanners.
    - **Work profile (company-owned)** (Android 11.0 or later): A corporate-owned device with a managed work profile alongside a separate personal space. Best for executive or hybrid-use devices.
    - **Work profile (BYOD)** (Android 7.0 or later): An employee-owned device gets an isolated managed work profile; personal apps and data stay untouched.

©2026 Tanium Inc. All Rights Reserved

5. In the **Validity & reuse** section, enter a value and unit (minutes, hours, days, or years) in **Valid for** to set how long the token can be used to enroll devices. The default is 30 days.
6. (Optional) Turn on **One-time use** to automatically revoke the token after its first successful enrollment.
7. Click **Continue**.
8. On the **Provisioning options** step, configure any of the following optional settings. These settings are encoded directly into the enrollment token and its QR code.
    - **Setup experience**: **Skip education screens**, **Leave all system apps enabled**, **Keep screen on during provisioning**, and **Skip device encryption**.
    - **Regional settings**: **Locale** and **Time zone** to set on the device at first boot.
    - **Connectivity for provisioning**: Turn on **Pre-configure Wi-Fi** to embed Wi-Fi credentials in the QR code so the device connects automatically at first boot, and, optionally, **Allow mobile data fallback** to bring up the SIM or eSIM if the configured Wi-Fi is unreachable.
    - **Additional data**: Enter up to 1,024 characters of custom metadata to forward to enrolling devices, such as a team or site tag.
9. Click **Create token**.
10. On the **Enroll** step, share the QR code, token value, or enrollment link with the user or IT team responsible for device setup, and then click **Done**.

    Note: The token value and QR code are retrieved from Google each time you view them and are not stored by Device Management.

Enroll a device with a token

About this task

After you create an enrollment token, use it to enroll a factory-reset or out-of-box Android device.

1. Factory-reset the device. New, out-of-box devices are already ready to enroll. A previously used device must be factory reset to return to the out-of-box setup wizard, which Android device-owner provisioning requires.
2. On the Welcome screen for the device, tap the screen six times in the same spot to open the QR scanner. On Android 7 and later, you can instead type `afw#setup` on the Google sign-in

©2026 Tanium Inc. All Rights Reserved

screen.

3. Point the camera at the enrollment token QR code. The device installs Android Device Policy, downloads its policy, and finishes setup in a managed state.

Result

Policy enforcement begins immediately after enrollment. The device appears in the device inventory within about a minute.

Link a zero-touch account for Android devices

About this task

Zero-touch enrollment lets you enroll company-owned Android devices without scanning a QR code or manually entering an enrollment token. A device that you purchase from a zero-touch reseller partner automatically downloads your configuration and enrolls in Android Enterprise management the first time the device starts.

> **Note:** Zero-touch enrollment requires an Android Enterprise that is already registered and a Google zero-touch customer account, which your device reseller sets up on your behalf.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Android** > **Enrollments**.
2. Click the **Zero-Touch Portal** tab.
3. In the **Link your zero-touch account to your EMM provider** section, click **Next**.
4. Sign in with the Google account that you gave your reseller when your zero-touch account was created.

   > **Important:** Use the Google account associated with your organization, not a personal Gmail account. This account is not necessarily the same account that you use to sign in to Google Workspace or to register your Android Enterprise.

5. Select the zero-touch account that you want to link to Device Management and click **Link**.

Result

©2026 Tanium Inc. All Rights Reserved

After you link your account, you can build and manage zero-touch device configurations directly in the embedded portal. The details panel for a company-owned enrollment token includes a zero-touch payload that you can copy or download and use when you build a device configuration in the portal. Devices provisioned through that configuration enroll using the settings for that token. To create or manage tokens, see Create an enrollment token on page 90.

Tip: If the embedded portal does not load, click **Reload portal**, or manage zero-touch enrollment directly at partner.android.com/zerotouch.

For more information, see Google Android Enterprise Help: Zero-touch enrollment for IT admins.

Clone an enrollment token

About this task

Clone an existing enrollment token to use its settings as the starting point for a new token.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Android** > **Enrollments**.
2. In the row for the token you want to clone, click Clone .
3. On the **Enrollment token** step, update the name, enrollment type, or validity settings as needed, and then click **Continue**.
4. On the **Provisioning options** step, update the provisioning options as needed, and then click **Create token**.

Delete an enrollment token

About this task

Delete an enrollment token to prevent new devices from enrolling with that token. Devices already enrolled are not affected. A deleted token remains visible in a revoked state until the enterprise is unbound.

1. From the Main menu, go to **Shared Services** > **Device Management** > **Android** > **Enrollments**.

©2026 Tanium Inc. All Rights Reserved

2. In the row for the token you want to remove, click Delete .
3. Click **Confirm**.

©2026 Tanium Inc. All Rights Reserved

Working with devices and device data

Use Tanium Reporting to view device information and take actions on devices.

Overview

By default, the **Device Management Overview** dashboard shows on the **Device Management Overview** page when the configuration is complete. Use the **Computer Group** and **Timeframe** filters to scope the dashboard. The **Device Registrations** section shows the following panels:

Apple Devices by Type

Shows macOS and iOS devices over time, broken down by device type.

Google Devices by Type

Shows Google-managed devices over time, broken down by device type.

iOS Devices by Version

Shows the current iOS devices by version.

Mac Devices by Version

Shows the current macOS devices by version.

ChromeOS Devices by Version

Shows the current ChromeOS devices by version.

Android Devices by Version

Shows the current Android devices by version.

Apple Devices Checked in by Day

Shows Apple device check-ins over time.

©2026 Tanium Inc. All Rights Reserved

Google Devices Checked in by Day

Shows Google device check-ins over time.

Apple Inactive Devices

Shows Apple devices that have not checked in for 30 days.

Google Inactive Devices

Shows Google devices that have not checked in for 30 days.

Software Update Install State

Shows the current Apple devices by software update install state.

Deadline Status

Shows the current Apple devices by software update deadline status.

Figure 16. Metrics on the Device Management **Overview** page

©2026 Tanium Inc. All Rights Reserved



View the details for a device

About this task

©2026 Tanium Inc. All Rights Reserved

Open the Endpoint Details page for the device to view information about the device. For more information, see Tanium Reporting User Guide: Working with a single endpoint.

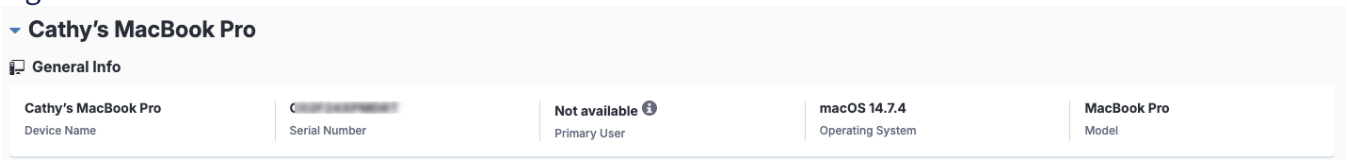
Note:

- The Endpoint Details page for devices enrolled with Device Management cannot be customized.
- To view device details, you must have the **Device Management Single Endpoint** permission.

General Info

The General Info banner shows high-level details about the device, such as the device name, serial number, primary user, operating system, and device type.

Figure 17. General Info



Endpoint Overview

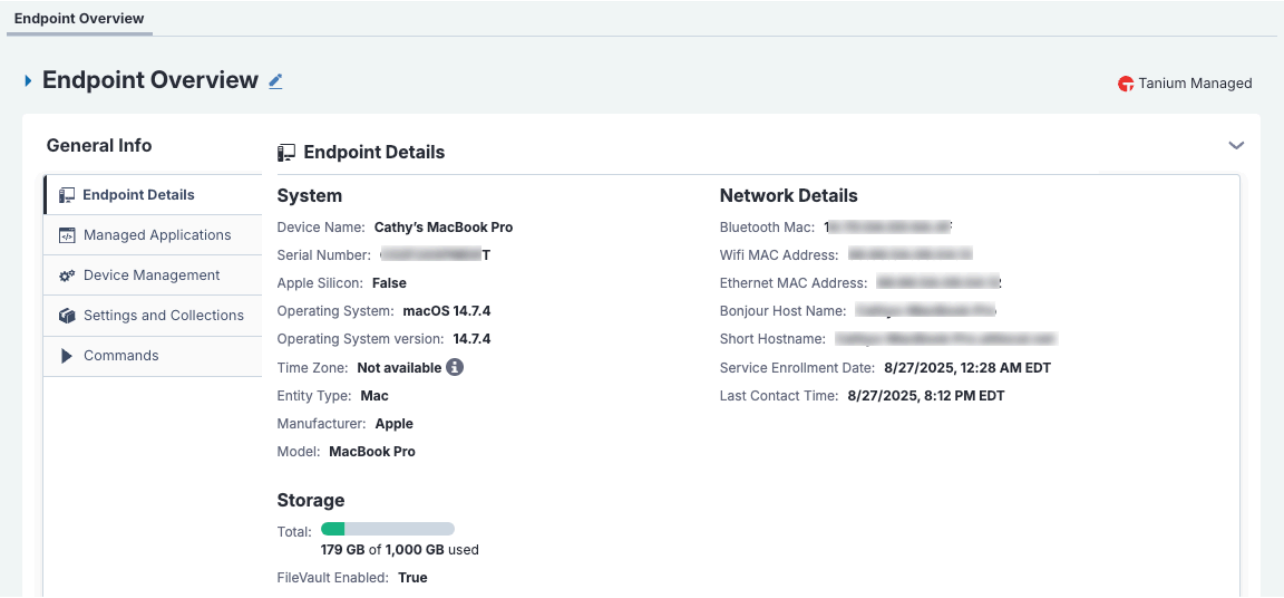
The **Endpoint Overview** section shows detailed information about the device:

Endpoint Details

Shows detailed information about the device.

Figure 18. Endpoint Details

©2026 Tanium Inc. All Rights Reserved



For Google-managed devices, the **Endpoint Details** tab also includes the following platform-specific sections:

- ChromeOS devices show a **Workspace Details** section with the device ID, organizational unit, groups, and enrollment status. This section does not show for Android Enterprise devices.
- Android Enterprise devices show a **Management & Policy** section (management mode, ownership, applied policy, intended policy, applied policy version, and last policy sync time) and a **Security & Compliance** section (device posture, policy compliance, any non-compliance details, and any security risks).

(Apple) Managed Applications

For Apple devices, shows the applications installed on the device.

(Android) Installed Applications

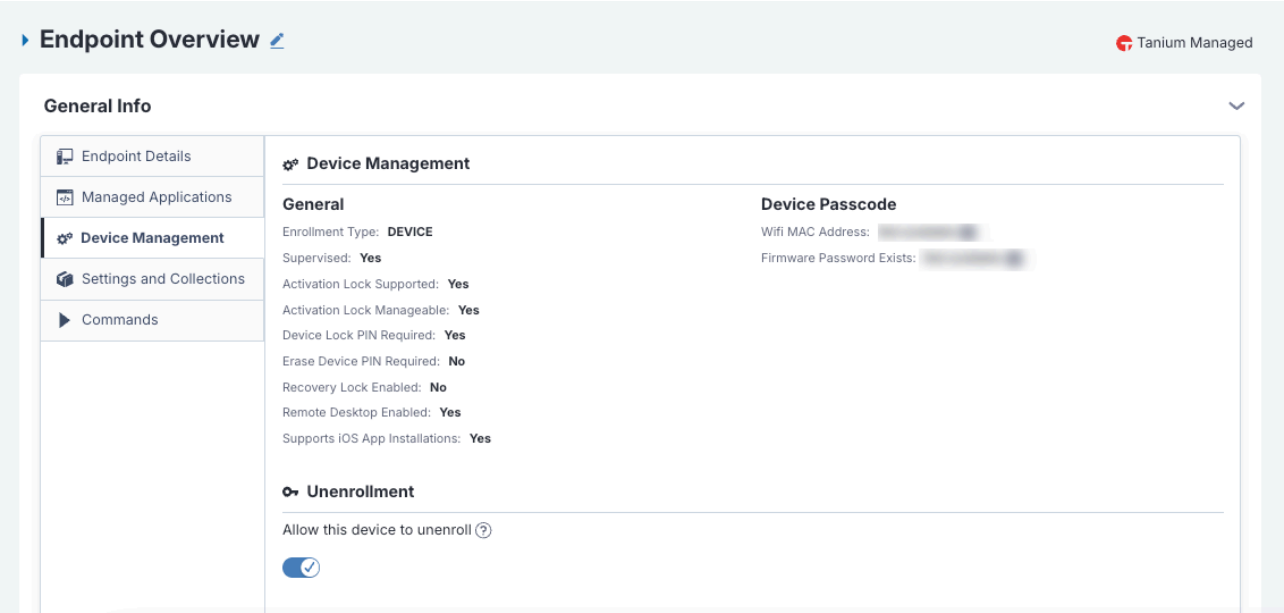
For Android Enterprise devices, shows the full inventory of installed applications. This is a separate tab from **Managed Applications**, which does not show for Android Enterprise devices.

(Apple) Device Management

For Apple devices, shows device management settings for the device, such as enrollment type.

Figure 19. Device Management tab

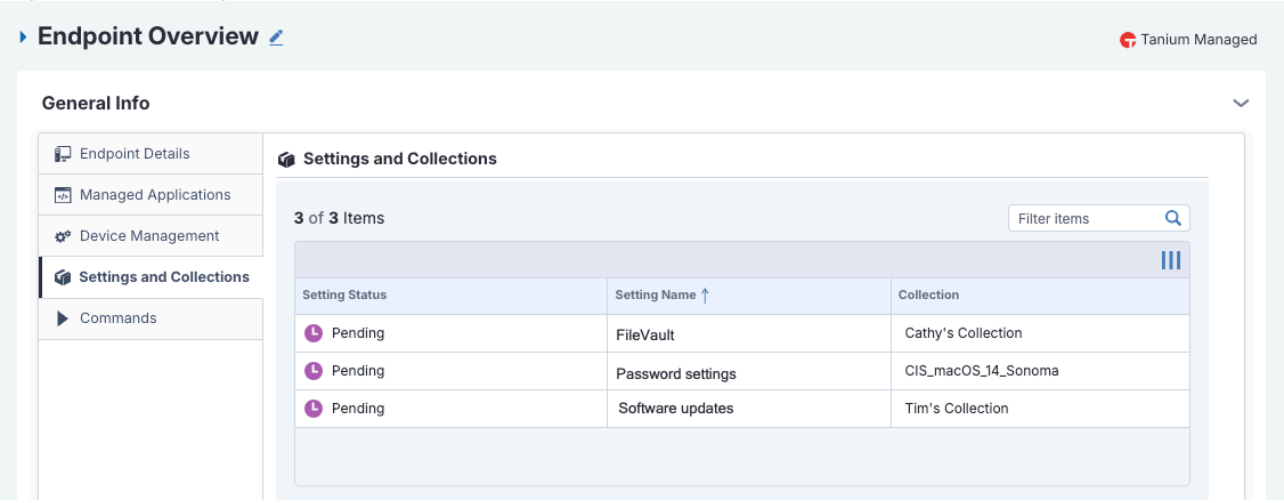
©2026 Tanium Inc. All Rights Reserved



(Apple) Settings and Collections

For Apple devices, shows the status of collections targeted to the device. For more information about collections, see (Apple) Managing collections on page 68.

Figure 20. Settings and Collections tab



Note: Web Clips show on the **Settings and Collections** tab on the Endpoint Details page. To access details about a Web Clip from Device Management, from the Main menu, go to **Shared Services** > **Device Management** > **Applications**. For more information, see Review web clips and applications on page 65.

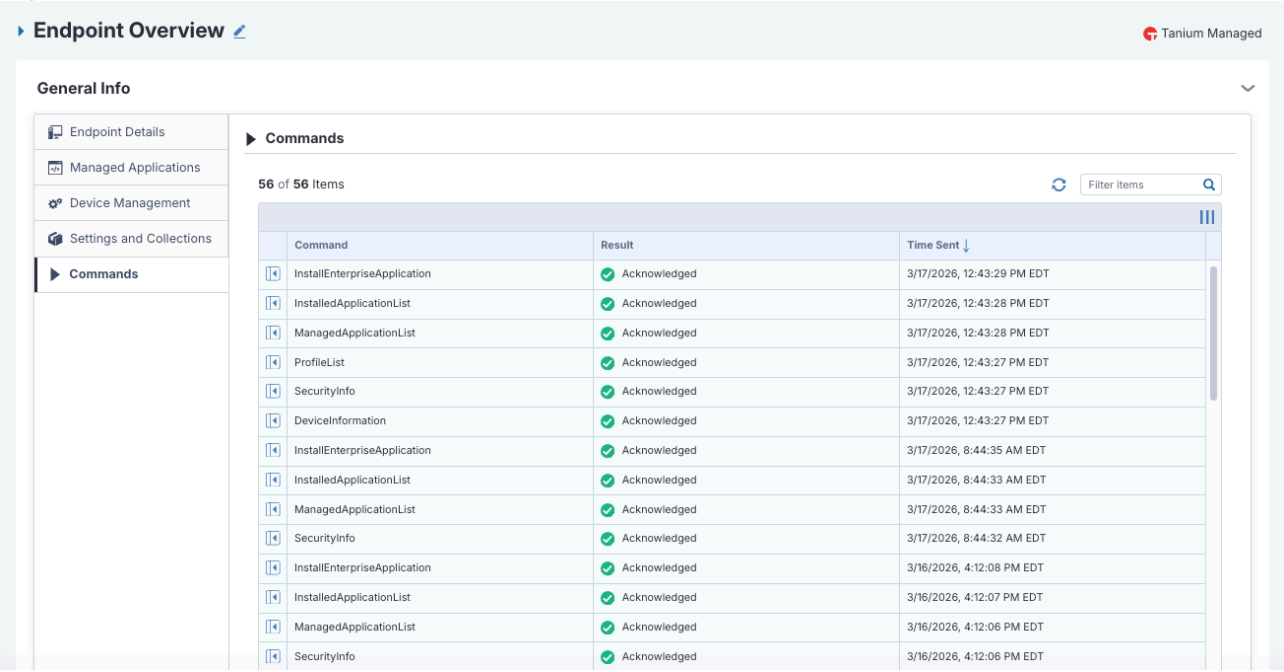
©2026 Tanium Inc. All Rights Reserved

(Apple) Commands

For Apple devices, shows details about commands that were recently run on the device. Click View command details to see the command and resulting response from the device.

