

ESET REMOTE ADMINISTRATOR PLUG- IN For ConnectWise Automate

Technical Setup and User Guide

[Click here to download the latest version of this document](#)

ESET REMOTE ADMINISTRATOR PLUG-IN FOR ConnectWise Automate

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

ESET REMOTE ADMINISTRATOR Plug-in FOR ConnectWise Automate 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

REV. 3/9/2017

1. Introduction	4	4.8 Using the ESET Dashboard	66
1.1 Platform Overview.....	4	4.8.1 Access and setup the ESET Dashboard	66
2. System Requirements.....	6	4.8.2 Filter data in the Dashboard.....	68
2.1 Installation prerequisites.....	6	4.8.3 Navigate the Overview window	70
2.2 Settings and Maintenance	7	4.8.4 Viewing reports.....	71
3. Migrating from version 5 to 6.....	8	4.8.4.1 View the License and Usage report.....	72
3.1 Migration considerations and prerequisites.....	8	4.8.4.2 View the Client/Location Usage report.....	72
3.2 Upgrade to 6.x on a new server	9	5. MSP and Licensing.....	73
4. Integrating and Using the ConnectWise Automate Plug-in.....	16	6. Support and Troubleshooting.....	75
4.1 Installing the ERA Plug-in for ConnectWise Automate	16	6.1 Database.....	75
4.1.1 Install the ERA Plug-in from Solution Center.....	16	6.2 Exporting to Common Formats.....	76
4.1.2 Install the ERA Plug-in from Plugin Manager.....	17	6.3 Development tickets.....	77
4.2 Install ERA Server 6.x.....	18	6.4 ConnectWise Automate Plug-in Feedback.....	81
4.3 Install ERA Agent 6.x.....	25	6.5 ConnectWise Automate Plug-in Known Issues.....	81
4.4 Managing ESET product deployments to ConnectWise Automate Agents.....	43	6.6 ERA 6 Plug-in for ConnectWise Automate Changelog.....	82
4.4.1 Deploy to a ConnectWise Automate group.....	43		
4.4.2 Deploy to a single agent, location, client or group from the context menu.....	44		
4.4.3 Monitor a Deployment task.....	45		
4.5 Managing ESET endpoints.....	46		
4.5.1 Manually map an ESET endpoint to a ConnectWise Automate Agent.....	47		
4.5.2 Managing ESET tasks.....	48		
4.5.2.1 Initiate a New Scan Task.....	48		
4.5.2.2 Initiate a New Update Task.....	49		
4.5.2.3 Initiate a New Activation Task.....	49		
4.5.3 View endpoint properties	50		
4.5.4 Archive endpoint threats	52		
4.6 Managing ESET policies.....	52		
4.6.1 ESET policy FAQ.....	53		
4.6.2 Create a policy.....	56		
4.6.3 Assigning policies.....	57		
4.6.3.1 Assign a policy from the Policies window.....	57		
4.6.3.2 Assign a policy from the Groups window.....	59		
4.6.4 Remove a policy from a group.....	60		
4.6.5 Hide groups without policies.....	61		
4.6.6 Import an existing policy from ERA.....	62		
4.6.7 Inherit/Merge Exclusions and Schedules.....	62		
4.7 Managing ESET servers.....	63		
4.7.1 Detect a server.....	63		
4.7.2 Force server detection.....	64		
4.7.3 Verify server detection.....	64		
4.7.4 Synchronize a server	65		
4.7.5 Update server connection settings	66		

1. Introduction

Thank you for using the ESET Remote Administrator (ERA) Plug-in for ConnectWise Automate.

The ESET Remote Administrator 6 Plug-in for ConnectWise Automate is developed by ESET in cooperation with ConnectWise Automate to deploy, manage and report on ESET endpoint products within your ConnectWise Automate Console. With a host of new features built based on customer feedback, this solution allows ConnectWise Automate users to more efficiently meet the needs of their customers. See the [ESET Remote Administrator Plug-in for ConnectWise Automate product page](#) for more information.

Version 5 ESET and Plug-in users: See the [ERA 5 Plug-in for ConnectWise Automate Online Help](#).

ERA 6 Plug-in for ConnectWise Automate users (version 2.5.0.x and later): See the following sections for instructions to manage the ERA 6 Plug-in for ConnectWise Automate:

- [Managing ESET product deployments to ConnectWise Automate Agents](#)
- [Managing ESET endpoints](#)
- [Managing ESET policies](#)
- [Managing ESET tasks](#)
- [Managing ESET servers](#)
- [Using the ESET Dashboard](#)

Migrate to version 6: See the section [Migrate from 5.x to 6.x](#).

ConnectWise Automate MSPs: See the section [MSP and Licensing](#) and the [Database](#) topic for reporting information.

ESET Partner feedback for the plug-in is greatly appreciated. Please use the [feedback form](#) available from the plug-in to submit your feedback directly to the ESET development team.

1.1 Platform Overview

The ESET Remote Administrator for ConnectWise Automate Plug-in is a component of ESET product management and the [ESET MSP Program](#) and consists of several systems to manage ESET products and licenses.

Agent —ConnectWise Automate Agent.

ERA Agent —The ESET Remote Administrator Agent (ERA Agent) is introduced in ERA 6.x and is an essential component of the ERA network. The ERA Agent facilitates all communications between client computers (both endpoints and servers) with ESET products installed and the ESET Remote Administrator Server (ERA Server). The ERA Agent is required for the remote management of client computers via ERA 6.x. The ERA Agent stores and enforces policies for the client computer on which it is installed with or without an internet connection. This allows client computers to respond more quickly to threats, and eliminates the risk of a client becoming vulnerable to a threat if it cannot communicate with the ERA Server.

Endpoint —Typically used to refer to an ESET product and the device it is installed on.

ERA Server —ESET Remote Administrator Server, sometimes referred to as an ESET Server. A lightweight server and database component used to monitor and administer multiple devices including other servers and endpoints.

ERA Web Console/ERAC —The ERA 6.x Web Console replaced ERAC and is accessed using any web browser. From the Web Console, you can make changes to and manage your ESET products.

For an overview of the components and infrastructure for ConnectWise Automate MSPs (Managed Service Providers), see [MSP and Licensing](#).

2. System Requirements

The ESET Remote Administrator 6 Plug-in for ConnectWise Automate requires use of ESET 6.x components and business products.

This section includes the following topics:

- [Installation prerequisites](#)
- [Configurable settings for the plug-in](#)

2.1 Installation prerequisites

ConnectWise Automate RMM

- ConnectWise Automate Server 2013 or later (Cloud or on-premise)

ConnectWise Automate Server:

For optimal operation of the ERA Plug-in for ConnectWise Automate, the ConnectWise Automate server should meet the minimum hardware and software requirements for your version of ConnectWise Automate.

- ConnectWise Automate 10.5 — [Installation Prerequisites](#)

NOTE: Your ConnectWise Automate server must have internet access to download dependencies from <https://update.esetusa.com>. To verify the connection, visit the following address: <https://update.esetusa.com/ConnectWiseAutomate/msi/>

ESET Remote Administrator (ERA) Version 6.x:

You can download the latest Windows installers for ERA 6.x from [eset.com](https://www.eset.com). We strongly recommend that you back up your ERA database before upgrading to the latest version of ESET Remote Administrator. We do not recommend installing ERA Server and ConnectWise Automate server on the same computer.

- [Download the ESET Remote Administrator 6 All-in-One ISO \(Windows Installer\)](#)
- [Download the ESET Remote Administrator 6 Virtual Appliance](#)

For best performance of the ERA Plug-in for ConnectWise Automate, make sure that your ERA Server meets the minimum hardware and software requirements detailed in the [ESET Remote Administrator 6 installation/upgrade guide](#).

Network Configuration

The ESET Server should be accessible from a static IP address or hostname (recommended). If ESET endpoints, the ConnectWise Automate server, or an instance of the ConnectWise Automate Control Center will connect from outside of a LAN, the server must be accessible from a public IP or a public host name (FQDN).

The following TCP ports must allow inbound connections to your ESET Server (Port forwarding / firewall configuration):

- **TCP 2222** - Endpoint connection
- **TCP 2223** - ERA API / Plug-in connection

2.2 Settings and Maintenance

The following settings for the ERA Plug-in for ConnectWise Automate can be configured:

- **List Separator:** Sets the delimiter to be used for the **Copy to Clipboard** buttons used by the plug-in (client-side setting)
- **Table Refresh Interval:** Sets the interval to automatically refresh the tables in the dashboard (client-side setting)
- **Show Archived Logs:** When enabled, all previously archived logs will be displayed after refreshing the dashboard (client-side setting)
- **Clean up logs older than:** Sets the maximum age of logs in the database. Logs older than the set value will be cleaned as part of maintenance.

Maintenance

- **Run manual ERA Sync:** Runs a synchronization similar to the sync that occurs on the ConnectWise Automate database. This will block the UI until synchronization is complete.
- **Reset Role Detection Strings:** Deletes and recreates the plug-in role detection strings in the event they are accidentally modified.

3. Migrating from version 5 to 6

ESET Remote Administrator (ERA) 6.x uses entirely new architecture.

- The ESET Remote Administrator Agent (ERA Agent) is introduced in ERA 6.x and is an essential component of the ERA network.
- The ERA Agent facilitates all communications between client computers (both endpoints and servers) with ESET products installed and the ESET Remote Administrator Server (ERA Server).
- The ERA Agent is required for the remote management of client computers via ERA.
- The ERA Agent stores and enforces policies for the client computer on which it is installed with or without an internet connection. This allows client computers to respond more quickly to threats, and eliminates the risk of a client becoming vulnerable to a threat if it cannot communicate with the ERA Server.

This section includes the following topics:

- [Migration considerations and prerequisites](#)
- [Upgrade to 6.x on a new server](#) (recommended path for MSPs)

3.1 Migration considerations and prerequisites

Network considerations prior to migrating to 6.x

It is important that existing ERA users verify their network is ready to upgrade and that the upgrade process will not result in any loss of functionality. Consider the following before upgrading:

- ERA 6.x uses a new configuration layout that is optimized for use with ESET Endpoint 6.x products. While it is possible to manage ESET Endpoint 5.x products (and earlier ESET Business Edition products) using ERA 6.x, only settings common across all versions will be manageable. For this reason, we strongly recommend you arrange to upgrade client workstations to ESET Endpoint 6.x products when you upgrade to ERA Serve 6.x.
- If you have password-protected settings on ERA 5.x endpoints, we highly recommend [disabling password protection before upgrading to ERA 6.x](#) to avoid issues during uninstallation.
- Due to the nature of MSPs, ERA, and the functionality of the plug-in, we do NOT recommend using the Migration Tool as a ConnectWise Automate/Plug-in Partner. If data retention is required for compliance, we recommend putting the ERA 5.x server into cold storage.

Migration prerequisites

- On your new ERA 6.x server, [verify proper ports are open and forwarded](#).
NOTE: ESET Endpoint 5.x products and ERA Agent 6.x both use port 2222. We recommend changing the ERA Agent Port after installation.
- Install [Java Runtime Environment](#) (version 7 or later) and verify Java is updating correctly.
- Install [Microsoft .NET Framework 3.5](#). Follow the installation process outlined in the following Microsoft Knowledgebase article: [Enable .NET Framework 3.5 by using the Add Roles and Features Wizard](#).
- [V6 Swap Agreement](#) must be signed and the migrating Partner must have the Security Admin credentials in place before migration may commence.
- Determine [what type of database](#) you will configure for use with the ERA Server.
NOTE: Microsoft Access is not supported by ERA Server. Microsoft SQL Server Express is included with the installer (5,000 +/- 1,000 total devices checking in to ERA). We also support the install of Microsoft SQL Server or MySQL version 5.5 or later.

3.2 Upgrade to 6.x on a new server

NOTE: This is the only supported migration path for MSPs.

To upgrade a new machine to ESET Remote Administrator (ERA) 6.x:

1. On your new server, [install ESET Remote Administrator \(ERA\) 6](#).
2. Make note of any group, task or policy settings used on your ERA 5.x client workstations.
3. In the ConnectWise Automate plug-in Navigation menu, click **Policies > New**. In this example, we will create a policy bundle for all installed ERA 6.x products at Client Site “Acme”.

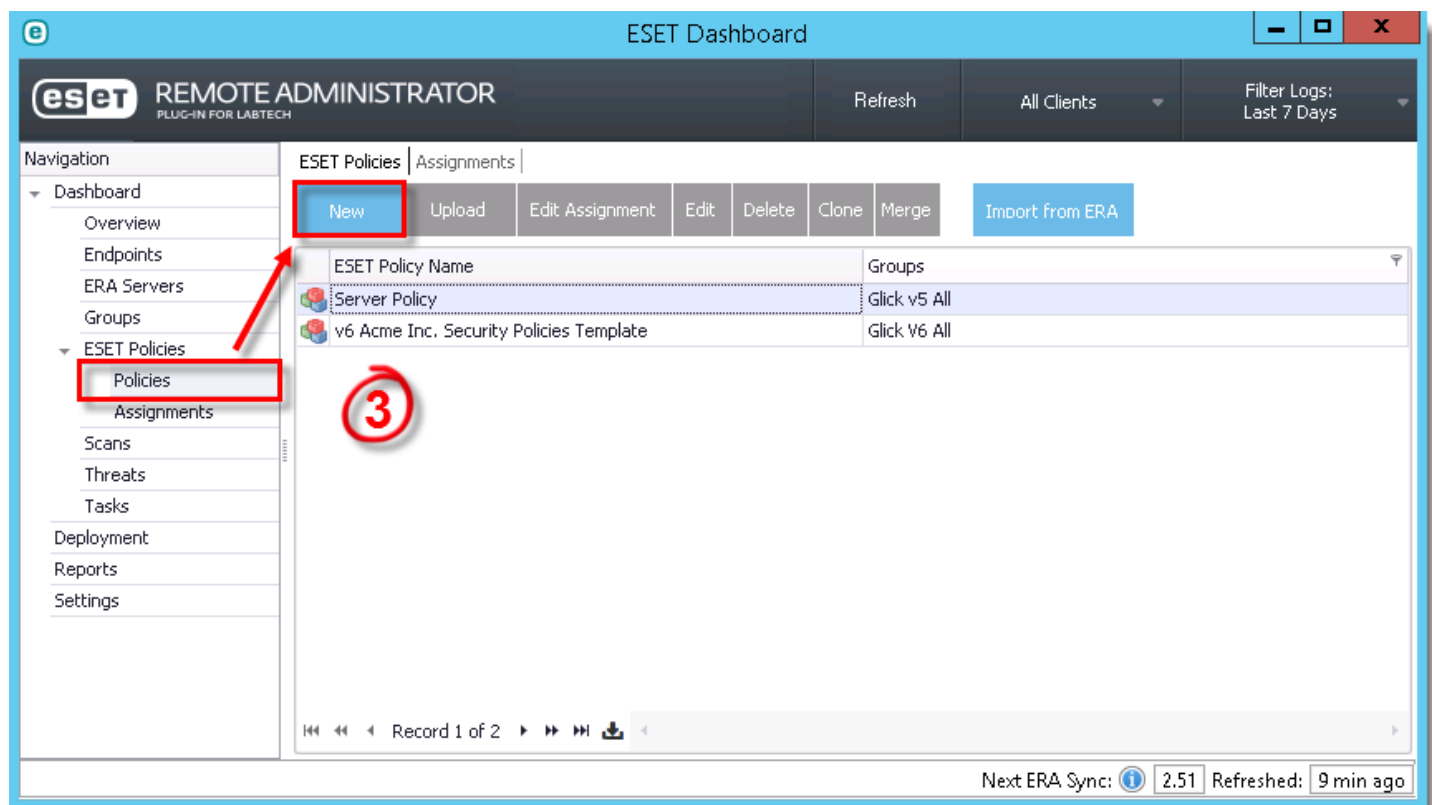


Figure 1-1

4. In the **ESET Policy Name** field, type a name for your policy. Click the **ERA V6** tab. In the **Add Product** drop-down menu, select **Remote Administrator Agent** and any other applicable security products managed for the client. Click **Save**.

