



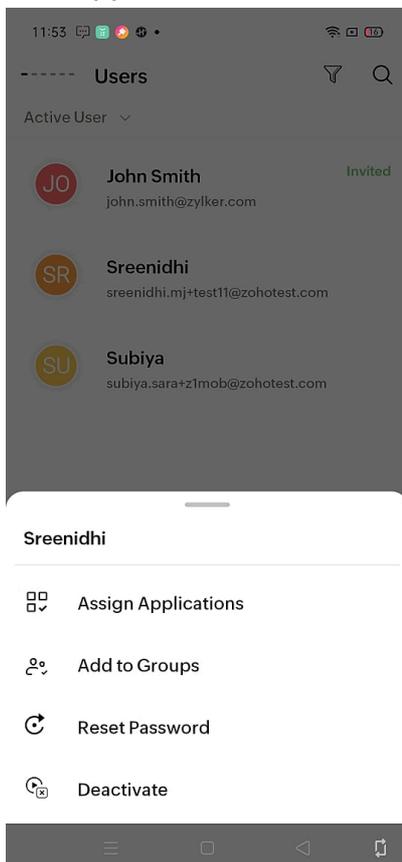
# Understanding Zoho One mobile's Directory

You can use the mobile app to access Directory, Zoho One's admin panel. Directory is where you can monitor your organization. Through single sign-on (SSO) and multi-factor authentication (MFA), you can manage users, control application access, and secure the digital identity of your workforce. You can also enforce security policies for your organization.

Directory is organized into the following tabs in the mobile app: *Users*, *Groups*, *Applications*, *Admins*, *Security Policies*, and *Device Management*. The app has only those tabs unlike the web app, so you can perform only selective tasks on the move.

## Users

In the *Users* tab, you can view the list of users you've added to the organization through the web app. You can use the [filter option](#) to view the users based on specific criteria.



The above screen is displayed when you long press on any user. You can choose to assign apps to the user, add them to a group, reset their password, or deactivate their account. To

[reset MFA](#) or to [manage email addresses](#), tap on the user, then tap on  on the right-hand side of the screen.

Though you can add a user manually, you can't import or export them in bulk here since bulk operations cannot be performed on a mobile app. In the case of a confirmed user with an unverified domain, you can't create a mailbox for them from here; that can only be done through the web application. You also have the option to [delete a pending user](#). Since you can neither configure nor manage a user's mail settings, there's no possibility of adding or editing custom fields in mobile.

## Groups

Once you're in the *Groups* tab, you can view the list of groups added to the organization and can tap on them to view further details. You can choose to either create a collaboration group or department. Once you've added either of those, you can then [add users](#) to them and [edit their details](#), but you don't have the option to change their logos. Although you can form a department or a collaboration group, you don't have the option to convert a collaboration group to a department or vice versa.

You can [configure mail settings for a group](#) by creating a group email address here. After setting up a group email address, you cannot filter potential spam emails, manage email notifications for that group, or set restrictions on who can send emails like you can in the web app. You also won't find the option to manage the group with MDM (mobile device management) in the app in order to manage the devices used by all the members of a group. You can [delete a group](#) on the move.

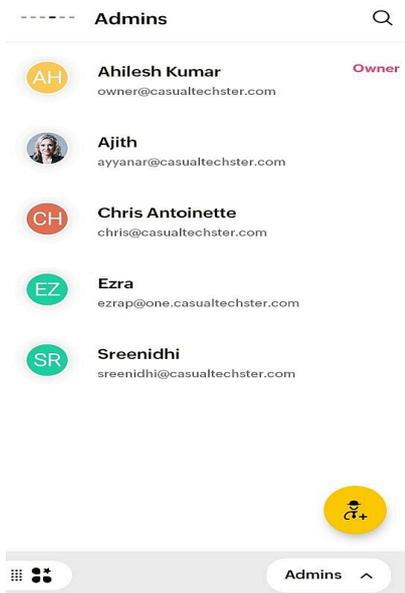
## Applications

The *Applications* tab lists the applications you added to your organization. With the filter option, you can set it to display applications based on their status, which includes *Active*, *Inactive*, and *Hidden* apps. You also have the option to hide apps on your mobile. You must tap on the required app and then the  icon to access the hide option. To add users or [service admins](#) to the app, you can tap on the preferred app to complete the action. You can also change the owner of an application.