Tip: The details on this tab can be helpful when troubleshooting issues with a specific device. If a device is experiencing issues, check to see whether the device is currently checking in with the Tanium Server and what commands recently ran on the device.

Figure 21. Commands tab



Deploy actions on a device

About this task

Deploy remote actions on a single device through the Endpoint Details page in Tanium Reporting. Available actions depend on the device platform. To perform these actions, you must have the **Device Management Push Command** permission and management rights on the target device, including management rights granted by an active Persona.

1. Open the Endpoint Details page for the device that requires an action. For more information, see Tanium Reporting User Guide: Working with a single endpoint.

©2026 Tanium Inc. All Rights Reserved

2. Click **Deploy Action**, select the action you want to perform, and specify the parameters as needed.
3. Click **Deploy Action**.

Result

The following tables describe available actions by platform.

Apple device actions

Action	Operating System	Description
Disable Activation Lock	iOS, iPadOS, macOS	Remove the Activation Lock, which associates a device with an Apple ID and password.
Lock Device	iOS, iPadOS, macOS	Lock a device, show a custom message, and require the configured PIN to access the device. Enter a **Message to display on lock screen**, **Phone number to display on lock screen**, and **Recovery PIN**. For more information, see Apple Platform Deployment Documentation: Lock and locate Apple devices.
Erase Device	iOS, iPadOS, macOS	Erase all content from the device. You can specify **Disallow proximity setup**, **Recovery PIN**, **Obliteration behavior**, and **Preserve cellular data plan for eSIM device**.
Refresh Device Data	iOS, iPadOS, macOS	Device data is typically refreshed every 24 hours. Use this action to refresh the data for the device outside of the automatic refresh interval.
Restart	iOS, iPadOS, macOS	Restart the device. You can specify **Notify user** and **Rebuild kernel cache**.
Shut Down Device	iOS, iPadOS, macOS	Shut down the device.
Unenroll Device	iOS, iPadOS, macOS	Unenroll the device from Device Management.

©2026 Tanium Inc. All Rights Reserved

Note: When a remote action request is deployed to an endpoint managed by Device Management, the Tanium Server sends the request to the Tanium Cloud MDM Service, which then communicates with enrolled endpoints and attempts to apply the remote action to the endpoint using the Apple Push Notification Service (APNs). This workflow might take several minutes.

Note: Google device actions are available only when the device status is Online or Connected.

Google device actions

Action	Operating System	Description
Deprovision Device	ChromeOS	Permanently removes an endpoint from management when the endpoint is being retired, replaced, resold, donated, or returned. Enter a reason for deprovisioning the endpoint.
Disable Device	ChromeOS	Prevents a lost or stolen endpoint from being used until the endpoint is recovered and re-enabled.
Powerwash Device	ChromeOS	Performs a factory reset of the device, removing all local user data and accounts. The device remains enrolled in management after the reset.
Pre-Provisioned Disable Device	ChromeOS	Disables a pre-provisioned device before it has been assigned to a user, preventing the device from being activated.
Pre-Provisioned Reenable Device	ChromeOS	Re-enables a pre-provisioned device that was previously disabled, allowing it to be activated and assigned to a user.
Reboot Device	ChromeOS	Remotely restarts the device.
Reenable Device	ChromeOS	Restores normal functionality to an endpoint that was previously disabled.
Wipe Users	ChromeOS	Removes all user accounts and associated data from the device without wiping the OS or removing device enrollment.

©2026 Tanium Inc. All Rights Reserved

Action	Operating System	Description
All Actions	ChromeOS	Go to the **Action Deployment** page to select other packages. In **Deployment Package**, enter `ChromeOS` to find packages available for ChromeOS devices. For more information, see Tanium Console User Guide: Action deployment overview.

Android Enterprise device actions

Action	Description
Lock Device	Locks the device, requiring the user to re-authenticate. Available when the device status is Active.
Reboot Device	Reboots the device. Requires a fully managed device running Android 7.0 or later. Available when the device status is Active.
Reset Password	Resets the password on the device. Available when the device status is Active.
Disable Device	Disables the device, blocking access until the device is re-enabled. Available when the device status is Active.
Reenable Device	Re-enables a previously disabled device, restoring access. Available when the device status is Disabled.
Start Lost Mode	Puts the device into lost mode, locking the device and displaying a custom message. Enter at least one of **Lost Message**, **Phone Number**, **Email Address**, or **Street Address**. Available when the device status is Active.
Stop Lost Mode	Takes the device out of lost mode. Available when the device status is Lost.
Wipe Device	Wipes the device: factory resets a company-owned device, or deletes the work profile on a personally owned device. This action cannot be undone. Requires permissions for the **Device Management - High Impact** content set. Available when the device status is Active, Lost, or Disabled.
Relinquish Ownership	Relinquishes ownership of a company-owned device with a work profile, converting the device to personally owned. Removes the work profile and all policies; re-enrollment is not expected. This action cannot be undone. Requires permissions for the **Device Management - High Impact** content set. Available when the device status is Active.

©2026 Tanium Inc. All Rights Reserved

Note:

- No Android Enterprise device actions are available when the device status is Deleted, Provisioning, Preparing for Migration, or Deactivated by Device Finance.

Issue questions to target devices enrolled with Device Management

You can use the **Provider Type**, **Provider Name**, and **Entity Type** sensors to return results from certain types of managed endpoints, such as endpoints managed using Tanium Client or endpoints managed using Device Management.

Entity providers and related sensor values

Entity Provider	Provider Type value	Provider Name value	Entity Type value
Tanium Client	Tanium Client	Tanium	Computer
Tanium Endpoint Management for Mobile	Device Management	• Device Management Computer (for macOS) • Device Management Mobile Device (for iOS and iPadOS)	• Computer (for macOS) • Mobile Device (for iOS and iPadOS)

The following question returns all mobile devices enrolled with Device Management:

```
Get Computer Name and Provider Type and Entity Type from all entities with Provider Name
equals Device Management Mobile Device
```

The following question returns all computers or workstations enrolled with Device Management:

```
Get Computer Name and Provider Type and Entity Type from all entities with Provider Name
equals Device Management Computer
```

The following question returns all endpoints enrolled with Device Management:

```
Get Computer Name and Provider Name and Provider Type and Entity Type from all entities with
Provider Type equals Device Management
```

The following questions returns all endpoints managed using the Tanium Client:

©2026 Tanium Inc. All Rights Reserved

```
Get Computer Name and Provider Name and Provider Type and Entity Type from all entities with
Provider Type equals Tanium Client
```

```
Get Computer Name and Provider Name and Provider Type and Entity Type from all entities with
Provider Name equals Tanium
```

Include devices enrolled with Device Management in a report

1. Perform one of the following steps based on whether you plan to edit an existing report or create a new view of device data that you might or might not save as a report.

    - Existing report: Open the report and click **Edit Data**.
    - New view or report: From the Main menu, go to **Data** > **Explore Data**.

    Tip: You can also access the **Explore Data** page from the following locations:

    - An existing report: Click **New Report** or, in a non-editable report, click **Explore Data**.
    - The **Data** > **Reports** page: Click **Create Report**.

2. Select a **Data Source** to limit the results to endpoints managed using Tanium Client or an entity provider. Alternatively, select **All Entities** to return results from all endpoints.

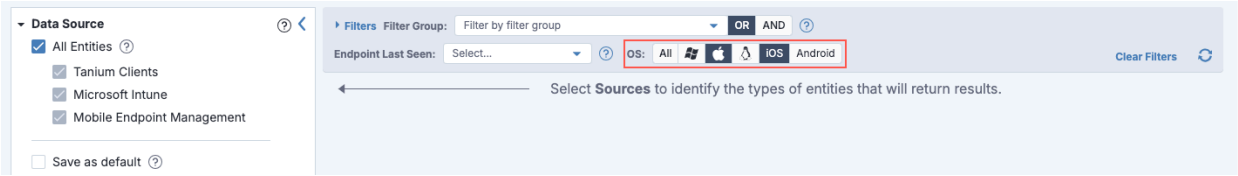
    Note: Select **Save as default** to save your current **Data Source** selection for future reports.

3. Configure the report. For more information, see Tanium Reporting User Guide: Explore data and create reports.

    Note: If you select **Device Management** or **All Endpoints** as the **Data Source**, you can filter results by operating system: macOS, iOS (which includes iPadOS), ChromeOS, or Android.

    Figure 22. Operating system filter

©2026 Tanium Inc. All Rights Reserved



Use Tanium Connect to export data about devices enrolled with Device Management

If the connection source supports Device Management device data, such as the **Tanium Reporting (Source Data)** source, you can export this data using Tanium™ Connect. For more information, see Tanium Connect User Guide: Overview.

©2026 Tanium Inc. All Rights Reserved

Maintaining Device Management

Perform annual maintenance tasks to ensure that Device Management successfully performs scheduled activities on all the targeted endpoints.

Perform annual maintenance

Renew an Apple MDM Push Certificate

About this task

Apple Push Certificates, also referred to as Apple Push Notification Service (APNs) certificates, are valid for one year. You must renew the certificate each year using the same Apple ID that you used to create the certificate. If you do not renew your certificate and instead request a new certificate, Device Management loses the ability to communicate with enrolled devices, and all devices must be re-enrolled.

Important: The Apple Push Certificates portal provides options to renew or to request a new certificate. You must select the option to renew your existing certificate. Otherwise, all users are required to re-enroll their devices.

Before you begin

Make sure you have the credentials for the same Apple ID that you used when you obtained the original Apple Push Certificate.

1. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings.
2. On the **Push Certificate** tab, in the **Certificate Signing Request** section, click **Download** to download the Tanium-signed certificate signing request, which is required when you request an Apple Push Certificate.
3. Click **Create Apple MDM Push Certificate** to go to the Apple Push Certificates Portal and request your Apple Push Certificate. Sign in to the Apple Push Certificates Portal with the same Apple ID you used to obtain the original certificate.

©2026 Tanium Inc. All Rights Reserved

> **Important:** Remember to select the option to renew your certificate.

4. In the **Apple ID** field, enter the Apple ID that you used to request the Apple Push Certificate.
5. Return to the Device Management settings and upload the new Apple Push Certificate file that you receive from Apple in the **Apple MDM Push Certificate Upload section**. Click **Apply**.

Update server tokens

About this task

Server tokens from your Apple enrollment system are valid for one year. Before a server token expires, you must download a new server token file from your Apple enrollment system and upload the token file to Device Management. For the best results, plan to update server tokens 1-2 weeks prior to the expiration date.

> **Important:** A server token can also become invalid before its expiration date. Apple Business Manager and Apple School Manager invalidate the token if the password changes for the Managed Apple Account that downloaded it, or if the MDM server registration is reassigned by downloading the token again for a different MDM system. This is because an Apple Business Manager or Apple School Manager MDM server registration can be linked to only one MDM system at a time. If either of these happens, devices fail enrollment even though the token has not reached its expiration date, and Device Management does not currently detect or flag the invalidation. If devices unexpectedly fail enrollment despite an unexpired token, download a new server token and upload it to Device Management, then sync devices.

1. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click **Automated Enrollment**.

   > **Tip:** You can see the expiration date for the current token on this tab.

2. On the **Automated Enrollment** tab, in the **Download the Public Key Certificate** section, click **Download** to download the Tanium-signed public key certificate, which is required when you configure an Apple enrollment system.
3. Go to the Apple website and upload the Tanium-signed public key certificate to associate it with your organization. Then download the service token for this configuration. For more

©2026 Tanium Inc. All Rights Reserved

information, see Apple Business Manager User Guide: Link to an external device management service in Apple Business Manager or Apple School Manager User Guide: Link to an external device management service in Apple School Manager.

4. Return to the Automated Enrollment tab of the Device Management settings. In the **Upload the Token file from Apple Business Manager** section, either browse to or drag and drop the P7M file from Apple Business Manager.
5. Click **Next**.

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Device Management

If Device Management is not performing as expected, you might need to troubleshoot issues or change settings.

Collect logs

About this task

The information is saved as a ZIP file that you can download with your browser. The ZIP file is also known as a support bundle.

1. From the Main menu, go to **Shared Services** > **Device Management**.
2. Click Help ? and then click the **Troubleshooting** tab if needed.
3. Click **Collect**. A productname-support.[timestamp].zip file downloads to the local download directory.
4. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 116.

Result

Tanium Endpoint Management for Mobile maintains logging information in the Device Management.log file in the <*Module Server*>services\Device Management directory.

Observed issues with specific settings

When configuring settings, note the following issues that were observed during testing. These behaviors are inherent to iOS and macOS and not caused by Device Management.

Password and Screen Unlock settings

©2026 Tanium Inc. All Rights Reserved

iOS devices must be unlocked for password settings to take effect

If you target a password setting (either through a curated or custom setting) to an iOS device that already has a passcode set, you might see a Failed status until the user unlocks the device, at which point the status should change to Installed. If you hover over the failed status on the **Devices** tab for the collection, the message shown is similar to:

```
[{"Code":"Error.ConfigurationCannotBeApplied","Description":"Configuration cannot be
applied","Details":{"Error":"Failed to install profile: Profile Installation
Failed"}},{"Code":"LegacyProfiles.ProfileInstallFailed","Description":"Failed to install
profile: Profile Installation Failed","Details":null}]
```

FileVault settings

Modifying certain FileVault settings for devices that already have a FileVault profile installed might cause errors

If you push a FileVault setting down to a device (whether the device is encrypted or not) and then attempt to make changes to certain settings, you might receive an `unknown error`. If you hover over the failed status on the **Devices** tab for the collection, the message shown is similar to:

```
[{"Code":"Error.ConfigurationCannotBeApplied","Description":"Configuration cannot be
applied","Details":{"Error":"Failed to install profile: The 'FileVault Settings' payload
could not be installed. an unknown error
occurred"}},{"Code":"LegacyProfiles.ProfileInstallFailed","Description":"Failed to install
profile: The 'FileVault Settings' payload could not be installed. an unknown error
occurred","Details":null}]
```

In this scenario, the FileVault settings profile is removed from the device, but the new settings are not pushed out to the device and the operation is not attempted again. One setting that is known to cause this behavior is the **Defer Enabling FileVault** option. You can make a trivial change to the settings or collection and attempt to push the settings out again, but the application might not succeed.

Best Practice: As a best practice, if you need to change the FileVault settings for devices where a FileVault profile exists, first remove the settings profile and decrypt the device. Then target the device with a new setting / collection, especially if you are changing the **Defer Enabling FileVault** option.

©2026 Tanium Inc. All Rights Reserved

User is not prompted to enable FileVault when Do not ask users to enable FileVault at logout is set to No

When a FileVault setting is applied on a device with the **Do Not Ask Users to Enable FileVault at Logout** option set to **No**, macOS sets an enablement deferral that prompts the user to enable FileVault during login or a restart. If this deferral is not set initially due to an issue or is removed before FileVault is enabled, the user might not be prompted to enable FileVault, and the system will not attempt to reset the deferral. If modifying the setting does not reset the deferral, try the following steps:

- Remove the existing FileVault setting from the collection and either re-add it or create a new one.
- Add or remove a different, unrelated setting from the same collection.

Wi-Fi Settings

Other settings fail to apply when included in a collection that defines a Wi-Fi network set to auto join

When you include a Wi-Fi setting that defines a Wi-Fi network that is previously unknown to the device and is set to **Auto Join** in a collection that contains other settings, other settings might intermittently fail to install with this error: `Failed to install profile: The Internet connection appears to be offline`.

With Auto Join enabled, the device might immediately attempt to connect to the new network, causing other settings that require network access to fail to apply. The settings should apply the next time the device syncs with the Tanium Cloud MDM Service.

Observed issues setting up Android Enterprise

When you register Device Management as the Android Enterprise EMM provider for your organization, you might encounter the following issues.

Setup was cancelled in the Google Admin Console

If you cancel the consent flow in the Google Admin Console before authorization completes, Device Management shows a message that the setup was cancelled. You can restart Android Enterprise

©2026 Tanium Inc. All Rights Reserved

registration at any time. For more information, see Set up Android Enterprise on page 83.

Registration fails because another provider is already connected

Your organization can be connected to only one device management provider for Android Enterprise. If another provider is already connected, registering Device Management fails. Use the Google Admin Console to remove the existing provider before retrying registration. After you change providers, Android devices that were previously enrolled must re-enroll with Device Management.

Registration fails because the Google account does not have sufficient privileges

You must sign in with a Google Workspace Super Admin account to authorize Device Management for Android Enterprise. If you sign in with an account that does not have Super Admin privileges, the registration fails. Sign in with a Super Admin account and try again.

Observed issues with Android Enterprise device actions and policies

An Android device action is unavailable

Available device actions depend on the device status. For example, **Reenable** is available only when the device status is Disabled, and **Stop Lost Mode** is available only when the device status is Lost. If you do not see an action that you expect, check the device status. Additionally, **Wipe** and **Relinquish Ownership** require permissions to the **Device Management - High Impact** content set; without that permission, these two actions do not show for the device. For more information, see Working with devices and device data on page 104.

Start Lost Mode is unavailable to deploy

The **Deploy Action** button for **Start Lost Mode** stays disabled until you enter a value in at least one of **Lost Message**, **Phone Number**, **Email Address**, or **Street Address**.

