Deploy ESET Endpoint Security for Android using ESET PROTECT

Steef | ESET Nederland - 2022-03-03 - Comments (0) - ESET PROTECT On-prem

Issue

- Remotely Deploy ESET Endpoint Security for Android to client devices using ESET PROTECT

Solution

Prerequisites

- ESET PROTECT and ESET Mobile Device Connector must be installed and activated. For more help, visit the ESET PROTECT Installation guide.
- You must have a valid ESET license. ESET Mobile Device Connector is activated with your ESET Endpoint Security license. How do I purchase a license?
- Managed devices must be running on Android version 5 and later.

To enroll Android devices in ESET Mobile Device Connector (MDC), follow the steps in each section:

> **Existing MDM Policy**
> If you already have a Mobile Device Management (MDM) Certificate and MDM Policy, enroll your Android device. Sections I and II only need to be completed again if a change was made to the hostname, policy, or certificate after the initial Certificate or Policy creation.

1. Create an MDM Certificate
2. Create an MDM Policy
3. Register your Android device in ESET PROTECT
4. Enroll your Android device
5. Create an Activation task for Android MDM

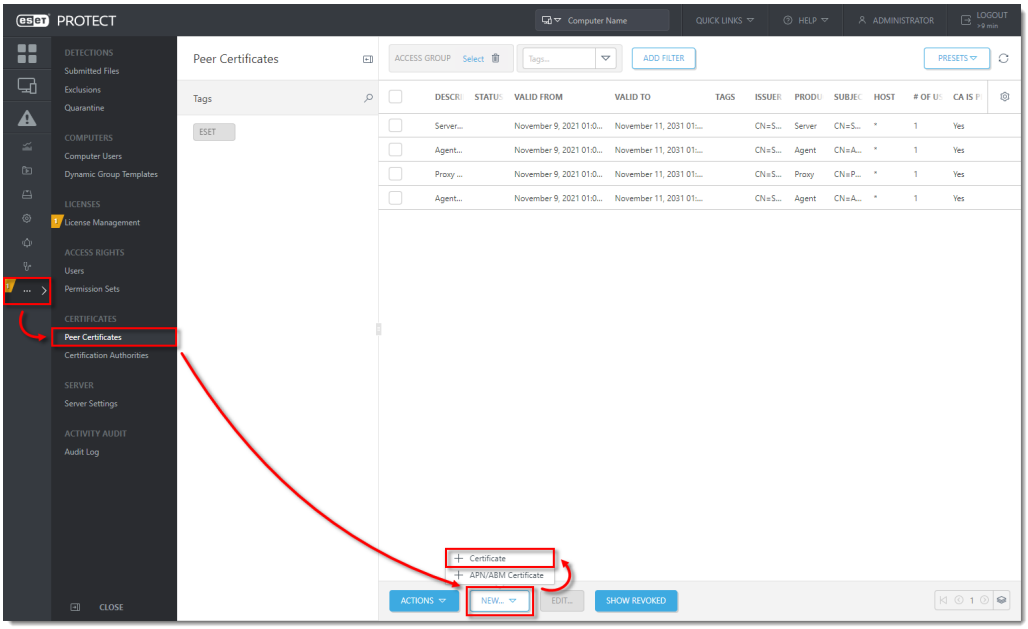
I. Create an MDM certificate

If you already have an MDM certificate, proceed to Section II: Create an MDM Policy.

> **MDM Certificate automatically created during some installations**
> The MDM certificate is automatically created if you used the all-in-one installation of ESET PROTECT Server with Mobile Device Connector or the Mobile Device Connector (Standalone) Installation.
>
> To verify the existence of an MDM certificate, follow these steps:
>
> 1. In the ESET PROTECT Web Console, click **Computers**.
> 2. Select the device on which Mobile Device Connector is installed and click **Show Details**.
> 3. Click **Configuration** → **Request Configuration**. The ESET PROTECT Mobile Device Connector configuration will be displayed. Select it and click **Open Configuration** to open it.
> 4. Click **General** → **HTTPS certificate** to verify that the MDM certificate is being applied.

1. Open the ESET PROTECT Web Console in your web browser and log in.

2. Expand **More**, click **Peer Certificate → New → Certificate**.



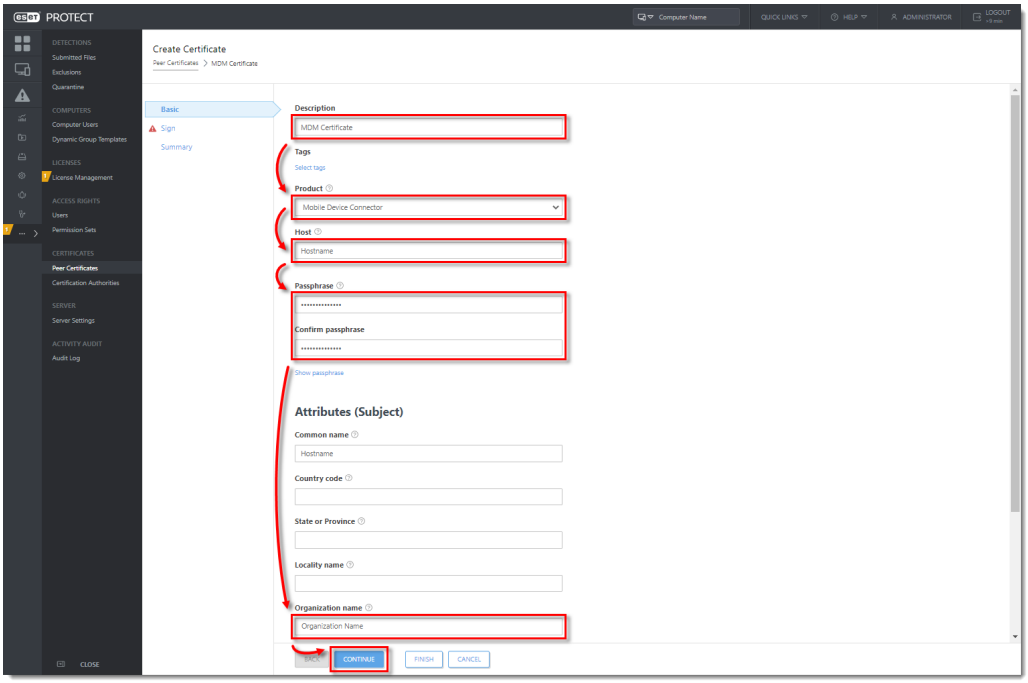
3. In the **Basic** section, type the **Description** of the certificate and select **Mobile Device Connector** from the **Product** drop-down menu. Type the IP address or Hostname of the server where Mobile Device Connector is installed in the **Host** field and type the **Passphrase** into respective fields. In the **Attributes (Subject)** section, type the organization name used in ESET PROTECT in the **Organization name** field. Click **Continue**.

If the MDM server does not have internet access and communications are port-forwarded from a router connected to an outside network

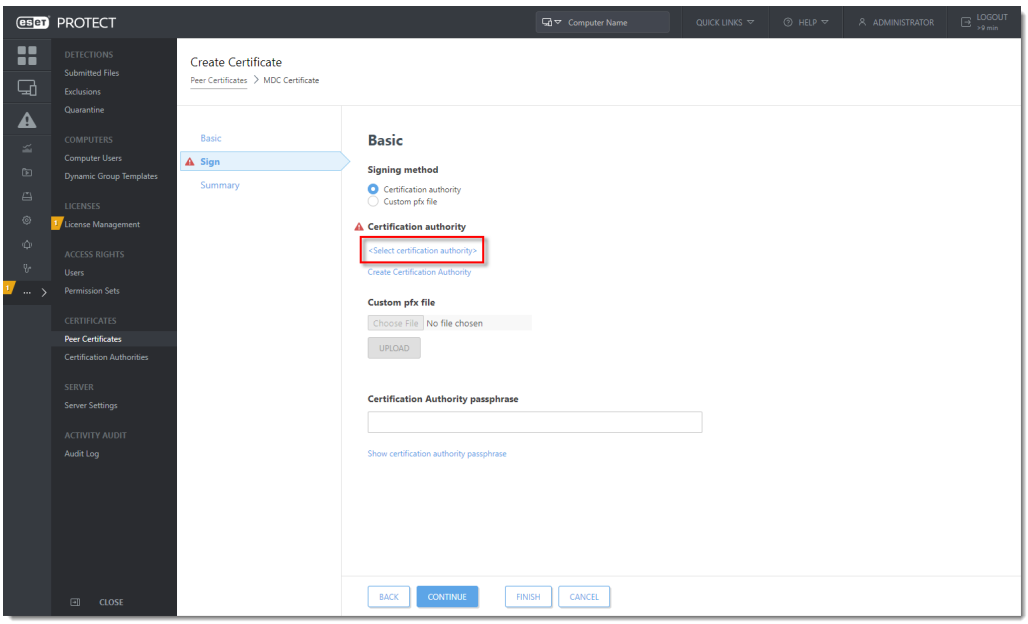
If the MDM server does not have internet access and communications are port-forwarded from a router connected to an outside network, use the IP address or Hostname of that router instead. You can also type in the IP address from the HTTPS certificate.

The Hostname in the HTTPS certificate must match the Hostname in the ESET Mobile Device Connector Policy

If you are using the hostname from the HTTPS certificate, you must also use this same hostname in the ESET Mobile Device Connector Policy.