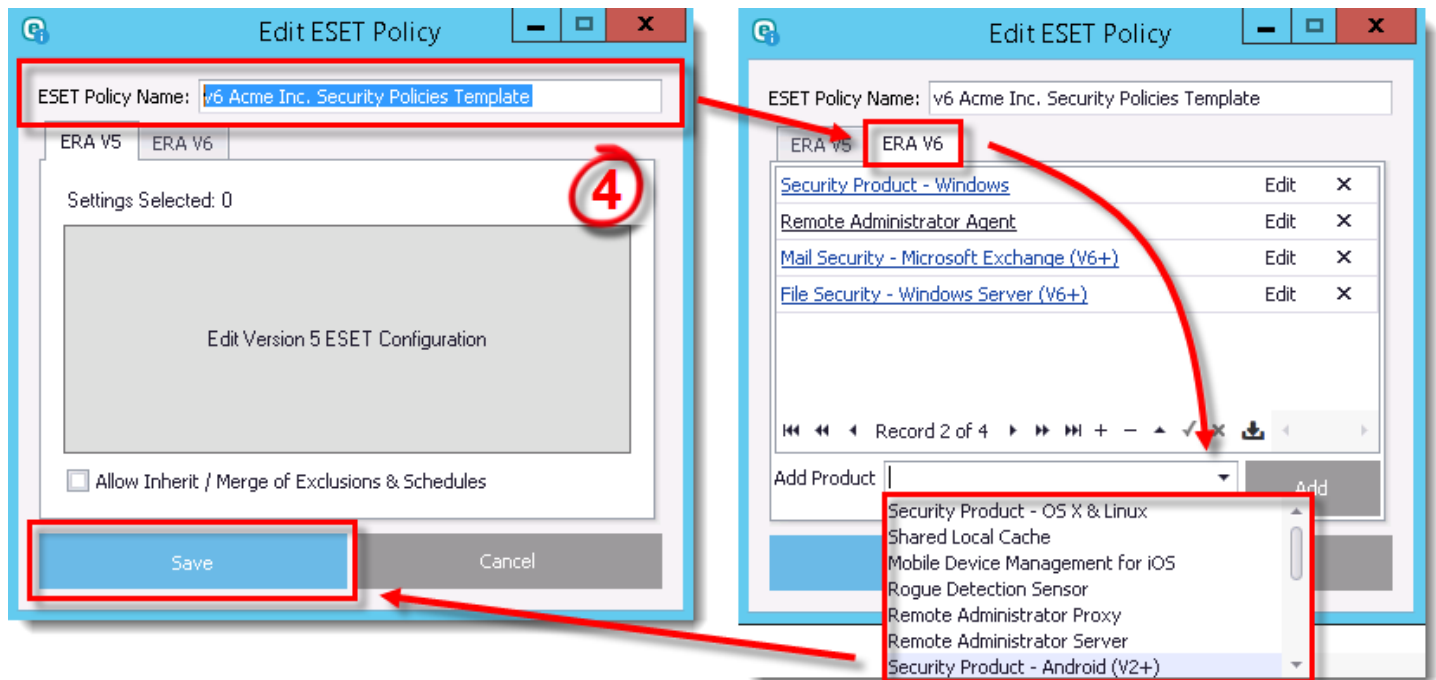


Figure 1-2

5. Select the policy you created in step 6 and click **Edit Assignment**.

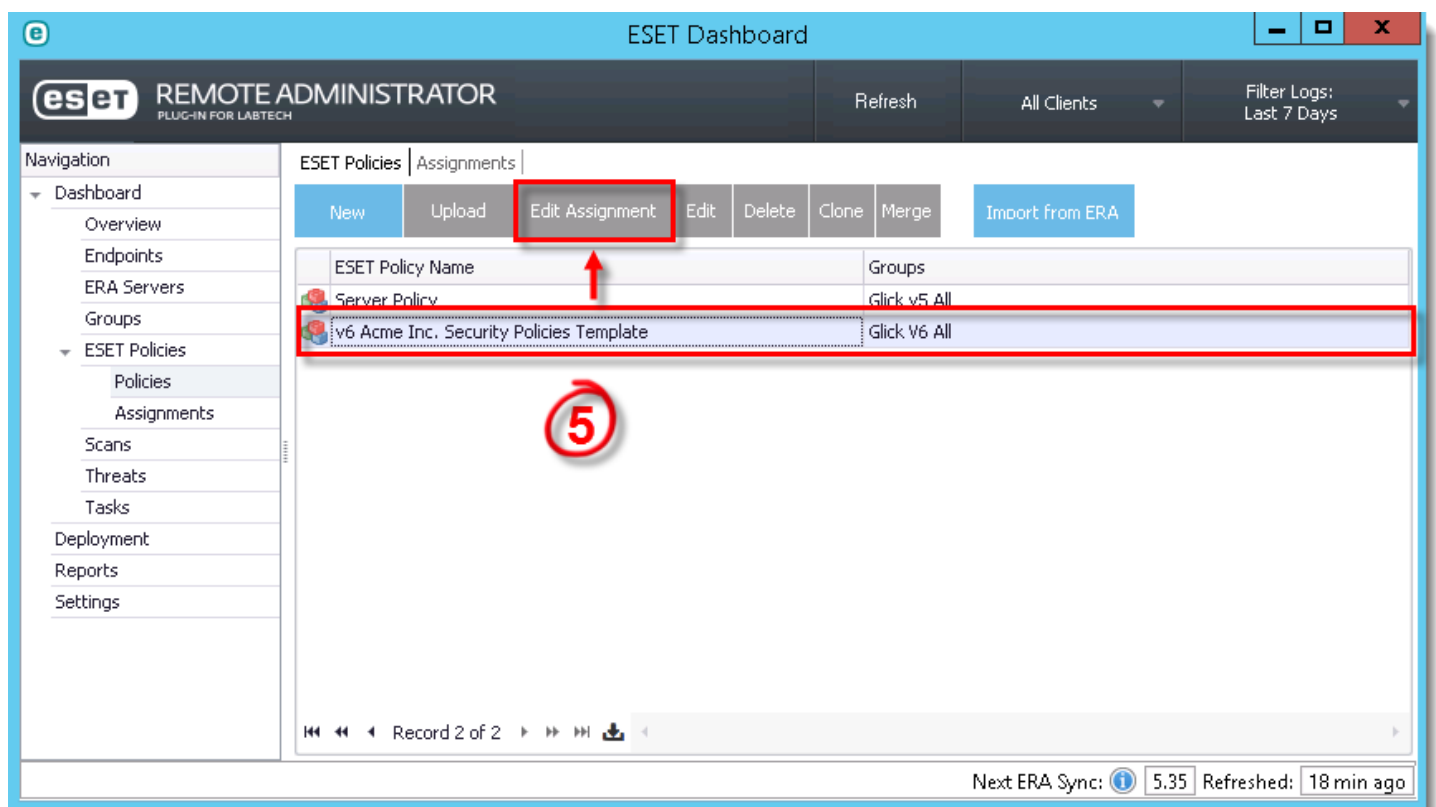


Figure 1-3

6. Select the appropriate group and click **Save**.

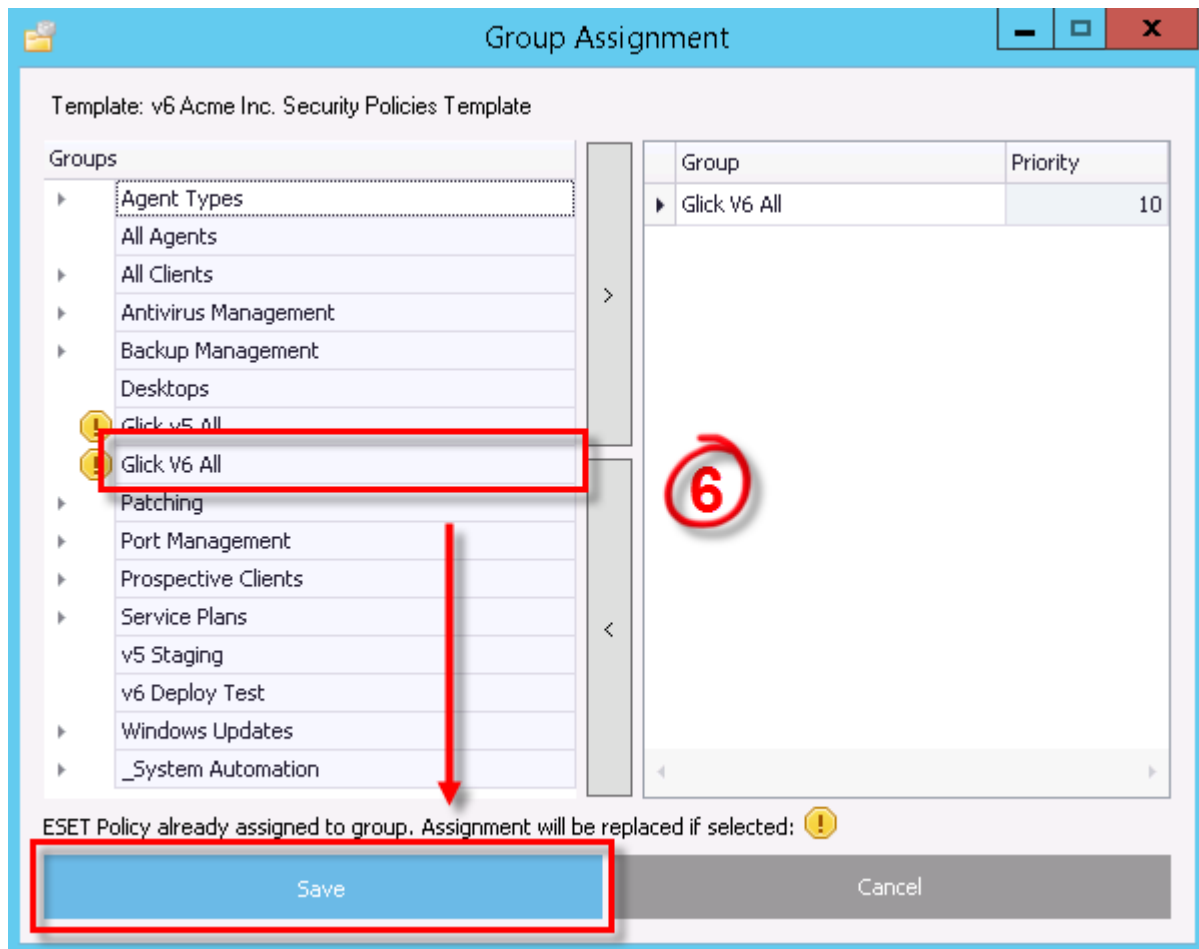


Figure 1-4

- To start migrating devices, in the ConnectWise Automate plug-in Navigation menu, select **Deployment**. Click **New Task**. In the **Task Name** field, type a name for your task, select **Migrate Version 5 Endpoints to Version 6** and then click **Continue**.

NOTE: An ERA 5.x Advanced Settings/Agent Password might be required. Enter the applicable credentials and click **Continue**.

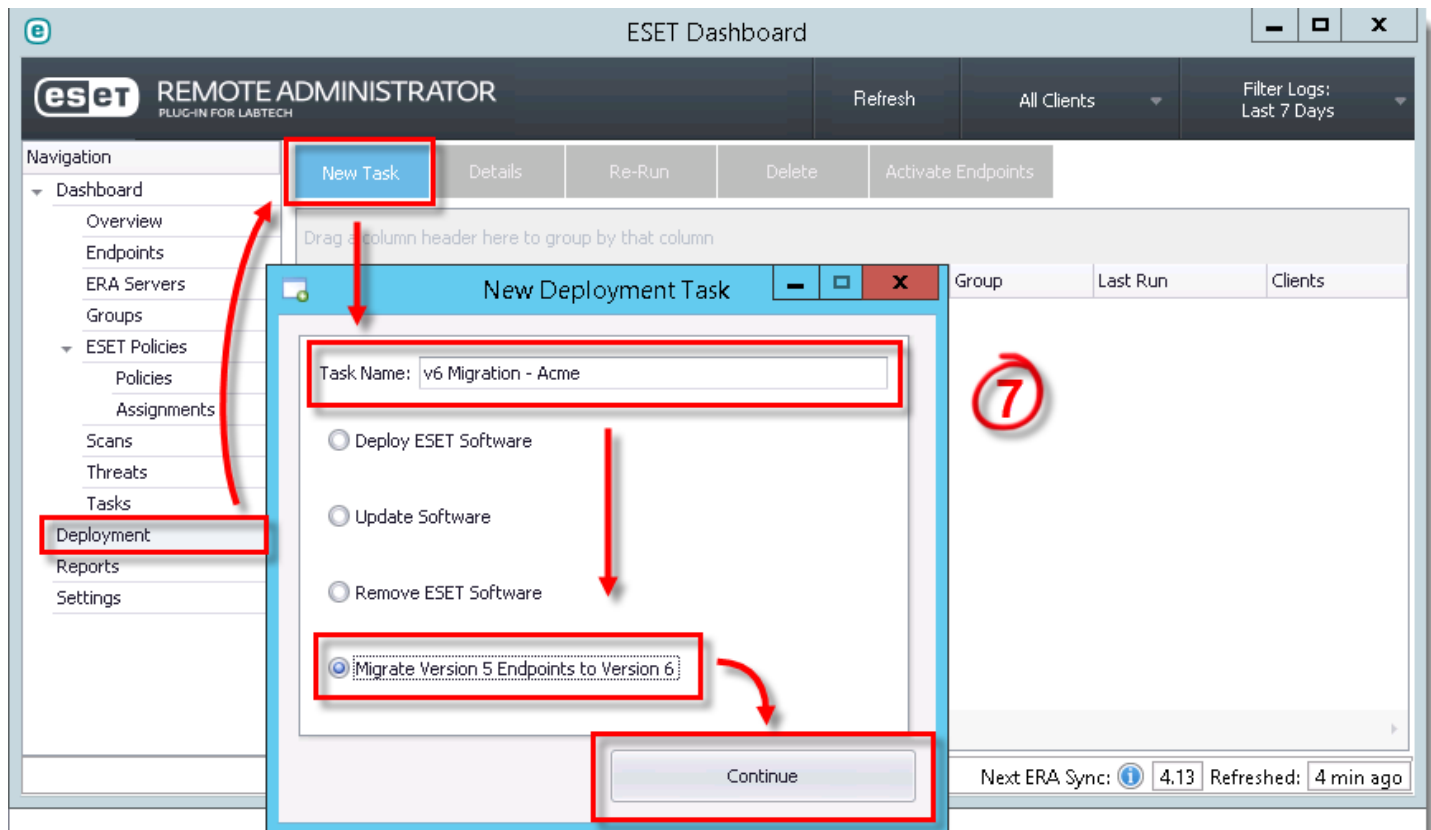


Figure 1-5

8. Select the Primary ERA Server, appropriate ESET Product and Language. In the **Agent Port** field, type the appropriate agent port number and click **Continue**.

