ESET Tech Center

How do I deploy ESET Endpoint Security for Android (2.x) using ESET Remote Administrator? (6.x)

Ondersteuning | ESET Nederland - 2017-11-08 - Comments (0) - 6.x

https://support.eset.com/kb3686

Issue

Remotely Deploy ESET Endpoint Security for Android 2.x to client devices using ESET Remote Administrator

Do you manage Apple iOS devices?

Solution

Before you continue, these prerequisites must be met:

ESET Remote Administrator 6.3 or later and ESET Mobile Device Connector must be installed and activated. For more help, visit the ERA 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 4 (Ice Cream Sandwich) and later.

ESET Remote Administrator version 6.3 and earlier:

For ERA version 6.3 continue here.

To enroll Android devices in ESET Mobile Device Connector, follow the

steps in each section:

I. Create an MDM Certificate

II. Create an MDM Policy

III. Register your Android device in ERA

IV. Enroll your Android device

V. Create an Activation task for Android MDM

Pre-existing MDM Policy

If you already have an MDM Certificate and MDM Policy, proceed to 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.

If you do not use ESET Remote Administrator to manage your network

Perform these steps on individual client devices.

I. Create an MDM certificate

If you already have an MDM certificate, proceed to 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 Remote Administrator Server with Mobile Device Connector or the Mobile Device Connector (Standalone) Installation. To verify the existence of an MDM certificate, navigate to the **Computers** section in the ERA

Web Console, select the device on which Mobile Device Connector is installed and click **Show Details**.
Click **Configuration → Request Configuration**. The ESET Remote Administrator Mobile Device Connector configuration will be displayed. Select it and click **Open Configuration** to open it. Click **General → HTTPS certificate** to verify that the MDM certificate is being applied.

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in. How do I open ERA Web Console?

2. Click **Admin→ Certificates → New → Certificate**.

Figure 1-1

Click the image to view larger in new window

3. In the **Basic** section, 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.

    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 enter the IP address from the HTTPS certificate.

The Hostname in the HTTPS certificate must match the Hostname that you will enter 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 **Attributes (Subject)** section, type the organization name used in ESET Remote Administrator in the **Organization Name** field.

Figure 1-2

Click the image to view larger in new window

5. Expand the **Sign** section and click **Select Certification Authority**.

Figure 1-3

Click the image to view larger in new window

6. Select the certification authority that you want to use and click **OK**.

Figure 1-4

Click the image to view larger in new window

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

II. Create an MDM Policy

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in. How do I open ERA Web Console?

2. Click **Admin** → **Policies**.

3. Click **New Policy**.

Figure 2-1

Click the image to view larger in new window

4. Expand **Basic** and type a name for the policy in the **Name** field (the **Description** field is optional).

5. Expand **Settings** and select **ESET Remote Administrator Mobile Device Connector** from the drop-down menu.

Figure 2-2

Click the image to view larger in new window

6. Type the IP address of the server where Mobile Device Connector is installed in the **Hostname** field. 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 adress or Hostname of that router instead.

> The Hostname in the HTTPS certificate must match the Hostname that you entered in the MDM Certificate from section I
>
> If you entered the IP address from the HTTPS certificate in section I step 3, you must also enter that same IP address in the **ESET Mobile Device Connector Policy**.

7. Type the organization name used in ESET Remote Administrator in the **Organization** field. This name will be used by the enrollment profile generator to update the profile.

8. In the **HTTPS certificate** section, click **Change certificate → Open certificate list**, select the **MDM Certificate** created in part II and then click **OK**.

Figure 2-3

Click the image to view larger in new window

9. Expand the **Assign** section and click **Assign** to display all Static and Dynamic Groups and their members. Select the Mobile Device Connector instance to which you want to apply the policy and click **OK**.

Figure 2-4

Click the image to view larger in new window

> ### Important!
>
> 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 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.

When you are finished, proceed to Register your Android device in ERA.

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

View instructions for ERA version 6.3 or earlier

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in. How do I open ERA Web Console?

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

Figure 3-1

Click the image to view larger in new window

3. In the **Add mobile devices** window, select **Enrollment via e-mail** and click **Continue**. Click here for instructions to enroll a single device at a time.

Figure 3-2

Click the image to view larger in new window

Configure SMTP Server Settings

Before you can add multiple devices using mass enrollment, you must setup the SMTP server. To do so, click **Configure server settings** in the **Add mobile devices** window, click **Server settings**, expand **Advanced settings**, and then select the slider bar next to **Use SMTP server** to enable it.

Complete the required fields in the **SMTP Server** section. To verify that everything is working, click **Send test email**. If you receive the test email, everything is working correctly. Click **Save** to save the changes and you can proceeed to the next step.

Figure 3-3

Click the image to view larger in new window

4. In the **General** section, select the target for **Mobile Device Connector**, the ESET **License** that will be used for mobile device activation, and the **Parent Group**.

5. In the **List of Devices** section, type in the **Email Address** (this email address will be used to deliver the enrollment email message), **Device Name** and **Description**. To assign a specific user, click **Pair** under **Assigned User** to match it to a designated policy. To add another row, click **+Add device**.

Figure 3-4

Click the image to view larger in new window

Import CSV File:

To simplify the mass enrollment process, prepare a CSV file with all of the required data. To import the CSV file, click **Import CSV**

The CSV file should be formatted as shown in the example below:

Email Adress, Device Name, Description

Example1@domain.com, Samsung S6, Manager phone

Example2@domain.com, HTC 10, Engineer's phone

Example3@domain.com, Moto X, Intern's phone

Click **Choose File** to select the CSV file to upload. After the file is uploaded, click **Upload** to proceed to the next section.