4. In the **Sign** section, click **Select certification authority**.



5. Select the check box next to the certification authority that you want to use and click **OK**.

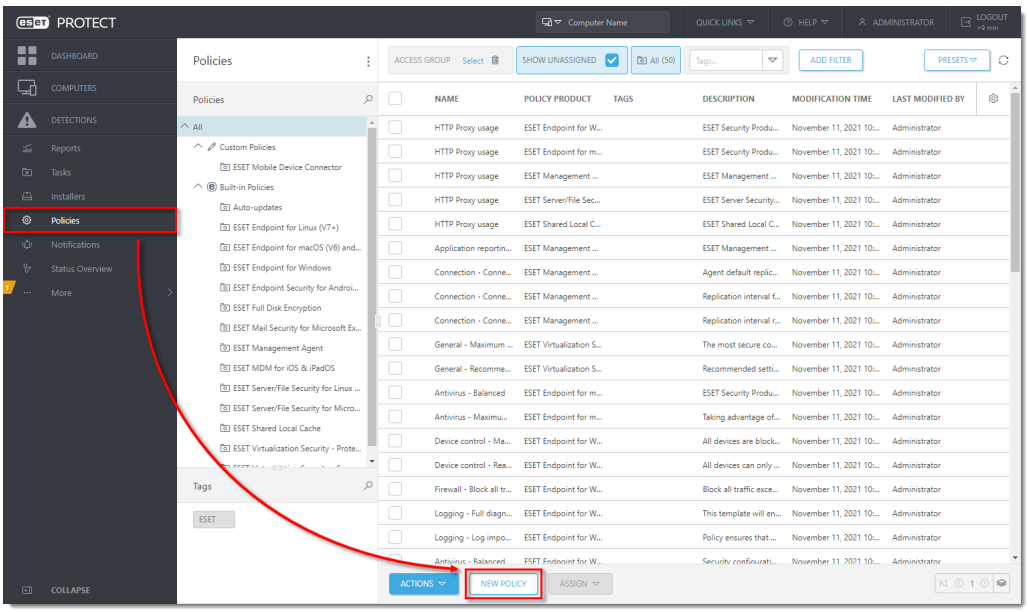


6. Click **Finish** and proceed to Create an MDM Policy.

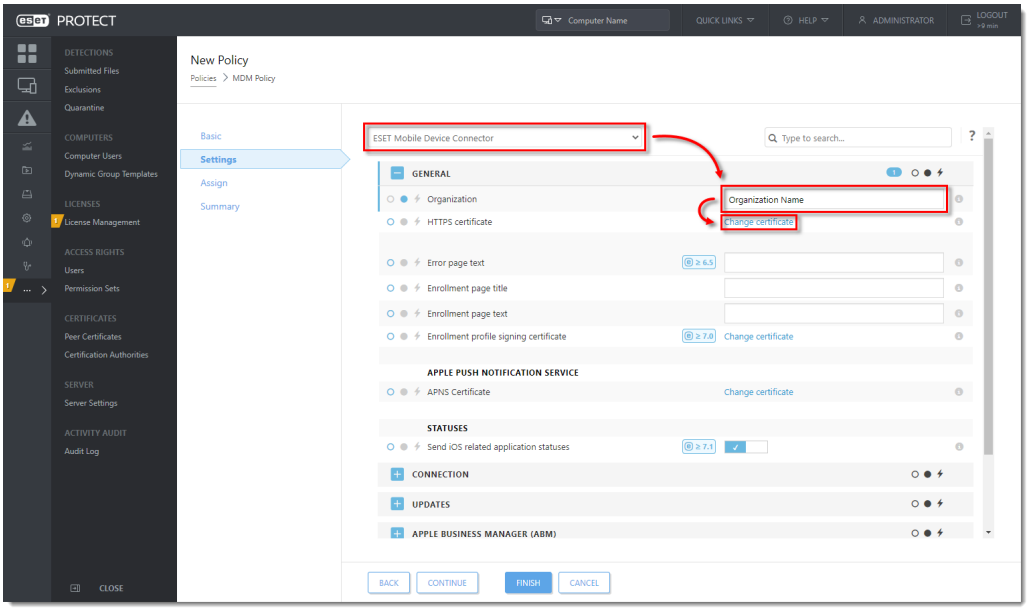
II. Create an MDM Policy

1. Open the ESET PROTECT Web Console in your web browser and log in.

2. Click **Policies → New Policy**.

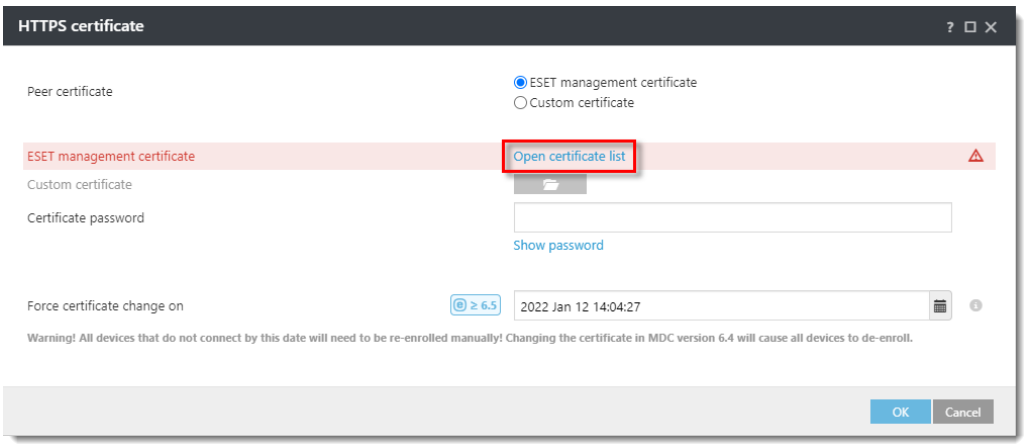


3. In the **Basic** section, type a name for the policy in the **Name** field (the **Description** field is optional). Click **Continue**.
4. In the **Settings** section, select **ESET Mobile Device Connector** from the drop-down menu. Type the organization name used in ESET PROTECT into the **Organization** field. This name will be used by the enrollment profile generator to update the profile. Click **Change certificate** next to **HTTPS certificate**.

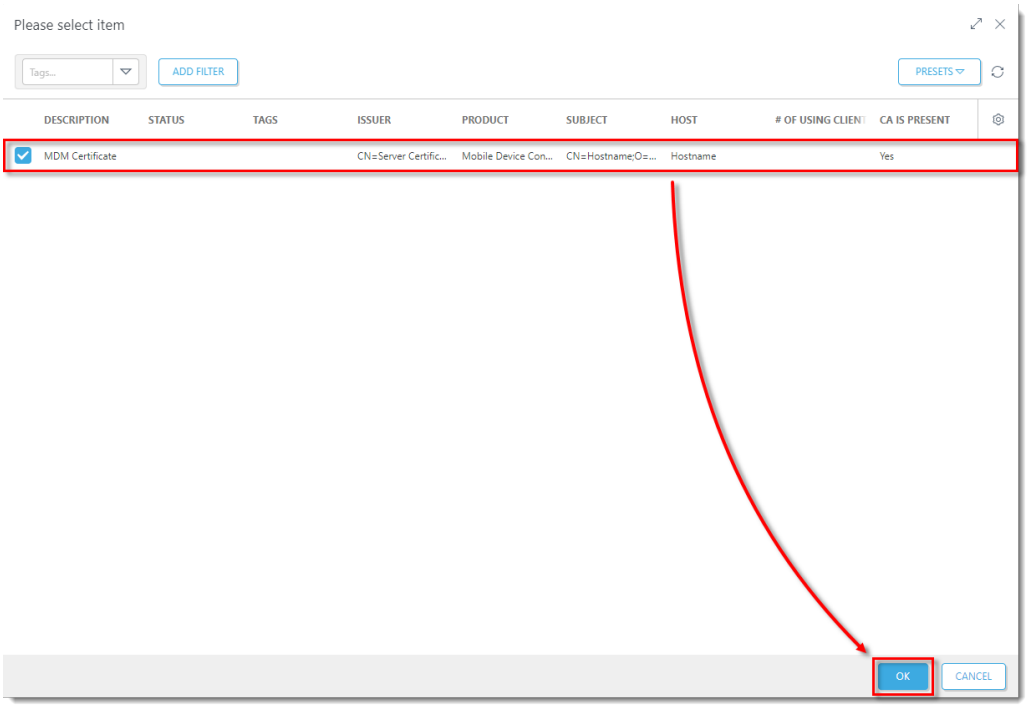


5. Click **Open certificate list**.

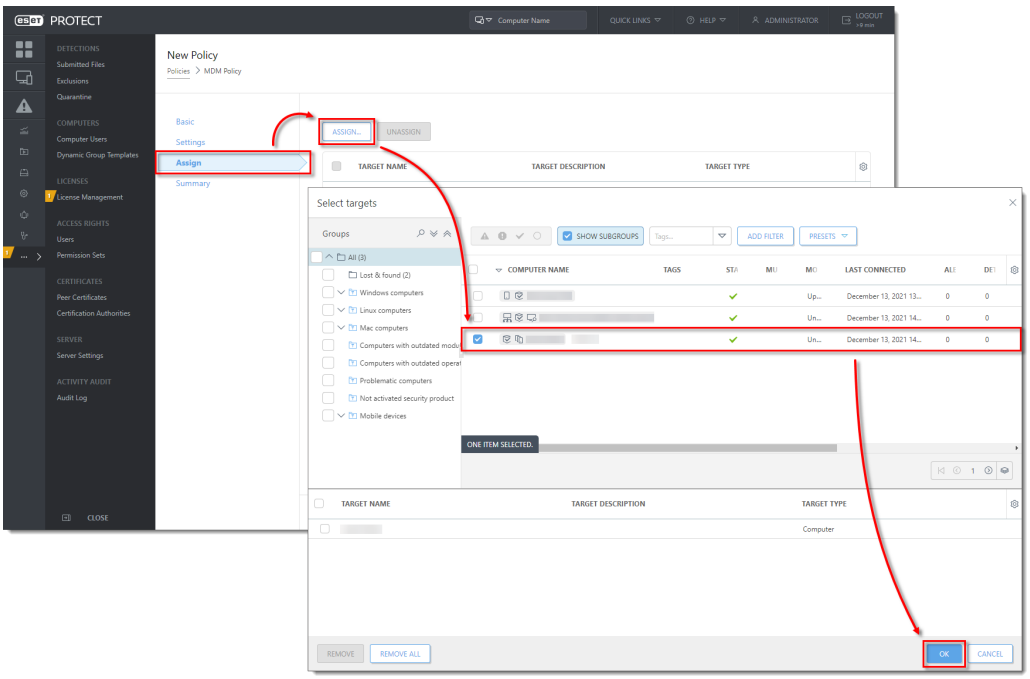
> **Changing the certificate used in your policy for MDM**
> When the certificate change is initiated, do not restart the MDM service or the MDM host device until the certificate change is completed. Restart during the certificate change may damage the process.



6. Select the **MDM Certificate** created in Section I and click **OK**.



7. In the **Assign** section, click **Assign** to display all Static and Dynamic Groups and their members. Select the check box next to the Mobile Device Connector instance to which you want to apply the policy and click **OK**.



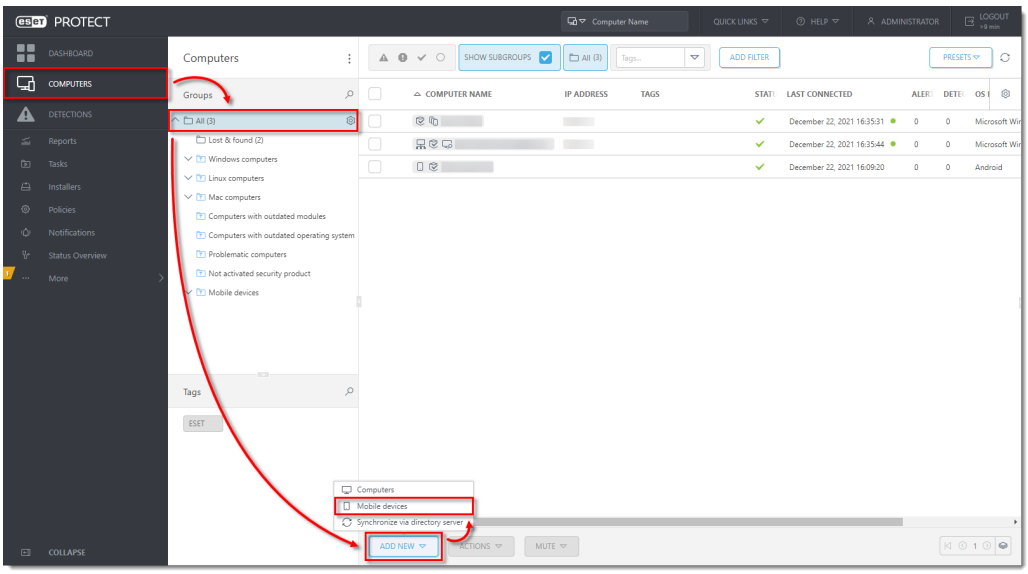
> **Changing the HTTPS certificate for MDC**
>
> When changing the HTTPS certificate used in your policy for MDC, follow the steps below to avoid disconnecting mobile devices from your MDM:
>
> 1. Create and apply the new policy that uses the new HTTPS certificate.
> 2. Allow devices to check in to the MDM server and receive the new policy.
> 3. Verify that devices are using the new HTTPS certificate (the HTTPS certificate exchange is completed).
> 4. Allow at least 72 hours for your devices to receive the new policy. After all the devices have received the new policy (MDM Core alert "HTTPS certificate change still in progress. The old certificate is still being used" is no longer displayed in the Alerts tab), you can delete the old policy.

