

Device Management User Guide

Autonomous IT. Unstoppable Business.

2025H2 Semiannual Release

Version 1.3

May 27, 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 services provided 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 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 at support@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 their respective owners.

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

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

© 2026 Tanium Inc. All Rights Reserved

© 2026 Tanium Inc. All rights reserved.

Table of contents

Tanium™ Endpoint Management for Mobile overview **8**

Architecture 8

Entities and devices 9

Entity providers 9

Tanium Cloud MDM Service 10

Interoperability with other Tanium products 10

Reporting 10

Getting started with Device Management **11**

Step 1: Configure Device Management users 11

Step 2: Configure an Apple Push Certificate 11

Step 3: (Optional) Configure an Apple enrollment system 11

Step 4: (Optional) Enroll endpoints 11

Step 5: Create settings 12

Step 5: Create a collection 12

Device Management requirements **13**

Core platform dependencies 13

Computer group dependencies 13

Endpoints 13

Supported Internet protocols 13

Supported operating systems 13

Third-party software 13

Host and network security requirements 14

Ports 14

Security exclusions 15

User role requirements 15

Endpoint information collection 18

Configuring Device Management **19**

© 2026 Tanium Inc. All Rights Reserved

Set up Device Management users ... 19
Configure an Apple Push Certificate to use with Device Management ... 20
Before you begin ... 20
Request and upload the Apple Push Certificate ... 21
(Automated device enrollment) Configure an identity provider ... 21
(Optional) Configure automated enrollment using an Apple enrollment system ... 24
Before you begin ... 25
Configure the enrollment system ... 25
(Optional) Configure Custom Tags for devices ... 26
Migrating from Tanium Mac Device Enrollment to Device Management ... 28
Step 1: Scope and inventory ... 28
Tanium Mac Device Enrollment ... 28
Tanium Patch ... 28
Tanium Enforce ... 28
Step 2: Configure Device Management ... 29
Step 3: Recreate Mac Device Enrollment settings and applications in Device Management ... 29
Step 4: Pilot enrollment ... 29
Step 5: Migrate devices ... 29
Migrate devices that were enrolled in Mac Device Enrollment using automated device enrollment ... 29
Migrate Devices that were enrolled in Mac Device Enrollment using the Mac Device Management enrollment portal ... 29
Apply settings to migrated devices ... 31
Step 6: Retire Mac Device Enrollment ... 31
Installing the Tanium Client ... 32
Overview ... 32
Select a Tanium Client deployment template ... 33
Before you begin ... 33
Select the deployment template ... 33
Upgrading the Tanium Client ... 33
Enrolling devices ... 34
Overview ... 34

© 2026 Tanium Inc. All Rights Reserved

Automated device enrollment ... 34
Manual enrollment ... 34
Managing settings ... **35**
Add a custom setting ... 35
Add a curated setting ... 35
Delete a setting ... 36
Review settings ... 36
What to do next ... 38
Configuring Software Update Settings and Software Enforcement settings ... **39**
Create a Software Update Settings setting ... 39
Create a Software Update Enforcement setting ... 39
What to do next ... 40
Managing web clips and applications ... **41**
(macOS) Add an enterprise application ... 41
(iOS) Add a web clip ... 41
Delete a web clip or application ... 42
Review web clips and applications ... 42
What to do next ... 44
Managing collections ... **45**
Before you begin ... 45
Create a collection ... 45
Delete a collection ... 46
Review collections ... 46
Working with devices and device data ... **49**
Overview ... 49
View the details for a device ... 50
General Info ... 50
Endpoint Overview ... 51
Deploy actions on a device ... 53
Issue questions to target devices enrolled with Device Management ... 55

© 2026 Tanium Inc. All Rights Reserved

Include devices enrolled with Device Management in a report ... 56
Use Tanium Connect to export data about devices enrolled with Device Management ... 56
Maintaining Device Management ... 57
Perform annual maintenance ... 57
Renew an Apple MDM Push Certificate ... 57
Before you begin ... 57
Renew your certificate ... 57
Update server tokens ... 57
Troubleshooting Device Management ... 59
Observed issues with specific settings ... 59
Password and Screen Unlock settings ... 59
iOS devices must be unlocked for password settings to take effect ... 59
FileVault settings ... 59
Modifying certain FileVault settings for devices that already have a FileVault profile installed might cause errors ... 59
User is not prompted to enable FileVault when Do not ask users to enable FileVault at logout is set to No ... 60
Wi-Fi Settings ... 60
Other settings fail to apply when included in a collection that defines a Wi-Fi network set to auto join ... 60
Observed issues with Web Clips and Enterprise Applications ... 60
iOS devices must be unlocked for Web Clips to Install ... 60
Contact Tanium Support ... 60
Reference: Configuring Identity Providers to use with Device Management ... 62
Before you begin ... 62
OIDC requirements ... 62
auth0 ... 63
Microsoft Entra ID ... 67
Okta ... 75
OneLogin ... 82
Troubleshooting ... 87
Error: error getting oauth2 endpoint ... 87
Reference: Filter operators ... 88

© 2026 Tanium Inc. All Rights Reserved

Tanium™ Endpoint Management for Mobile overview

NOTE

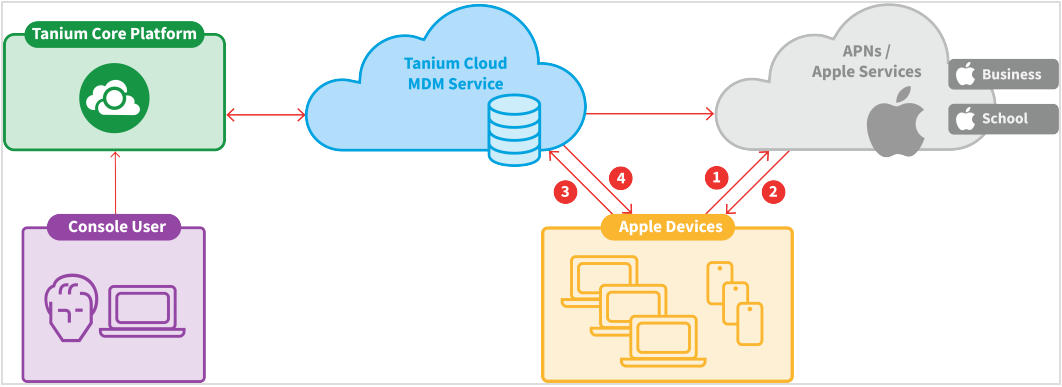
Tanium Device Management is part of the Tanium™ Endpoint Management for Mobile solution.

Tanium Device Management extends your visibility and management of Apple devices. Integrations with Apple's web-based portals, Apple Business Manager and Apple School Manager, enable you to simplify your device enrollment. You can also configure collections of settings and apply them to enrolled devices.

Architecture

Device Management works by connecting the Tanium™ Server to the Tanium Cloud MDM Service, which then communicates with enrolled 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.

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:
   - 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.

© 2026 Tanium Inc. All Rights Reserved

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 Configuring Software Update Settings and Software Enforcement settings.
- 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.

Entities and devices

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

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.
- 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
    - By direct connections to an entity, such as OT devices (used to monitor industrial or operational machinery that uses OT protocols like Profinet or ControlBus)
    - Through third-party services, such as the Apple Push Notification Service

© 2026 Tanium Inc. All Rights Reserved

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 Endpoint Management for Operational Technology	Operational Technology	*<configured-entity-provider-name>*	Operational Technology Device

Tanium Cloud MDM Service

Tanium Cloud MDM Service is a cloud-based service that enables your 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. 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. To access the page, see Working with devices. For more information about device details, see Tanium Reporting User Guide: Viewing and managing a single endpoint.

© 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 19



Only users with the Device Management Administrator role can access the configuration settings in the Device Management workbench.

Step 2: Configure an Apple Push Certificate

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

For more information, see Configure an Apple Push Certificate to use with Device Management on page 20.

Step 3: (Optional) Configure an Apple enrollment system

Enable Device Management to interact with Apple enrollment system, either Apple Business Manager or Apple School Manager, to automatically enroll endpoints. For more information, see (Optional) Configure automated enrollment using an Apple enrollment system on page 24.

Step 4: (Optional) 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 Enrolling devices on page 34.

© 2026 Tanium Inc. All Rights Reserved

Step 5: 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 Managing settings on page 35.

Step 5: 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 Managing collections on page 45.

© 2026 Tanium Inc. All Rights Reserved

Device Management requirements

Review the requirements before you 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™ Client: No client requirements

Computer group dependencies

Tanium Cloud automatically imports the computer groups that Device Management requires:

- All Mobile Devices

Endpoints

Supported Internet protocols

Device Management supports IPv4 and IPv6 addresses.

Supported operating systems

The following endpoint operating systems are supported with Device Management.

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

Third-party software

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

- 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

© 2026 Tanium Inc. All Rights Reserved

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



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).

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
Enrolled devices	Tanium Cloud MDM Service	443	HTTPS	Allows communication with Tanium Cloud MDM Service to retrieve certificates during device enrollment



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 Tanium Cloud User Guide: Host and network security requirements.

© 2026 Tanium Inc. All Rights Reserved

Security exclusions

Device Management requires no specific security exclusions. For a list of all security exclusions to define across Tanium, see Tanium Client Management Guide: Reference: Endpoint security exclusions.

User role requirements

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

- Device Management solution permissions on page 15
- Device Management requirements on page 13: 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 19.

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

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

Device Management solution permissions

Permission	Device Management Administrator	Device Management Operator	Device Management Read Only
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

Device Management solution permissions (continued)

Permission	Device Management Administrator	Device Management Operator	Device Management Read Only
Device Management Administrator Allows full control of Device Management	✓ ADMINISTER	✗	✗
Device Management API Read data from Device Management	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE
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 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

© 2026 Tanium Inc. All Rights Reserved

Device Management solution permissions (continued)

Permission	Device Management Administrator	Device Management Operator	Device Management Read Only
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 required to take actions on Device Management devices from the Endpoint Details page	✓ COMMAND	✓ COMMAND	✗
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

© 2026 Tanium Inc. All Rights Reserved

Device Management solution permissions (continued)

Permission	Device Management Administrator	Device Management Operator	Device Management Read Only
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 Tanium Console User Guide: View effective role permissions.

Device Management administration and platform content permissions

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

To view the content sets to which the platform content permissions apply, see Tanium Console User Guide: View effective role permissions.

Endpoint information collection

Device Management uses the following sensors to collect information about the endpoints enrolled with Device Management. The information that is collected enables identification and auditing of devices and enables Tanium to target configuration profiles to endpoints or groups of endpoints.

- **Device Management - Device ID**
- **Device Management - Enrollment Type**
- **Device Management - Is Supervised**

© 2026 Tanium Inc. All Rights Reserved

Configuring Device Management

Set up Device Management users

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 15.

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

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.
- 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.

© 2026 Tanium Inc. All Rights Reserved

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

Configure an Apple Push Certificate to use with Device Management

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



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.

Before you begin

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



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 57.



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.

© 2026 Tanium Inc. All Rights Reserved

Request and upload the Apple Push Certificate

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

   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 Architecture on page 8.

   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**.

(Automated device enrollment) Configure an identity provider

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

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: Configuring Identity Providers to use with Device Management on page 62.

© 2026 Tanium Inc. All Rights Reserved

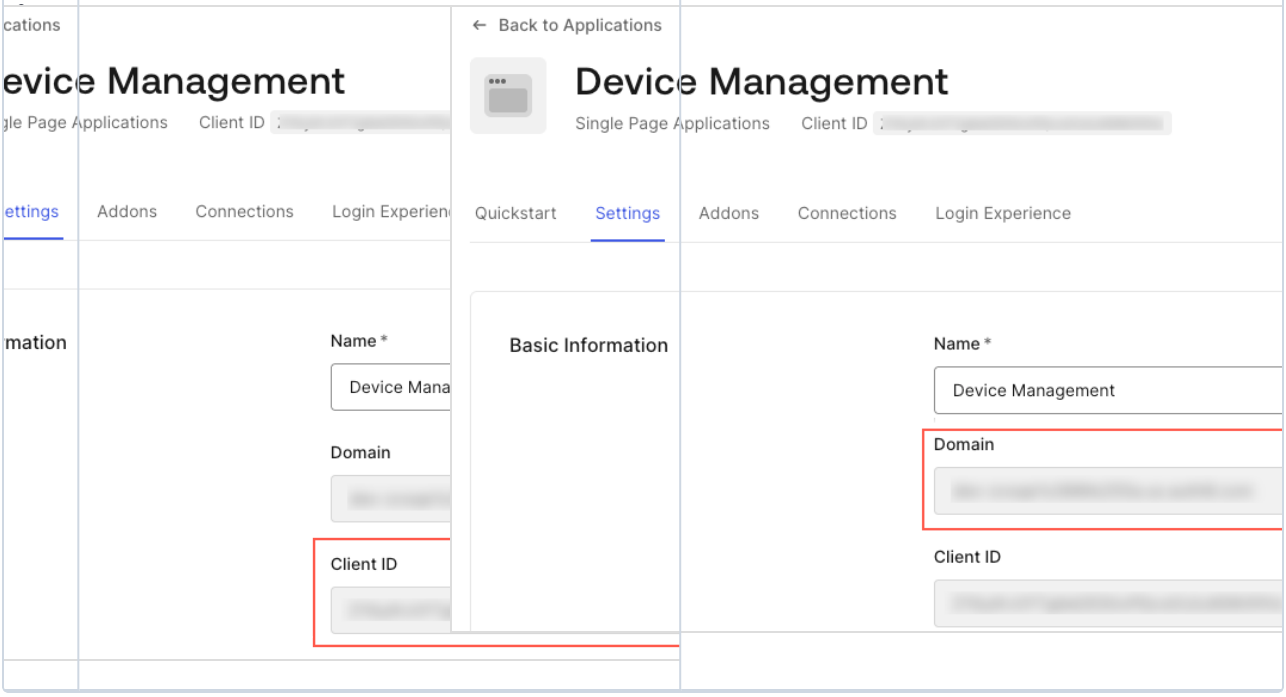
1. From the Main menu, go to **Shared Services > Device Management**. Click Settings and then click **IDP Configuration**.
2. Update your IdP with the **Redirect URI**. Your IdP redirects users to this URI. The redirect URI is required for your IdP to integrate with Device Management.
3. Enter the **Client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

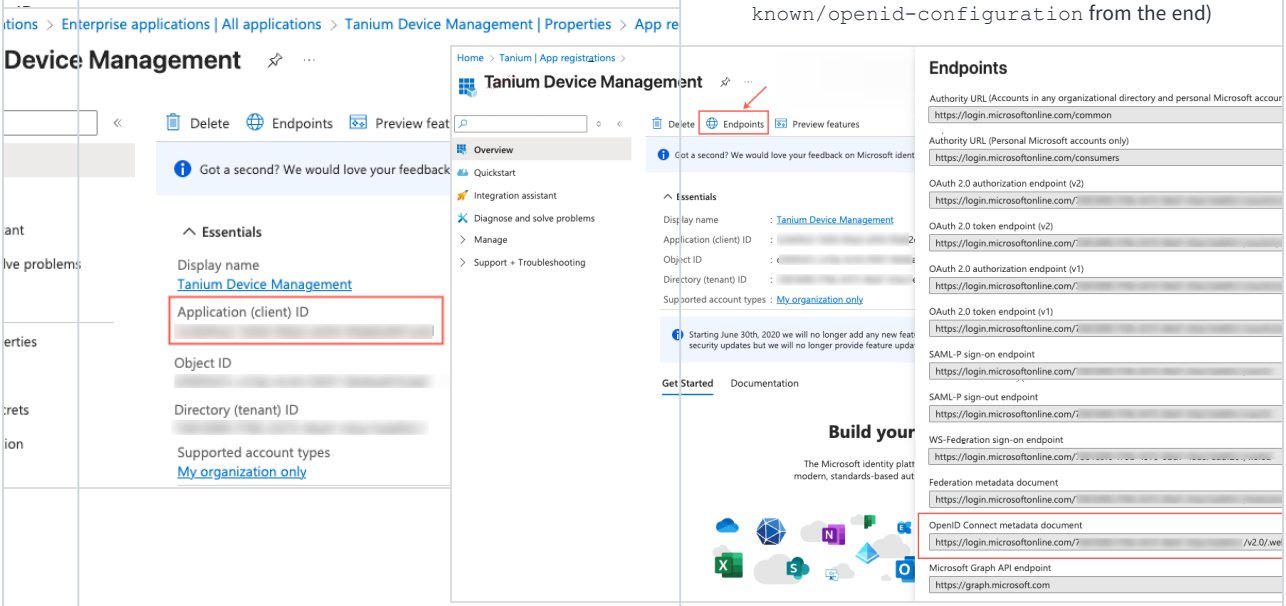
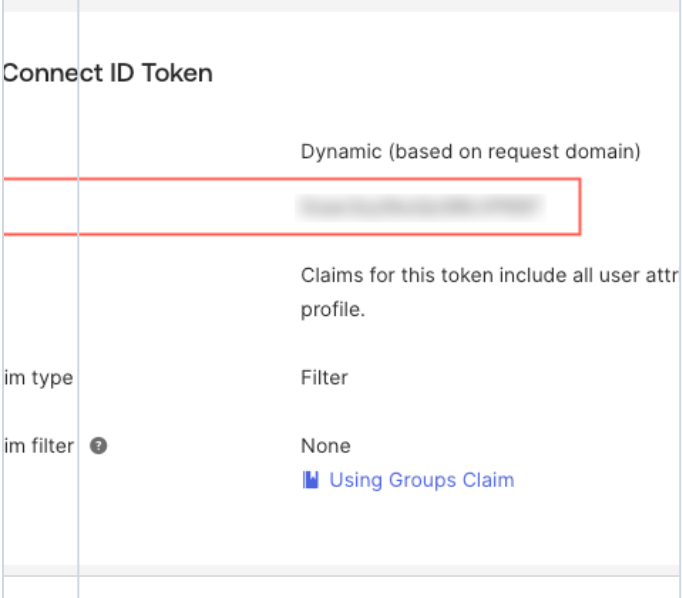
Client IDs and Issuers for IdPs

Identity Provider	Use this value for Client ID	Use this value for Issuer
auth	**Client ID**	**Domain** (add `https://` to the beginning)



