



Device Management

Table of contents

- Devices
- Profiles
- Enrollment

Managing your employees' devices is just as crucial as monitoring their online identities when it comes to making sure they are handling company data responsibly. This is where device management comes in. Zoho One has device management features that can help you make sure that only authorized people and devices are using privileged resources. These features include enrolling both employee personal devices and company-owned devices in your organization, managing what employees can do with their devices by setting up policies and constraints, and ensuring employees get the necessary apps on their devices. [Learn more about device management](#)

When you open the **Device Management** tab, you'll be shown three tabs in the top bar: Devices, Profiles, and Enrollment.

The screenshot shows the Zoho One interface with the 'Device Management' section selected in the left sidebar. The main content area displays the 'Active Devices' tab, which includes a search bar, a '+ Enroll Devices' button, and a table with the following data:

DEVICE NAME	NAME / EMAIL ADDRESS	GROUPS	PROFILES	APPS
[Redacted]	[Redacted]	1	1	0
[Redacted]	[Redacted]	2	1	21

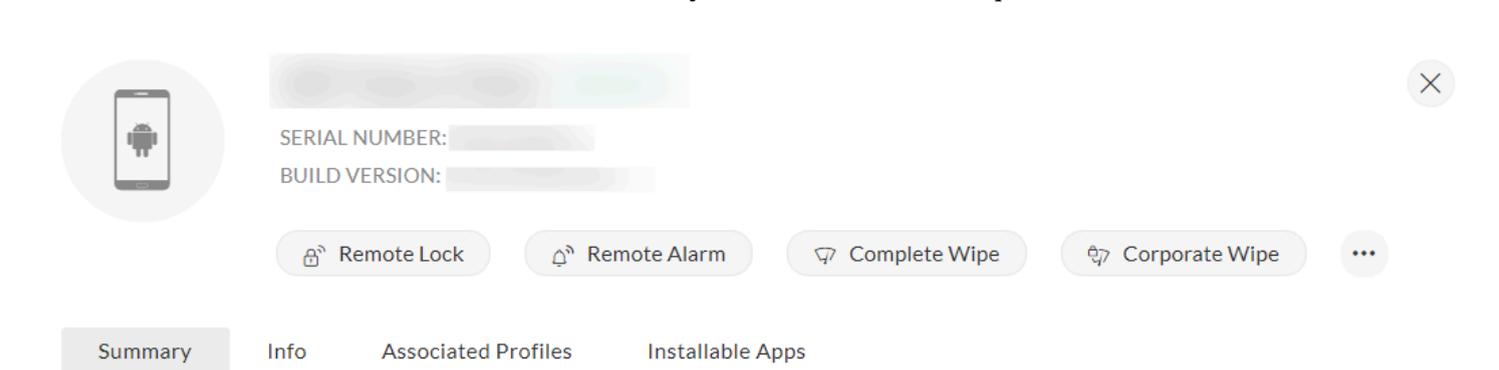
Devices

This page displays details and specifications of individual enrolled devices, such as device type, security, and network information. You can view the device's name, their email addresses, the number of groups they are added to, the number of profiles, and the total number of applications assigned to them.

You can add more devices to your organization by clicking **Enroll Devices**. Once you click, you'll be taken to the Enrollment tab, where you'll be asked to either share an enrollment link or enroll the device on your own. If you want to [reassign a device](#) to a new user, hover over the device profile to select **Reassign Device**. Once you've reassigned the device, profiles associated with the old user will be removed from the device and will be replaced with the profiles associated with the new user.

Every device has enrollment status (*Active, Staged, and Enrollment pending*). Learn more about [enrolling devices](#). With the filter option, you can set a specific enrollment status to view device-specific data.

To view detailed information of an enrolled device, you can click on the required device's name from the list.



The screenshot displays a device management interface for an Android device. On the left is a circular icon with an Android robot. To its right, the device name is blurred. Below the name are two fields: 'SERIAL NUMBER:' and 'BUILD VERSION:', both with blurred content. A row of four buttons is visible: 'Remote Lock', 'Remote Alarm', 'Complete Wipe', and 'Corporate Wipe'. A three-dot menu button is on the far right. At the bottom, there are four tabs: 'Summary' (selected), 'Info', 'Associated Profiles', and 'Installable Apps'. A close button (X) is in the top right corner.