8. When you are finished, proceed to Section III: Register your Android device in ESET PROTECT and send an enrollment link.

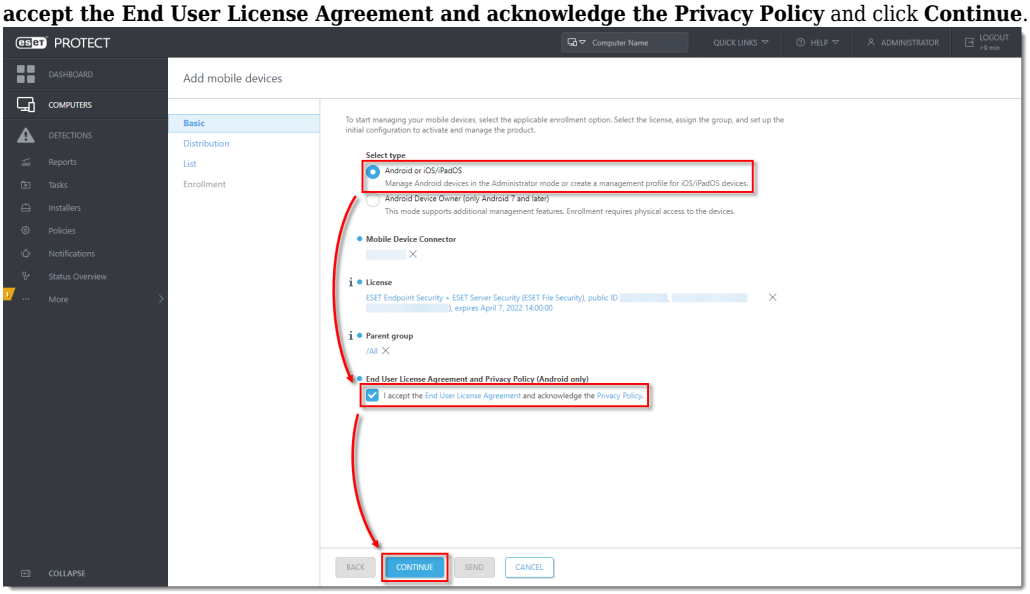
III. Register your Android device in ESET PROTECT and send an enrollment link

1. Open the ESET PROTECT Web Console in your web browser and log in.

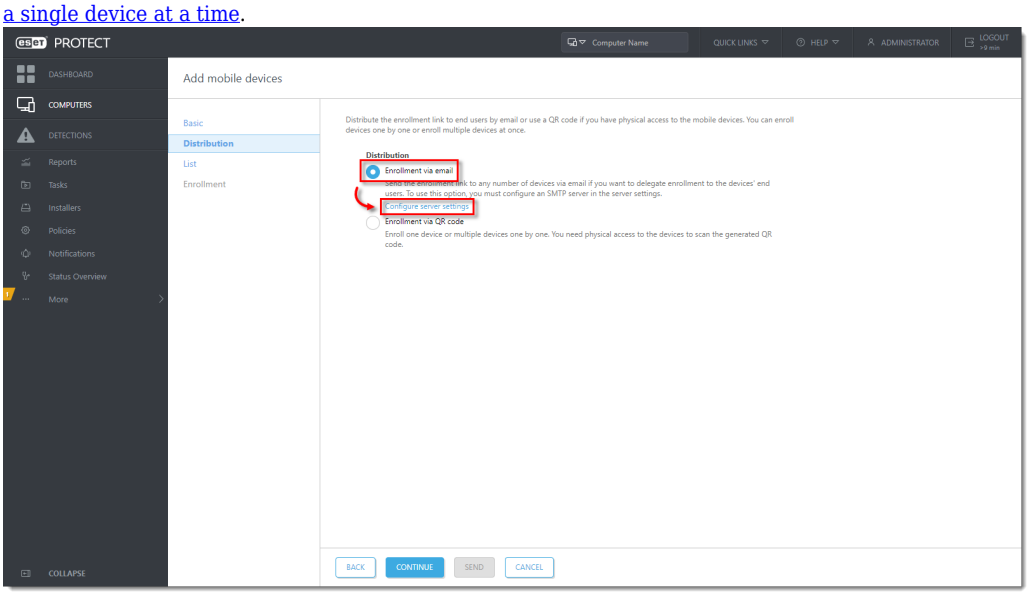
2. Click **Computers**, select the group to which you want to add your mobile device and then click **Add New → Mobile devices**.



3. In the **Basic** section, ensure that **Android or iOS/PadOS** is selected. Select the check box next to **I accept the End User License Agreement and acknowledge the Privacy Policy** and click **Continue**.



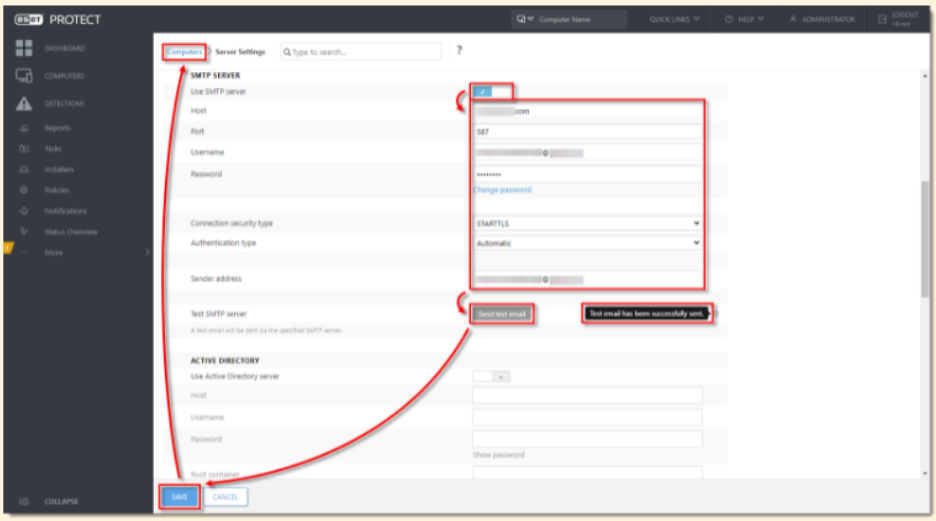
4. In the **Distribution** section, select **Enrollment via email** and click **Configure server settings**. Enroll a single device at a time.



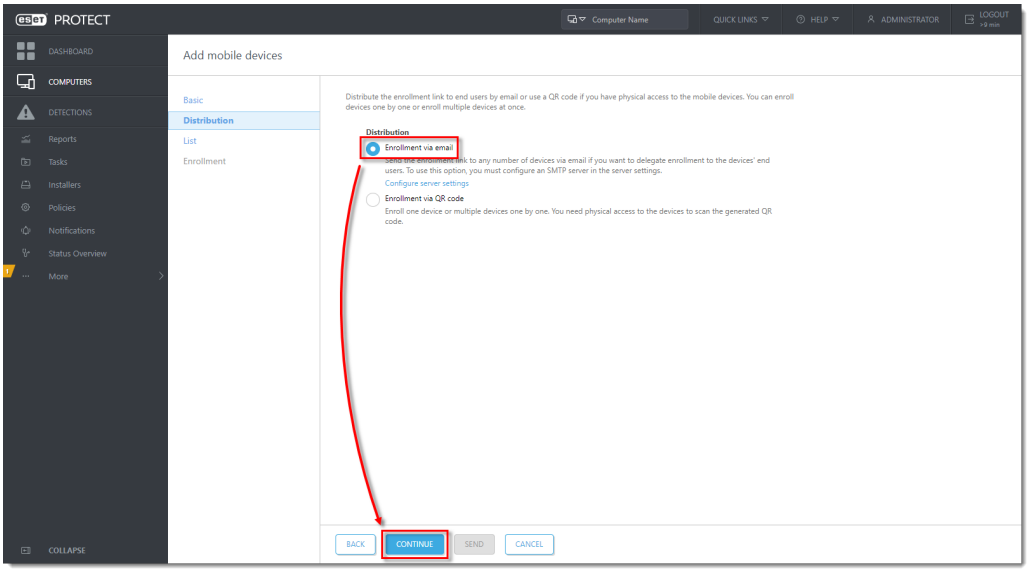
Configure SMTP server settings

Before you can add multiple devices using mass enrollment, you must set up the Simple Mail Transfer Protocol (SMTP) server.

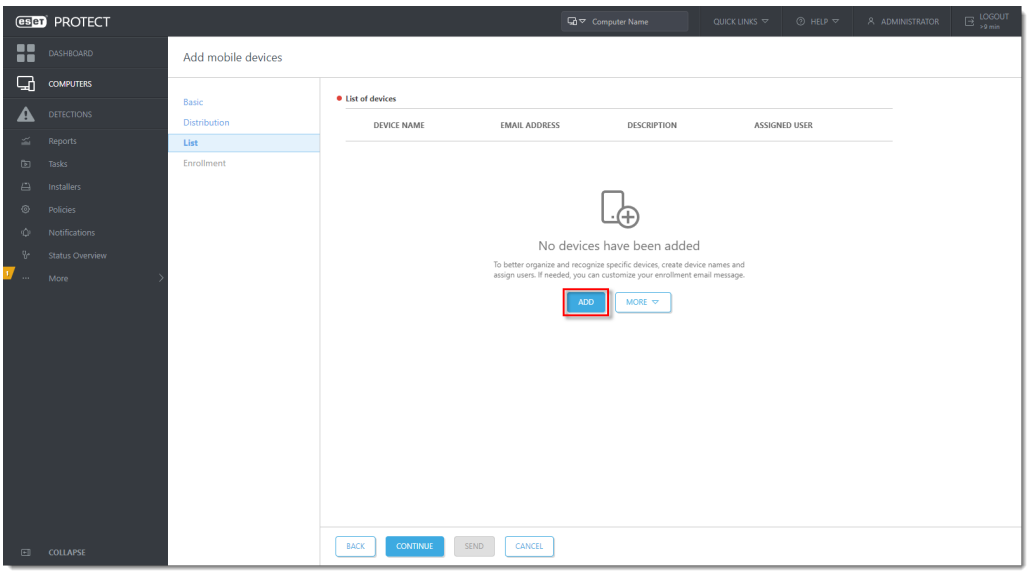
Click the slider bar next to **Use SMTP server** to enable it. Complete the required fields as shown in Figure 3-4. To verify that everything works correctly, click **Send test email**. If you get the **Test email has been successfully sent** notification, check your mailbox. If you receive the test email, everything is working correctly. Click **Save** to save the changes and click **Computers**.



