ESET REMOTE ADMINISTRATOR PLUG-IN FOR KASEYA

Technical Setup and User Guide

Click here to download the latest version of this document

ENJOY SAFER TECHNOLOGY™

ESET REMOTE ADMINISTRATOR PLUG-IN FOR KASEYA

ESET REMOTE ADMINISTRATOR Plug-in FOR KASEYA was developed by ESET, spol. s r.o.
For more information visit www.eset.com.

Customer Care Worldwide: www.eset.com/support

REV. 1/12/2016

1. Introduction

Thank you for using the ESET Remote Administrator (ERA) Plug-in for Kaseya. The ERA Plug-in for Kaseya is designed to allow an administrator to manage ESET endpoint products from within the Kaseya Virtual System Administrator. Version 2.2.0.0 of the ERA Plug-in for Kaseya offers the following functionalities:

- Deploy the latest versions of ESET endpoint products and ESET File Security for Microsoft Windows Server to Kaseya clients.
- Monitor clients, threats, scans, and tasks using a dashboard similar to ESET Remote Administrator.
- Run scans or updates and distribute configuration policy changes to ESET-protected endpoints.
- Create alarms, notification emails, Kaseya Agent procedures, and configurable triggers for ESET endpoint products.
- Generate detailed reports about the health of your environment using Kaseya Info Center.
- View global events using the audit log.

Enhancements and bug fixes in version 2.2.1.0:

- Enhancement: Removed forced reboot after running ESET Install/Uninstall deployment scripts
- Bug fix: Fixed an issue that caused certain IIS configurations to not correctly serve javascript associated with plug-in pages
- Bug fix: Fixed an issue where use of specific Kaseya role permission settings caused UI buttons not to display
- Bug fix: Fixed an issue where a single client with multiple network adapters could be displayed as a duplicate
- Bug fix: Fixed an issue where Install/Uninstall would not run with specific SQL Server configurations
- Bug fix: Fixed an issue where Install pop-up windows were not closed after clicking 'install'

Enhancements and bug fixes in version 2.2.0.0:

- Enhancement: Added support for ESET Remote Administrator 5.3
- Enhancement: 'Last Connected' field shows "Less than a minute ago" rather than the exact number of seconds
- Enhancement: Deployment description is now more accurate. "Autoselect...EEA/EES for Workstations" has been changed to "Autoselect EEA/EES for Workstations EFSW for Servers"
- Enhancement: Added the ability to install and uninstall ESET solutions directly from the plug-in
- Enhancement: Added the ability to assign policies to multiple machines or entire Kaseya machine groups
- Enhancement: Added the ability to create and modify ESET Remote Administrator 6 policies
- Enhancement: email and alert notifications can now be modified without the need to re-create the notification
- Enhancement: Plug-in permissions are now far more granular
- Bug fix: Client matching now displays the internal IP address instead of the connecting IP address
- Bug fix: Fixed an issue that could cause the plug-in to be unresponsive when refreshing data
- Bug fix: Fixed an issue that would cause errors if no clients were contained in the ESET Remote Administrator

Server

- Removed: Removed support for ESET Remote Administrator 5.2

2. Plug-in Installation Prerequisites

The ESET Remote Administrator Plug-in for Kaseya must be installed using the System Administrator account on your Kaseya Server (Kaseya VSA 7.0 and later are supported). The following versions of ESET Remote Administrator Server are supported:

ESET Remote Administrator Server 6.2 — Download ERA 6.2

ESET Remote Administrator Server 5.3 — Download ERA 5.3

Note: While the Plug-in must be installed directly on your Kaseya VSA server, ESET Remote Administrator may be installed on a separate server.

To review Kaseya Server system requirements, please visit the Kaseya home page.

3. Plug-in Installation

Note: During the installation process you will be prompted to reapply your Kaseya VSA schema, which will temporarily take your Kaseya server offline. This step is necessary and must be performed for the Plug-in to function correctly.

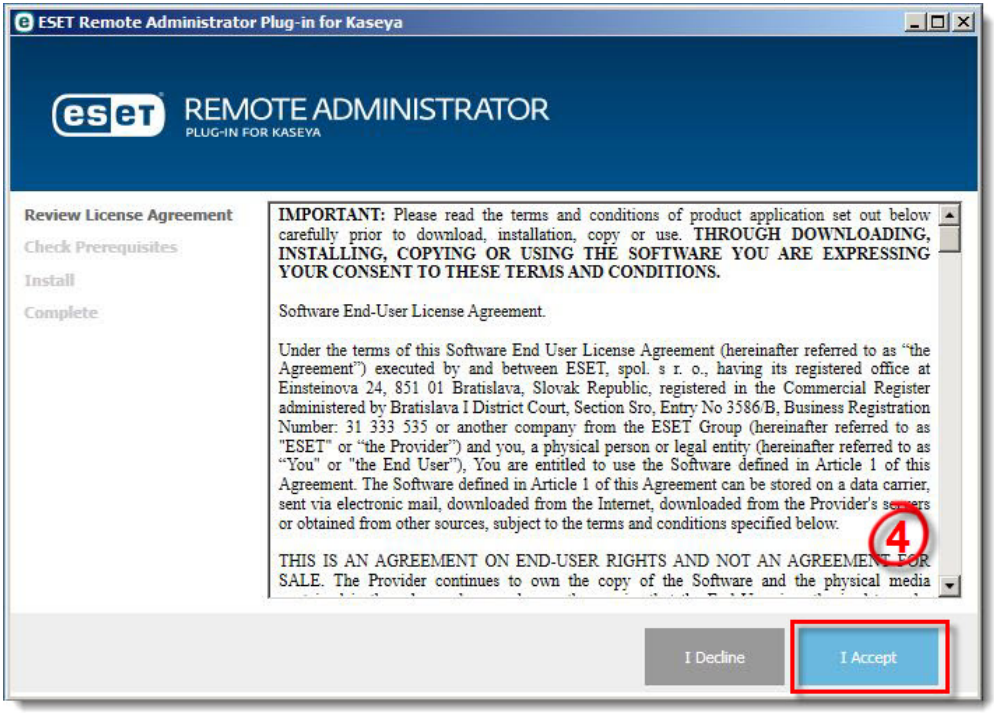
1. Log in to the server on which Kaseya is installed using the System Administrator account.

2. Click the following link to download the ESET Remote Administrator Plug-in for Kaseya installer file:http://download.eset.com/download/plugins/kaseya/eset_era_kaseya_plugin.exe

3. Double click the ESET Remote Administrator Plug-in for Kaseya setup file (.exe) to start the installation wizard.

Figure 1-1

4. Read the End-User License Agreement and click **I Accept** if you agree to the terms.



IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS.**

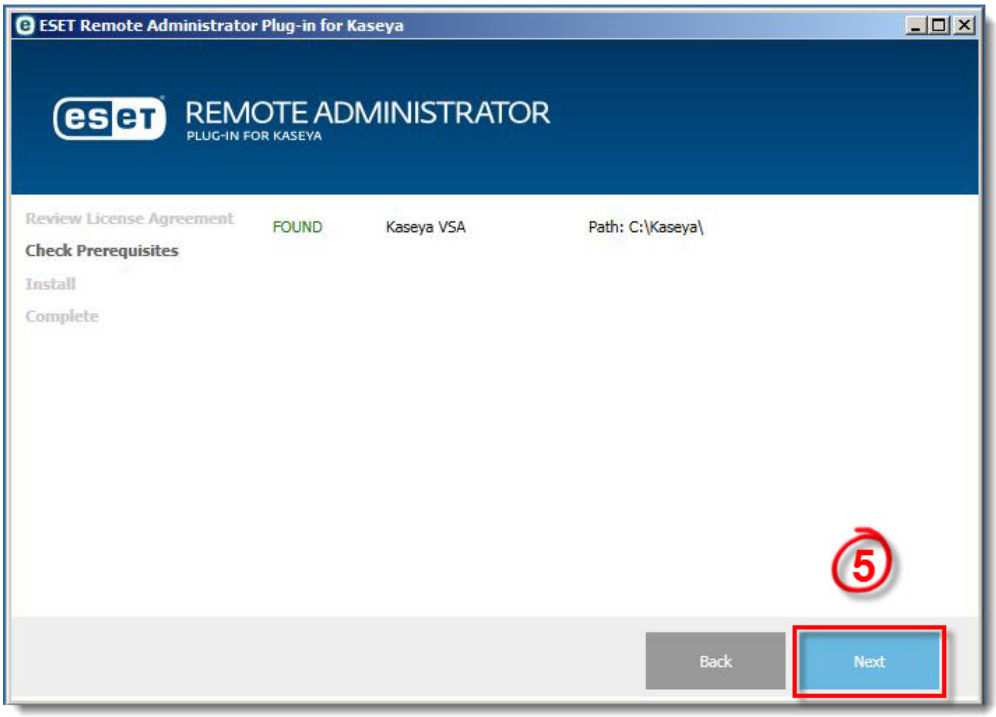
Software End-User License Agreement.

Under the terms of this Software End User License Agreement (hereinafter referred to as "the Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31 333 535 or another company from the ESET Group (hereinafter referred to as "ESET" or "the Provider") and you, a physical person or legal entity (hereinafter referred to as "You" or "the End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END-USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media

Figure 1-2

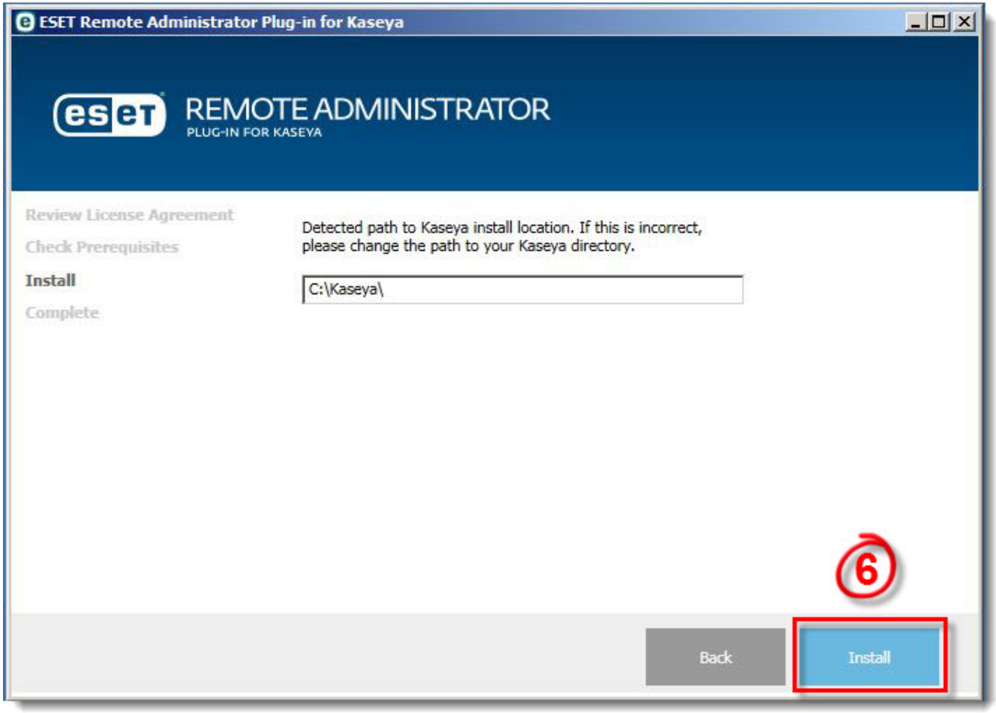
5. Click **Next** after the installer finishes checking for prerequisites.



FOUND Kaseya VSA Path: C:\Kaseya\

Figure 1-3

6. The directory where the ESET Remote Administrator Plug-in for Kaseya will be installed will be displayed. Make any desired changes to the install directory and then click **Install**.

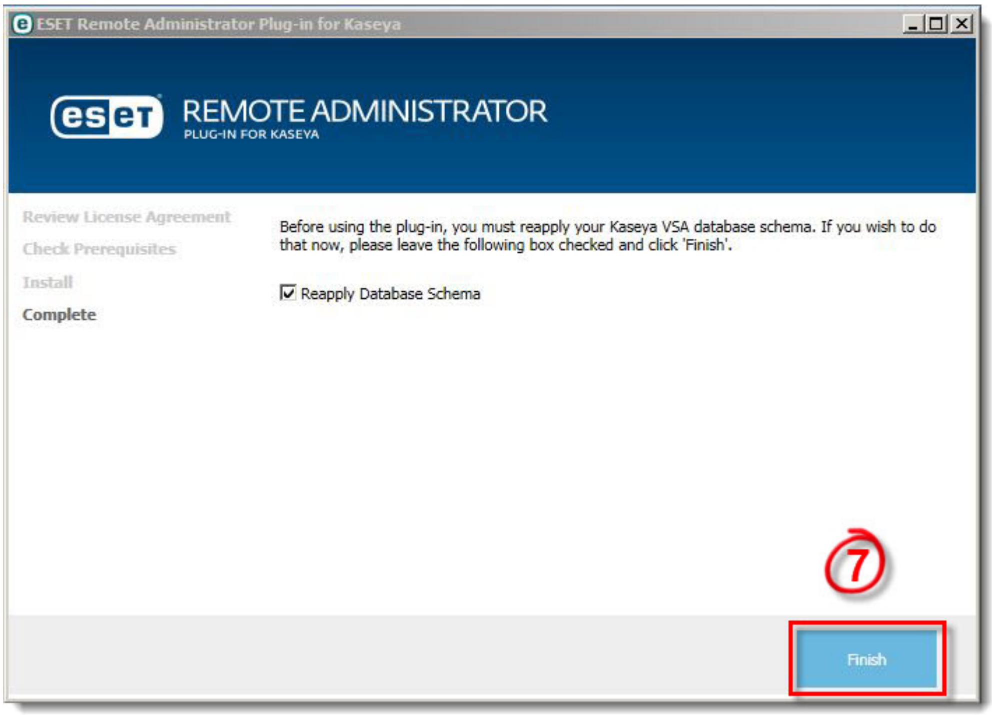


Detected path to Kaseya install location. If this is incorrect, please change the path to your Kaseya directory.

C:\Kaseya\

Figure 1-4

7. When installation is complete, click **Finish**. The installer will automatically reapply the database schema for your database.



Before using the plug-in, you must reapply your Kaseya VSA database schema. If you wish to do that now, please leave the following box checked and click 'Finish'.

