ESET Tech Center

ESET Mobile Device Management for Apple iOS (6.3 and later)

Ondersteuning | ESET Nederland - 2017-11-08 - Comments (0) - MDM for iOS

https://support.eset.com/kb5771

Issue

Configure ESET Remote Administrator 6.3 or 6.4 to manage iOS devices using ESET Mobile Device Management

For version 6.5 and later.

For version 6.5 and later please follow this KB article.

Details

Solution

Before you continue, make sure these prerequisites are met:

ESET Remote Administrator 6.3 or 6.4 and ESET Mobile Device Connector must be installed and **activated**—for more help see the ERA Installation guide.
You must have an Apple iTunes ID.
Visit appleid.apple.com to create an Apple ID.
You must have a valid ESET license. ESET Mobile Device Connector is activated by ESET Endpoint for Android license. How do I purchase a license?
Managed devices must be running on iOS 8+ (iPhone and iPad).

To enroll iOS device in ESET Mobile Device Connector, follow these steps:

I. Create a MDM Certificate

II. Create an APN Certificate

III. Create an MDM Policy

IV. Register your iOS device in ERA

V. Enroll your iOS device

VI. Create an activation Task for iOS MDM

I. Create a MDM certificate

This step is not required if you already have HTTPS certificate (3rd party HTTPS certificate signed by trusted Certification Authority, or certicate created in ERA and signed by ERA CA). In that case, skip part I. and move to part II.

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 2-1

Click the image to view larger in new window

3. In the **Basic** section, complete the following fields:

   Product: Select **Mobile Device Connector** from the **Product** drop-down menu.

   Host: Type the IP address or Hostname of the server where Mobile Device Connector is installed into the **Host** field.

In case the MDM server is not visible from the internet and the communication is port-forwarded from a router that is visible to the outside network, use the IP adress or Hostname of the router instead.

Warning:

The **Host** in the **HTTPS** certificate **MUST MATCH** the **Hostname** that you set up in the **ESET Mobile Device Connector Policy**.

Figure 2-2

Click the image to view larger in new window

If you get the Profile Installation Failed error, click here for steps to resolve the issue.

Remove any previous MDM profiles from device settings—there should be no other MDM profiles enrolled on the device.
Make sure all MDM ports are open—communication between the device and MDM could be blocked.
Try using the device's Serial Number (instead of its IMEI number) when adding your iOS device into ERA.

4. In the **Attributes (Subject)** section:

   Organization: Type your Organization name used in ESET Remote Administrator.

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

Figure 2-3

Click the image to view larger in new window

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

Figure 2-4

Click the image to view larger in new window

7. Click **Finish** and proceed to part II.

II. Create an APN certificate

1. Click **Admin** → **Certificates** → **New** → **APN Certificate**.

2. Specify the certificate attributes and then click **Submit Request**.

3. In the **Download** section, use the links provided to download the **Private Key** and **CSR** and save to your hard drive.

Figure 3-1

Click the image to view larger in new window

4. Click **Open Apple Portal** or navigate to https://identity.apple.com/pushcert in your web browser and sign in with your Apple ID.

Figure 3-2

Click the image to view larger in new window

5. Click **Create a Certificate**.

Figure 3-3

Click the image to view larger in new window

6. If you agree to the Apple Push Certificates Portal Terms of Use, click **Accept**.

7. Click **Browse**, select the CSR certificate you downloaded in step 3 above, click **Open** and then click **Upload**.

Figure 3-4

Click the image to view larger in new window

8. After the upload completes (this may take some time and you may need to refresh the browser), click **Download** next to the **Mobile Device Management** certificate and save the certificate to your hard drive.

Figure 3-5

Click the image to view larger in new window

9. Proceed to part III.

III. 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 **Policies** → **New**.

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

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

6. Type the **Hostname** (IP address) of the server where Mobile Device Connector is installed. In case the MDM server is not visible from the internet and the communication is port-forwarded from a router that is visible to the outside network, use the IP adress or Hostname of the router instead.

> **Warning:**
>
> The **Host** in the **HTTPS** certificate **MUST MATCH** the **Hostname** that you set up in the **ESET Mobile Device Connector Policy**.

7. Type your actual organization's name used in ESET Remote Administrator into the **Organization** field (this name is used by the enrollment profile generator to include this information in the profile).

Figure 4-1

Click the image to view larger in new window

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

9. In the **Apple Push Notification Service** section, upload the two **Apple Push Notification Service** files to their respective items:

    - APNS Certificate (signed by Apple) - this is the file downloaded from the Apple's portal, usually named: `MDM_ESET, spol. s.r.o._Certificate.pem`

    - APNS Private Key - this is the file created in part II, step 3, usually named: `APN Private Key Export CN= ... .pem`

10. In the **Agents** section, click **Change certificate**. Click **Open certificate list** and select the **Agent Certificate** you created after installing ESET Remote Administrator.

11. Click **Assign** to display all Static and Dynamic Groups and their members. Select the Mobile Device Connector instance that you want to apply an APNS Certificate to and click **OK**.

When you are finished, proceed to part IV.