© 2026 Tanium Inc. All Rights Reserved

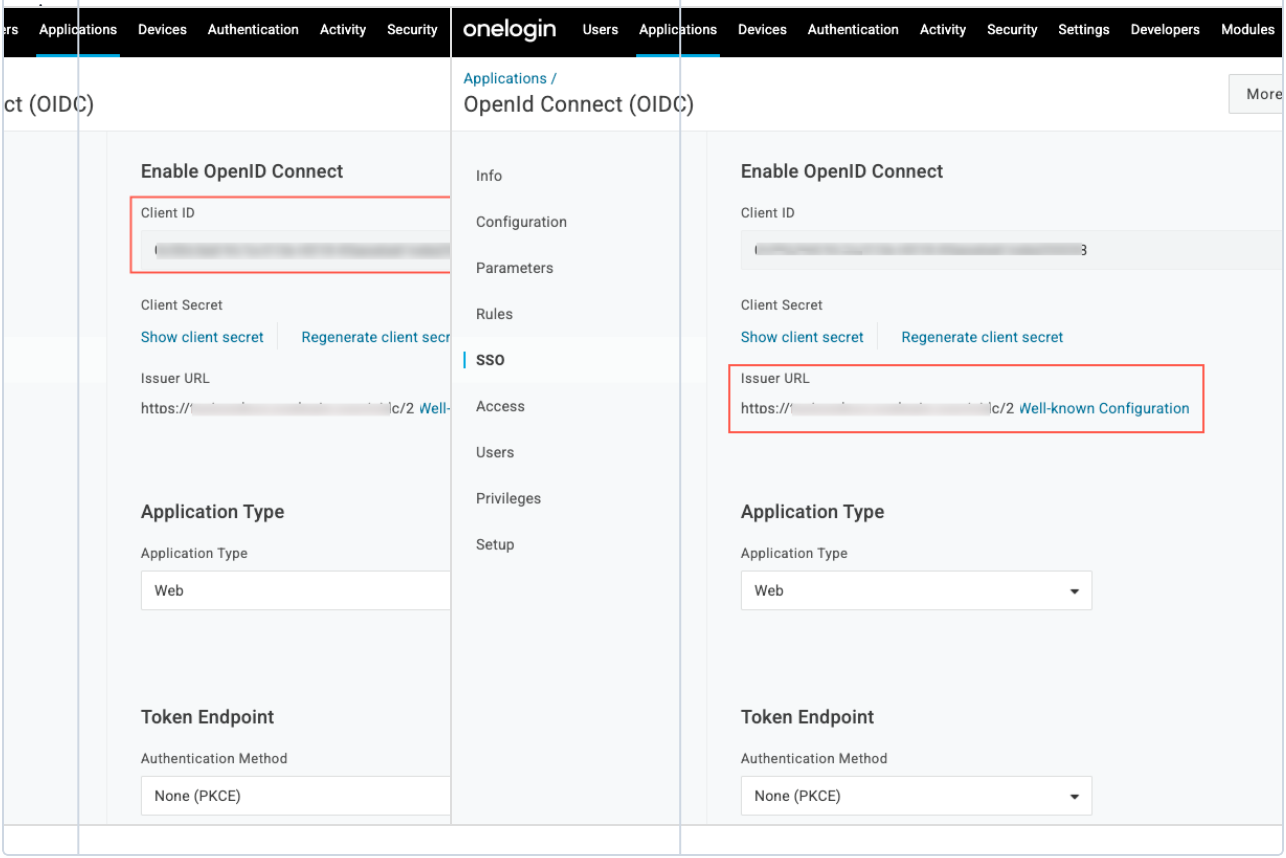
Client IDs and Issuers for IdPs (continued)

Identity Provider	Use this value for Client ID	Use this value for Issuer
Entra	**Application (client) ID** 	**OpenID Connect metadata document** (omit the `/.well-known/openid-configuration` from the end)
Okta	**Audience** 	Okta instance URL

© 2026 Tanium Inc. All Rights Reserved

Client IDs and Issuers for IdPs (continued)

Identity Provider	Use this value for Client ID	Use this value for Issuer
OneL	**Client ID**	**Issuer URL**



4. Click **Apply**.

(Optional) Configure automated enrollment using 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 devices.

© 2026 Tanium Inc. All Rights Reserved

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 Configure an Apple Push Certificate to use with Device Management.
- Configure an identity provider. For more information, see (Automated device enrollment) Configure an identity provider on page 21.

Configure the enrollment system

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.
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.

© 2026 Tanium Inc. All Rights Reserved

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**.
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**.
12. Click **Save**.

(Optional) Configure Custom Tags for devices

A custom tag is a user-defined label that you can assign to, or unassign from, endpoints. Tags are useful for defining computer group membership if you sometimes want to change which endpoints are members. For more information, see 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.

© 2026 Tanium Inc. All Rights Reserved

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 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

        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

Migrating from Tanium Mac Device Enrollment to Device Management

Tanium Mac Device Enrollment is deprecated as of December 15, 2025, and will sunset September 1, 2026. Migrate your existing MDM settings and devices to Device Management.

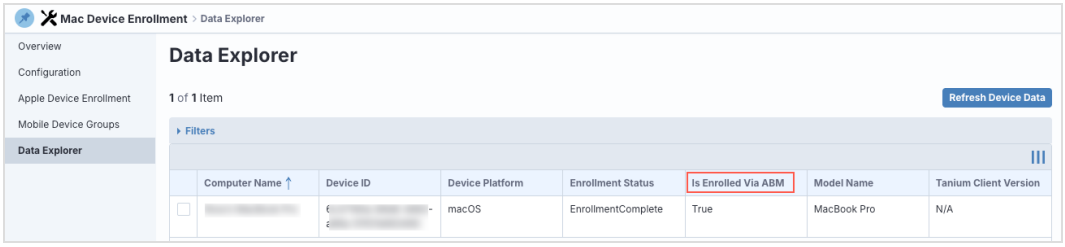
Step 1: Scope and inventory

Review and inventory the existing enrollment profiles, settings, and enrolled devices to determine the scope of the migration:

Tanium Mac Device Enrollment

Review the settings and applications configured in Mac Device Enrollment profiles. For more information, see Tanium Mac Device Enrollment User Guide: View and edit enrollment profiles.

Inventory the enrolled devices and the enrollment method that was used for the devices (automated through Apple Business or School Manager or user-assisted through the Tanium Mac Device Management enrollment portal). One way to determine how a device was enrolled is from the **Data Explorer** page in Mac Device Enrollment.



TIP

You might need to add the **Is Enrolled Via ABM** column on this page. To add this column, click Customize Columns and select **Is Enrolled Via ABM**.

Tanium Patch

Review the configured settings. For more information, see Tanium Patch User Guide: Configuring settings for Mac.

Tanium Enforce

Review configured Mac Device Configuration Profile policies enforced on enrolled devices. From the Main menu, go to **Modules > Enforce > Policy Configuration**. Click **Apple** to filter the list to show only Mac policies. Compile a list of settings to recreate in Device Management.

© 2026 Tanium Inc. All Rights Reserved

Step 2: Configure Device Management

Configure Device Management. For more information, see Configuring Device Management.

Step 3: Recreate Mac Device Enrollment settings and applications in Device Management

Recreate the settings and applications in Device Management and create collections to group the applications and settings to apply to target devices. For more information, see Managing settings, Add an enterprise application, and Managing collections. During this stage, Mac Device Enrollment remains active (independent from Device Management).

Step 4: Pilot enrollment

Enroll several devices in Device Management as a pilot. Target collections to these devices to validate settings, applications, and reporting. For more information, see Managing collections and Working with devices and device data.

Step 5: Migrate devices

Enroll the remaining devices into Device Management.

Migrate devices that were enrolled in Mac Device Enrollment using automated device enrollment

If a device is running macOS 26 or later and enrolled with Mac Device Enrollment using automated device enrollment (Apple Business Manager or Apple School Manager), you can migrate the device to Device Enrollment using the applicable Apple enrollment service. For more information, see:

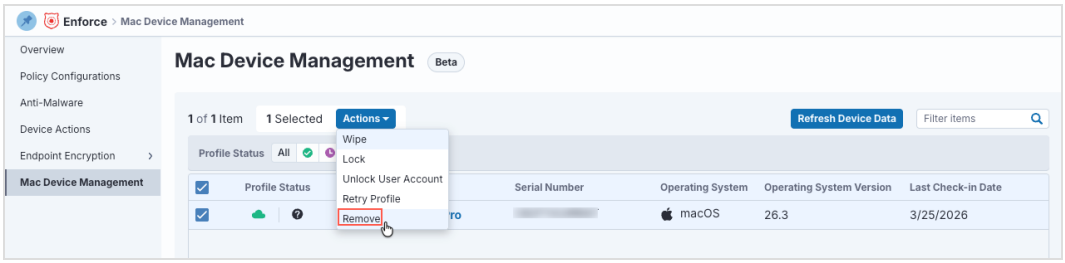
- Apple Platform Deployment Documentation: Migrate managed devices to another device management service
- Apple Business Manager User Guide: Migrate devices to a new management service in Apple Business Manager
- Apple School Manager User Guide: Migrate devices to a new management service in Apple School Manager

Migrate Devices that were enrolled in Mac Device Enrollment using the Mac Device Management enrollment portal

For devices that enrolled with Mac Device Enrollment using the Tanium Mac Device Management enrollment portal (user-assisted enrollment), you must remove the device from Mac Device Enrollment and remove the enrollment profile from the device before you can migrate the device to Device Management. One way to remove the device from Mac Device Management is to use the Mac Device Management page in Enforce. From the Main menu, go to **Modules > Enforce > Mac Device Management**. Select one or

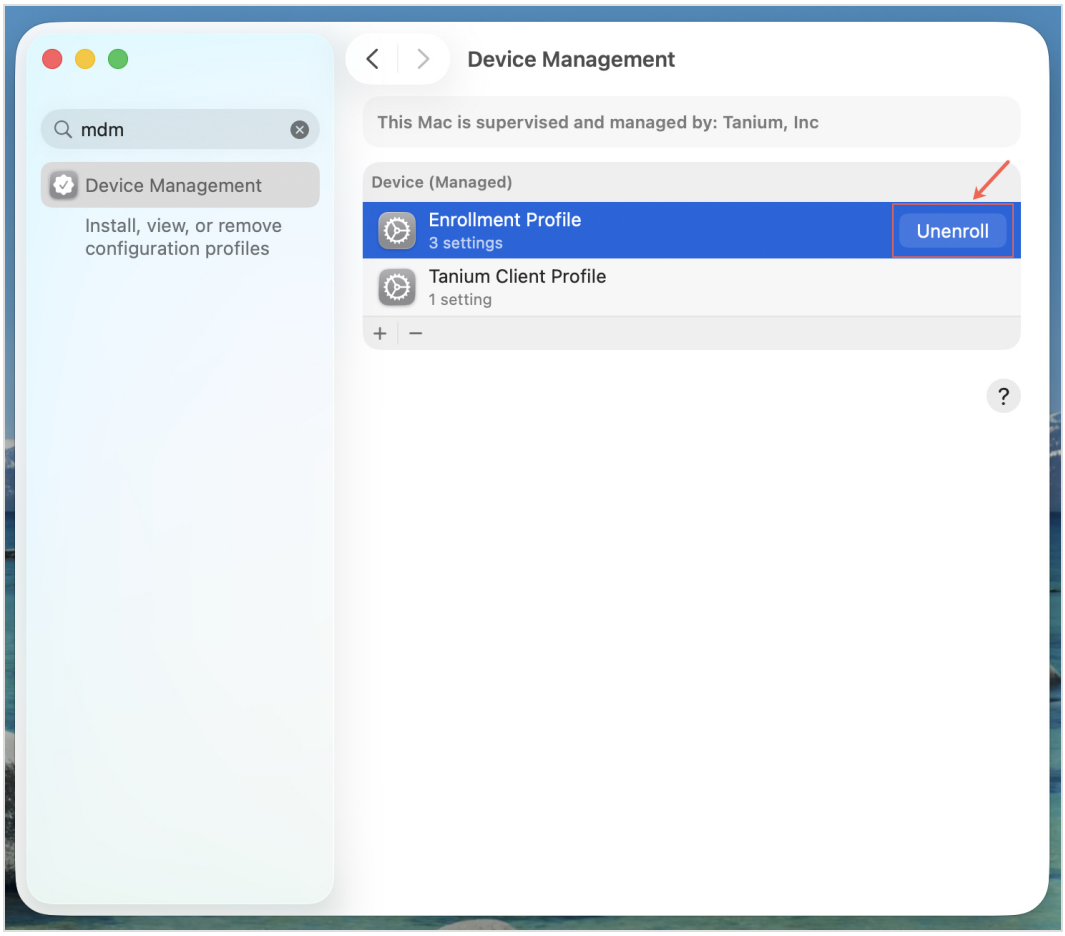
© 2026 Tanium Inc. All Rights Reserved

more devices and click **Actions > Remove**.



This action should automatically remove the Mac Device Enrollment profile from the device.

If needed, the user can manually unenroll by clicking **Unenroll** next to the enrollment profile in the macOS system settings.



This option is available only for devices that enrolled using the Tanium Mac Device Management enrollment portal (user-assisted/manual enrollment). For more information, see Mac User Guide: Change Device Management settings on Mac.

After the Mac Device Enrollment profile is removed from the device, enroll the device with Device Management. For the best experience, use the automated device enrollment method. For more information, see (Optional) Configure automated enrollment using an Apple enrollment system.

© 2026 Tanium Inc. All Rights Reserved

NOTE

Devices that were enrolled using the Tanium Mac Device Management enrollment portal (user-assisted enrollment) might need to be wiped and re-enrolled.

Apply settings to migrated devices

Target collections to the migrated devices to validate settings, applications, and reporting. For more information, see Managing collections and Working with devices and device data.

Step 6: Retire Mac Device Enrollment

Disable Mac Device Enrollment content after policy parity and adoption thresholds are reached.

© 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.

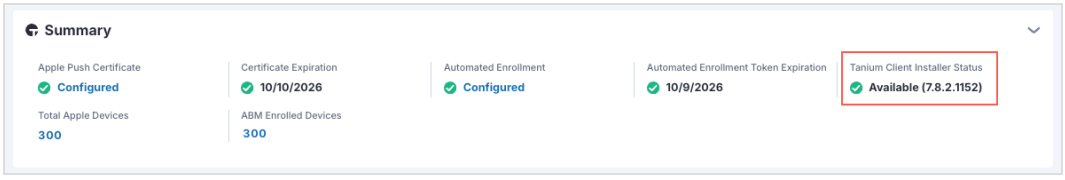
Overview

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 Configure an Apple Push Certificate to use with Device Management.
- 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: Create a Client deployment template and Select a Tanium Client deployment template.

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)**).



- **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, the Tanium Client pushes out to enrolled devices. 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.

© 2026 Tanium Inc. All Rights Reserved

Select a Tanium Client deployment template

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

Select the 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**.

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

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 (Optional) Configure automated enrollment using an Apple enrollment system on page 24.
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 Managing settings on page 35.
3. Create collections to target settings to these devices. For more information, see Managing collections on page 45.

Manual enrollment

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



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

Managing settings

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

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 > 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

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 > Settings**.
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

© 2026 Tanium Inc. All Rights Reserved

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 are not available through the encryption key recovery portal.

6. Click **Save**.

Delete a setting

IMPORTANT

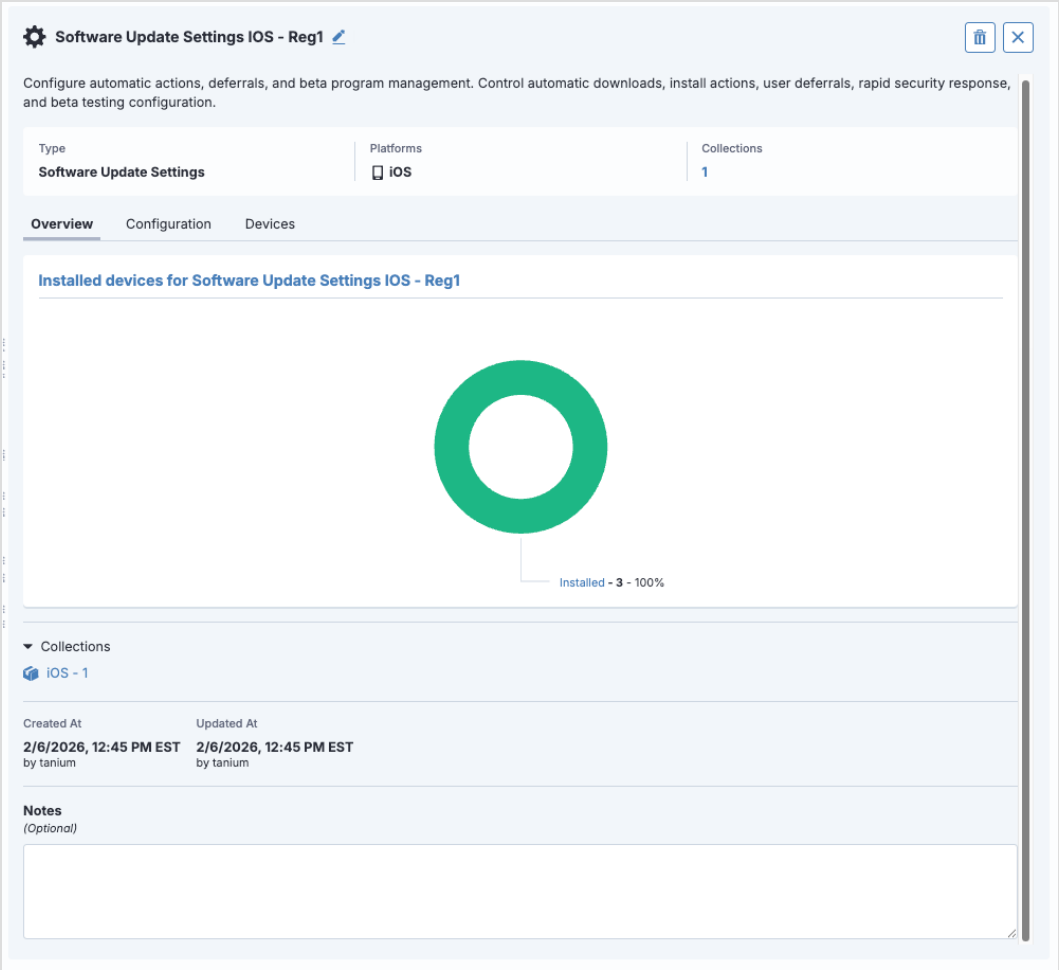
You can delete settings that are used in collections. Confirm the usage and deployment before you delete a setting.

