This guide has been designed to assist with the set up and management of Android Enterprise Essentials.

Table of Contents

Overview and features 3
Supported devices 4
Getting started 5
Android Enterprise Essentials 6
Using the Android Enterprise Essentials portal 7
  Find specific devices 7
  Device statuses 7
Activating an Android Enterprise Essentials device 8
Device management 9
  Reset the screen lock on a device 9
  Wipe a device 10
  Remove a device 11
Portal management 12
  Rename a device 12
  Add multiple resellers from customer portal 12
  Portal languages 12
  Supported browsers 12
User management 13
  Types of user roles 13
  Manage users 13
Get help 14
  Contact your reseller for support 14
  Ask the Help Community 15
Overview and features

Android Enterprise Essentials is a simple, secure management service that makes it easy to protect your business by automatically enabling and enforcing the critical features and functionality required to keep your devices and data safe.

Features include:

- Simple remote deployment
- Screenlock and encryption enforcement
- Mandatory malware protection
- Remote data wipe
Supported devices

All devices that support zero-touch enrollment also support Essentials. Devices that support zero-touch are:

- All Android devices running Android 9.0 or above that originally shipped with the Google Play Store
- Select devices running Android 8.0

Questions?
If you have any questions about specific device support, consult your reseller.
Getting started

Android Enterprise Essentials can only be procured from a list of official resellers. Once you've found your reseller and you've ordered your devices you will need to provide them your organization's name, your email address and, optionally, an additional email address of a colleague who will also have access to the portal. After your reseller creates your account and assigns devices to your unique Essentials portal, you'll receive a welcome email with information about how to access the portal.

If the email address you provided for your reseller is a Google Account:

1. Click the link in your welcome email to open the Android Enterprise Essentials portal.
2. Login to the portal using your Google Account credentials.

Your Google Account is now an owner of the portal.

If the email address you provided for your reseller isn't a Google Account:

1. Click the link in your welcome email to activate the Essentials portal. Note: The activation link expires after 90 days.
2. When prompted, create a Google Account (or select an existing one).
3. Login to the portal using your Google Account credentials.

Your Google Account is now an owner of the portal.

Set up process

We've streamlined the setup process to be as easy as turning on the device. So as soon as the device's have been added to the Essentials portal by your reseller you can send them straight to your users!

Tip

We recommend adding at least one more portal owner (see Manage portal users)
What does it mean to have a device managed by Android Enterprise Essentials?

When a device is Active in the Android Enterprise Essentials portal all of the security measures are applied. This does the following:

- Requires a screenlock to be applied to any device within Essentials.
- Ensures device encryption is enforced.
- Enforces mandatory malware protection with the most widely deployed mobile threat detection service with Google Play Protect.
- Blocks the installation of applications from unknown sources.
Using the Android Enterprise Essentials portal

As a portal owner or admin, you can see a list of your organization’s Essentials devices. You can see details including the device name and manufacturer, and the last time it synchronized with Essentials. From the list, you can reset the password on a device, wipe data from a lost device, and more.

Upon logging into your portal you will see the devices with a list of the following information:

- Device name
- Manufacturer
- IMEI or serial number
- The last time the device synchronized with Essentials
- Device status

Device statuses

- **Ready to set up**
  - The device is assigned to your organization but hasn't been activated.

- **Active**
  - The device has been activated and is protected by Essentials. See “Activating an Android Enterprise Essentials device” for steps on how to activate your devices.

- **Wiped**
  - The device was wiped using the Essentials portal and is ready to set up again.
Activating an Android Enterprise Essentials device

Once your reseller has assigned the devices to your organization, and they will be listed in the portal as Ready to set up, and they will remain in this state until you activate them. To activate a device please follow the steps below:

1. Turn on the device.

2. When prompted, connect the device to a Wi-Fi network. The device is now activated and Essentials security requirements are automatically enforced.

3. Follow the on-screen instructions to complete the setup.

Tip
During the setup process the device will display a screen notifying the user the device is being managed by their employer.

Once a device is active, you can use the Essentials portal to:
Assign a new name to the device to make it easier to identify.
Reset the screen lock or wipe the device at any time.
Device management

Essentials allows you to take proactive action on your devices should it be required. Devices will require an internet connection to receive actions sent from the Essentials portal.

**Reset the screen lock on a device**

1. Login to the Essentials portal.
2. Find the device you want to reset the screen lock for. The device must be active.
3. At the right of the device status, click More ➔ Reset screen lock.
4. Enter a new passcode. It must be between four and 16 characters.
5. Click Reset.

**Tip**

You can also do all of these actions by clicking on a device, this will bring up a side panel with information specific to the device you clicked on.

**When might you take this action?**

It can be common for users to forget their passcode on their device, leading to extensive troubleshooting with the user to guide them through remembering the passcode or being forced to factory reset the device to regain access. Resetting the passcode on behalf of the user allows them to quickly get back up and running. It is highly recommended that you encourage the user to change their passcode themselves once you’ve taken this action.

**What will your users experience?**

If the device is locked when the user goes to interact with it again they’ll need to input the new passcode. If the device is unlocked when the reset takes place the device will lock and request the input of the new passcode.
Device management

Essentials allows you to take proactive actions on your devices should it be required. Devices will require an internet connection to receive actions sent from the Essentials portal.

