Remote installation requirements and checklist for ESET Remote Administrator Agent

Ondersteuning | ESET Nederland - 2025-03-07 - Reacties (0) - Legacy ESET Remote Administrator (6.x / 5.x / 4.x)

https://support.eset.com/kb82

Issue

Push installation fails
Computers disappear from the Push install tab of ESET Remote Administrator
Push installations hang at "In Progress"
For registry permissions issues, review HKEY_LOCAL_MACHINE permissions

Solution

Click to view instructions to perform a push installation.

ESET Remote Administrator (ERA) allows remote or "push" installations from the ESET Remote Administrator Console (ERAC) to any workstation on the network with a supported Windows operating system (see supported versions of Windows). The steps in this document describe the main requirements for the execution of this process. Verifying each of the tasks below is strongly recommended before performing the first trial installation on client workstations:

Important!

It is important that any previously installed antivirus software is uninstalled from your client workstations before attempting a push installation:

Uninstallers (removal tools) for common antivirus software

1. The client workstation where you are trying to install the ESET client solution remotely must answer a ping from the computer where ERA Server is installed.

2. If both the client workstation and the server are in a mixed environment of Domain and Work Group (or if ERA Server is running Windows 2003), **Use simple file sharing** (located under the **Tools → Folder Options → View**) should be disabled.

3. Workstation must have the shared resource ADMIN$ activated (**Start → Control Panel → Admin Tools → Computer Mgmnt → Shared Folders → Shares**).

4. The user performing the remote installation must have administrator rights.

5. For Windows Vista, Windows 7 and Windows Server 2008 operating systems, verify the following:

    - To set Domain Admin. permissions for ERA, navigate to **Start → Control Panel → Administrative Tools → Services**. Right-click the **ESET Remote Administrator Server** service and click **Properties** from the context menu.

    - Click the **Log On** tab, and then select the radio button next to **This account**. Enter your Domain name and Admin account name in the **This account** field (for example: *MyDomain\AdministratorAccountName*), and then enter your Admin password in the **Password** and **Confirm Password** fields.

    - The ESET Remote Administrator service should be run with Domain Administrator permissions.

6. The user with administrator rights must not have a blank password.

7. Verify that you can remotely log on to the workstation from the server.

8. Verify that the workstation can access IPC, by issuing the following from the Command Prompt on the workstation:

```
net use \\servername\IPC$
```

where `servername` is the name of the server running ERA.

9. The firewall on the network must not block communications or file sharing between servers and workstations.
10. The ERA Server must allow data reception on ports 2221-2224.
11. For Windows operating systems, verify the following:

    Client workstations are visible in both the server and the workstation connection.
    "File and Print Sharing for Microsoft Networks" is enabled (**Control Panel→ Network Connections→ Network→ Properties**).
    The Remote Procedure Call (RPC) service is running on the workstation.
    The Remote Registry service is running on the workstation.
    The RPC Locator service should be set to "manual" and need not be running.

DNS Issues troubleshooting

If a computer disappears from ESET Remote Administrator (ERA), or hangs at "In Progress" during deployment, one of the following DNS troubleshooting processes could resolve the issue:

Use the 'nslookup' command of the IP address and hostname of the server and/or the clients having push install issues. The results should match the information from the machine. For instance, an nslookup of a hostname should resolve to the IP address an ipconfig command shows on the host in question. The 'nslookup' command will need to be run on the clients and the server.

Manually examine DNS records for duplicates.