You should take measures to avoid misuse or security breaches when allowing your staff to access company resources from their devices. You can achieve this by establishing policies to control access and following up on device usage. If a device is lost, misplaced, stolen, or compromised, Zoho One offers various methods to secure devices and protect the data on them.

As seen in the image above, you can secure device data by [locking it remotely](#), [set off an alarm](#) on a lost gadget to find it, select [complete wipe](#) to erase all the data on the device including the user's personal data, or select [corporate wipe](#) to erase all the data distributed by Zoho One (such as apps and settings). You can also choose to [clear or reset your password](#), or enable [lost mode](#).

You can view more information about the device under the following tabs:

Summary: A summary of device's memory, network, and OS.

Info: A detailed information on the device and its SIM and network. [Learn more device summary and info](#)

Associated Profiles: Displays information such as profile's name, when the device was assigned, what version was distributed, and its execution status. You can click on **Associate Profiles** to add more profiles to the device. You can always choose to disassociate a profile at any given stage.

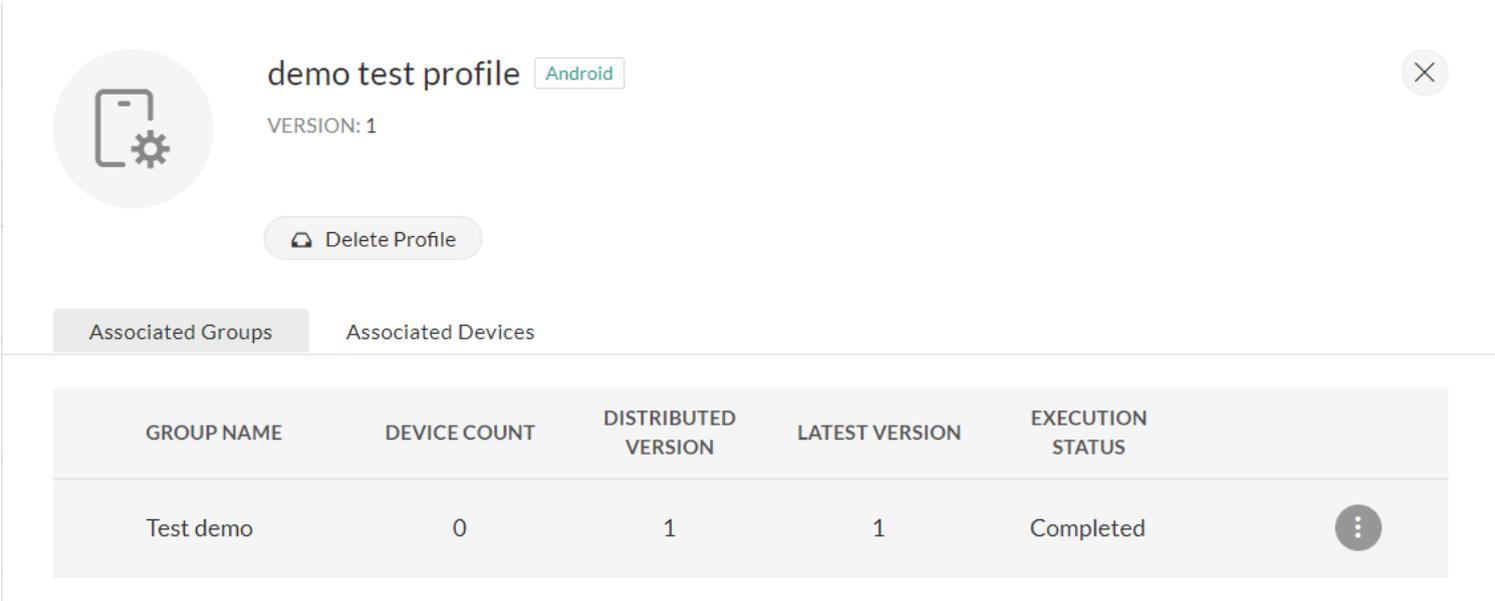
Installable Apps: Displays information such as the app name distributed to the device, assigned time, distributed version, and execution status. You can click on **Distribute Apps** to assign more apps to the device. Later, you can remove any app distributed to the device at any given stage.

Profiles

You can create and link profiles after enrolling devices in Zoho One. Profiles are used to impose policies to configure the device and set certain restrictions on device usage. Under the **Profiles** tab, you can view the list of profile names, their email addresses, the number of groups they are added to, and the total number of devices associated with the profile.

To add more profiles, click [Create Profile](#) and select the required device model from the list.