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

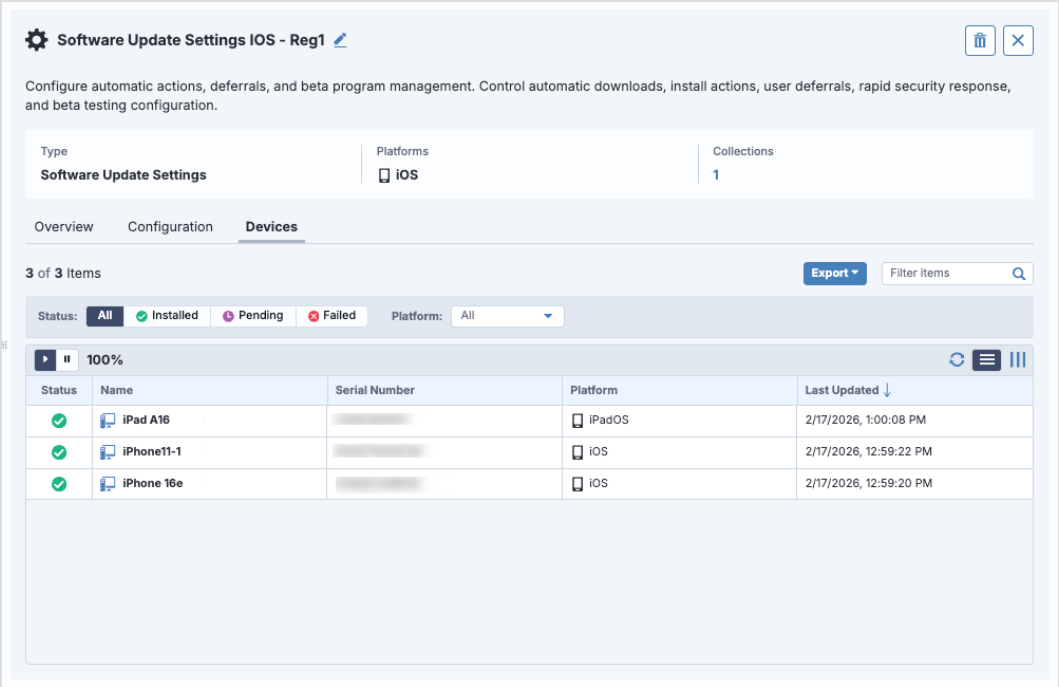
© 2026 Tanium Inc. All Rights Reserved



- (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.

© 2026 Tanium Inc. All Rights Reserved

- The **Devices** tab shows details about the endpoints where the settings are applied.



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 Managing collections.

© 2026 Tanium Inc. All Rights Reserved

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

Define the device software update settings and restrictions.

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

Define the update deadlines and target build versions.

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

© 2026 Tanium Inc. All Rights Reserved

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 Managing settings.
- To target these settings to devices, create a collection and target the collection to a group of devices. For more information, see Managing collections.

© 2026 Tanium Inc. All Rights Reserved

Managing web clips and applications

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

You can create configurations for web clips, which add a shortcut to a website on a user's Home Screen and enterprise applications. For more information about web clips, see Apple documentation: Web Clips device management payload settings for Apple devices.

(macOS) Add an enterprise application

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

   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 > 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.

© 2026 Tanium Inc. All Rights Reserved

6. For the **Is Removable** field, select **Yes** if you want to allow the user to remove the web clip from their 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**.

Delete a web clip or application



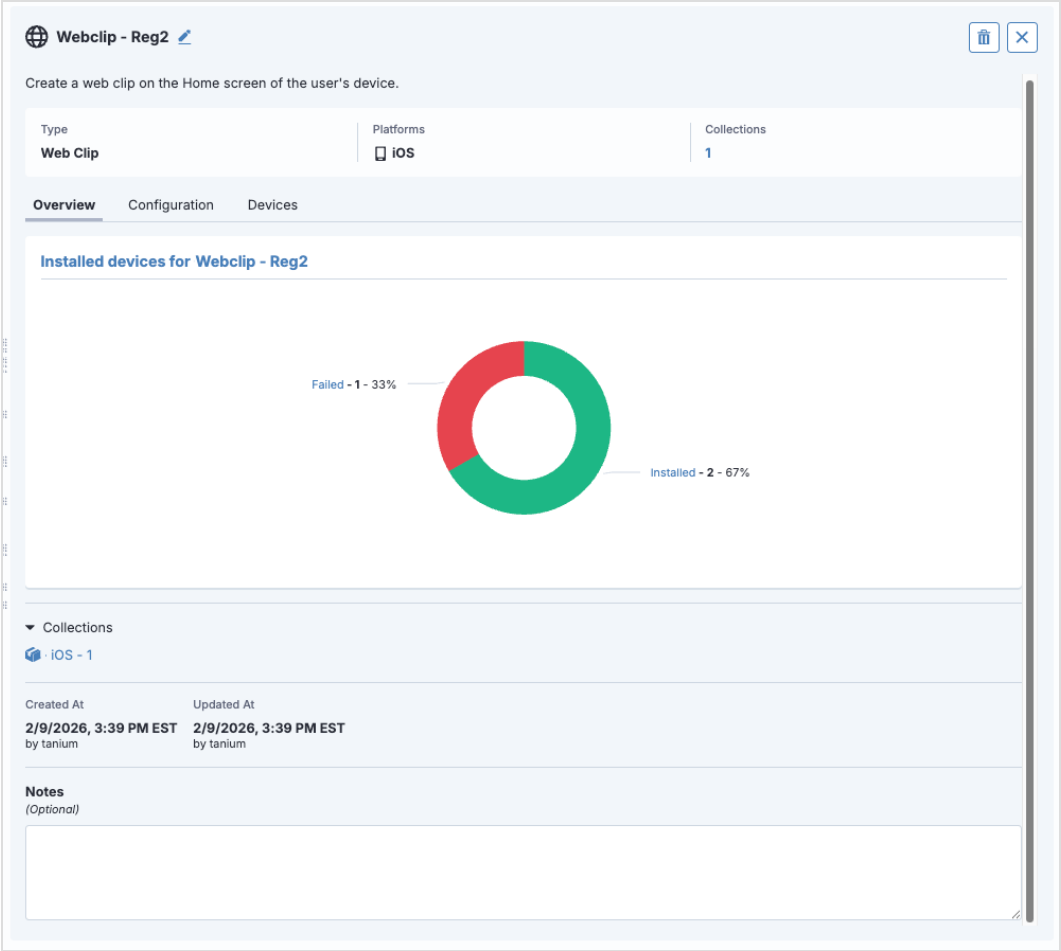
You can delete web clips and applications that are used in collections. Confirm the usage and deployment before you delete them.

1. From the Main menu, go to **Shared Services > Device Management > Applications**.
2. In the **Applications** list, click on 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 > Applications**.
2. In the **Applications** list, click on the name of the web clip or application that you want to review.
    - On the **Overview** tab, you can see 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 on a status in the donut chart to see a list of the endpoints with that status.

© 2026 Tanium Inc. All Rights Reserved

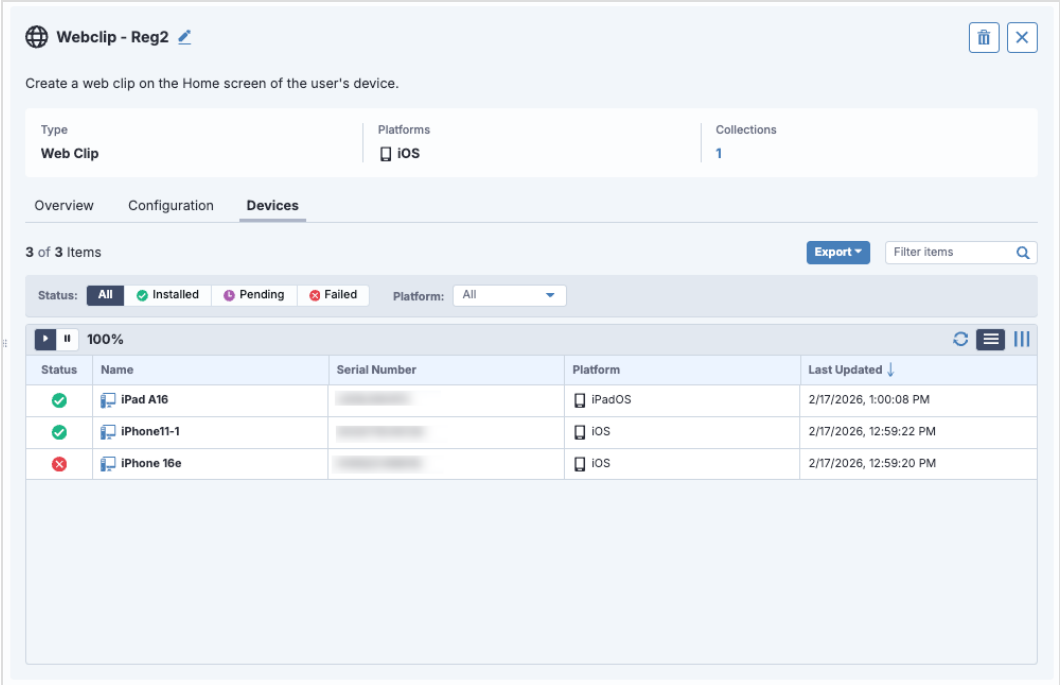


- The **Configuration** tab shows the configuration for the application or web clip.

> **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.

© 2026 Tanium Inc. All Rights Reserved

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



What to do next

To install enterprise applications and configure web clips on devices, create a collection and target the collection to a group of devices. For more information, see Managing collections.

© 2026 Tanium Inc. All Rights Reserved

Managing collections

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

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 Managing settings on page 35 and Managing web clips and applications.

Create a collection

1. From the Main menu, go to **Shared Services > Device Management > 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 application or web clip that you want to add to the collection and click **Next**.
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 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**).

© 2026 Tanium Inc. All Rights Reserved

- 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

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.

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

IMPORTANT

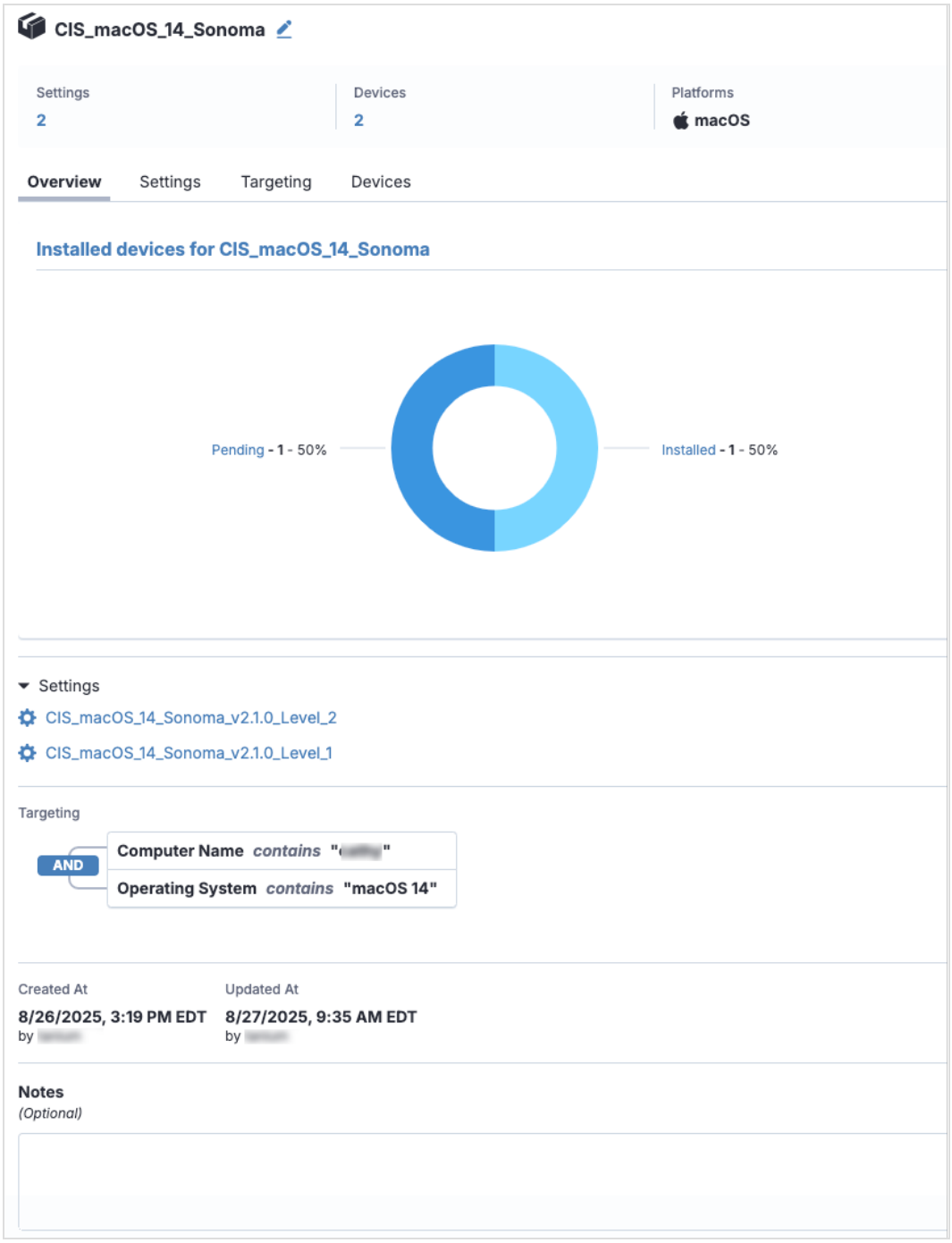
You can delete collections that are applied to devices. Confirm the usage and deployment before you delete a collection.

1. From the Main menu, go to **Shared Services > Device Management > Collections**.
2. In the **Collections** list, click on 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 > Collections**.
2. In the **Collections** list, click on 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 on a status in the donut chart to see a list of the devices with that status.

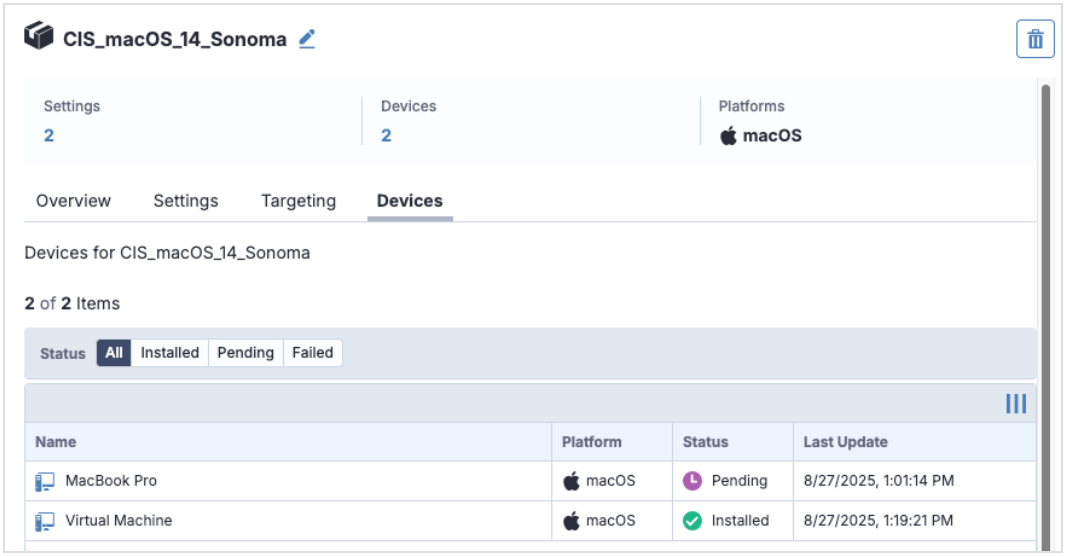
© 2026 Tanium Inc. All Rights Reserved



- The **Settings** tab shows the settings in the collection. Click on the name of the setting to review the details. Click to add or remove settings from the collection.

© 2026 Tanium Inc. All Rights Reserved

- The **Applications** tab shows the applications and web clips in the collection. Click on 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.
- 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.



© 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. This dashboard shows the following panels:

Devices by Type

Shows the number of macOS and iOS devices over time.

iOS Devices by Version

Shows the current iOS devices by operating system version.

Mac Devices by Version

Shows the current macOS devices by operating system version.

Devices Checked in By Day

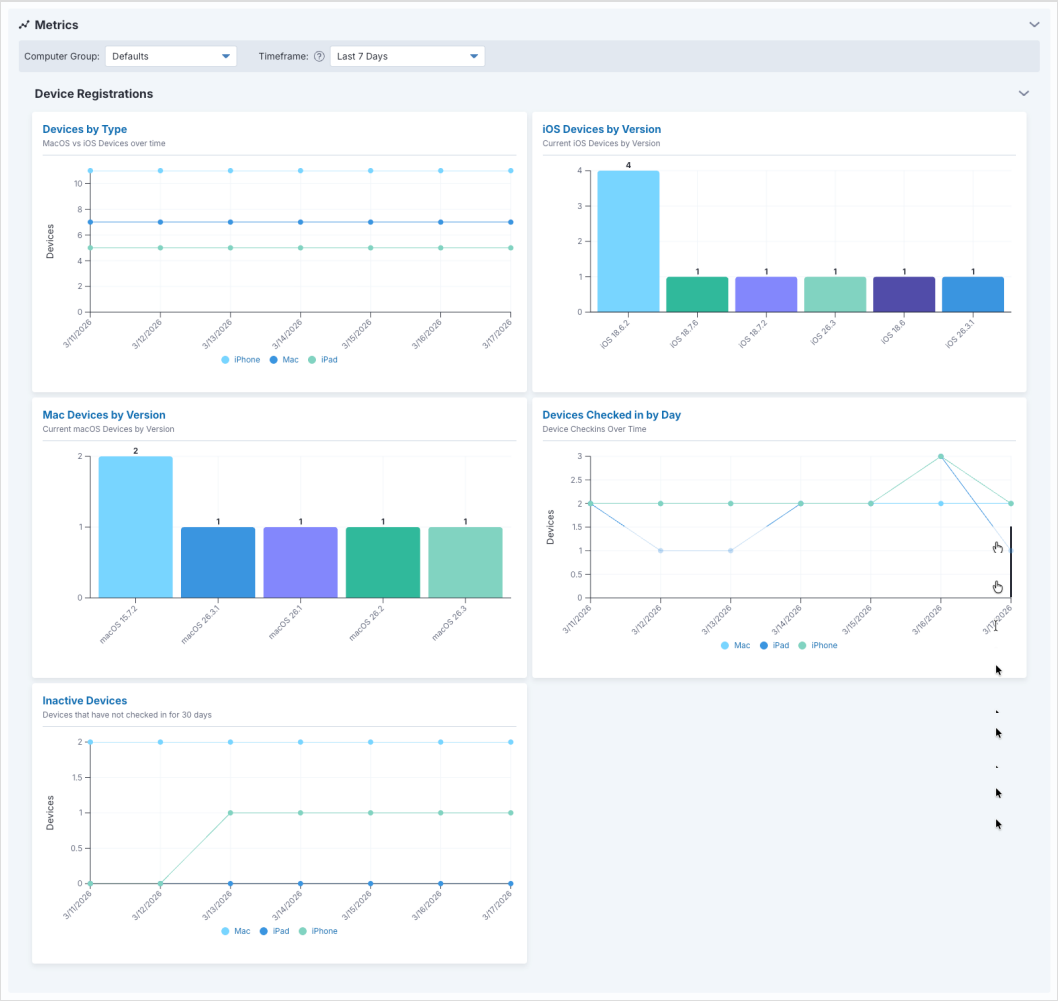
Shows the devices that check in over time.