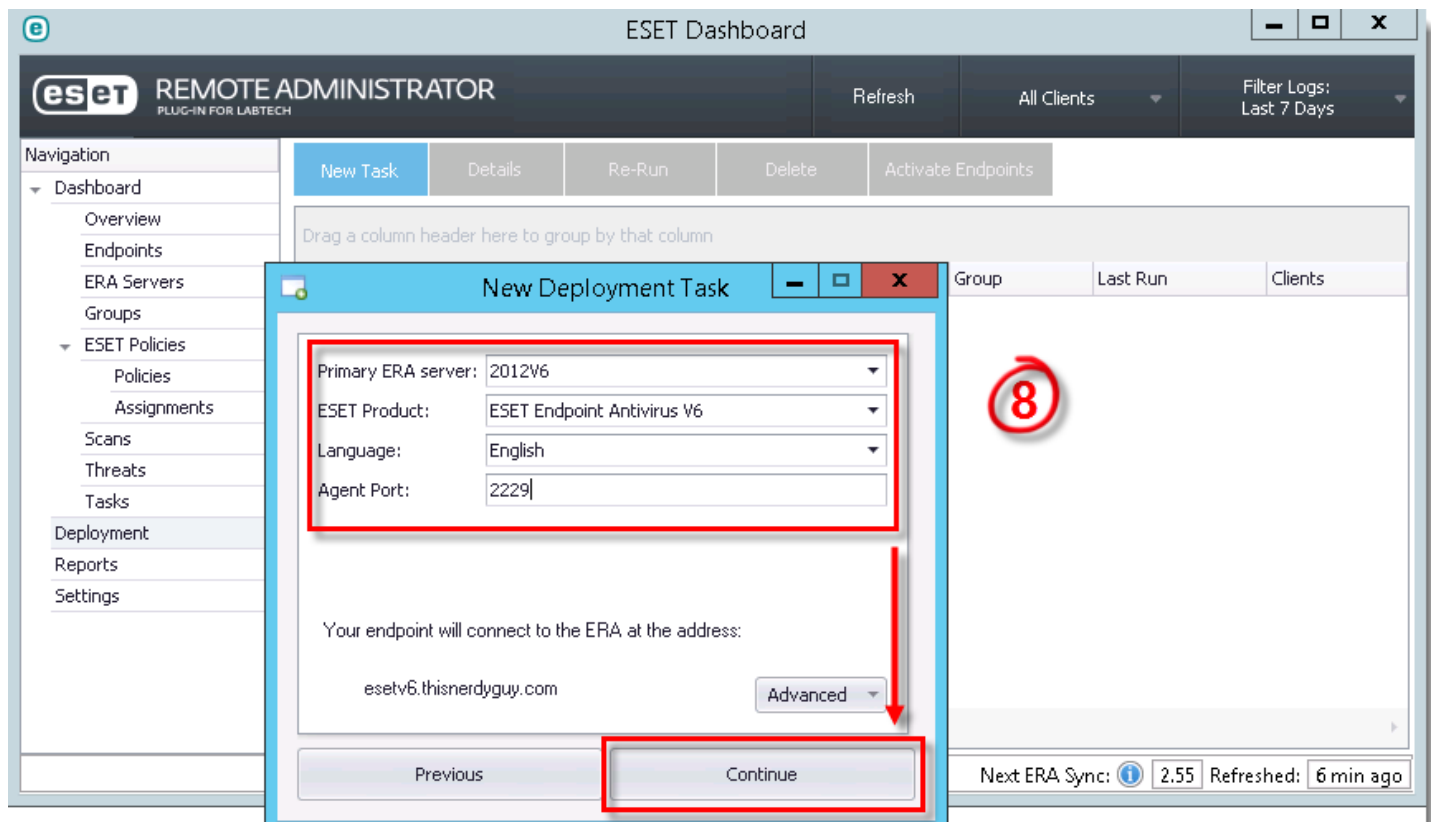


Figure 1-6

9. In the **ConnectWise Automate Group to Target** field, select the applicable groups for this task, click **Select** and then click **Continue**.

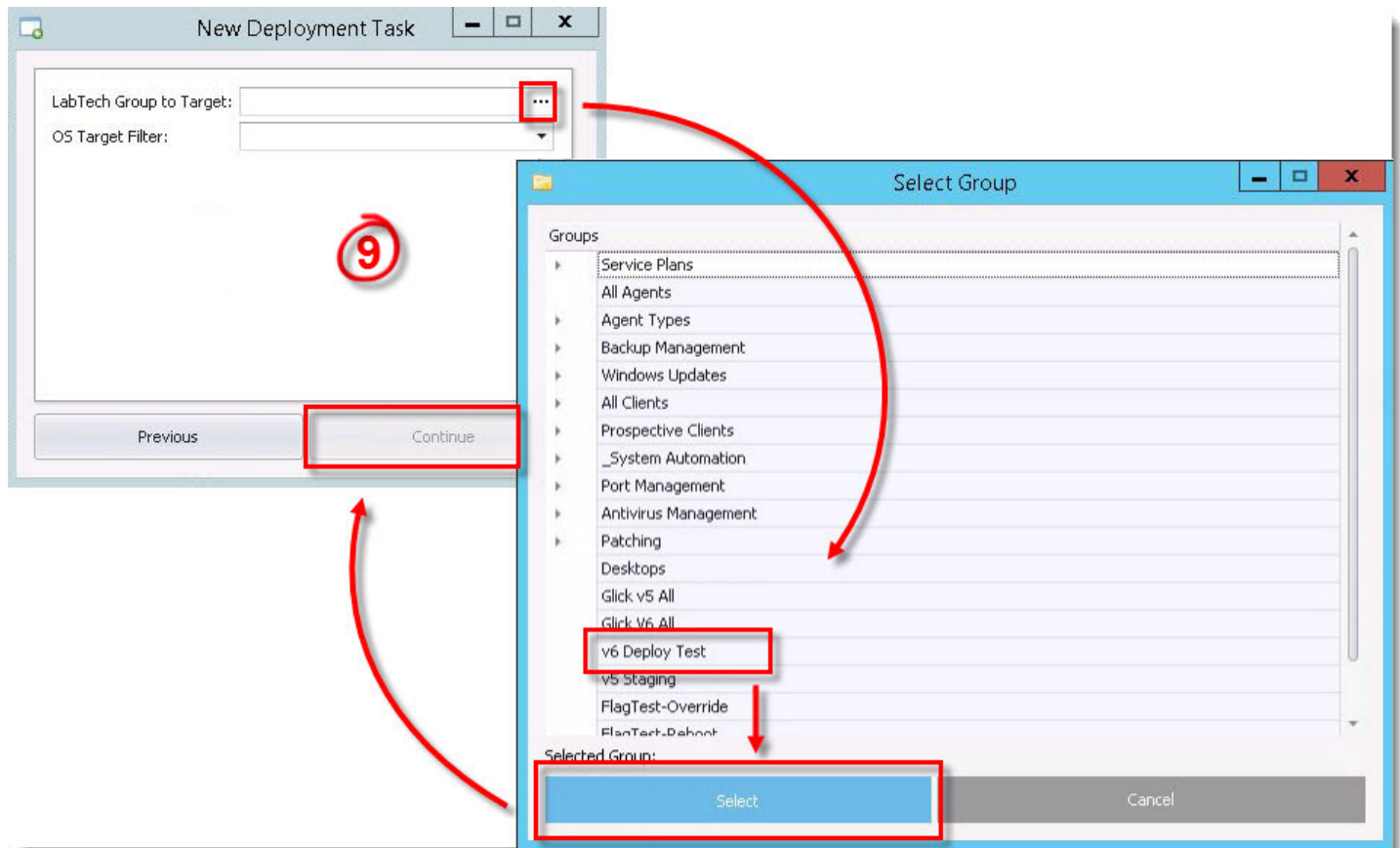


Figure 1-7

10. Select the applicable License and Agent Certificate and then click **Continue**.

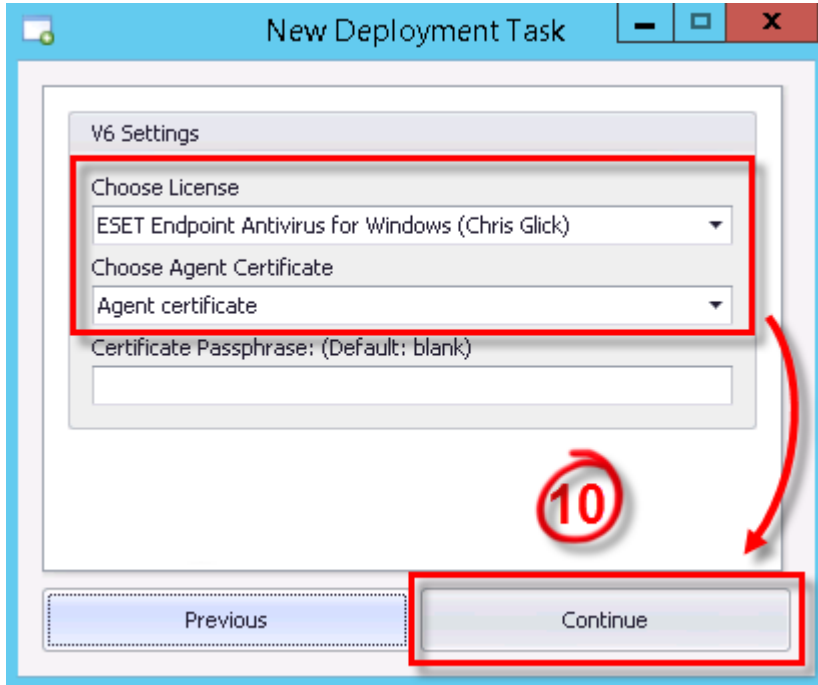


Figure 1-8

11. To start the task, click **Save Task**.

NOTE: This task is subject to sync delays.

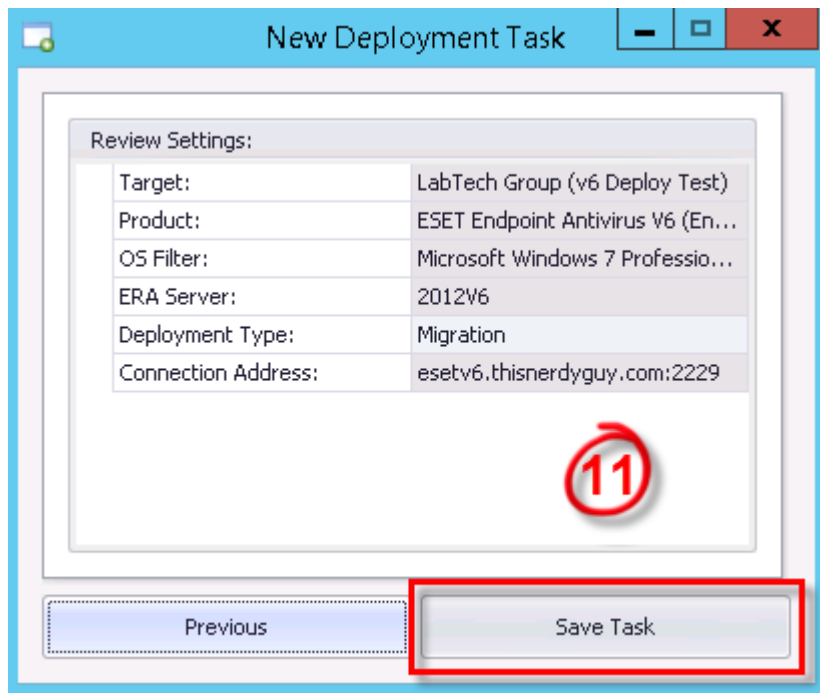


Figure 1-9

12. Check the value in the **Clients** field to determine when the task is complete.

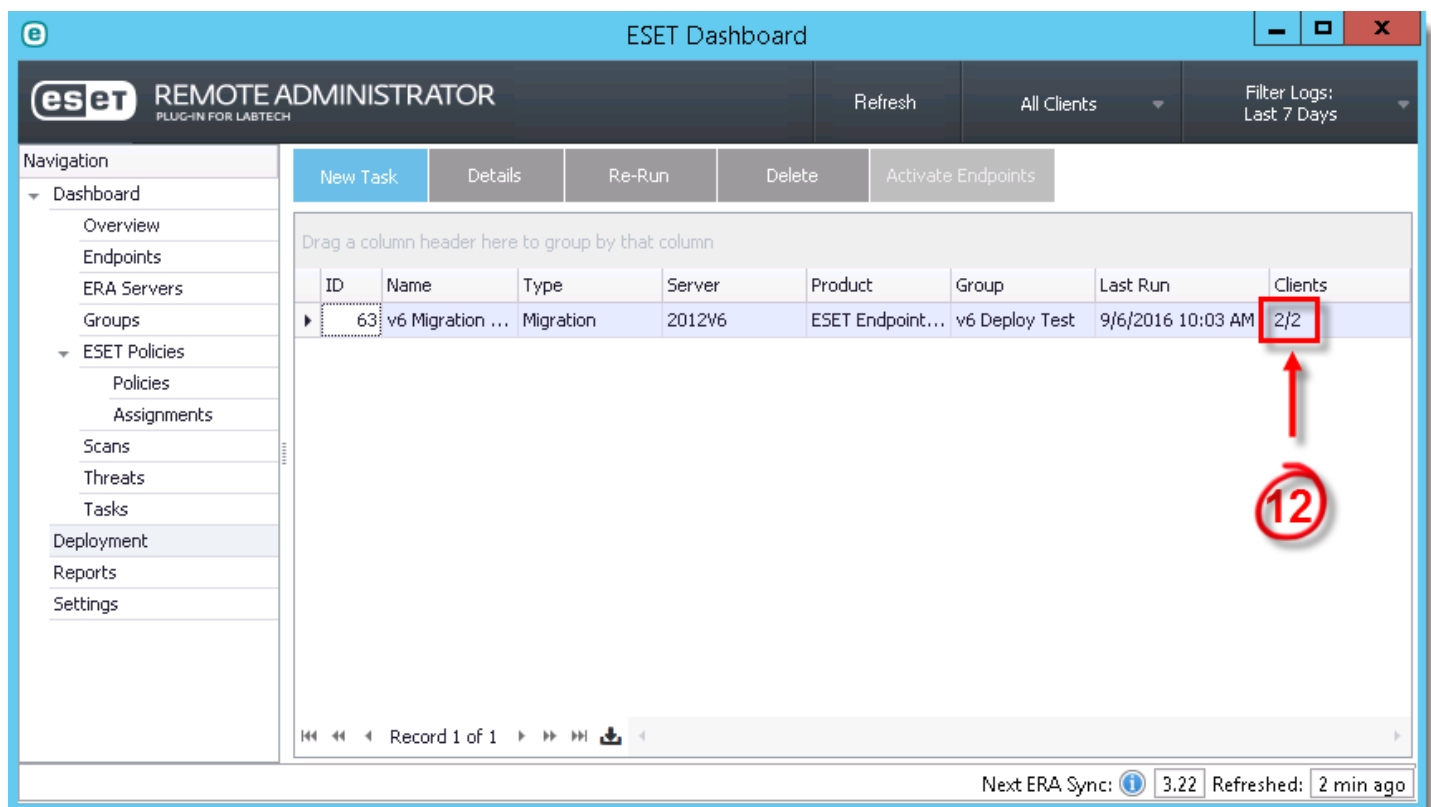


Figure 1-10

13. After the task completes, in the ConnectWise Automate plug-in Navigation menu, click **Endpoints**. The newly migrated devices will still reflect the ERA 5.x version number in the **Version** field. This is a known issue.