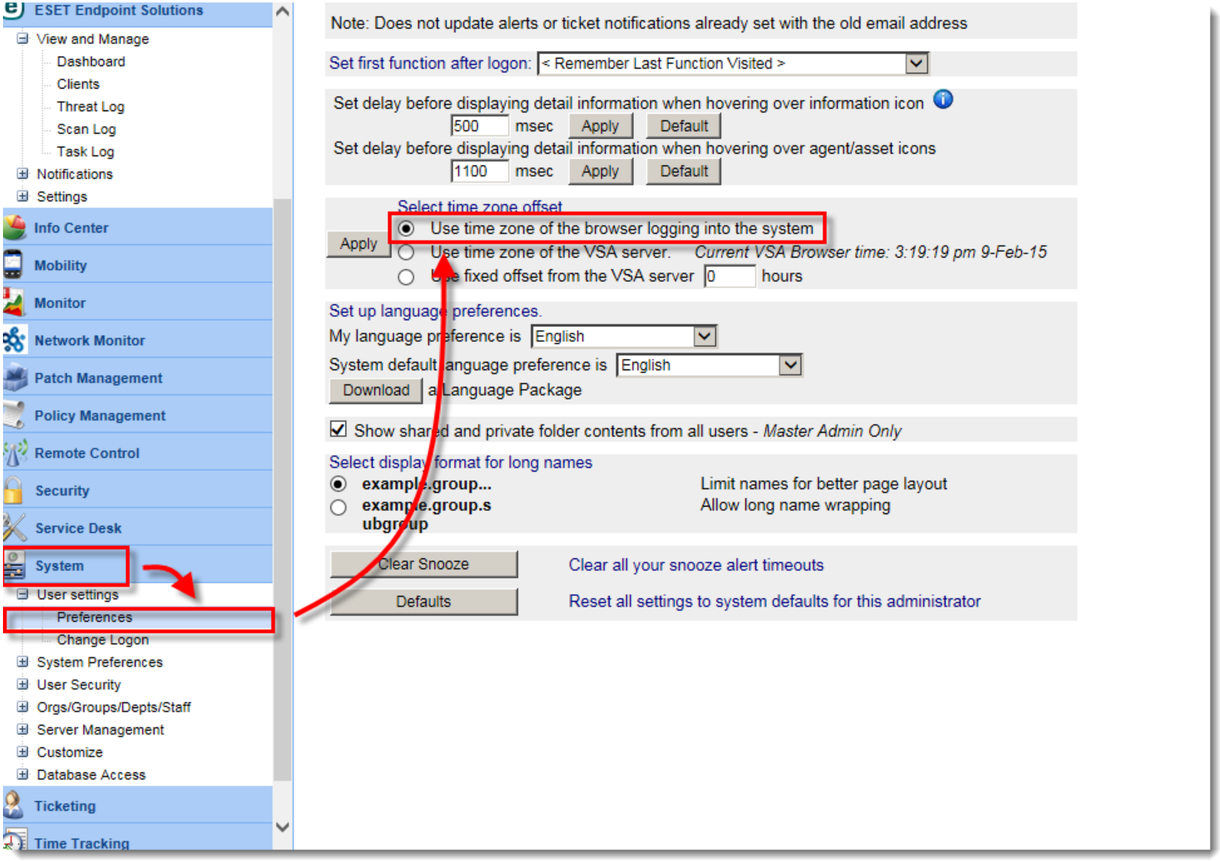
☑ Reapply Database Schema

Figure 1-5

4. Setup Wizard

After installation is complete, open Kaseya and click **Getting Started > Setup Wizard**. The Setup Wizard will help you configure the Plug-in to communicate with the ESET Remote Administrator Server.

Note: Before running the Setup Wizard, you can configure Kaseya to convert logging times to the time zone used by your web browser, rather than UTC. To do so, open Kaseya and navigate to **System > User Settings > Preferences** and select **Use time zone of the browser logging into the system**. Click **Apply** when you are finished.



Note: Does not update alerts or ticket notifications already set with the old email address

Set first function after logon: < Remember Last Function Visited >

Set delay before displaying detail information when hovering over information icon
500 msec Apply Default

Set delay before displaying detail information when hovering over agent/asset icons
1100 msec Apply Default

Select time zone offset
Apply
● Use time zone of the browser logging into the system
○ Use time zone of the VSA server. *Current VSA Browser time: 3:19:19 pm 9-Feb-15*
○ Use fixed offset from the VSA server 0 hours

Set up language preferences.
My language preference is English
System default language preference is English
Download a Language Package

☑ Show shared and private folder contents from all users - *Master Admin Only*

Select display format for long names
● **example.group...** Limit names for better page layout
○ **example.group.subgroup** Allow long name wrapping

Clear Snooze Clear all your snooze alert timeouts
Defaults Reset all settings to system defaults for this administrator

Figure 1-6

1. Expand **ESET Endpoint Solutions > Settings** and click **ERA Servers**.

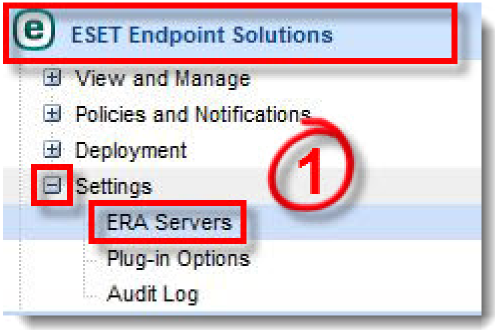
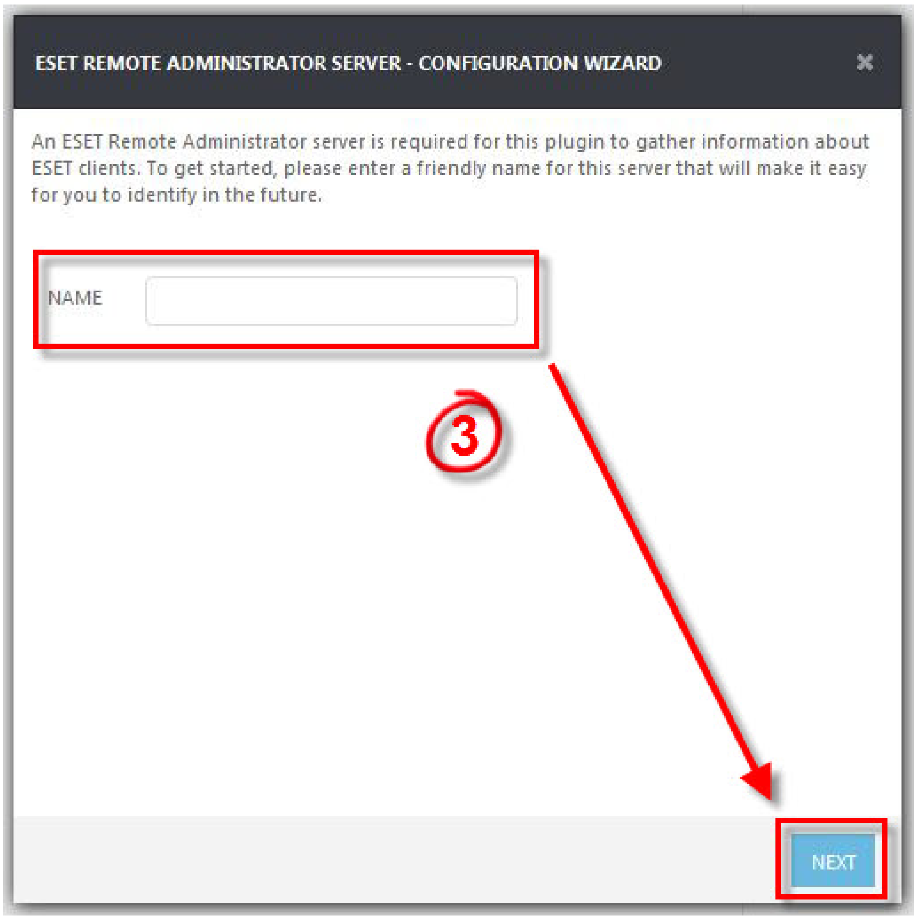


Figure 1-7

2. Click **New** to create a new server entry.

3. Type a name for your new server into the **Name** field and click **Next**.



ESET REMOTE ADMINISTRATOR SERVER - CONFIGURATION WIZARD

An ESET Remote Administrator server is required for this plugin to gather information about ESET clients. To get started, please enter a friendly name for this server that will make it easy for you to identify in the future.

NAME

Figure 1-8

4. Enter the following information using the corresponding fields in the Setup Wizard (see figure 1-9).

   a. A name for your ERA Server

   b. The version of ERA you will be connecting to

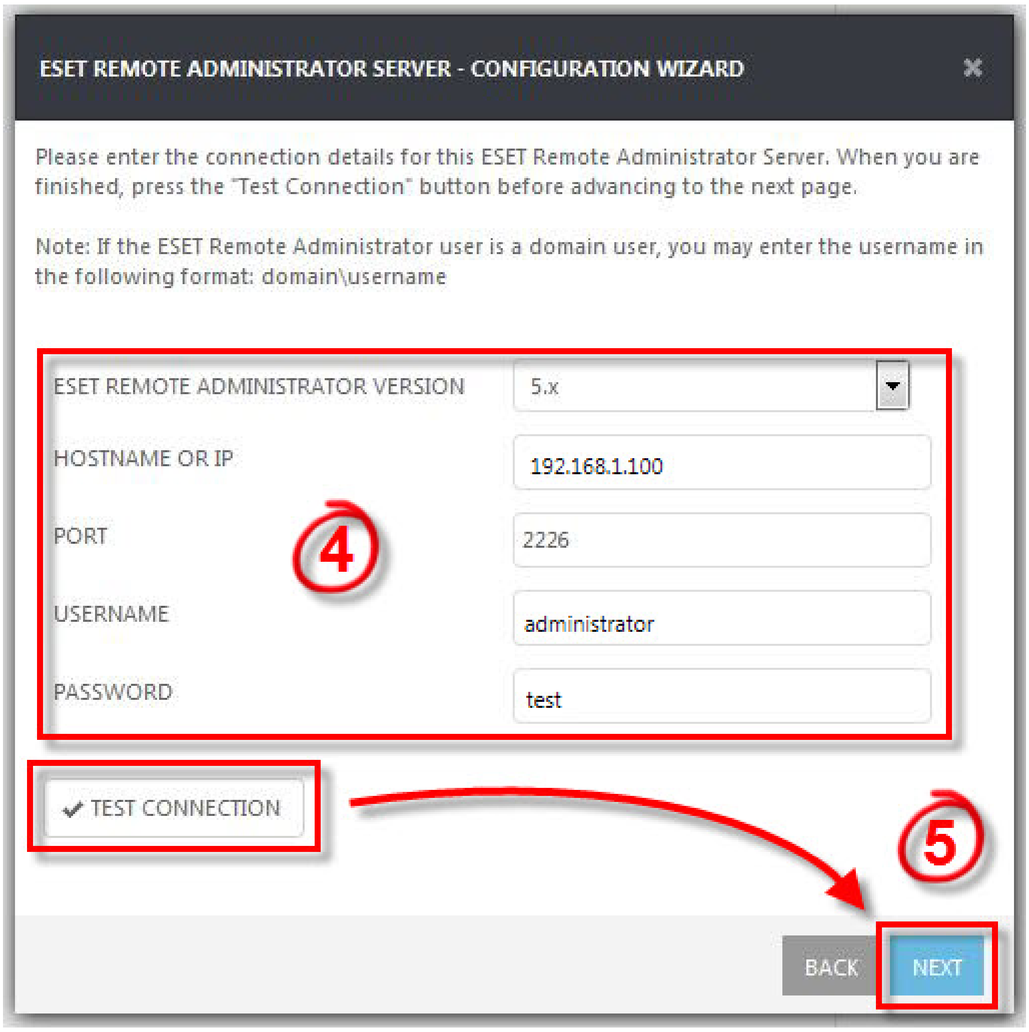
   c. The hostname or IP address of your ERA Server

   d. The port used to connect to ERA Server (port 2226 is the default value)

   e. Your ESET Remote Administrator (ERA) username (*Administrator* is the default value). Windows Domain is supported in the format (Domain\[admin user])

   f. Your ERA password (blank by default). This is the password that you have defined for the Administrator in ESET Remote Administrator.

5. Click **Test Connection** when you are finished making changes to verify that your settings are correct and then click **Next**.



ESET REMOTE ADMINISTRATOR SERVER - CONFIGURATION WIZARD

Please enter the connection details for this ESET Remote Administrator Server. When you are finished, press the "Test Connection" button before advancing to the next page.

Note: If the ESET Remote Administrator user is a domain user, you may enter the username in the following format: domain\username

ESET REMOTE ADMINISTRATOR VERSION: 5.x

HOSTNAME OR IP: 192.168.1.100

PORT: 2226

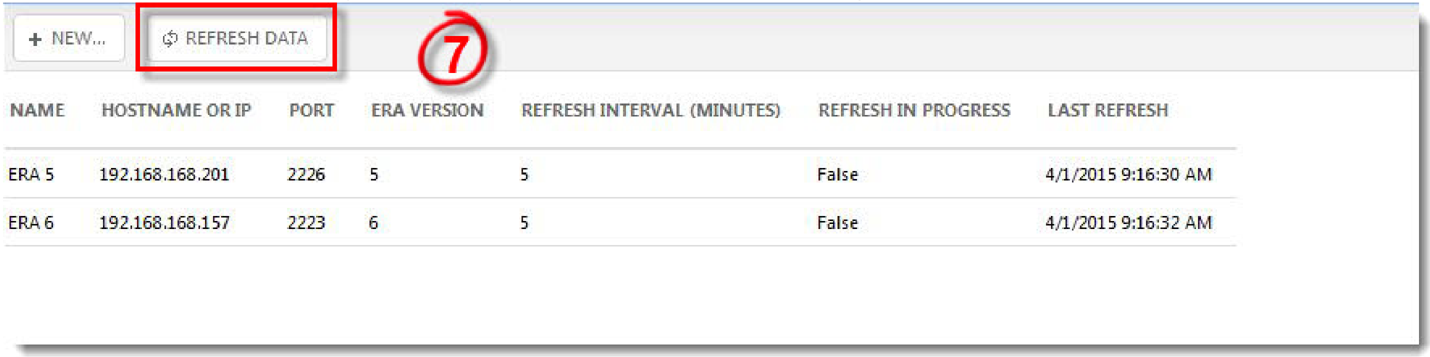
USERNAME: administrator

PASSWORD: test

Figure 1-9

6. If the connection is successful, you will be prompted to set the polling refresh rate. The default value is 5 minutes. Make your desired changes and then click **Finish**.

7. Your new server will be displayed in the ERA Server list. We recommend that you click **Refresh Data** to have your server connect to Kaseya immediately rather than at the next polling interval.