Inactive Devices

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

Metrics on the Device Management Overview page

© 2026 Tanium Inc. All Rights Reserved



View the details for a device

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

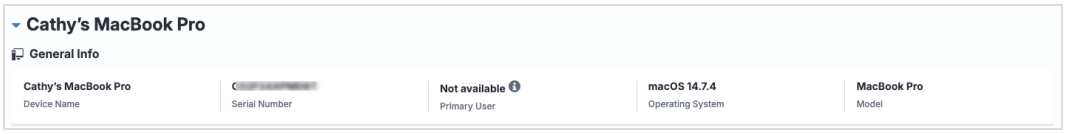
- The Endpoint Details page for devices enrolled with Device Management cannot be customized.
- To view device details, you must have the **Device Management Single Endpoint** permission.

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.

© 2026 Tanium Inc. All Rights Reserved

General Info



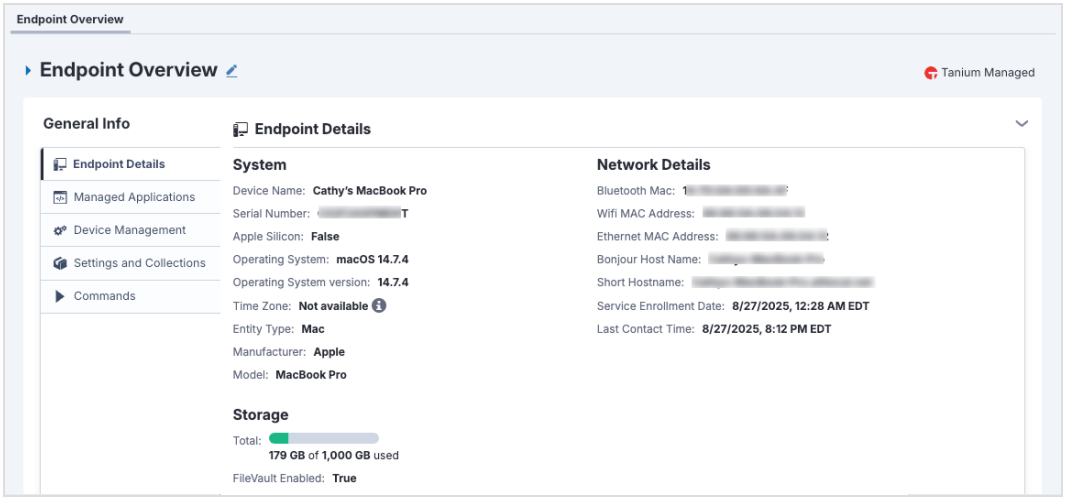
Endpoint Overview

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

Endpoint Details

Shows detailed information about the device.

Endpoint Details



Managed Applications

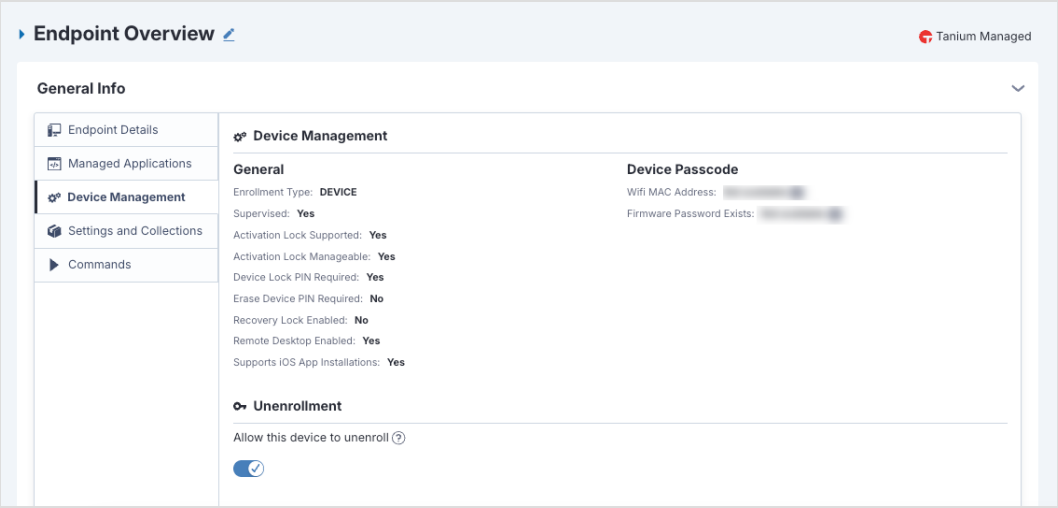
Shows the applications installed on the device.

Device Management

Shows device management settings for the device, such as enrollment type.

© 2026 Tanium Inc. All Rights Reserved

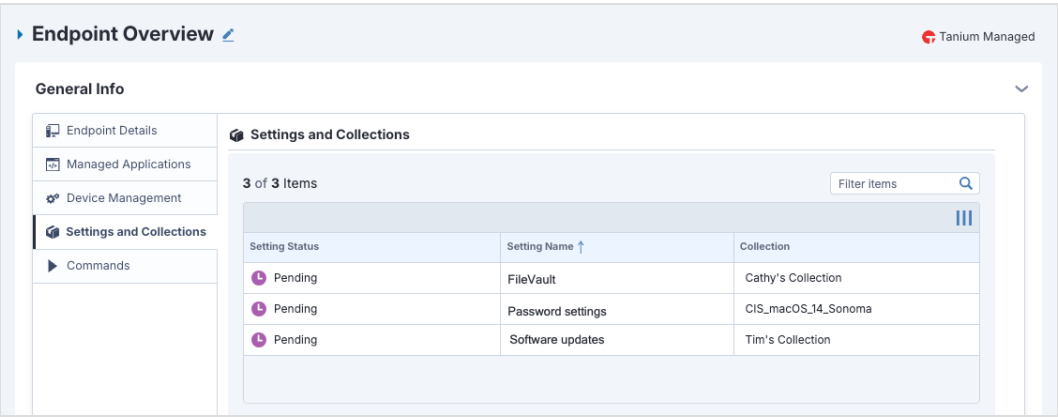
Device Management tab



Settings and Collections

Shows the status of collections targeted to the device. For more information about collections, see Managing collections on page 45.

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.

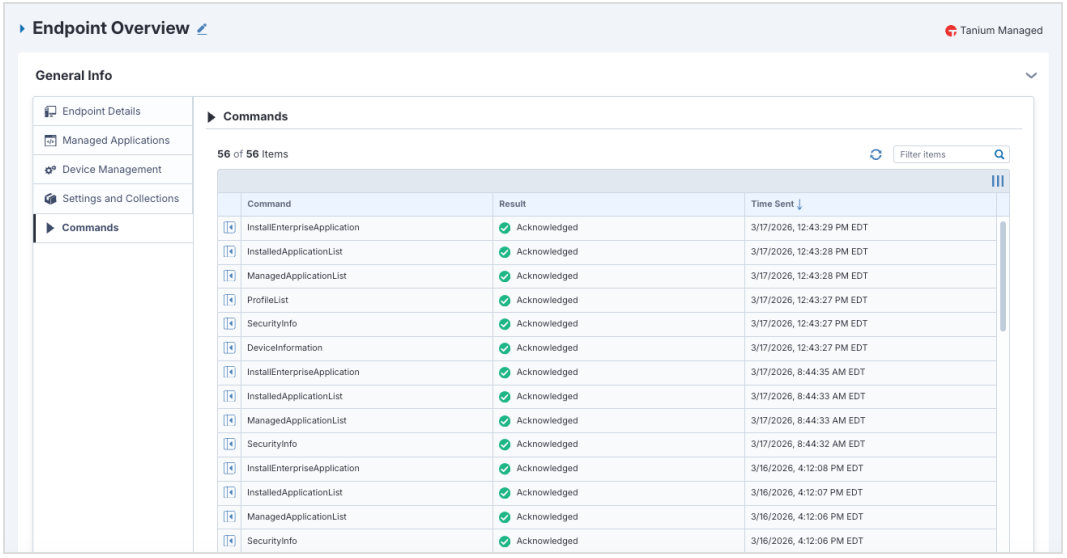
© 2026 Tanium Inc. All Rights Reserved

Commands

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.

Commands tab



Deploy actions on a device

You can deploy the following actions on a single device through the Endpoint Details page in Tanium Reporting: Restart, Erase Device, Shut Down Device, Unenroll Device, and Lock Device. To perform these actions, you must have the **Device Management Push Command** permission.

© 2026 Tanium Inc. All Rights Reserved

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

Endpoint actions

Action	Description	Parameters
Lock Device	Lock a device, show a custom message, and require the configured PIN to access the device.	• **Message to display on lock screen** • **Phone Number to display on lock screen** • **Recovery PIN** For more information, see Apple Platform Deployment Documentation: Lock and locate Apple devices.
Erase Device	Erase (or wipe) all content from the device.	• **Disallow proximity setup** • **Recovery PIN** • **Obliteration behavior** • **Preserve cellular data plan for eSIM device**
Refresh Device Data	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 Device	Restart the device.	• **Notify user** • **Rebuild kernel cache**
Shut Down Device	Remove company data and settings from a device, and leave personal data intact.	none
Unenroll Device	Unenroll the device from Device Management.	none



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.

3. Click **Deploy Action**.

© 2026 Tanium Inc. All Rights Reserved

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)
Tanium Endpoint Management for Operational Technology	Operational Technology	*<configured-entity-provider-name>*	Operational Technology Device

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 Tanium Client:

```
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
```

© 2026 Tanium Inc. All Rights Reserved

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.

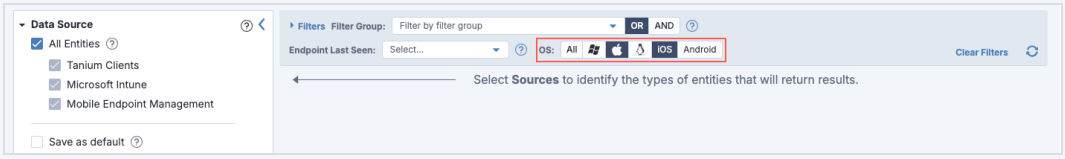
    NOTE

    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 to show only devices running the macOS or iOS (which includes iPadOS) operating system.

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

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.



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.

RENEW YOUR 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.

   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

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.

© 2026 Tanium Inc. All Rights Reserved

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

   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 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.

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

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.

© 2026 Tanium Inc. All Rights Reserved

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.