Observed issues with Web Clips and Enterprise Applications

When configuring Web Clips and Enterprise Applications, note the following issues that were observed during testing. These behaviors are inherent to iOS and macOS and not caused by Device

©2026 Tanium Inc. All Rights Reserved

Management.

iOS devices must be unlocked for Web Clips to Install

If you target a Web Clip or Enterprise Application to an iOS device that has a passcode set, you might see a Failed status until the user unlocks the device, at which point the status should change to Installed. If you hover over the failed status on the **Devices** tab for the collection, the message shown is similar to:

```
[{"Code":"Error.ConfigurationCannotBeApplied","Description":"Configuration cannot be
applied","Details":{"Error":"Failed to install profile: Profile Installation
Failed"}},{"Code":"LegacyProfiles.ProfileInstallFailed","Description":"Failed to install
profile: Profile Installation Failed","Details":null}]
```

Issues with Apps & Books

When you configure or use Apps & Books, you might encounter the following issues.

Content token expiring or expired

Device Management shows a warning banner 30 days and 7 days before an organizational unit's content token expires. After a content token expires, license assignment is blocked for that organizational unit until you renew the content token in Apple Business Manager or Apple School Manager.

Important: A content token can also become invalid before its expiration date. Apple Business Manager and Apple School Manager invalidate the token if the password changes for the Managed Apple Account that downloaded it. If this happens, license assignment is blocked even though the token has not reached its expiration date, and Device Management does not currently detect or flag the invalidation. If license assignment unexpectedly stops working despite an unexpired content token, download a new content token and upload it to the organizational unit.

Assignment shows a Pending license status

If the number of devices that you target for an App Store application exceeds the available license count, Device Management assigns the license to devices up to the available count. The remaining devices show a status of **Pending license**. To resolve this, reduce the number of targeted devices or purchase additional licenses in Apple Business Manager or Apple School Manager, and then sync the

©2026 Tanium Inc. All Rights Reserved

organizational unit.

Assignment shows a Not enrolled status

A device must be enrolled with Device Management to receive a license assignment for an App Store application. If a targeted device is not enrolled, the assignment record shows a status of **Not enrolled** and no install command is sent to the device.

Apple Apps & Books service unavailable

If the Apple Apps & Books service is unavailable, license sync is deferred and Device Management shows the last successful sync time for the organizational unit. Sync resumes automatically after the service becomes available again.

Assignment shows a Failed status

If a device rejects the MDM install command for an App Store application, the assignment record shows a status of **Failed** along with the reason that the device returned.

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about submitting a support case, see Case Submission Form.

©2026 Tanium Inc. All Rights Reserved

Reference: (Apple) Configuring Identity Providers to use with Device Management

Device Management supports integration with these Identity Providers (IdPs):

- OpenID Connect (OIDC) compliant identity provider:
    - auth0
    - Entra ID
    - Okta
    - OneLogin

> **Note:**
>
> The identity provider administrator must have access to manage user roles, user permissions, user mappings, and user attributes; configure applications; and assign users to applications. Refer to your identity provider documentation to understand the required roles and permissions.
>
> For example, the Okta App Admin role provides the needed permissions: Manage Profile Editor, Manage Profile Mappings, View applications or application instances, Add and configure applications, Assign user access to applications, and Create and modify an OIDC App.
>
> The IdP must have the application configured as a Single Page Application (SPA) using Proof Key for Code Exchange (PKCE).

Before you begin

©2026 Tanium Inc. All Rights Reserved

Before you configure an IdP, you must configure an Apple Push Certificate to use with Device Management. For more information, see (Apple) Configure an Apple Push Certificate to use with Device Management on page 37. After you configure the push certificate, copy the Redirect URI for your Device Management instance:

From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click **IDP Configuration**. Copy the **Redirect URI**.

Note: This section describes one way to configure these Identity Providers. You might need to modify these steps and the suggested selections and values depending on your environment. Ensure that you test this configuration in a lab or test environment before you use it in a production environment. Consult the documentation for the IdP for detailed steps.

OIDC requirements

The IdP application must meet the following requirements to integrate with Device Management:

- **OAuth flow:** Authorization Code with Proof Key for Code Exchange (PKCE). Configure the application as a public client (Single Page Application) with no client secret.
- **Scopes:** Grant the `openid`, `email`, and `profile` scopes to the application.
- **ID token claims:** The ID token must include the `email` claim, which Device Management uses as the user identity on the device. The `name` claim is optional. If the ID token does not include the `email` claim, Device Management retrieves the email from the IdP UserInfo endpoint using the access token.
- **Audience:** The `aud` claim in the token must contain either the Issuer URL or the Client ID that is configured in Device Management.
- **Issuer URL and discovery:** Device Management retrieves the IdP configuration from {IssuerURL}/.well-known/openid-configuration and verifies that the `issuer` field in the response matches the Issuer URL configured in Device Management exactly. The trailing slash, scheme, and path must all match. A mismatch is the most common cause of the `error getting oauth2 endpoint` error during enrollment.
- **Cross-origin resource sharing (CORS):** The enrollment flow runs in the browser, so the IdP

©2026 Tanium Inc. All Rights Reserved

token endpoint must allow cross-origin requests from the Device Management Redirect URI host. For most IdPs, the token endpoint is configured for CORS automatically when you select the Single Page Application application type. If the IdP does not configure CORS automatically, configure the token endpoint to return the following headers:

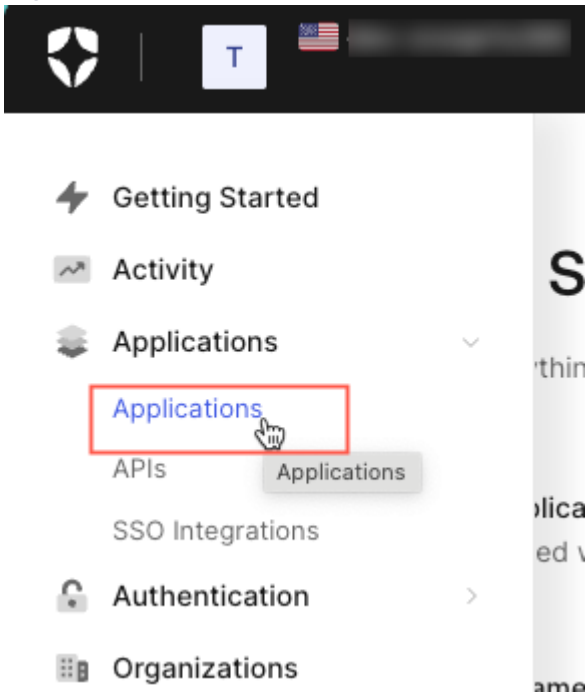
- `Access-Control-Allow-Origin: <Redirect URI host>`
- `Access-Control-Allow-Methods: POST`
- `Access-Control-Allow-Headers: Content-Type`

auth0

About this task

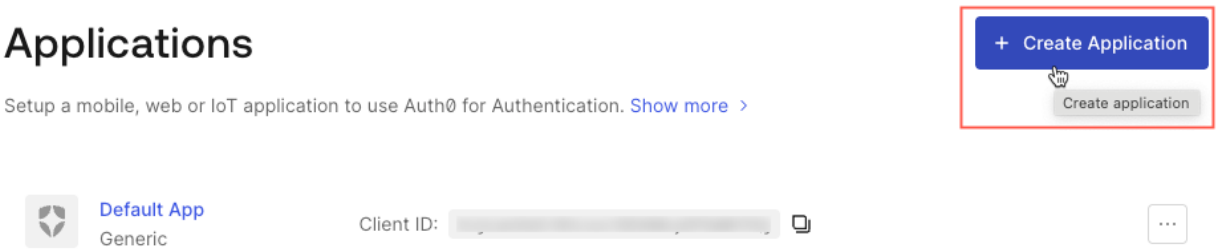
For more information about configuring auth0, see auth0 documentation: Applications in Auth0.

1. From the auth0 menu, click **Applications** > **Applications**.
   Figure 23. Applications link in auth0

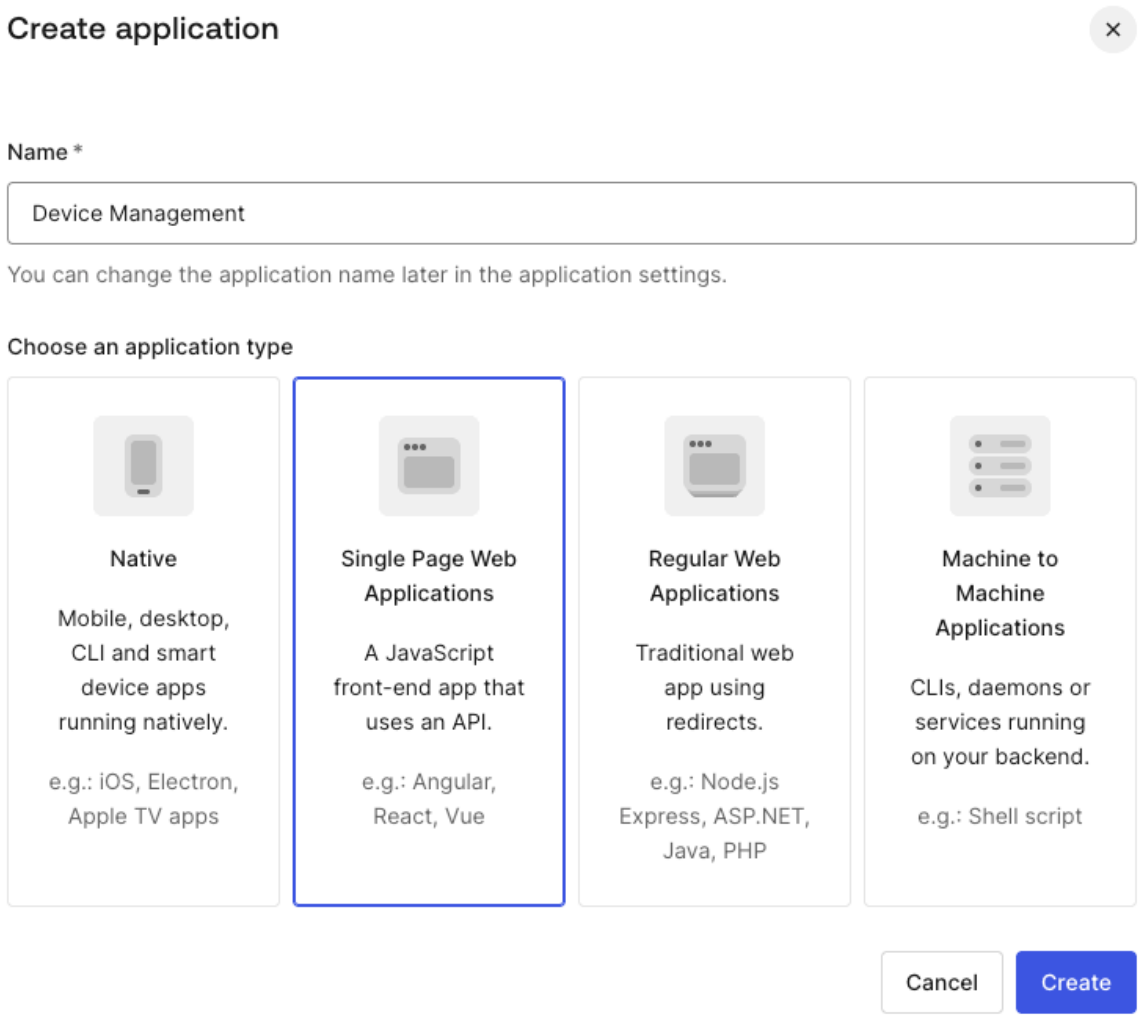


2. Click **Create Application**.
   Figure 24. Create application button in auth0

©2026 Tanium Inc. All Rights Reserved

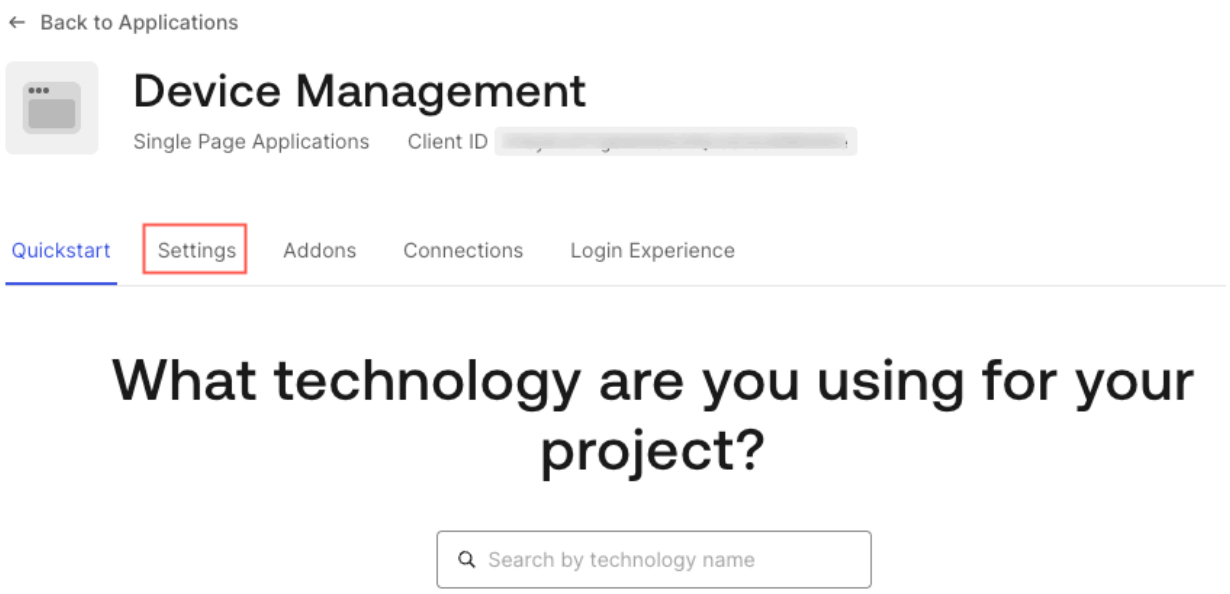


3. Specify a **Name** for the application and select **Single Page Web Application**. Click **Create**.
   Figure 25. Single Page Web Application option in auth0

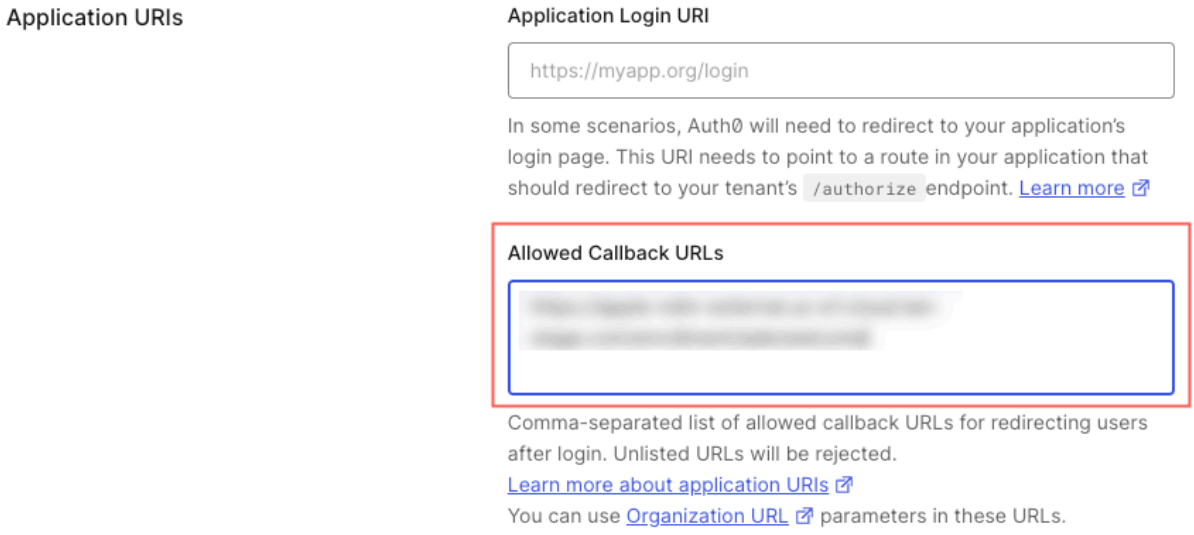


4. On the application page, click the **Settings** tab.
   Figure 26. Settings tab in auth0

©2026 Tanium Inc. All Rights Reserved

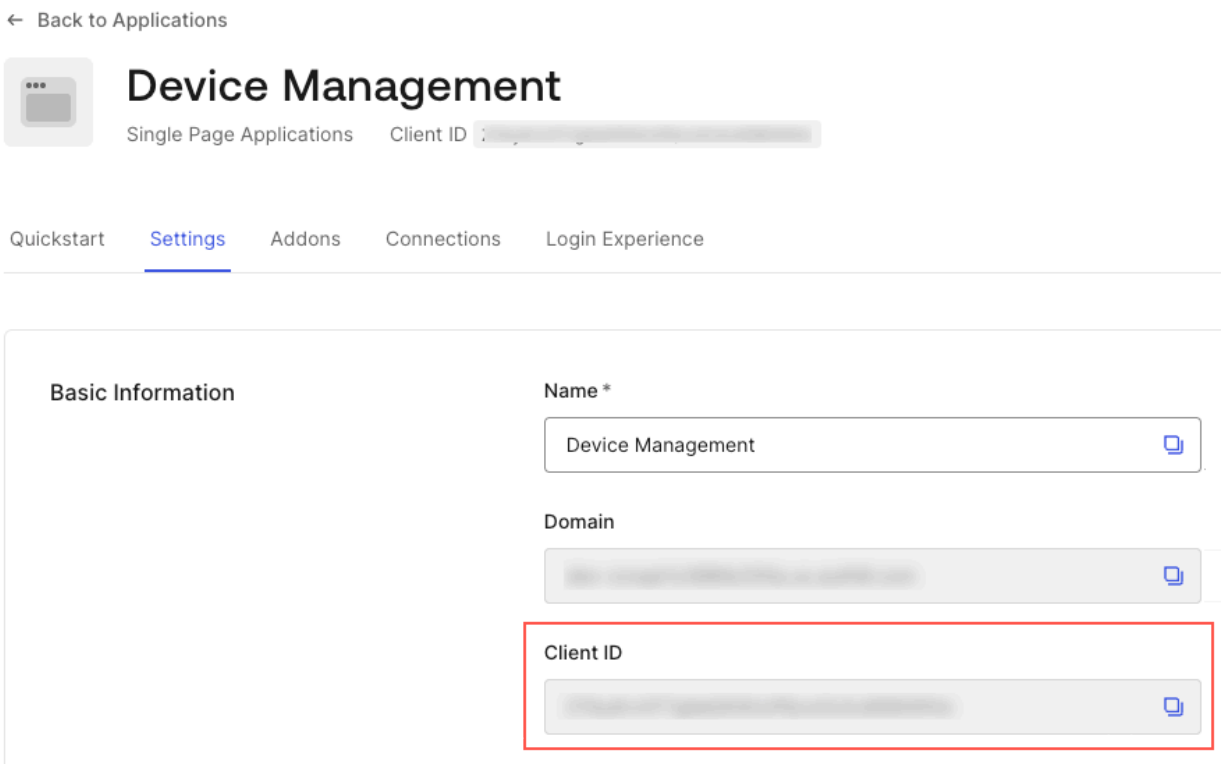


5. In the **Allowed Callback URLs** field, enter the URI that you copied from the Device Management settings.
   Figure 27. Allowed Callback URLs field in auth0



