

ESET Tech Center

Kennisbank > Legacy > Legacy ESET Remote Administrator (6.x / 5.x / 4.x) > 6.x > Deploy the ESET Remote Administrator Agent via SCCM or GPO using an MST transformation file (6.x)

Deploy the ESET Remote Administrator Agent via SCCM or GPO using an MST transformation file (6.x)

Ondersteuning | ESET Nederland - 2017-11-08 - Reacties (0) - 6.x

<https://support.eset.com/kb3675>

Issue

Prepare the ESET Remote Administrator Agent (ERA Agent) installer file for distribution via Group Policy Object (GPO) or Software Center Configuration Manager (SCCM).

Alternative method to distribute ERA Agent for enterprise environments or environments with a high number of client computers.

Details

Solution

Getting Started with ERA: Step 4 of 6

← [Add Client Computers](#) | [Deploy ESET endpoint solutions](#) →

This process is for ESET Remote Administrator version 6.4 and later

Version 6.3 and earlier 6.x users, [refer to the process below](#).

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](#)

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

[Click to view permissions](#)
Default certificates
Peer cert

ification
and
Certification
Authority
created
during
the
installation
are
by
default
contained
in
the
static
group

All.

1. On your ERA Server, go to the [ESET Remote Administrator 6 Download](#) page and click **Standalone installers**.



Figure 1-1

Click the image to view larger in new window

2. In the **Configure download** section, select the information below and then click **Download**. Save the ERA Agent installer .msi file to a shared folder your client computers can access.

- **Select component:** Select **Agent**
- **Operating system and Bitness:** Select the operating system of the client



Figure 1-2

Click the image to view larger in new window

3. [Open ESET Remote Administrator Web Console](#) (ERA Web Console) in your web browser and log in.

3. Click **Deploy ERA Agent**.



Figure 1-3

Click the image to view larger in new window

5. In the **Use GPO or SCCM for deployment** section, click **Create Script**.



Figure 1-4

Click the image to view larger in new window

6. Click **Create Package**. 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 ERA](#) 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 **Security**. 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

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

[How do I deploy the ESET Remote Administrator Agent using GPO?](#)

[How do I deploy the ESET Remote Administrator Agent using SCCM?](#)

8. 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 ERA.

Version ERA Server 6.3 and earlier 6.x versions

Prerequisites

The Orca database editor tool must be installed on your computer. Orca is available as part of the Windows SDK. For instructions to download and install Orca, visit the following Microsoft Knowledge Base article: [How to use the Orca database editor to edit Windows Installer files](#).

The ERA Agent installer file must be present on your system. You can download the installer file from within ESET Remote Administrator. [Click here for step-by-step instructions](#).

To access the .msi Agent installer file

When you export the Agent installer file from ERA, it will be a .bat file. Run the .bat file as though you were installing Agent, but do not complete the installation. This will download the .msi, which you can then edit to create your MST file. See below for step-by-step instructions:

1. Double click the .bat file to run it and click **Cancel** when the ESET Setup Wizard is displayed. This will download the .msi installer file without overwriting your existing ERA Agent.

1. The .msi file will automatically be downloaded to the following directory:

C:\ProgramData\ESET\RemoteAdministrator\Agent\SetupDate\Installer

Edit the ESET Remote Administrator installer file

1. Click **Start** → **All Programs** → **Orca** to launch Orca database editor.

1. Click **File** → **Open**, navigate to the ERA Agent installer file that you want to apply the transformation file to, select it and then click **Open**.

1. Click **Transform** → **New Transform**.



Figure 2-1

Click the image to view larger in new window

4. Select **Property** from the **Tables** section, right-click anywhere in the list of property values and select **Add Row** from the context menu.



Figure 2-2

Click the image to view larger in new window

5. Add the property **P_HOSTNAME** and type the hostname or IP address of your ESET Remote Administrator Server (ERA Server) into the **Value** field.


5. Repeat steps 4 and 5 to add the property **P_PORT**, where the value is the port used to connect to your ERA Server (2222 by default).



Figure 2-3

Click the image to view larger in new window

7. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in. [How do I open ERA Web Console?](#)

7. Click **Admin**  → **Certificates** → **Peer Certificates**, locate the Agent certificate for the ERA Agents you will be distributing, click

it and select **Export as Base64**. Save the exported file to your Desktop.



Figure 2-4

Click the image to view larger in new window

9. Click **Certificate Authorities**, click your ERA Certificate Authority and select **Export public key as Base64**. Save the exported file to your Desktop.



Figure 2-5

Click the image to view larger in new window

10. In Orca, add the following three rows to the file (see steps 4 and 5 above for instructions). See below for property value details:

P_CERT_CONTENT: Copy the contents of the peer certificate file into the value field (open it in a text editor such as notepad).

P_CERT_PASSWORD: Only create this if your peer certificate requires a password. Enter the password to use the peer certificate.

P_CERT_AUTH_CONTENT: Copy the contents of the Certificate Authority public key file into the value field (open it in a text editor such as notepad).

Important!

Both **P_CERT_CONTENT** and **P_CERT_AUTH_CONTENT** must be of **Base64** encoding.

Alternative method: make the certificate available locally

For special cases, you can substitute this method for step 10.

1. Export the peer certificate for the Agent and the public key of the certificate authority used to sign

the Server's peer certificate from the ERA Server. Make these files available to client computers using a shared folder or another resource that all clients can access.

1. In Orca, add the following three rows to the file (see steps 4 and 5 above for instructions). See below for property value details:

P_CERT_PATH: The path to the exported .pfx certificate.

P_CERT_PASSWORD: Only create this if your peer certificate requires a password. Enter the password to use the peer certificate.

P_CERT_AUTH_PATH: The path to the public key of the Certificate Authority that will be used to install ERA Agent.

11. Click **Transform** → **Generate Transform** and save the transform file to your Desktop. Refer to one of the processes below to deploy the file:

- [How do I deploy the ESET Remote Administrator Agent using GPO?](#)
- [How do I deploy the ESET Remote Administrator Agent using SCCM?](#)



Figure 2-6

Click the image to view larger in new window

12. 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 ERA.

Tags

ERA 6.x

ERA Agent