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 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 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}]
```

Contact Tanium Support

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

© 2026 Tanium Inc. All Rights Reserved

For more information about how to submit a support case, see Case Submission Form.

© 2026 Tanium Inc. All Rights Reserved

Reference: 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

Before you configure an IdP, you must configure an Apple Push Certificate to use with Device Management. For more information, see Configure an Apple Push Certificate to use with Device Management on page 20. 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:

© 2026 Tanium Inc. All Rights Reserved

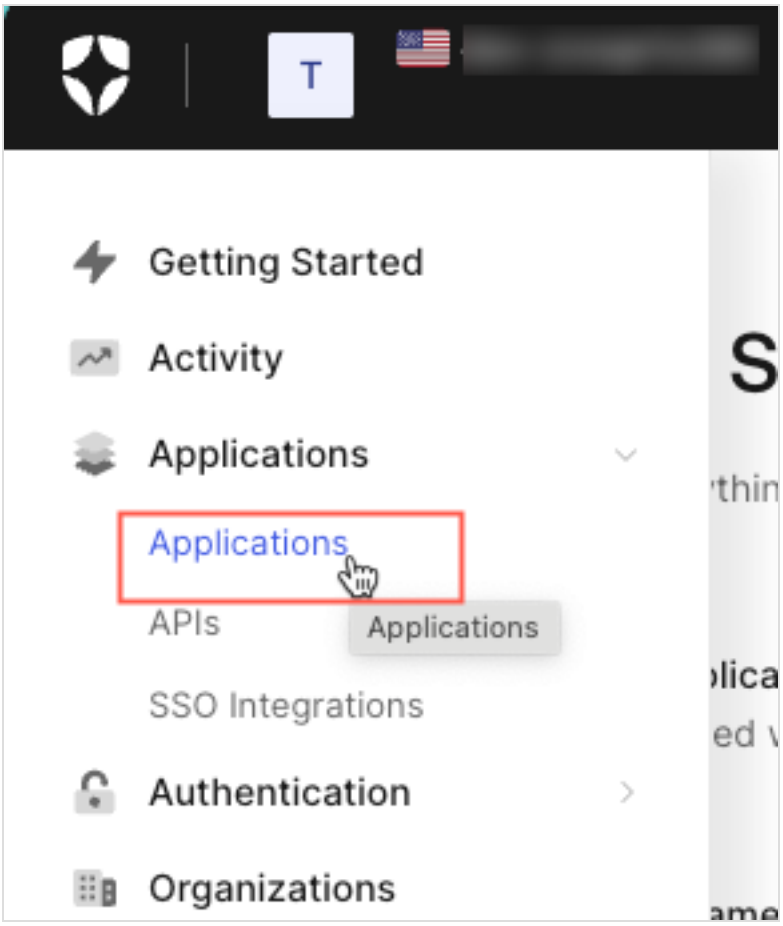
- **OAuth flow:** Authorization Code with Proof Key for Code Exchange (PKCE). Configure the application as a public client (Single Page Application) with no client secret.
- **Scopes:** Grant the `openid`, `email`, and `profile` scopes to the application.
- **ID token claims:** The ID token must include 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 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

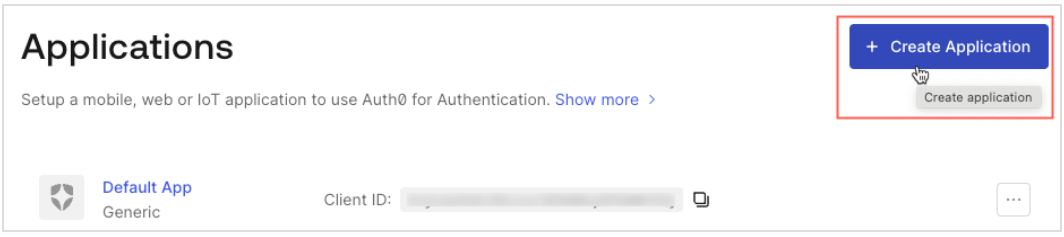
For more information about configuring auth0, see auth0 documentation: Applications in Auth0.

© 2026 Tanium Inc. All Rights Reserved

1. From the auth0 menu, click **Applications > Applications**.

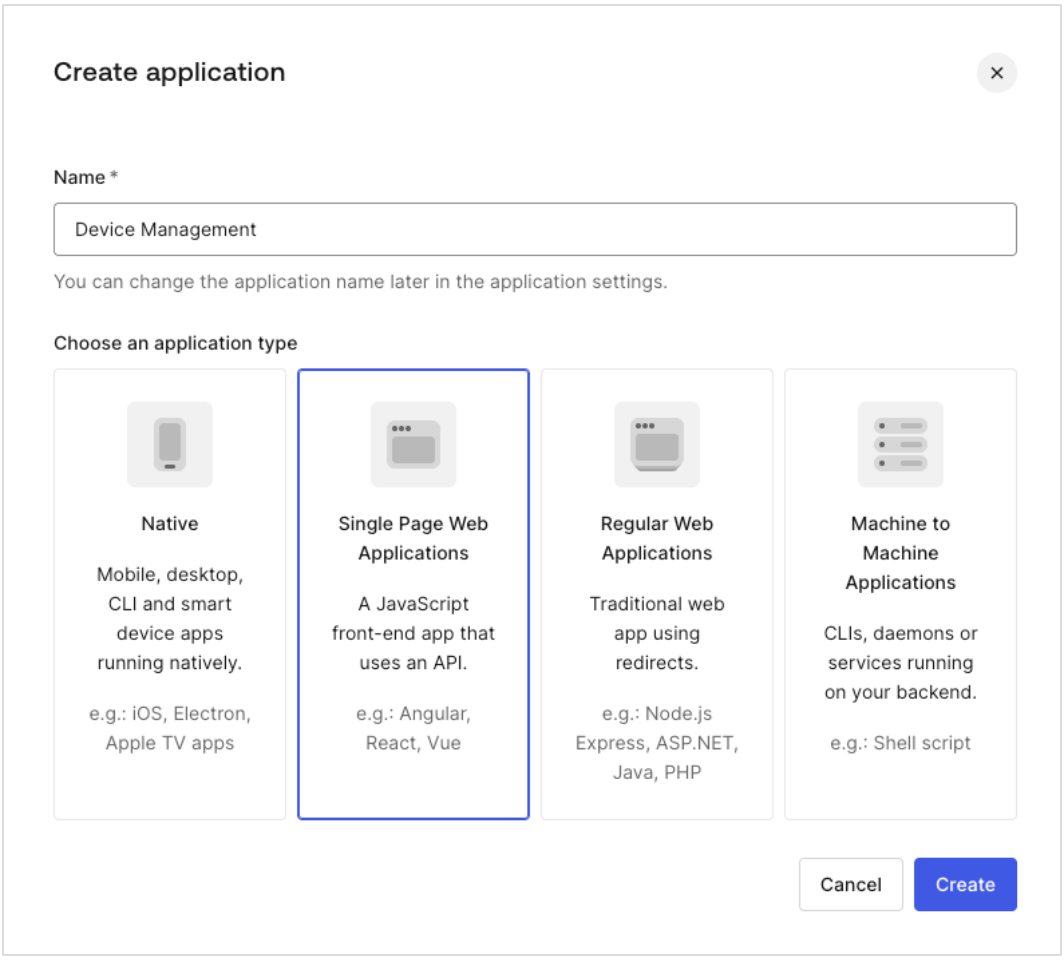


2. Click **Create Application**.

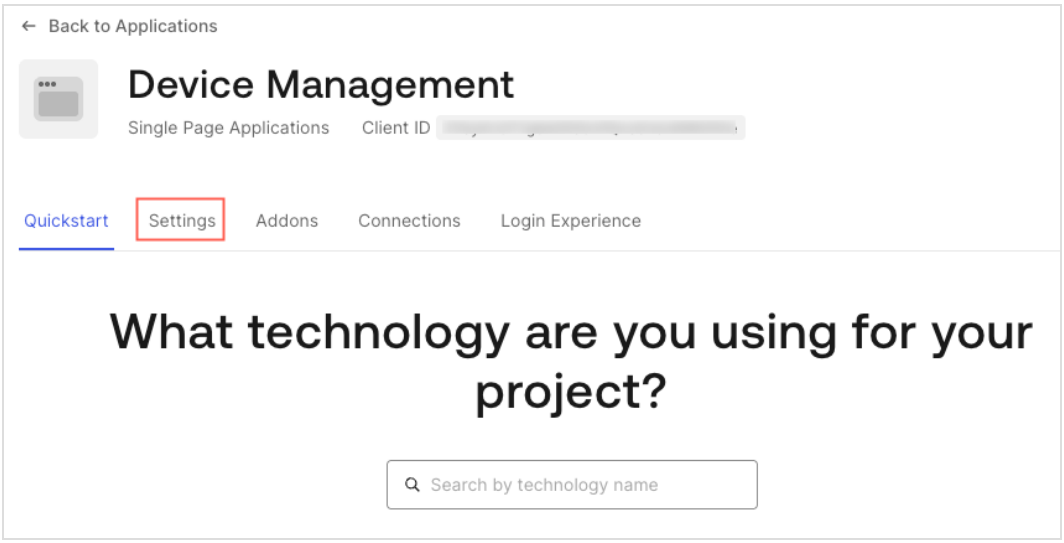


© 2026 Tanium Inc. All Rights Reserved

3. Specify a **Name** for the application and select **Single Page Web Application**. Click **Create**.

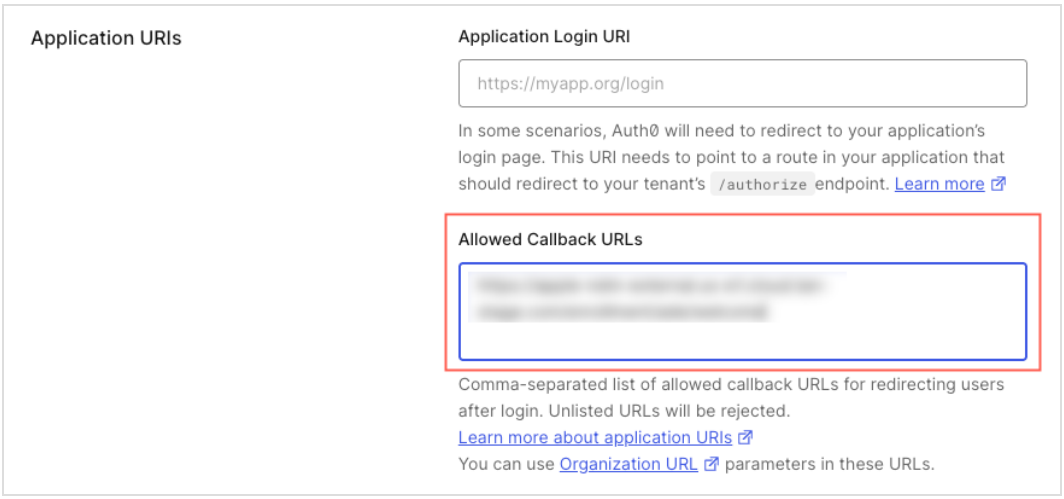


