ESET Direct Endpoint Management for Solarwinds RMM

User guide

Click here to display the Online help version of this document

Technical Support: https://support.eset.com

REV. 9/7/2021

Introduction

The ESET Direct Endpoint Management for Solarwinds RMM is a Remote Management and Monitoring (RMM) tool that makes monitoring and management easy for ESET Managed Service Providers (MSPs). RMM tools typically monitor system information as well as patch status, antivirus status and other computer health issues. RMM tools also provide a certain level of automation for fixing any health issues that arise or creates a support ticket for the MSP to resolve when the issue cannot be resolved through automation. For more information about the ESET MSP program, contact your local ESET partner or visit the ESET Managed Service Provider Program page.

Managing ESET endpoint products from ESET PROTECT

The ESET PROTECT offers additional functionality such as reporting, dynamic groups and specific client task policies. If you would like to take advantage of these additional functionalities, you will also need to install the ESET Management Agent on the endpoints you are managing.

Integrating with ESET endpoint products

ESET Direct Endpoint Management for Solarwinds RMM provides MSPs with the ability to verify the ESET endpoint product installation status and monitor the protection status and the scan/threat logs of endpoint machines using Automation Policies and Custom Services. The DEM components of this integration require ESET endpoint for Windows products version 6.6 and later and ESET File Security for Windows version 6.5 and later.

System Requirements

The ESET Direct Endpoint Management plug-in for Solarwinds RMM automation policies and custom services must be imported to your Solarwinds RMM server. These components have been developed to work with ESET endpoint products as low as version 6.6 without the use of ESET PROTECT. While the ESET PROTECT is not required with these components, it can still be used in conjunction for additional functionality. Currently these components only support ESET version 6.6 and up on Windows operating systems.

Currently these components support the following ESET endpoint products:

- ESET Endpoint Antivirus 6.6 and higher
- ESET Endpoint Security 6.6 and higher
- ESET Endpoint Antivirus for macOS 6.7 and higher
- ESET Endpoint Security for macOS 6.7 and higher
- ESET File Security for Microsoft Windows Server 7.0 and higher

- ESET Mail Security for Microsoft Exchange Server 7.0 and higher

For ESET endpoint requirements, refer to the system requirements.

These components rely on a companion program, eRMM, which is downloaded automatically to each endpoint once an ESET-specific automation policy has been run on it. This software automatically updates and only requires an internet connection. The eRMM software acts as a means of communication between ESET and Solarwinds RMM.

EULA: https://update.esetusa.com/plugin/ermm/esetlicense.pdf

The ESET Direct Endpoint Management plug-in for SolarWinds RMM provides checks and tasks for both Windows and macOS endpoints.

Add scripts

ESET Direct Endpoint Management for Solarwinds RMM provides files that need to be uploaded to the SolarWinds RMM integration manually.

- **macOS:** Checks and tasks in the form of BASH files (extension `.sh`)
- **Windows:** Checks and tasks in the form of `.amp` files