NAME	HOSTNAME OR IP	PORT	ERA VERSION	REFRESH INTERVAL (MINUTES)	REFRESH IN PROGRESS	LAST REFRESH
ERA 5	192.168.168.201	2226	5	5	False	4/1/2015 9:16:30 AM
ERA 6	192.168.168.157	2223	6	5	False	4/1/2015 9:16:32 AM

Figure 1-10

5. Manage ESET endpoint products

Information about all Kaseya endpoints is displayed under **View and Manage > Clients**. Each client will display information about the ESET product installed on that client and the last time that it checked into the ESET Remote Administrator Server. Select a client (or hold **CTRL** to select multiple clients) to view more detailed information about that client.

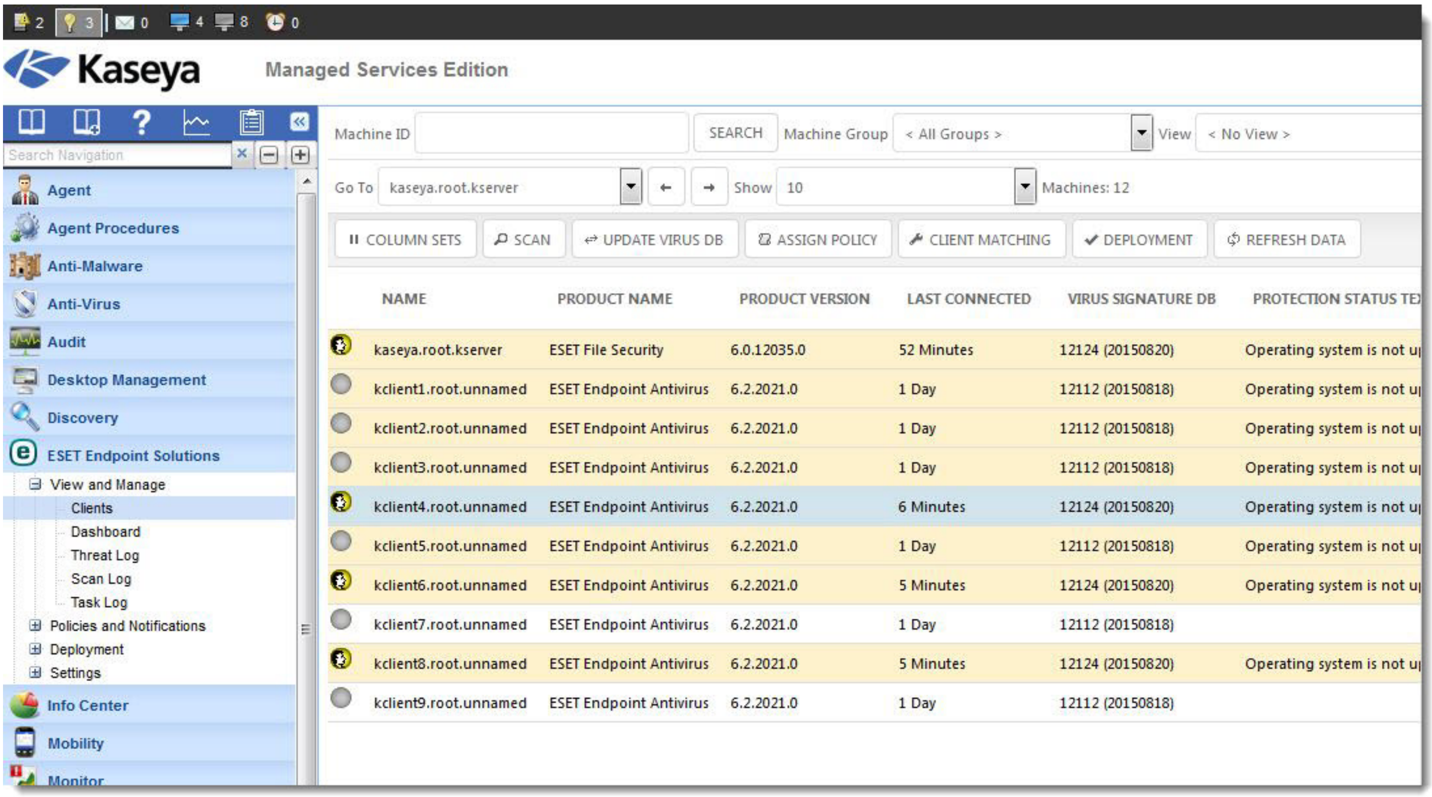
A. Initiate a client task

- Click **Scan Task** or **Update Task** to apply these tasks on your selected clients. You can assign policies to clients that are connected to ERA 5.2. To do so, click **Assign Policy**.

B. Sort and edit columns

- By default, clients that need attention or have a changed value in the **Protection Status Test** column, are displayed in orange. This usually relates to a functionality issue, such as an outdated operating system or virus signature database.

- Click **Column Sets** to edit the information categories displayed in this window. See Column Set Management for more details on this feature.



	NAME	PRODUCT NAME	PRODUCT VERSION	LAST CONNECTED	VIRUS SIGNATURE DB	PROTECTION STATUS TE
●	kaseya.root.kserver	ESET File Security	6.0.12035.0	52 Minutes	12124 (20150820)	Operating system is not u
○	kclient1.root.unnamed	ESET Endpoint Antivirus	6.2.2021.0	1 Day	12112 (20150818)	Operating system is not u
○	kclient2.root.unnamed	ESET Endpoint Antivirus	6.2.2021.0	1 Day	12112 (20150818)	Operating system is not u
○	kclient3.root.unnamed	ESET Endpoint Antivirus	6.2.2021.0	1 Day	12112 (20150818)	Operating system is not u
●	kclient4.root.unnamed	ESET Endpoint Antivirus	6.2.2021.0	6 Minutes	12124 (20150820)	Operating system is not u
○	kclient5.root.unnamed	ESET Endpoint Antivirus	6.2.2021.0	1 Day	12112 (20150818)	Operating system is not u
●	kclient6.root.unnamed	ESET Endpoint Antivirus	6.2.2021.0	5 Minutes	12124 (20150820)	Operating system is not u
○	kclient7.root.unnamed	ESET Endpoint Antivirus	6.2.2021.0	1 Day	12112 (20150818)	
●	kclient8.root.unnamed	ESET Endpoint Antivirus	6.2.2021.0	5 Minutes	12124 (20150820)	Operating system is not u
○	kclient9.root.unnamed	ESET Endpoint Antivirus	6.2.2021.0	1 Day	12112 (20150818)	

Figure 1-11

6. Policies

You can create and edit policies for Kaseya clients with ESET solutions installed. Navigate to **Policies and Notifications** > **Policies** to view policies that currently exist on your ESET Remote Administrator servers.

- Policy manager displays policies for version 5 ESET products in the policy tree.
- Policies for version 6 ESET products are sorted by priority (descending) and name (ascending).
- Policies for version 5 ESET products are created and modified using an XML file. Download and run ESET Configuration Editor on your local system to edit these policies.
- Policies for version 6 ESET products are created and modified from ESET Remote Administrator Web Console, which can be accessed using your web browser.
- Select a policy to see Kaseya machines or machine groups to which that policy is assigned.

Policy actions:

- **New**—Create a new policy for the specified ERA server. For ERA version 5 servers, the new policy will be created as a child of the currently selected policy or ERA server. Policies created for ERA version 6 servers all reside at the same tree level, since child policies are not used in this version.
- **Edit**—Opens the editor for the currently selected policy.
- **Delete**—ERA version 6 policies only. This button will delete the currently selected policy.
- **Assign Policy**—This button will open the policy assignment dialog for the currently selected policy. This feature allows you to assign policies to individual machines or groups.
- **Allow Assignment / Disallow Assignment**—Click this to allow the selected policy to be assigned directly to a machine via the Clients view. By default, policies must be explicitly "Allowed" before they will appear in the "Assign Policy" drop-down menu of the Clients view.
- **Export Configuration**—This button allows you to export settings for the currently selected policy. (.xml for ERA 5.x and .dat for ERA 6.x).

6.1 Create a policy for version 5.x ESET endpoint products

1. Navigate to **Policies and Notifications** > **Policies**, locate your ERA version 5 server and then select the node that you want to act as a parent of the policy you are creating.

2. Click **New**.

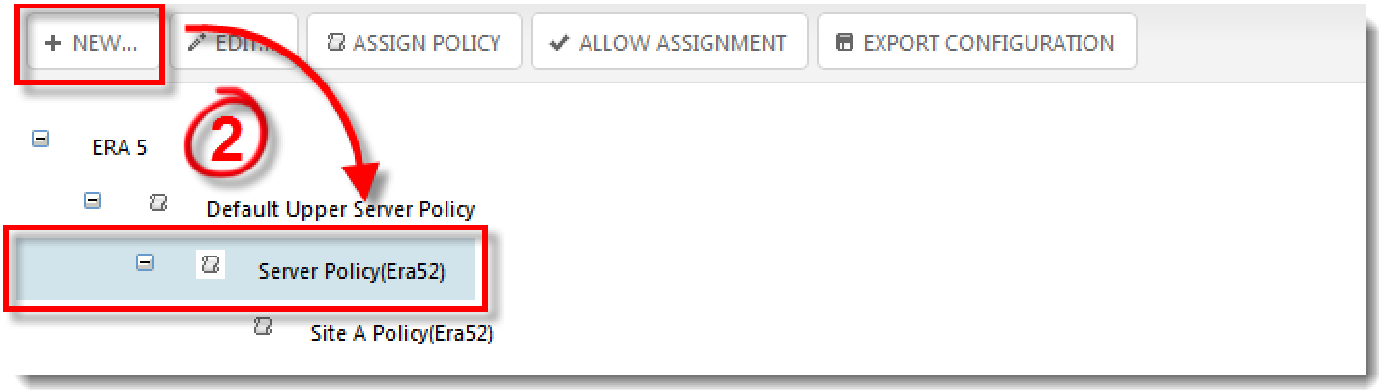
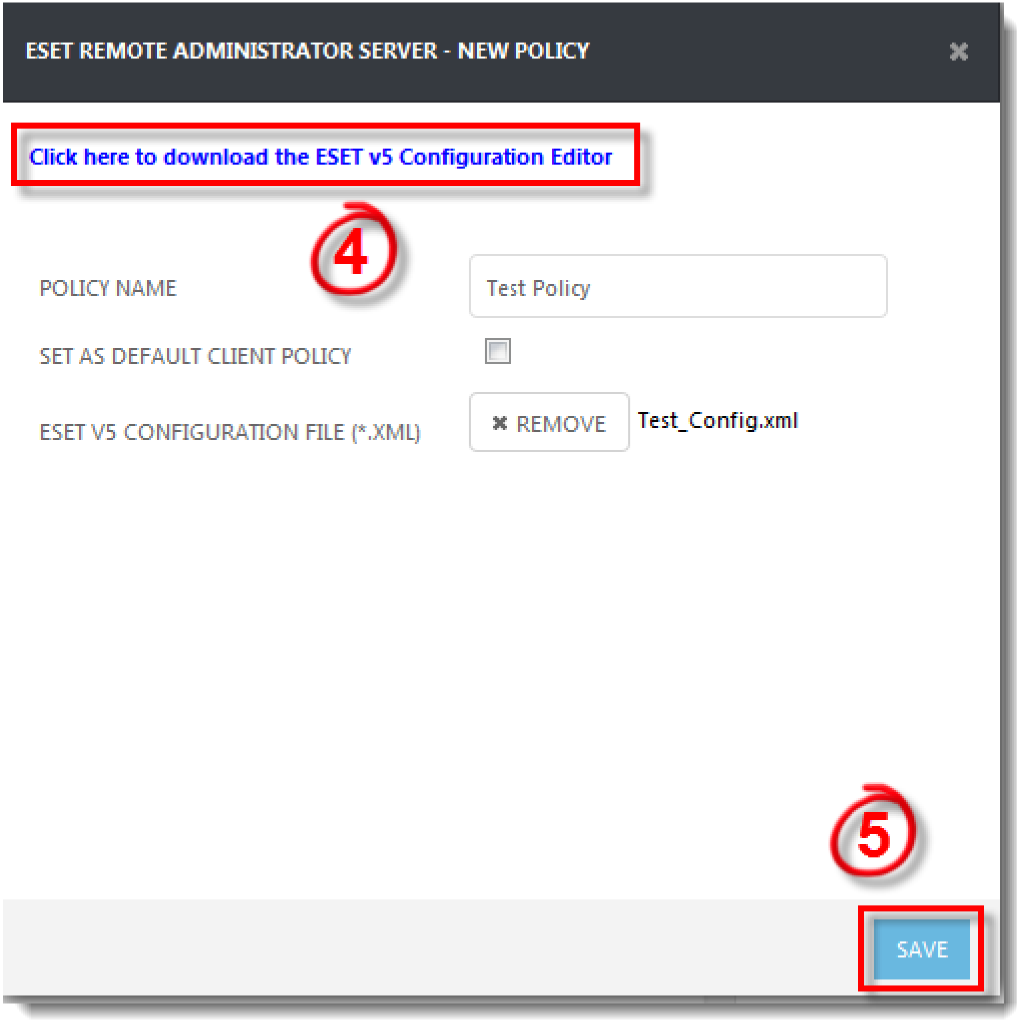


Figure 1-12

3. Type a name for the policy. If you have already created an XML file containing your policy settings, skip to step 7.

4. If you do not have this XML file, click the download link to download ESET Configuration Editor. When your download finishes, double-click the .exe file to open ESET Configuration Editor.

5. Use ESET Configuration Editor to create your desired policy. Click **Save** when you are finished and save the file.



ESET REMOTE ADMINISTRATOR SERVER - NEW POLICY

Click here to download the ESET v5 Configuration Editor

POLICY NAME: Test Policy

SET AS DEFAULT CLIENT POLICY: □

ESET V5 CONFIGURATION FILE (*.XML): ✖ REMOVE Test_Config.xml

Figure 1-13

6. Click **Browse**, navigate to your saved .xml configuration and then click **Open**.

7. Click **Save** to create the policy.

6.2 Create a policy for version 6.x ESET endpoint products

1. Under **Policies and Notifications** > **Policies**, locate your ERA 6.x server and select the parent node representing the server you would like to create the policy for.

