ESET Mobile Device Management for Apple iOS (6.5 and later)

Perry | ESET Nederland - 2018-01-11 - 0 Comments - in MDM for iOS

Issue

Configure ESET Remote Administrator 6.5 or later to manage iOS devices using ESET Mobile Device Management

For version 6.4 and earlier

For version 6.4 and earlier please follow this KB article.

Details

Solution

Before you continue, these prerequisites must be met:

ESET Remote Administrator 6.5 or later and ESET Mobile Device Connector must be installed and activated. For more help, visit the ERA Installation guide.
You must have an Apple iTunes ID.
Visit appleid.apple.com to create an Apple ID.
For Apple DEP enrollment: verify that Apple DEP is available in your country; also check the Apple deployment program requirements, Apple DEP

requirements and DEP device requirements.
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 iOS 8 or later (iPhone and iPad).

To enroll iOS devices in ESET Mobile Device Connector, follow the steps in each section:

I. Create an MDM Certificate

II. Create an APN/DEP 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

Pre-existing MDM Policy

If you already have an MDM Certificate, MDM Policy, and APN/DEP Certificate, proceed to Enroll your iOS device. Sections I, II, and III only need to be completed again if a change was made to the hostname, policy, or certificate after the initial Certificate or Policy creation.

I. Create an MDM certificate

If you already have an MDM certificate (3rd party HTTPS certificate signed by trusted Certification Authority, or certificate created in ERA and signed by ERA CA), proceed to Create an APN/DEP Certificate.

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**.

Profile Installation Failed error: click here for the 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, 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 APN/DEP certificate.

II. Create an APN/DEP certificate

1. Click **Admin** → **Certificates** → **New** → **APN/DEP Certificate**.
2. Enter the certificate attributes and then click **Submit Request**.

Figure 2-1

Click the image to view larger in new window

3. Expand the **Download** section, click **Download Private Key** and **Download CSR** and save the certificates to your hard drive.

Figure 2-2

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 2-3

Click the image to view larger in new window

5. Click **Create a Certificate**.

Figure 2-4

Click the image to view larger in new window

6. If you agree to the Apple Push Certificate 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 2-5

Click the image to view larger in new window

8. After the upload completes (this may take time and it might be necessary to refresh the browser), click **Download** and save the certificate to your hard drive.

Figure 2-6

Click the image to view larger in new window

If you are completing a DEP enrollment, continue on to steps 9-12. If you are completing a non-DEP enrollment, proceed to Create an MDM Policy.

9. Click **Open Apple DEP Portal** or navigate to https://deploy.apple.com in your web browser and sign in with your Apple DEP Account.

Figure 2-7

Click the image to view larger in new window

10. Click **Manage Servers → Add MDM Server**. Type the **MDM**

Server Name in the field and select the check box next to **Automatically Assign New Devices** if you want all new devices connected to your Apple DEP account to be assigned to this MDM server, and then click **Next**.

Figure 2-8

Click the image to view larger in new window

11. Upload your public key (this is the Private key file you downloaded in step 3). Click **Choose File**, select the public key file, upload it and then click **Next**.

Figure 2-9

Click the image to view larger in new window

12. Download the Apple DEP Server token. Click **Your Server Token**, save the file on your hard drive and click **Done**.

Figure 2-10

Click the image to view larger in new window

13. Proceed to Create an MDM Policy

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 **New Policy**.

Figure 3-1

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 3-2

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 address 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**.

When changing the certificate used in your policy for MDC

Once 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.

Figure 3-3

Click the image to view larger in new window

9. In the **Apple Push Notification Service** section, upload the two **Apple Push Notification Service** files:

    - 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`

Figure 3-4

Click the image to view larger in new window

If you are completing a DEP enrollment, continue on to steps 10-12. If you are completing a non-DEP enrollment, skip to step 12

10. In the **Apple Device Enrollment Program (DEP)** section, click the file icon next to **Upload authorization token** and upload the Apple DEP Server Token - this file is usually named: `<MDM_Server_Name>_Token_... .p7m`.

11. Configure the MDC DEP settings.

Supervised mode: provides all the DEP-only iOS policy settings and allows you to fully manage the iOS device.
Mandatory Installation: requires iOS device users to install the MDM Profile. Users will be unable to use the iOS device without installing the MDM profile.
Allow user to remove MDM profile: allows users to remove the MDM profile after it is installed. The iOS device must have the Supervised mode setting enabled to remove the option to remove the MDM profile. Click **Edit** next to **Skip setup items** to choose which of the initial setup steps during the initial iOS setup will be skipped. You can find more information about each of these steps in the Apple Knowledgebase Article.

Figure 3-5

Click the image to view larger in new window

Changes made to settings will require re-enrollment

If any of the settings in the **Apple Device Enrollment Program (DEP)** section are changed after the initial device enrollment, they will only be applied only after the iOS device is re-enrolled.

12. 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 3-6

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 iOS device in ERA.

IV. Register your iOS device in ERA and send an enrollment link

If you are doing DEP enrollment, proceed here.

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 4-1

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 step-by-step instructions to enroll a single device at a time.

Figure 4-2

Click the image to view larger in new window

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 proceed to the next step.

Figure 4-3

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 4-4

Click the image to view larger in new window

Import CSV File:

To simplify the mass enrollment process, create a CSV file in advance 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, iPhone 6S Plus, Manager phone

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

Example3@domain.com, iPhone SE, 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 4-5

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 4-6

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 4-7

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.

Figure 4-8

Click the image to view larger in new window

7. Click **Enroll** and proceed to Enroll your iOS device.

Enroll a single device

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

Figure 4-9

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 4-10

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 iOS device. To enroll another device, click **Enroll Another** and repeat step 2.

Figure 4-11

Click the image to view larger in new window

Add your DEP mobile device in the DEP portal and ERA

For DEP enrollmnent, you do not need to add the mobile device into ERA nor do you need to perform the mobile device enrollment. This will occur automatically; when the iOS device is added into DEP it is assigned to your MDM server. If you selected the **Automatically Assign New Devices** check box when you connected your MDM server with the DEP portal, all of the iOS devices assigned to your DEP account will automatically connect to the selected MDM server.

To add an iOS device manually, follow these steps:

1. Log in to the DEP portal (deploy.apple.com).

2. Click **Device Enrollment Program → Manage Devices** from the menu on the left.

3. Choose from the following three options to add an iOS device into the DEP portal.

    a. **Serial Number** - type in the serial numbers of iOS devices you want to add (separated by commas) in the field and proceed to the next step.

Figure 4-12

Click the image to view larger in new window

b. **Order Number** - type in the order number for the designated iOS devices in the field and proceed to the next step.

Figure 4-13

Click the image to view larger in new window

c. **Upload CSV File** - click **Download Template File** to download the template for the csv file, type in the required information and then click **Choose File** to upload the csv file.

Figure 4-14

Click the image to view larger in new window

4. In the **Choose Action** section, select **Assign to Server** from the drop-down menu, select the MDM server for the iOS device and click **OK**.

Figure 4-15

Click the image to view larger in new window

When the iOS device is first powered on, it will enroll into DEP and ESET Remote Administrator MDM; once setup is complete, the device

will be added into ERA. Proceed to Create an Activation task for iOS MDM.

V. Enroll your iOS device

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

Figure 5-1

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

Figure 5-2

3. Tap **Trust** to allow installation of the new profile.

Figure 5-3

4. After installing the new profile, the **Signed by** field will show that the profile is **Not Signed**. This is standard behavior for any MDM enrollment because iOS does not yet recognize the certificate.

5. Proceed to Create activation task for iOS MDM.

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 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 → 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)