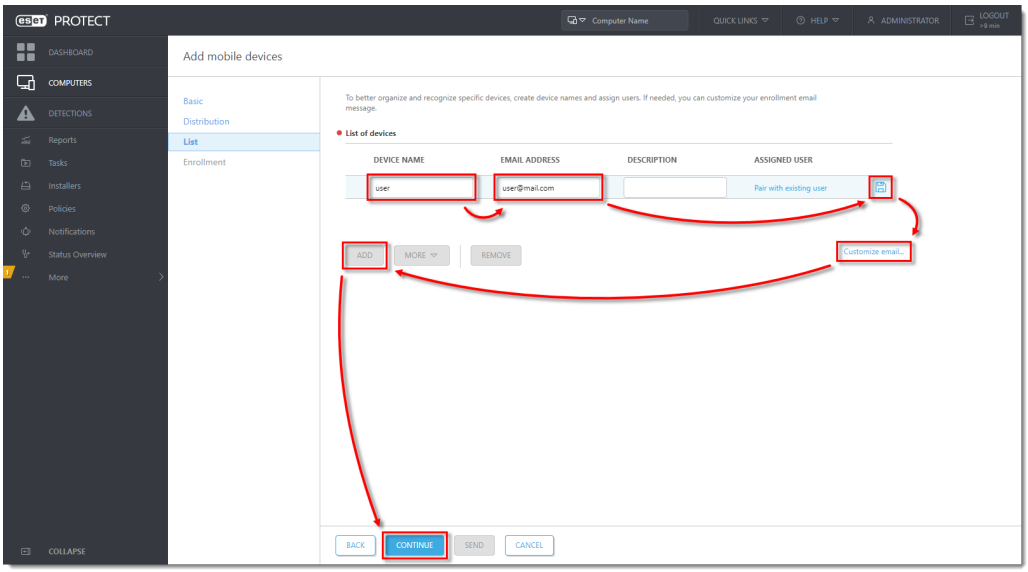
5. Follow steps 2-3 of this section again. Select **Enrollment via email** and click **Continue**.



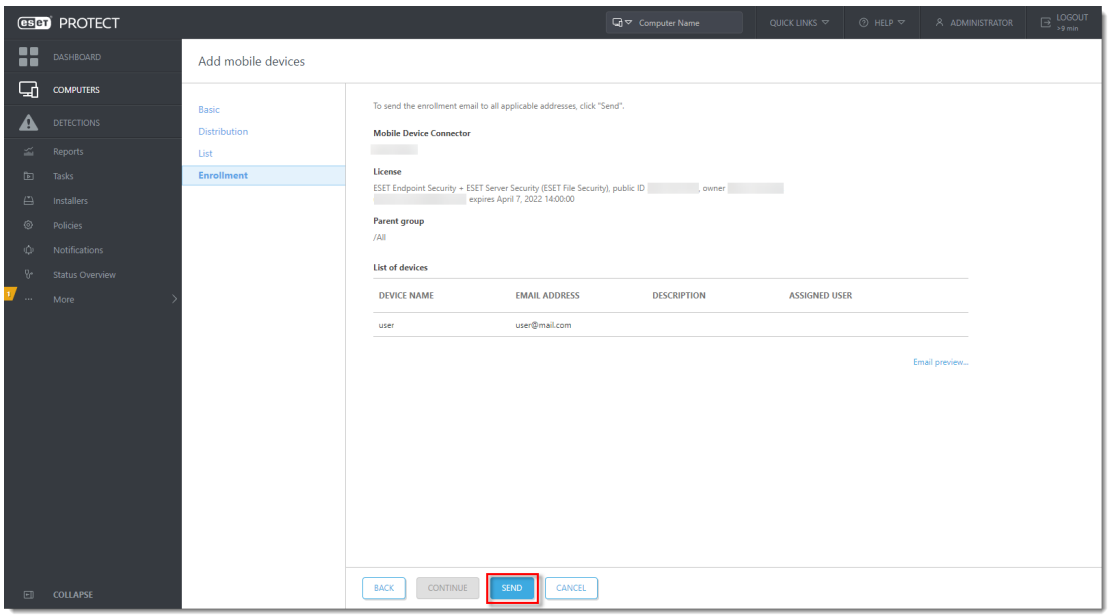
6. In the **List** section, click **Add**.



7. Type in the **Device name** and **Email Address** (this email address will be used to deliver the enrollment email message). The **Description** field is optional. To assign a specific user, click **Pair with existing user** to match it to an existing Computer User. Click the **Save** icon to save the device. Click **Customize email** if you want to make changes to the enrollment email. To add another device, click **Add**. Click **Continue** when you are finished adding devices.



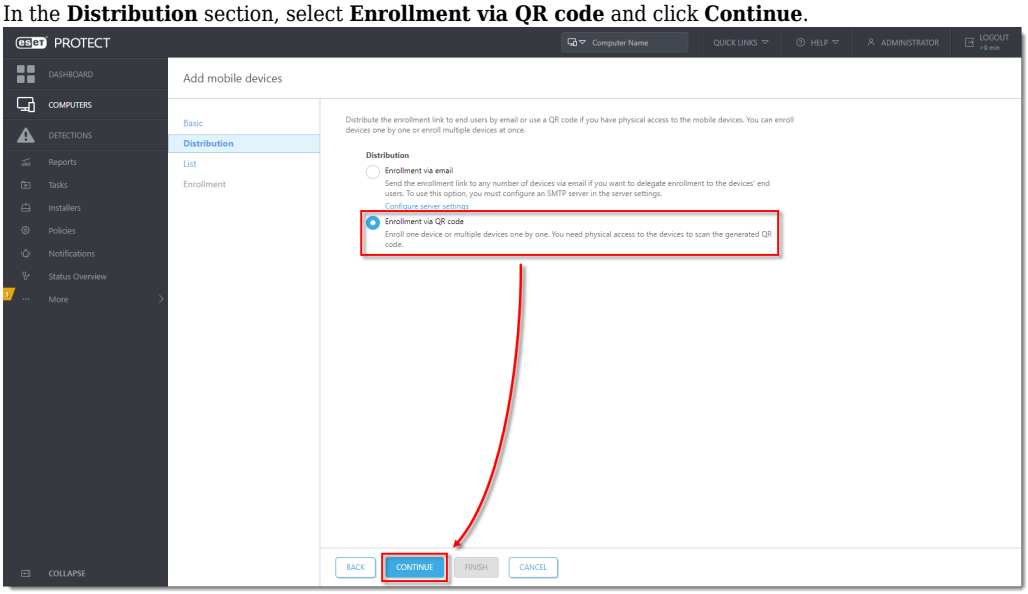
8. In the **Enrollment** section, click **Send**. The enrollment link will be sent to chosen devices.



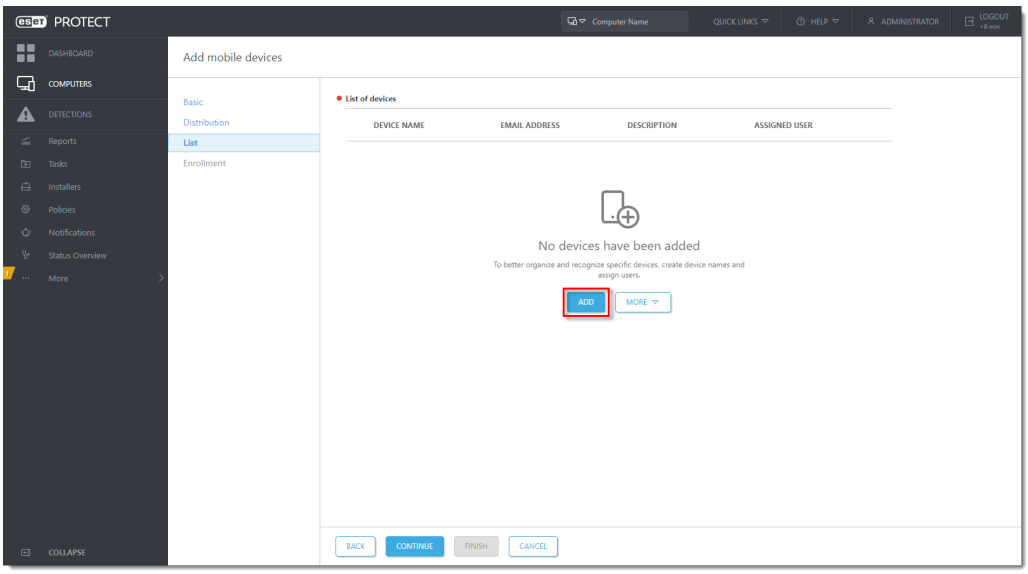
Enroll a single device

1. Follow steps 2-3 of Register your Android device in ESET PROTECT and send an enrollment link section above.

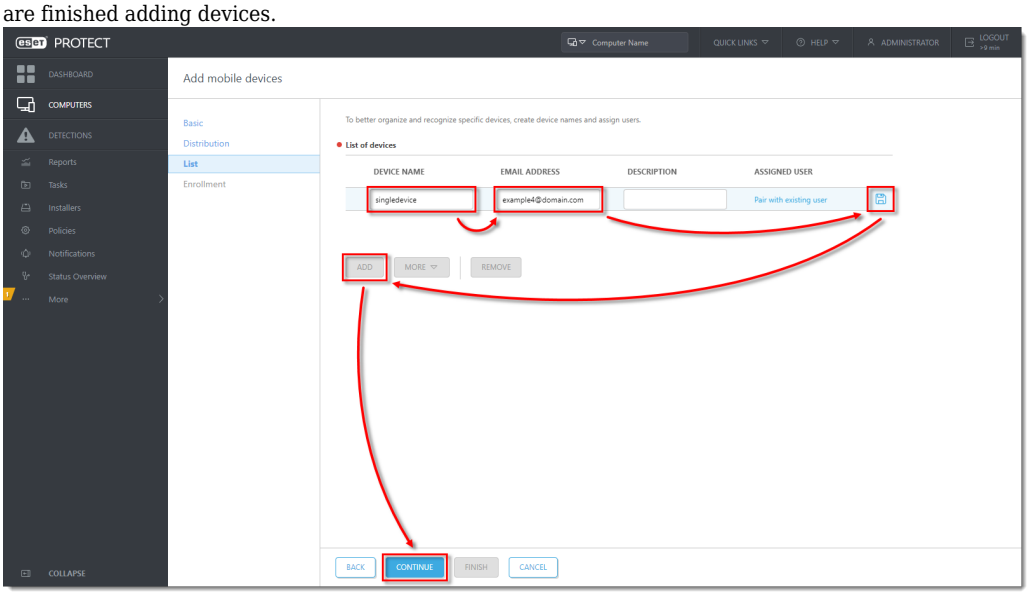
2. In the **Distribution** section, select **Enrollment via QR code** and click **Continue**.



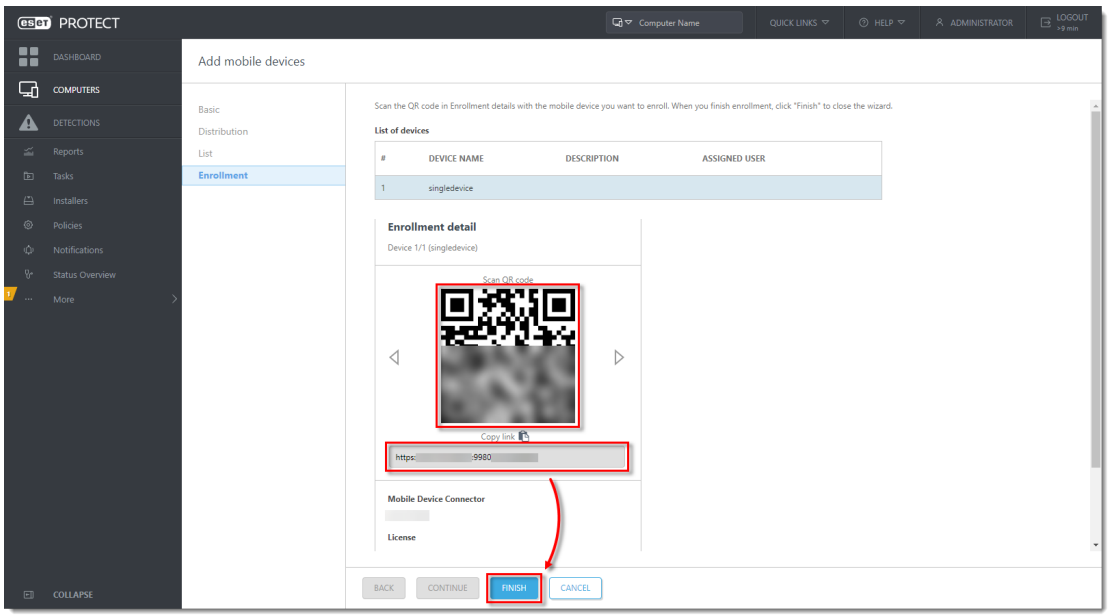
3. In the **List** section, click **Add**.