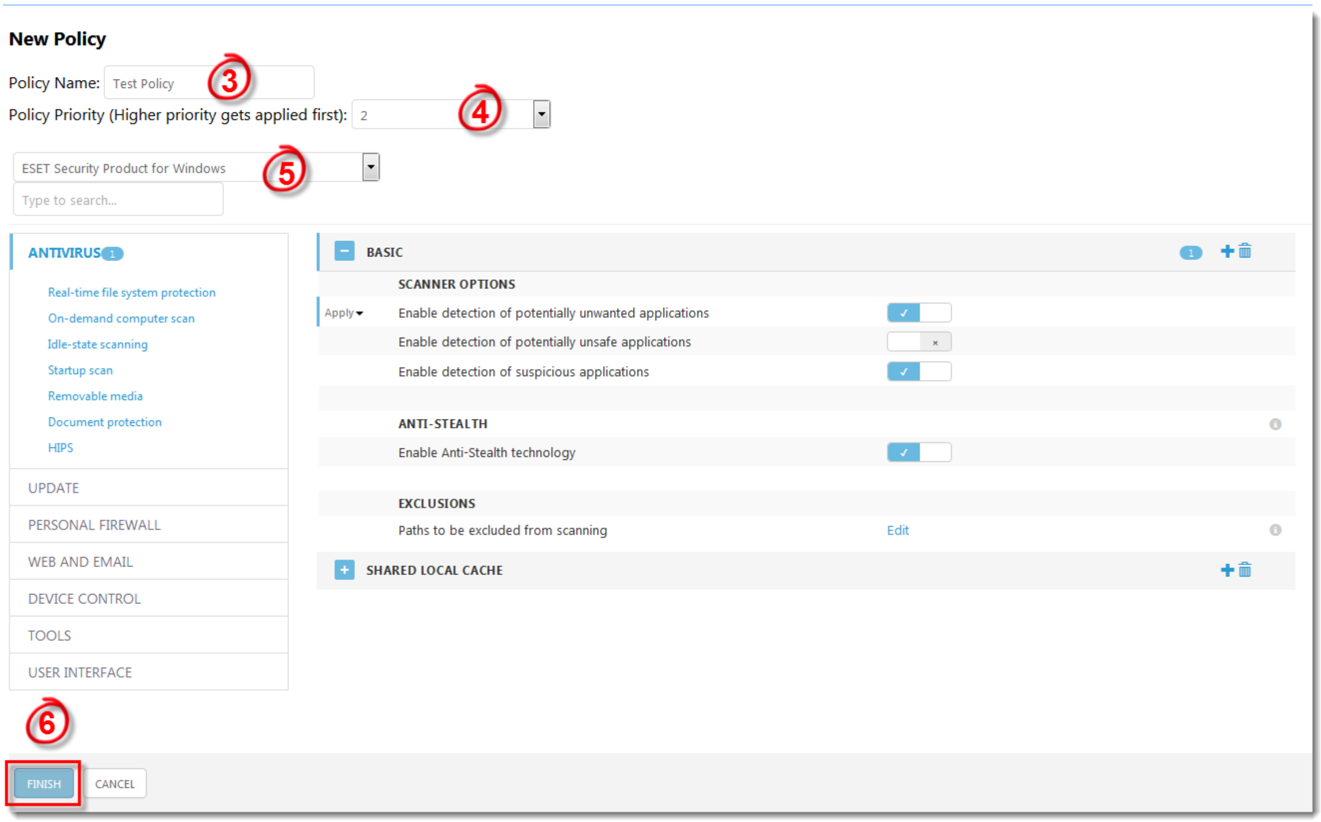
2. Click **New**.

3. Type a name for the policy.

4. Select the policy priority. This is important in the event that you have more than one conflicting policy assigned to the same machine. Policies are applied to the machine in the order of their priority values.

5. Select the ESET product that you want the policy to apply to from the drop-down menu.

6. Make changes that you want to apply to client computers using the policy settings tree.



New Policy

Policy Name: Test Policy

Policy Priority (Higher priority gets applied first): 2

ESET Security Product for Windows

Type to search...

ANTIVIRUS 1
- Real-time file system protection
- On-demand computer scan
- Idle-state scanning
- Startup scan
- Removable media
- Document protection
- HIPS

UPDATE

PERSONAL FIREWALL

WEB AND EMAIL

DEVICE CONTROL

TOOLS

USER INTERFACE

BASIC

SCANNER OPTIONS

Apply	Enable detection of potentially unwanted applications	✓
	Enable detection of potentially unsafe applications	×
	Enable detection of suspicious applications	✓

ANTI-STEALTH

Enable Anti-Stealth technology	✓

EXCLUSIONS

Paths to be excluded from scanning	Edit

SHARED LOCAL CACHE

Figure 1-14

7. Click **Finish** when you are finished making changes.

6.3 Policy assignment

A new feature of the ESET Remote Administrator Plug-in for Kaseya is the ability to assign a policy to an entire group of machines at once.

For ERA 5.x clients, each machine is only able to adopt a single policy. Policies inherit settings from their parent nodes.The policy applied to 5.x clients is dictated by the following:

- If the machine has multiple policies assigned by group and no policies applied directly to the machine, the machine will adopt the policy most recently assigned to its group
- If the machine has any policies applied directly, it will adopt the most recent policy it was assigned to.

For ERA 6.x clients, multiple policies can be applied to a single client. The policies applied to each v6 client is dictated by the following:

- Policies that are applied to a machine group in order of priority
- Policies that are applied directly to a specific machine in order of priority

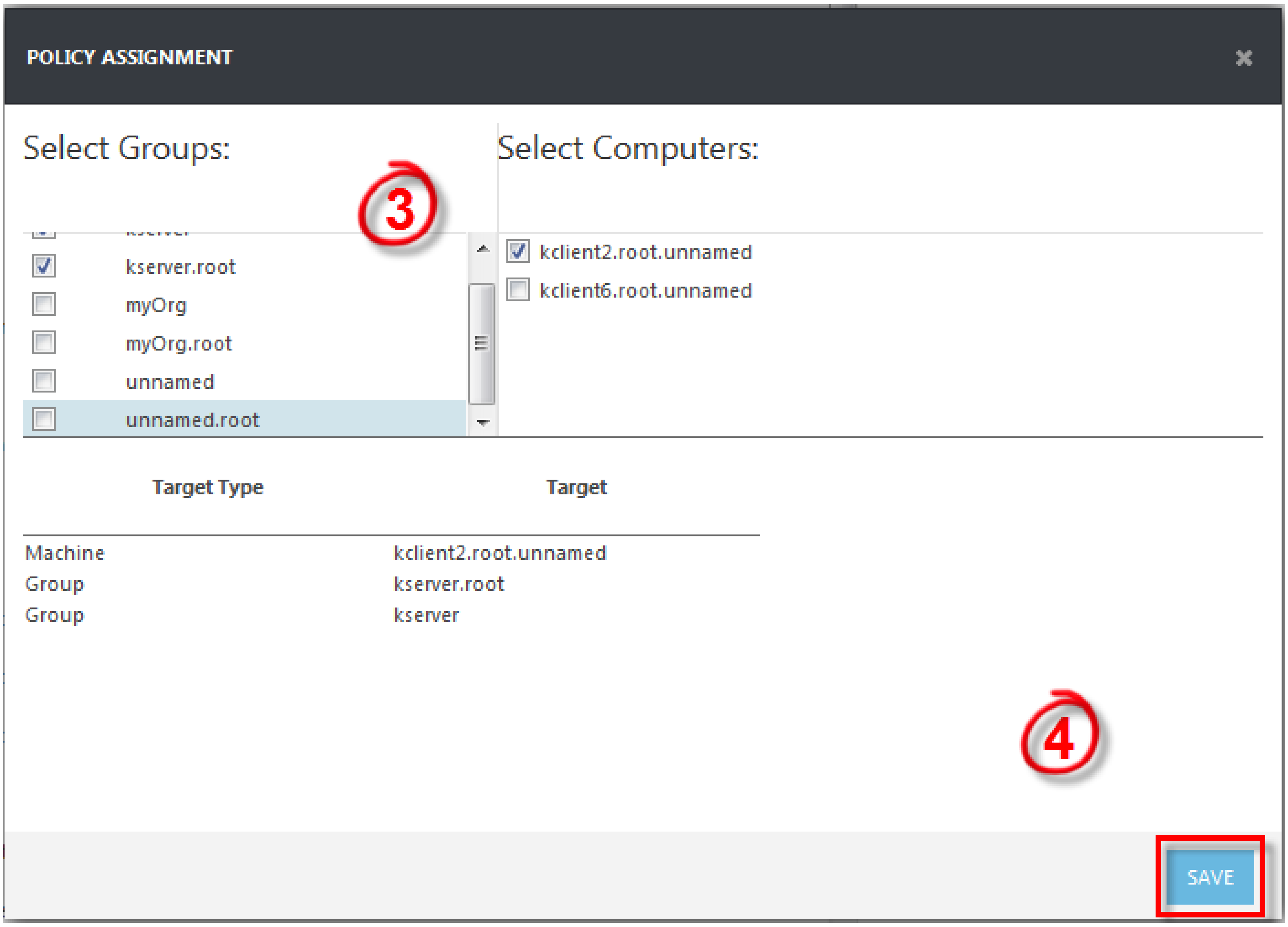
To assign a policy to a machine group or specific machine

1. Navigate to **Policies and Notifications** > **Policies**.

2. Select the policy you want to assign and click **Assign Policy**.

3. Select the check box next to the name of a machine group to assign the current policy to that group. When you select the name of the group, a list of clients in the group that can accept this policy will be displayed. Select the check box next to the name of a client to assign the policy to that specific client. All groups and clients assigned to a policy will be displayed at the bottom of the **Policy Assignment** window.

4. Click **Save** when you are satisfied with your assignments.



POLICY ASSIGNMENT

Select Groups:

- ☑ kserver.root
- ☐ myOrg
- ☐ myOrg.root
- ☐ unnamed
- ☐ unnamed.root

Select Computers:

- ☑ kclient2.root.unnamed
- ☐ kclient6.root.unnamed

Target Type	Target
Machine	kclient2.root.unnamed
Group	kserver.root
Group	kserver

Figure 1-15

7. Deploy ESET products

Navigate to **Deployment** > **Packages** to create install packages that will be run as agent procedures on the machine. This feature is currently only available for Windows ESET products. During the execution of the deployment package, it will download the latest version of the selected ESET software and configure it to connect to the specified ESET Remote Administrator server to allow management using the plug-in.

7.1 Create version 5.x ESET product packages

1. Navigate to **Deployment** > **Packages**.

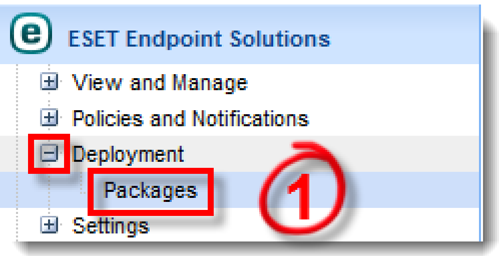


Figure 1-16

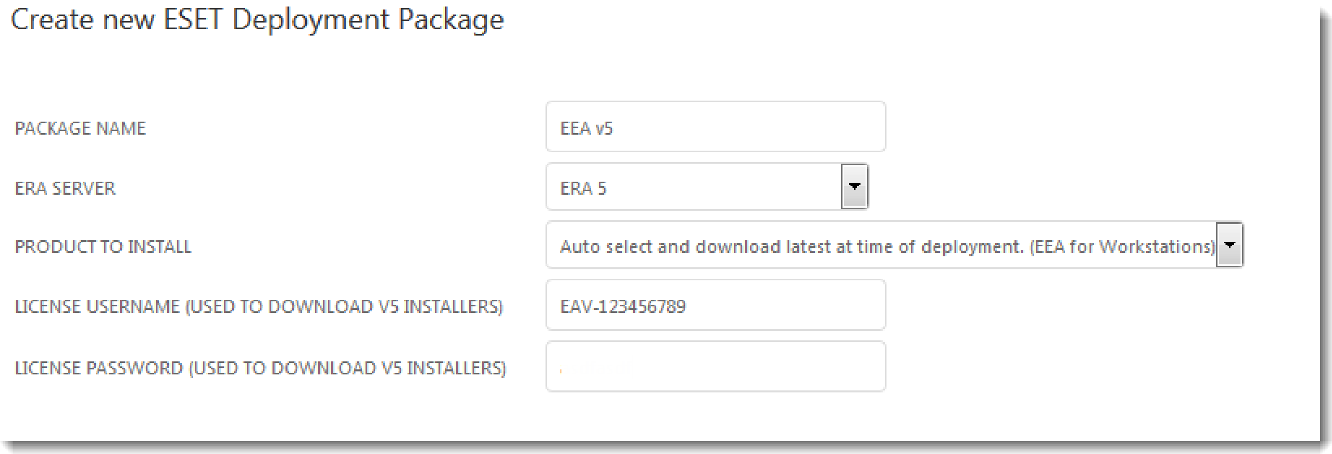
2. Click **New**.

3. Type a name for your new deployment package and select your ERA 5.x server from the drop-down menu.

4. Select the product that you would like to install:
   a. *"Auto select and download latest at time of deployment (EEA for Workstations)"* will deploy ESET Endpoint Antivirus to workstations and ESET File Security for Windows Server to servers.
   b. *"Auto select and download latest at time of deployment (EES for Workstations)"* will deploy ESET Endpoint Security to workstations and ESET File Security for Windows Server to servers.