6. Copy the **Domain** and **Client ID** from the application details and save it for use in Device Management.
   Figure 28. Client ID field in auth0

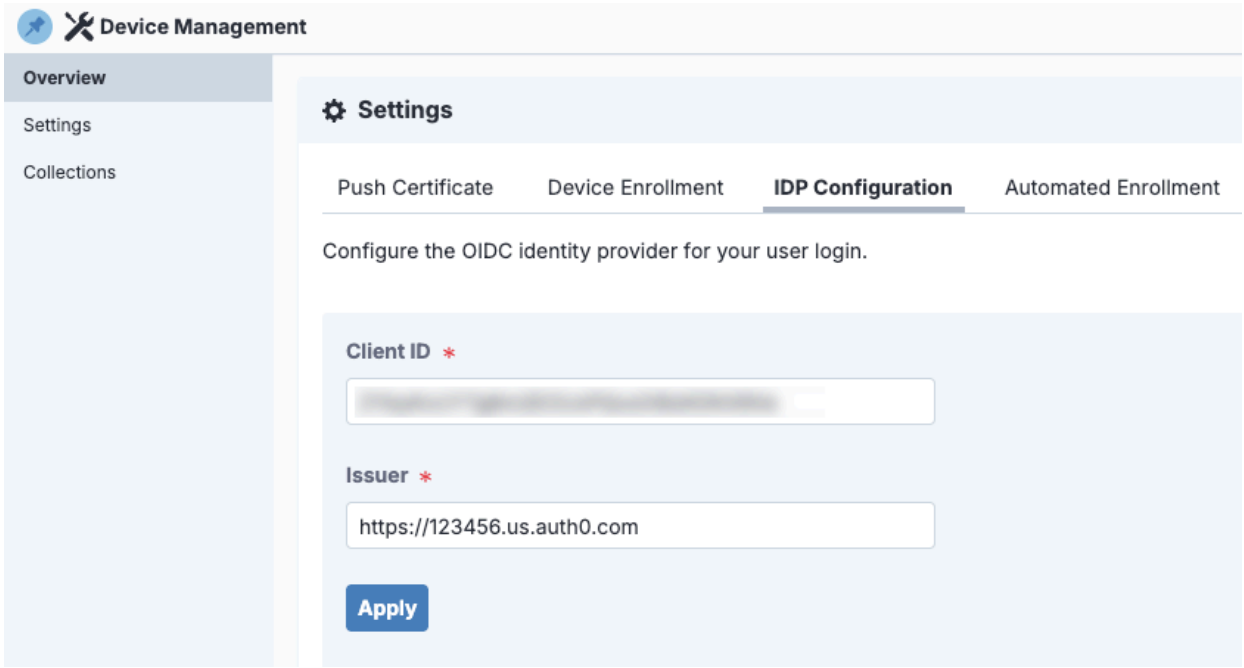
©2026 Tanium Inc. All Rights Reserved



7. Return to Tanium Console. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click **IDP Configuration**.

8. Set the **Client ID** to the **Client ID** value that you copied from auth0, and set the **Issuer** as the **Domain** that you copied from auth0, with https:// added to the beginning. For example, `https://123456.us.auth0.com`. Click **Apply**.

Figure 29. Client ID field in the Device Management settings



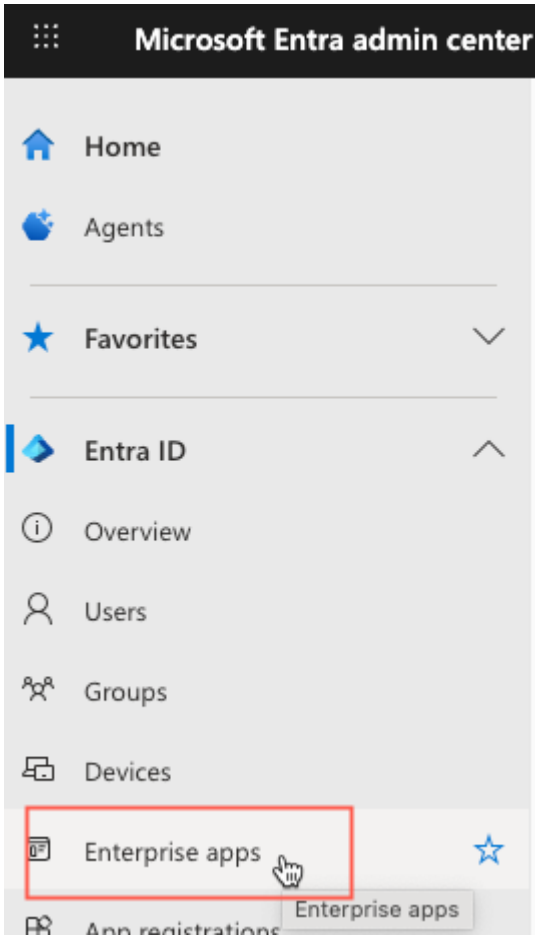
©2026 Tanium Inc. All Rights Reserved

Microsoft Entra ID

About this task

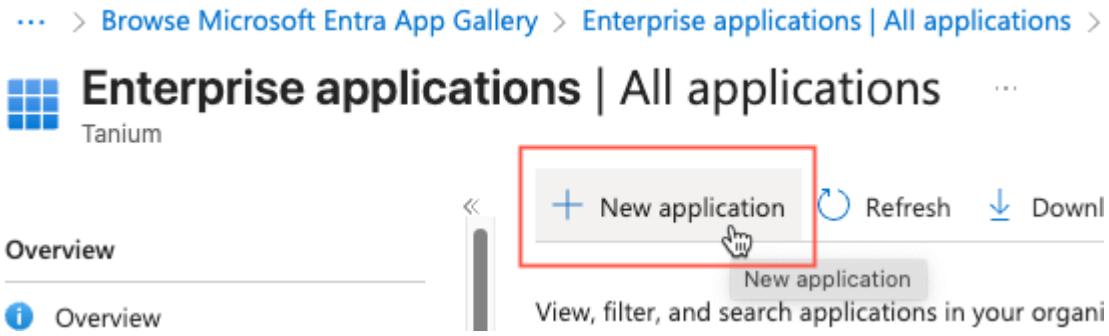
For more information about configuring Microsoft Entra ID, see Microsoft Entra Documentation: Single-page application: Code configuration.

1. From the Entra menu, click **Enterprise Applications**.
   Figure 30. Enterprise Apps link in Entra ID



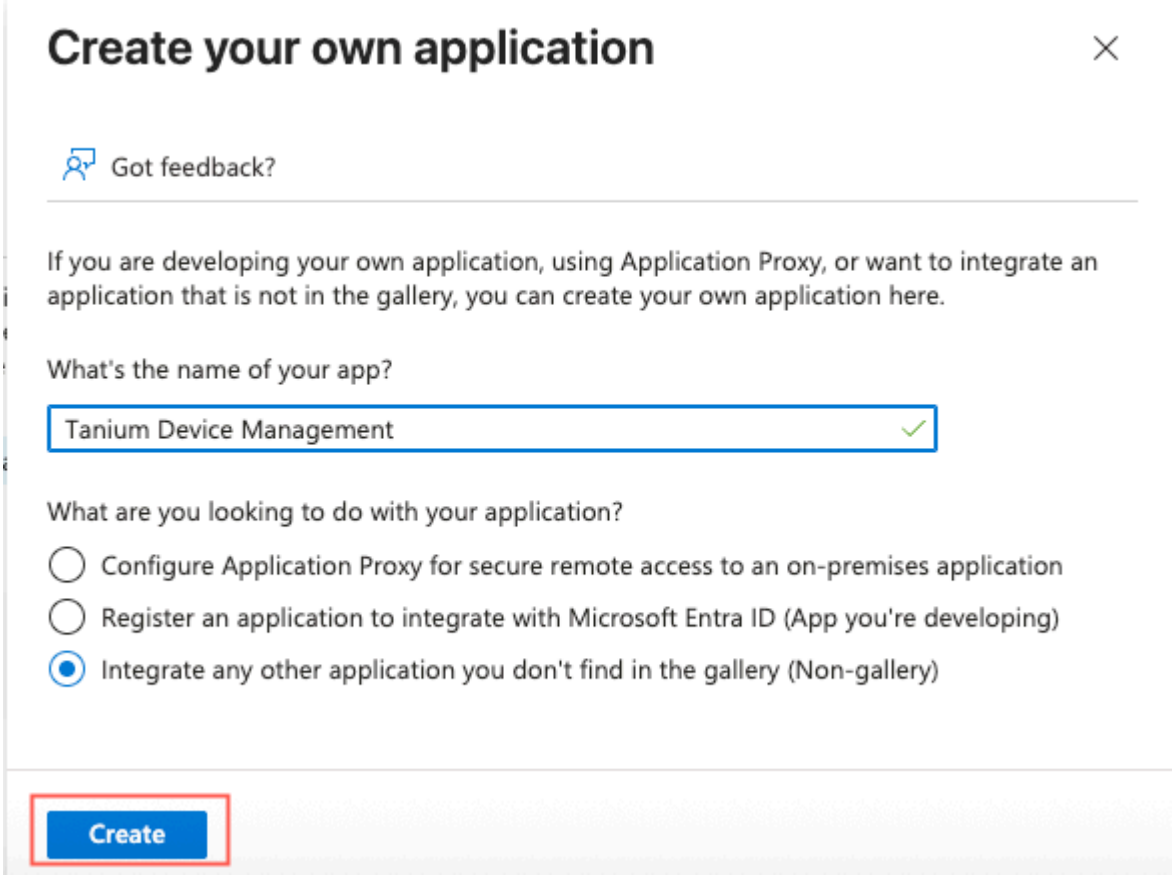
2. Click **New Application**.
   Figure 31. New application link in Entra ID

©2026 Tanium Inc. All Rights Reserved



3. Click **Create your own application**.
4. Specify a name for the application.
5. Select this option: **Integrate any other application you don't find in the gallery**.
6. Click **Create**.

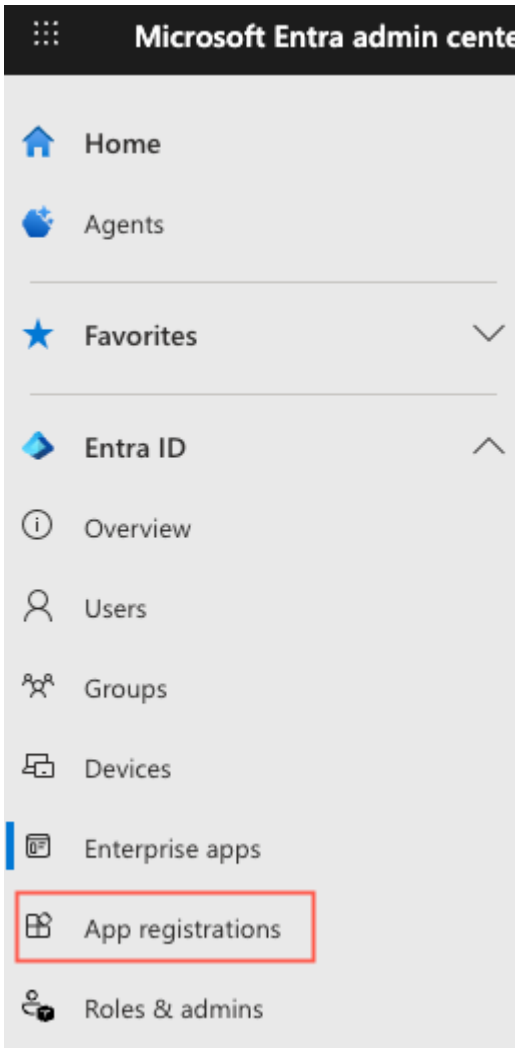
Figure 32. Create an application in Entra ID



7. From the Entra menu, click **App registrations**.

Figure 33. App registrations link in Entra ID

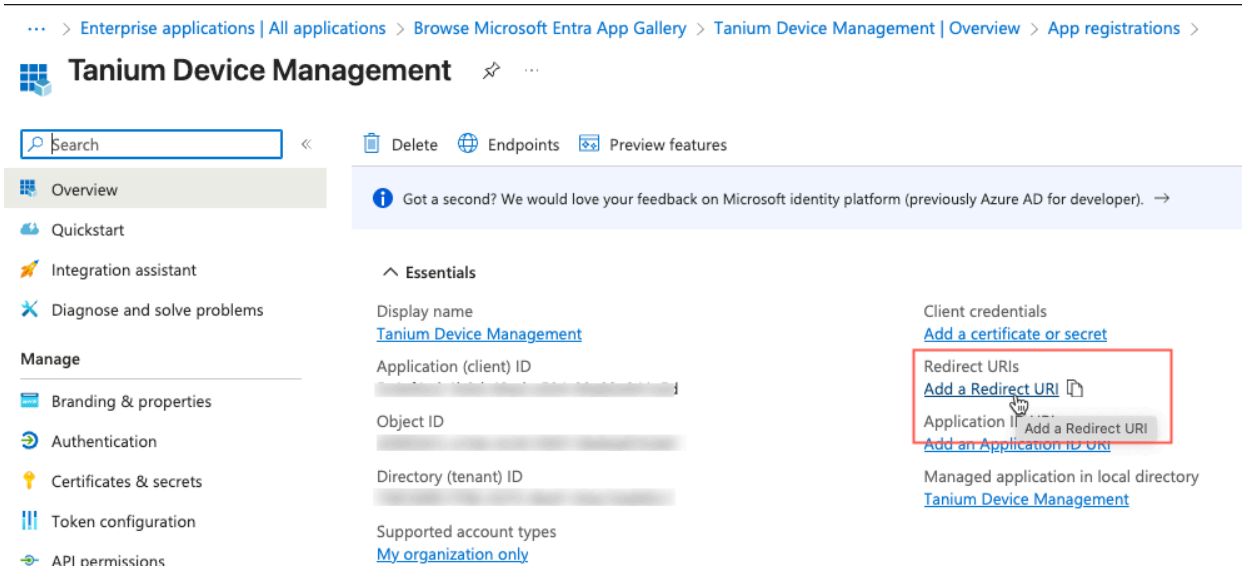
©2026 Tanium Inc. All Rights Reserved



8. Click the name of the app that you created.

9. Click **Add a Redirect URI**.

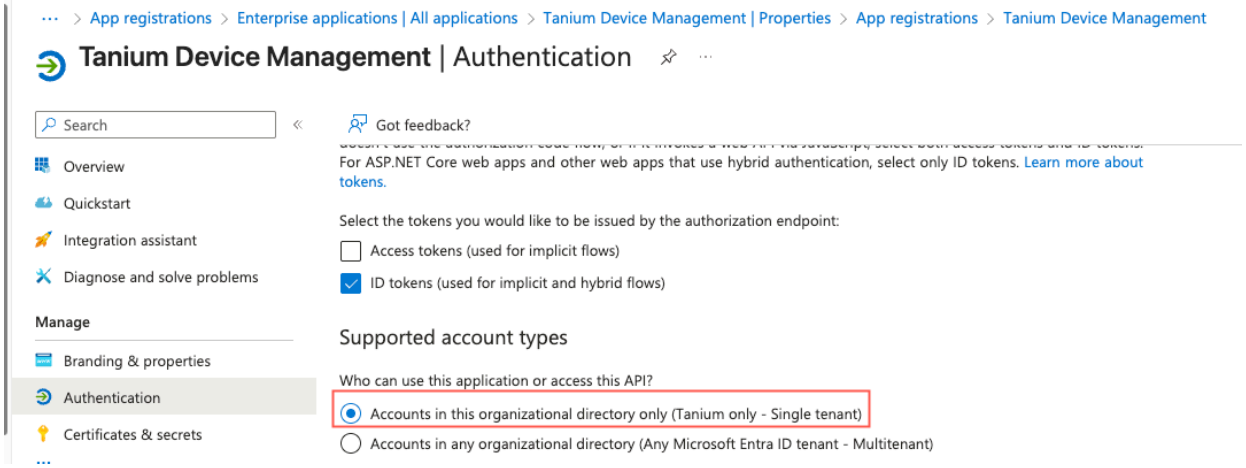
Figure 34. Redirect URI link in Entra ID



©2026 Tanium Inc. All Rights Reserved

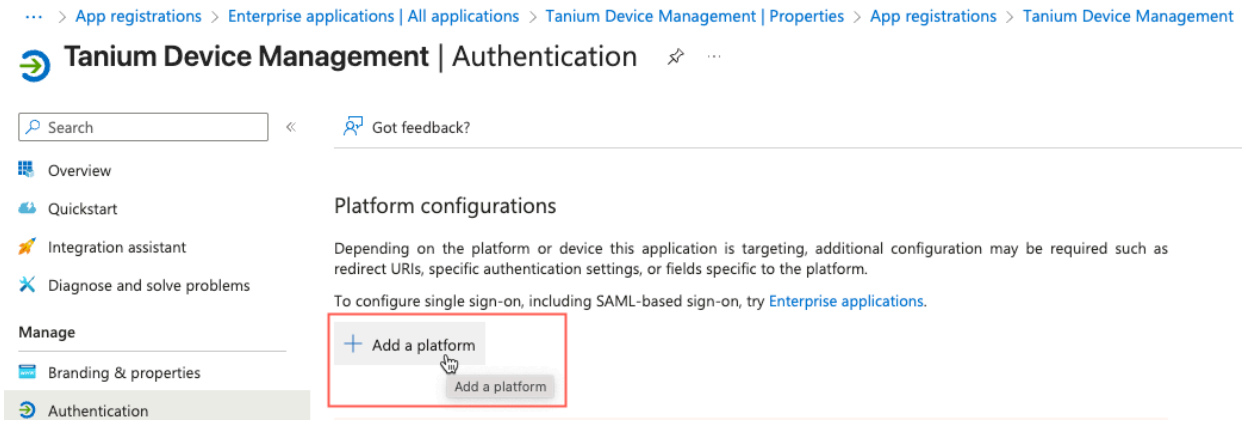
10. Confirm that the **Supported account types** field is set to **Accounts in this organizational directory only**.