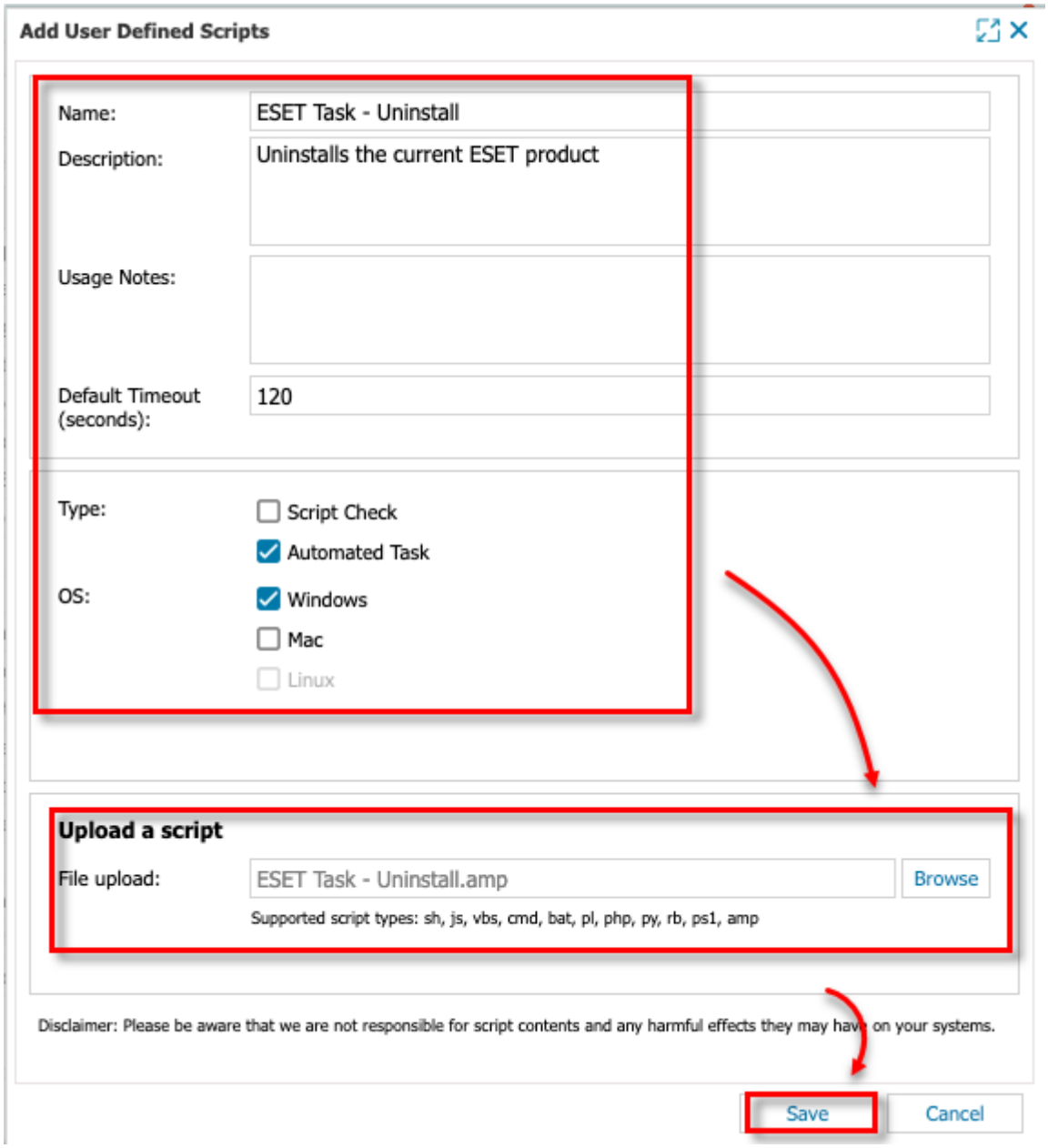
Import script files

When uploading the script, it is important to correctly define whether the uploaded script is a **Script Check** or **Automated Task** and whether it is created for Windows or Mac.

1. In the Dashboard, click **Settings** > **Script Manager**.

2. In the form, click the **+ New** button to add scripts.

3. When uploading the bash scripts to the RMM server, you can decide to sort them among **Script checks** or **Automated tasks**.



Continue with adding tasks and checks.

> You can find syntax schemes for tasks and checks in the Windows and macOS (Mac) topics.

Windows AMP scripts syntax

Checks

Check	Parameter	Note
Product Activated		Fails if the product is not activated. Suggested action: Activate
Product Installed		Fails if the product is not installed. Suggested action: Deploy w Activate
Protection Status		Reports status. Flags if the status is not “Fully Protected”.
Scans		Reports if new scans have been performed since last checked.
Threats		Flags if new threats have been detected. Suggested action: Perform In-Depth scan

Was Configured	age (in following format: n[m|h|d] as in 4d for 4 days, or 2h for 2 hours...)	Flags If the last configuration change is older than age.
Was Updated	age (in following format: n[m|h|d] as in 4d for 4 days, or 2h for 2 hours...)	Flags If the last update is older than age.

Tasks

Task	Parameter	Note
Activate	License in the form of a license key (“XXXX-XXXX-XXXX-XXXX-XXXX”) or ESET MSP Administrator Credentials and Public License ID (“username password PLI-DPLIDP”)	
Configure	Configuration file path.	
Deactivate	Product {EEA|EES|EFSW|EMSX} License in the form of a license key (“XXXX-XXXX-XXXX-XXXX-XXXX”) or ESET MSP Administrator Credentials and Public License ID (“username password PLI-DPL-IDP”)	
Deploy w Activate		
Repair	Product {EEA|EES|EFSW|EMSX} License in the form of a license key (“XXXX-XXXX-XXXX-XXXX-XXXX”) or ESET MSP Administrator Credentials and Public License ID (“username password PLI-DPL-IDP”)	This task reruns the following checks and acts on the issues as necessary: • If the product is not installed, Repair attempts installation • If the product is not activated, Repair attempts activation • If new threats were detected, Repair starts an in-depth scan • In all cases, Repair performs a signature update

On-demand Scan	Targets: “|” (pipe) separated list of Files, Folders or Macros, examples:
	`“c:\users\john\file.tmp”`
	`“c:\users\john”`
	`“${DriveAll}\|${Memory}”`
	
	Profile: scan profile, examples:
	`“@Smart profile”`
	`“@In-depth profile”`	

Uninstall	Uninstall Password (if set)	
Update Module		
Upgrade	Product {EEA|EES|EFSW|EMSX}	

macOS Bash scripts syntax

Checks

Check	Parameter	Note
Product Activated		Fails if the product is not activated. Suggested action: Activate
Product Installed		Fails if the product is not installed. Suggested action: Deploy w Activate
Protection Status		Reports status, Flags if the status is not “Fully Protected”.
Scans		Reports if new scans have been performed since last checked.
Threats		Flags if new threats have been detected. Suggested action: Perform In-Depth scan
Was Configured	`--age` (in following format: n[m|h|d] as in 4d for 4 days, or 2h for 2 hours...) Example: `--age 10m`	Flags If the last configuration change is older than age.
Was Updated	`--age` (in following format: n[m|h|d] as in 4d for 4 days, or 2h for 2 hours...) Example: `--age 10m`	Flags If the last update is older than age.

