

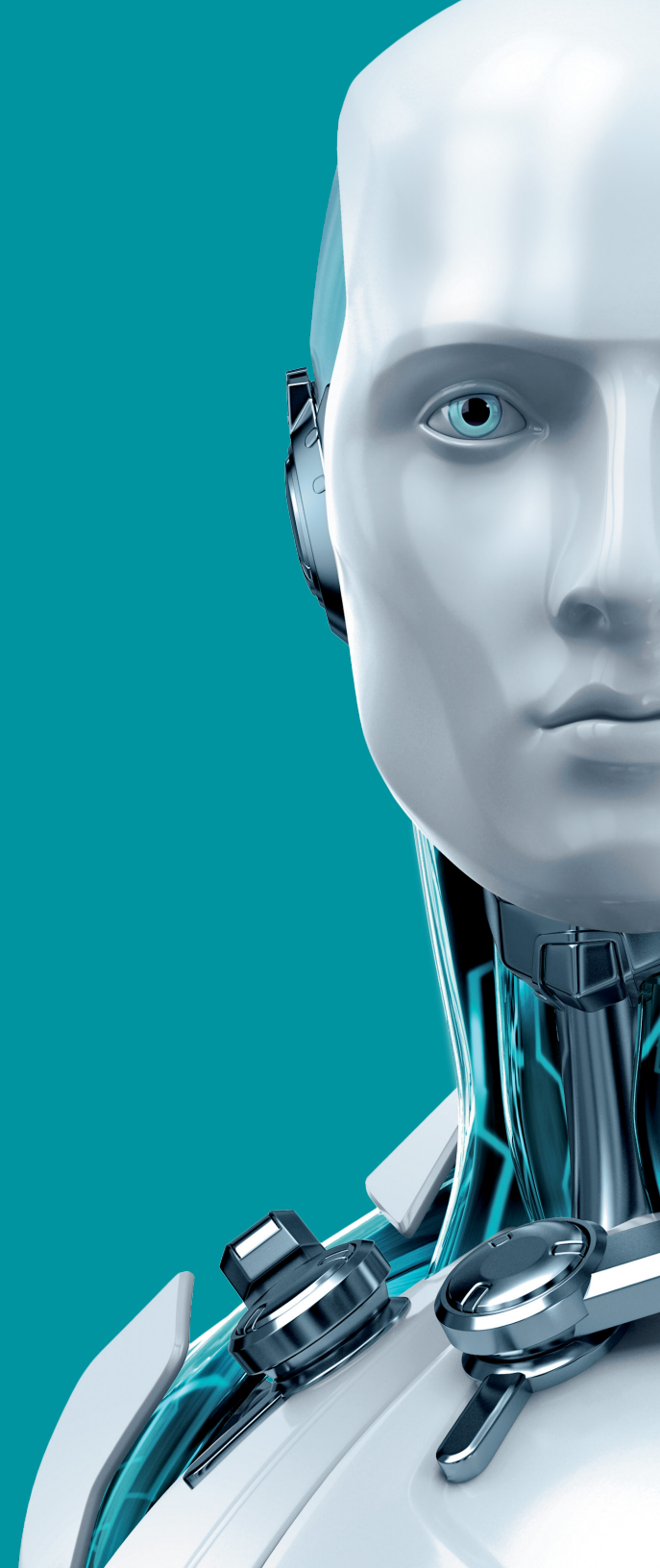


# MSP PROGRAM

ESET Remote Administrator Plugin for Kaseya



ENJOY SAFER TECHNOLOGY®





# MSP PROGRAM

ESET REMOTE ADMINISTRATOR  
PLUGIN FOR KASEYA

## Kaseya® Virtual System Administrator™

is widely used to manage a variety of IT services including antimalware and endpoint security. ESET now offers a solution for delivering best-in-class malware protection through the Kaseya environment.

**The ESET Remote Administrator Plugin for Kaseya** integrates with the Kaseya Virtual System Administrator to provide central management of ESET Endpoint Solutions across distributed networks. Controlling ESET's powerful, proactive malware detection using Kaseya's familiar console delivers ease of administration and a common interface for configuring and reporting.

## Benefits

<b>Expanded options</b>	Offer additional antimalware options to your network of managed clients. Replace existing solutions with ESET's lightweight clients for low system resource usage and proactive detection of multiple threat vectors.
<b>Ease of management</b>	The familiar Kaseya console provides ease of management and adoption of ESET solutions without requiring a second console.
<b>Satisfied end users</b>	Real-time monitoring and remediation helps resolve security issues quicker and makes for confident helpdesk techs and satisfied end users.

## Features

<b>Manage client endpoint security</b>	Deploy ESET endpoint software directly from your Kaseya console. Initiate on-demand endpoint scans and virus signature database updates. Customize and sort your client display with over 20 client attributes.
<b>Manage client configurations</b>	Set ESET-specific configuration policies on Windows®, Mac® or Linux™ clients.
<b>Monitor threats</b>	View and sort threat data, choosing up to 15 threat attributes to display.
<b>Dashboards</b>	Customize your dashboard view to display threat data in easy-to-read graphs and charts. Dashboards show client, threat and scan information broken down by Kaseya organization.
<b>Reporting</b>	Create report templates and generate PDF reports using the Kaseya Info Center.
<b>Alerts</b>	Create Kaseya alerts for specific machine groups, based on selectable client status triggers such as: detected threats, virus definitions or license out of date, client reboot or no connection to ESET Remote Administrator after specified number of days. Set up alerts to either email IT technicians or run Kaseya agent procedure scripts. Trigger ESET scan and virus signature database updates.
<b>Admin permissions</b>	Define permissions for different user roles to allow or deny access to different product settings.

