ESET Tech Center

How do I push install ESET Endpoint Security for Android (1.x) using ESET Remote Administrator (5.x)?

Ondersteuning | ESET Nederland - 2024-08-28 - Reacties (0) - 5.x

https://support.eset.com/kb3168

Issue

Create an ESET Remote Administrator policy for clients using Android devices
Install ESET Endpoint Security for Android on your mobile devices with update parameters (and additional configuration settings) already in place

Details

Solution

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

Perform these steps on individual client devices.

Before you begin

In order to perform the push installation described below, you must upgrade ESET Remote Administrator 5 to the latest version.

ESET Remote Administrator 6.x users: Click here for instructions to push install ESET Endpoint Security for

Android (2.x)

I. Create a policy for your Android devices

I. Configure SMTP settings for ESET Remote Administrator

I. Push ESET Endpoint Security for Android to mobile users

I. Create a policy for your Android devices

1. Open ESET Remote Administrator Console by clicking **Start → All Programs → ESET → ESET Remote Administrator Console → ESET Remote Administrator Console**.

1. Click **Tools → Policy Manager**. Select the **Default Parent Policy** and click **New Policy Child**.

Figure 1-1

Click the image to view larger in new window

2. Type a name for your new policy in the **Policy name** field, configure your policy settings and then click **OK**.

Figure 1-2

3. Select the child policy that you created in steps 2 and 3 and then click **Edit**.

Figure 1-3

Click the image to view larger in new window

4. Expand **Mobile devices → Endpoint Security for Android → Remote administration → Settings**, click **Primary remote server name** and type the IP address of the Remote Administrator Server for remote management into the **Value** field. This is often the same server on which ESET Remote Administrator Console (ERAC) is installed.

Figure 1-4

Click the image to view larger in new window

5. Expand **Update → Settings**, click **Username** and type your ESET-issued Username into the **Value** field.

Figure 1-5

Click the image to view larger in new window

6. Click **Password → Set Password**. Type your ESET-issued Password into the **Enter Password** and **Confirm Password** fields and then click **OK**.

Figure 1-6

7. If you want to use the same security password (different from the update password you entered in step 8—a security password protects your settings from unauthorized users) on all client phones,
expand **General → Settings → Password → Security password**, click **Set Password**, type your settings password into the **Enter Password** and **Confirm Password** fields and then click **OK**. This will automatically resolve the security password security risk that appears following the installation of ESET Endpoint Security for Android.

Security risks: Steps 8-10

After installation, ESET Mobile Security for Android will prompt users to resolve three security risks. You can resolve two of these security risks by defining the security password and adding an

admin contact in your ERA policy. However, setting ESET as device administrator, the third and final security risk, must be resolved locally on the client device.

Figure 1-7

Click the image to view larger in new window

8. To configure client phones to use SIM matching whenever applicable, expand **Anti Theft** → **Settings**, click **Enable SIM matching** and then select the check box next to **Value**.

Figure 1-8

Click the image to view larger in new window

9. Expand **Endpoint Security for Android** → **Anti Theft**, click **List of Admin Contacts: 0 entries** and then click **Edit**. Type the admin contact into the blank field, following the format "Admin name;Admin number" , click **Add** and then click **OK** to save your changes. Make any additional changes you want applied to client devices in the Configuration Editor and then click **Console** → **Yes** to save all of your changes.

Figure 1-9

Click the image to view larger in new window

10. Click the **Policy Rules** tab and click **New Rule** → **Create New**.

Create Mobile Device Policy Rules

These steps will show you how to create rules that apply your mobile device policy for new client devices without overriding settings already applied to existing mobile devices.

Figure 1-10

Click the image to view larger in new window

11. Enter a name for your new rule, select the policy you just created from the **Policy** drop-down menu and then click **Edit**.

Figure 1-11

12. Select the check boxes next to **IS New Client** and **Product Name IN (specify)**. Click **Specify** and type ***Android** into the **Enter rule condition** field and then click **Add**. Once you are finished, click **OK**. Your new rule will appear in the **Policy Rules** window.

Figure 1-12

Click the image to view larger in new window

13. Repeat steps 2-3 to create an additional child policy, but do not make any changes to the default configuration.

1. Repeat steps 10-13 to create a new policy rule with the **Product Name IN** condition, but not the **IS New Client** condition (see Figure 1-12). This will prevent client phones that have already received the policy from inheriting new settings each time that they check in.

Figure 1-13

2. Once you are finished, click **OK**. Continue to part II below to send the Endpoint Security for Android installer file and configuration settings to your client devices.

II. Configure SMTP settings for ESET Remote Administrator

1. Open ESET Remote Administrator Console by

clicking **Start → All Programs → ESET → ESET Remote Administrator Console → ESET Remote Administrator Console**.

1. Click **Tools → Server Options**.

1. Click the **Other Settings** tab and enter your SMTP information into the appropriate fields.

1. Click **Send Test Email**, enter the test email address into the **Email** field and click **Send** to verify your settings. When prompted, click **OK** and continue to part III below.

Figure 2-1

III. Push ESET Endpoint Security for Android to mobile users

1. Click the **Remote Install** tab, right-click and select **Send via Email** from the context menu.

Figure 3-1

Click the image to view larger in new window

2. In the **Send ESET Installer via Email** window, select **ESET Security Products for Android** from the **Type** drop-down menu.

1. Click **Browse** (**. . .**), navigate to the installation package

and click **Open** to attach it to this email.

1. Enter the user email address(es) into the **To** field.

1. Click **Send**.

Figure 3-2

2. **On the mobile device**: Open the email client, open the email that you generated in the steps above and then tap **Install**. Follow the on-screen instructions to complete the installation of ESET Endpoint Security for Android.

Figure 3-3

3. Once the installation is complete, tap **Done**, return to the email that you accessed in step 6, tap the link in the email and then tap **ESET Endpoint Security**.

Figure 3-4

Click the image to view larger in new window

4. Open ESET Endpoint Security and tap **Remote Administration → Connect to ERA**. If successful, a "Connection with ERA server was successful" notification will be displayed and the settings that you configured in part I will automatically be applied to this mobile device.

Figure 3-5

5. Resolve any remaining security risks on the client mobile device.

Related articles:

ESET Endpoint Security for Android FAQ (1.x)

[How do I configure ESET Endpoint Security for Android (1.x) to connect to the ESET Remote Administrator Server (5.x)?]

[How do I resolve the Security Risk warning after installing ESET Mobile Security for Android? (1.x)(ARCHIVED)]

Tags

Android

ERA 5.x