Tasks

Task	Parameter	Note

Activate	activation “XXXX-XXXX-XXXX-XXXX|ELA_user ELA_password ELA_public_key” (use license key or ESET License Administrator username, password, and public key) Example: `--activation “ABCD-EFGH-IJKL-1234-5678”`	
Configure	`--file filePath.config` (configuration file path) Example: `--file ”config000.xml”`	
Deactivate		
Deploy w Activate	`--accept_eula` (mandatory) `--product {EEA|EES}` `--activation` (see activate above) Example: `--accept_eula --product EEA --activation “ABCD-EFGH-IJKL-1234-5678”`	
Repair	`--accept_eula` (mandatory) `--product {EEA|EES}` `--activation` (see activate above) Example: `--accept_eula --product EEA --activation “ABCD-EFGH-IJKL-1234-5678”`	This task reruns the following checks and acts on the issues as necessary: • If the product is not installed, Repair attempts installation • If the product is not activated, Repair attempts activation • If new threats were detected, Repair starts an in-depth scan • In all cases, Repair performs a signature update

On-demand Scan	`--targets {file|folder}`
	`--profile profile`
	
	Example: `--targets “/” --profile “@Smart scan”`	

Uninstall		
Update Module		
Upgrade	`--accept_eula` (mandatory) `--product {EEA|EES}` `--activation` (see activate above) Example: `--accept_eula --product EES --activation “ABCD-EFGH-IJKL-1234-5678”`	

Using checks, tasks and templates

Adding Checks and Tasks

Checks can be performed at regular intervals (for example, every 30 minutes), or daily at a predetermined time. When a check fails, an associated task can be performed, usually to fix the issue detected by the check. Tasks can be set to execute at regular intervals (for example, periodic scans), or manually on demand, or upon failure of the check.

Setting Monitoring Templates

Computers with assigned checks and tasks can be used as a template to assign checks and tasks to other computers. Create a monitoring template from a computer and then assign that template to other machines.

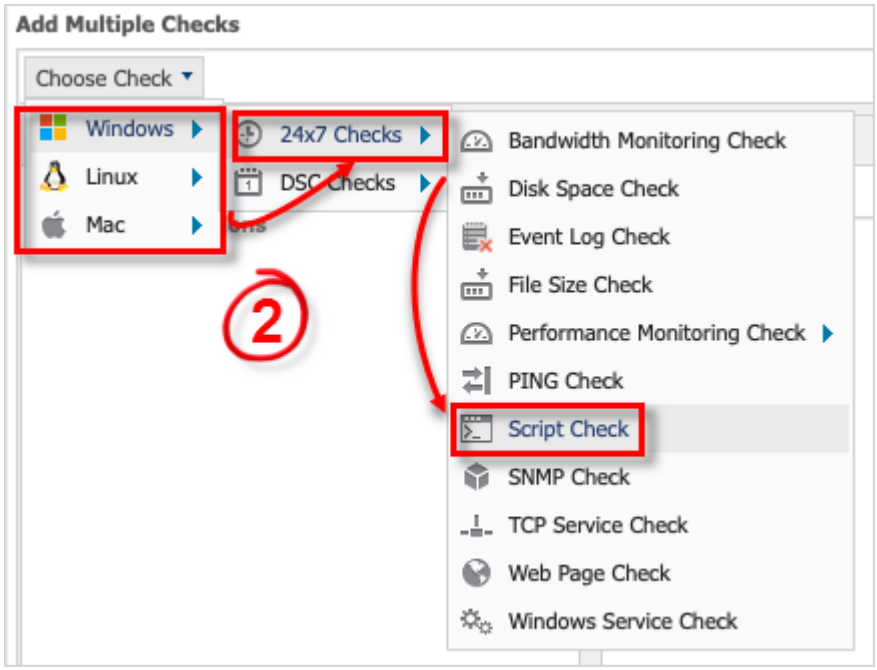
Adding checks

Checks can be performed at regular intervals (for example, every 30 minutes), or daily, at a predetermined time. When a check fails, an associated task can be performed, usually to fix the problem detected by the check.

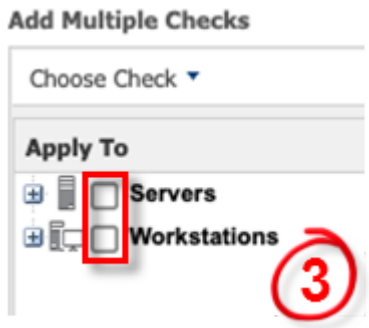
> i You can find syntax schemes for tasks and checks in the Windows and macOS (Mac) topics.

