ESET Tech Center

Requirements for remote deployment of ESET Management Agent to Windows targets from ESET PROTECT

Steef | ESET Nederland - 2021-06-18 - Comments (0) - ESET PROTECT On-prem

Issue

- Remote deployment of ESET Management Agent to Windows targets fails or hang at "In Progress"

Solution

For more information on Agent deployment failure, refer to:

- ESET Management Agent deployment troubleshooting (Knowledgebase article)
- ESET Management Agent deployment troubleshooting (Online Help)
- For registry permissions issues, review HKEY_LOCAL_MACHINE permissions.

> Previous antivirus software
> It is important that any previously installed antivirus software is uninstalled from your client workstations before attempting a remote deployment of ESET Management Agent: Uninstallers (removal tools) for common antivirus software

ESET PROTECT allows remote deployment of ESET Management Agent from the ESET PROTECT Web Console to any workstation on the network.

The steps in this document describe the main requirements for remote deployment of ESET Management Agent to Windows targets. We strongly recommend that you verify each of the tasks below before performing the first installation of ESET Management Agent on client workstations:

- The client workstation where you are trying to install the ESET client solution remotely must answer a ping from the computer where the ESET PROTECT Server is installed.
- If both the client workstation and the server are in a mixed environment of Domain and Work Group, disable the Simple File Sharing:
  In **File Explorer**, click **View → Options → Change folder and search options → View →** unselect the check box next to **Use Sharing Wizard** option.
- Workstation must have the **ADMIN$** shared resource activated:
  Start → Control Panel → Administrative Tools → Computer Management → Shared Folders → Shares).
- The user performing the remote installation must have Administrator rights.
- Set the Domain Admininistrator permissions for **ESET PROTECT Server** service:

    - On the ESET PROTECT Server machine, click **Start →** type Services.msc and press **ENTER**. Right-click the **ESET PROTECT Server** service and click **Properties** from the context menu.
    - Click **Log On**, and select **This account** and enter your domain name and administrator account name next to it (for example *MyDomain\AdministratorAccountName*). Enter administrator password in the **Password** and **Confirm password** fields.
    - Run the **ESET PROTECT Server** service with Domain Administrator permissions.
- The user with administrator rights must not have a blank password.
- Verify that you can remotely log in to the workstation from the server.
- Verify that you can access the workstation IPC from the Server machine by issuing the following from the Command Prompt on the Server machine:
    - net use \\workstation\IPC$ *where workstation is the name of the workstation*
- The firewall on the network must not block communication or file sharing between ESET PROTECT Server and the workstation.
- The ESET PROTECT Server must allow network traffic on port 2222.
- Client workstations are visible in both the server and the workstation connection.
- The **File and Print Sharing for Microsoft Networks** option is enabled on the workstation:
  Control Panel → Network and Sharing Center → Change adapter settings → right-click the network adapter **→ Properties**).
- The **Remote Procedure Call (RPC)** service is running on the workstation.
- The **Remote Procedure Call (RPC) Locator** service should be set to **Manual** and should not be running.
- The **Remote Registry** service is running on the workstation.