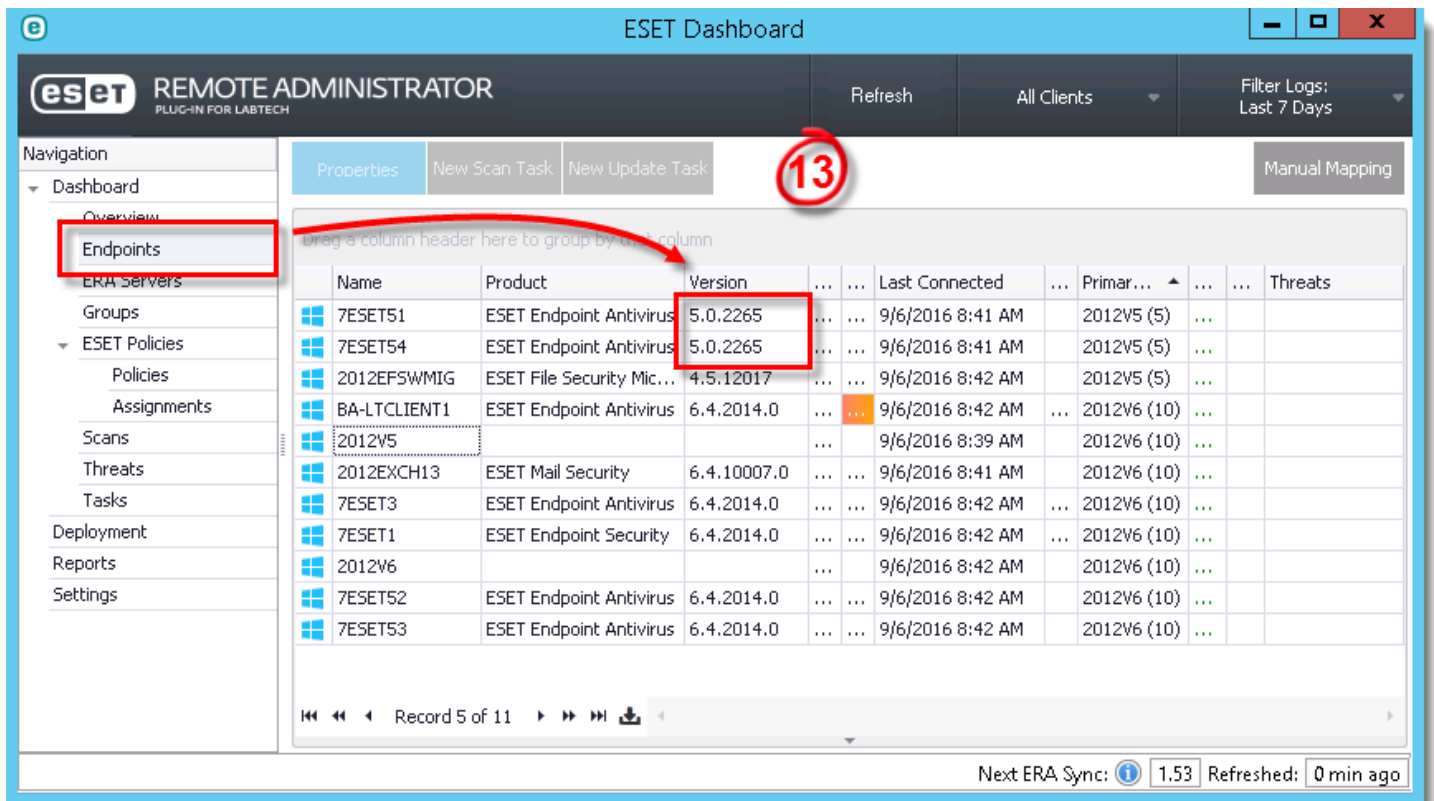


Figure 1-11

14. On your ERA 5.x server, select the devices, right-click and select **Delete**. During the sync cycle, the plug-in will detect the endpoint's new ERA 6.x version number, and update accordingly.

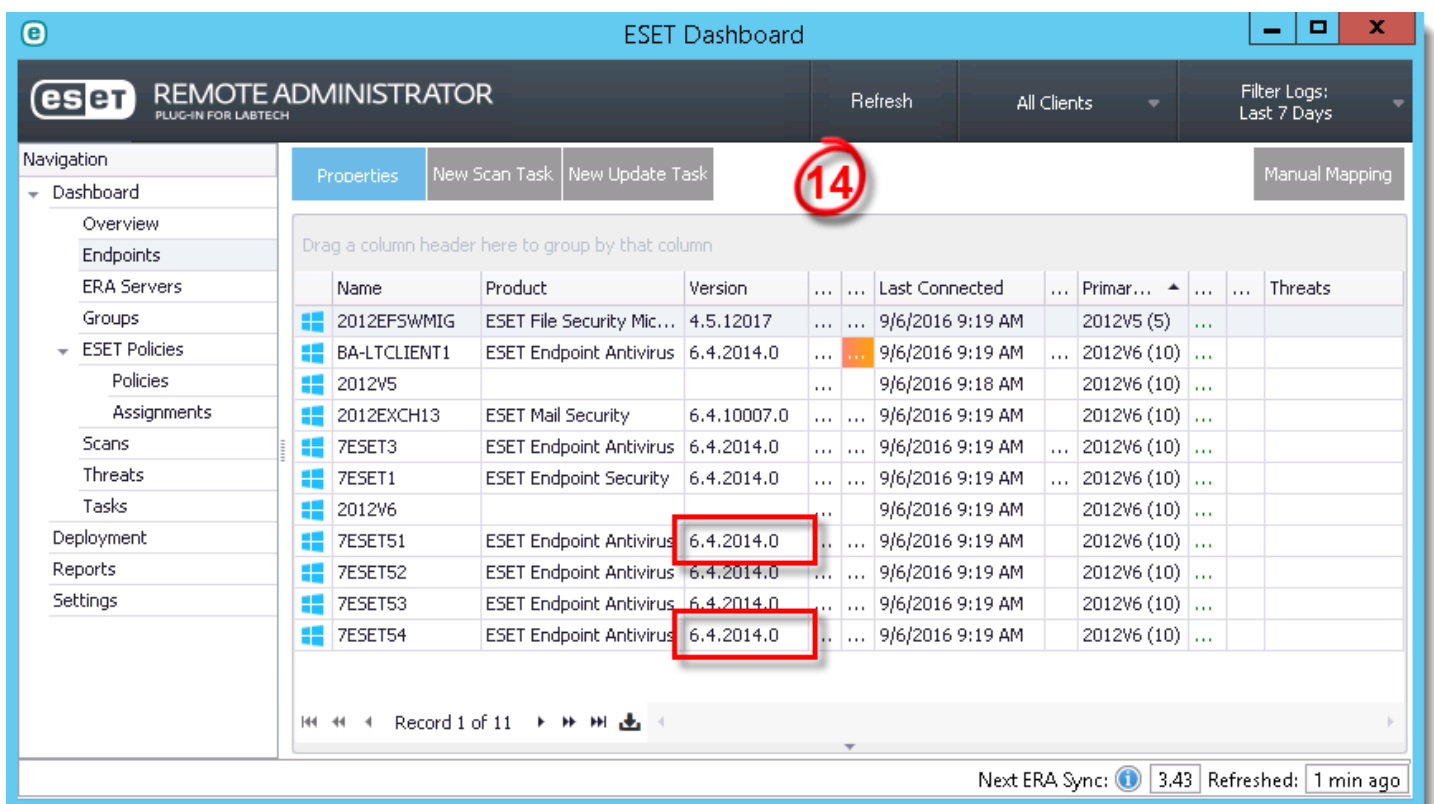


Figure 1-12

The Client Site has been successfully migrated to ERA 6.x.

4. Integrating and Using the ConnectWise Automate Plug-in

To integrate and use the ConnectWise Automate Plug-in:

1. [Install the ERA Plug-in for ConnectWise Automate.](#)
2. [Install your Client Site's ERA Server.](#)
3. [Install the ERA Agent.](#)

4.1 Installing the ERA Plug-in for ConnectWise Automate

Installing the ESET Remote Administrator (ERA) Plug-in for ConnectWise Automate will differ slightly depending on the version of ConnectWise Automate you are using:

- **ConnectWise Automate 10**—[Install the ERA Plug-in from Solution Center](#)
- **ConnectWise Automate 2013**—[Install the ERA Plug-in from Plugin Manager](#)

4.1.1 Install the ERA Plug-in from Solution Center

This method is intended for ConnectWise Automate 10 users.

Users can only access Solution Center from a ConnectWise Automate server. If you do not have access to your ConnectWise Automate server, please contact ConnectWise Automate support for assistance. To install the ERA Plug-in for ConnectWise Automate from Solution Center:

1. On your ConnectWise Automate server, open a new instance of ConnectWise Automate Control Center.
2. Click **Tools > Solution Center**.
3. Click **Security**.
4. Select **ESET Plugin v2** and click **Queue**.

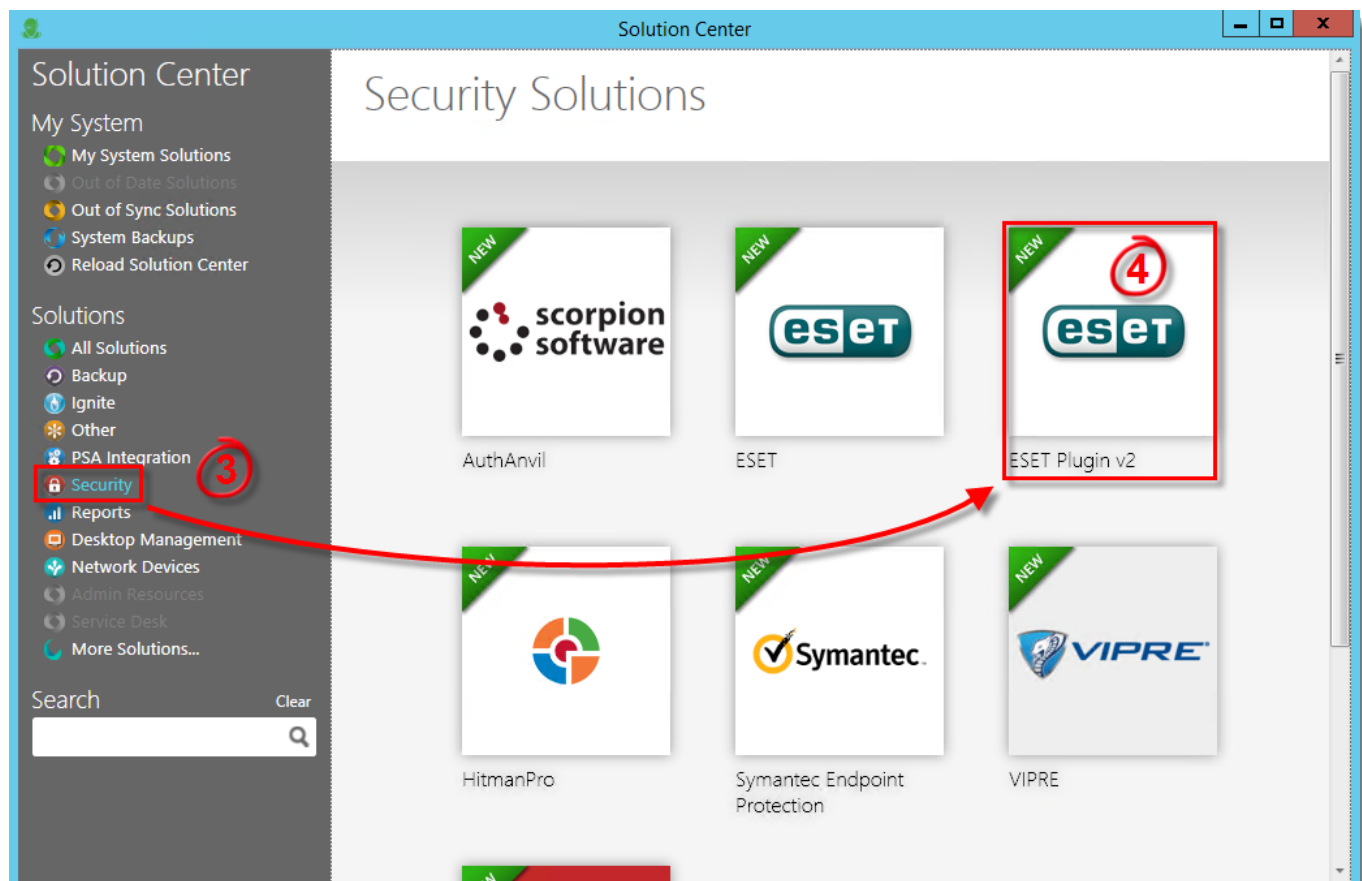


Figure 1-1

5. Click the navigation item **(1) Solution in Queue**.
6. Click **Install/Update**.
7. Specify your backup preferences and then click **Yes** when prompted.
8. Click **Finished** and close Solution Center.
9. Restart any open ConnectWise Automate Control Center instances to allow the new plug-in to load.

4.1.2 Install the ERA Plug-in from Plugin Manager

This method is intended for ConnectWise Automate 2013 users.

To install the ERA Plug-in for ConnectWise Automate from Plugin Manager:

1. Download the latest [ESET Remote Administrator Plug-in for ConnectWise Automate](#).
2. When your download finishes, extract the .zip file to a safe location.
3. Open ConnectWise Automate Control Center and click **Help > Plugin Manager**.
4. Click **Add a Plugin**.

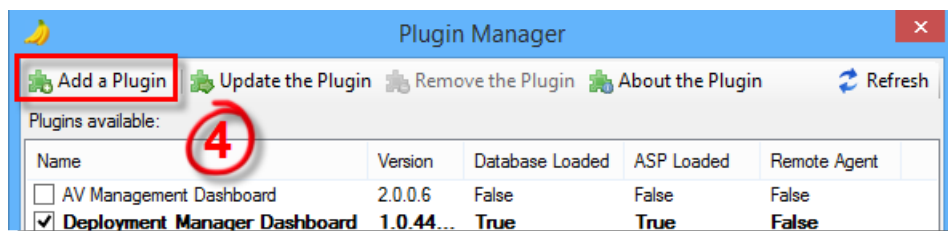


Figure 1-1

5. Navigate to the files you saved in step 2, select **ESET Remote Administrator V2.dll** and click **OK**.
6. Verify the check box next to **Remote Agent** is deselected and click **Save and Close**.

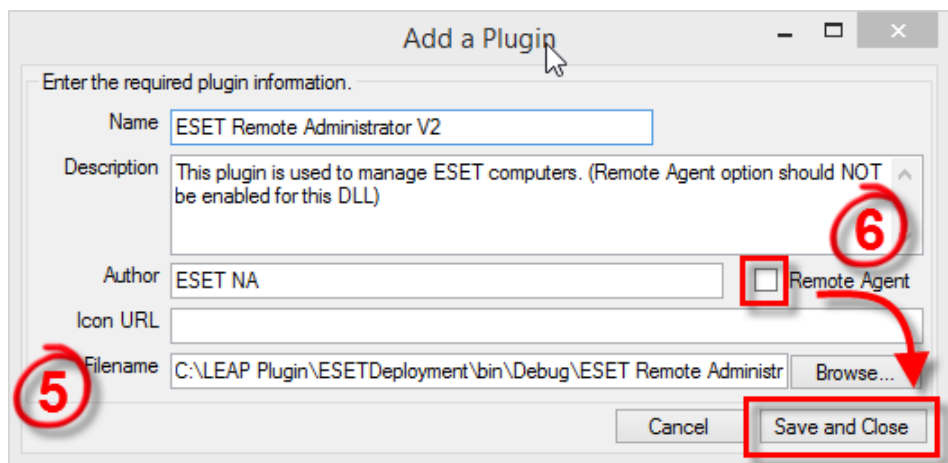


Figure 1-2

7. Click **Add a Plugin**.
8. Navigate to the files you saved in step 2, select **ESET Remote Administrator V2 - Deployment.dll** and click **OK**.

9. Verify the check box next to **Remote Agent** is selected and click **Save and Close**.

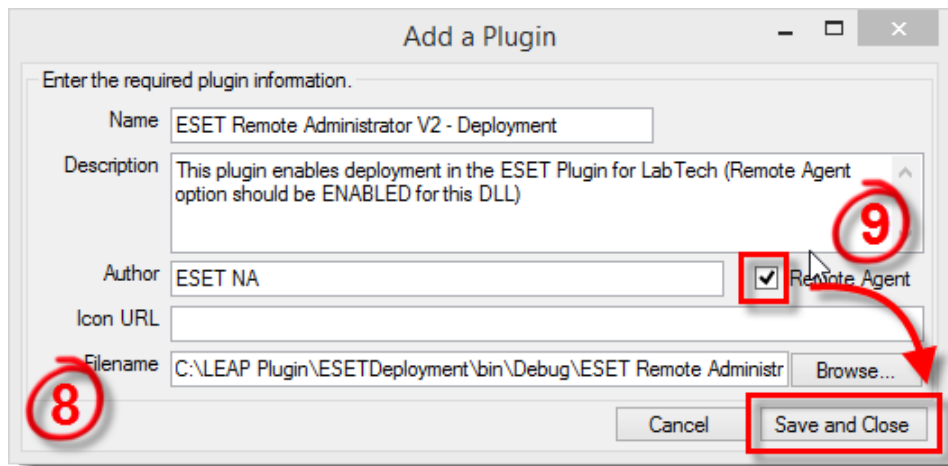


Figure 1-3

10. In ConnectWise Automate Plugin Manager, click **Refresh**.

11. Close ConnectWise Automate Plugin Manager. If you are prompted, click **OK**.

12. Restart the ConnectWise Automate database agent (**Control Center > Help > Server Status > Restart Database Agent**).