1. In the Dashboard, click **File** > **Add check**.

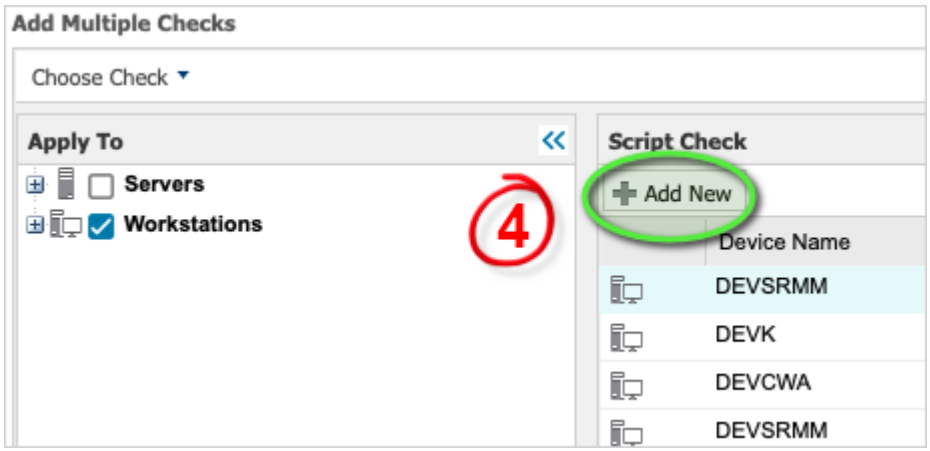
2. Click **Choose Check** and select **Windows** or **Mac** > **24x7 Checks** (or **DSC checks** depending on the frequency you need) > **Script Check**. One check can only be applied on Windows or Mac (macOS) machines, not both.



3. Select a target for the check (**Server**, **Workstation**...) and the client/location for which you want the check(s) applied.

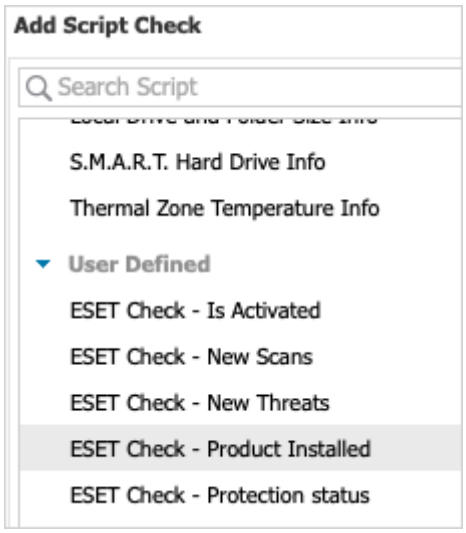


4. Click **Add New** to add more scripts.



5. In the **Add Script Check** window, scroll down to the **User Defined** section select the applicable

script and then click **Next**.



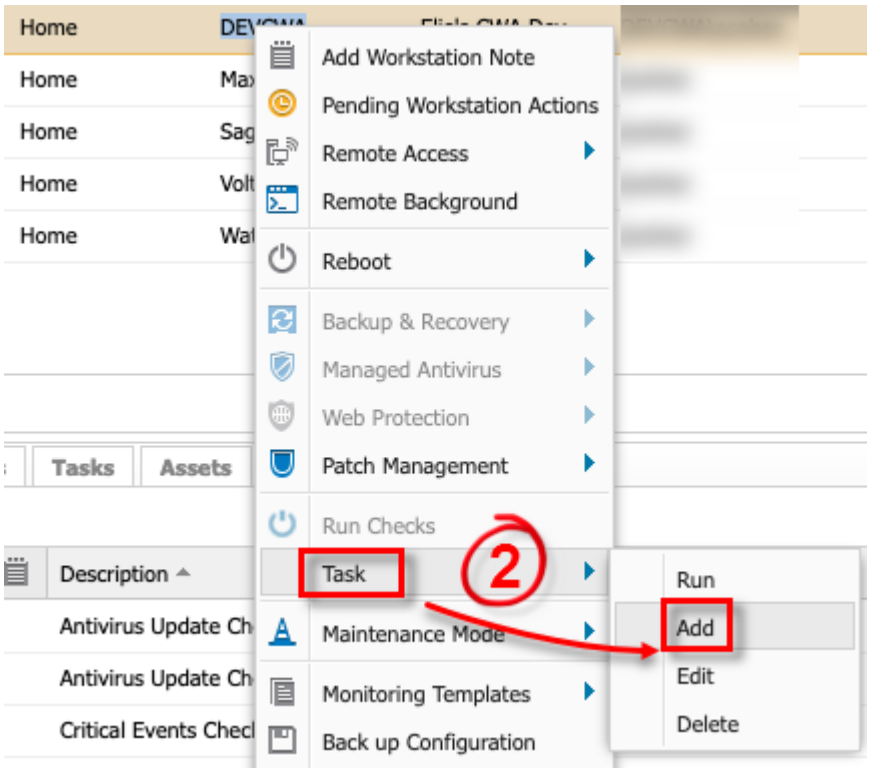
6. Choose an execution time-out then click **Finish**.

