ESET Tech Center

Create a dual update profile configuration in ESET Remote Administrator (6.x)

Ondersteuning | ESET Nederland - 2017-12-04 - Reacties (0) - 6.x

https://support.eset.com/kb3621

Issue

Configure client workstations/mobile users to download updates directly from ESET update servers if they cannot download updates from the primary update server

Solution

ESET Remote Administrator version 6.1.28.0 and later only

The steps below should only be performed using ESET Remote Administrator version 6.1.28.0 and later.

Which version of ESET Remote Administrator Server and components do I have? (6.x)

Click here to configure dual update profile for ESET macOS and Linux products

Permissions changes in ESET Remote administrator 6.5 and later

Before proceeding, please note important changes to user

access rights and permissions in the latest versions of ESET Remote Administrator.

View Permissions Changes

I. Create a new profile

A user must have the following permissions for the group that contains the modified object:

Functionality	*Read*	*Use*	*Write*
Policies	✓	✓	✓

A user must have the following permissions for each affected object:

Functionality	*Read*	*Use*	*Write*
Groups & Computers	✓	✓	✓

Once these permissions are in place, follow the steps below.

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in.
2. Click **Admin** → **Policies** and select the policy you want to modify.
3. Click **Policies** → **Edit**.

When creating a new policy

In this example, we will modify an existing policy. If you

are creating a new policy, you must enter information about your server (mirror server IP address, for example). If you are using the ERA or HTTP Proxy for distributing updates, you do not need to specify any of this information in your policy.

Figure 1-1

Click the image to view larger in new window

4. Expand **Settings**.
5. Click **Update**, expand **Profiles** and click **Edit**.

Figure 1-2

Click the image to view larger in new window

6. Type a name into the blank field and click **Add**.

Figure 1-3

7. Click **Save**.

Figure 1-4

8. Select the profile you just created from the **Select profile to edit** drop-down menu.

ERA 6.4 users

Select the profile you just created from the **Selected profile** drop-down menu.

Figure 1-5

Click the image to view larger in new window

9. Expand **HTTP Proxy**, select **Do not use proxy server** from

the **Proxy mode** drop-down menu and then click **Finish**.

In the future, client workstations assigned to the policy you modified (see step **II**) will first attempt to download updates from the default profile—if this fails, client workstations will then attempt to download updates from ESET servers.

Figure 1-6

Click the image to view larger in new window

II. Modify the regular automatic update task

A user must have the following permissions for the group that contains the modified object:

Functionality	*Read*	*Use*	*Write*
Policies	✓	✓	✓

A user must have the following permissions for each affected object:

Functionality	*Read*	*Use*	*Write*
Groups & Computers	✓	✓	✓

Once these permissions are in place, follow the steps below.

Complete the steps below to ensure that the latest virus signature database updates will be downloaded when an end-user clicks **Update now** in their ESET endpoint product. Manual updates initiated by the user will fail if the regular automatic update task isn't modified. However, the ESET endpoint product (assigned to the policy you modified in part I) will still automatically download updates according to the default interval specified in the regular automatic update task.

1. Open the ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in.
2. Click **Admin** → **Policies** and select the policy you want to

modify.

3. Click **Policies** → **Edit**.

Figure 2-1

Click the image to view larger in new window

4. Expand **Settings** and make sure **ESET Security Product for Windows** is selected from the drop-down menu.
5. Click **Tools**, expand **Scheduler** and then click **Edit**.

Figure 2-2

Click the image to view larger in new window

6. Select **Regular automatic update** and click **Edit**.

Figure 2-3

Click the image to view larger in new window

7. Click **Next**.

Figure 2-4

8. Click **Next**.

Figure 2-5

9. Leave the **Interval between task execution (min.)** at 60 and click **Next**.

Figure 2-6

10. Make sure that **At the next scheduled time** is selected and click **Next**.

Figure 2-7

11. Click the slider bar next to **Use default profile** (under **Profile to use for update**) and make sure that the default profile (**My profile**) is selected from the **Profile** drop-down menu**.**
12. Click the slider bar next to **Use default profile** (under **Secondary profile to be used for update**), select the profile that you created in part I (Internet Updating (non-proxy) and then click **Finish**.

Figure 2-8

13. Click **Save**.

Figure 2-9

Click the image to view larger in new window

14. Click **Finish**.

Figure 2-10

Click the image to view larger in new window

15. To test the new profile configuration, perform the following steps on a client computer.

    Click **Tools → Scheduler**.

Figure 2-11

Click the image to view larger in new window

16. Select the appropriate **Update** task, right-click it and select **Run Now**.

Figure 2-12

Click the image to view larger in new window

17. Click **Yes**.

Figure 2-13

Click the image to view larger in new window

Configure dual update profiles for ESET macOS and Linux products

A user must have the following permissions for the group that contains the modified object:

Functionality	*Read*	*Use*	*Write*
Policies	✓	✓	✓

A user must have the following permissions for each affected object:

Functionality	*Read*	*Use*	*Write*
Groups & Computers	✓	✓	✓

Once these permissions are in place, follow the steps below.

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in.
2. Click **Admin** → **Policies** and select your **macOS and Linux** policy.
3. Click **Policies** → **Edit**.
4. Expand **Settings**, click **Update** → **Primary Server**.
5. To configure the settings:
    a. Expand **HTTP Proxy** and select **Connection through a proxy server** in the **Proxy mode** drop-down menu.
    b. Type the IP address into the **Proxy server** field and port number (default is 3128) into the **Port** field.

    If the proxy requires login credentials, enter them in the **Username** and **Password** fields (for example, within your company's network).

Figure 3-1

Click the image to view larger in new window

6. Click **Secondary Server** to configure:
    a. Expand **Basic** and make sure that the **Update server** drop-down menu is set to **Choose automatically** (it is by default).
    b. Leave the **Username** and **Password** field empty (because the product is already activated and these credentials are not needed).
7. Click **Finish** to save your changes.

Figure 3-2

Click the image to view larger in new window

Tags

Update