Figure 35. Accounts in this organizational directory only option in Entra ID



11. In the **Platform configurations** section, click **Add a platform**.

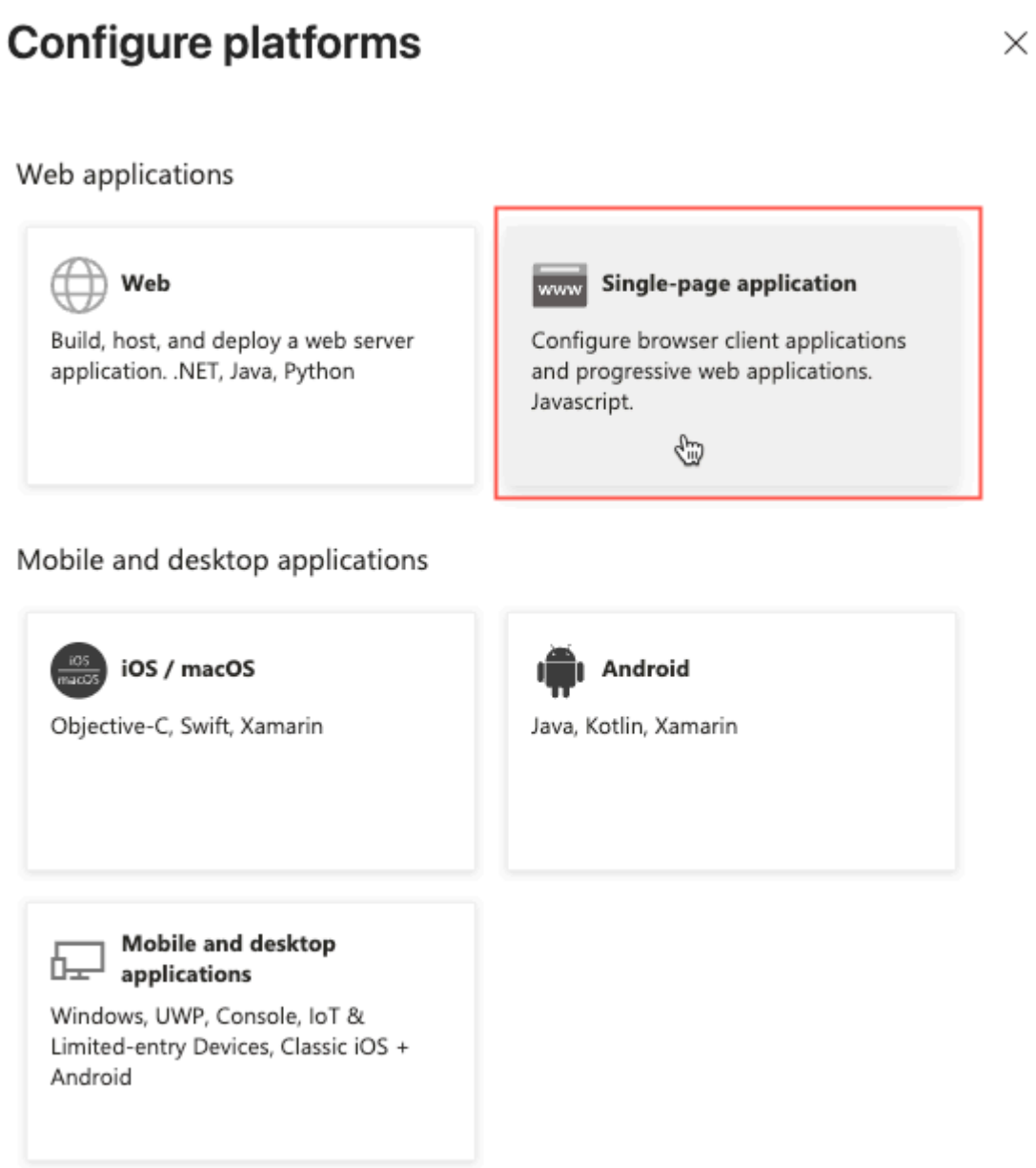
Figure 36. Add Platform button in Entra ID



12. Click **Single-page application**.

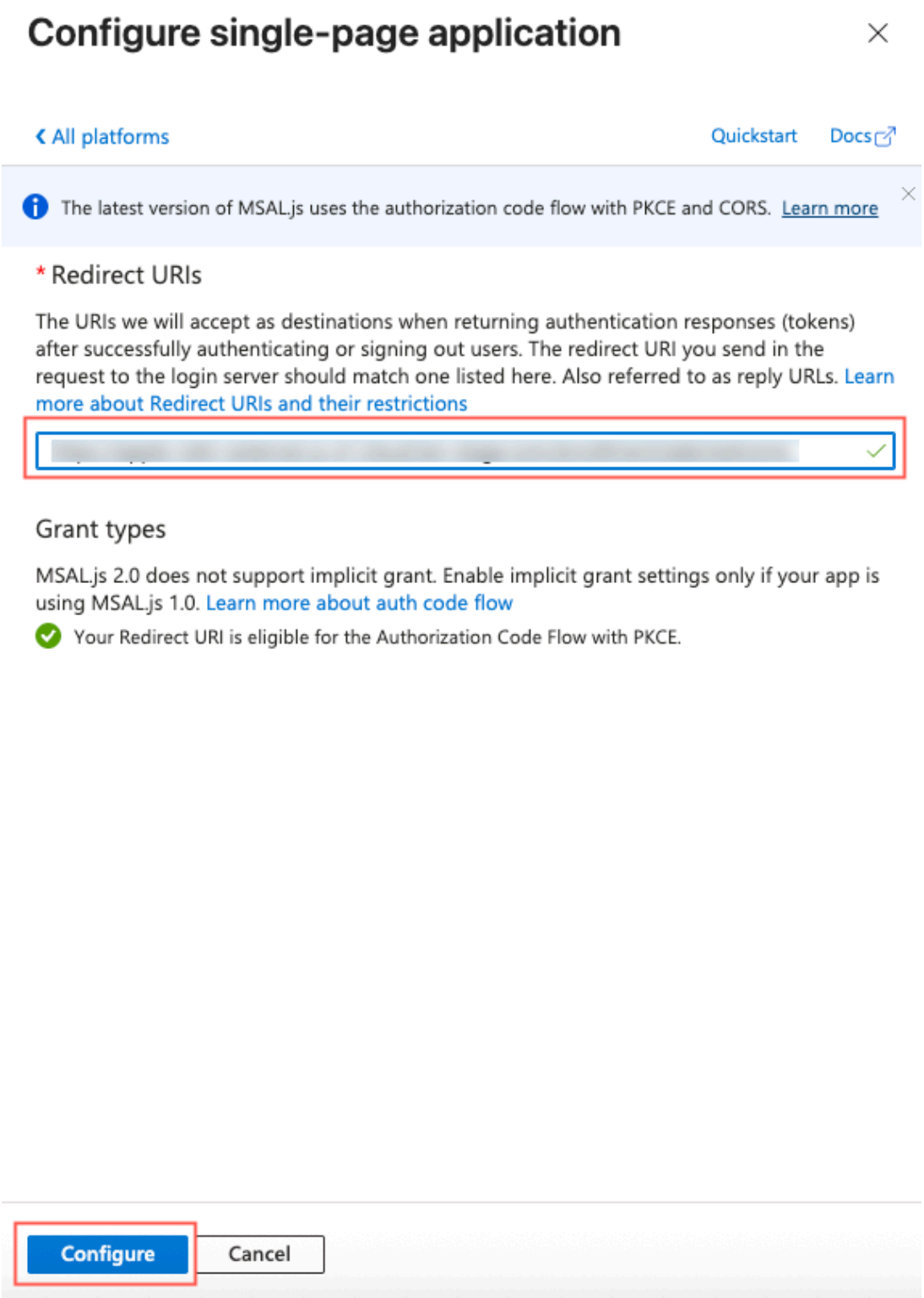
Figure 37. Single-page application option in Entra ID

©2026 Tanium Inc. All Rights Reserved



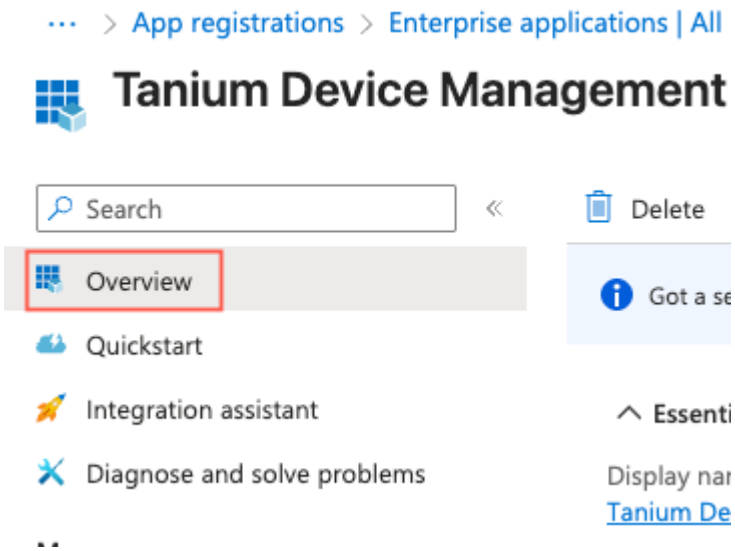
13. In the **Redirect URIs** section, enter the URI that you copied from the Device Management settings. Click **Configure**.
    Figure 38. Redirect URIs link in Entra ID

©2026 Tanium Inc. All Rights Reserved



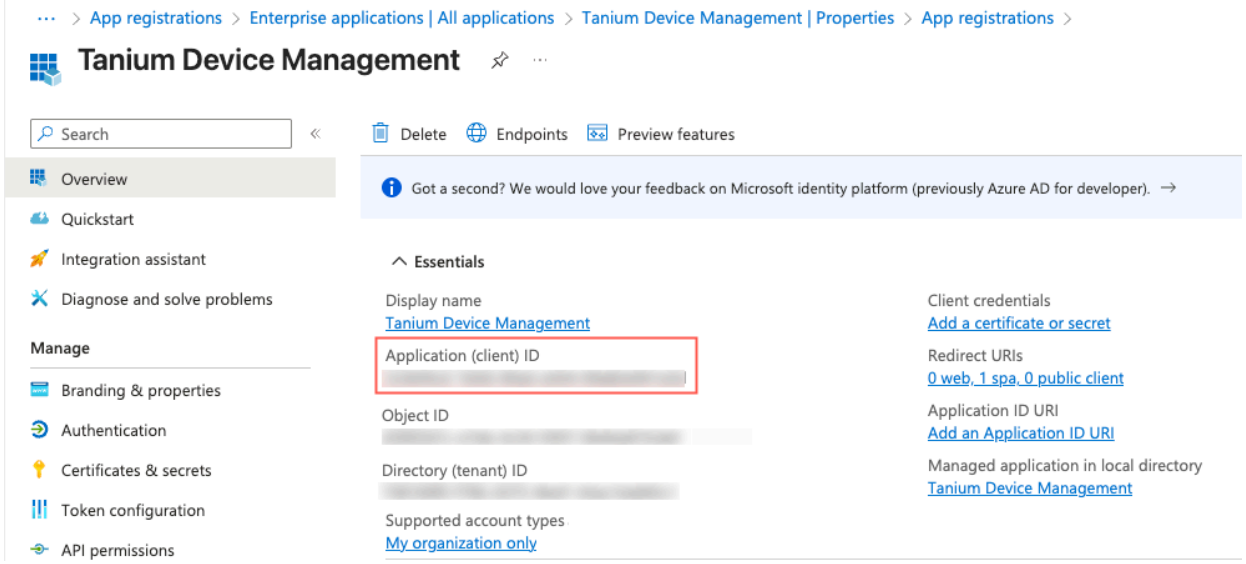
14. Click **Overview** to return to the application details.
    Figure 39. Link to application Overview page in Entra ID

©2026 Tanium Inc. All Rights Reserved



15. Copy and save the value for the **Application (client) ID**.

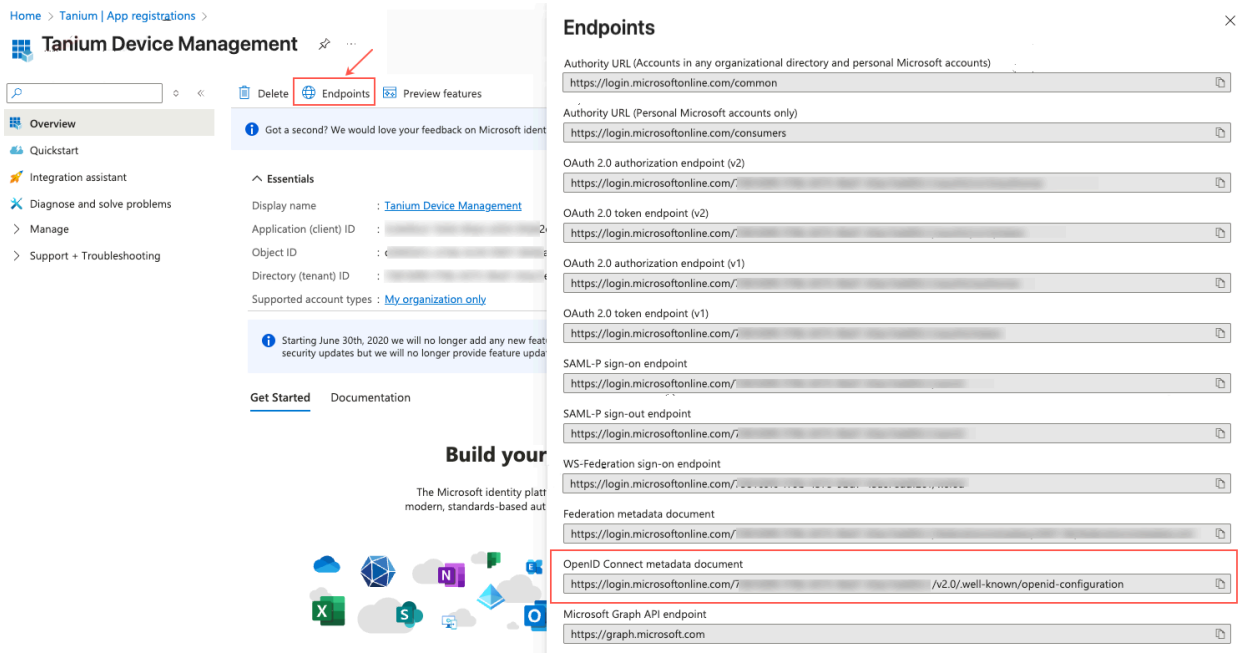
Figure 40. Application (client) ID field in Entra ID



16. Click the **Endpoints** tab. Copy and save the value for the **OpenID Connect metadata document** value, omitting the /.well-known/openid-configuration from the end.