Adding a task

> You can find syntax schemes for tasks and checks in the Windows and macOS (Mac) topics.

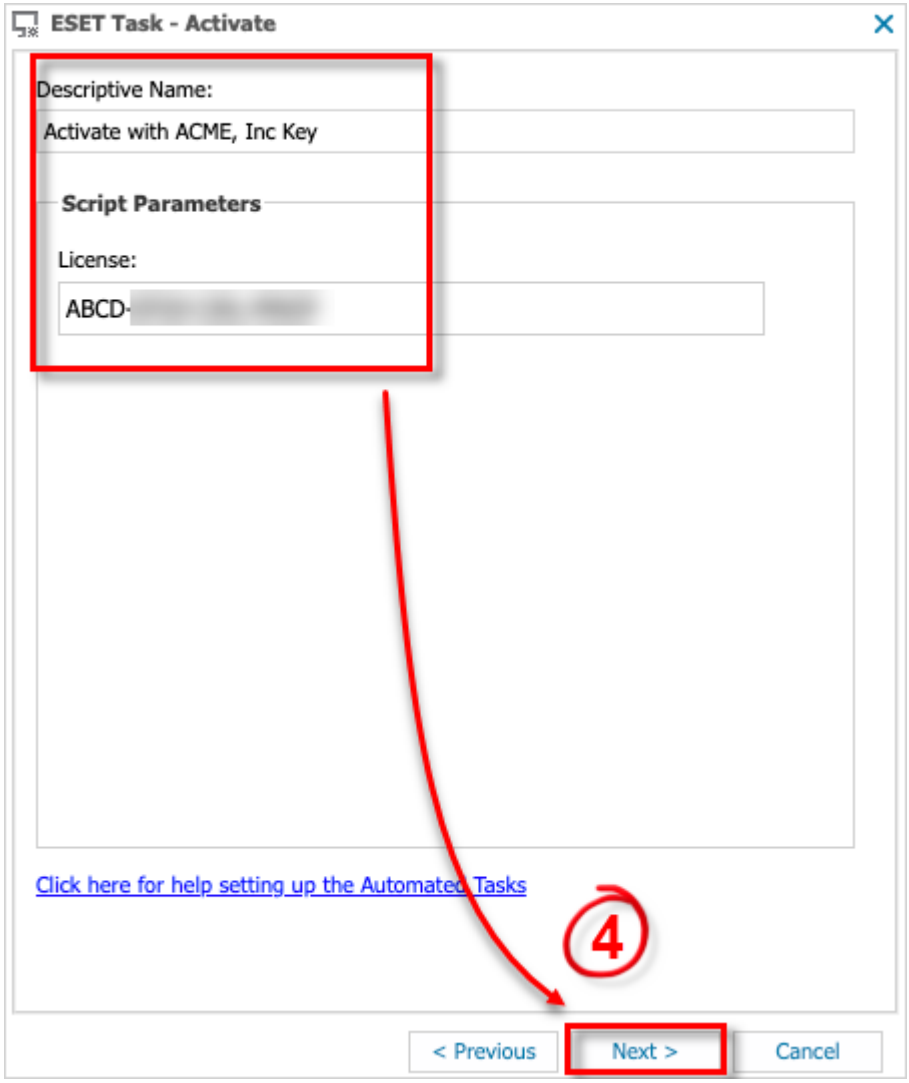
1. In the computer list, select the applicable Windows or Mac computer. One task can only be applied on Windows or Mac (macOS) machines, not both.