13. Restart any open ConnectWise Automate Control Center instances to allow the new plug-in to load.

4.2 Install ERA Server 6.x

Follow the instructions below to install the ESET Remote Administrator (ERA) Server.

NOTE: For those who are migrating from version 5 to 6, ERA Server installation was part of the migration process. Skip to the [Install ERA Agent 6.x](#) section.

If you have already installed and need to activate using a Security Admin, see [Activate ESET Remote Administrator using Security Admin credentials](#).

1. Download and run the [ESET Remote Administrator \(ERA\) Server installer file](#).

NOTE: Occasionally during installation of ERA, the notification "Error code 1603- Installation ended prematurely" will be displayed. Use the following troubleshooting steps to resolve this error:

- If you are running ESET Live Installer from a shared location, copy the live installer file to the local disk and attempt installation again.
- When you run the ERA Agent Live installer, right-click it and select **Run as Administrator** from the context menu.
- If the issue persists, collect and submit logs to ESET Customer Care.

2. Click **Next**.

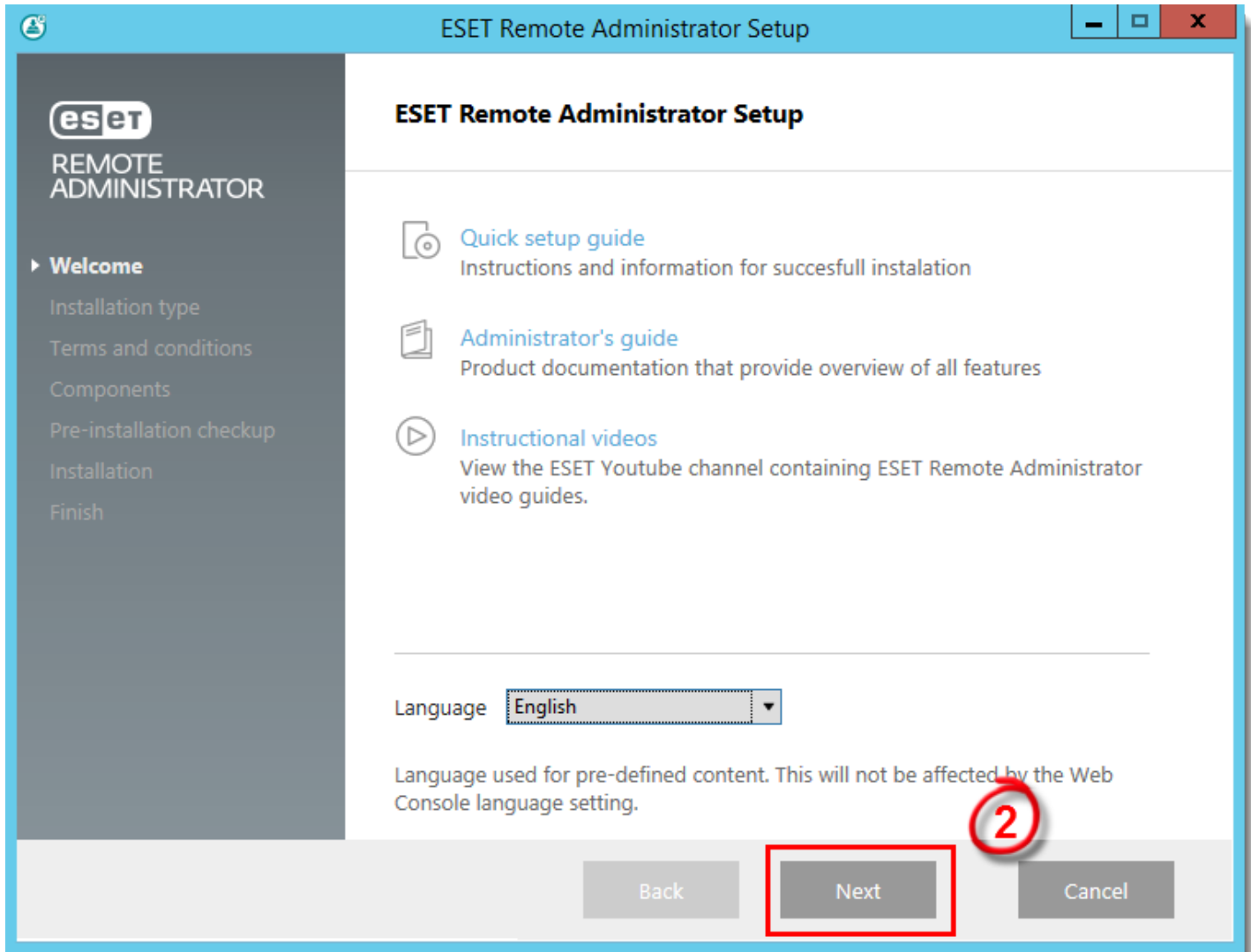


Figure 1-1

3. Select **Install Remote Administrator Server** and click **Next**.

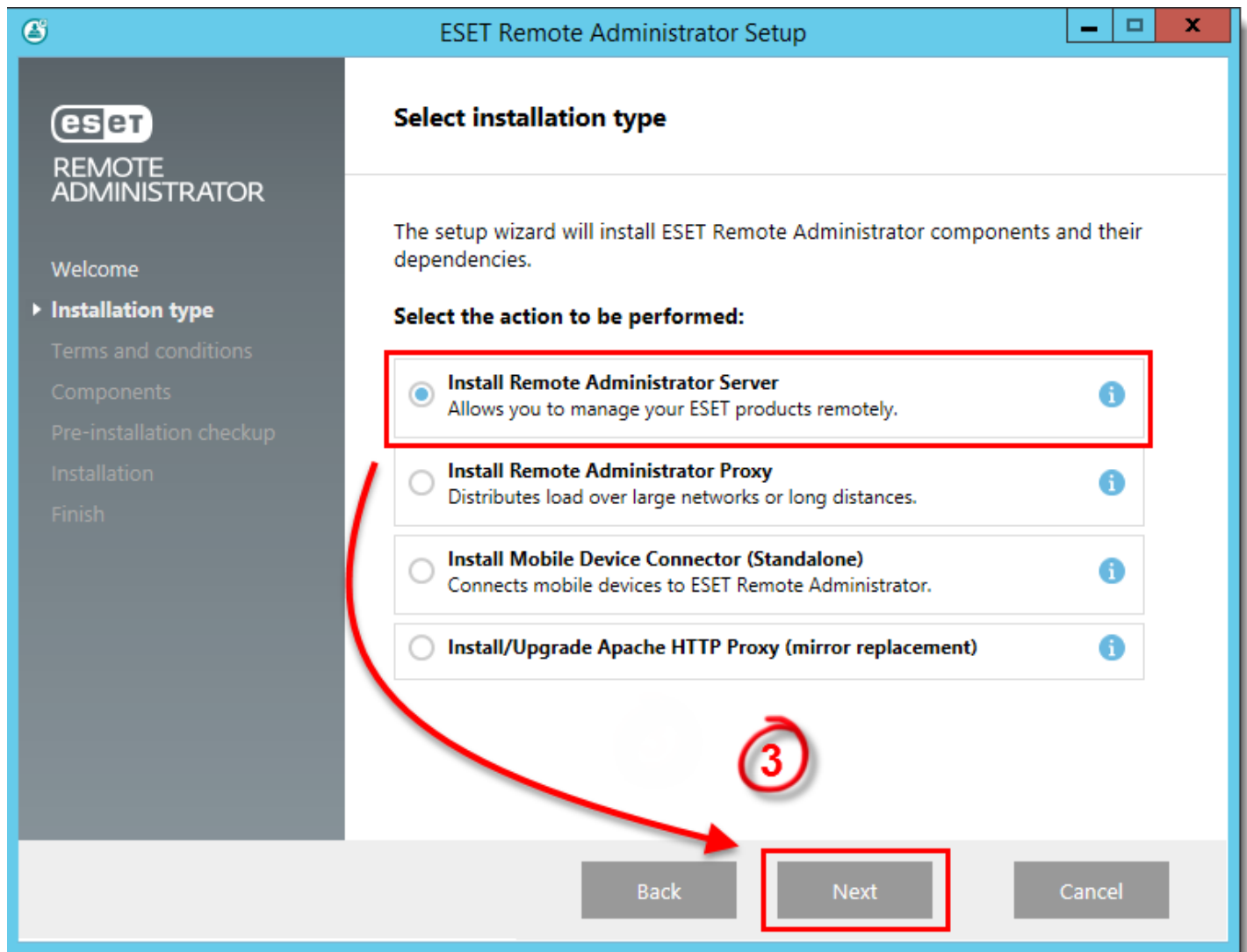


Figure 1-2

4. Read the End-User License Agreement. If you agree, select **I accept the terms in the license agreement** and click **Next**.
5. Your network architecture will determine which components should be installed. Read the descriptions below and deselect the check box next to any components you do not want to install:
 - **Microsoft SQL Server Express:** If you have an existing Microsoft SQL or MySQL database that you will use with ESET Remote Administrator, deselect this check box. Leave this check box selected to create a new Microsoft SQL Server Express database for use with ESET Remote Administrator.
 - **Web Console:** This will install the Apache Tomcat service necessary for ESET Remote Administrator Server to manage clients. This is required.
 - **ESET Mobile Device Connector:** This will install the ESET Mobile Device Connector (EMDC) component, which allows for the remote management of Android and iOS devices. For more information, review the following Knowledgebase article: [Manage mobile devices using ESET Remote Administrator - FAQ \(6.x\)](#).
 - **ESET Rogue Detection Sensor:** This will install ESET Rogue Detection Sensor, a component that helps locate unmanaged computers on your network. It is recommended to leave ESET Rogue Detection Sensor installed; however, this component is not fully operational in an MSP environment due to it being required on each subnet of every Client Site.
 - **Apache HTTP Proxy:** This will install Apache HTTP Proxy, a component used to cache both update definitions and program component updates locally. However, MSPs seldom use this component, as there is no benefit to tunneling clients through the MSPs' internet pipe. Using HTTP Proxy will create and apply several proxy-based policies for clients and apply them automatically, which can affect your ability to download updates. You can [install Apache HTTP Proxy](#) later if you want.

Click **Next** when you are done selecting components. Installation time will vary depending on your system configuration. If a prerequisite is not satisfied or an error occurs, follow the instructions from the installer to resolve any issues.

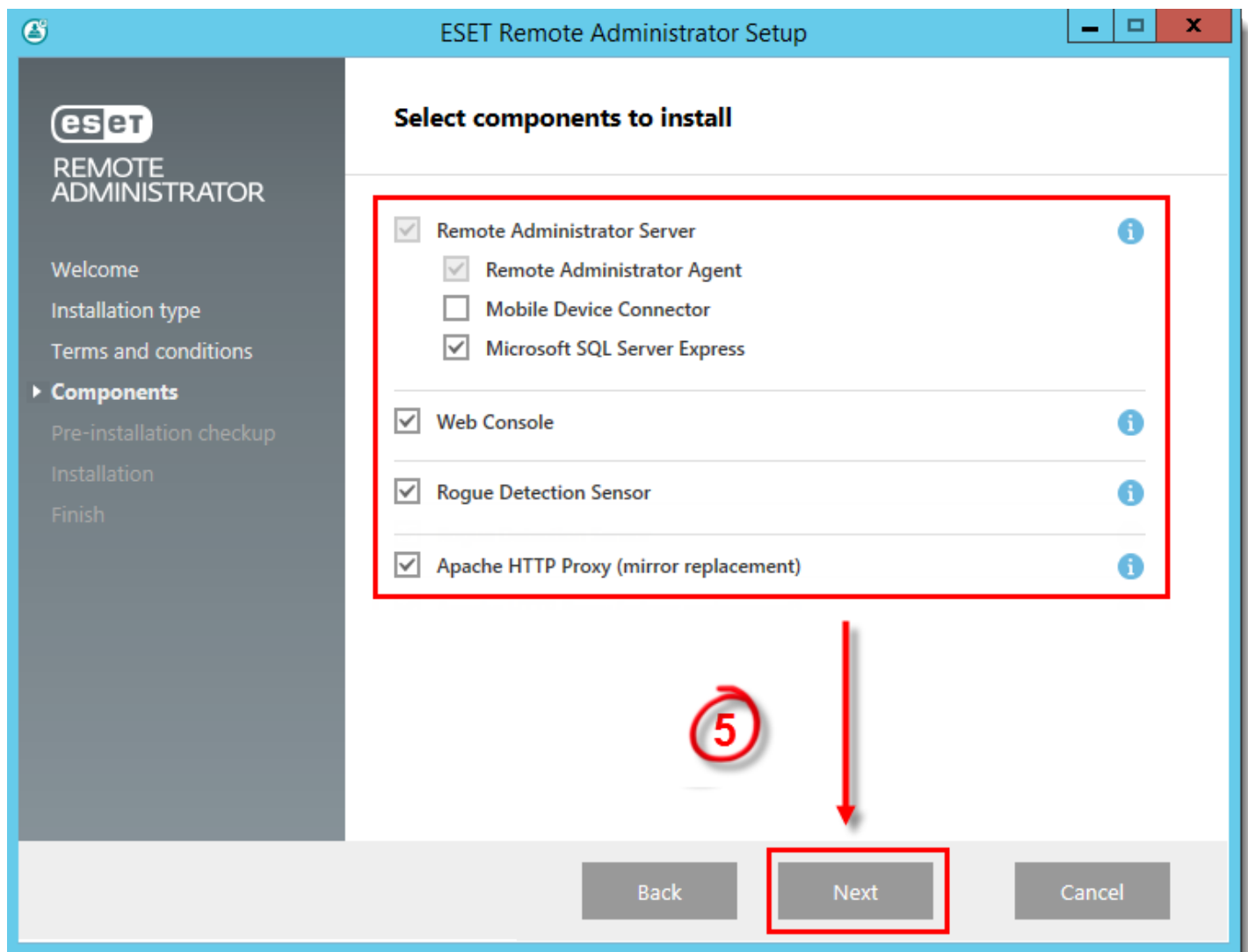


Figure 1-3

6. In the **ESET Remote Administrator Server Setup** window, click **Next**.
7. Select **Activate later**. You will activate using your ConnectWise Automate-provided Security Admin account later.