Figure 3-5

Expand the **Delimiter** section and select the delimiters that will divide the data in the CSV file from the drop-down menu, or select the check box next to **Other** and specify the delimiter that is in your CSV file. Check the output from the CSV file in the **Data Preview** section.

Figure 3-6

Expand the **Column Mapping** section, select the check box next to **First line fo CSV contains headings** to separate the headings (if applicable) in your CSV file. In the **Map Columns** section, use the drop-down menus to select the data types in your uploaded CSV file. Preview the results in the **Table Preview** section. Once you are finished, click **Import** to import the data.

Figure 3-7

6. Once you have finished adding mobile devices, continue to the **Enrollment Email Message** section. Make any desired modifications to the **Subject** line and the **Content** section of the enrollement email message. The **Instructions** field displays the body of the enrollment email message with the steps that must be performed by the user on the mobile device.
7. Click **Enroll** and proceed to Enroll your Android device.

Figure 3-8

Click the image to view larger in new window

Enroll a single device

1. Select **Individual enrollment via link or QR code** in the **Add mobile devices** window and click **Continue**.

Figure 3-9

Click the image to view larger in new window

2. Type the **Device name** and **Description** in the appropriate fields, select the appropriate **Mobile Device Connector** and ESET **License**, and then click **Next** to proceed.

Figure 3-10

Click the image to view larger in new window

3. The last preview window will display a summary of the enrollment, including the download link and 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 Enroll your Adnroid device. To enroll another device, click **Enroll Another** and repeat step 2.

Figure 3-11

Click the image to view larger in new window

IV. Enroll your Android device and deploy ESET Endpoint Security for Android (2.x)

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

Figure 4-1

Your Connection is not private:

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)**.

Figure 4-2

2. Tap **Connect**.

Figure 4-3

3. Tap **Accept** to accept the Google Play terms of service.

Figure 4-4

4. Tap **Install**.

Figure 4-5

5. Review the permissions for ESET Endpoint Security for Android and tap **Accept**.

Figure 4-6

6. After the installation is complete, tap **Open** to open ESET Endpoint Security for Android.

Figure 4-7

7. Tap **Admin setup**.

Figure 4-8

8. Select the **Language** and **Country**. Select the check box next to **I want to help improve ESET products by sending anonymous data about application usage** if you would like to and tap **Accept** to continue. By tapping "Accept" you agree to the End User License Agreement.

Figure 4-9

9. Tap **Accept** to accept the User consent.

Figure 4-10

10. Type in the name for your device and tap **Save**. This will help the administrator recognize your device.

Figure 4-11

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

Figure 4-12

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

Figure 4-13

13. Tap **Finish**.

Figure 4-14

14. Proceed to Create activation task for Android MDM.

Reboot or wake up

Reboot or wake up reconnects the device. Android connects to MDM approximately every hour.

Unactivated devices

Devices that are not activated will have the red "License not activated" protection status and will refuse to handle tasks, set policies and deliver non-critical logs. Tasks sent to the unactivated device will fail with the error "License not activated. Policies and logs will fail silently.

V. Create activation Task for Android MDM

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

To send an activation task from ESET Remote Administrator, follow the instructions in Activate ESET business products in ESET Remote

Administrator (6.x)

VI. ERA version 6.3 and earlier:

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in. How do I open ERA Web Console?
2. Click **Computers**, select the desired group for your mobile device(s), click **Add New** and then click **Mobile devices**.

Version 6.2 and earlier:

Select **Mobile Devices** under **Device Type**.

Figure 5-1

Click the image to view larger in new window

3. Type a name for your task in the **Name** field of the **Basic** section.

4. Expand the **Settings** section.Type the name for your mobile device in the **Name** field. Type the IMEI/WiFi MAC Address or MEID (ERA 6.2 and earlier) for your device in the **Device Identification** field.

Figure 5-2

Click the image to view larger in new window

Enrollment Link

Select your preferred method to enroll mobile devices. You can select one or both of the options to fit your needs:

Display enrollment link after task is created: A custom QR code that can be scanned to trigger enrollment will be displayed in the ERA Web Console. This option allows you to quickly enroll multiple devices if they are physically present.

Email enrollment link: An email with a hyperlink to trigger enrollment will be sent to the email address associated with each new device.

Figure 5-3

Click the image to view larger in new window

5. If you are addig multiple devices, click **+ Add Another** to add another device. Click **Finish** when you have finished entering the names and identifications for all devices to display the enrollment link and/or email client devices.

   Complete steps 6-12 on the Android device you are enrolling

6. On your Android device, open the enrollment email and tap the enrollment link.

Figure 5-4

Your connection is not private

You may be notified that the link to your server is not private if you do not use SSL protocol, if you receive this notification, tap **Advanced Proceed to → (host address)**.

Figure 5-5

Click the image to view larger in new window

7. Tap **Connect**.

Figure 5-6

8. Tap **Accept** to accept the Google Play terms of service.

Figure 5-7

9. Tap **Install**.

Figure 5-8

10. Review the permissions for ESET Endpoint Security for Android and tap **Accept**.

Figure 5-9

11. Tap **Open** to open ESET Endpoint Security for Android following installation. You will be prompted to enter a name, enable uninstall protection, and activate device administration.

Figure 5-10

12. When the **Setup finished** screen is displayed, you (or your admin) can send an activation task to the device to complete activation of ESET Endpoint Security for Android.

Figure 5-11

If you do not use ESET Remote Administrator to manage your network

Perform these steps on individual client devices.

Related articles:

Deploy or upgrade ESET endpoint products using ESET Remote Administrator (6.x)

Install ESET Mobile Device Connector (6.x)

Tags

Android

ERA 6.x

MDM