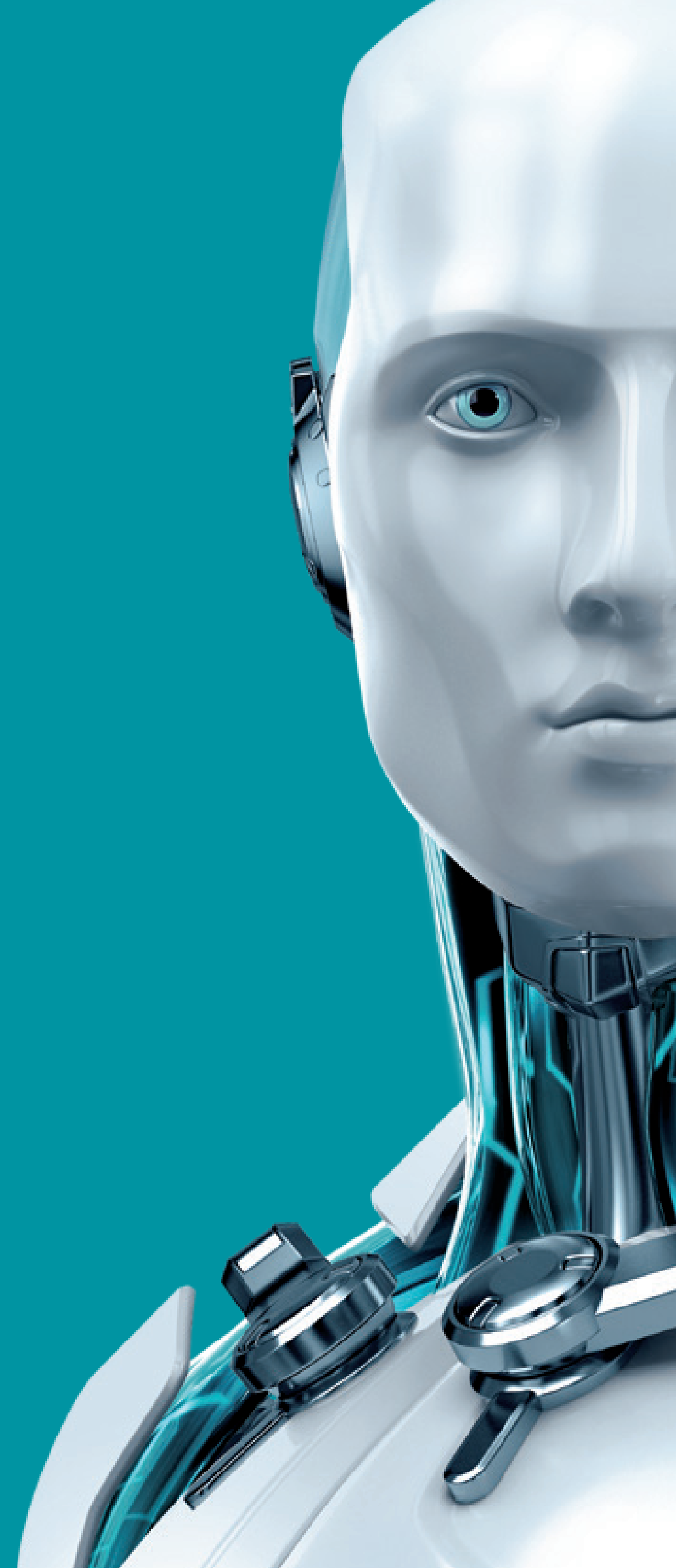
ESET®

DIRECT ENDPOINT MANAGEMENT

PLUGIN FOR SOLARWINDS N-CENTRAL

BUSINESS

ENJOY SAFER TECHNOLOGY™



DIRECT ENDPOINT MANAGEMENT

PLUGIN 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 plugin for SolarWinds N-Central** is the most advanced endpoint protection plugin available on the platform.