Figure 41. OpenID Connect metadata document field on the Endpoints tab in Entra ID

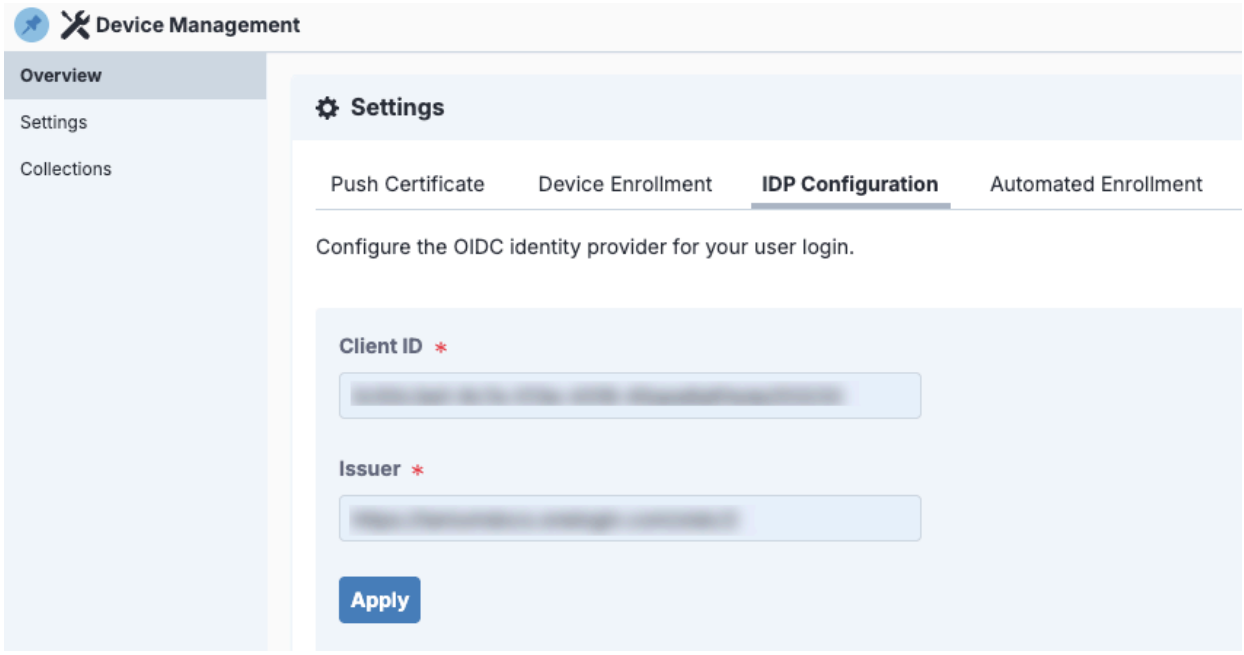
©2026 Tanium Inc. All Rights Reserved



17. Return to Tanium Console. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click **IDP Configuration**.

18. Set the **Client ID** to the **Application (client) ID** value that you copied from Entra ID, and set the **Issuer** as the **OpenID Connect metadata document** (omitting the /.well-known/openid-configuration from the end) that you copied from Entra ID. Click **Apply**.

Figure 42. IdP configuration settings in Device Management



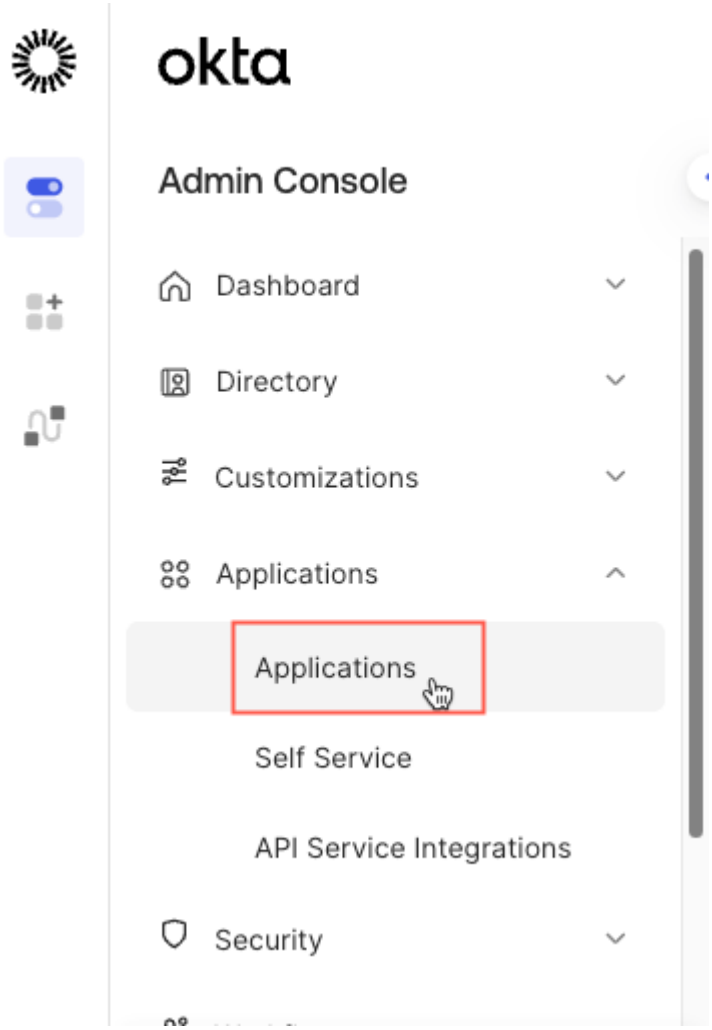
Okta

©2026 Tanium Inc. All Rights Reserved

About this task

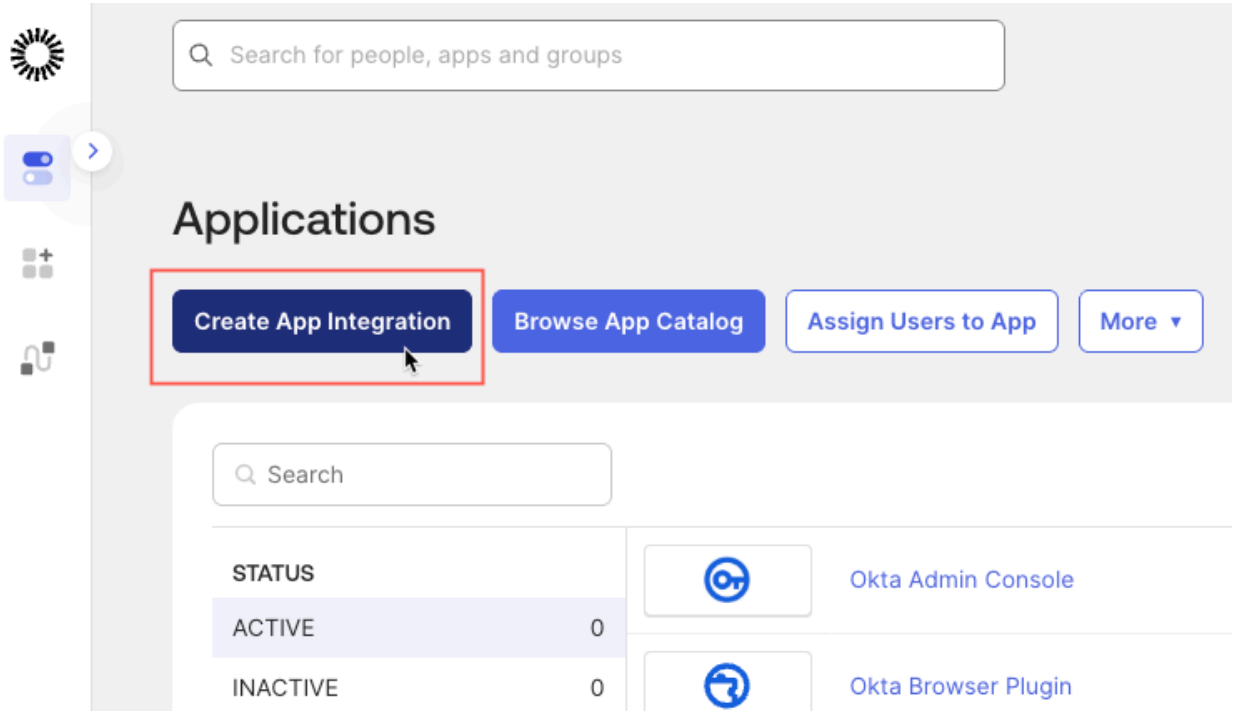
For more information about configuring Okta, see Okta documentation: Create OpenID Connect app integrations.

1. From the Okta Admin Console menu, click **Applications** > **Applications**.
   Figure 43. Applications link in Okta



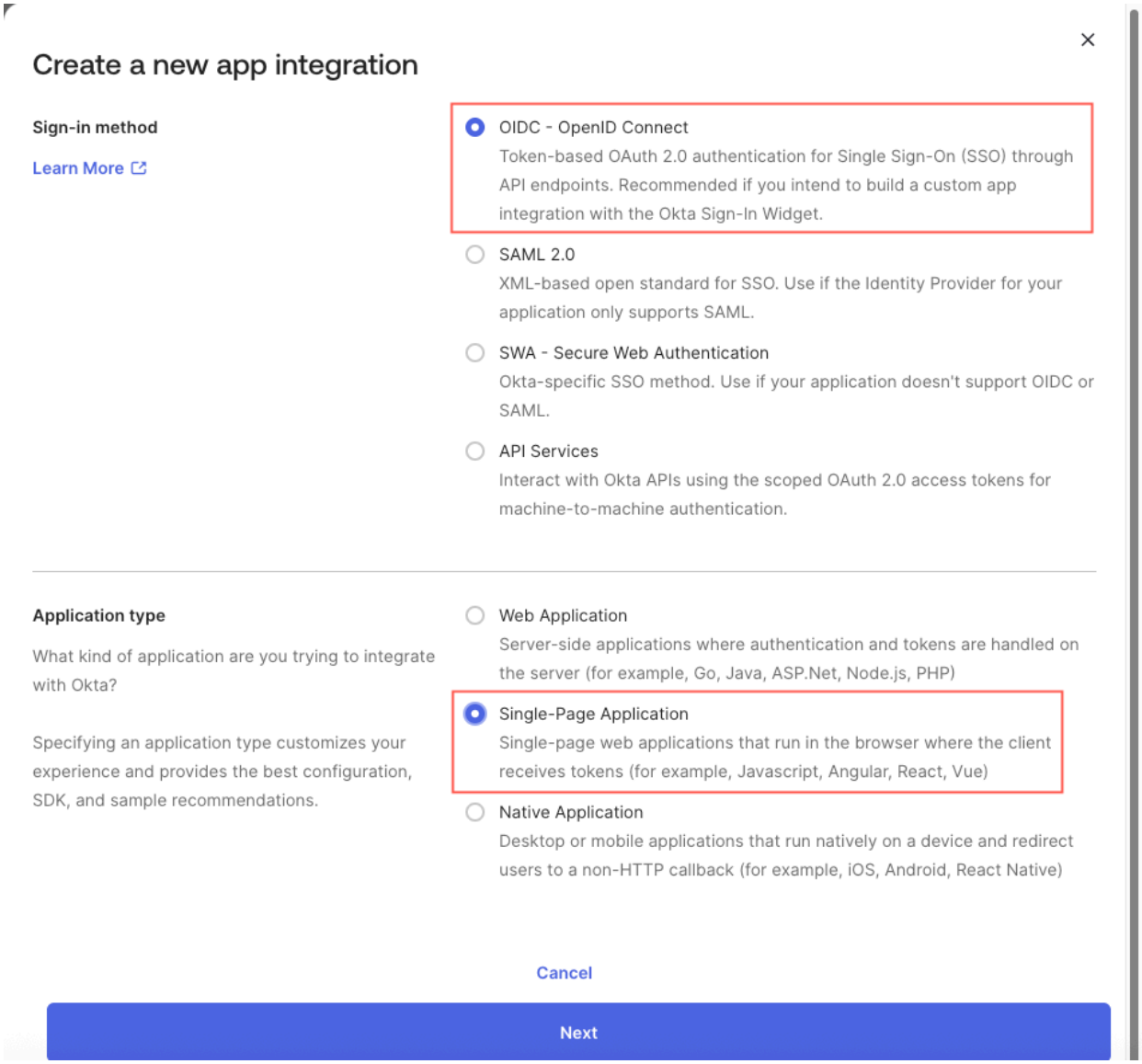
2. Click **Create App Integration**.
   Figure 44. Create App Integration in Okta

©2026 Tanium Inc. All Rights Reserved



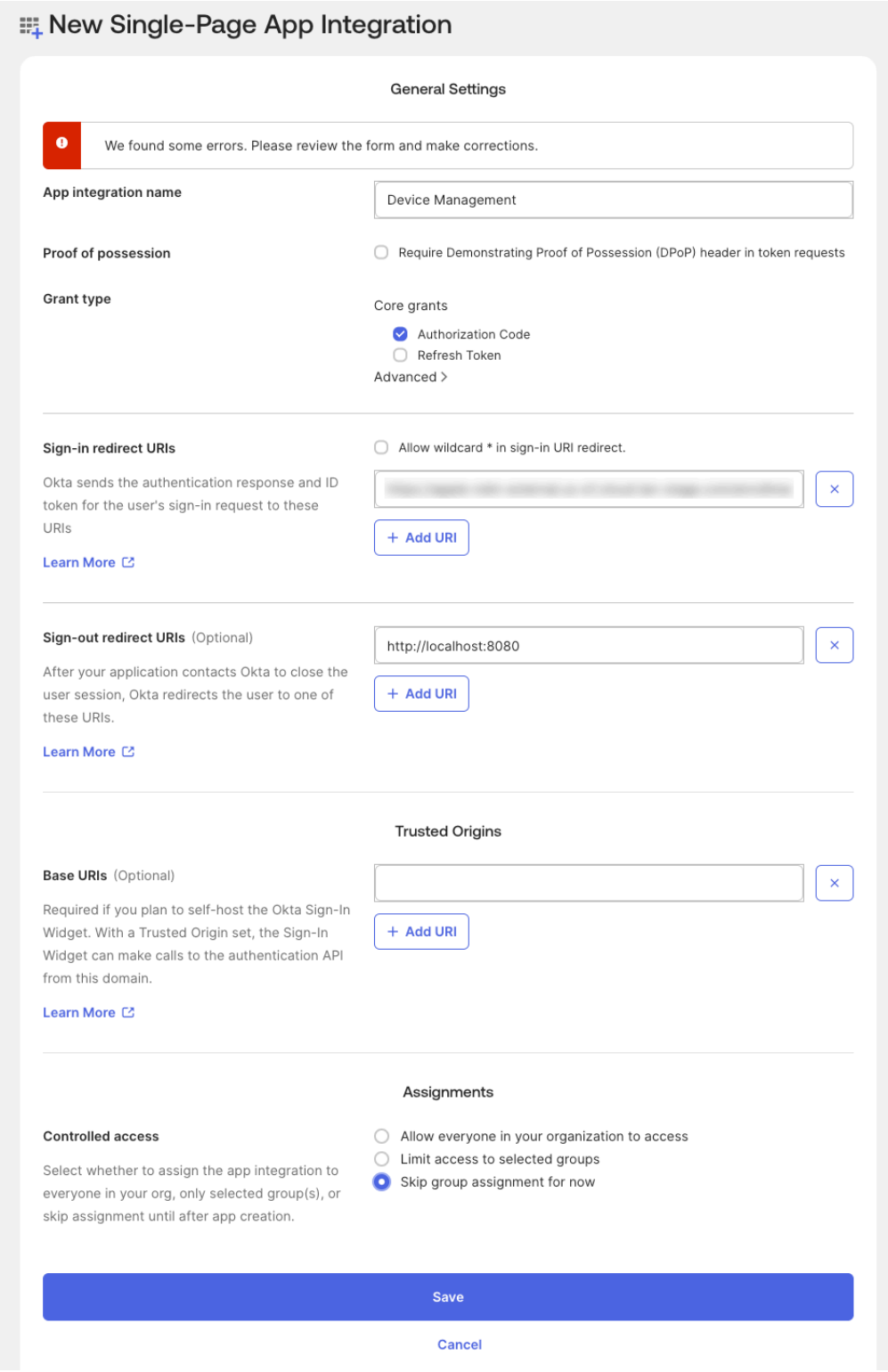
3. For the sign-in method, select **OIDC - OpenID Connect**, and select **Single-Page Application** for the application type. Click **Next**.
   Figure 45. OIDC - OpenID Connect and Single-Page Application options in Okta

©2026 Tanium Inc. All Rights Reserved



4. Specify a name for the application in the **App integration name** field.
5. In the **Sign-in redirect URIs** field, enter the URI that you copied from the Device Management settings.
   Figure 46. Sign-in redirect URIs field in Okta