4. Type the **Device name** and **Email address** in the appropriate fields. The **Description** field is optional. To assign a specific user, click **Pair with existing user** to match it to a designated policy. Click the **Save** (floppy disk) icon to save the device. To add another device, click **Add**. Click **Continue** when you are finished adding devices.

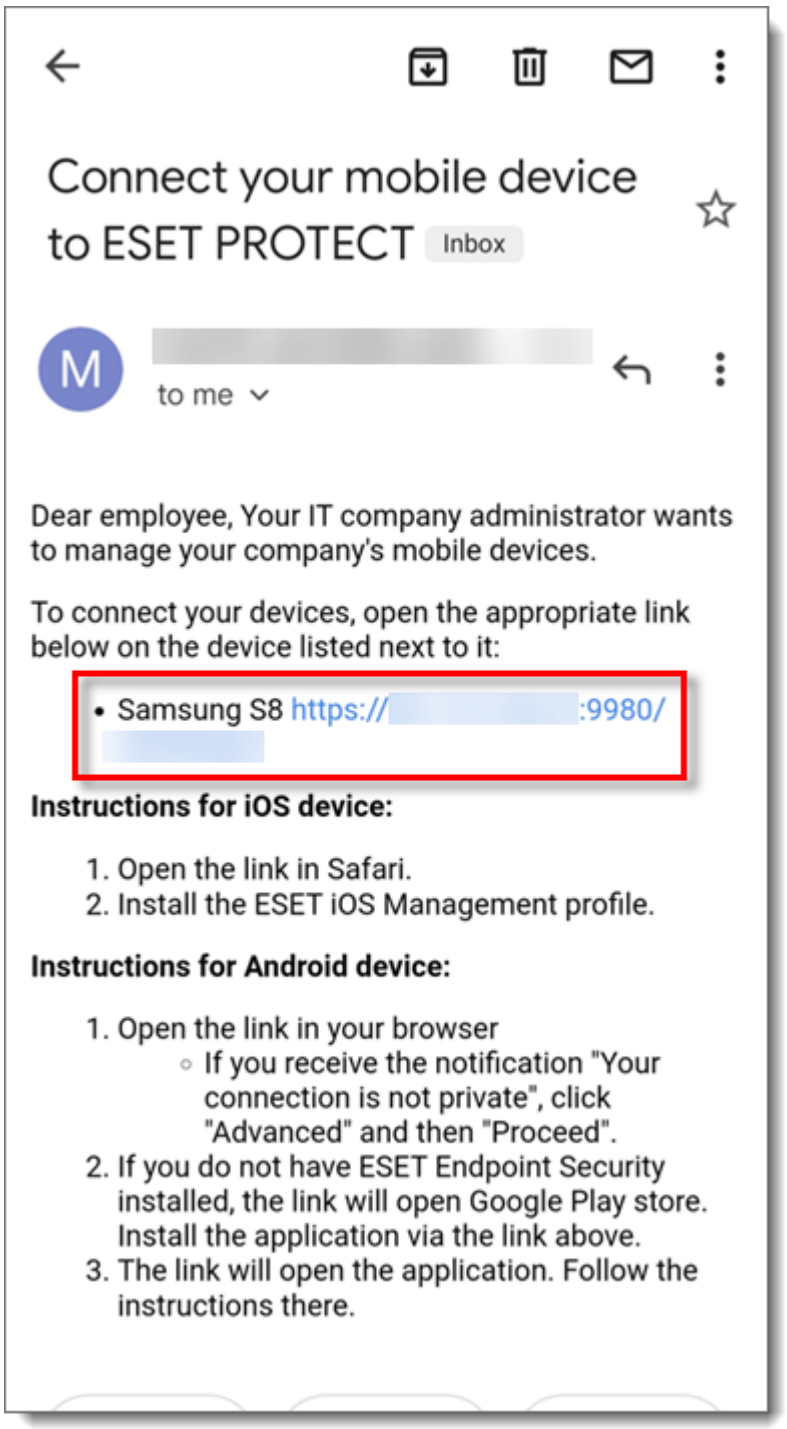


5. In the **Enrollment** section, the preview window will display a summary of the enrollment, including the download link and the QR code. Send the enrollment link to the mobile device using email or an instant messaging application if the device is not physically present. If the device is physically present, scan the QR code with the mobile device and proceed to Section IV: Enroll your Android device and deploy ESET Endpoint Security for Android. To enroll another device, click **Finish** and repeat the process described in this sub-section.



IV. Enroll your Android device and deploy ESET Endpoint Security for Android

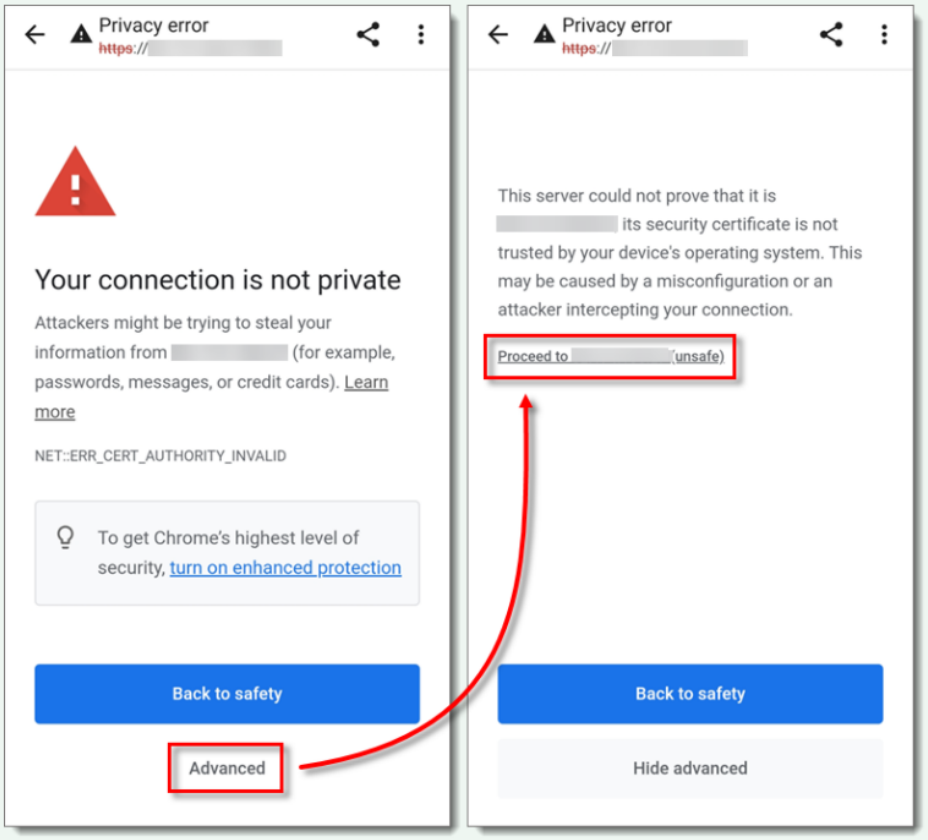
1. On the mobile device, open the enrollment email that was sent in Section III above and tap the



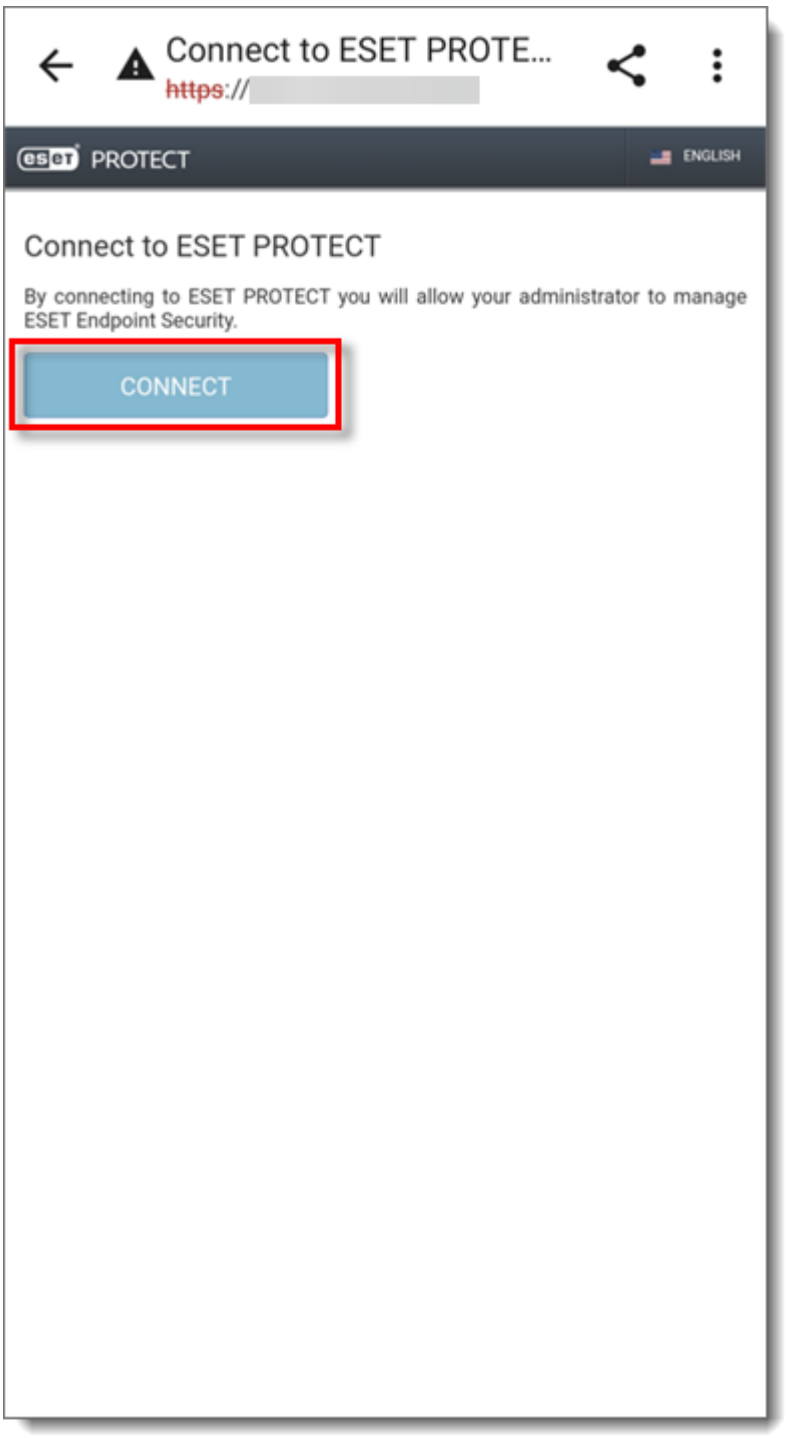
enrollment link.