The plugin 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.

Questions about product or a partnership?
Contact your ESET representative.
www.eset.com

Benefits

Fast deployment	With the in-buit install and activation capabilities, you're customer's network is protected within minutes.
Quick learning curve	The direct endoint management plugin connects directly to the familiar environment of SolarWinds N-Central. No need to learn how to use it.
Best plugin functionality	With ESET Direct Endoint Management plugin for SolarWinds N-Central, you get the best endpoint protection plugin, with the widest range of capabilities and automation options.

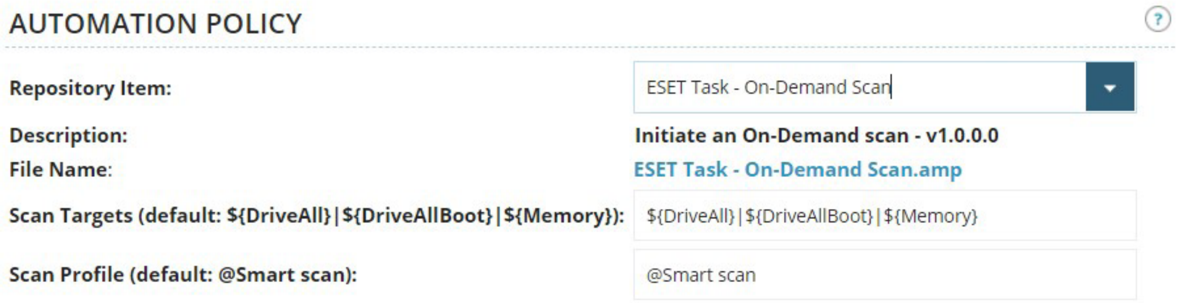
Capabilities

ESET Direct Endpoint Management plugin 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**. Task can be run separately, or they can be triggered by the above monitors. There are altogether 7 types of tasks:

Deploy and Activate	Downloads, installs and activates the most recent ESET product version. (Also unistall is available)
Activate	A standalone activation task – re-sends license information to the endoint to activate it
De-activate	Rescinds activation from the product
On-demand Scan	Initiates a scan; 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



AUTOMATION POLICY

Repository Item: ESET Task - On-Demand Scan

Description: **Initiate an On-Demand scan - v1.0.0.0**

File Name: **ESET Task - On-Demand Scan.amp**

Scan Targets (default: ${DriveAll}|${DriveAllBoot}|${Memory}): ${DriveAll}|${DriveAllBoot}|${Memory}

Scan Profile (default: @Smart scan): @Smart scan

Figure 1 On-demand scan setup

How to automate

These are the examples of how you can use the plugin 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: to automatically trigger a full-disk scan when a new threat has been detected.

2. **Ensure continuous protection**
   a. Situation: For any number of reasons, customers' endpoints may end up without ESET installed or activated antimalware.
   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 being triggered.

3. **Ensure detection definitions updates**
   a. Situation: While ESET antimalware has a default update task running, 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, have the Task component apply the desired configuration.