5. Enter your ESET-issued Username and Password (for example, EAV-123456789).

6. Click **Save**.



Create new ESET Deployment Package

PACKAGE NAME	EEA v5
ERA SERVER	ERA 5
PRODUCT TO INSTALL	Auto select and download latest at time of deployment. (EEA for Workstations)
LICENSE USERNAME (USED TO DOWNLOAD V5 INSTALLERS)	EAV-123456789
LICENSE PASSWORD (USED TO DOWNLOAD V5 INSTALLERS)	

Figure 1-17

7.2 Create version 6.x ESET product packages

1. Navigate to **Deployment** > **Packages**.

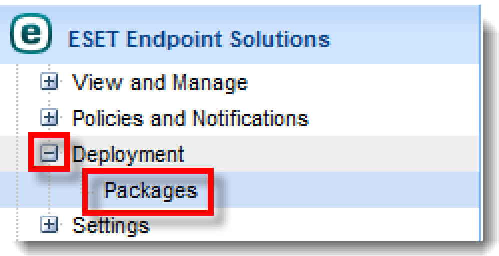


Figure 1-18

2. Click **New**.

3. Type a name for your new deployment package and select your ERA 6.x server from the drop-down menu.

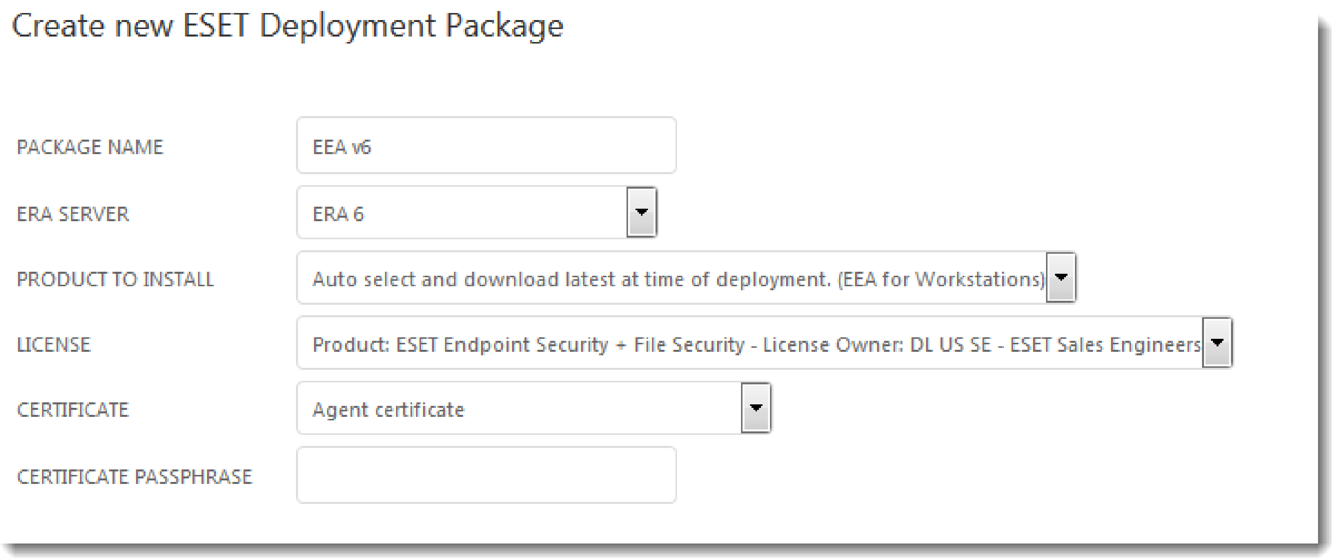
4. Select the product that you would like to install:
   a. *"Auto select and download latest at time of deployment (EEA for Workstations)"* will deploy ESET Endpoint Antivirus to workstations and ESET File Security for Windows Servers to servers.
   b. *"Auto select and download latest at time of deployment (EES for Workstations)"* will deploy ESET Endpoint Security to workstations and ESET File Security for Windows Server to servers.

5. Choose your desired license from the drop-down menu.

6. Choose your desired agent certificate from the drop-down menu.

7. If applicable, enter your certificate passphrase.

8. Click **Save**.



Create new ESET Deployment Package

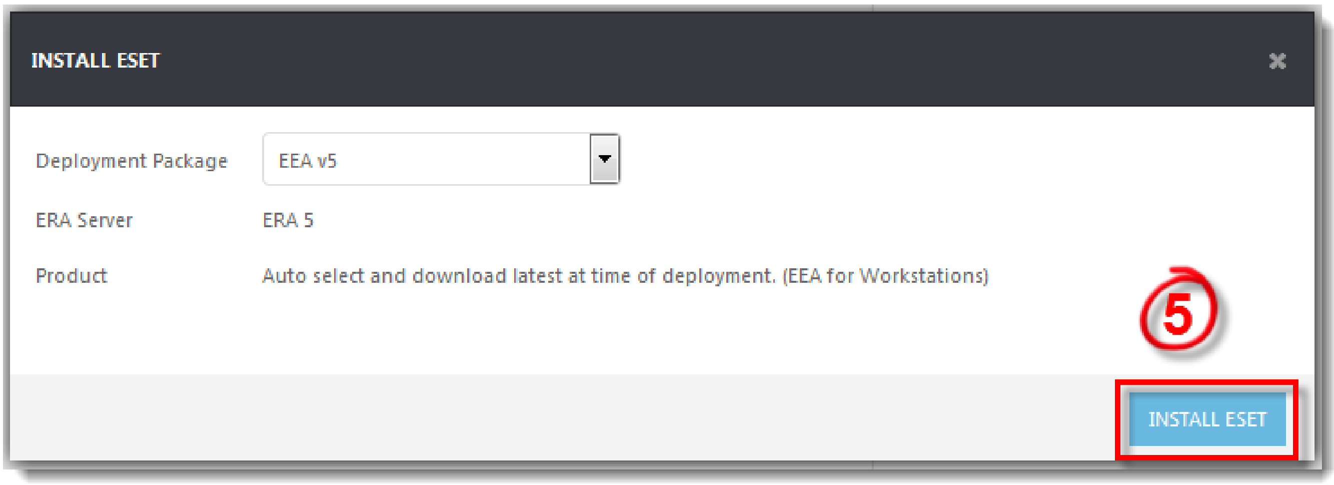
PACKAGE NAME	EEA v6
ERA SERVER	ERA 6
PRODUCT TO INSTALL	Auto select and download latest at time of deployment. (EEA for Workstations)
LICENSE	Product: ESET Endpoint Security + File Security - License Owner: DL US SE - ESET Sales Engineers
CERTIFICATE	Agent certificate
CERTIFICATE PASSPHRASE	

Figure 1-19

7.3 Deploy packages

ESET packages are deployed to machines under **View and Manage** > **Clients**.

1. Navigate to **View and Manage** > **Clients**.
2. Select the client or clients you want to deploy to and click **Deployment**.
3. Click **Install ESET**.
4. Choose the desired deployment package from the drop-down menu.
5. Click **Install ESET**. The next time the Kaseya agent connects, the deployment package will be sent to the machine to run. Upon execution, the installer will download the latest ESET product version from the website and install it. Once installation completes, the user will be prompted to reboot.



Deployment Package: EEA v5

ERA Server: ERA 5

Product: Auto select and download latest at time of deployment. (EEA for Workstations)

Figure 1-20

__Uninstalling ESET from the Plug-in__

1. Navigate to **View and Manage** > **Clients**.
2. Select the client or clients you want to deploy to and click **Deployment**.
3. Click **Uninstall ESET**.
4. If your ESET installation is password-protected, enter the settings password.
5. Click **Uninstall ESET.** Clients with ESET products installed will be prompted to reboot to complete the uninstall. In ERA 6.x, clients that you deploy an uninstall command to will automatically be removed. In ERA 5.x, you will need to remove these clients manually (select them and press **Delete** on your keyboard).

8. Generate a Report

You can export a report from the ESET Remote Administrator Plug-in for Kaseya to view various data about client systems. To do so, you must define a report template, which you can then use to preview and create a report once it is ready.

Create a new report template

1. Expand **Info Center > Configure and Design** and click **Report Templates**.

2. Select a folder where you want to store your new report template or click **Add Folder** to create a new folder.

3. Select your new folder and click **Add** to create a new report template.

4. Specify a report title and name for the template and then click **Next**.

5. You can add different report parts to your new report template in the **Layout** tab. To do so, expand the **ESET** folder and then click and drag any of the available report parts into the layout window on the right.

Preview and save a report

1. Once you have defined a new report template, expand **Info Center > Configure and Design > Report Templates**, open the folder where you saved your report template and click **Preview** to view the report. Click **OK** if a warning message is displayed.

2. Specify the data filters you want to use when previewing the report and click **Next**.

3. A window will open to display the new report. Click **Save** to export a copy of the report.

9. Permissions

You can define permissions within the ESET Remote Administrator Plug-in for Kaseya for different Virtual System Administrator (VSA) Admin roles. We recommend that you only allow access to Plug-in settings to trusted Kaseya VSA Admins. Navigate to **System > User Security > User Roles**.

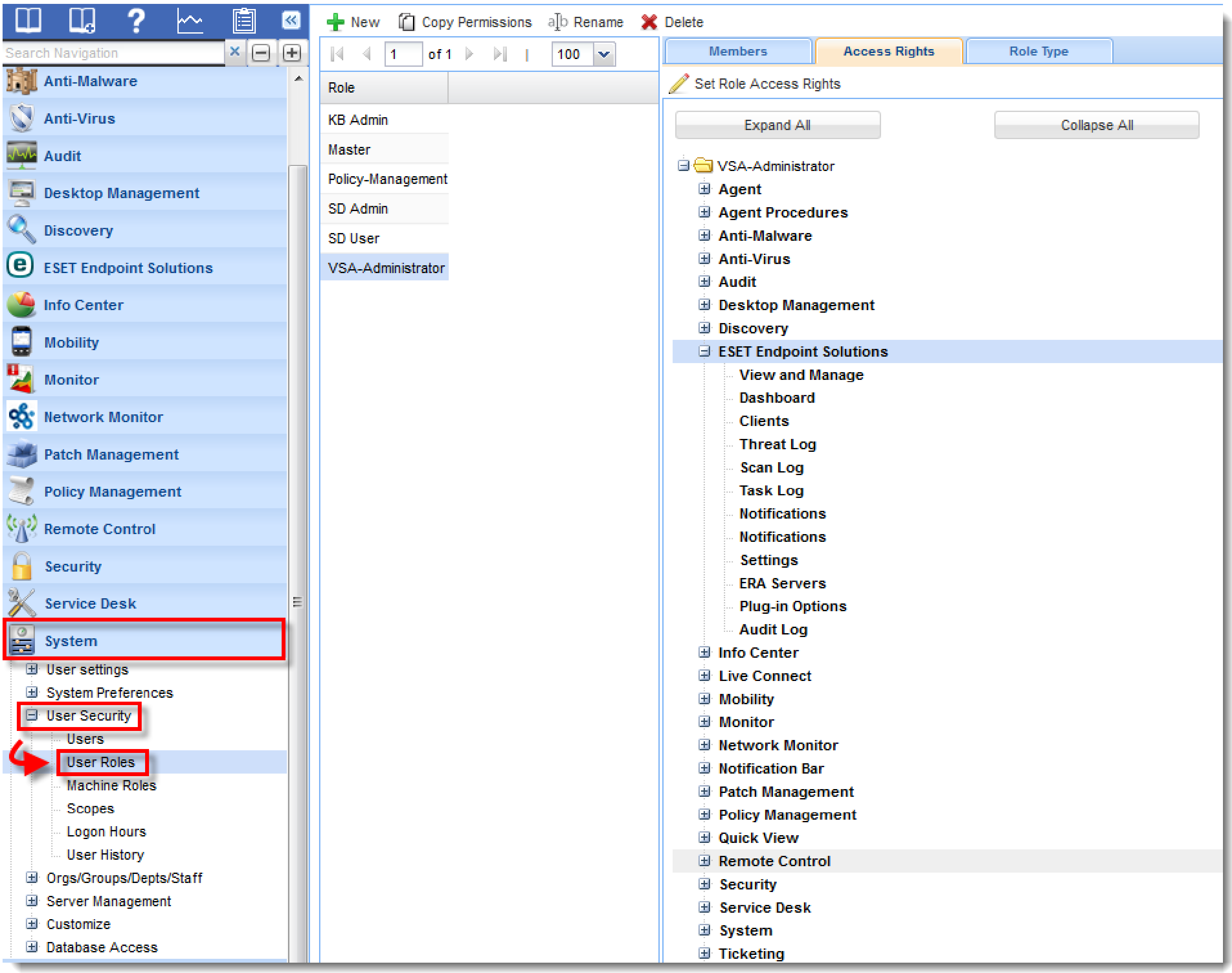


Figure 1-21

10. Column Set Management

Using the column set manager, you can define the information displayed in different windows within the Plug-in. You can define multiple column sets, each with unique data sets arranged in the order that the administrator would like them to appear.

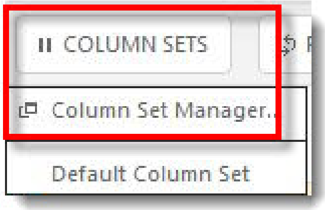


Figure 1-22

1. Click **Column Sets** in any Plug-in window and then click **Column Set Manager** to specify column sets for that window.