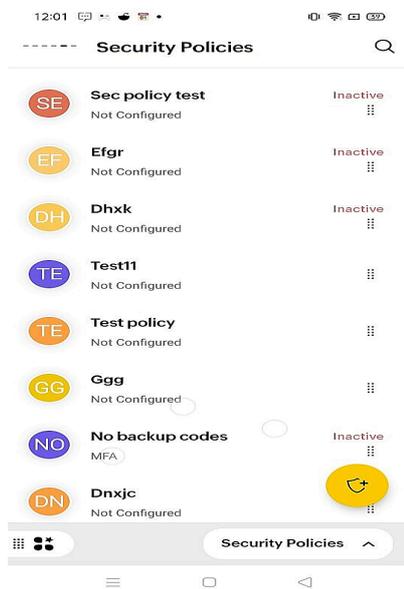
When it comes to assigning apps, it can only be done for an **individual user** and not to a group or with conditions for specific users. When a user in your organization has requested access to an app, the admin can accept or deny access from their mobile app. Unlike through the web app, an app cannot be personalized by changing its logo or display name.

## Admins

The list of Zoho One admins and the organization admin are displayed on the mobile interface when you tap on *Admins*. There isn't a distinct tab for service administrators; you can only access them by tapping on specific applications. This tab offers the ability to **assign** or **unassign** admins via your mobile device.



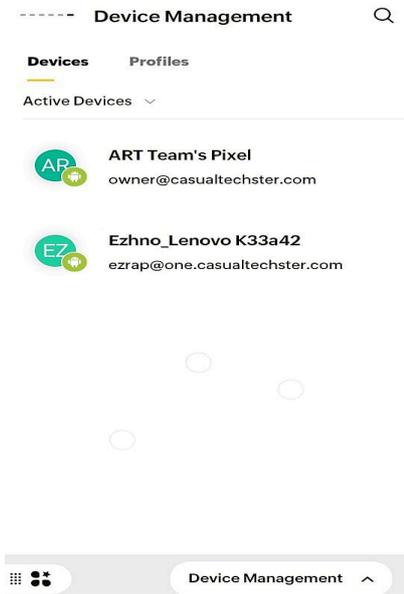
## Security Policies



When you tap on the *Security Policies* tab, you'll be shown only the list of security policies added to your organization; no custom authentication settings are available on the mobile device app. Hence, you won't have the option of setting up custom authentication with an IdP of your choice here. You can view the status of security policies, whether they are active or inactive, [add](#), rename, or [delete](#) a security policy, and have a look at the groups they have been applied to.

You can also configure [password policy](#), [MFA](#), [IP restrictions](#), and [session management](#) with a security policy here.

## Device Management



The *Device Management* tab displays two tabs: *Devices* and *Profiles*. The mobile app does not give you the option to enroll and manage your organization's devices, but, similar to the web app, 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. To examine device-specific data, you can use the filter option to set a certain enrollment state.

Similar to the web console, you may secure device data with actions like remote lock, remote alarm, complete wipe, and corporate wipe. Additionally, you can utilize the mobile app to activate lost mode and reassign a device to a user. The *Profiles* tab displays two tabs: *Associated Groups* and *Associated Devices*. A profile can be deleted, but there's no possibility to add or remove profiles from a group or device.

<https://help.zoho.com/portal/en/kb/one/getting-started-with-zoho-one/articles/understanding-zoho-one-mobile-s-directory#Users>