DIRECT ENDPOINT MANAGEMENT

PLUG-IN FOR SOLARWINDS N-CENTRAL

Bringing MSPs the opportunity to manage and deploy their customers' ESET protection directly from SolarWinds N-Central, **ESET Direct Endpoint Management plug-in for SolarWinds N-Central** is the most advanced endpoint protection plug-in available on the platform. The plug-in provides MSPs with all the capabilities needed for seamless day-to-day management of endpoints with ESET antimalware, from deployment to alerts and configuration changes. The automation monitors help you automate the processes and remediate any potential issues without the need for your manual intervention.

Benefits

Fast deployment	With the built-in install and activation capabilities, your customer's network is protected within minutes.
Quick learning curve	The Direct Endpoint Management plug-in connects directly to the familiar environment of SolarWinds N-Central. No need to learn how to use it.
Best plug-in functionality	With ESET Direct Endpoint Management plug-in for SolarWinds N-Central, you get the best endpoint protection plug-in, with the widest range of capabilities and automation options.
Save time and earn money	The plug-in's capabilities combined with ESET's trademark detection and extremely low support burden give you an unparalleled profit-per-seat ratio.

Capabilities

ESET Direct Endpoint Management plug-in for SolarWinds N-Central relies on **automation monitors**, executed at predefined time intervals. You can monitor the following:

- Check if ESET antimalware is installed
- Check the protection status
- Report the last on-demand scan
- Report the last threat detection (on-access detection)

Besides monitors, there are **tasks**. Tasks can be run separately, or they can be triggered by the above monitors. There are altogether seven types of tasks:

Deploy and activate	Downloads, installs and activates the most recent ESET product version (uninstall also available)
Activate	A standalone activation task re-sends license information to the endpoint to activate it
De-activate	Rescinds activation from the product
On-demand scan	Initiates a scan, and lets you define scan targets and the scan profile
Configure	Sends a configuration file with policy to endpoints
Update	Updates detection definitions
Upgrade	Performs an upgrade to a newer product version

System requirements

ESET Business Product Licenses

Active licenses of any of the following ESET endpoint products:

- ESET Endpoint Antivirus for Windows
- ESET Endpoint Security for Windows
- ESET File Security for Microsoft Windows Server
- ESET Mail Security for Microsoft Exchange Server

SolarWinds N-Central*

*To review the system requirements, please visit SolarWinds N-Central's website.

How to automate

Following are examples of how you can use the plug-in components to your advantage to automate the management of endpoint security, and save time creating and resolving tickets.

1. Automatically scan a device after threat detection
   a. Situation: When a new threat is detected on an endpoint, you may want more than just an alert or ticket.
   b. How to automate: Have an On-Demand Scan task—a full disk scan—set up for situations when a new threat has been detected by the on-access scanner.
2. Ensure continuous protection
   a. Situation: For any number of reasons, customers' endpoints may end up without ESET installed or activated.
   b. How to automate: To achieve continuous uptime, combine the Product Installation Monitor with the automation policy Deploy and Activate. For situations where you receive a not-installed result, have Deploy and Activate task automatically run remote installation. Analogically, for when you receive a not-activated monitor result, have automatic activation task triggered.
3. Ensure detection definitions updates
   a. Situation: While ESET antimalware has a default update task built in, you can set up an additional remote update in case the default one fails.
   b. How to automate: Set up an update task for situations where an endpoint reports that it hasn't been updated in the specified time frame.
4. Enforce configuration
   a. Situation: You want to make sure that all devices within the given group are using the same configuration/policies.
   b. How to automate: Have the Task component regularly run on the device group and overwrite any configuration that is older than the specified time frame, and have the Task component apply the desired configuration.