ESET Tech Center

Deploy the ESET Management Agent via SCCM or GPO (7.x)

Anish | ESET Nederland - 2018-09-12 - Comments (0) - Deployment

Issue

- Prepare the ESET Management Agent installer file for distribution via Group Policy Object (GPO) or Software Center Configuration Manager (SCCM)
- Alternative method to distribute ESET Management Agent for enterprise environments or environments with a high number of client computers

Details

Solution

Getting Started with ESMC: Step 4 of 6

← **Add Client Computers** | **Deploy ESET endpoint solutions** →

ESET Security Management Center (ESMC) 7 User Permissions

This article assumes that your ESMC 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 Security Management Center 7.x

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.

1. On your ESMC Server, go to the ESET Security Management Center 7 Download page and click **Standalone installers.**

Figure 1-1

Click the image to view larger in new window

1. In the **Configure download** section, select the information below and then click **Download**. Save the ESET Management Agent installer `.msi` file to a shared folder your client computers can access.
    - **ESMC Component:** Select **Agent**.
    - **Operating system | Bitness:** Select the 32-bit or 64-bit Windows operating system.

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

1. Open ESET Security Management Center Web Console (ESMC Web Console) in your web browser and log in.
2. Click **Quick Links → Other Deployment Options**.

Figure 1-3
Click the image to view larger in new window

1. Click **Use GPO or SCCM for deployment** and click **Create Script**.

Figure 1-4

1. Click **Finish**. Save the `install_config.ini` file to the same shared folder from Step 2. For customers using custom certificates, refer to the Custom certificates with ESMC Online Help topic for more details.

Figure 1-5
Click the image to view larger in new window

Client computers need read/execute access

Verify all appropriate client computers have read/execute access to the folder containing the `.msi` and `.ini` files. Right-click the folder from Step 2 and click **Properties**. Click the **Security** tab. Review each machine and confirm the check box next to **Read & execute** is selected under the **Allow** column. If not, click **Edit**, adjust the settings and click **Apply**.

Figure 1-6

1. Refer to one of the processes below to deploy the package:

- Deploy the ESET Management Agent using a Group Policy Object (GPO)
- Deploy the ESET Management Agent using System Center Configuration Manager

(SCCM)

1. Once you have completed the instructions from the appropriate article, proceed to Step 5, deploy ESET endpoint products to your client computers if you are performing a new installation of ESMC.

KB Solution ID: KB6863 |Document ID: 25831|Last Revised: August 30, 2018