# System requirements

ESET Remote Administrator 6.5+  
ESET Remote Administrator 5.3.x

## ESET Business Product Licenses

Active licenses of any of the following ESET endpoint products:

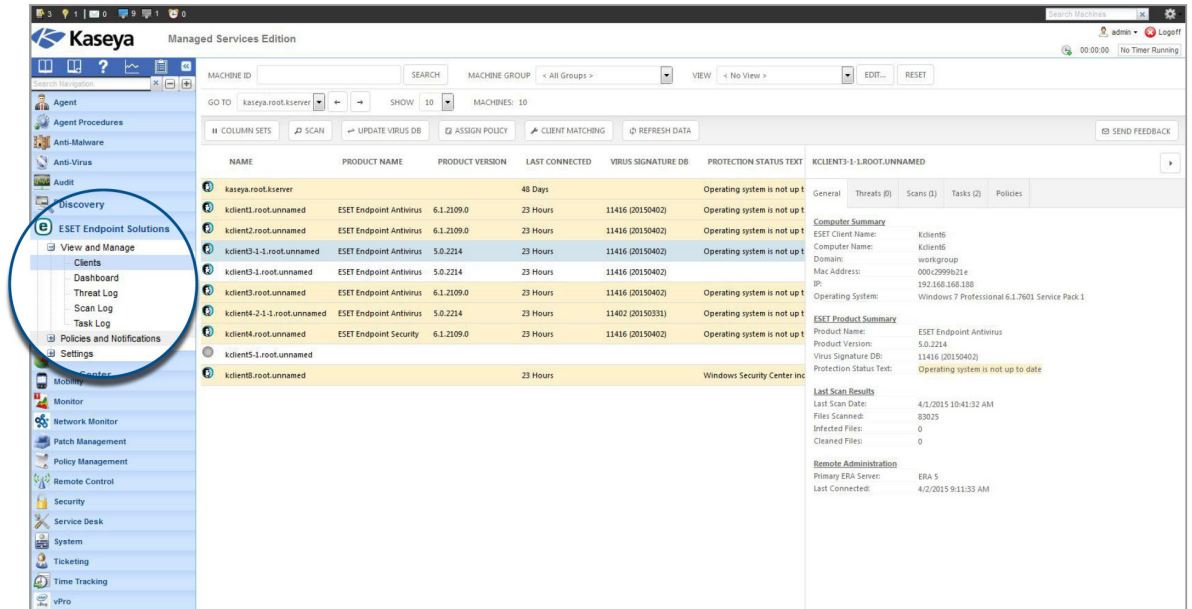
- ESET Endpoint Antivirus for Windows
- ESET Endpoint Security for Windows
- ESET NOD32 Antivirus Business Edition for macOS
- ESET Smart Security Business Edition for macOS
- ESET NOD32 Antivirus Business Edition for Linux Desktop

Also can be used to manage and monitor select ESET Windows or Linux File Server products

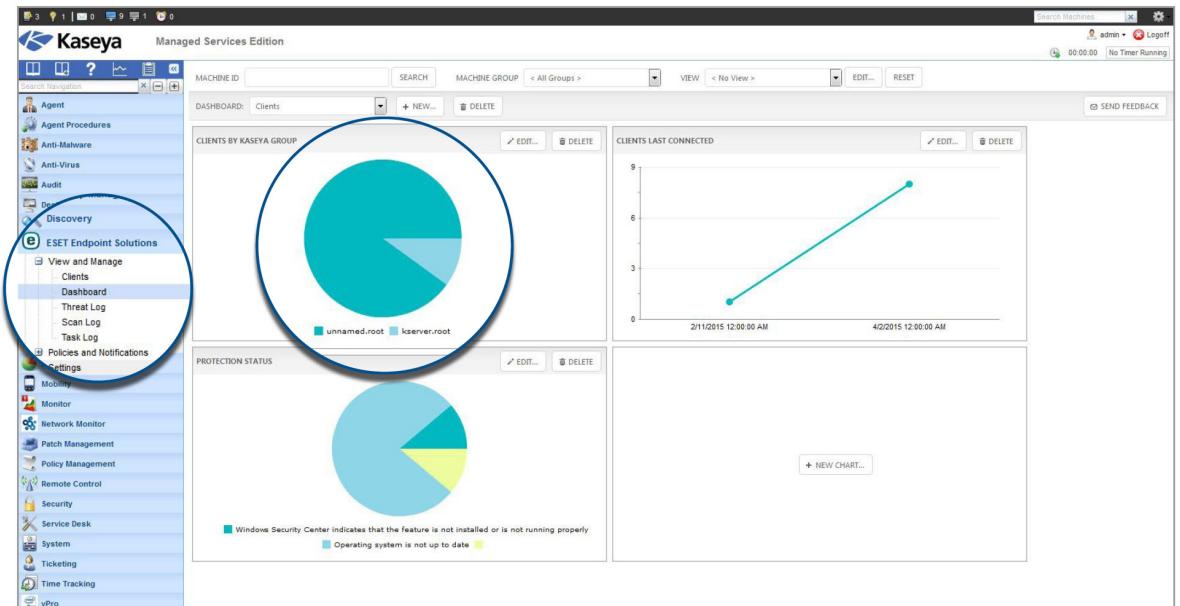
## Kaseya Virtual System Administrator 7.0 and newer\*\*

\*\*To review Kaseya Server system requirements, please visit Kaseya's website.

Easily manage ESET endpoints through familiar Kaseya console.



Customize your dashboard view to display threat data in easy to read graphs and charts.



© 1999-2017 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.