4. On the application page, click the **Settings** tab.

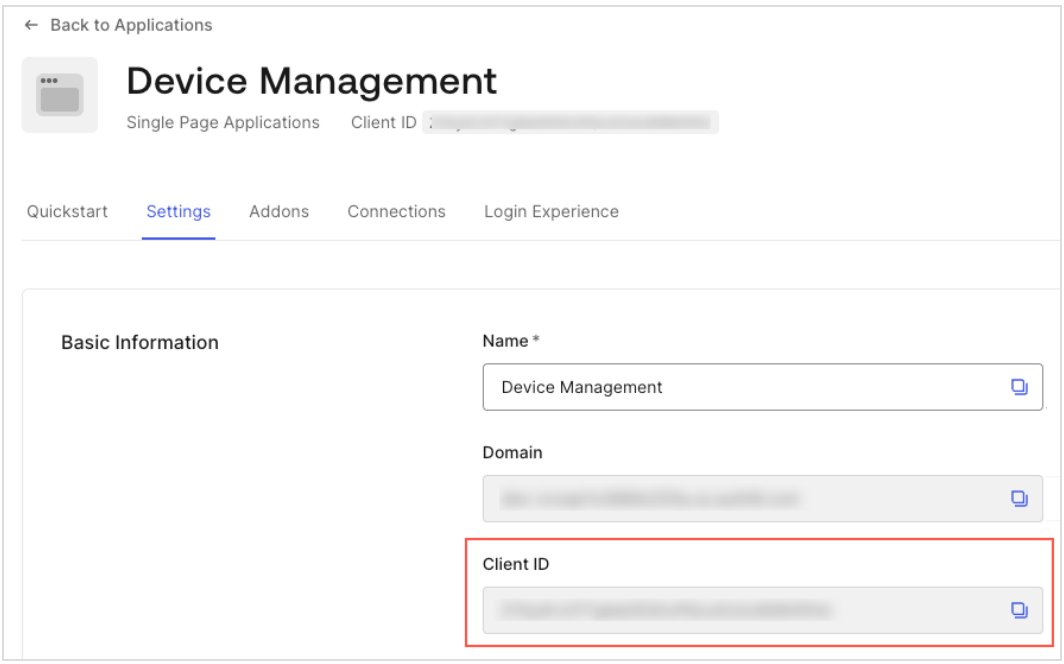


© 2026 Tanium Inc. All Rights Reserved

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



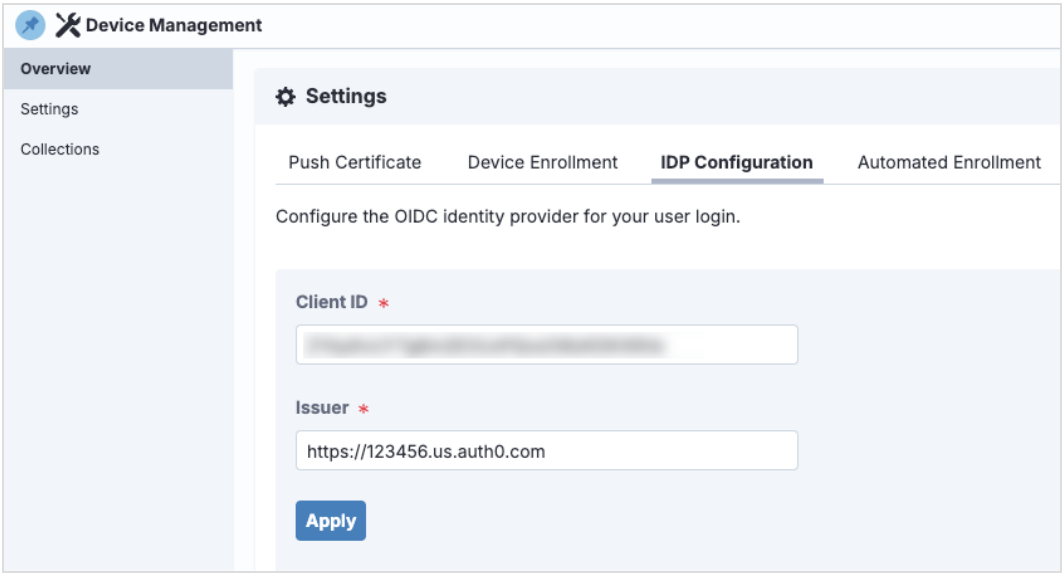
6. Copy the **Domain** and **Client ID** from the application details and save it for use in Device Management.



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

© 2026 Tanium Inc. All Rights Reserved

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**.

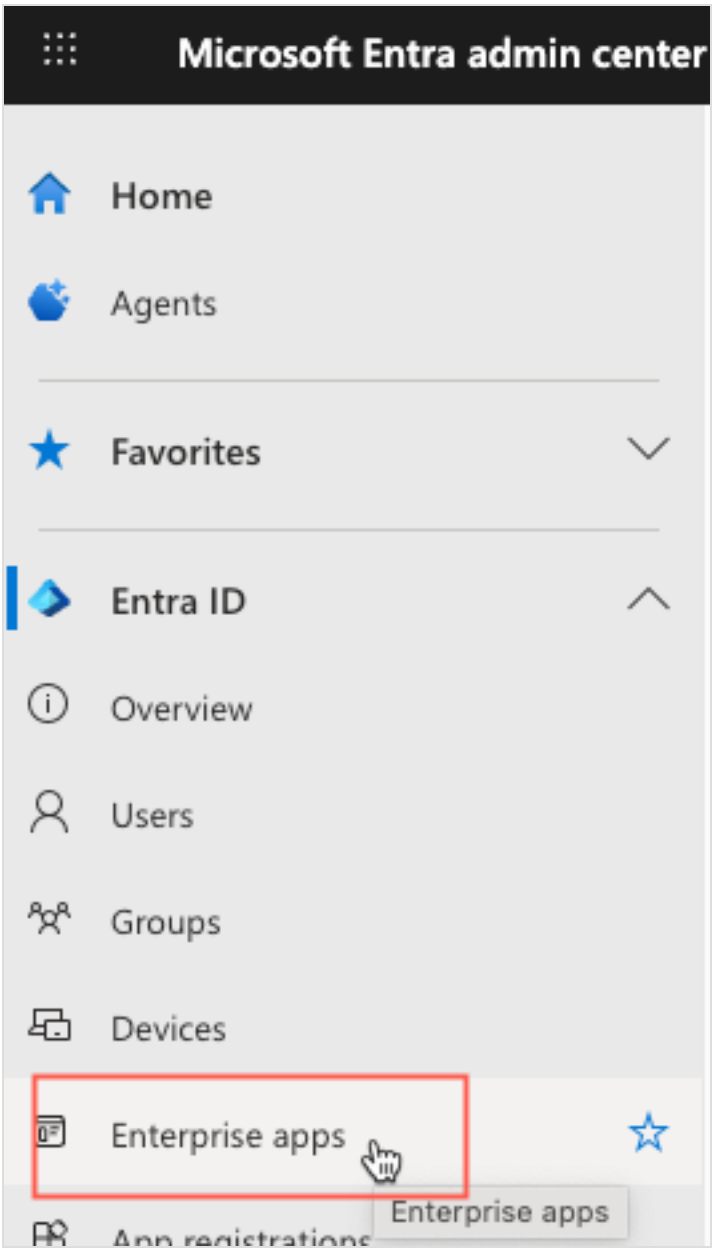


Microsoft Entra ID

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

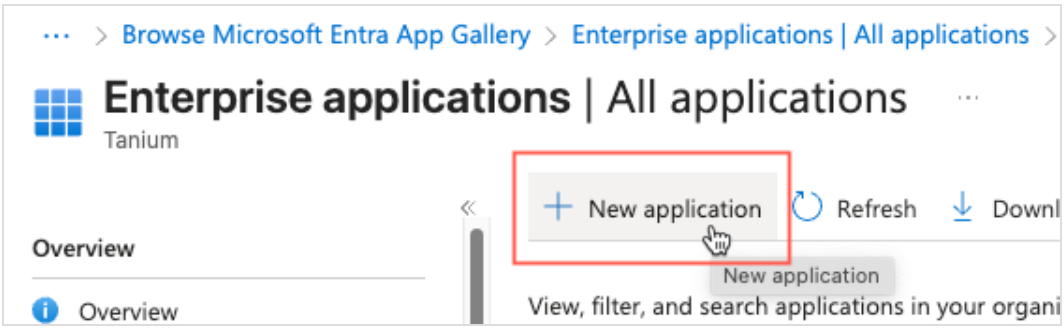
© 2026 Tanium Inc. All Rights Reserved

1. From the Entra menu, click **Enterprise Applications**.

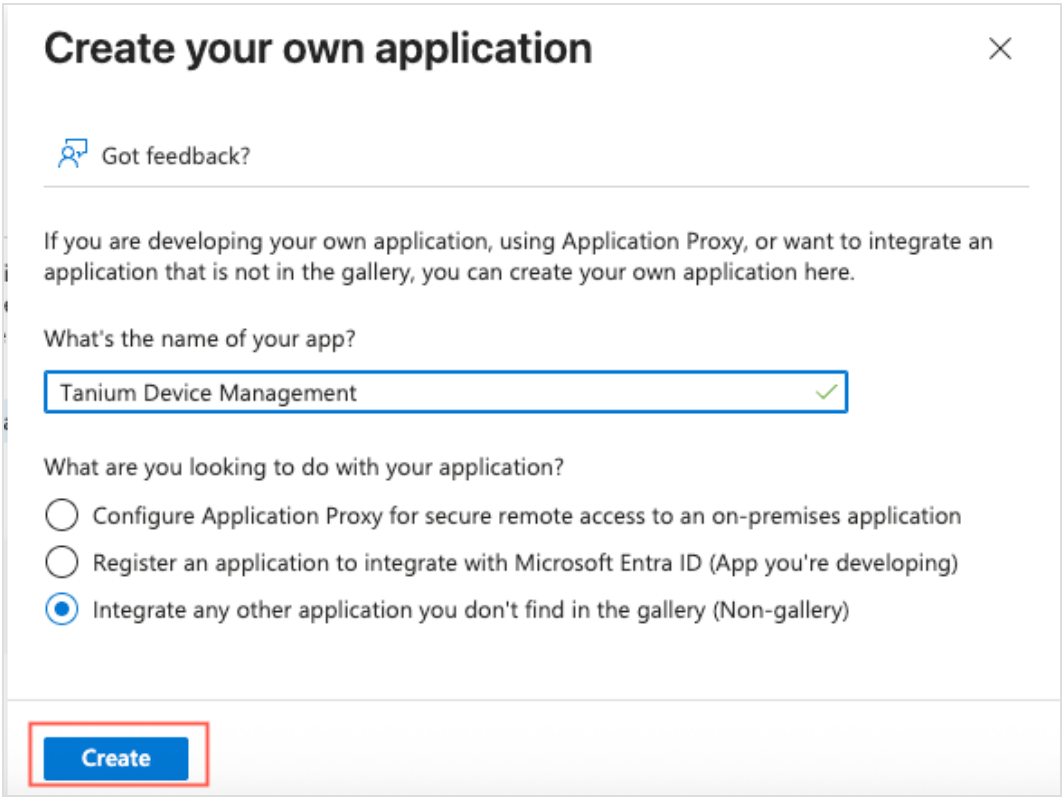


© 2026 Tanium Inc. All Rights Reserved

2. Click **New Application**.

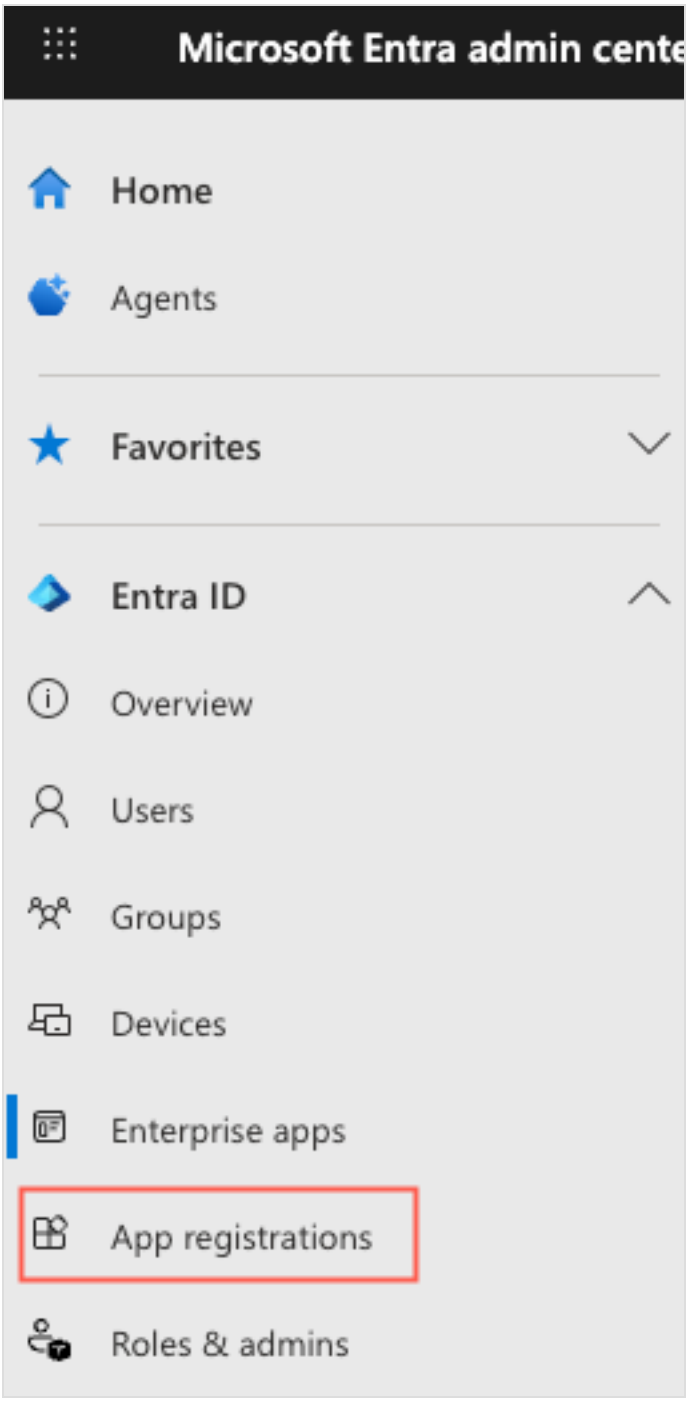


3. Click **Create your own application**.
4. Specify a name for the application.
5. Select this option: **Integrate any other application you don't find in the gallery**.
6. Click **Create**.



© 2026 Tanium Inc. All Rights Reserved

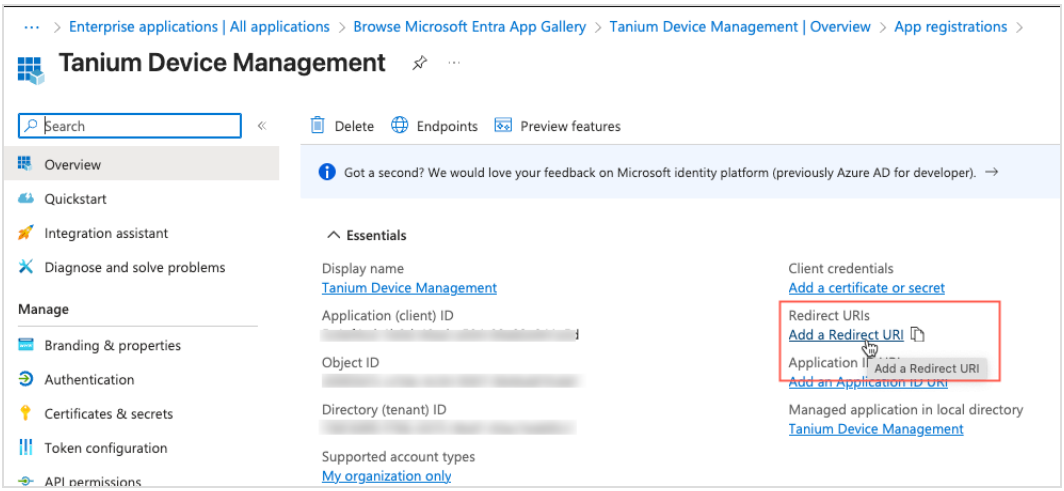
7. From the Entra menu, click **App registrations**.



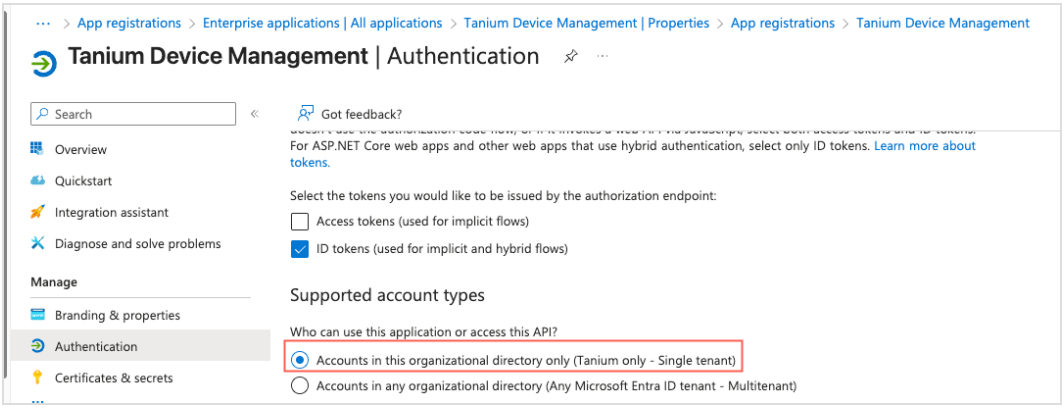
8. Click the name of the app that you created.

© 2026 Tanium Inc. All Rights Reserved

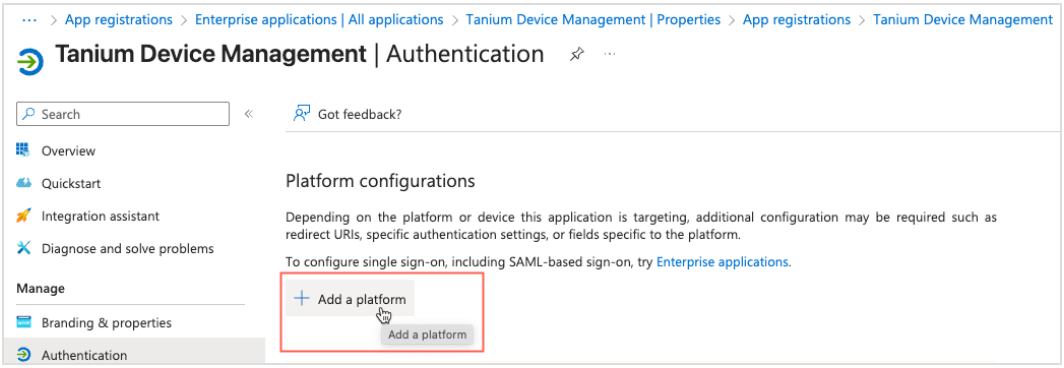
9. Click **Add a Redirect URI**.



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

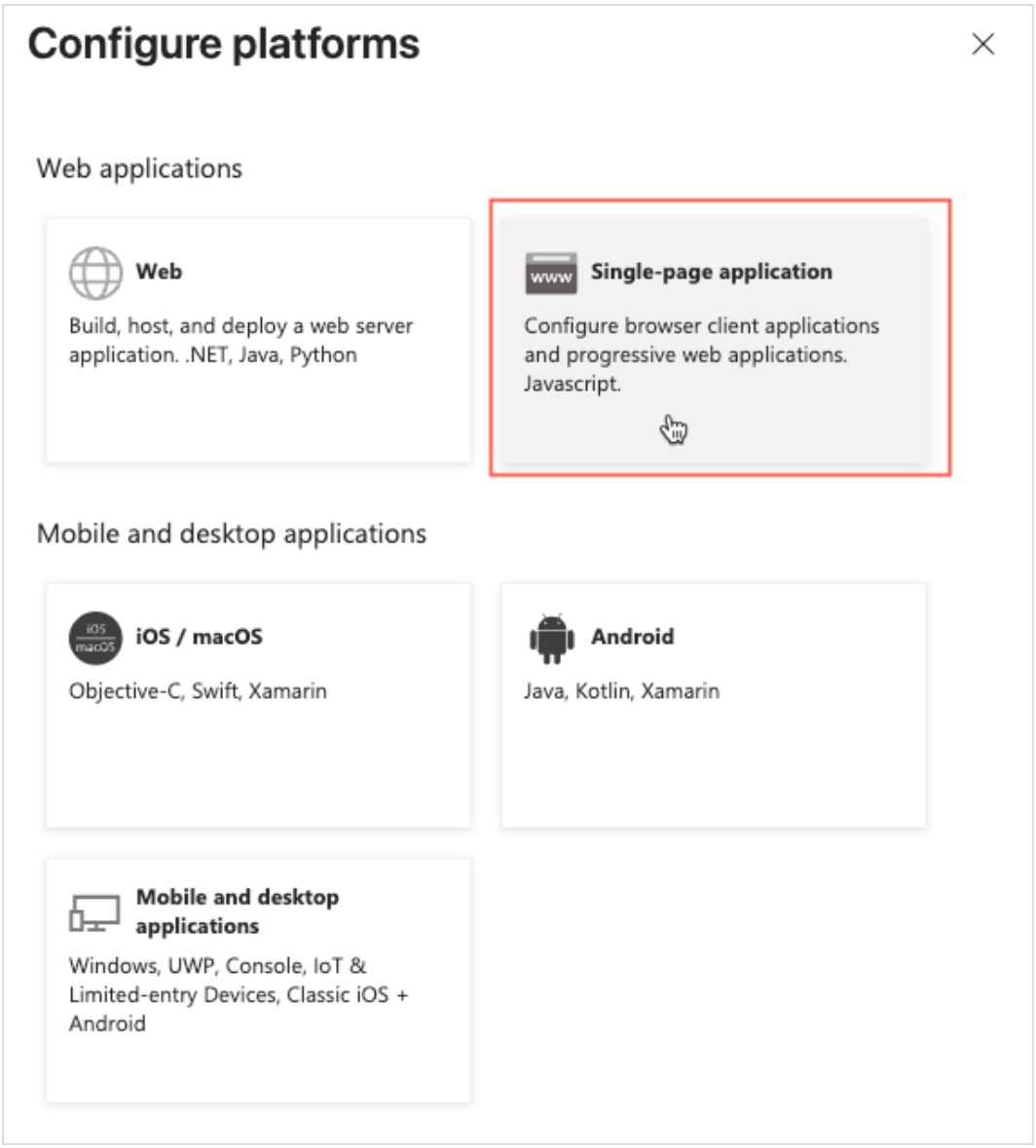


11. In the **Platform configurations** section, click **Add a platform**.



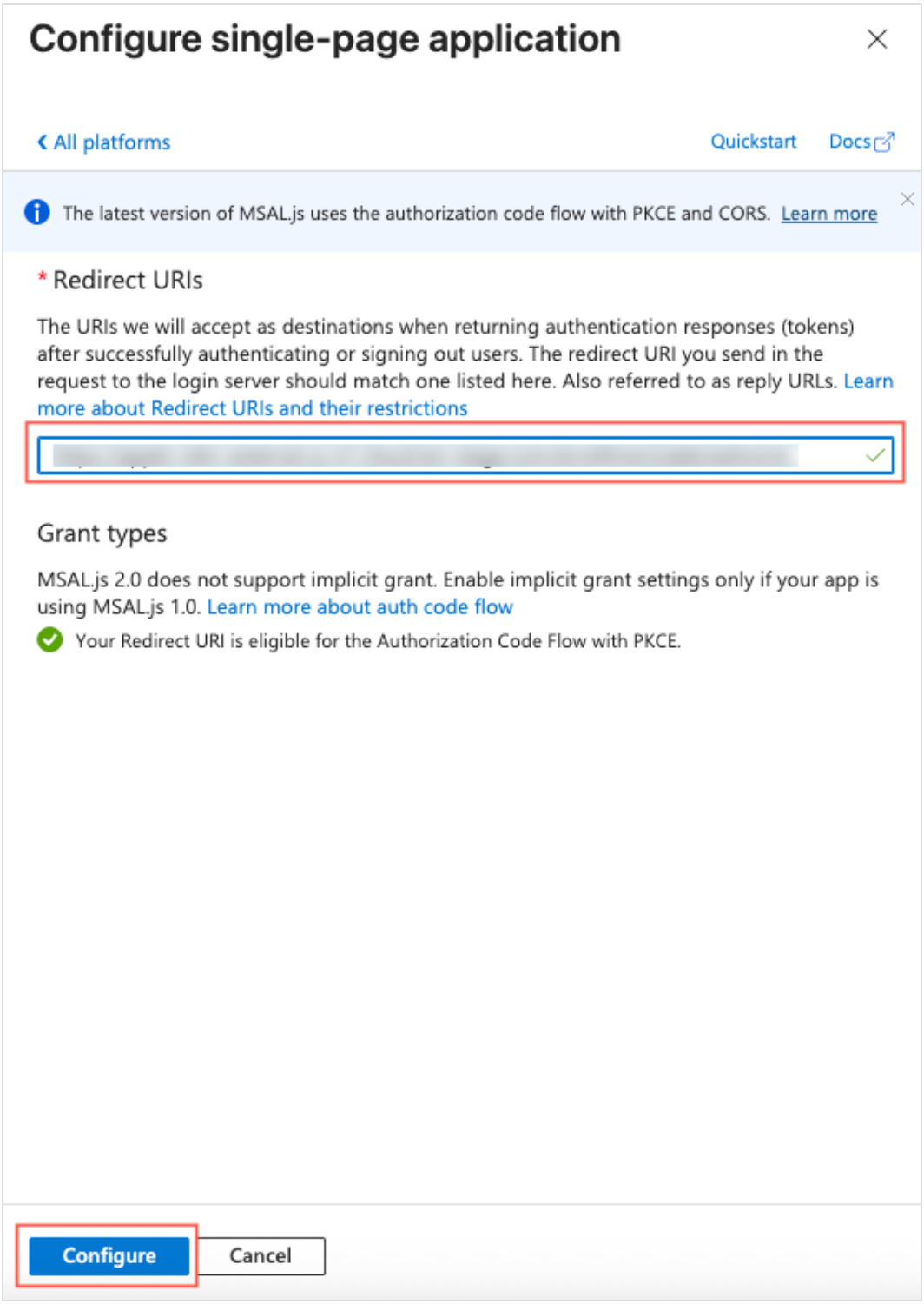
© 2026 Tanium Inc. All Rights Reserved

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



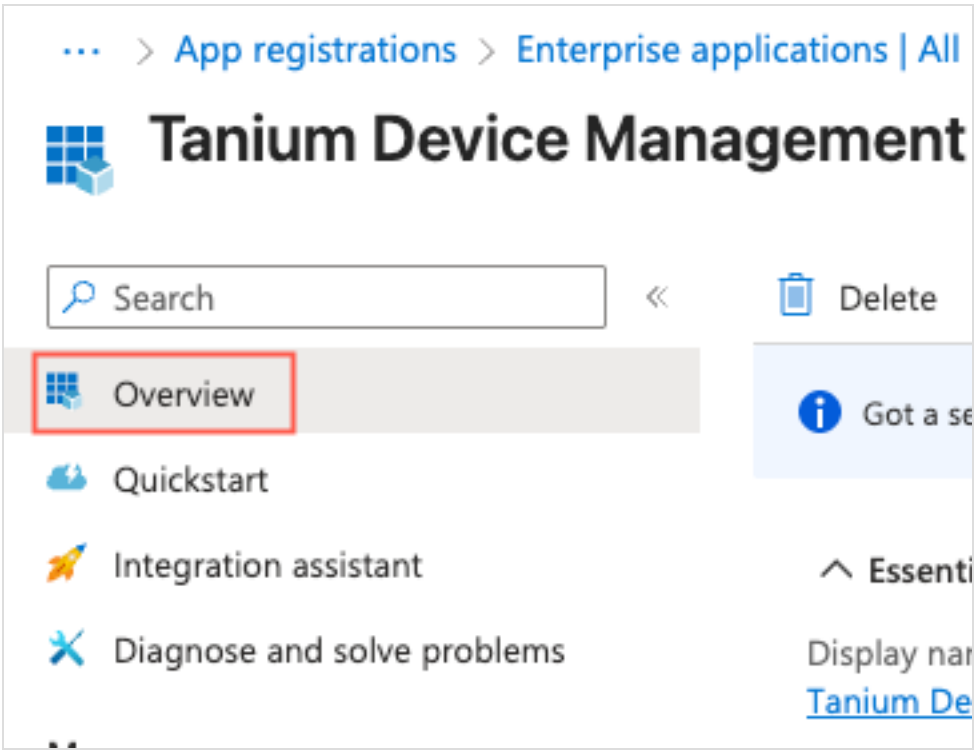