2. Click **Save** when you are finished making changes.

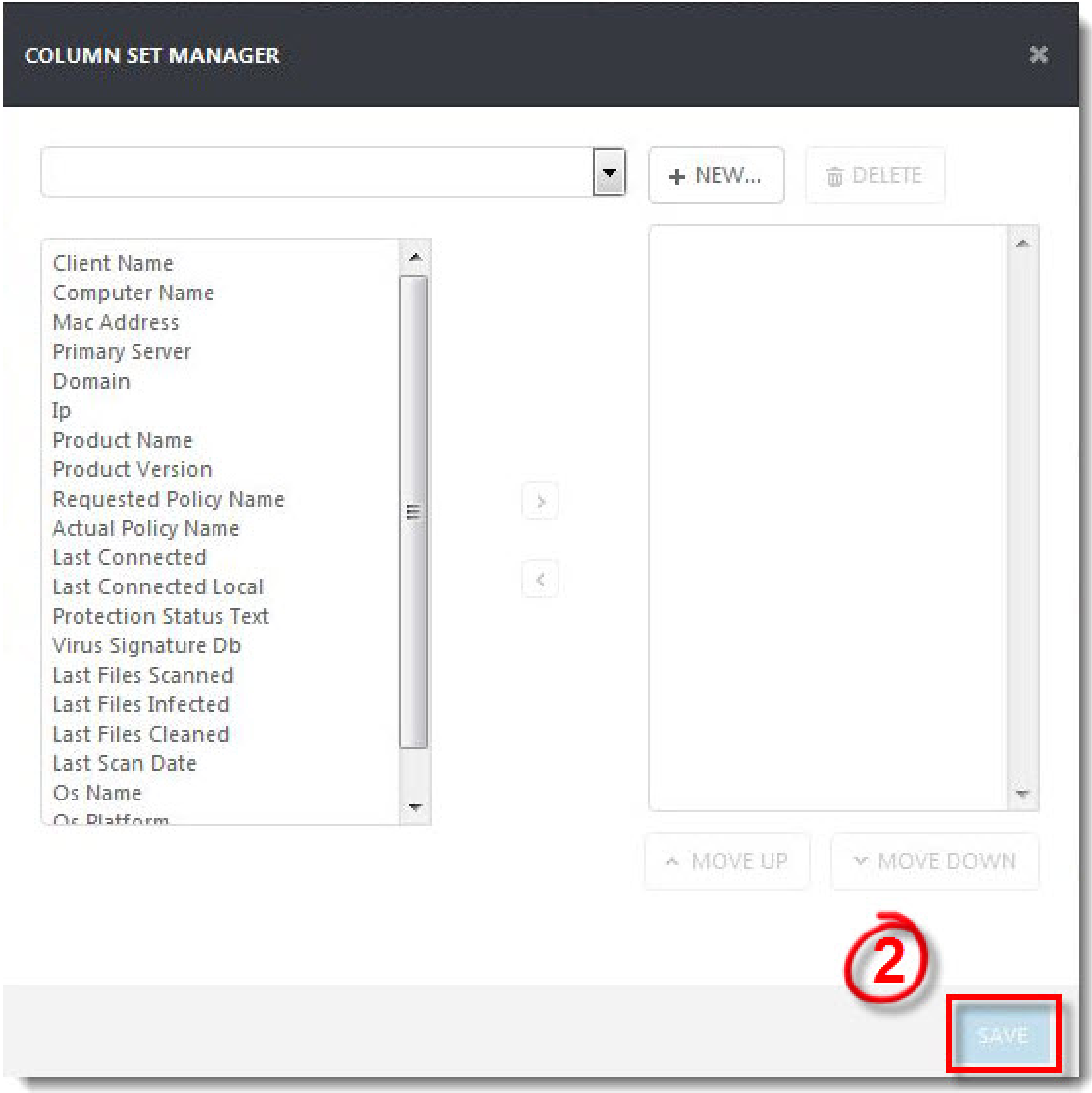


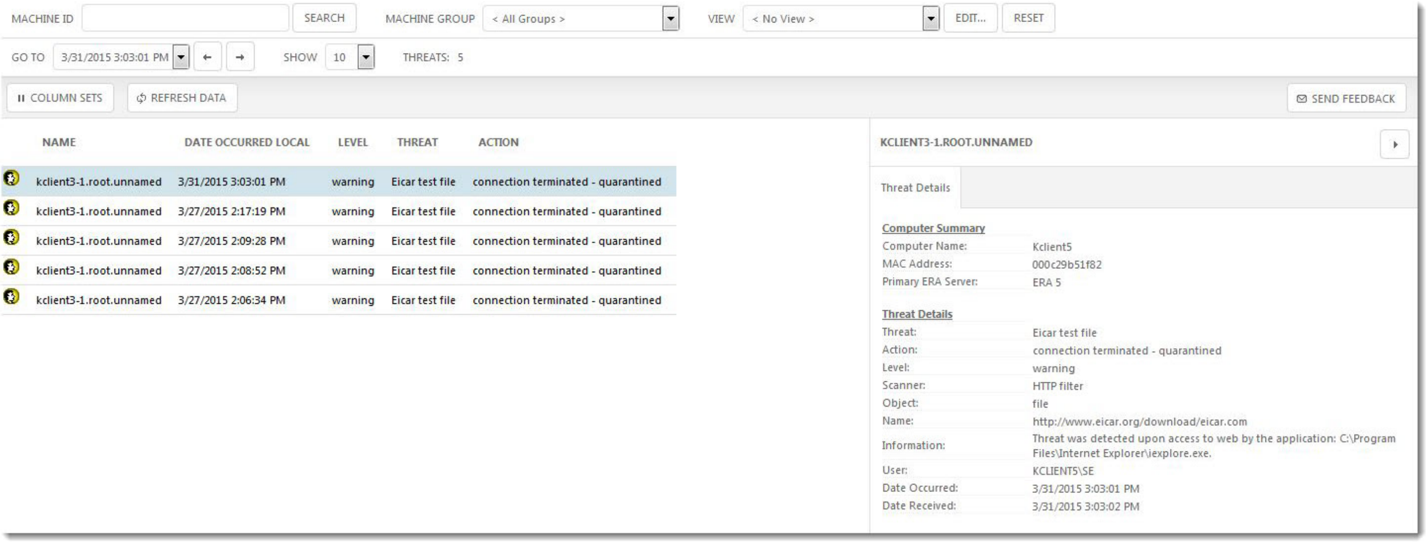
Figure 1-23

11. Threats

To view threat history for your environment, select **View and Manage > Threat Log**. The threat menu option lists detailed information about threats. For each client workstation the following information is available:

- Detected threats
- Time of detection
- Name of the threat
- Any actions taken.

You can use **Column Sets** and **Filter** to customize your view.



NAME	DATE OCCURRED LOCAL	LEVEL	THREAT	ACTION
kclient3-1.root.unnamed	3/31/2015 3:03:01 PM	warning	Eicar test file	connection terminated - quarantined
kclient3-1.root.unnamed	3/27/2015 2:17:19 PM	warning	Eicar test file	connection terminated - quarantined
kclient3-1.root.unnamed	3/27/2015 2:09:28 PM	warning	Eicar test file	connection terminated - quarantined
kclient3-1.root.unnamed	3/27/2015 2:08:52 PM	warning	Eicar test file	connection terminated - quarantined
kclient3-1.root.unnamed	3/27/2015 2:06:34 PM	warning	Eicar test file	connection terminated - quarantined

KCLIENT3-1.ROOT.UNNAMED

Threat Details

Computer Summary

Computer Name:	Kclient5
MAC Address:	000c29b51f82
Primary ERA Server:	ERA 5

Threat Details

Threat:	Eicar test file
Action:	connection terminated - quarantined
Level:	warning
Scanner:	HTTP filter
Object:	file
Name:	http://www.eicar.org/download/eicar.com
Information:	Threat was detected upon access to web by the application: C:\Program Files\Internet Explorer\iexplore.exe.
User:	KCLIENT5\SE
Date Occurred:	3/31/2015 3:03:01 PM
Date Received:	3/31/2015 3:03:02 PM

Figure 1-24

12. Dashboards

A Dashboard is a set of reports that are automatically updated with new data to give a comprehensive overview of your endpoints. You can have up to four configurable charts per dashboard page. Click **New** to add a new dashboard.

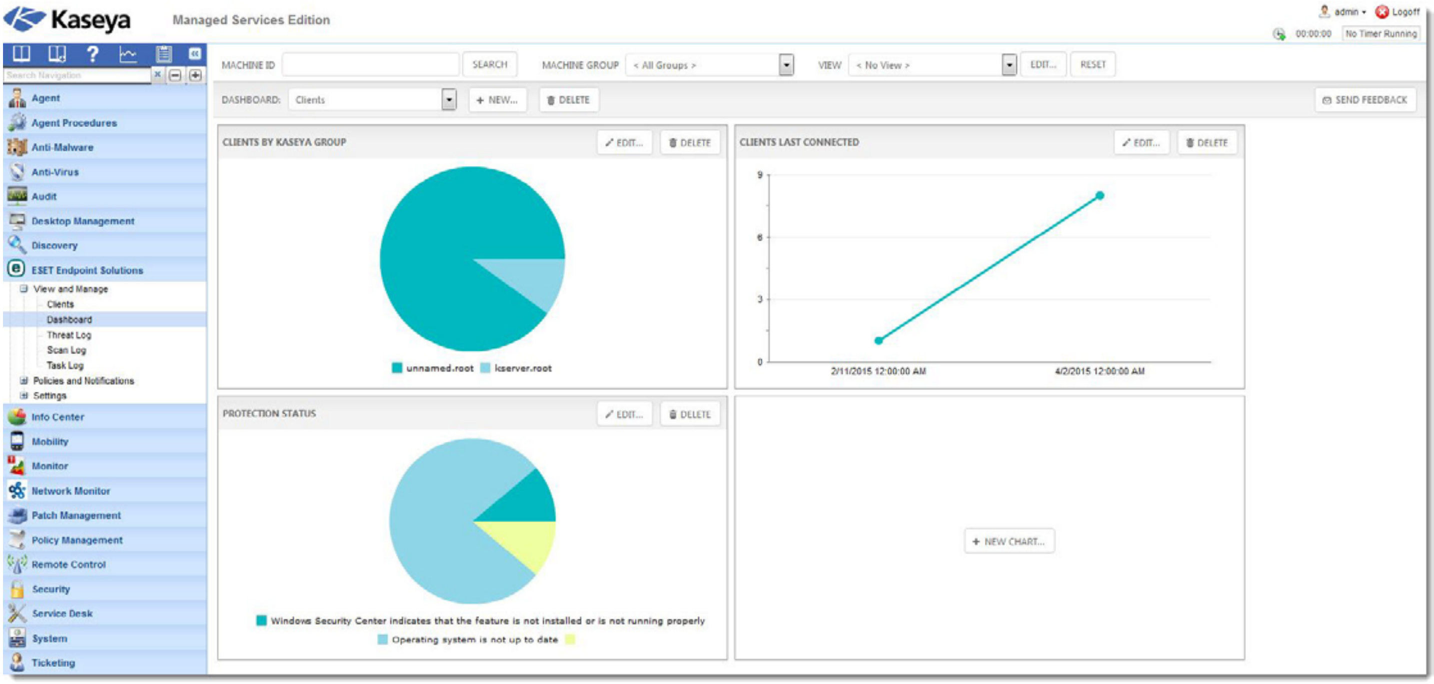
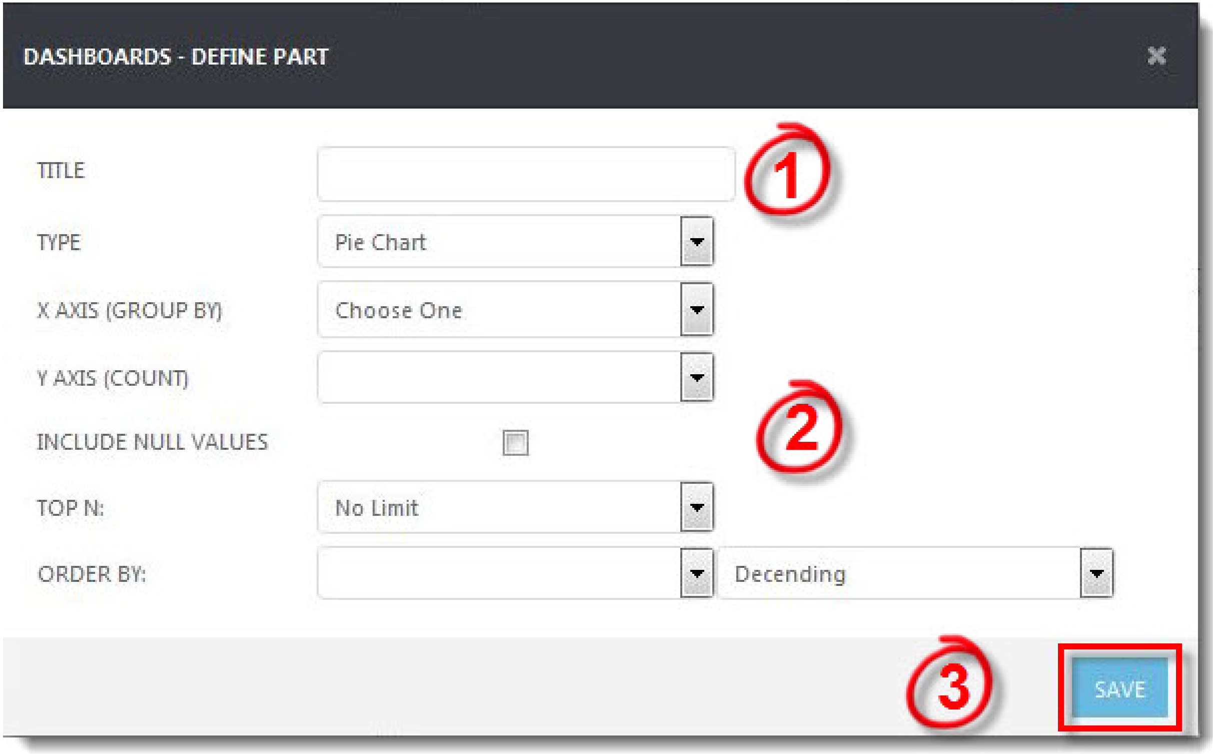


Figure 1-25

Add a new chart to your Dashboard

1. Click **New Chart** to add an individual chart to a dashboard.
2. Give your new chart a title and select your preferences for the chart parameters.
3. Click **Save** when you are finished making changes.

See Appendix A for a list of commonly used dashboard charts with configuration settings.



DASHBOARDS - DEFINE PART

TITLE

TYPE: Pie Chart

X AXIS (GROUP BY): Choose One

Y AXIS (COUNT)

INCLUDE NULL VALUES ☐

TOP N: No Limit

ORDER BY: Decending

SAVE

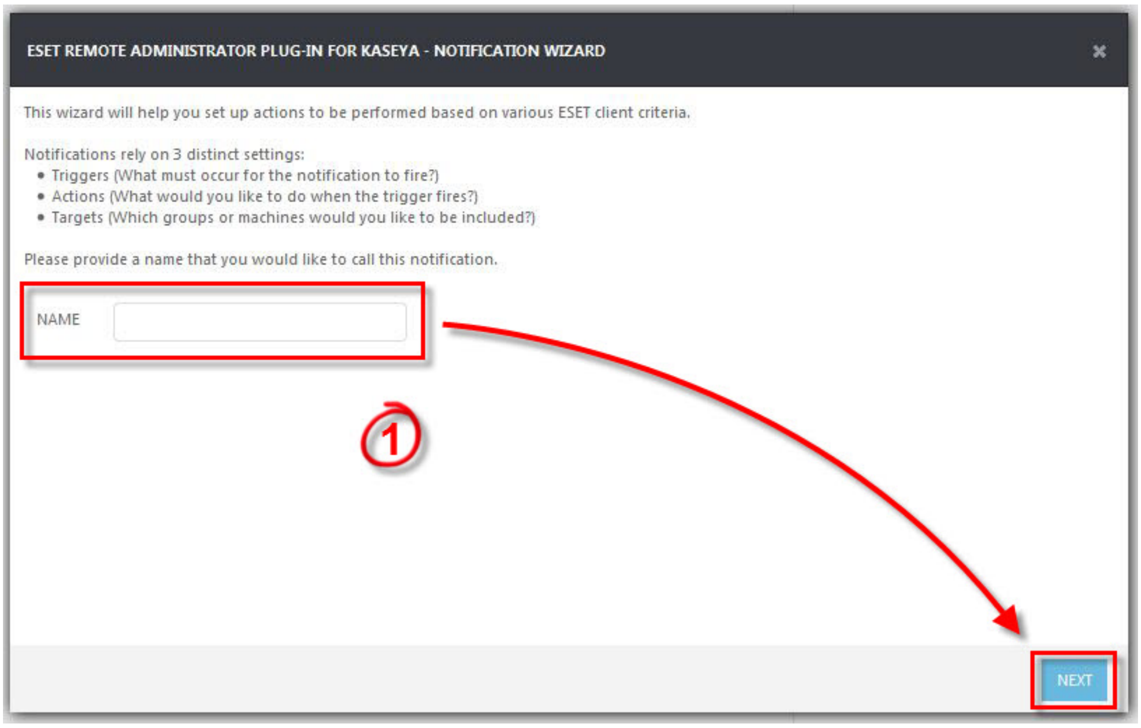
Figure 1-26

13. Notifications

Using Alerts, a systems administrator can configure email notifications that are automatically sent out when an endpoint has failed to update in a given period of time, is not communicating with the server, or there are other issues.