2. Right-click the computer, select **Task** > **Add**.

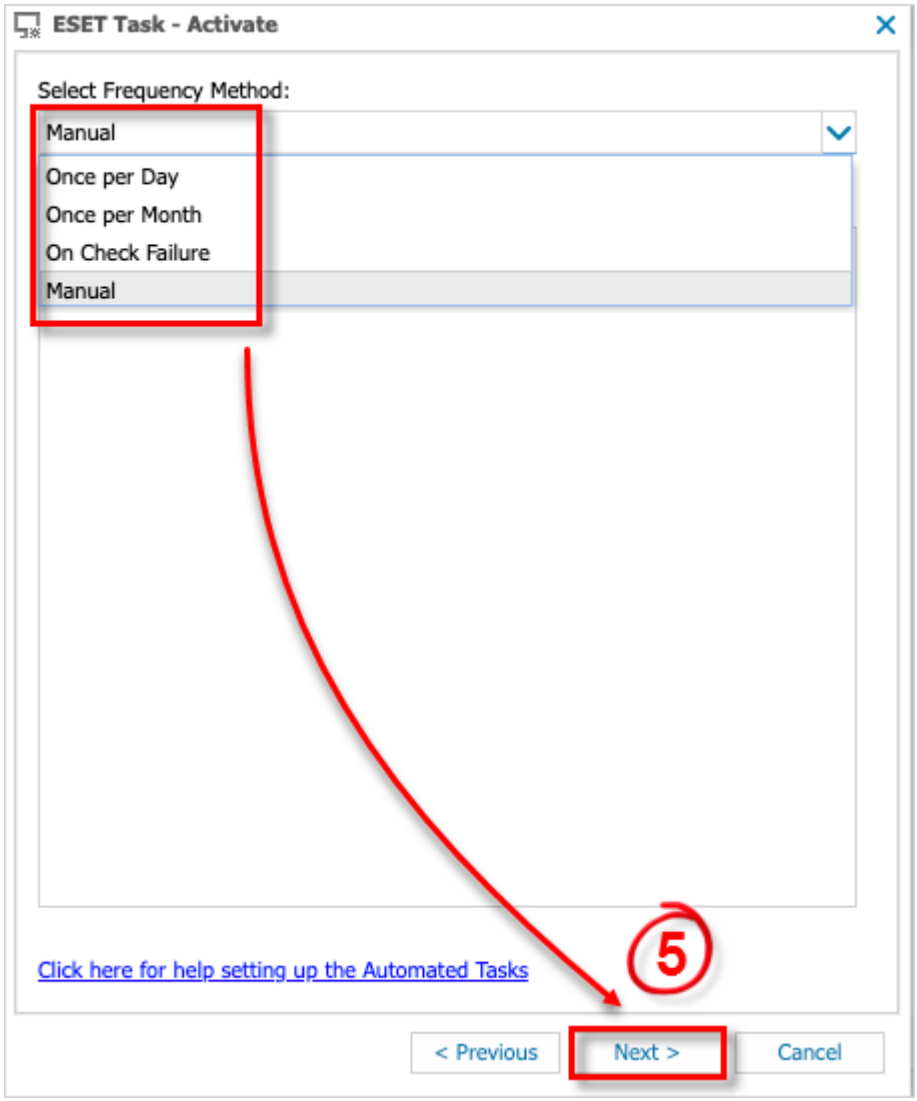


3. In the **Search script** field, type ESET (if you have used the naming convention ESET) and the type of script. You receive all available ESET tasks.

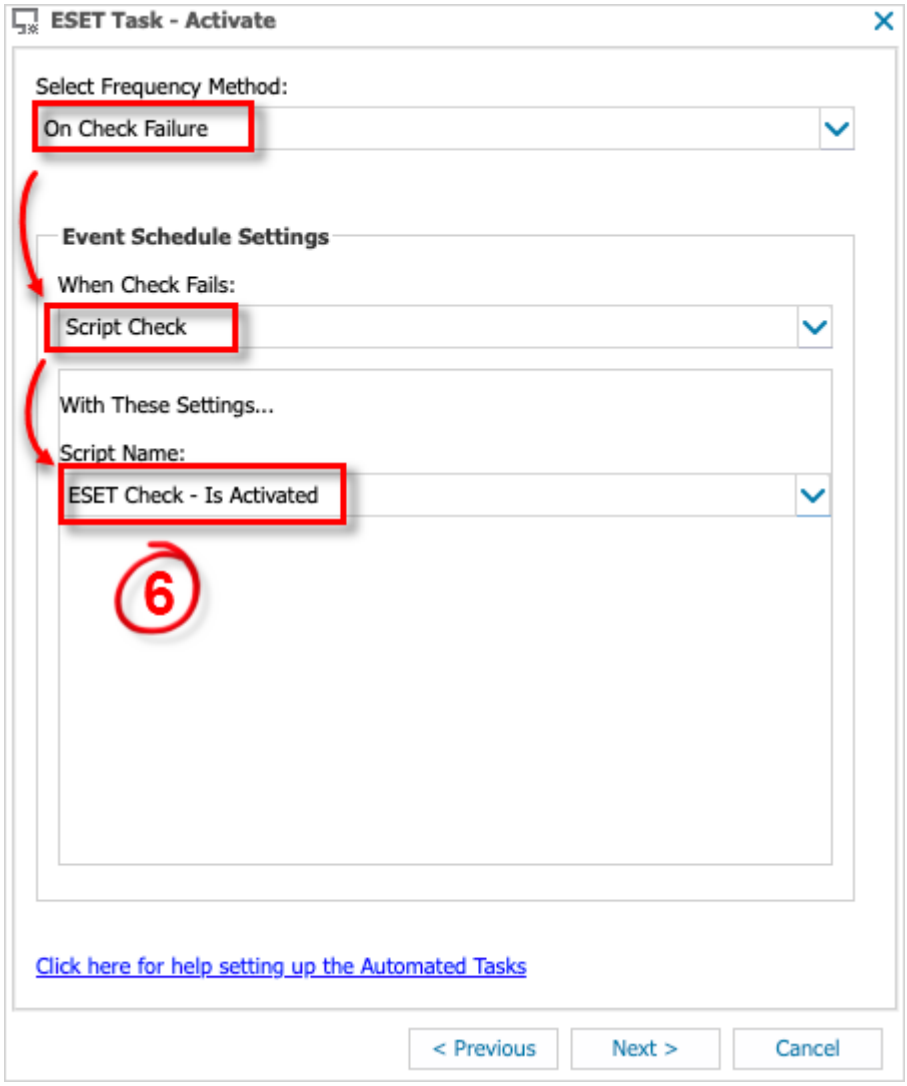
4. Select the applicable task, add the applicable task type script parameters (for example, Activation) and click **Next**.



