



DIRECT ENDPOINT MANAGEMENT

PLUGIN FOR DATTO RMM

CYBERSECURITY
EXPERTS ON YOUR SIDE

Capabilities

The plugin consists of three components, each providing MSPs with different functionalities.

DEPLOYMENT COMPONENT

Directly deploys ESET Security products to secure endpoints. The component's capabilities include installing, re-installing and uninstalling ESET antimalware.

TASK COMPONENT

Allows you to easily perform tasks on endpoints. Includes **Activation** and **Deactivation**, **Configuration** changes, Running **remote scans and updates**. The Task component also integrates with Datto RMM's Quick Jobs or Scheduled Jobs.

ESET Direct Endpoint Management plugin for Datto RMM offers MSPs a wide range of functionality, from fast installation and deployment, to policy and alert management, allowing for a very high level of automation. Last but not least, there's no need to install any additional cloud or on-premise console as the plugin works from Datto RMM and communicates directly with endpoints.

MONITORING COMPONENT

Monitors **Detection updates, ESET product status (installed, running), Protection Status, Activation status, Threat log** and **Scan log events**, and also creates comprehensive **Diagnostic summaries**. Lets you limit monitoring based on the severity, and **automatically generate a ticket** in Datto RMM or send an email to the admin in case an intervention is required.

SYSTEM REQUIREMENTS

ESET Business Product Licenses

Active licenses of any of the following ESET endpoint products:

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

For the complete list of supported ESET products visit help.eset.com.

Datto RMM

To review Datto RMM system requirements, please visit Datto RMM's website.

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

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

Situation: When a new threat is detected on an endpoint, you may want more than just an alert or ticket.

How to automate: Combine Monitoring and Task components to automatically trigger a full-disk scan when a new threat has been detected.

2. ENSURE CONTINUOUS PROTECTION

Situation: For any number of reasons, customers' endpoints may end up without ESET installed or activated antimalware.

How to automate: To achieve continuous uptime, combine Monitoring and Deployment or Task Components. For situations where you receive a not-installed alert, have Deployment tool automatically run remote installation. Trigger automatic activation task for each not installed alert in chronological order.

3. ENSURE DETECTION DEFINITIONS UPDATES

Situation: While ESET antimalware has a default update task running, you can set up an additional remote update in case the default one fails.

How to automate: If the endpoint reports that it hasn't been updated in the specified time frame.

4. ENFORCE CONFIGURATION

Situation: You want to make sure that all devices within the given group are using the same configuration policies.

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.

Benefits

FAST DEPLOYMENT

With no need to install a cloud or on-premise console, you're up and running within minutes.

QUICK LEARNING CURVE

The direct endpoint management plugin connects directly to the familiar environment of Datto. There is no need to learn how to use it.

BEST PLUGIN FUNCTIONALITY

With ESET Direct Endpoint Management plugin for Datto RMM, you get the best endpoint protection plugin, with the widest range of capabilities and automation options.

SAVE TIME AND MONEY

The plugin's capabilities combined with ESET's trademark detection and extremely low support burden give you an unparalleled profit-per-seat ratio.

The screenshot shows the ESET Endpoint Management interface. The main window displays a table of devices under the 'SITE: QA' view. A dialog box titled 'Select component to use in quick job' is open, allowing the user to choose between 'ESET Direct Endpoint Management - Deployment' and 'Kaspersky Endpoint Security 10.3 [WIN]'. The 'ESET Direct Endpoint Management - Tasks' option is selected, and its configuration fields are visible: ACCEPT_EULA (ACCEPT), TASK (SCAN), SCAN_PROFILE (SCAN), SCAN_TARGETS (\$[Boot]), ACTIVATION (empty), CONFIG_FILE (empty), and CONFIG_PASSWORD (empty). The background table lists devices with columns for Hostname, Description, IP Address, Ext IP Addr, Last User, and Operating System.

The 'Update a Monitor' dialog box is shown, detailing the configuration for a monitor. It includes sections for Monitor Details, Response Details, and Ticket Details. The Trigger Details section is expanded, showing the following configuration: Run the Component Monitor [ESET Direct Endpoint Management - Monitor] configured with the following Variables: ACCEPT_EULA: ACCEPT, MONITOR: PROTECTION, SEVERITY: diagnostic, info_w, and executed every 0 : 1 (hrs : mins). The Alert Details section shows 'Raise an alert of priority: Moderate'. The Auto-Resolution Details section shows 'After 1 minute' resolve the alert if it is no longer applicable. The dialog has 'Back' and 'Next' buttons at the bottom right.

ESET IN NUMBERS

110m+
users
worldwide

400k+
business
customers

200+
countries
& territories

4000+
MSPs
worldwide