© 2026 Tanium Inc. All Rights Reserved

13. In the **Redirect URIs** section, enter the URI that you copied from the Device Management settings. Click **Configure**.

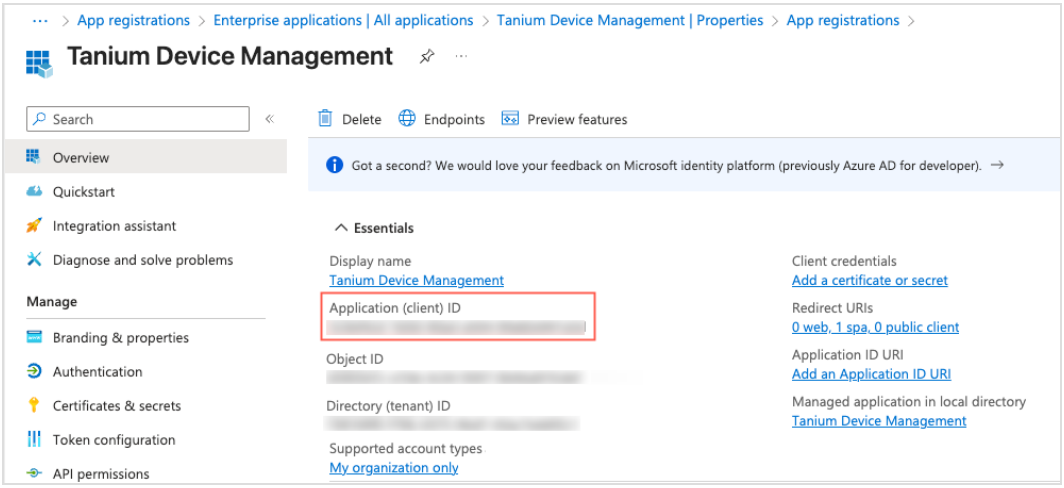


© 2026 Tanium Inc. All Rights Reserved

14. Click **Overview** to return to the application details.

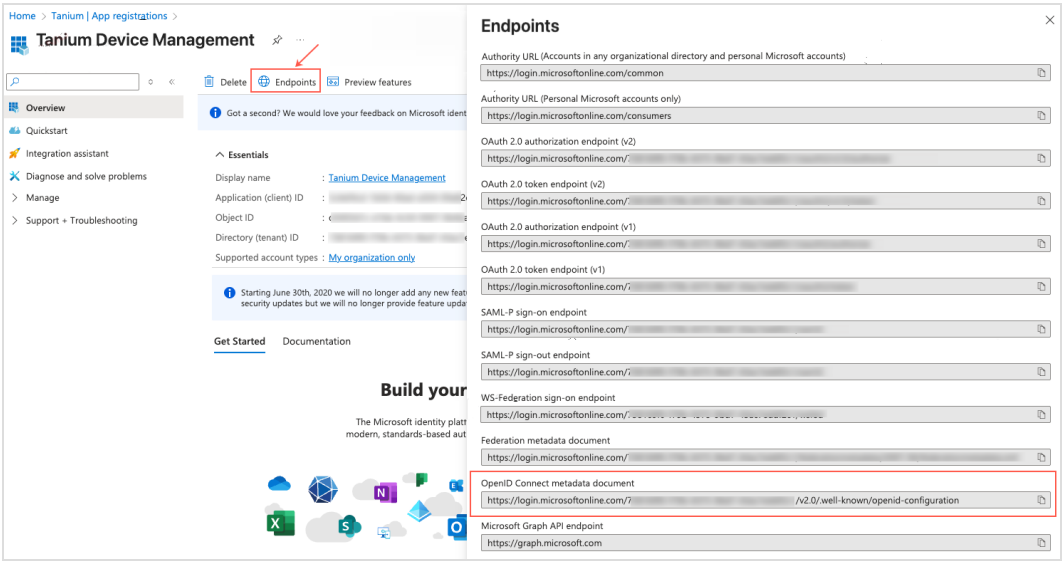


15. Copy and save the value for the **Application (client) ID**.



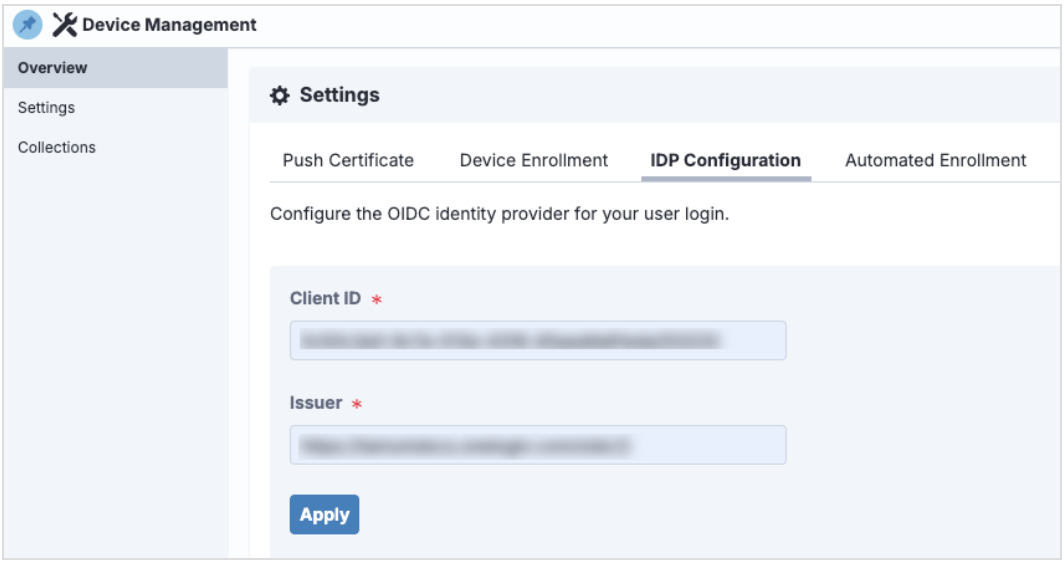
© 2026 Tanium Inc. All Rights Reserved

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.



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**.

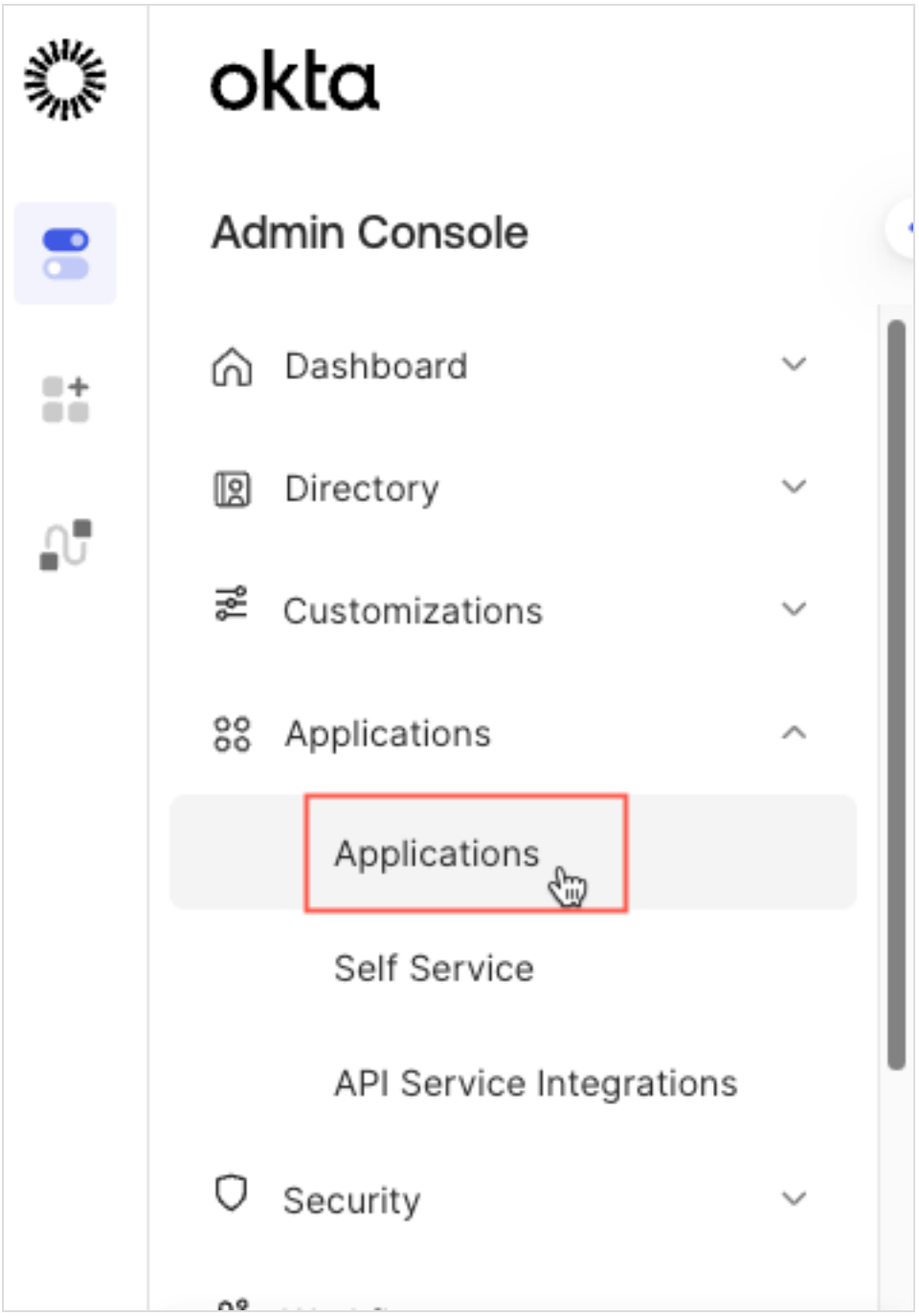


Okta

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

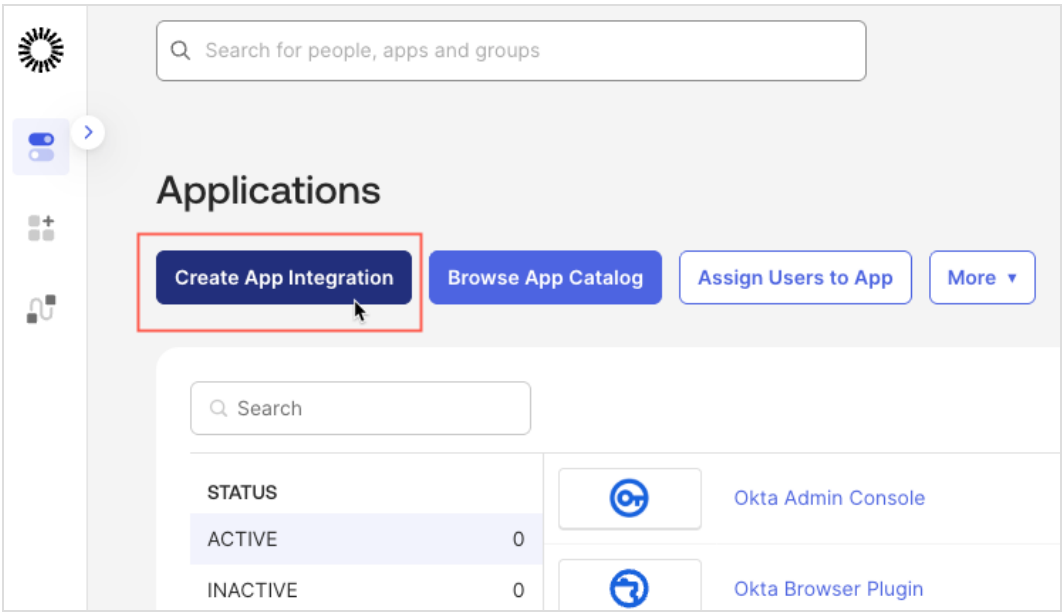
© 2026 Tanium Inc. All Rights Reserved

1. From the Okta Admin Console menu, click **Applications > Applications**.



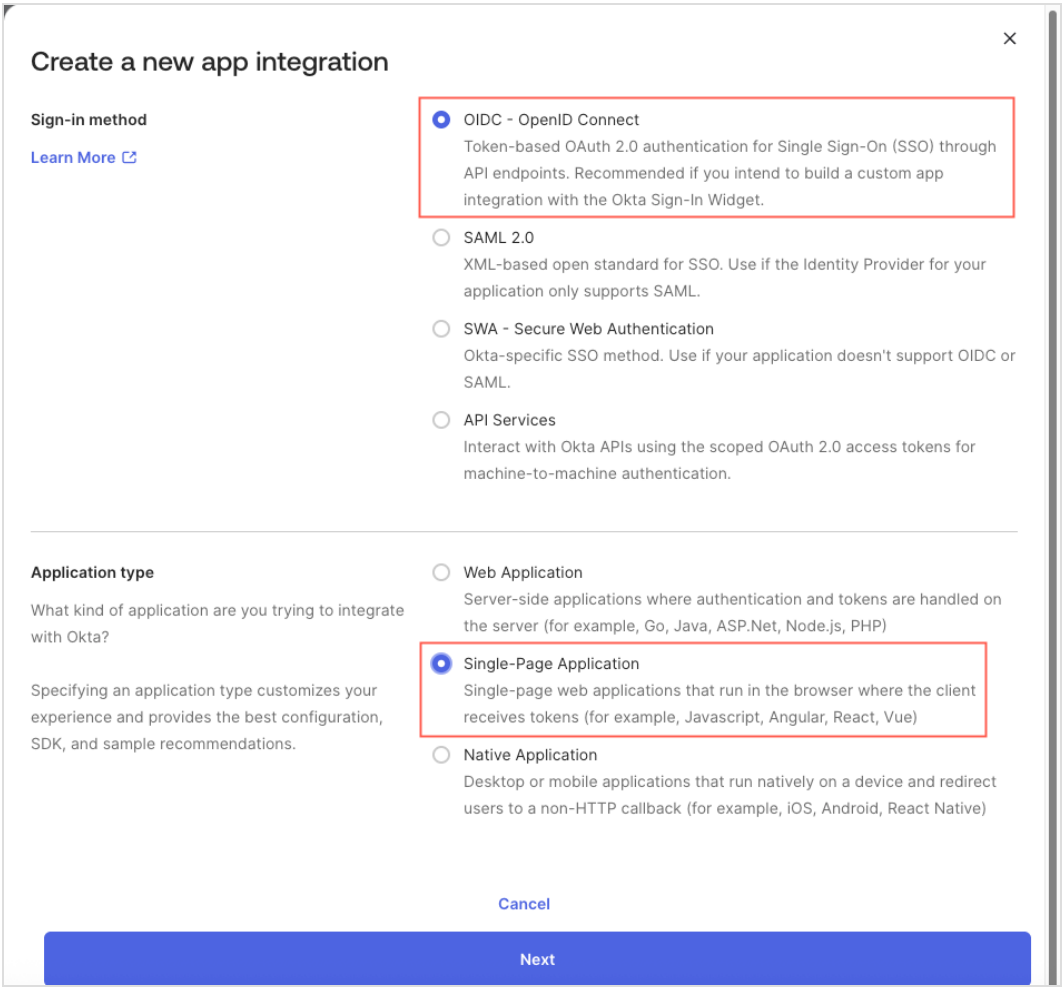
© 2026 Tanium Inc. All Rights Reserved

2. Click **Create App Integration**.



© 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**.

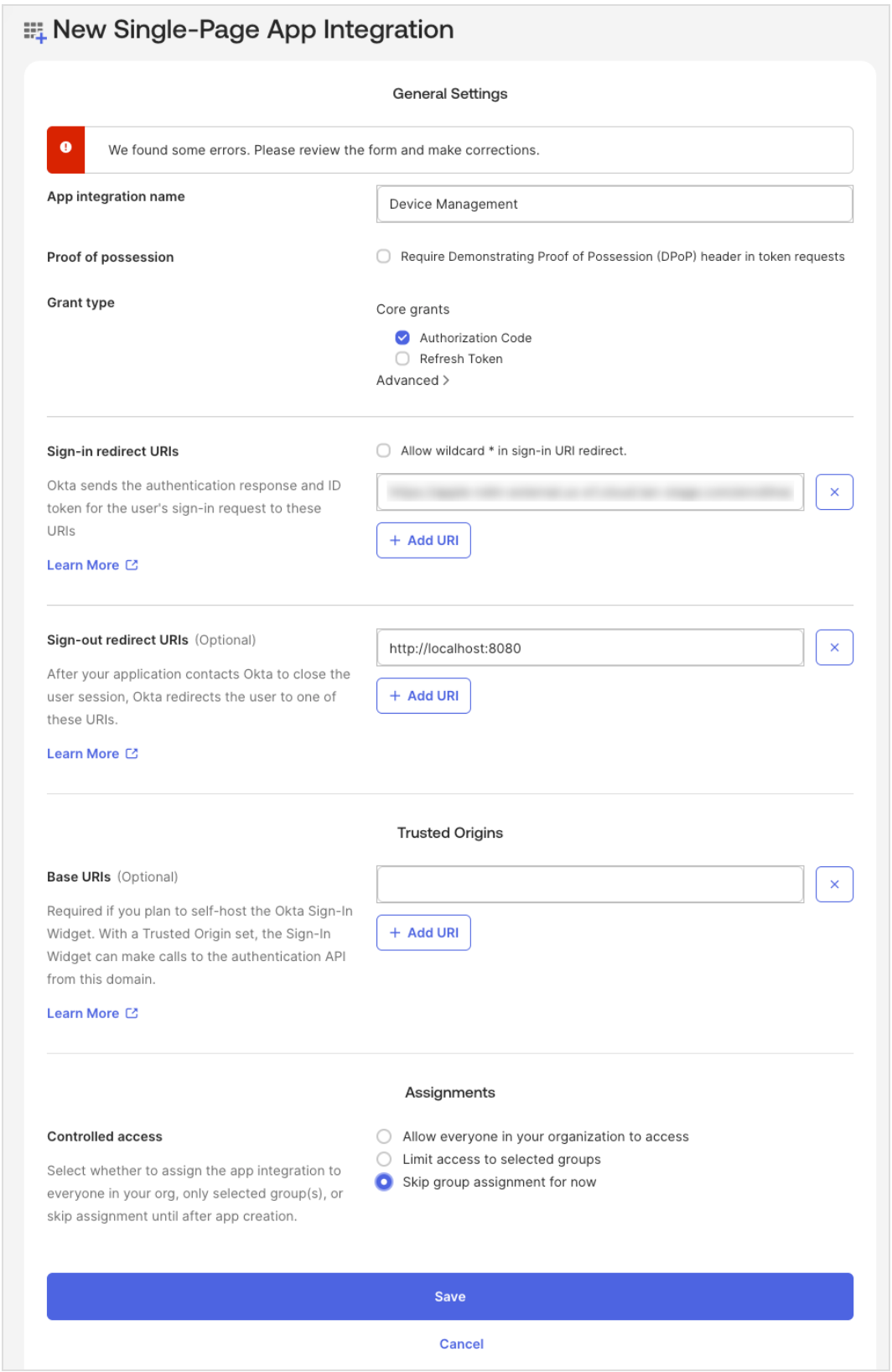


4. Specify a name for the application in the **App integration name** field.

© 2026 Tanium Inc. All Rights Reserved

5. In the **Sign-in redirect URIs** field, enter the URI that you copied from the Device Management settings.

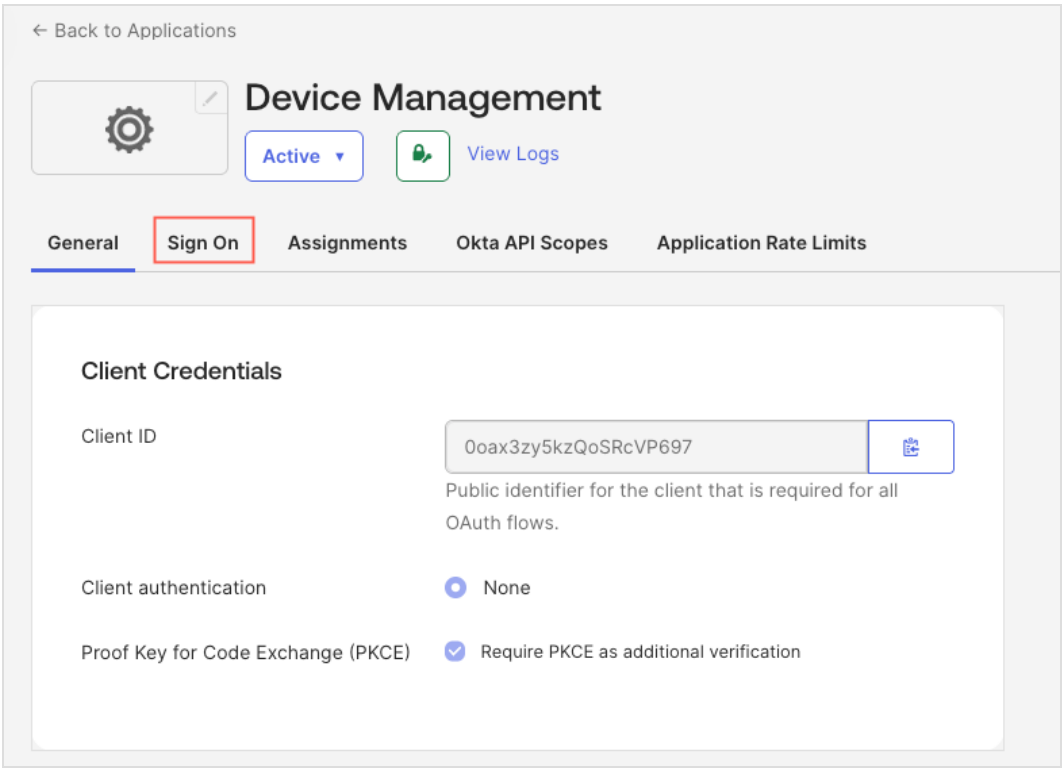
© 2026 Tanium Inc. All Rights Reserved



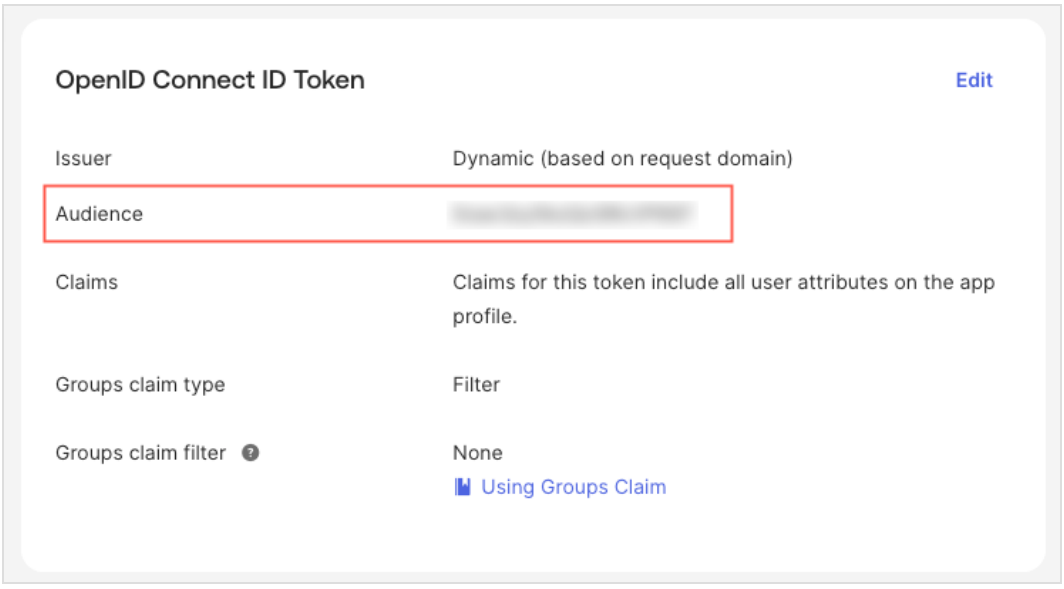
6. In the **Controlled access** section, select an assignment. Leave the other settings at their default values. Click **Save**.

© 2026 Tanium Inc. All Rights Reserved

7. On the application page, click the **Sign On** tab.



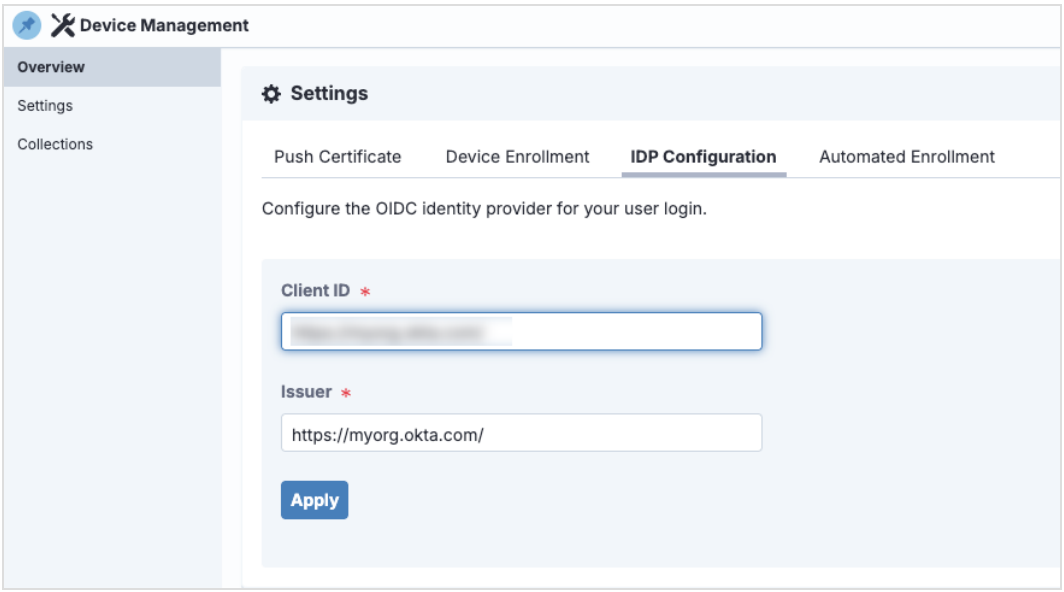
8. Copy the value for **Audience**.



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