5. Select the applicable frequency method and click **Next**.



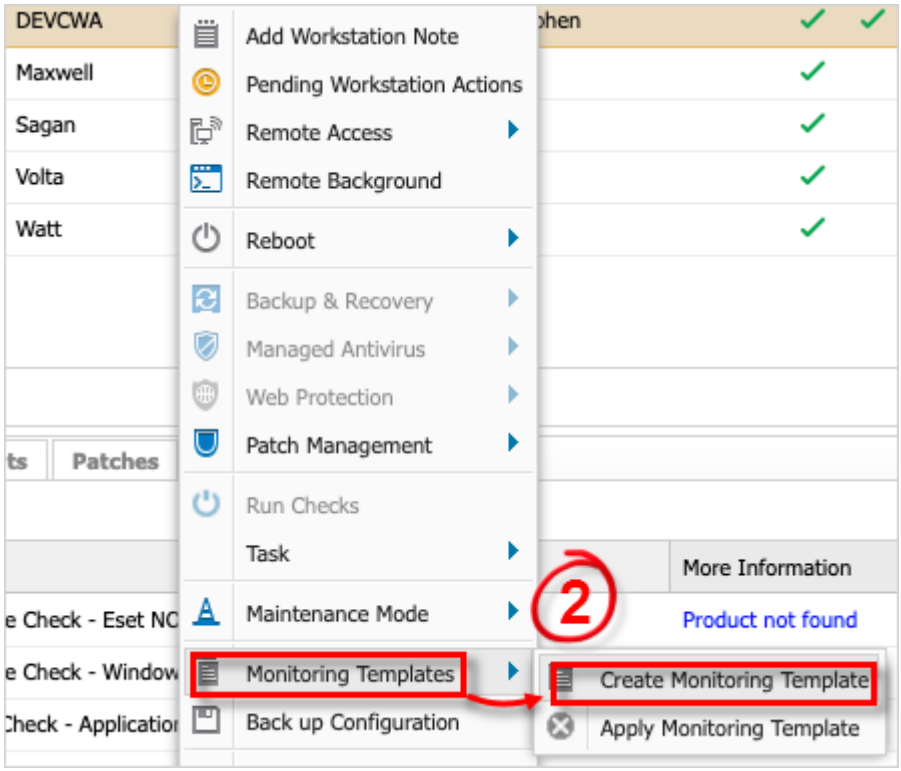
6. If you choose **On Check Failure**, you can choose what kind of previously added check should be the one that triggers a given task.



7. Set an execution time limit.
8. Click **Finish**.

Create a monitoring template

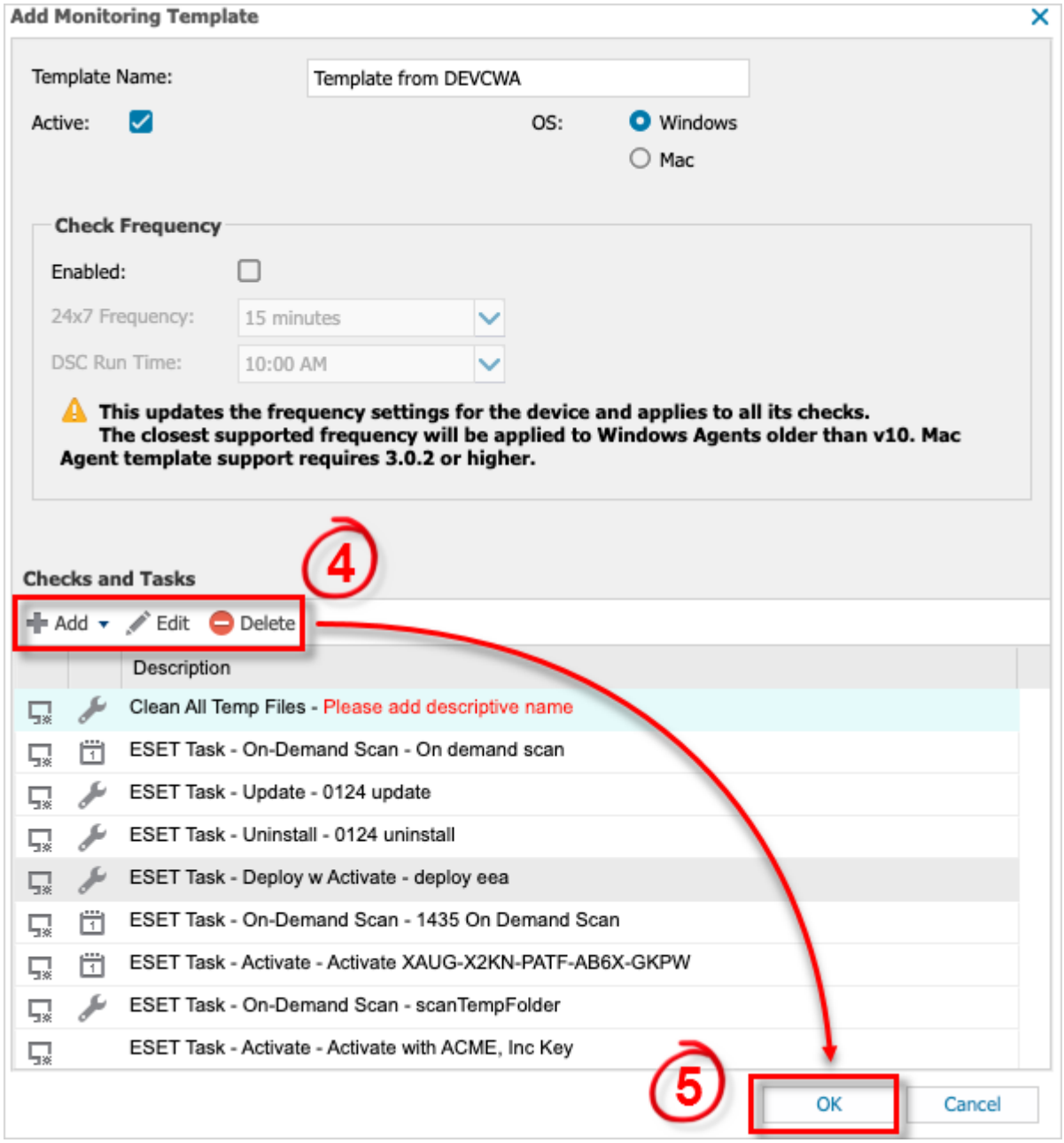
1. Select the applicable computer.
2. Right-click the machine, select **Monitoring templates** > **Create Monitoring Template**.



