ESET Tech Center

Change the ESET Security Management Center Server address used by the ESET Management Agent (7.x)

Anish | ESET Nederland - 2018-09-12 - Reacties (0) - ESET Security Management Center

Issue

- Direct clients to connect to a new ESET Security Management Center Server (ESMC Server) by migrating certificates and setting your policy to the new server's address.

Details

Solution

There are three ways to specify a new server address for the ESET Management Agent to use when migrating to a new ESET Security Management Center Server (ESMC Server).

- Migrate certificates and adjust the ESET Management Agent Policy in the ESMC Web Console
- Modify ESET Management Agent settings
- Redeploy the ESET Management Agent

ERA 6.5 User Permissions

This article assumes that your ERA user has the correct access rights and permissions to perform the tasks below.

If you are still using the default Administrator user, or you are unable to perform the tasks below (the option is grayed out), see the following article to create a second administrator user with all access rights (you only need to do this once):

- Create a second administrator user in ESET Remote Administrator 6.5

Migrate certificates and create new ESET Management Agent Policy

View permissions needed for least privilege user access

Default certificates

Peer certificates and Certification Authority created during the installation are by default

contained in the static group All.

I. [Migrate certificates to new server address](#)

II. [Migrate client computers to new server address](#)

Modify ESET Management Agent Settings

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

Functionality	*Read*	*Use*	*Write*
Certificates	✓	✓	

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

Default certificates

The Peer certificates and Certification Authority that were created during the installation are by default contained in the static group All.

1. [Open the ESET Security Management Center Web Console](#).

2. Click **More → Certificates → Peer Certificates**, and then select the check box next to your default **Agent certificate**.

3. Click **Actions → Export** and save the `.pfx` file to a save location of your choice.

   Figure 2-1
   Click the image to view larger in new window

4. Click **More → Certificates → Certification Authorities**, and then select the check box next to the ERA Certification authority used to sign your exported Agent Certificate.

5. Click **Actions →** select **Export Public Key** and then save the .der file to a save location of your choice.

   Figure 2-2
   Click the image to view larger in new window

6. Click **Start → Control Panel → Programs → Programs and Features** (**Windows XP / Windows Server 2003 users**: Double-click **Add or Remove Programs**).

7. Select **ESET Management Agent** and click **Change**.

   Figure 2-3

8. Click **Next**.

   ![x]

   Figure 2-4

9. Click **Repair**.

   ![x]

   Figure 2-5

10. In the **Agent configuration** screen, enter the address of your new ESMC Server into the **Server host** field. Other settings should be left unchanged unless you are using a different port than the default port for ESMC Server. Click **Next** when you are finished.

    ![x]

    Figure 2-6

11. In the **Peer certificate** window, browse for the **Agent Certificate** (`.pfx`) and **Certificate Authority** (.der) files you exported in step 3 and then click **Next**.

    ![x]

    Figure 2-7

12. Click **Repair**. Your client computer(s) will be able to communicate with your new ESMC Server after the changes have been made.

    ![x]

    Figure 2-8

Redeploy the ESET Management Agent

When migrating to a new ESMC Server, you can send an updated instance of the ESET Management Agent from your new server to client machines. During the ESET Management Agent deployment process, you will be prompted to enter connection information for your new ESMC Server.

- Click here for step-by-step instructions to deploy the ESET Management Agent.

KB Solution ID: KB6723 |Document ID: 25412|Last Revised: August 16, 2018