



# DIRECT ENDPOINT MANAGEMENT

PLUG-IN FOR AUTOTASK AEM



For MSPs (Managed Service Providers) using the **Autotask AEM Remote Monitoring and Management** (RMM) tool, ESET provides a state-of-the-art plug-in to connect Autotask AEM directly with ESET antimalware solutions for endpoints. **ESET Direct Endpoint Management plug-in for Autotask AEM** 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 plug-in works from Autotask AEM and communicates directly with endpoints.

## Benefits

<b>Fast deployment</b>	Without the need to install a cloud or on-premise console, you're up and running within minutes.
<b>Quick learning curve</b>	The Direct Endpoint Management plug-in connects directly to the familiar environment of Autotask AEM. No need to learn how to use it.
<b>Best functionality</b>	With ESET Direct Endpoint Management plug-in for Autotask AEM, you get the best endpoint protection plug-in, with the widest range of capabilities and automation options.
<b>Save time and earn money</b>	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

The plug-in consists of three components, each providing MSPs with different functionalities.

<b>Deployment component</b>	Directly deploys ESET Security products to secure endpoints. The component's capabilities include installation, re-installation and the option to uninstall ESET antimalware.
<b>Monitoring component</b>	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 filter events based on the severity and automatically generate a ticket in Autotask AEM or send an email to the admin in case an intervention is required.
<b>Task component</b>	Allows you to easily perform tasks on endpoints. Includes activation and deactivation, configuration changes, and running remote scans and updates. The task component also integrates with Autotask AEM's Quick Jobs or Scheduled Jobs.

# 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

## Autotask AEM\*

\*To review Autotask AEM system requirements, please visit Autotask AEM'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

- 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 component 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.
- How to automate: To achieve continuous uptime, combine Monitoring and Deployment or Task component. For situations where you receive a not-installed alert, have Deployment tool automatically run remote installation. Analogically, on each not-activated alert, have automatic activation task triggered.

### 3. Ensure detection definitions updates

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

- 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, and have the Task component apply the desired configuration.

The screenshot displays the ESET Direct Endpoint Management (DEM) console interface. The main window shows a list of devices under the 'SITE: QA' group, with columns for IP Address, Ext IP Addr, Last User, and Operating System. A 'Select component to use in quick job' dialog is open, showing a tree view of components including 'ESET Direct Endpoint Management - Deployment', 'ESET Direct Endpoint Management - Tasks', 'ACCEPT\_EULA', 'SCAN', 'SLEEP', 'SCAN\_PROFILE', 'SCAN\_TARGETS', 'ACTIVATION', 'CONFIG\_FILE', and 'CONFIG\_PASSWORD'. A second dialog, 'Update a Monitor', is also open, showing 'Monitor Details' for 'ESET Direct Endpoint Management - Monitor'. The 'Trigger Details' section shows 'ACCEPT\_EULA' set to 'ACCEPT', 'MONITOR' set to 'PROTECTION', and 'SEVERITY' set to 'diagnostic\_info.w'. The 'Alert Details' section shows 'Alert Details' set to 'Moderate' and 'Auto Resolution Details' set to 'After 1 minute'.

© 1999-2018 ESET, LLC, d/b/a ESET North America. All rights reserved.

ESET, the ESET Logo, ESET android figure, ESET SMART SECURITY, ESET CYBER SECURITY, ESET.COM, ESET.EU, NOD32, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid and LiveGrid logo are trademarks, service marks and/or registered trademarks of ESET, LLC, d/b/a ESET North America and/or ESET, spol. s r. o., in the United States and certain other jurisdictions. All other trademarks and service marks that appear in these pages are the property of their respective owners and are used solely to refer to those companies' goods and services.