IV. Add your mobile device in ERA and send an enrollment link

ERA version 6.3 and earlier: Click here for instructions.

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(s), and then click **Add New → Mobile devices.**

Figure 5-1

Click the image to view larger in new window

3. In the **Add mobile devices** window, select **Enrollment via e-mail** and click **Continue**. To enroll a single device at a time, select **Individual enrollment via link or QR code**. Click here for step-by-step instructions.

Figure 5-2

Click the image to view larger in new window

SMTP Server Settings

Before you can add multiple devices using mass enrollment, it is required to setup the SMTP server. Click on the **Configure server server settings** in the pop-up window to proceed to **Server settings → Advanced settings** and enable the SMTP server.

Fill in the required fields for the SMTP server. If you want to verify that everything is working, click **Test SMTP settings → Send test email**. If you received the test email, everything is working correctly and you can proceeed to the

next step.

Figure 5-3

Click the image to view larger in new window

4. Select the target MDM Connector, the ESET license that will be used for activation, and the target group.

5. To simplify the mass enrollment process, you can create a CSV file in advance, which will include the required data. To import a CSV file, click **Import CSV**.

CSV File form

The CSV file should be in the form displayed in the example below:

Email Adress, Device Name, Description

Example1@domain.com, iPhone 6S Plus, Manager phone

Example2@domain.com, iPhone 6, Engineer's phone

Example3@domain.com, iPhone SE, Intern's phone

6. Expand **Delimiter** and select the delimiter you used in the file (semicolon, comma, space).

7. Expand **Column Mapping**, use the drop-down menus next to **Email Address**, **Device Name**, and **Description** to assign the columns from your CSV file to the designated columns required for the import. When you are finished, click **Import**.

8. Click **Enroll** and proceed to part V.

Enroll a single device

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

2. Type in the **Device name** and **Decsription**, select the MDM Connector and ESET License, and then click **Next**to proceed.
3. In the last preview window you can see a summary of the enrollment, including the download link and QR code.
   Click **Enroll** and proceed to part V.

V. Enroll your iOS device

1. On your mobile device(s), access the enrollment email that you sent in part IV above and tap the enrollment link.

Figure 6-1

2. At the **Install Profile** screen, tap **Install**, and then tap **Install** again.

Figure 6-2

Figure 6-3

3. Tap **Trust** to allow installation of the new profile.
4. After installing the new profile, the **Signed by** field will display that the profile is **Not Signed**. This is a standard behavior for any MDM enrollment because iOS does not yet recognize the certificate.
5. Continue to part VII to activate the product.

Reboot or wake up

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

Unactivated devices

Devices which are not activated will report red protection status "License not activated" and will refuse to handle tasks, set policies and deliver non-critical logs.

Tasks will fail with error "License not activated. Policies and logs will fail silently.

VI. Create activation Task for iOS MDM

After completing parts 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 → iOS devices**.

Send an activation task from ESET Remote Administrator using the instructions in the following article: How do I activate ESET business products in ESET Remote Administrator? (6.x)

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

Device enrollment for ERA 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 group to which you want to add your mobile device(s), and then click **Add New → Mobile devices**.

Figure 7-1

Click the image to view larger in new window

3. Type a name for the task into the **Name** field.

Figure 7-2

Click the image to view larger in new window

4. Expand **Mobile Device Connector** and click **Select**. Select the MDC instance you will use to distribute the MDM profile and then click **OK**.

Figure 7-3

Click the image to view larger in new window

5. Expand **Settings** and type the following information into their respective fields:

    a. Type the **Name** of the mobile device (this name will be shown in the list of **Computers**).

    b. Type the IMEI number, Wi-Fi Mac address or Serial Number (use the Serial Number for iOS devices without cellular capability, such as iPads and iPods) for your device into the **Device Identification** field.

    > To locate your device IMEI, Serial Number or MAC address on iOS
    >
    > On your iOS device, go to **Settings** → **General** → **About** (or for more instructions, visit the ESET ERA Online Help topic Mobile Device ID location).

    c. Type the email address that is associated with the mobile device.

    > ## If you want to add multiple devices
    >
    > Click **+ Add Another** to open a new line (or click **Import** to to upload a .csv file containing a list of mobiles to add).

6. Select the **Email enrollment link** option.

Figure 7-4

Click the image to view larger in new window

7. Click **Finish** when you are finished entering names and identification information for all of your devices.
8. Click **Send enrollment link** to send your enrollment emails to client devices.

> ### Customize contents of enrollment emails to client devices
>
> You can customize the **Subject** and **Message Contents** of the email containing your enrollment link by editing the corresponding fields, but make sure you do not change enrollment URL.

Continue to Part V below to add the MDM profile on your client devices.

Warning:

The **Hostname** in the **HTTPS** certificate **MUST MATCH** the **Hostname** that you set up in the **ESET Mobile Device Connector Policy**.

Warning:

The **Hostname** in the **HTTPS** certificate **MUST MATCH** the **Hostname** that you set up in the **ESET Mobile Device Connector Policy**.

Tags

iOS

MDM