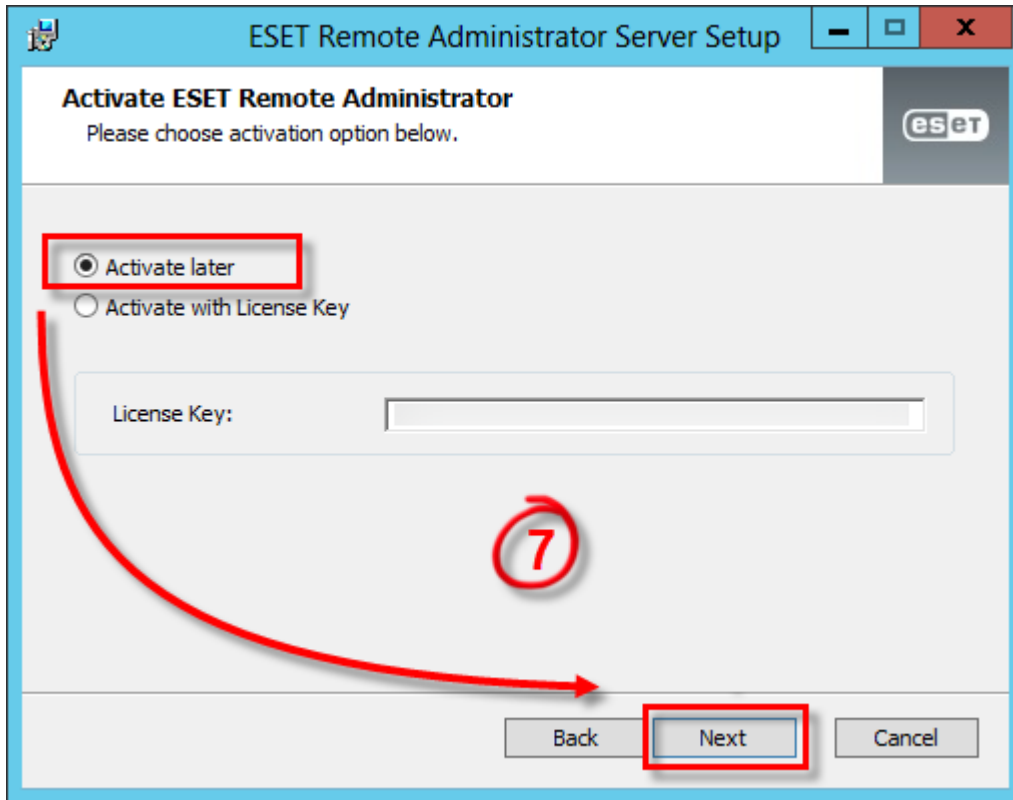


Figure 1-4

8. If you chose to have Microsoft SQL Server Express installed in step 5, click **Next** to perform a database connection check and continue to step 9.

Users with a pre-existing database (MSSQL or MySQL): Select the appropriate database type from the **Database** drop-down menu. Type the **Database name**, **Hostname** and **Port** (you can find this information in SQL Server Configuration Manager) for your database into the appropriate fields and then click **Next**. In the following window, select **Use existing user** and then enter the **Database username** and **Password** if one is used.

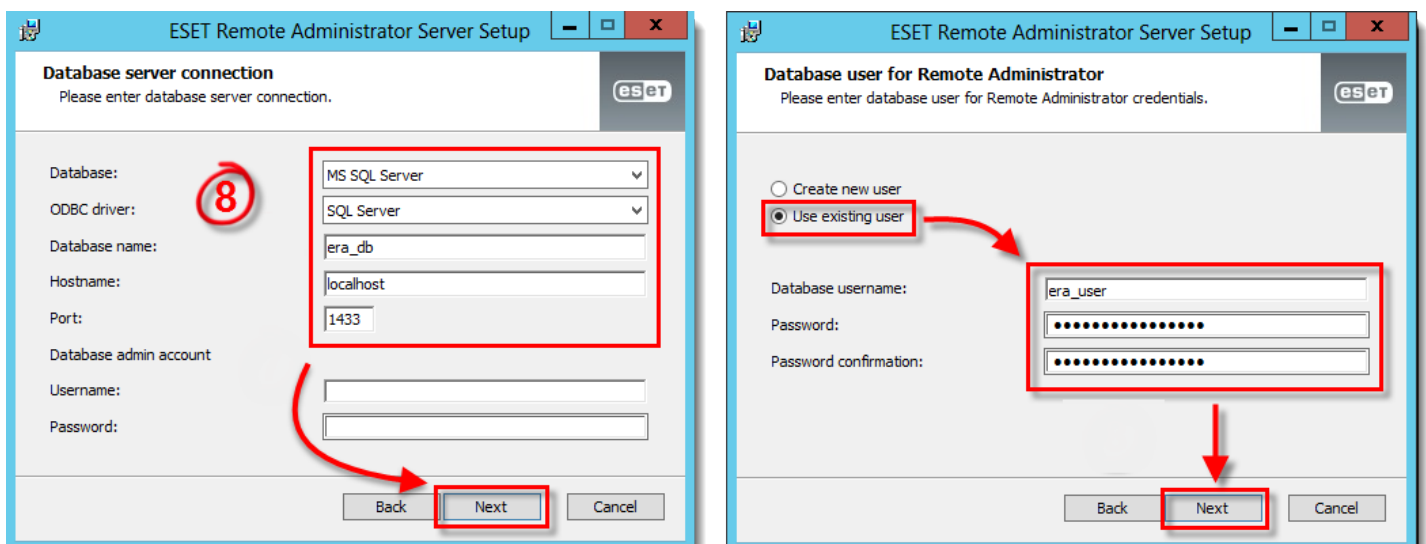


Figure 1-5

9. Type the password you will use to log into ESET Remote Administrator Web Console (ERA Web Console) into the **Password** and **Confirm Password** fields. Make sure to record this password for use later and then click **Next**.

ESET Remote Administrator Server Setup

WebConsole user & server connection
Please enter WebConsole user password and server connection.

WebConsole user: Administrator

Password:

Confirm password:

Agent port:

Console port:

Back **Next** Cancel

Figure 1-6

10. In the **Certificate information** window you will create your ERA Certificate Authority. The only mandatory fields are **Certificate validity** and **Authority common name**. Enter any other applicable information about your certificate authority here and then click **Next**.

NOTE: If a password (not required) is created be sure to record it. All client computers using this specific certificate will require that particular password. If the password is lost, the ERA Agent must be re-deployed.

ESET Remote Administrator Server Setup

Certificate information
Please enter common certificate information below.

Organizational unit:

Organization:

Locality:

State / Country:

Certificate validity: *

Authority common name: *

Authority password:

* required fields

Back **Next** Cancel

Figure 1-7

11. Click **Install**.

12. In the **Installation successful** window, click the Web Console link and log in. We recommend you bookmark or make note of this URL for future reference. By default, the ERA installer will create a link to the ERA Web Console in your Start menu. [How do I open ERA Web Console?](#)

NOTE: ERA does not provide threat protection for your server. We recommend you [install ESET File Security for Microsoft Windows Server](#) to protect your ERA Server before you continue with deployment of ESET solutions on your network.

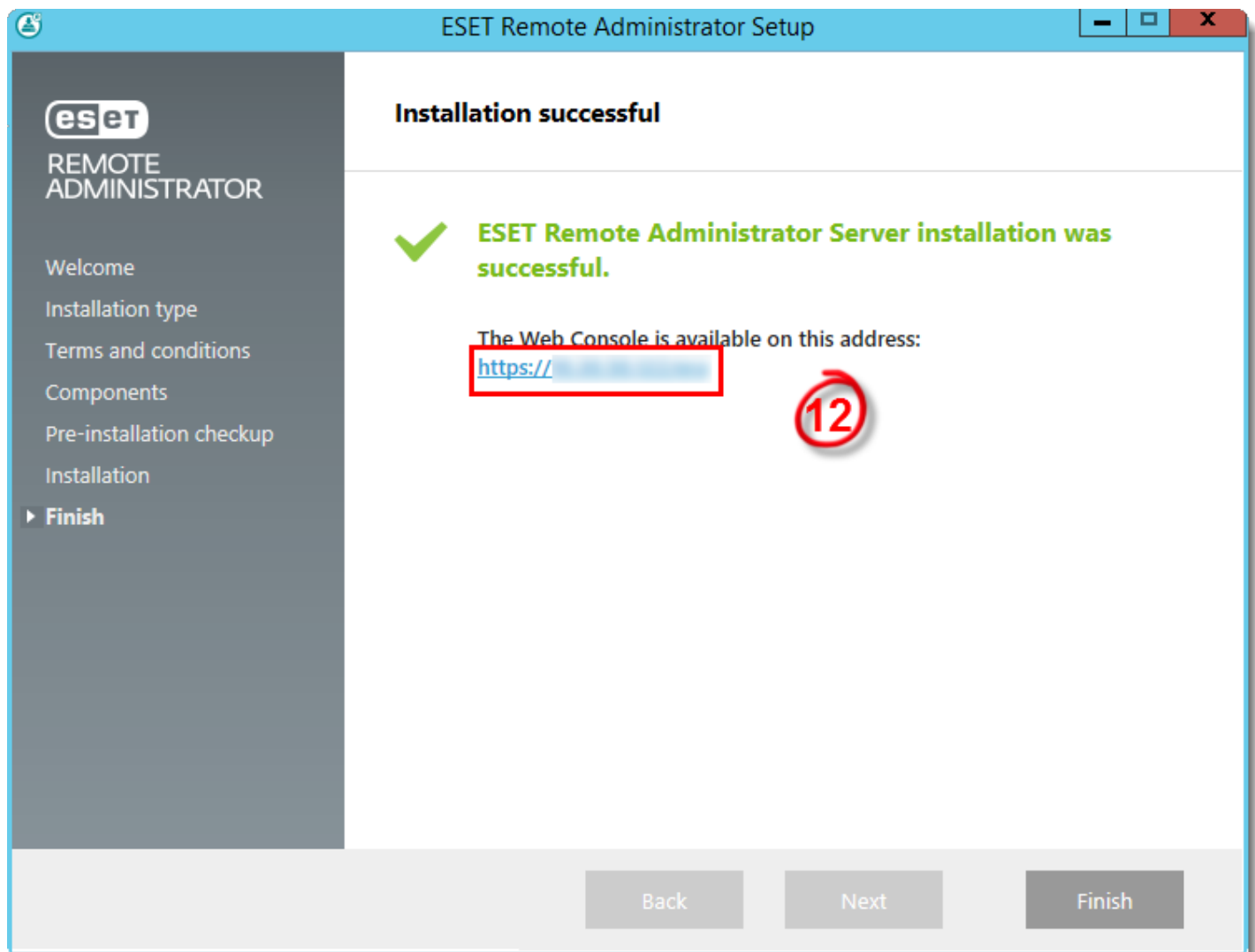


Figure 1-8

You have successfully installed ERA Server 6.x.

Activate ESET Remote Administrator using Security Admin credentials

The ERA Plug-in for ConnectWise Automate connects to ELA using the [Security Admin account](#) to retrieve license credentials. After installing ERA Server, activate your products using your Security Admin account.

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in. [How do I open ERA Web Console?](#)
2. Click **Admin > License Management**.
3. Click **Add Licenses**, expand **Security Admin Credentials**, type your **Security Admin Login** and **Password** into the appropriate fields and click **Add Licenses**.

< BACK Add License - Security Admin Credentials

+ LICENSE KEY

- SECURITY ADMIN CREDENTIALS

SECURITY ADMIN LOGIN

PASSWORD

SHOW PASSWORD

+ LICENSE FILE

3

ADD LICENSES CANCEL

Figure 1-9

For more information about authorizing a Security Admin in ELA, see [Assign Security Admin credentials](#).

4.3 Install ERA Agent 6.x

To create a new peer certificate, dynamic group and Agent Live Installer in the ESET Remote Administrator (ERA) Web Console for ERA Agent installation:

NOTE: As part of the installation process, ESET Remote Administrator (ERA) requires you to create a peer certificate for Agents. Certificates are used to authenticate products distributed under your license, identify computers on your network, allow secure communication between your ERA Server and clients, and establish a secured connection for the ERA Web Console. In some cases, you might also want to create a new certificate, for example, a client site, which allows for automatic grouping and ERA 6.x automation, in general. We recommend creating a custom agent certificate per client site.

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in.
2. Create a new peer certificate.
 - a. Click **Admin > Certificates > New > Certificate**.

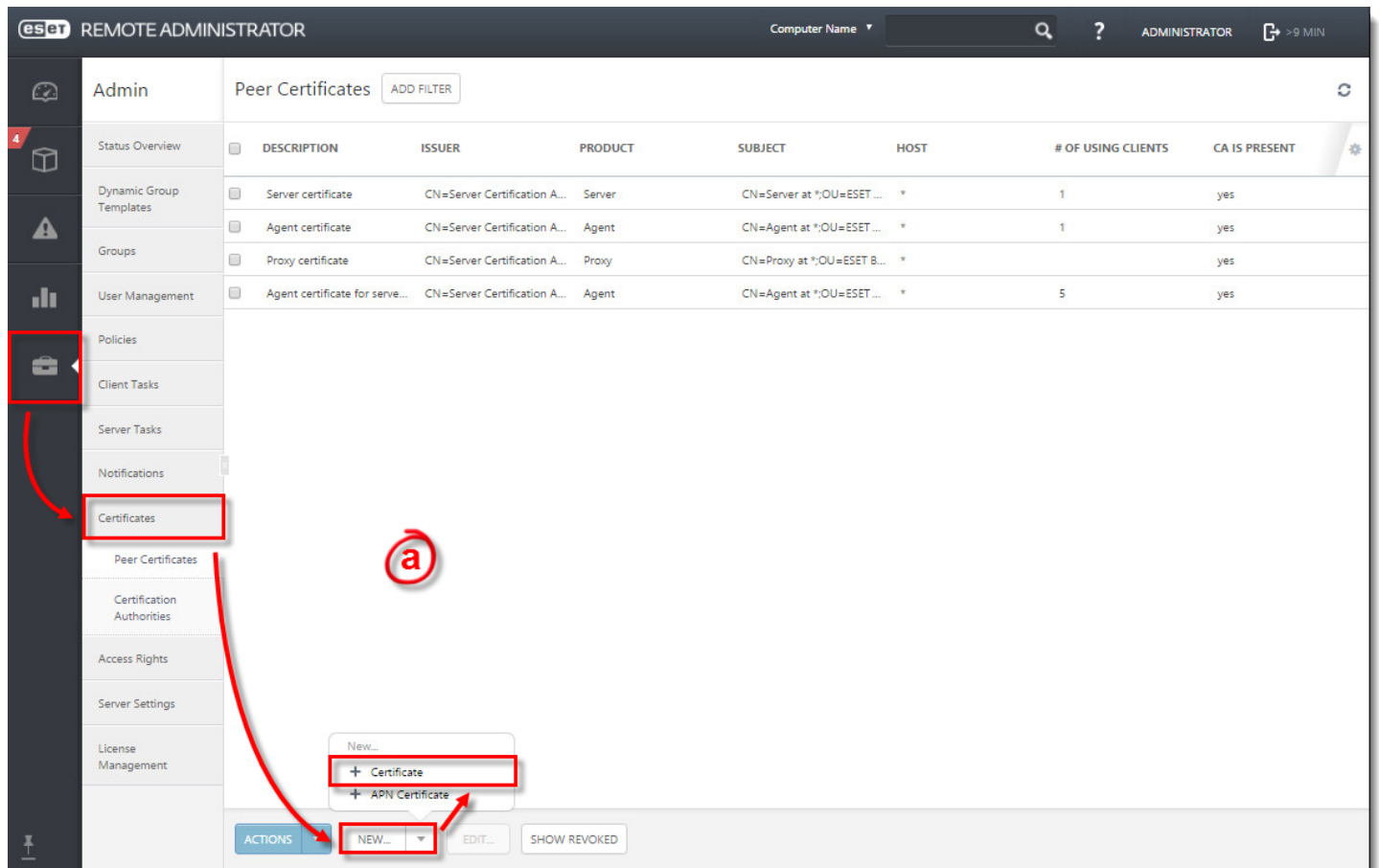


Figure 1-1

- b. In the **Basic** section, complete the following :
 - **Description:** For ease of administration, type the Client Site name.
 - **Product:** Select the applicable certificate from the drop-down menu.
 - **Host:** Leave the default value (an asterisk) in the Host field to allow for distribution of this certificate with no association to a specific DNS name or IP address.
 - **Passphrase:** We recommend you leave this field blank, but if desired you can set a passphrase for the certificate that will be required when clients attempt to activate.

eset REMOTE ADMINISTRATOR Computer Name [] ? ADMINISTRATOR >9 MIN

< BACK Create Certificate - Basic **b**

BASIC

DESCRIPTION Acme

PRODUCT Agent

HOST *

PASSPHRASE

CONFIRM PASSPHRASE

SHOW PASSPHRASE

ATTRIBUTES (SUBJECT)

COMMON NAME Agent certificate for host *

COUNTRY CODE

STATE OR PROVINCE

LOCALITY NAME

ORGANIZATION NAME

FINISH MANDATORY SETTINGS > CANCEL

Figure 1-2

- c. Expand **Sign**. Next to **Certification Authority**, click <Select Certification Authority>.