Create a new Notification

1. Click **Notifications > Notifications > New**, type a name for your new notification and an optional description, and then click **Next**.



ESET REMOTE ADMINISTRATOR PLUG-IN FOR KASEYA - NOTIFICATION WIZARD

This wizard will help you set up actions to be performed based on various ESET client criteria.

Notifications rely on 3 distinct settings:

- Triggers (What must occur for the notification to fire?)
- Actions (What would you like to do when the trigger fires?)
- Targets (Which groups or machines would you like to be included?)

Please provide a name that you would like to call this notification.

NAME

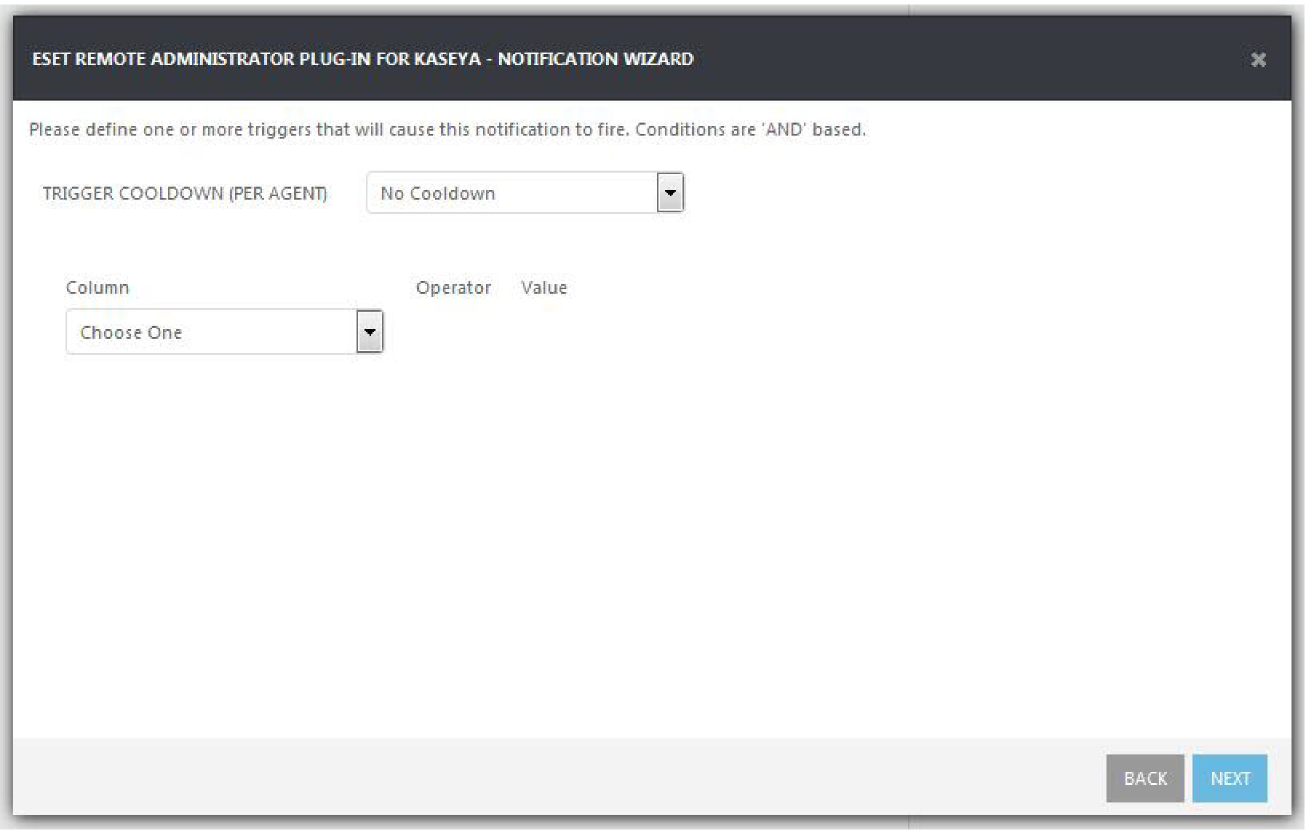
Figure 1-27

2. You can configure alert triggers and the cool down period required between alerts. After you create an alert and define its trigger, you can assign actions that correspond to that alert in the **Alert actions** tab. Click **Create alarm**, **email recipients**, or **run agent procedure** to automatically execute these actions when an alert is triggered. Information about alerts will be recorded automatically in the **Monitor** tab under **Status > Alarm Summary**. For a list of sample notifications and settings to configure them, see Appendix B.

Note:

- When creating a new notification you can specify multiple **AND** conditions, all of which will be evaluated when the notification is triggered

- To create a wildcard, leave blank the **Value** field that follows the **Like** or **Not Like** operator



ESET REMOTE ADMINISTRATOR PLUG-IN FOR KASEYA - NOTIFICATION WIZARD

Please define one or more triggers that will cause this notification to fire. Conditions are 'AND' based.

TRIGGER COOLDOWN (PER AGENT): No Cooldown

Figure 1-28

14. Technical Config. and Troubleshooting

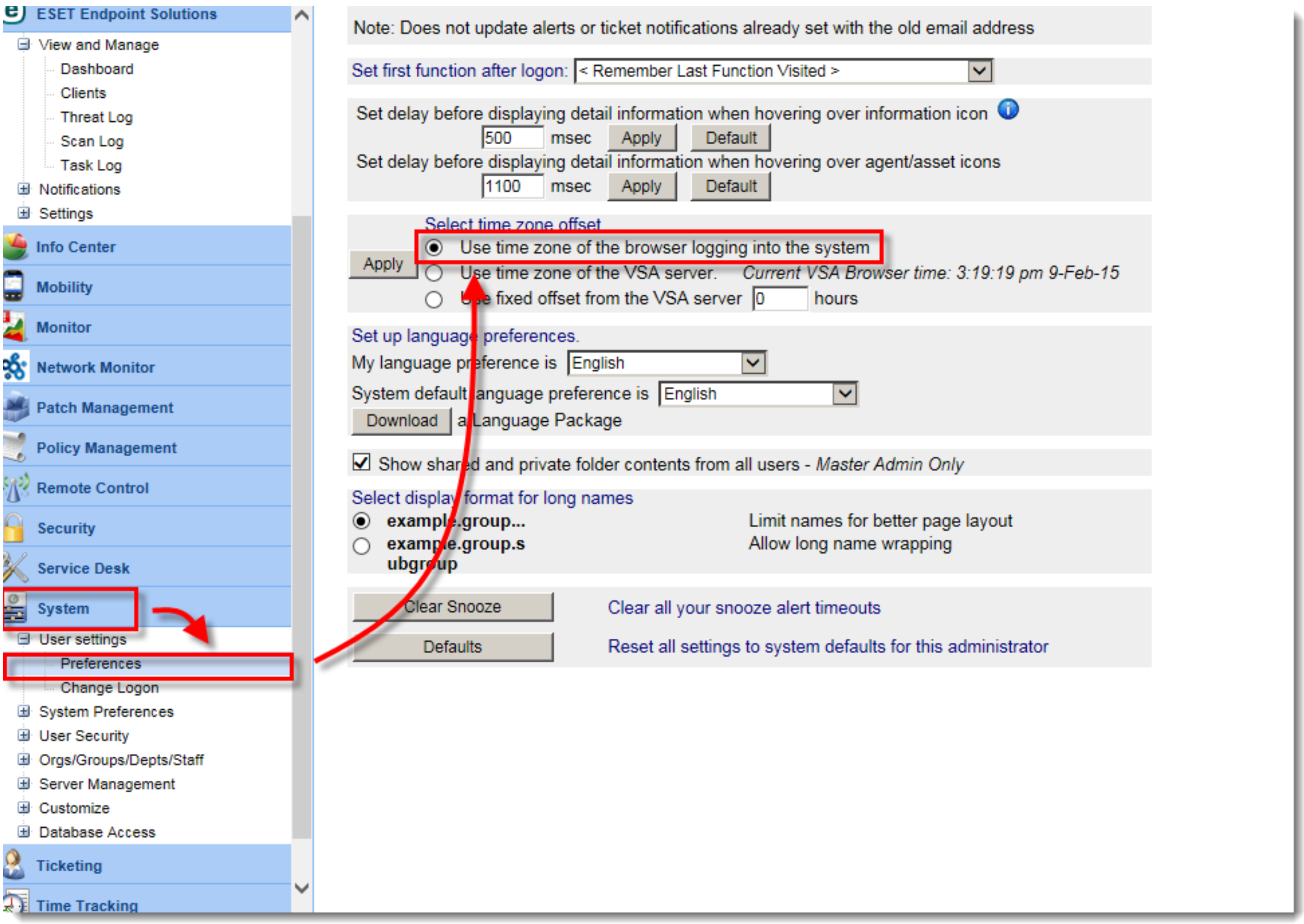
Known issues are listed in bold. Recommended steps to resolve an issue are included below the issue description.

Plug-in does not display in the Kaseya VSA navigation panel or viewing sections of the Plug-in results in a database error.

> This can occur if the Database Schema was applied incorrectly during Plug-in installation. Open the ESET Remote administrator Plug-in for Kaseya, navigate to **System > Server Management > Configure** and click **Reapply Schema**. Note that reapplication of the schema will temporarily take your Kaseya VSA server offline.

Dates and times do not display correctly in the Plug-in.

> The ERA Plug-in for Kaseya uses time zone settings that are specific to each VSA administrator. If times are not displayed at all, or are displaying incorrectly, open the ESET Remote administrator Plug-in for Kaseya and navigate to **System > User Settings > Preferences.** Select **Use time zone of the browser logging into the system** and click **Apply**.



Note: Does not update alerts or ticket notifications already set with the old email address

Set first function after logon: < Remember Last Function Visited >

Set delay before displaying detail information when hovering over information icon
500 msec Apply Default

Set delay before displaying detail information when hovering over agent/asset icons
1100 msec Apply Default

Select time zone offset

Apply
● Use time zone of the browser logging into the system
○ Use time zone of the VSA server. *Current VSA Browser time: 3:19:19 pm 9-Feb-15*
○ Use fixed offset from the VSA server 0 hours

Set up language preferences.

My language preference is English

System default language preference is English

Download a Language Package

☑ Show shared and private folder contents from all users - *Master Admin Only*

Select display format for long names

● **example.group...** Limit names for better page layout
○ **example.group.subgroup** Allow long name wrapping

Clear Snooze Clear all your snooze alert timeouts

Defaults Reset all settings to system defaults for this administrator

Figure 1-29

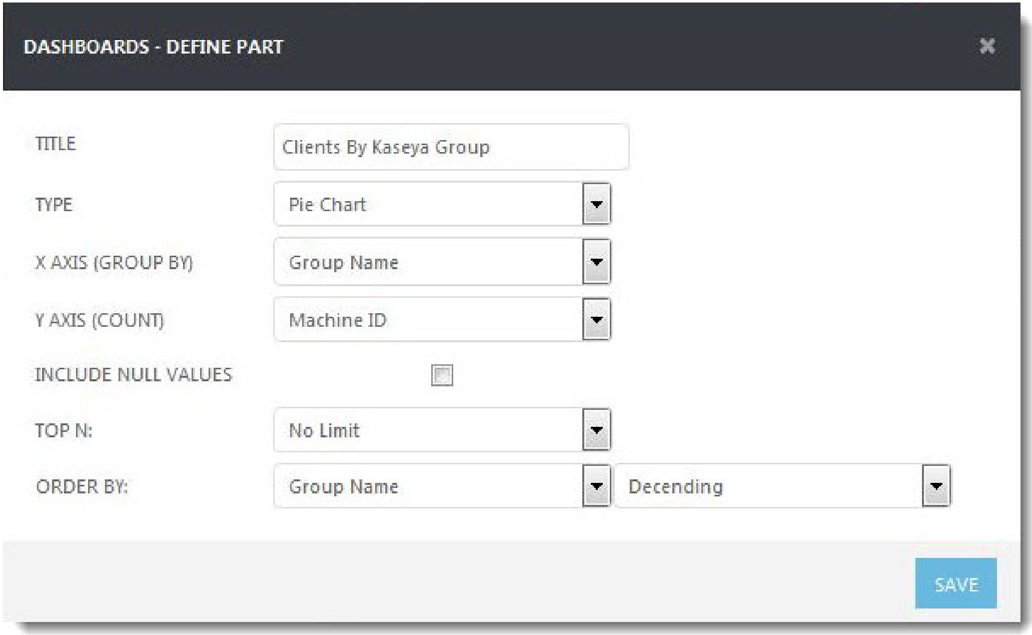
Dashboards do not display graphs

> Install Adobe Flash Player if it is not already installed. If the issue persists, contact Kaseya support to review requirements for cookies, JavaScript and pop-ups.

15. Appendix A: Sample Dashboard Charts

See below for sample configuration settings you can use to add several informative dashboard charts. See Dashboards for instructions to add a new chart.