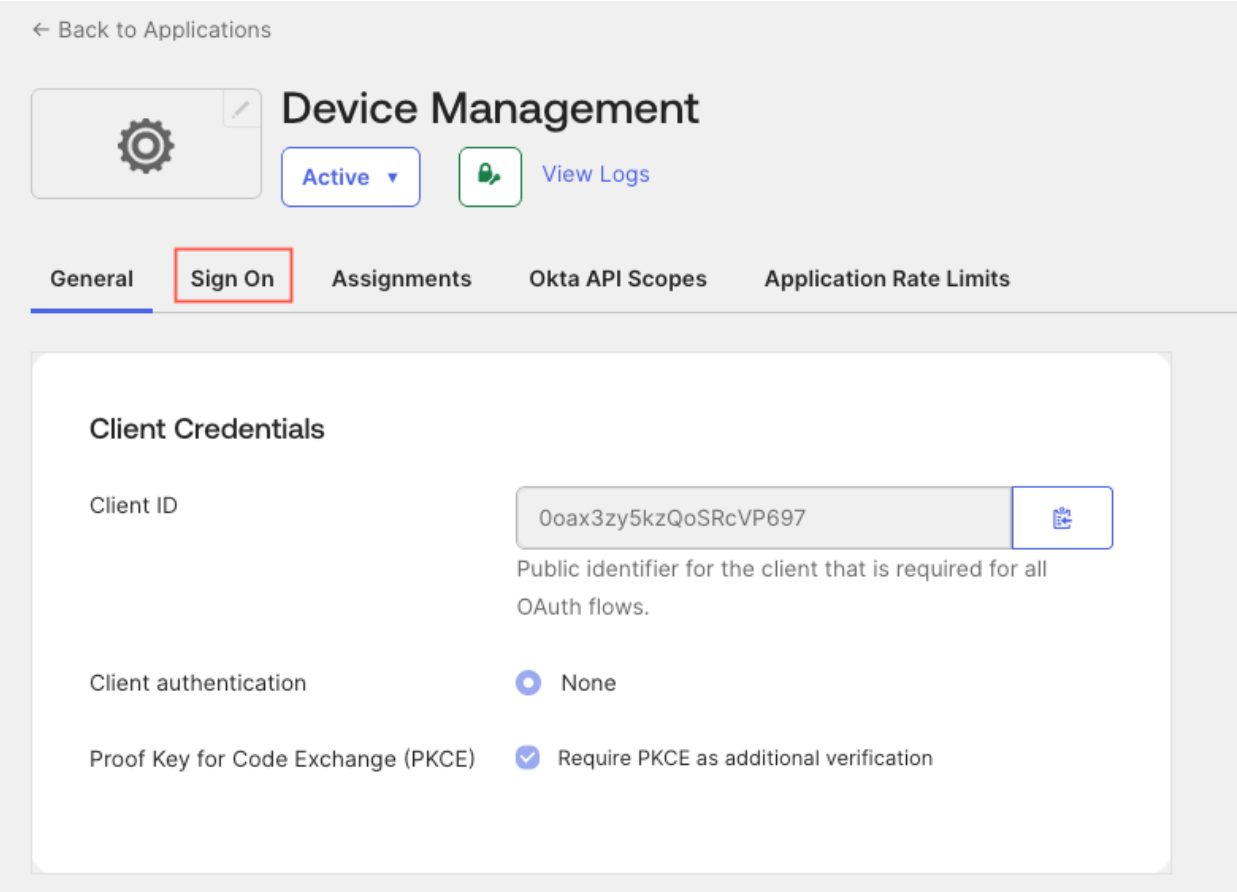
©2026 Tanium Inc. All Rights Reserved



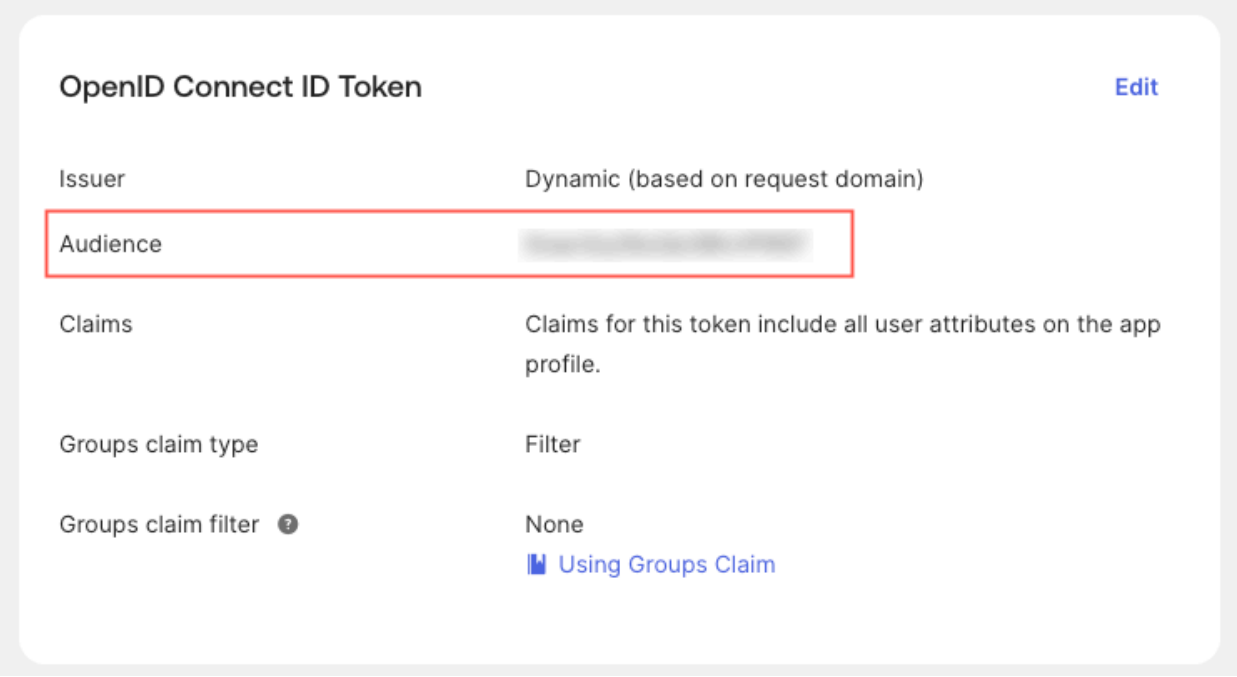
6. In the **Controlled access** section, select an assignment. Leave the other settings at their default values. Click **Save**.

7. On the application page, click the **Sign On** tab.
   Figure 47. Sign On tab in Okta

©2026 Tanium Inc. All Rights Reserved



8. Copy the value for **Audience**.
   Figure 48. Audience field in Okta



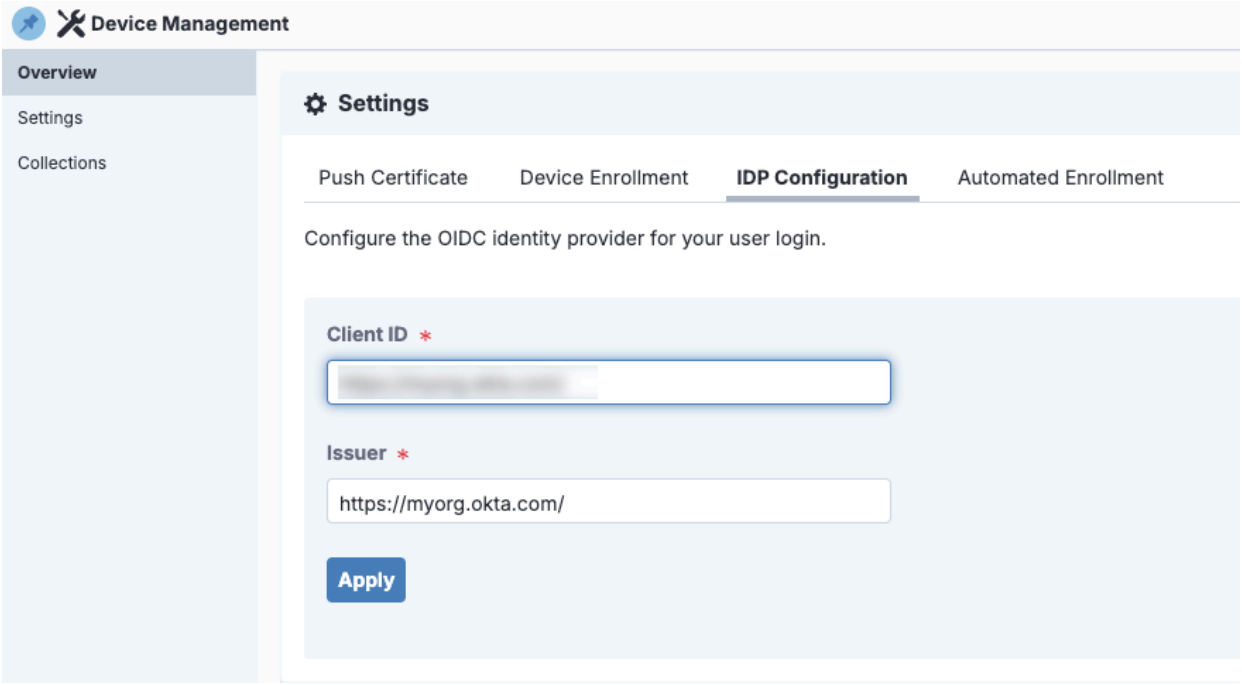
9. Note the URL for the Okta instance where you configured the application. For example,

©2026 Tanium Inc. All Rights Reserved

https://myorg.okta.com.

10. Return to Tanium Console. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click **IDP Configuration**.

11. Set the **Client ID** to the **Audience** value that you copied from Okta, and set the **Issuer** as the Okta instance URL. Click **Apply**.
    Figure 49. IdP configuration settings in Device Management



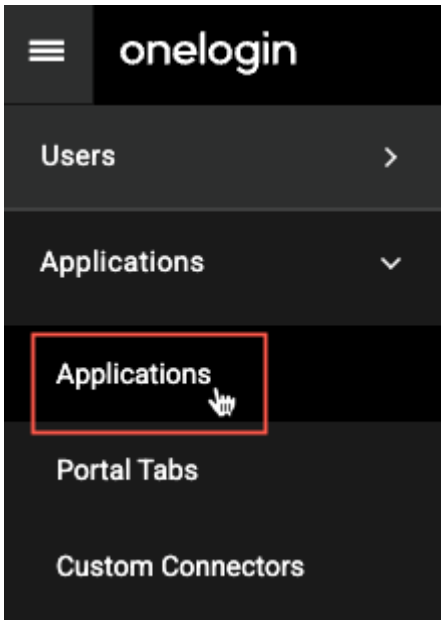
OneLogin

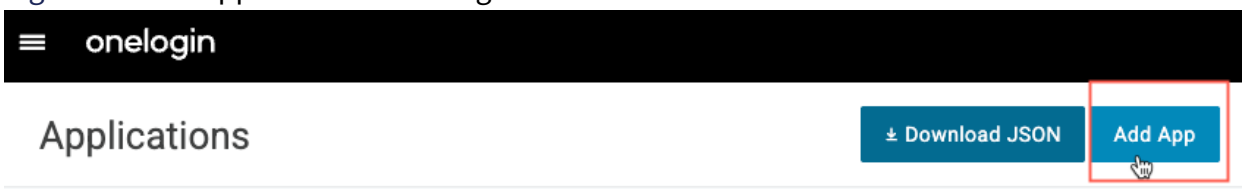
About this task

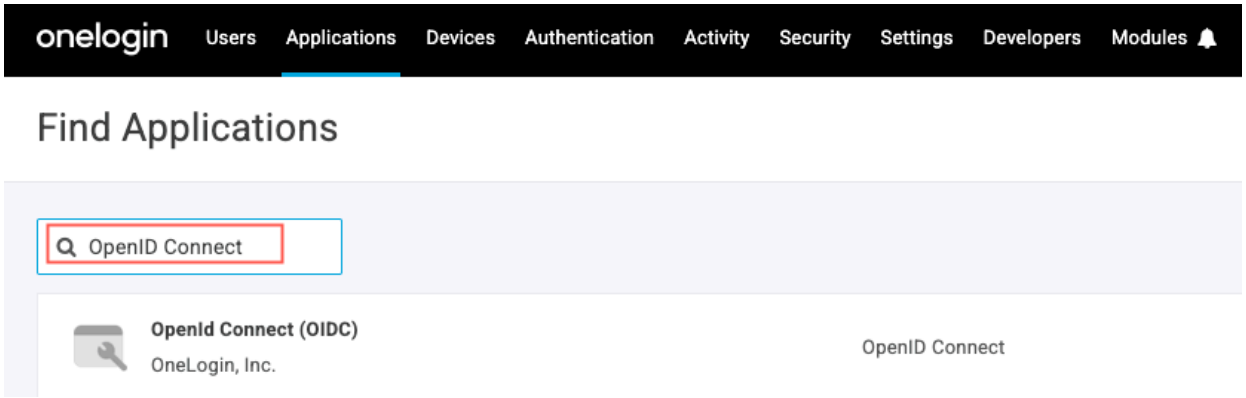
For more information about configuring OneLogin, see OneLogin Docs: OpenID Connect (OIDC) Custom Connector.

1. From the OneLogin administration menu, click **Applications** > **Applications**.
   Figure 50. Applications tab in OneLogin

©2026 Tanium Inc. All Rights Reserved



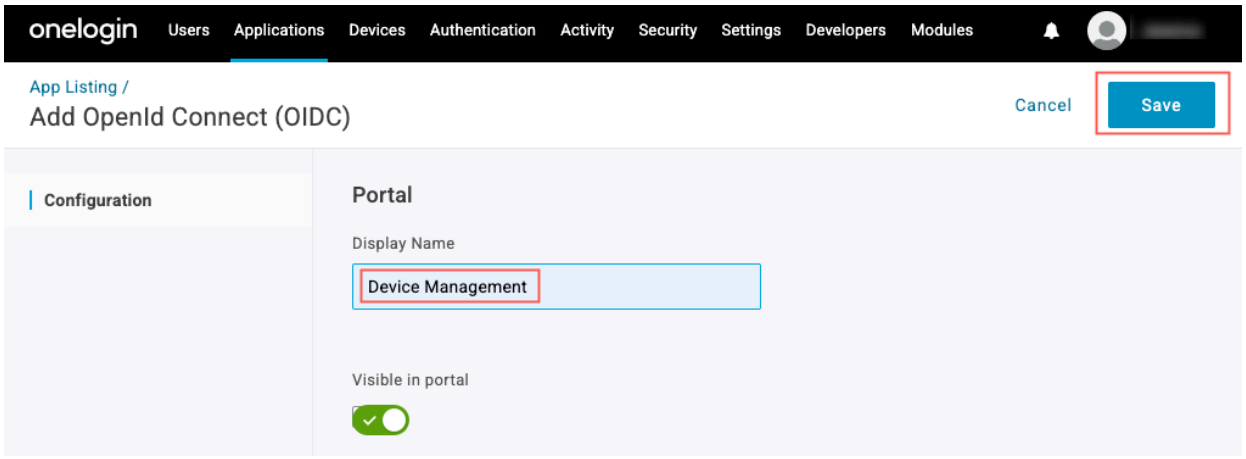
2. Click **Add App**.
   Figure 51. Add App button in OneLogin
   

3. Search for `OpenID Connect (OIDC)`.
   Figure 52. OpenID Connect search in OneLogin
   

4. Click the app to add it.

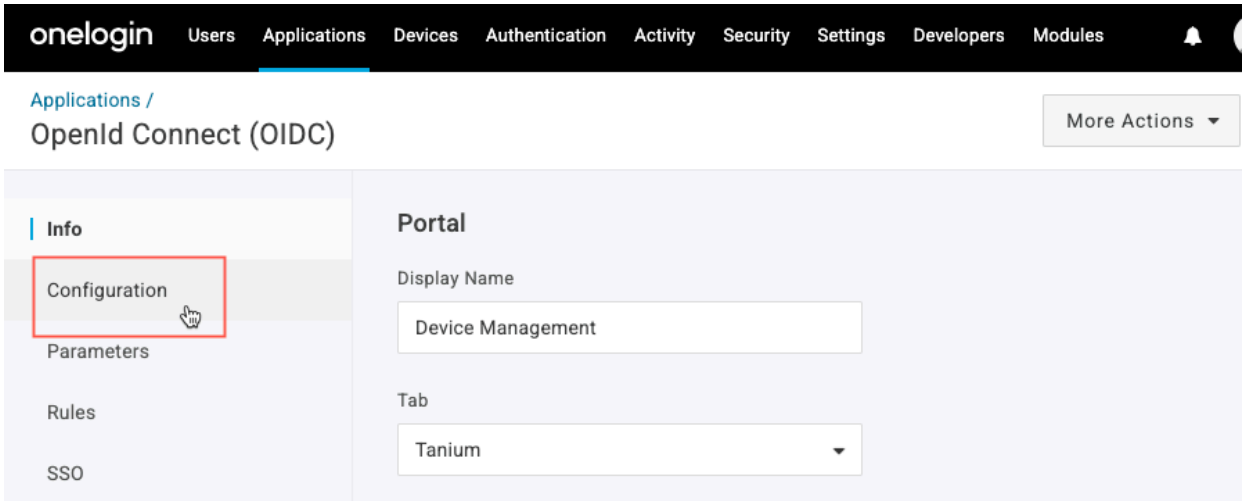
5. Specify a **Display Name** and, optionally, the icons for the app. Click **Save**.
   Figure 53. Display Name field in OneLogin

©2026 Tanium Inc. All Rights Reserved



6. Click the **Configuration** tab.

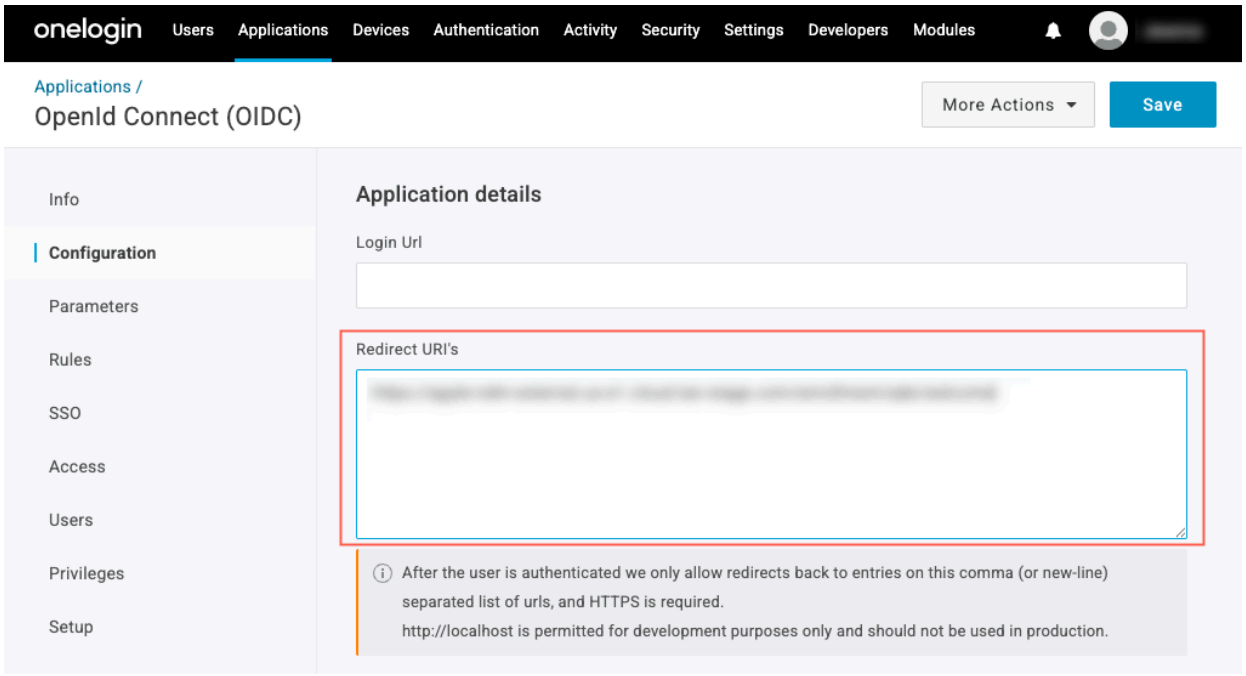
Figure 54. Configuration tab in OneLogin