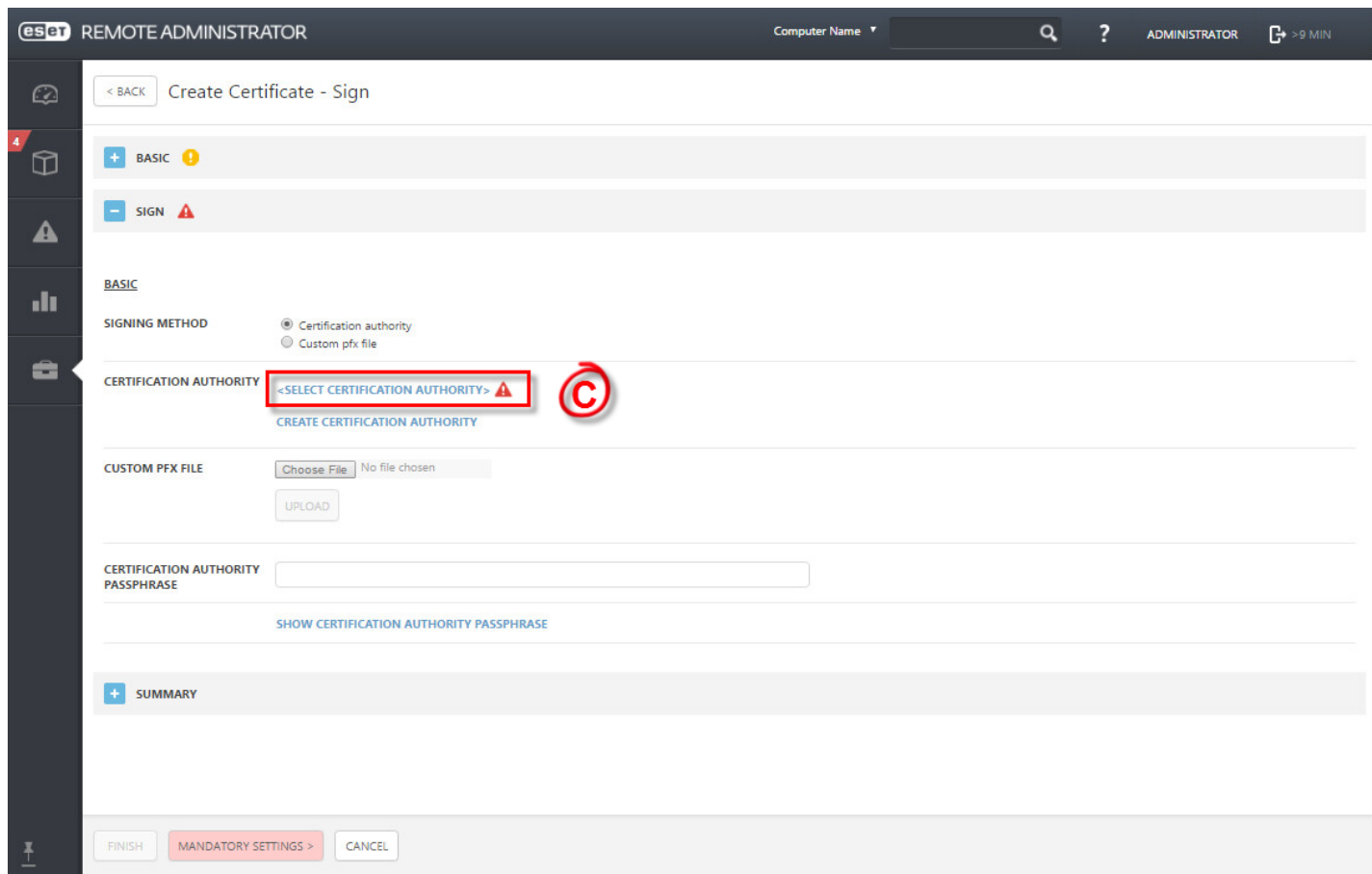


Figure 1-3

- d. Select the ERA Certification authority created during ERA install and click **OK**.

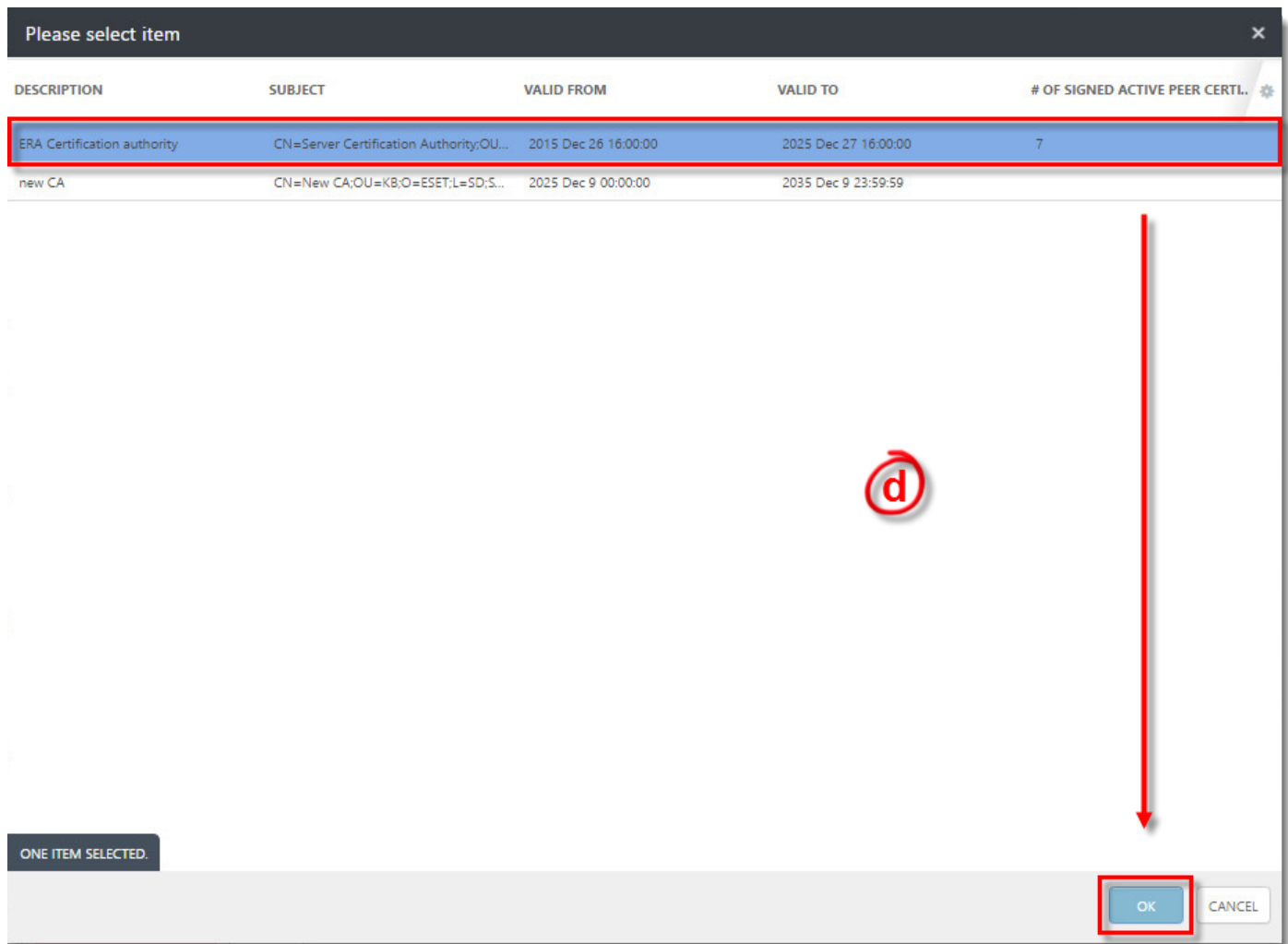


Figure 1-4

e. Click **Finish**. Your new certificate will be displayed in the list of peer certificates.

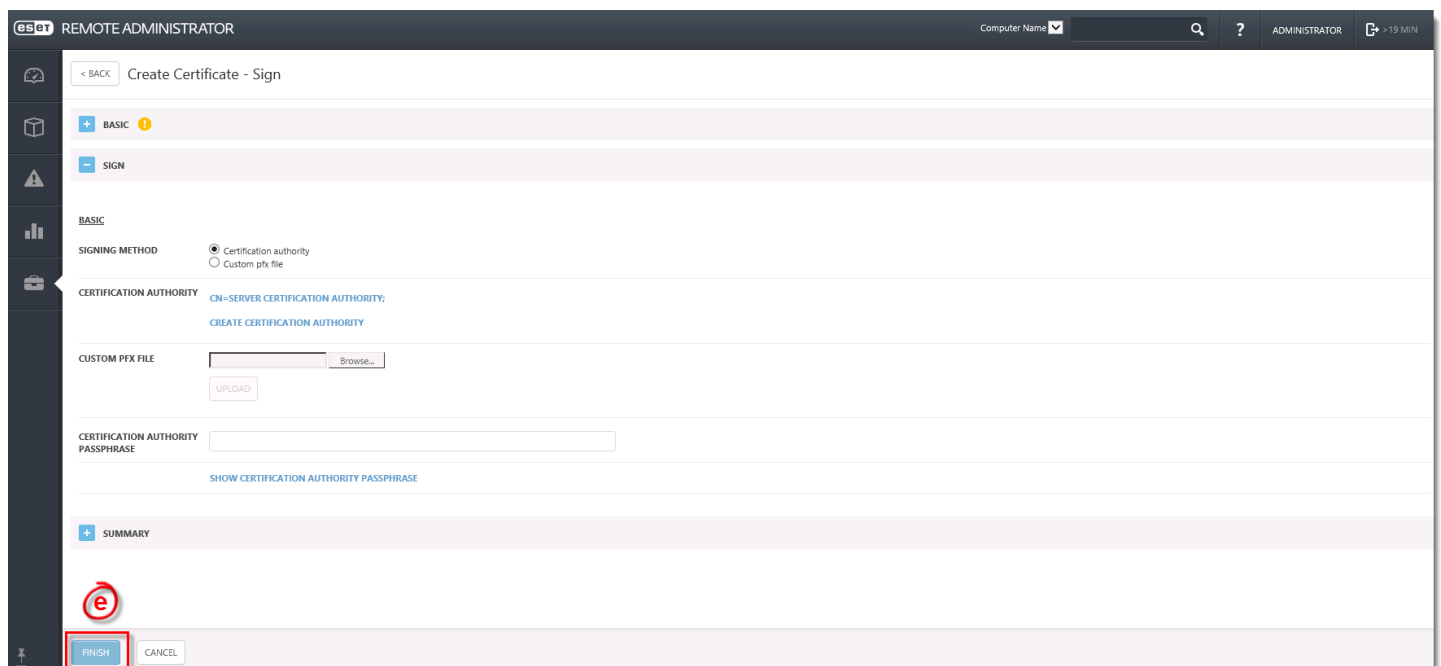


Figure 1-5

f. In the **Peer Certificates** list, select the new certificate and click **Edit**.

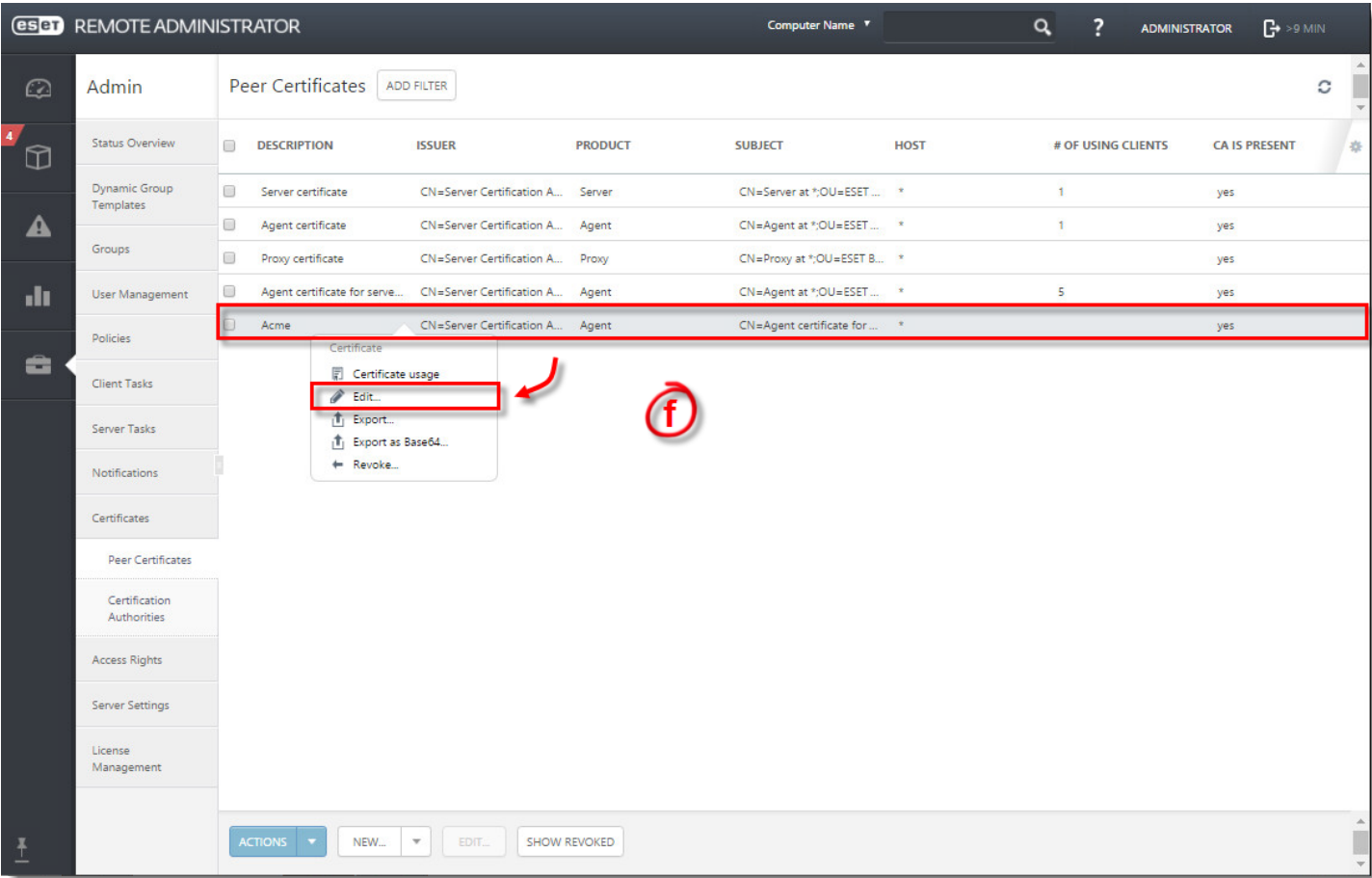


Figure 1-6

g. Copy the number displayed in the **Serial Number** field.