Clients by Kaseya group

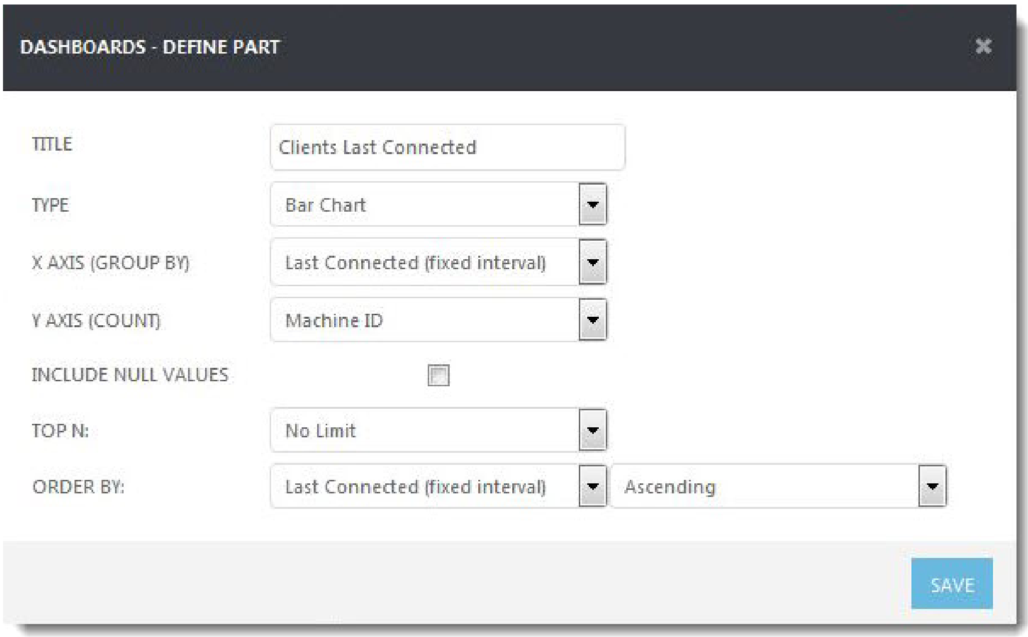


DASHBOARDS - DEFINE PART

TITLE	Clients By Kaseya Group
TYPE	Pie Chart
X AXIS (GROUP BY)	Group Name
Y AXIS (COUNT)	Machine ID
INCLUDE NULL VALUES	□
TOP N:	No Limit
ORDER BY:	Group Name / Decending

Figure A-1

Clients last connected

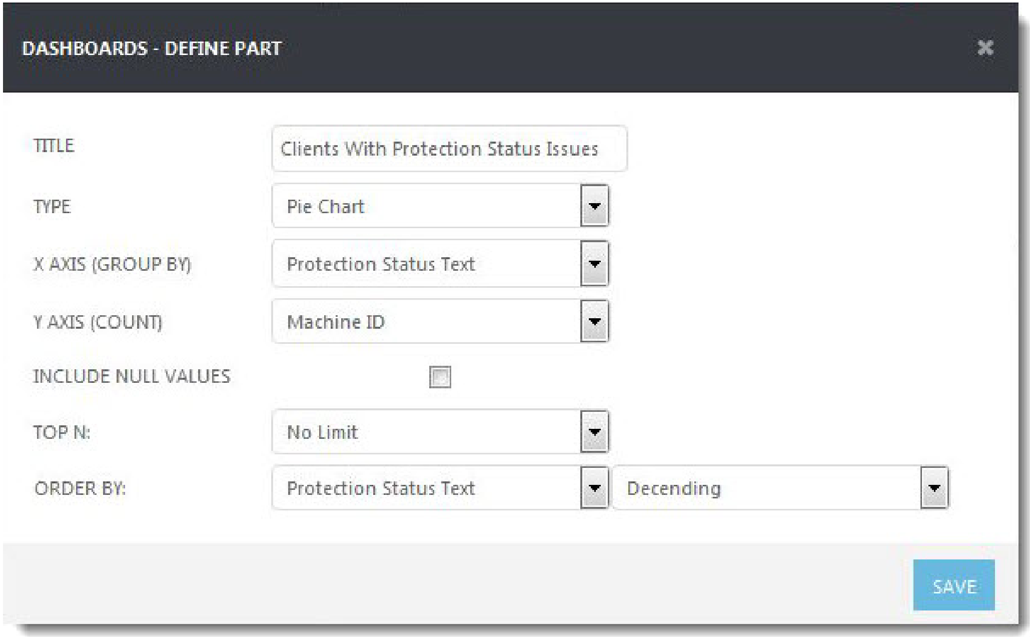


DASHBOARDS - DEFINE PART

TITLE	Clients Last Connected
TYPE	Bar Chart
X AXIS (GROUP BY)	Last Connected (fixed interval)
Y AXIS (COUNT)	Machine ID
INCLUDE NULL VALUES	□
TOP N:	No Limit
ORDER BY:	Last Connected (fixed interval) / Ascending

Figure A-2

Clients with protection status issues



TITLE: Clients With Protection Status Issues

TYPE: Pie Chart

X AXIS (GROUP BY): Protection Status Text

Y AXIS (COUNT): Machine ID

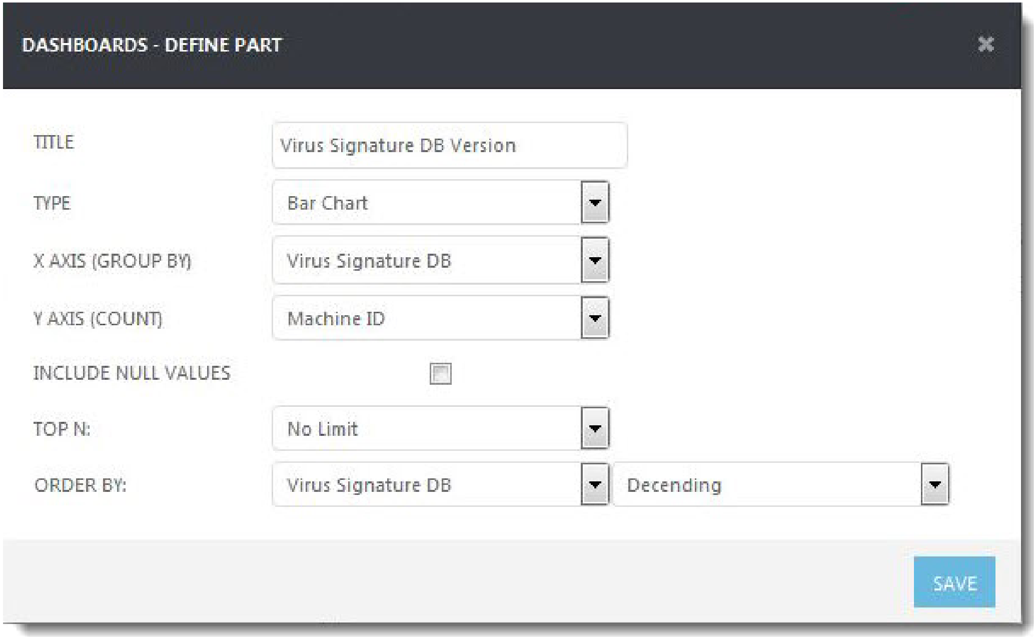
INCLUDE NULL VALUES: □

TOP N: No Limit

ORDER BY: Protection Status Text | Decending

Figure A-3

Client virus signature database version



TITLE: Virus Signature DB Version

TYPE: Bar Chart

X AXIS (GROUP BY): Virus Signature DB

Y AXIS (COUNT): Machine ID

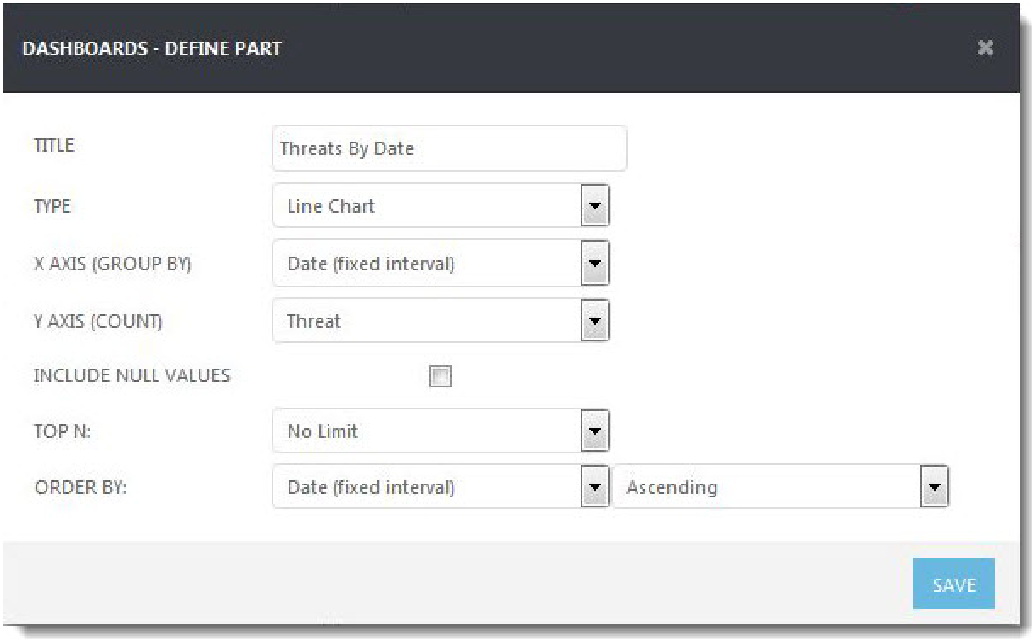
INCLUDE NULL VALUES: □

TOP N: No Limit

ORDER BY: Virus Signature DB | Decending

Figure A-4

Number of threats by date

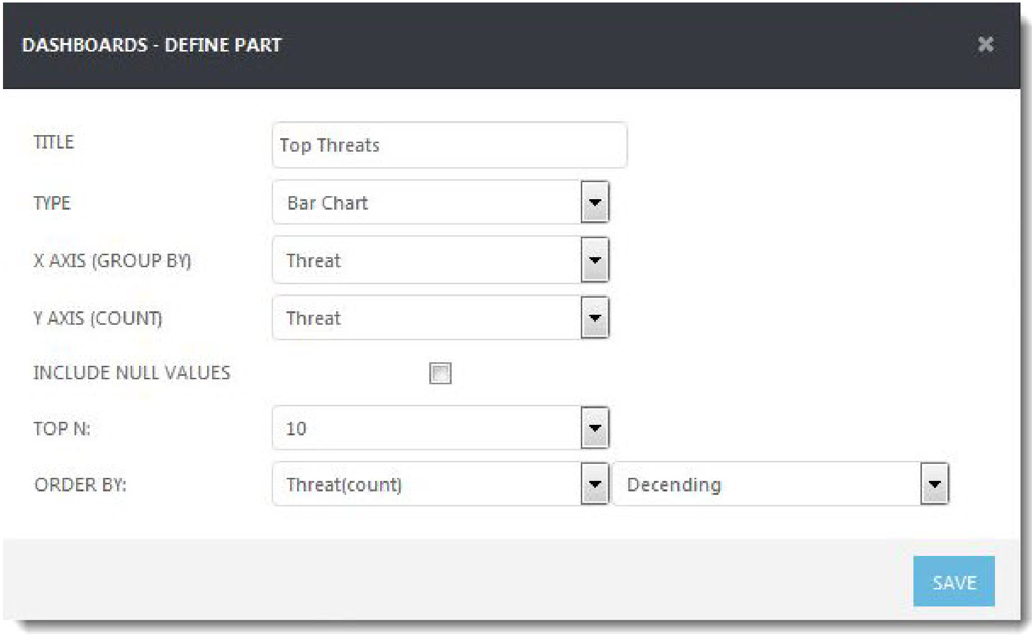


DASHBOARDS - DEFINE PART

TITLE	Threats By Date	
TYPE	Line Chart	
X AXIS (GROUP BY)	Date (fixed interval)	
Y AXIS (COUNT)	Threat	
INCLUDE NULL VALUES	□	
TOP N:	No Limit	
ORDER BY:	Date (fixed interval)	Ascending

Figure A-5

Top threats



DASHBOARDS - DEFINE PART

TITLE	Top Threats	
TYPE	Bar Chart	
X AXIS (GROUP BY)	Threat	
Y AXIS (COUNT)	Threat	
INCLUDE NULL VALUES	□	
TOP N:	10	
ORDER BY:	Threat(count)	Decending

Figure A-6

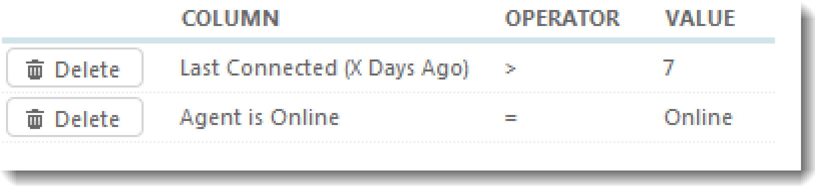
16. Appendix B: Sample Notifications

See below for sample notification settings you can use to add several informative notifications. See Notifications for instructions to create a new notification.

Note:

- When creating a new notification you can specify multiple **AND** conditions, all of which will be evaluated when the notification is triggered.
- To create a wildcard, leave the **Value** field following the **Like** or **Not Like** operator blank.

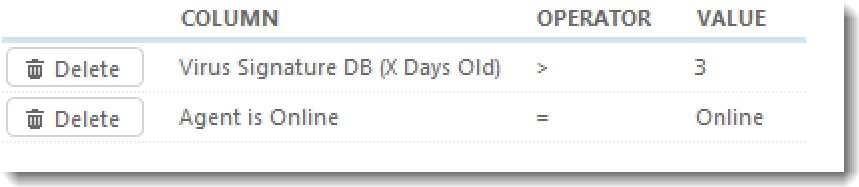
Client has missed its check-in interval — This will fire if the Kaseya Agent is online, but the ESET endpoint has not checked in to the ERA Server in over 7 days. We recommend that you specify a one day cool down period for this trigger.



	COLUMN	OPERATOR	VALUE
🗑 Delete	Last Connected (X Days Ago)	>	7
🗑 Delete	Agent is Online	=	Online

Figure B-1

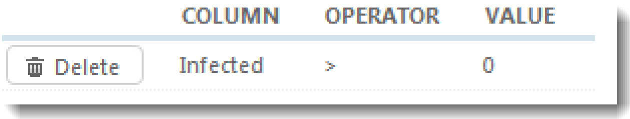
Virus signature database is out of date — This set of triggers will fire if the Kaseya Agent is online and the ESET virus signature database is over three days old.



	COLUMN	OPERATOR	VALUE
🗑 Delete	Virus Signature DB (X Days Old)	>	3
🗑 Delete	Agent is Online	=	Online

Figure B-2

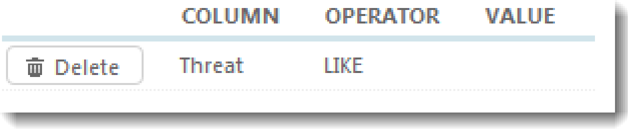
Virus scan detected infected files — This will fire if one or more infected files are found during a scan.



	COLUMN	OPERATOR	VALUE
🗑 Delete	Infected	>	0

Figure B-3

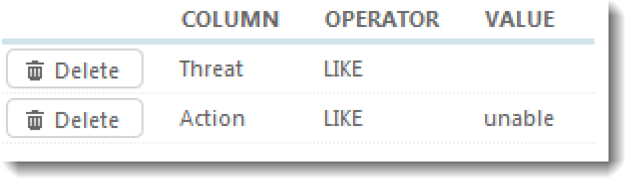
Threats detected — This will fire any time that threats are detected and reported to the ERA Server.



	COLUMN	OPERATOR	VALUE
🗑 Delete	Threat	LIKE	

Figure B-4

Threats detected—Unable to clean — This will fire any time that a detected threat cannot be removed by ESET.



	COLUMN	OPERATOR	VALUE
🗑 Delete	Threat	LIKE	
🗑 Delete	Action	LIKE	unable

Figure B-5