'Your Connection is not private' error message

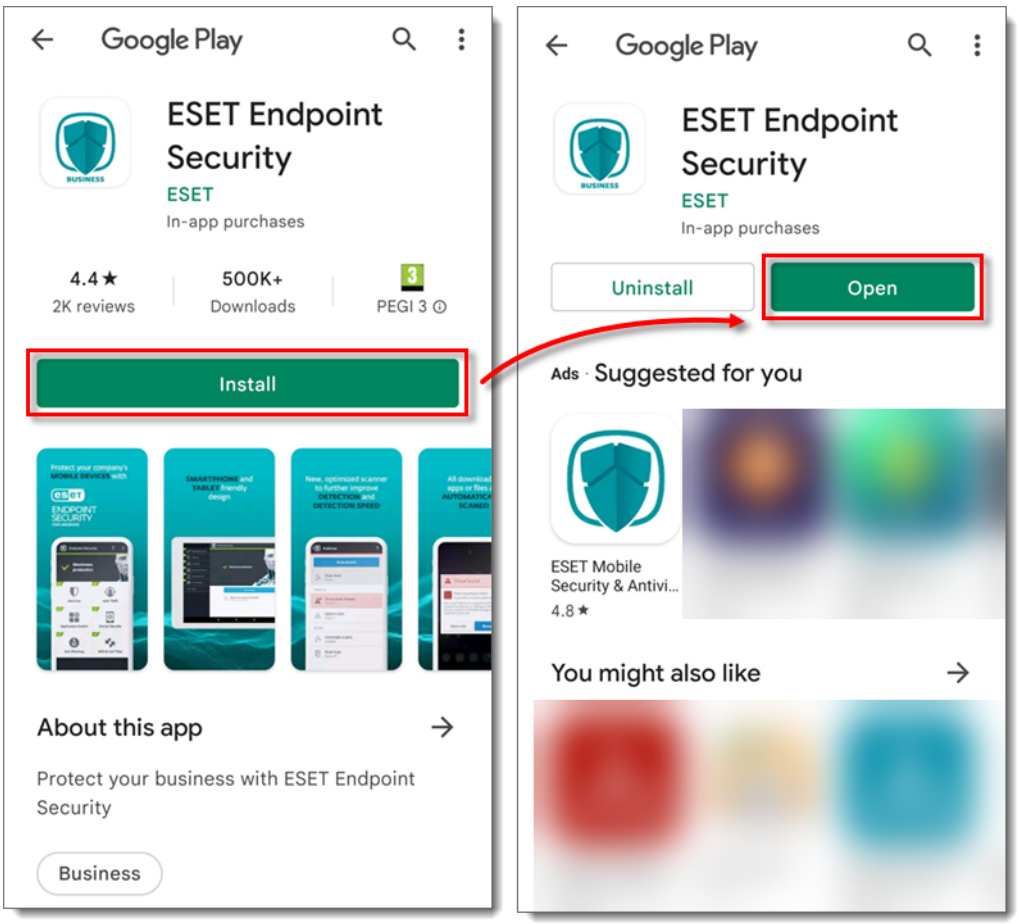
If you do not use SSL protocol you may be notified that the enrollment link is not private. If you receive this notification, tap **Advanced** and on the next screen, tap **Proceed to *hostname* (Unsafe)**.



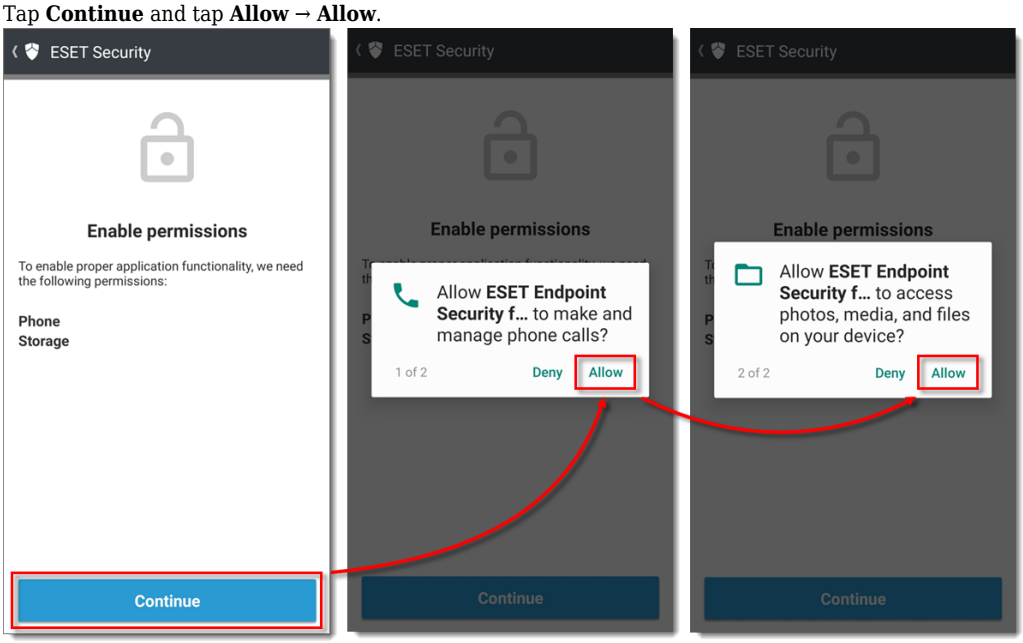
2. Tap **Connect**.



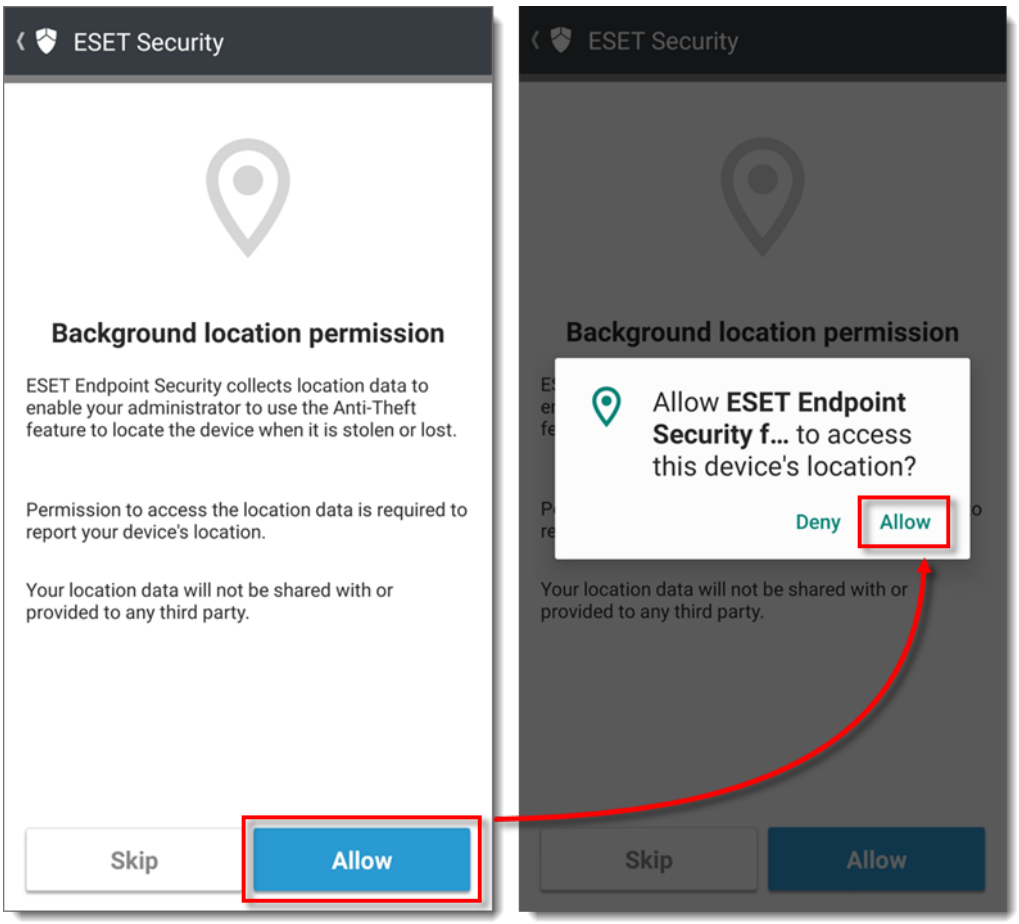
3. You will be redirected to Google Play Store. Tap **Install** and wait for the installation to finish. Tap **Open**.



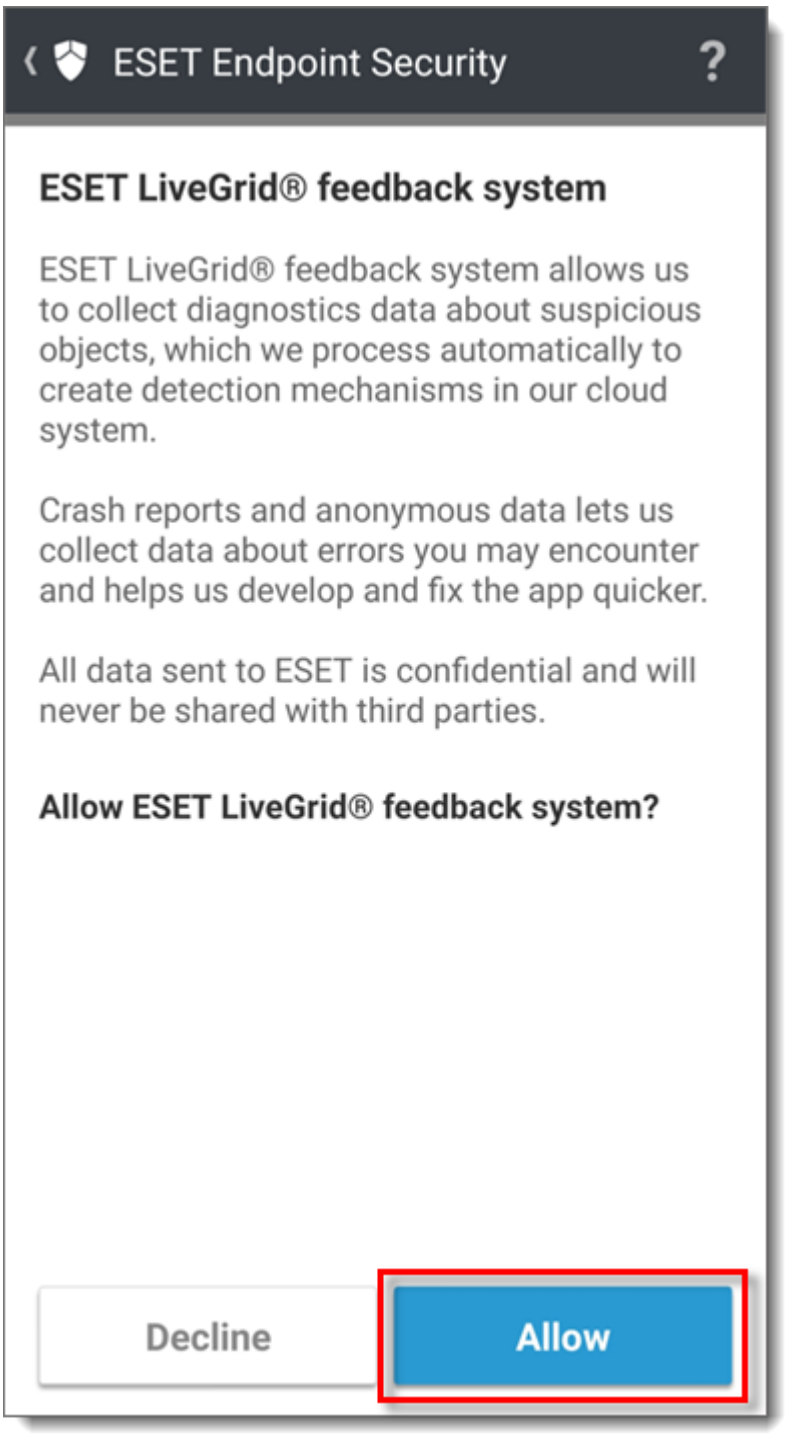
4. Tap **Continue** and tap **Allow** → **Allow**.