If the profile is in draft mode and if you've configured all the required policies and restrictions, hover over the draft profile to click **Publish Profile**. You have the option to [delete any profile](#) at any given stage.



demo test profile Android ×

VERSION: 1

🗑️ Delete Profile

Associated Groups Associated Devices

GROUP NAME	DEVICE COUNT	DISTRIBUTED VERSION	LATEST VERSION	EXECUTION STATUS	
Test demo	0	1	1	Completed	⋮

When you click on any profile, the above page will be displayed where two tabs are shown: Associated Groups and Associated Devices. Under the **Associated Groups** tab, you'll be shown the list of groups added, the number of devices distributed in the group, versions of the distributed devices, the current version running, and their status of execution. You have the option to [disassociate profiles from a group](#) at any given stage. Under the **Associated**

Devices tab, you can view the list of devices' names, their email addresses, versions of the distributed devices, the current version running, and their status of execution. You have the option to [disassociate profiles from a device](#) at any given stage. [Learn more about profile management](#)

Enrollment

Enrollment allows you to manage your organization's devices through Zoho One. You can assign devices to users in Zoho One after devices have been enrolled. Under the Enrollment tab, you'll be shown three tabs: BYOD Enrollment, Corporate Enrollment, and Settings.

App Settings
Directory

Devices Profiles Enrollment

BYOD Enrollment Corporate Enrollment Settings

Apple devices can be enrolled only after configuring an APNs certificate. [Configure Certificate](#)

Share Enrollment Link

Email the enrollment links to users and enable them to enroll their personal devices themselves.

Individual Group

Choose Users

[Send Invite](#)

Enroll Device Yourself

Generate a unique enrollment link for each device and enroll users' personal devices.

[Generate Link](#)

The Bring Your Own Device (**BYOD**) **Enrollment** enables admins to enroll employees' personal devices in Zoho One either by sharing enrollment links with users or groups through email, or by generating an enrollment link to enroll each device. Before enrolling for Apple devices, you [should have configured an Apple Push Notification service \(APNs\) certificate](#). [Learn more about BYOD Enrollment](#)

The screenshot shows the Zoho One Directory App Settings interface. The left sidebar contains navigation options: Dashboard, Organization, Applications, Users, Admins, Groups, Domains, Security, Device Management (highlighted), Marketplace, Active Directory, and Reports. The main content area is titled 'Enrollment' and has tabs for 'BYOD Enrollment', 'Corporate Enrollment' (selected), and 'Settings'. Under 'Corporate Enrollment', there are sub-tabs for 'Apple' and 'Android'. A dropdown menu for 'Select Enrollment Type' is set to 'Apple Enrollment (ABM/ASM)'. A yellow warning banner states: 'Create APNs to manage iOS Devices. Create and upload an APNs certificate to start managing Apple devices. Create Now'. Below this, the 'Apple Enrollment (ABM/ASM)' section includes a description, a 'Key Benefits' list (Simplified Setup, Out of the box enrollment, Mandatory MDM management, Over-the-air supervision), and two buttons: 'Enroll devices for business' and 'Enroll devices for schools'. A note mentions availability in specific countries and suggests the 'Apple Configurator'. A video link 'Need a demo for enrolling devices through ABM/ASM? Watch video' is at the bottom.

Under the **Corporate Enrollment** tab, you can view different enrollment types to enroll company-owned iOS and Android devices where admins enroll them in Zoho One as they'd have complete control over those devices. For Apple devices, [Apple Enrollment \(ABM/ASM\)](#) and [Apple Configurator](#) enrollment type are available. For Android devices, [EMM Token Enrollment](#), [Zero Touch Enrollment](#), [NFC Enrollment](#), and [Knox Mobile Enrollment](#) are available. Links to demonstration videos on how to complete each enrollment type are available on the page.

The screenshot shows the Zoho One Directory App Settings interface, specifically the 'Settings' tab under 'Corporate Enrollment'. The 'APNs Certificate' section is active, with a description: 'APNs certificates are used by Zoho One to communicate with your Apple iOS devices. They have to be configured before enrolling iOS devices.' A 'Configure Certificate' button is visible below the text.

Under the **Settings** tab, a link to configure APNs certificate is displayed. APNs certificate helps to create a secure link between the apps and the iOS devices for sharing information. You will require a [certificate created using the APNs](#) certificate gateway in order to enroll iOS devices in Zoho One. [Learn more about device enrollment](#)