3. Select **Include checks** and **Include tasks**, click **Next**.

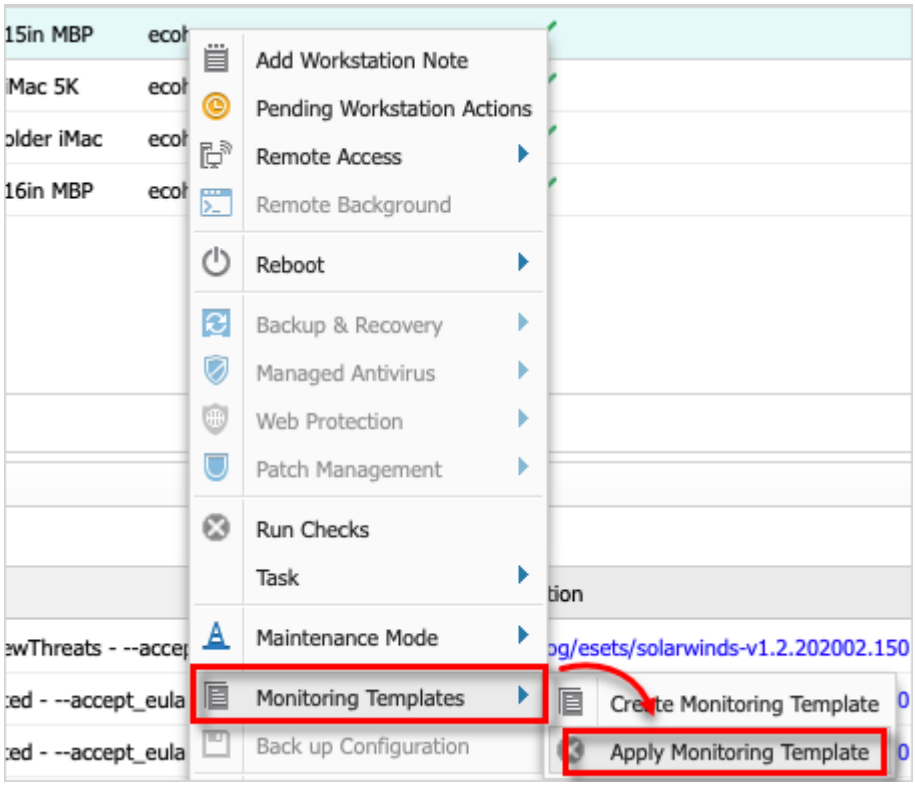
4. In the **Add Monitoring Template**, add or remove checks and tasks as necessary.

5. Click **OK**.



Apply template to other computers

1. In the Dashboard, select the applicable computers.
2. Right-click the computer, select **Monitoring Templates** > **Apply Monitoring Template**.



3. Follow the instructions on screen.

Support and Troubleshooting

Assistance

If you require assistance on the ESET Direct Endpoint Management for Solarwinds RMM, contact your ESET partner.

Feedback

Submit feedback, make feature requests and send comments about ESET Direct Endpoint Management for Solarwinds RMM to our development team at: gpcf@eset.com. Your feedback is greatly appreciated, and we encourage you to provide a contact number and email address if you would like a response from our team.