ESET
REMOTE ADMINISTRATOR PLUG-IN
For Kaseya
Technical Setup and User Guide

Click here to download the latest version of this document
ESET REMOTE ADMINISTRATOR PLUG-IN
FOR KASEYA

Copyright 2017 by ESET, spol. s r.o.

ESET REMOTE ADMINISTRATOR Plug-in FOR Kaseya was developed by ESET, spol. s r.o.

For more information visit www.eset.com.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

Customer Care Worldwide: www.eset.com/support
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. 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.
2. System Requirements

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 6.5 [Download ERA 6.5]
- ESET Remote Administrator Server 5.3 [Download ERA 5.3]

**NOTE:** The Plug-in must be installed directly on your Kaseya VSA Server, however ESET Remote Administrator may be installed on a separate server.

To review Kaseya Server system requirements, visit the [Kaseya home page](#).
3. Integrating and Using the Kaseya Plug-in

This section includes the following topics:

- Install the ERA Plug-in for Kaseya
- Configure the Kaseya Plug-in using the Setup wizard

3.1 Install the ERA Plug-in for Kaseya

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: https://www.eset.com/us/business/remote-management/remote-administrator/plugin/kaseya/
3. Double-click the ESET Remote Administrator Plug-in for Kaseya setup file (.exe) to start the installation wizard.
4. Read the End-User License Agreement and click I Accept if you agree to the terms.
5. Click Next after the installer finishes checking for prerequisites.
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.

7. When installation is complete, click Finish. The installer will automatically reapply the database schema for your database.
Figure 1-5
3.2 Configure the Kaseya Plug-in using the 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 the 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.

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

2. Click New to create a new server entry.

3. Type a name for your new server into the Name field and click Next.
4. Enter the following information in the corresponding fields in the Setup Wizard (see figure 1-4).
   
a. The version of ERA you will be connecting to
b. A name for your ERA Server
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**.
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.
3.3 Creating and using Policies

You can create and edit policies for Kaseya client devices with ESET products installed. Navigate to Policies and Notifications > Policies to view existing policies 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 the Machines or Groups to which that policy is applied

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 Machines**—Opens the policy assignment dialog for the currently selected policy. This feature allows you to assign policies to individual devices.
- **Assign Groups**—Opens the policy assignment dialog for the currently selected policy. This feature allows you to assign policies to Kaseya Groups.
- **Allow Assignment / Disallow Assignment**—Click to allow the selected policy to be assigned directly to a device from 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)

![Policy Tree Screenshot](image)

This section includes the following topics:
• Create a policy for version 5.x endpoint products
• Create a policy for version 6.x endpoint products
• Assign policies to computers

3.3.1 Create a policy for version 5.x 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.

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

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

### 3.3.2 Create a policy for version 6.x endpoint products

1. Navigate to **Policies and Notifications > Policies**, locate your ERA 6.x server and select the parent node representing the server for which you would like to create the policy.
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 device. Policies are applied to the device 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.
3.3.3 Assign policies to computers

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 any policies applied directly, it will adopt the most recent policy assigned to it.

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

- Policies are applied to a machine group in order of priority.

Assign a policy to a specific machine or a Machine Group

1. Navigate to Policies and Notifications > Policies.
2. Select the policy you want to assign and click Assign Machines or Assign Groups.
3. Select the check box next to the name of a machine or group to assign the current policy. You can also filter the client list using the filtering bar. 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.

7. Click Finish when you are finished making changes.
3.4 Managing ESET 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.

This section includes the following topics:

- **Initiate a client task**
- **Sort and edit columns**
3.4.1 Initiate a client task

Click **Scan** or **Update Virus DB** to apply these tasks on your selected clients. You can also assign policies and create activation tasks for version 6 clients.

![Figure 1-1](image-url)
3.4.2 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.

![Figure 1-1](image)

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 1-1](image)

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.
3.4.3 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.
3.4.4 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 1-1](image)

3.4.5 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.
3.4.6 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.

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 below for sample configuration settings you can use to add several informative dashboard charts.
Clients by Kaseya group

![Dashboard Definition](image)

**Figure 1-2**
Clients last connected

**Figure 1-3**

Clients with protection status issues

**Figure 1-4**

Client virus signature database version
<table>
<thead>
<tr>
<th>TITLE</th>
<th>Virus Signature DB Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Bar Chart</td>
</tr>
<tr>
<td>X Axis (Group By)</td>
<td>Virus Signature DB</td>
</tr>
<tr>
<td>Y Axis (Count)</td>
<td>Machine ID</td>
</tr>
<tr>
<td>Include Null Values</td>
<td>No</td>
</tr>
<tr>
<td>Top N:</td>
<td>No Limit</td>
</tr>
<tr>
<td>Order By:</td>
<td>Virus Signature DB Decending</td>
</tr>
</tbody>
</table>

**Figure 1-5**
Number of threats by date

Figure 1-6

Top threats

Figure 1-7
3.4.7 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** and type a name for your new notification in the **Name** field.

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**. See below for sample notification settings you can use to add several informative notifications.

**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.

![Figure 1-1](image)

**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.

![Figure 1-2](image)
Figure 1-3

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

Figure 1-4

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

Figure 1-5

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

Figure 1-6

3.5 Deploying 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.

This section includes the following topics:

- Create version 5.x ESET product packages
- Create version 6.x ESET product packages
- Deploy packages
- Share deployment packages
- Uninstall ESET
3.5.1 Create version 5.x ESET product packages

1. Navigate to Deployment > Packages.

![Figure 1-1](image)

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.

![Figure 1-2](image)

3.5.2 Create version 6.x ESET product packages

1. Navigate to Deployment > Packages.

![Figure 1-1](image)

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.