5. **Tap Allow → Allow.**



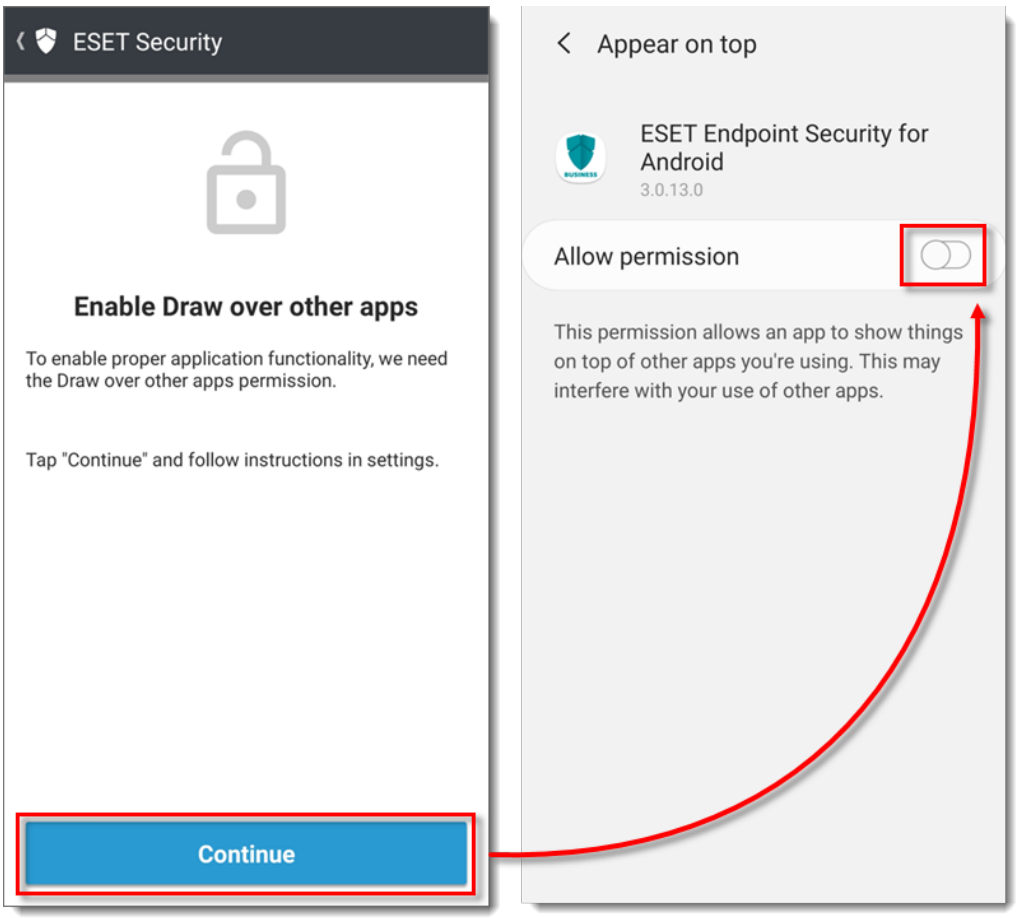
6. Tap **Allow** if you want to allow the ESET LiveGrid feedback system.



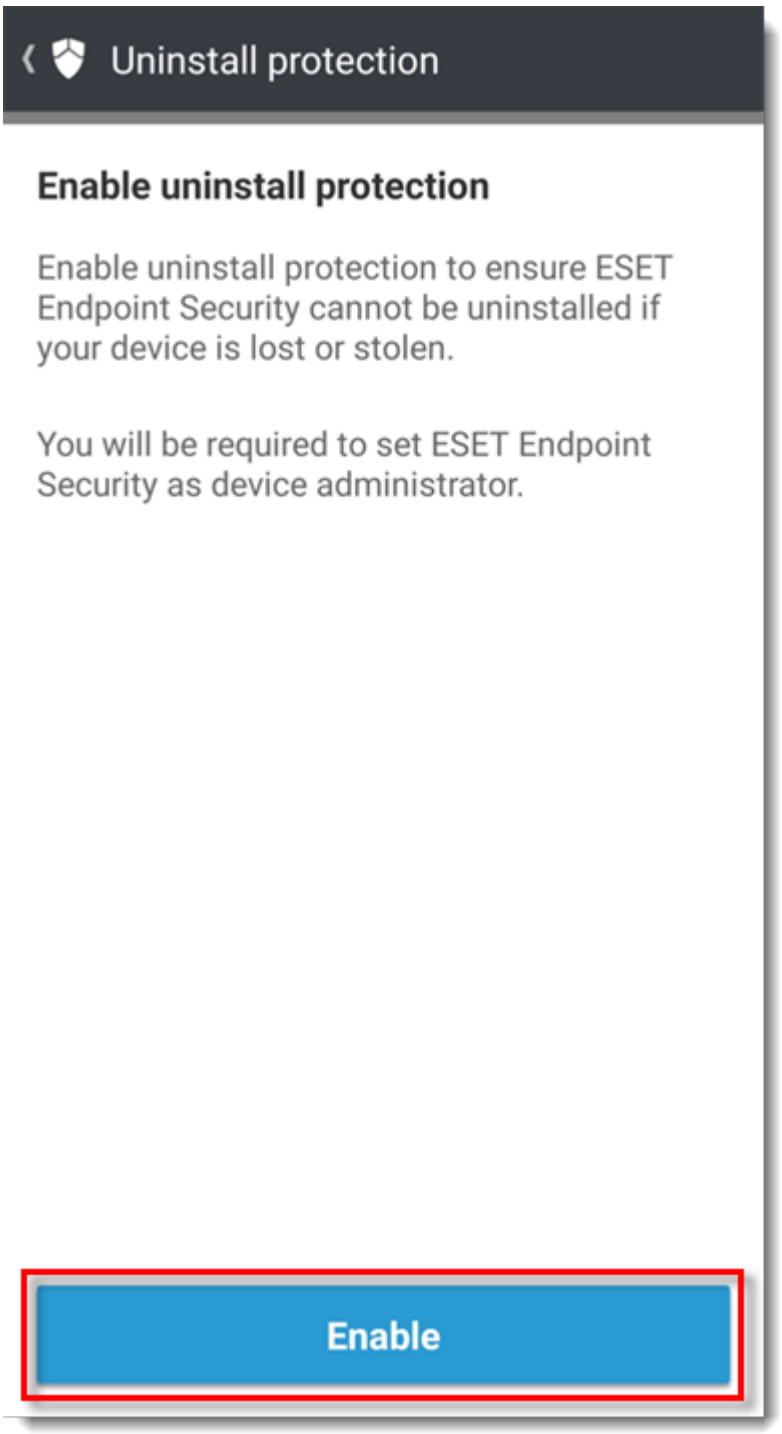
7. Type your name into the **Name** field and tap **Save**. This will help the administrator recognize your device.



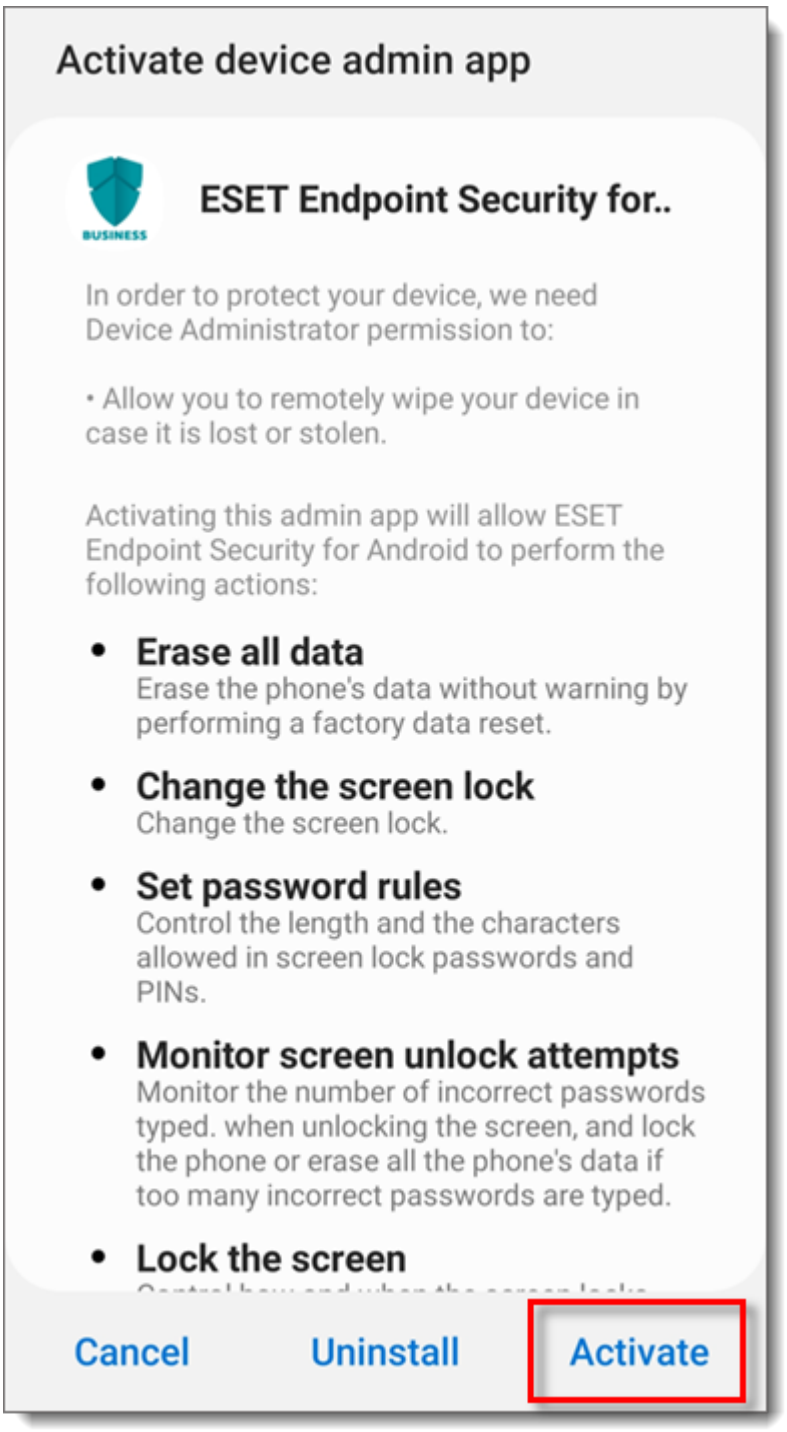
8. Tap **Continue** and tap the slider bar next to **Allow permission** to enable it.