Wipe a device

Wiping a device deletes all data on the device and resets it to factory settings. Wiped devices are listed in your Essentials portal as Wiped. When a wiped device is set up again, Essentials security features will be re-enabled and its status will be updated to Active. To wipe a device:

1. Login to the Essentials portal.
2. Find the device you want to wipe. The device must be active.
3. At the right of the device status, click More ➔ Wipe device.
4. Click Wipe.

When might you take this action?

If a device is lost or stolen with little to no chance of recovery it may be in your interest to wipe the device of all its corporate data. Note that when the device next connects to a network after the reset it will reconnect to Essentials unless it has been removed from the portal. You may also take this action if you wish to reallocate the device to another user.

What will your users experience?

If the device has Internet connectivity it will reset immediately. Should the device be disconnected from the Internet it will reset once a connection has been established.
Device management

Devices will require an internet connection to receive actions sent from the Essentials portal.

Remove a device

Removing a device deletes all data on the device, resets it to factory settings, and removes the device from the Essentials portal. After a device is removed, Essentials security features won't be enforced.

To remove a device:

1. Login to the Essentials portal.
2. Find the device you want to remove.
3. At the right of the device status, click More ➤ Remove device.
4. Click Remove.

When might you take this action?

Removing a device from Essentials signals you’re no longer actively using the device within your organization. This could be due to the device being lost or stolen, or if you are looking to retire the device from your organization.

You might also take this action if you wish to manage this device in some other way, such as using an Enterprise Mobility Management (EMM) solution.

What will your users experience?

The user experience will be identical to wiping the device.

Tip

If a device is lost it may be easier to wipe it first before removing it. A device that is removed from the Essentials portal can only be re-added by a reseller.
Portal management

Rename a device
This name isn't visible or displayed on the device. It may be beneficial to rename a device to identify its use case, which user it is associated with, or which country it may be deployed to.

1. Login to the Essentials portal.
2. Find the device you want to rename.
3. At the right of the device status, click More → Rename device. Enter a name for the device. Click Rename.

Add multiple resellers from customer portal
If your organization purchases devices from multiple resellers you can add them into your existing Essentials portal. To add a reseller, follow the steps below:

1. Open the zero-touch customer portal. You might need to sign in.
2. Click Resellers in the sidebar.
3. For the reseller you would like to enroll, see under the Other resellers column.
4. Click Enroll next to reseller names.
5. It will be visible under Active resellers.

Portal languages
You can use the portal in one of the following languages:
American English, British English, Danish, Dutch, French, German, Italian, Japanese, Norwegian, Polish, Portuguese, Spanish, or Swedish.

To change to another language, update the preferred language in your Google Account. For more help, follow the instructions in Change language.

Supported browsers
Access the Essentials portal on your computer using the latest version of Chrome, Safari, Firefox for the best experience.

If you’re having trouble using your Essentials portal, try upgrading your browser to the latest version.

Tip
Renaming your devices makes the portal much easier to manage. You could look to name your devices after the user it’s being used by or their internal directory user name.
User management

When you sign up for Android Enterprise Essentials, the Google Account you use to first access the Essentials portal becomes an owner of the portal. As an owner, you can add other users to help you manage tasks in the portal.

Types of user roles

**Admin**
Access the portal and use the portal to view and manage devices.

**Owner**
The same privileges as an Admin, plus the ability to grant and revoke access to the Essentials portal.

Manage users
Only an owner can perform these tasks.

Add a new admin or owner

Tip
Add another Admin to your Essentials account, this will ensure your business can continue as usual should your main Admin be out of office.

1. Login to the [Essentials portal](#).
2. From the side menu, click Users.
3. Click Add user.
4. Enter the user’s email address. This must be a Google Account.
5. From the dropdown menu, choose Admin or Owner.
6. Click Add.

Edit an existing admin or owner

1. Login to the [Essentials portal](#).
2. From the side menu, click Users.
3. Select the user you want to edit.
4. Click Change role.
5. From the dropdown menu, choose Admin or Owner.
6. Click Update.

Remove an admin or owner

1. Login to the [Essentials portal](#).
2. From the side menu, click Users.
3. Select the user you want to remove.
4. Click Remove user.
5. Click OK.
Get help

For additional support, you can find answers to many questions about Android Enterprise Essentials in the following articles:

- Overview
- Sign up for Android Enterprise Essentials
- Essentials and Google Workspace basic mobile management
- Set up an Android Enterprise Essentials device
- Use the Android Enterprise Essentials portal

The Android Enterprise Help Community and your Essentials reseller and can help with the rest.

Contact your reseller for support
Get in touch with your Android Enterprise Essentials reseller if you:

- Are experiencing service, registration, or billing issues.
- Lose access to your owner account(s) and are unable to add a new owner in the portal.
- Need to reinstate a device that was unintentionally removed from your Essentials portal.
Get help

Ask the Help Community

If you have a general question about Android Enterprise Essentials or need help troubleshooting an issue that your reseller can’t address, post a question in the Android Enterprise help community and get answers from community experts.

I need more functionality

Android Enterprise Essentials has been designed to provide you just that, the essentials of device management. However, Android has a vast majority of great management functionality that you can migrate to through one of our Enterprise Mobility Management partners. In addition to the Android Enterprise Essentials functionality, our EMM partners extend additional Android Enterprise functionality including:

- Distributing and configuring applications
- Separating work and personal data
- Configuring settings and networks
- Managing devices in kiosk mode