System requirements

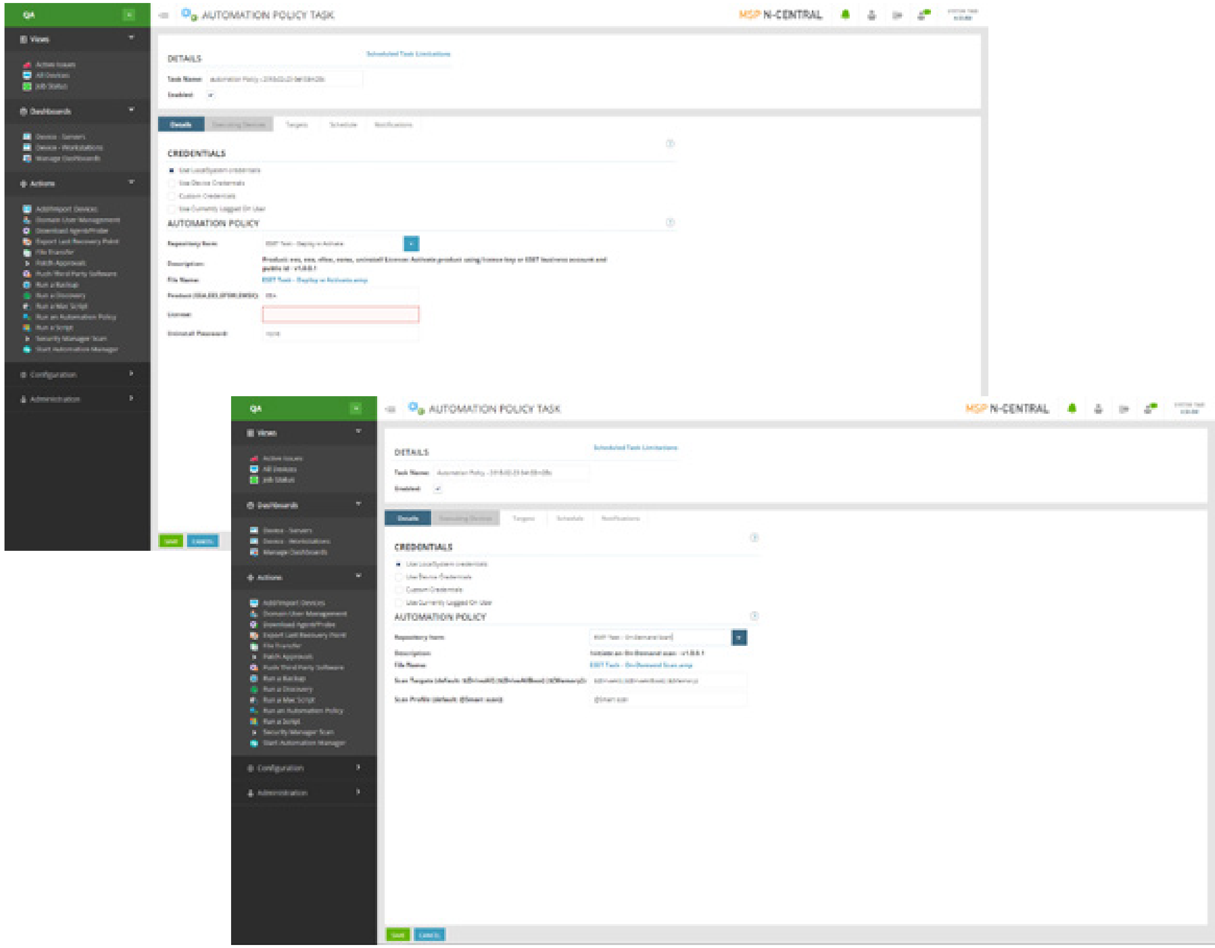
ESET Business Product Licenses

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.


QA
Views
Active Issues
All Devices
Job Status
Dashboards
Device - Servers
Device - Workstations
Manage Dashboards
Actions
Add/Import Devices
Domain User Management
Download Agent/Probe
Export Last Recovery Point
File Transfer
Patch Approvals
Push Third Party Software
Run a Backup
Run a Discovery
Run a Mac Script
Run an Automation Policy
Run a Script
Security Manager Scan
Start Automation Manager
Configuration
Administration
AUTOMATION POLICY TASK
MSP N-CENTRAL
DETAILS
Scheduled Task Limitations
Task Name:
Enabled:
Details
Targets
Schedule
Notifications
CREDENTIALS
Use LocalSystem credentials
Use Device Credentials
Custom Credentials
Use Currently Logged On User
AUTOMATION POLICY
Repository Item:
Description:
File Name:
License:
Uninstall Password:
SAVE
CANCEL