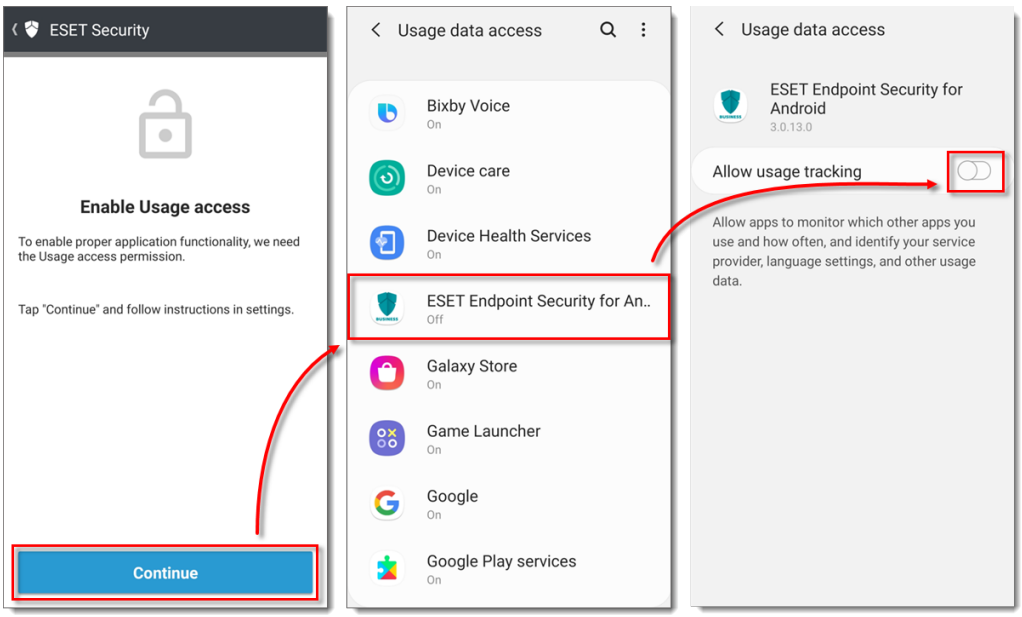
9. Tap **Enable** to enable uninstall protection. Uninstall protection restricts unauthorized users from uninstalling ESET Endpoint Security for Android.



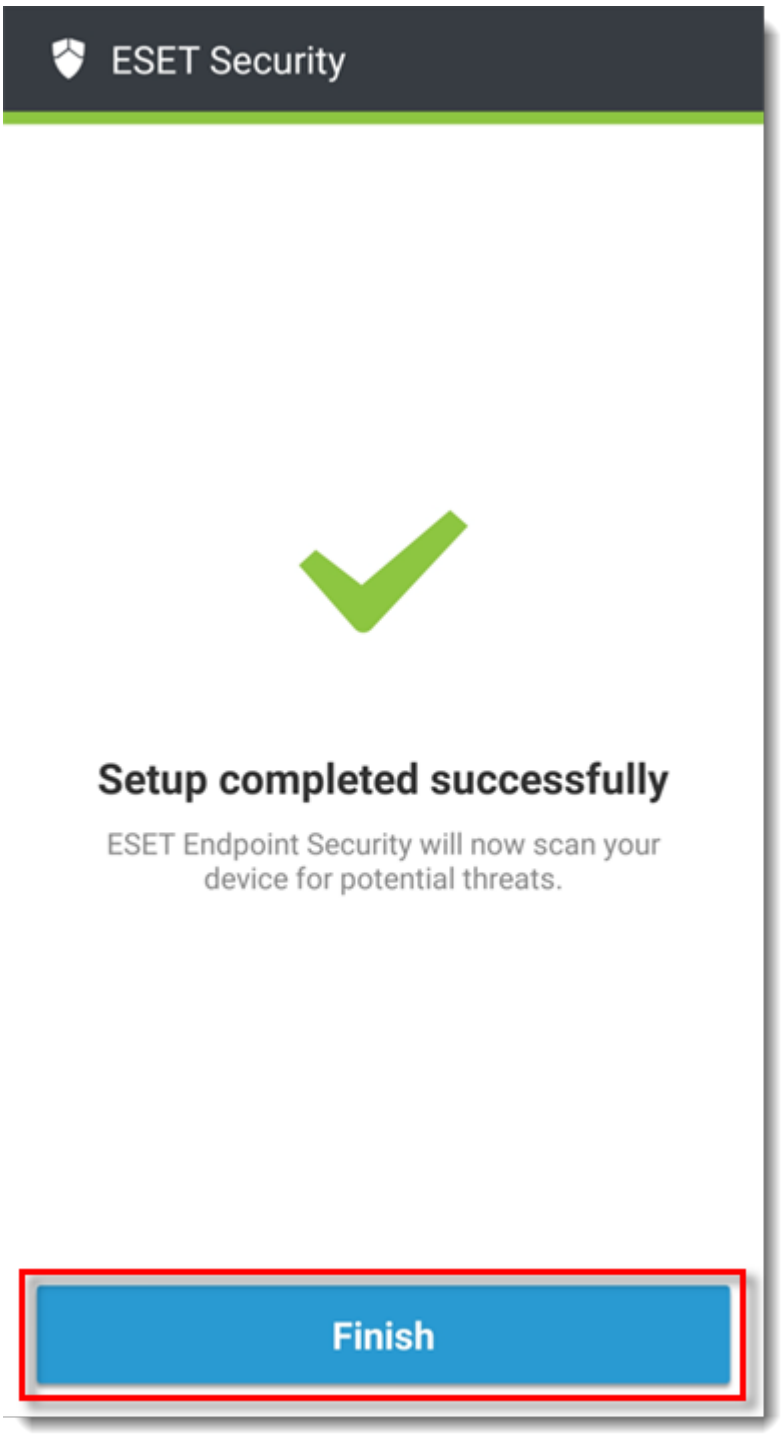
10. Tap **Activate** to activate the Admin app.



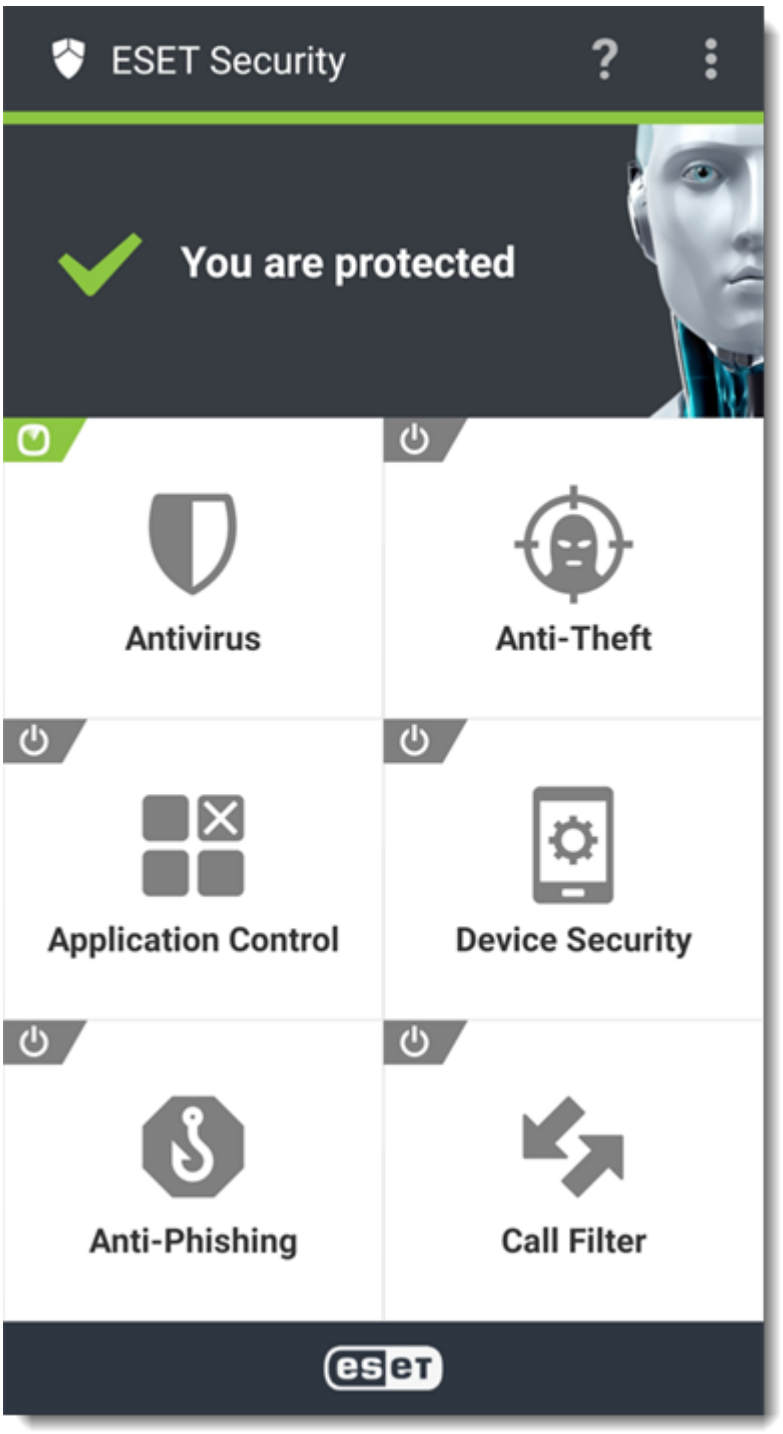
11. Tap **Continue → ESET Endpoint Security for Android**. Tap the slider bar next to **Allow usage tracking** to enable it.



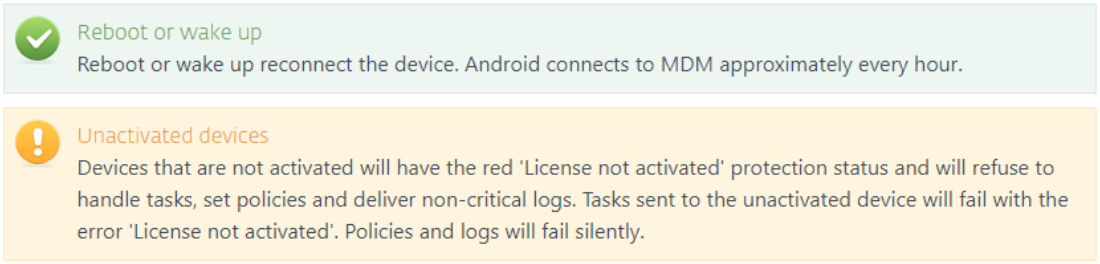
12. Tap **Finish** to activate ESET Endpoint Security for Android as Device Administrator.



13. The Android device is now protected.



14. Proceed to Section V: Create activation task for Android MDM.



V. Create activation Task for Android MDM

After completing sections I-IV above, the device will appear in the **Computers** section of ESET PROTECT under **Lost & Found** and will automatically be added to the dynamic group **Mobile devices → Android devices**.

Follow the instructions to activate ESET business products using ESET PROTECT.