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.

**Figure 1-2**

### 3.5.3 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.
3.5.4 Share deployment packages

**Note:** The ERA version 6.5 compatible Kaseya plug-in includes a new feature that allows administrators to limit the visibility of deployment packages to a specific admin group or user. Previously created deployment packages will retain their global visibility. You must create new deployment packages to leverage this new functionality.

Follow the steps below to share a deployment package to a specific group or user:

1. Navigate to **Deployment > Packages**.
2. Select the deployment package you would like to share.
3. Click **Share**.
4. In the **Select Roles** section, select the check box next to each Role with whom you are sharing the deployment package.
5. Select the check box next to **Edit** to give permissions to the selected roles to edit the deployment package.

The table below shows how package permissions are applied:

<table>
<thead>
<tr>
<th>Role</th>
<th>Can Deploy</th>
<th>Can Edit</th>
<th>Can Delete</th>
<th>Can Share</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legacy Deployment Packages (v2.4.0.0 and earlier)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All Users</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N / A</td>
</tr>
<tr>
<td><strong>Deployment Package (v2.5.0.x)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master Admin</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Package Creator</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Other Users / Roles</td>
<td>If allowed</td>
<td>If allowed</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

6. Click **Add** to add the selected roles or users to the **Shared Rights for the Deployment Package** list.

7. Repeat steps 3-5 for users in the **Select Users** section.

8. Once you have finished making changes, click **Save**.
3.5.5 Uninstall ESET

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).
4. 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.

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.
5. Feedback

We at ESET hope that the ESET Remote Administrator Plug-in for Kaseya will be a useful asset, and are dedicated to continue improving the Plug-in according to your feedback. Follow the steps below to send us your feedback:

1. Click **Send Feedback** to view the feedback form.

![Figure 1-1](image)

2. Complete the **Subject** and **Category** fields by typing the appropriate information or using the drop-down menu to select the appropriate value.

3. Type your feedback into the **Message** field.

4. Type the appropriate information in the **Contact** fields.

5. Click **Send** to submit your feedback.
Your constructive feedback is important! Please use this form to submit general feedback, feature requests and anything else that you might like to share with the developers.

**SUBJECT**

**CATEGORY**
General Feedback

**MESSAGE**

**CONTACT NAME**

**CONTACT NUMBER**

**CONTACT EMAIL**

**SEND**

Figure 1-2
6. ERA 6 Plug-in for Kaseya Changelog

Version 2.5.0.15:

- **Plug-in now supports:** ESET Remote Administrator 5.3 and ESET Remote Administrator 6.5. ESET Remote Administrator 6.2-6.4 are no longer supported
- **Enhancement:** Deployment packages created are “private” and can be shared with specific users and roles. *Note:* "Legacy" deployment packages retain their previous visibility and permissions
- **Enhancement:** ESET Deployment on Windows machines retrieves the log files created during deployment. These can be found in the normal "Get File" location
- **Enhancement:** Exposed a button in the plug-in options to allow the administrator to repair their deployment scripts without having to Reapply Schema or manually run SQL
- **Enhancement:** When creating a new deployment package, you may specify an agent port other than 2222

Version 2.4.0.0:

- **Plug-in now supports:** ESET Remote Administrator 5.3 and ESET Remote Administrator 6.3-6.4. ESET Remote Administrator 6.2 and earlier are no longer supported
- **Enhancement:** Kaseya group may be assigned policies
- **Enhancement:** Policy view now reflects the usability changes implemented in ERA 6.4
- **Enhancement:** Plug-in supports uninstall of password protected ESET agent
- **Enhancement:** Plug-in now supports language selection when creating deployment packages

Version 2.3.1.0:

- **Plug-in now supports:** ESET Remote Administrator 5.3 and ESET Remote Administrator 6.3. ESET Remote Administrator 6.2 is no longer supported
- **Enhancement:** Plug-in now supports Kaseya cloud (multitenancy)
- **Enhancement:** Added WSC reported AV column to "Clients" view
- **Enhancement:** Added ability to create activation task via "Clients" view
- **Enhancement:** Added ability to remove Plug-in assigned policies from "Clients" view
- **Enhancement:** "Task Execution Log" has been updated to reflect the change to new task workflow in ESET Remote Administrator 6.3
- **Enhancement:** Added support for Custom Deployment. EMU MSPs can deploy ESET solutions to clients without specifying a Username and Password
- **Enhancement:** Added support for MAC OS X deployment
- **Enhancement:** Updated notifications UI
- **Enhancement:** Updated Policy Assignment UI with improved filtering

*NOTE:* Plug-in users who were previously assigning policies or notifications to Kaseya groups rather than specific clients should use the new assignment interface to re-assign policies and notifications. The plug-in no longer assigns these items to groups due to multi-tenancy changes introduced in this version.

- **Enhancement:** Licenses are now sorted by License Owner and product name
- **Bug Fix:** Fixed an issue that caused erroneous activation tasks to be created following deployment of version 6 solutions
- **Bug Fix:** Fixed an issue that caused reapply schema errors on new (non-upgrade) installations
- **Bug Fix:** Fixed an issue introduced in version 2.2.2.1 that prevented version 5 deployments from being edited
- **Bug Fix:** Fixed an issue that caused the plug-in not to register that an ESET Remote Administrator Server update had completed
- **Bug Fix:** Fixed an issue that caused deployment to Windows Server 2012 to install the wrong client solution
- **Bug Fix:** Fixed an issue that caused V6 deployment packages not to auto-select their correct agent certificate during edit
- **Bug Fix:** Fixed an issue that caused multiple actions not to fire when a notification included a cooldown task

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'

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