© 2026 Tanium Inc. All Rights Reserved

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**.

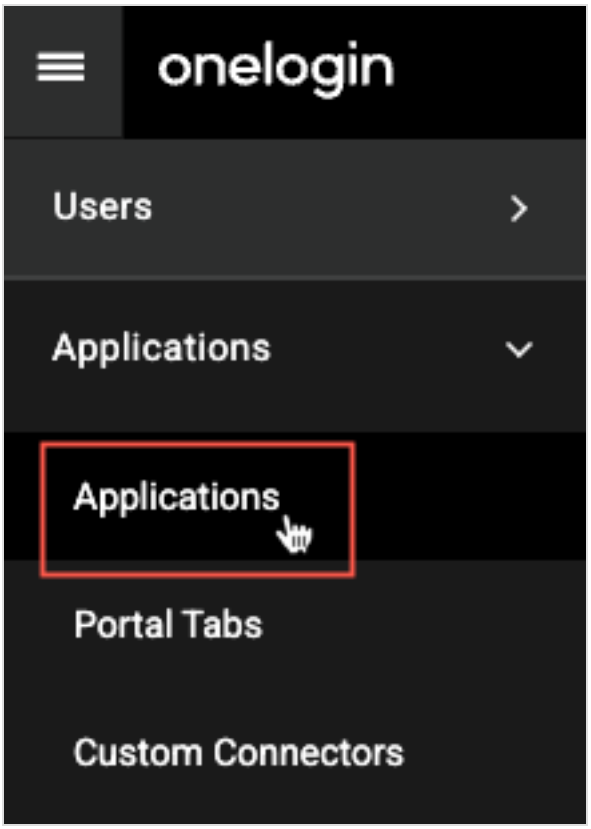


OneLogin

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

© 2026 Tanium Inc. All Rights Reserved

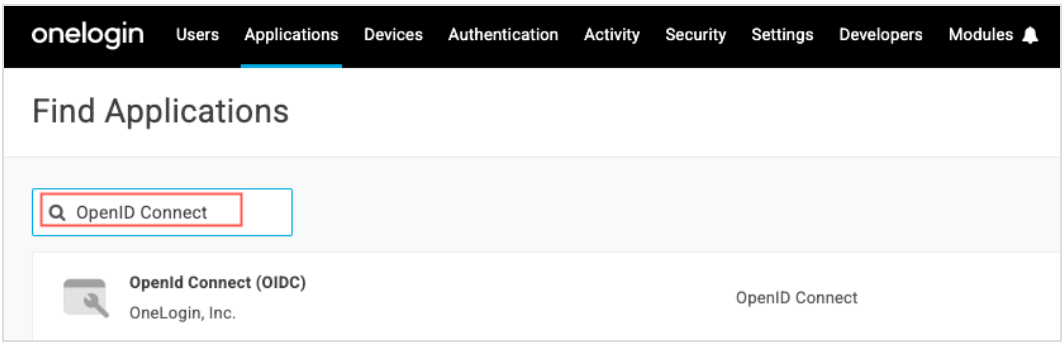
1. From the OneLogin administration menu, click **Applications > Applications**.



2. Click **Add App**.



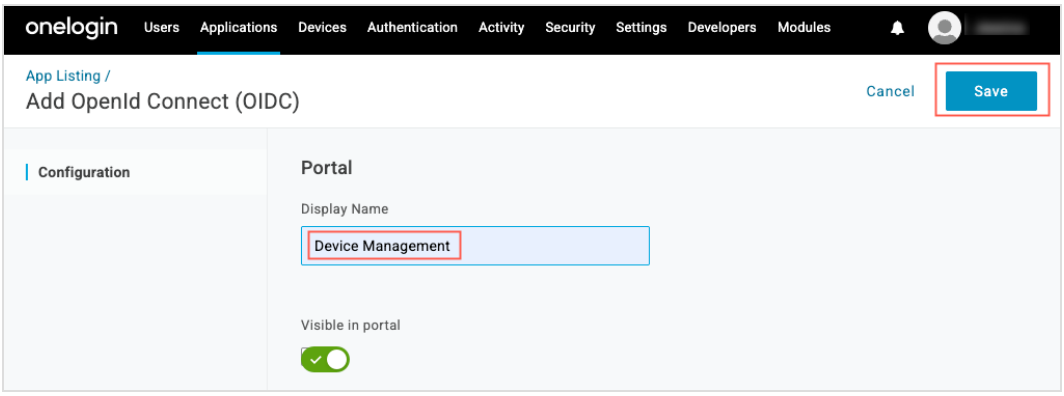
3. Search for `OpenID Connect (OIDC)`.



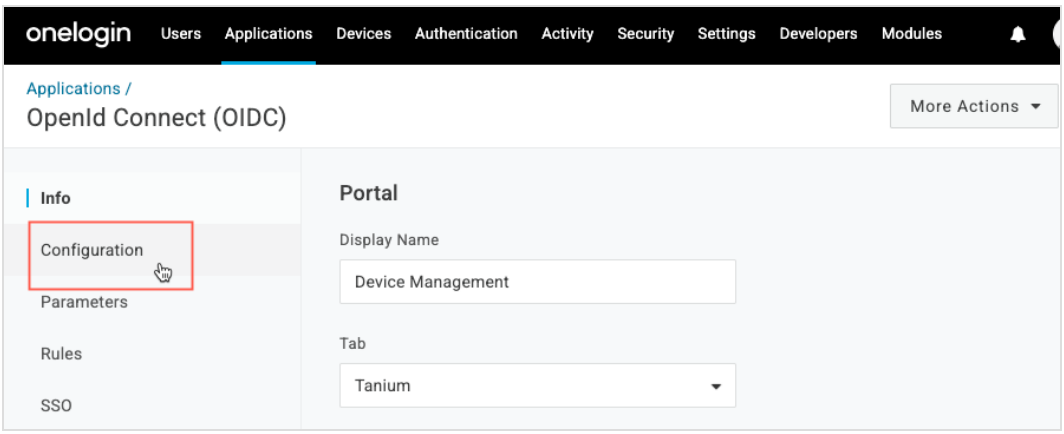
4. Click the app to add it.

© 2026 Tanium Inc. All Rights Reserved

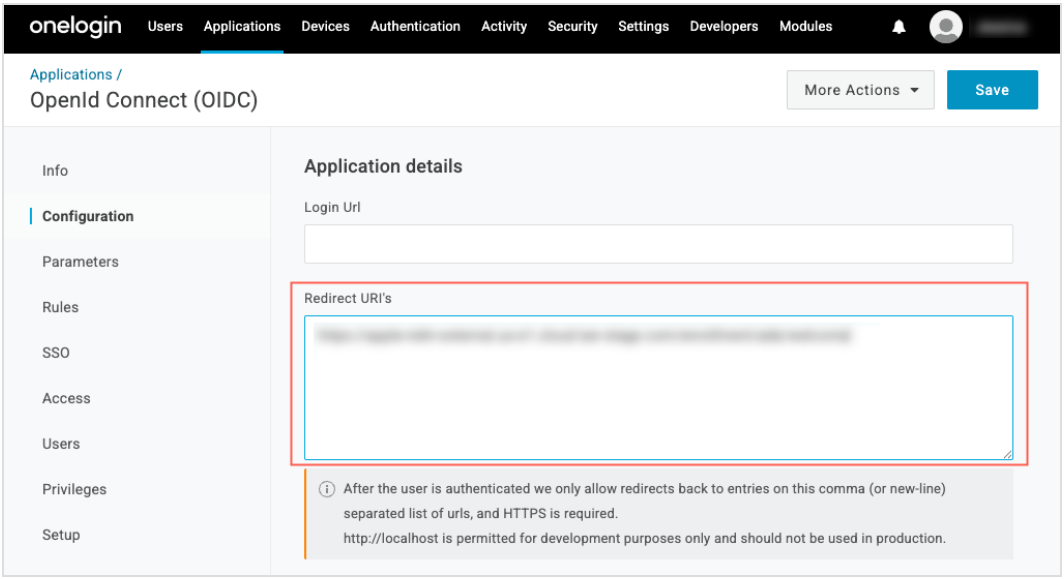
5. Specify a **Display Name** and, optionally, the icons for the app. Click **Save**.



6. Click the **Configuration** tab.

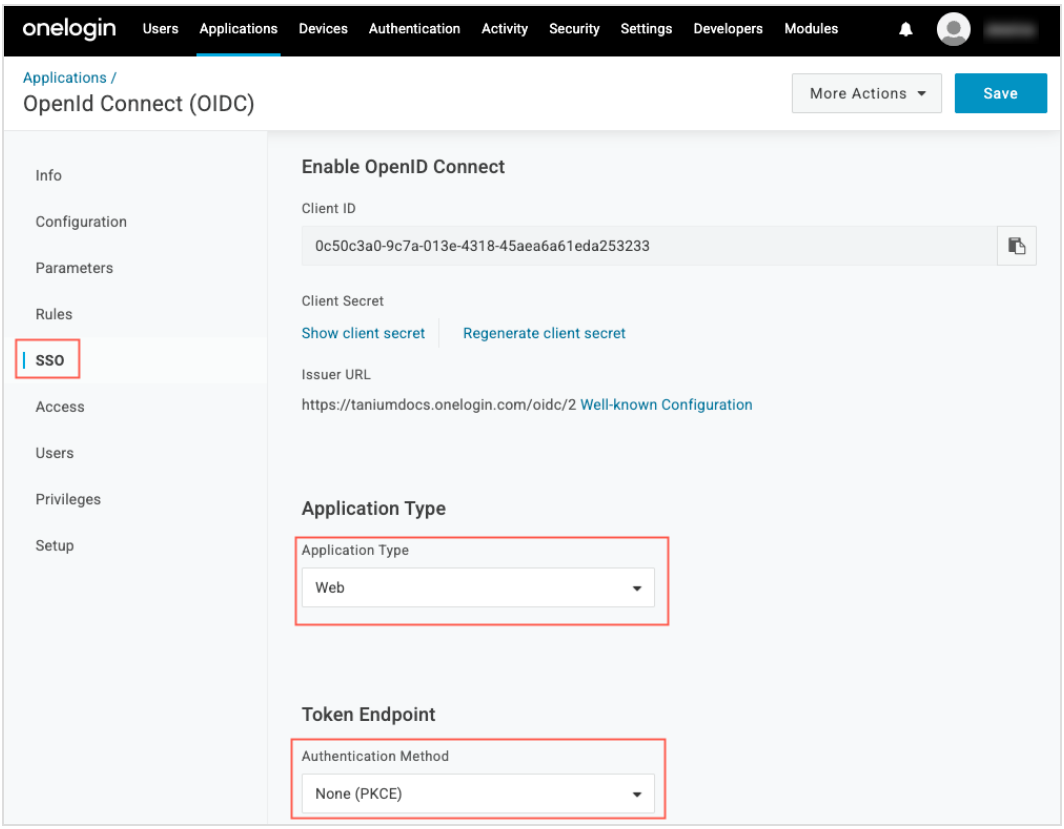


7. In the **Redirect URI's** field, enter the URI that you copied from the Device Management settings.



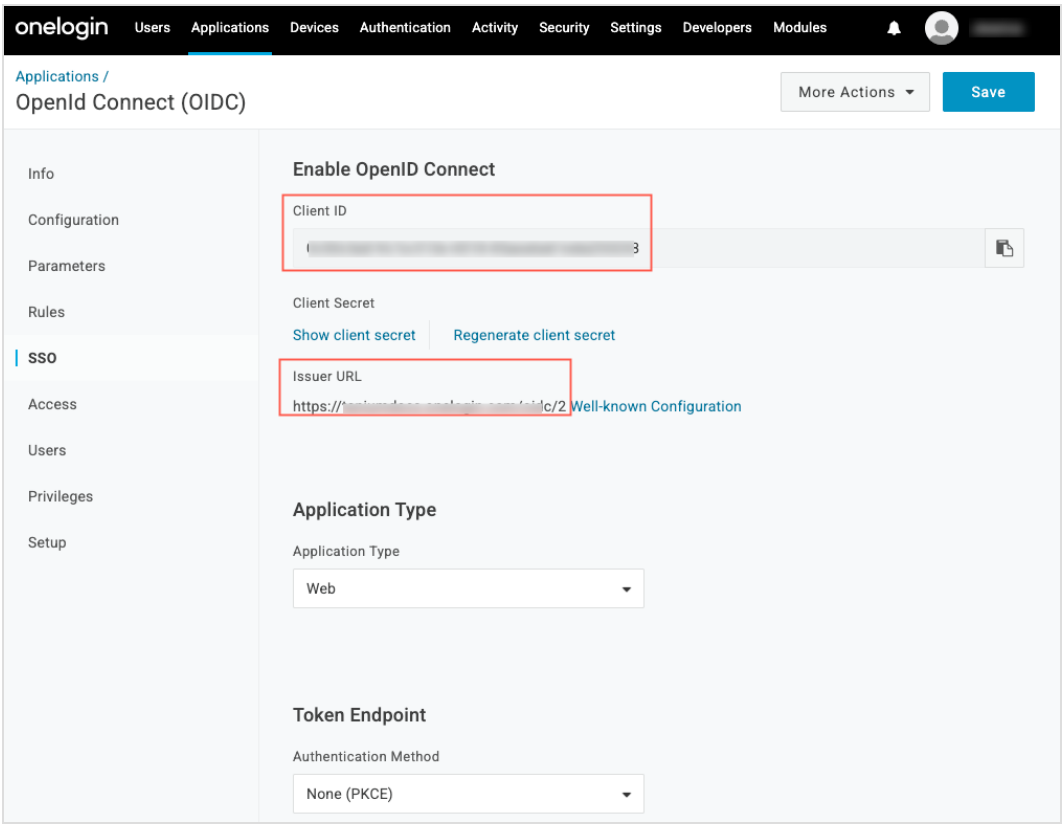
© 2026 Tanium Inc. All Rights Reserved

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



© 2026 Tanium Inc. All Rights Reserved

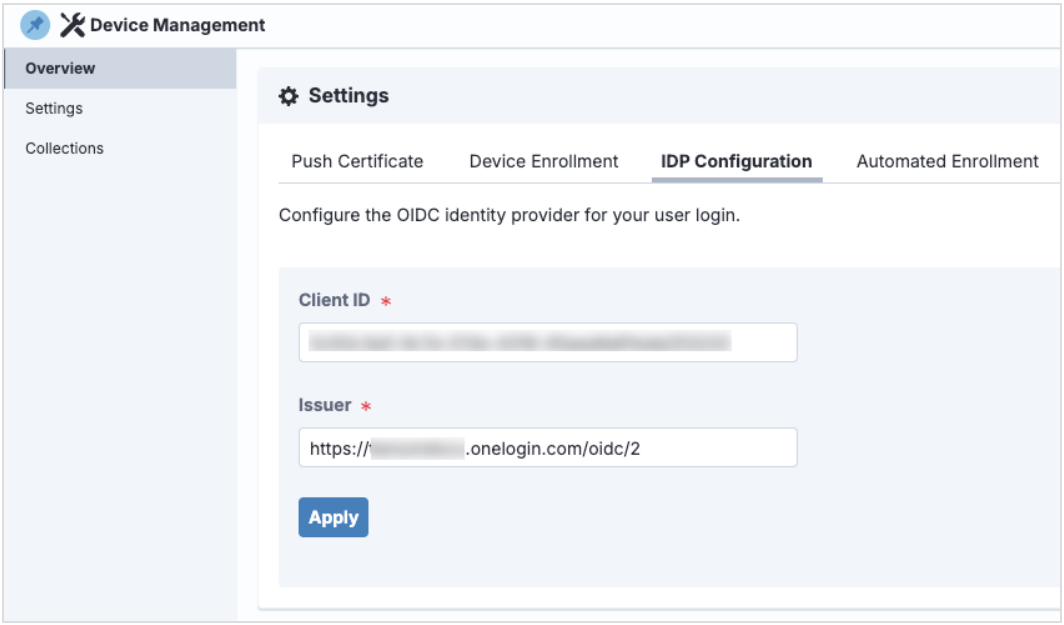
9. Copy and save the **Client ID** and **Issuer URL**.



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

© 2026 Tanium Inc. All Rights Reserved

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**.



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 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 more information, see Reference: Filter operators on page 88. For sensors in the `get` clause of a question, use the `matches` operator to match any value in a list. For 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.

© 2026 Tanium Inc. All Rights Reserved

Filter operators (continued)

Filter operator	Usage
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