DIRECT ENDPOINT MANAGEMENT

PLUG-IN FOR AUTOTASK AEM

Autotask® AEM
Autotask Endpoint Management

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

Fast deployment	Without the need to install a cloud or on-premise console, you're up and running within minutes.
Quick learning curve	The Direct Endpoint Management plug-in connects directly to the familiar environment of Autotask AEM. No need to learn how to use it.
Best functionality	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.
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

The plug-in 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 installation, re-installation and the option to uninstall ESET antimalware.
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 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.
Task component	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
   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: Combine Monitoring and Task component 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.
   b. 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
   a. 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.
   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.