7. In the **Redirect URI's** field, enter the URI that you copied from the Device Management settings.

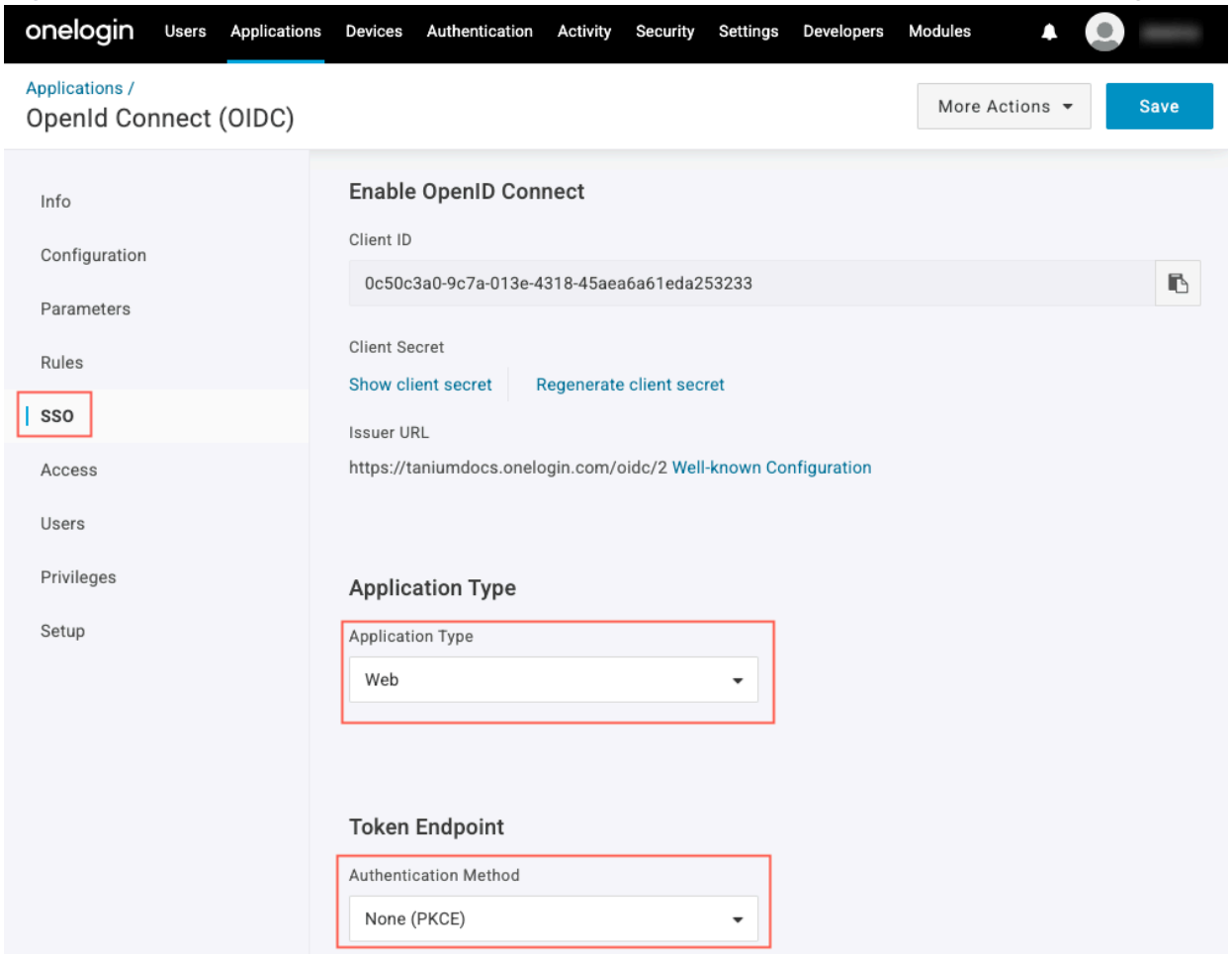
Figure 55. Redirect URI's field in OneLogin

©2026 Tanium Inc. All Rights Reserved



8. On the **SSO** tab, set the **Application Type** to **Web** and the **Authentication Method** to **None (PKCE)**.

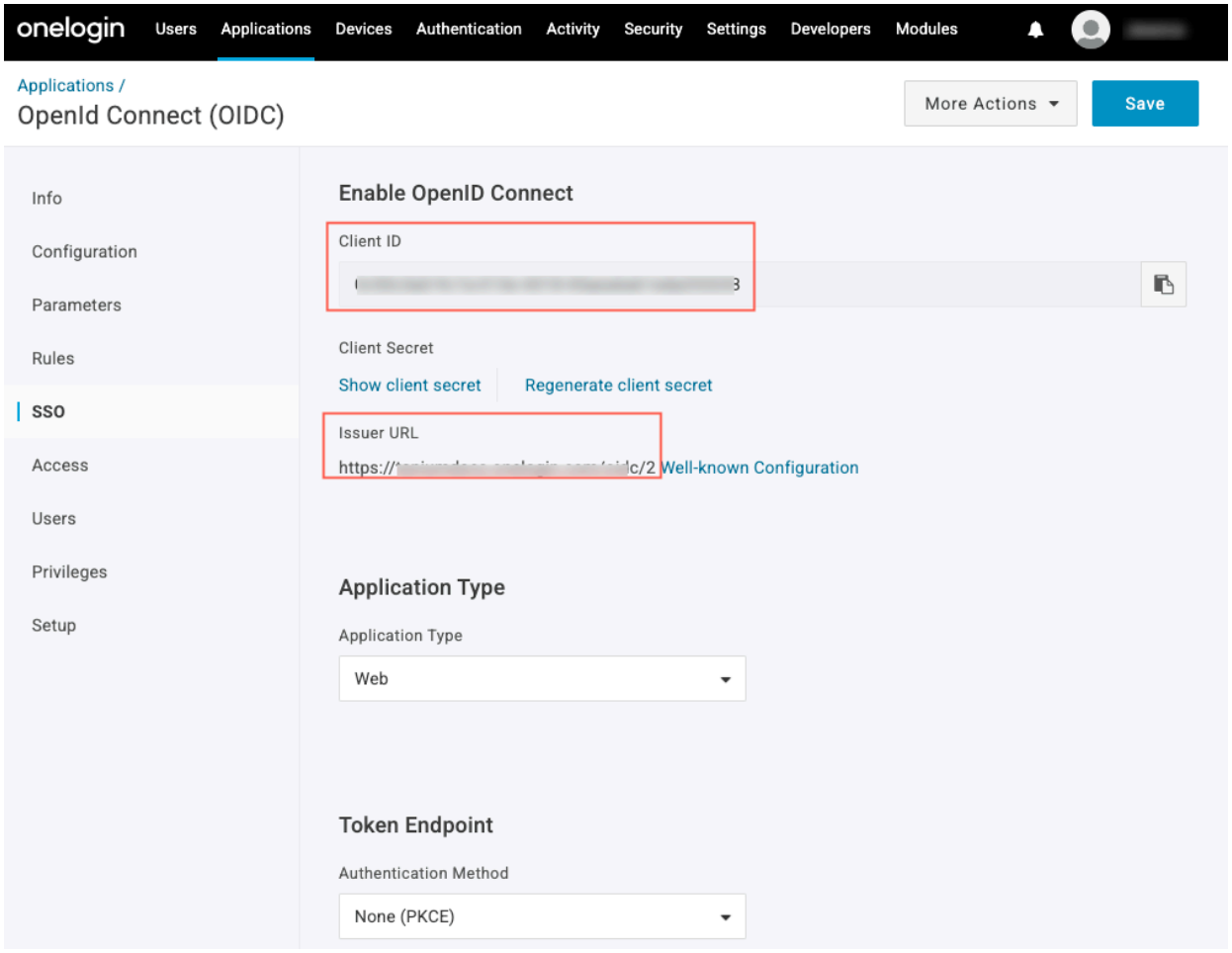
Figure 56. Application Type and Authentication Method fields on the SSO tab in OneLogin



©2026 Tanium Inc. All Rights Reserved

9. Copy and save the **Client ID** and **Issuer URL**.

   Figure 57. Client ID and Issuer URL fields in OneLogin

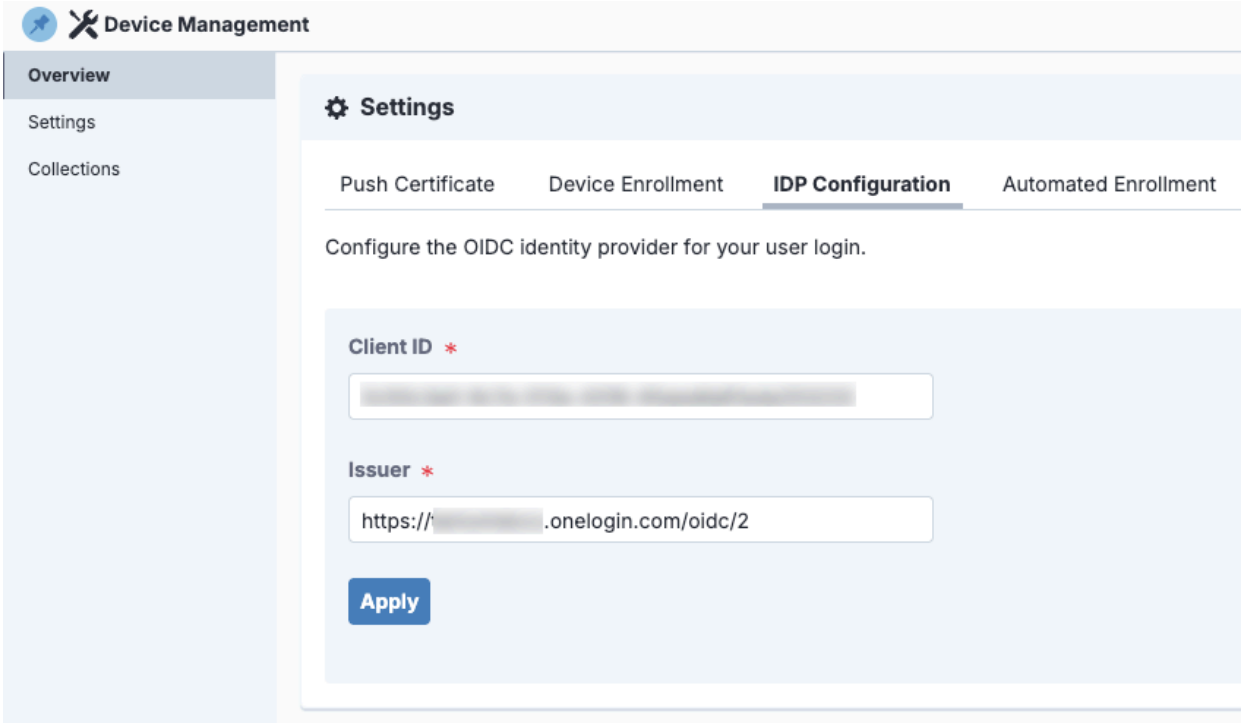


10. Return to Tanium Console. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click **IDP Configuration**.

11. Set the **Client ID** to the **Client ID** value that you copied from OneLogin, and set the **Issuer** as the **Domain** that you copied from OneLogin. Click **Apply**.

    Figure 58. IdP configuration settings in Device Management

©2026 Tanium Inc. All Rights Reserved



Troubleshooting

Error: error getting oauth2 endpoint

Cause

During enrollment, Device Management could not match the `issuer` field returned by the IdP discovery document to the Issuer URL configured in Device Management. The most common cause is a difference in the trailing slash, scheme, or path between the two values.

Solution

Compare the Issuer URL configured in Device Management against the `issuer` field returned by the IdP discovery document, and update the Device Management setting to match exactly.

1. In a browser, open {IssuerURL}/.well-known/openid-configuration and note the value of the `issuer` field in the response.
2. From the Main menu, go to **Shared Services** > **Device Management**. Click Settings and then click **IDP Configuration**.
3. Verify that the **Issuer** value matches the `issuer` field from the discovery document

©2026 Tanium Inc. All Rights Reserved

exactly, including trailing slash, scheme, and path. Update the value if necessary and click **Apply**.

©2026 Tanium Inc. All Rights Reserved

Reference: Filter operators

Filter expressions in targeting filters can match strings or regular expressions. The following table describes the supported filter operators as they appear when you use a sensor in a targeting filter for a collection.

For more information, see Tanium Console User Guide: Reference: Advanced question syntax in Console and Interact.

Filter operators

Filter operator	Usage
contains	The sensor value contains the specified string. Example: `running processes contains "chrome"`
does not contain	The sensor value does not contain the specified string.
starts with	The sensor value starts with the specified string. Example: `starts with "chrome"` When the filter is evaluated, the expression is translated to a regular expression using the `matches` operator.
does not start with	The sensor value does not start with the specified string.
ends with	The sensor value ends with the specified string. Example: `ends with "chrome.exe"` When the filter is evaluated, the expression is translated to a regular expression using the `matches` operator.
does not end with	The sensor value does not end with the specified string.
matches	The sensor value matches the specified regular expression. For sensors in the `get` clause of a question, use the `matches` operator to match any value in a list. For

©2026 Tanium Inc. All Rights Reserved

Filter operator	Usage
	example, the following question matches the user names `root` or `reboot`: `Get Last Logged In User matches (root|reboot) from all machines` In the `from` clause of a question, you can also use the `in` operator to match values in a list.
does not match	The sensor value does not match the specified regular expression.
in (`from` clause only)	The sensor value is equal to one of the specified strings. Enclose the values in parentheses and use commas as separators.
is equal to	The sensor value is equal to the specified value or string.
is not equal to	The sensor value is not equal to the specified value or string.
is less than	The sensor value is less than the specified value.
is less than or equal to	The sensor value is less than or equal to the specified string.
is greater than	The sensor value is greater than the specified value.
is greater than or equal to	The sensor value is greater than or equal to the specified string.

©2026 Tanium Inc. All Rights Reserved

Tanium Client PPPC profile

Overview

When a Mac enrolls with Device Management, the Tanium Cloud MDM Service deploys the Tanium Client PPPC profile to the device. The profile grants the Tanium Client, Tanium Client Extensions, and Tanium End User Notifications the required macOS permissions. The profile is named `Tanium Client Profile` on the device. It is a Privacy Preferences Policy Control profile that provides permissions that the Tanium Client requires.

The profile applies only to macOS. For more information about how the Tanium Client is installed on enrolled devices, see Installing the Tanium Client on page 48.

Permissions provided by the Tanium Client PPPC profile

Permissions provided by the Tanium Client PPPC profile

Application	Location	Required permissions	Apple Events
Tanium Client	/Library/Tanium/TaniumClient/TaniumClient	All System Files, Admin System Files, Post Events	System Events, SystemUIServer, Finder
Tanium Client Extensions	/Library/Tanium/TaniumClient/TaniumCX	All System Files, Admin System Files, Post Events	System Events, SystemUIServer, Finder
	/Library/Tanium/TaniumClient/TaniumCX.app	All System Files, Admin System Files, Post Events	System Events, SystemUIServer, Finder
Tanium End User Notifications	/Library/Tanium/EndUserNotifications/bin/Launcher.app	Post Events	System Events, SystemUIServer, Finder

Note: On macOS endpoints that run the universal Tanium Client binary, you must also grant All System Files, Admin System Files, and Post Events permissions to /Library/Tanium/TaniumClient/TaniumCX.app/Contents/MacOS/TaniumCX for System Events, SystemUIServer, and Finder Apple events. The Tanium Client PPPC profile does not set these permissions.

As a best practice, use the universal binary for all Macs that run macOS 11 or later.

The permissions in the table correspond to the following PPPC services in the profile:

©2026 Tanium Inc. All Rights Reserved

- All System Files: `SystemPolicyAllFiles`
- Admin System Files: `SystemPolicySysAdminFiles`
- Post Events: `PostEvent`
- Apple Events: `AppleEvents`, sent to the Finder (`com.apple.finder`), SystemUIServer (`com.apple.systemuiserver`), and System Events (`com.apple.systemevents`)

Profile properties

Tanium Client PPPC profile properties

Property	Value
Profile name	Tanium Client Profile
Profile identifier	`com.tanium.dcp.tc.pppc`
Organization	Tanium, Inc.
Scope	System
Payload type	`com.apple.TCC.configuration-profile-policy` (payload name: Tanium Client PPPC)
Team identifier for Tanium applications	`TZTPM3VTUU`

Each permission in the profile is allowed (`Allowed` is set to `true`) and is tied to the code signing requirement of the application, so that only the signed Tanium application receives the permission. The applications use the following code signing identifiers:

Code signing identifiers

Application	Identifier
Tanium Client	`com.tanium.TaniumClient`
Tanium Client Extensions	`com.tanium.TaniumCX`
Tanium End User Notifications	`f7c4440096a56f643afdccfa48c6f5f7`

The code requirement for each application uses the following format, where *identifier* is the value from the preceding table:

```
identifier "identifier" and anchor apple generic and certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
TZTPM3VTUU
```

©2026 Tanium Inc. All Rights Reserved

Configure the permissions with other MDM systems

Only one MDM system can manage each device. The Tanium Cloud MDM Service installs the Tanium Client PPPC profile only on devices that are enrolled with Device Management. If a Mac is managed by a different MDM system, that MDM system must deliver the same permissions for the Tanium Client to function fully on macOS 10.14 or later.

Important: If you previously created a PPPC custom payload for a Tanium Client version earlier than 7.2.314.3608, update the code signing requirement for newer versions of the Tanium Client.

For more information about creating a PPPC payload for devices that are not managed by Device Management, see Tanium Client Management User Guide: Deploying the Tanium Client using Client Management. For more information about MDM on macOS, see Apple Platform Deployment.

©2026 Tanium Inc. All Rights Reserved