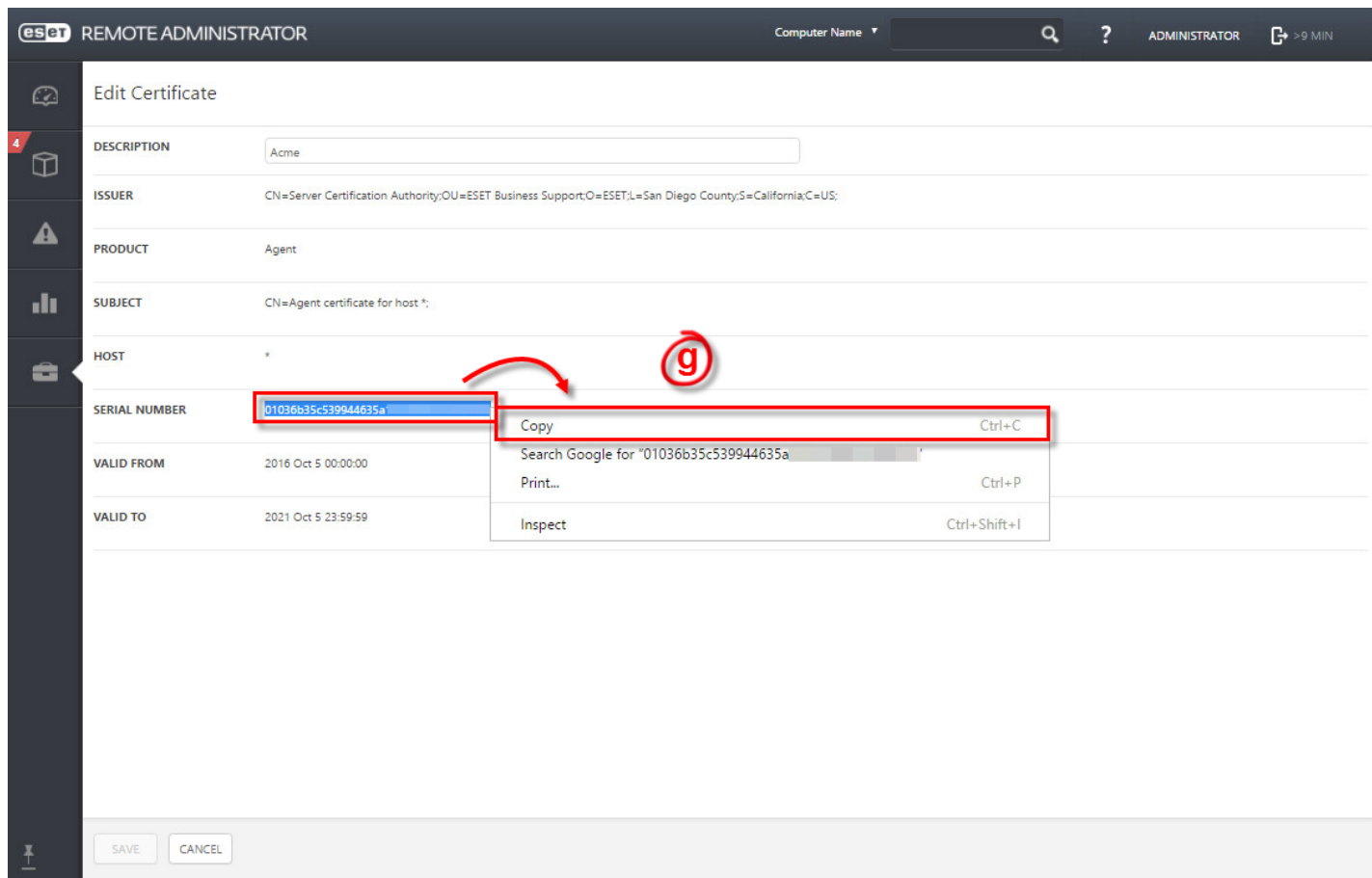


Figure 1-7

3. Create a new dynamic group.

- a. Click **Computers**, click the gear icon next to **All** and then select **New Dynamic Group**.

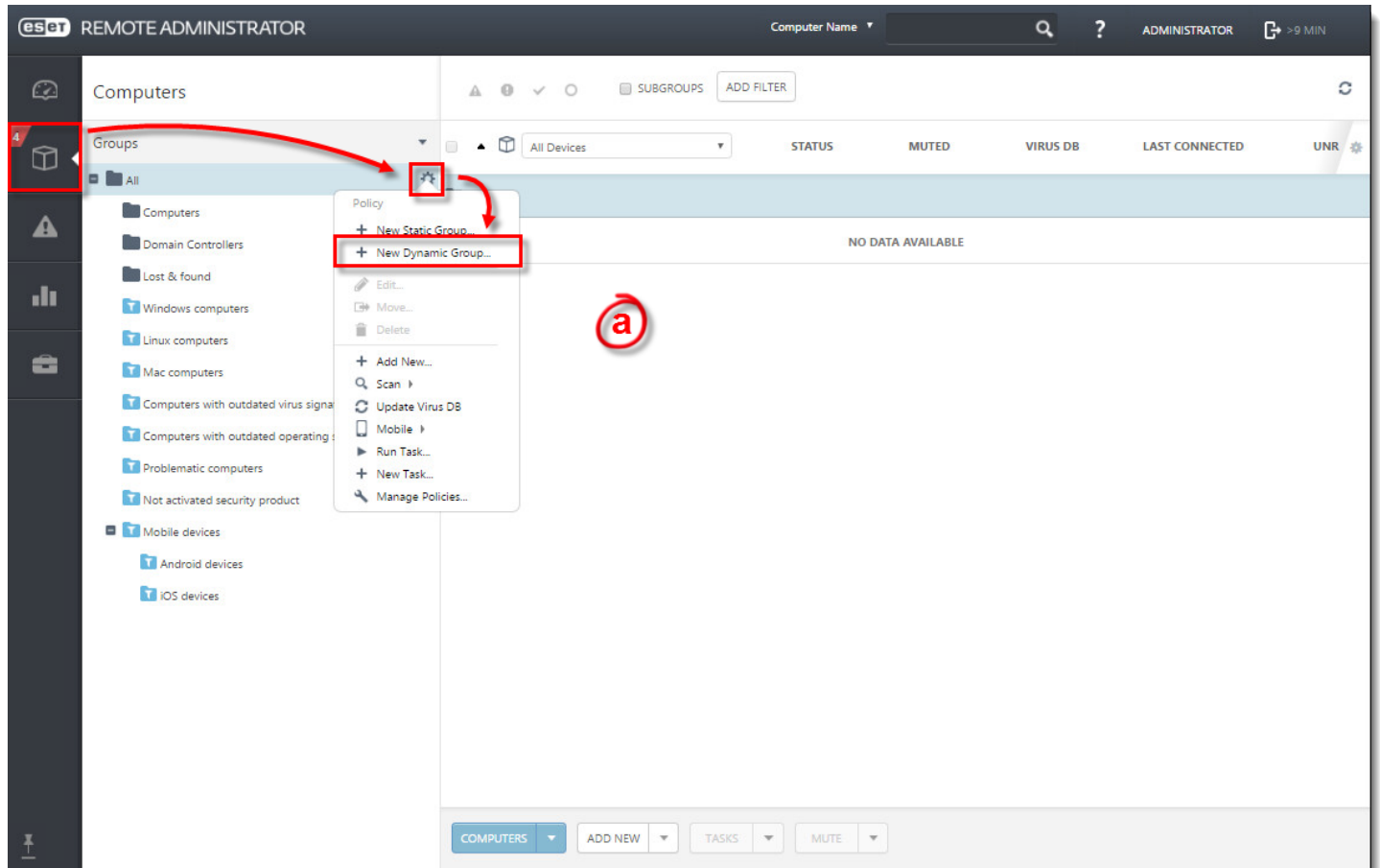


Figure 1-8

- b. In the **Name** field, type the Client Site name for ease of administration.

esct REMOTE ADMINISTRATOR Computer Name [] ? ADMINISTRATOR >9 MIN

< BACK New Dynamic Group - Basic

4

BASIC

NAME [Acme] **b**

DESCRIPTION []

PARENT GROUP All

CHANGE PARENT GROUP

+ TEMPLATE ⚠

+ SUMMARY

FINISH MANDATORY SETTINGS > CANCEL

Figure 1-9

- c. Expand **Template** and click **New**.

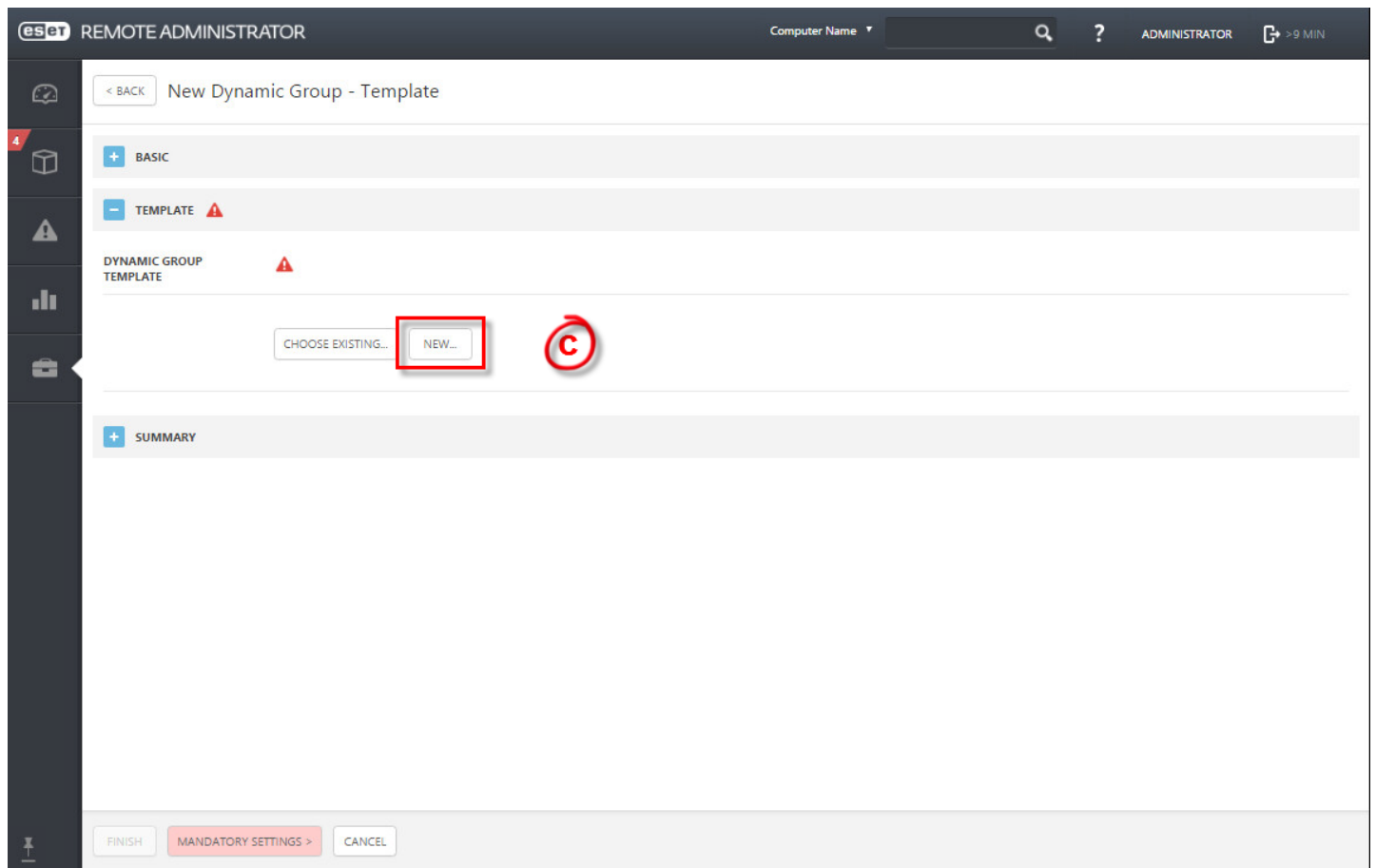


Figure 1-10

- d. In the **Name** field, type the Client Site name for ease of administration.

[< BACK](#) New Template - Basic

— BASIC

NAME

Acme

DESCRIPTION

+ EXPRESSION

FINISH

CANCEL

Figure 1-11

- e. Expand **Expression** and click **Add Rule**.

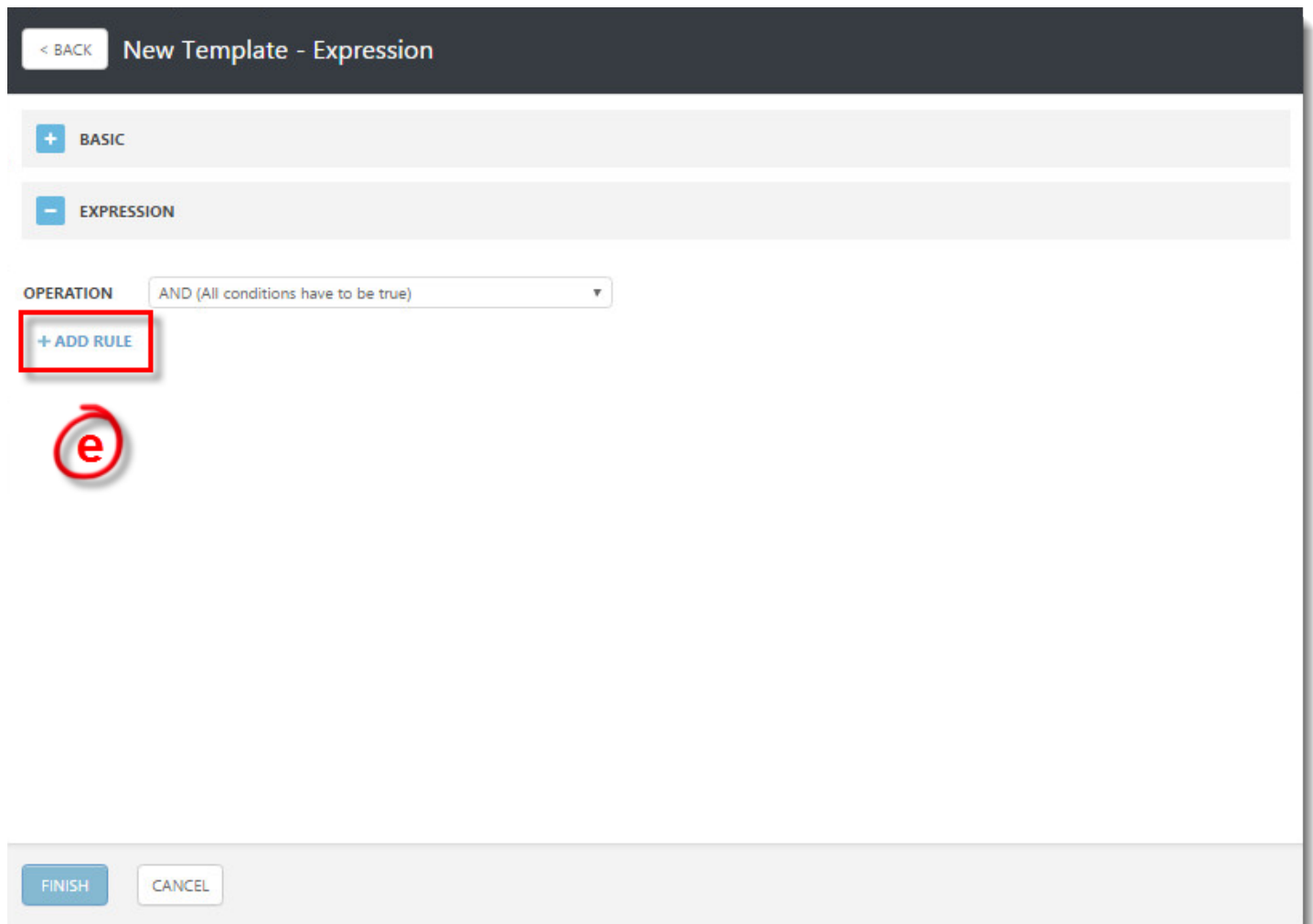


Figure 1-12

- f. To create a dynamic group that filters on the Client Site Certificate Serial Number, expand **Peer Certificate**, select **Serial Number** and then click **OK**.

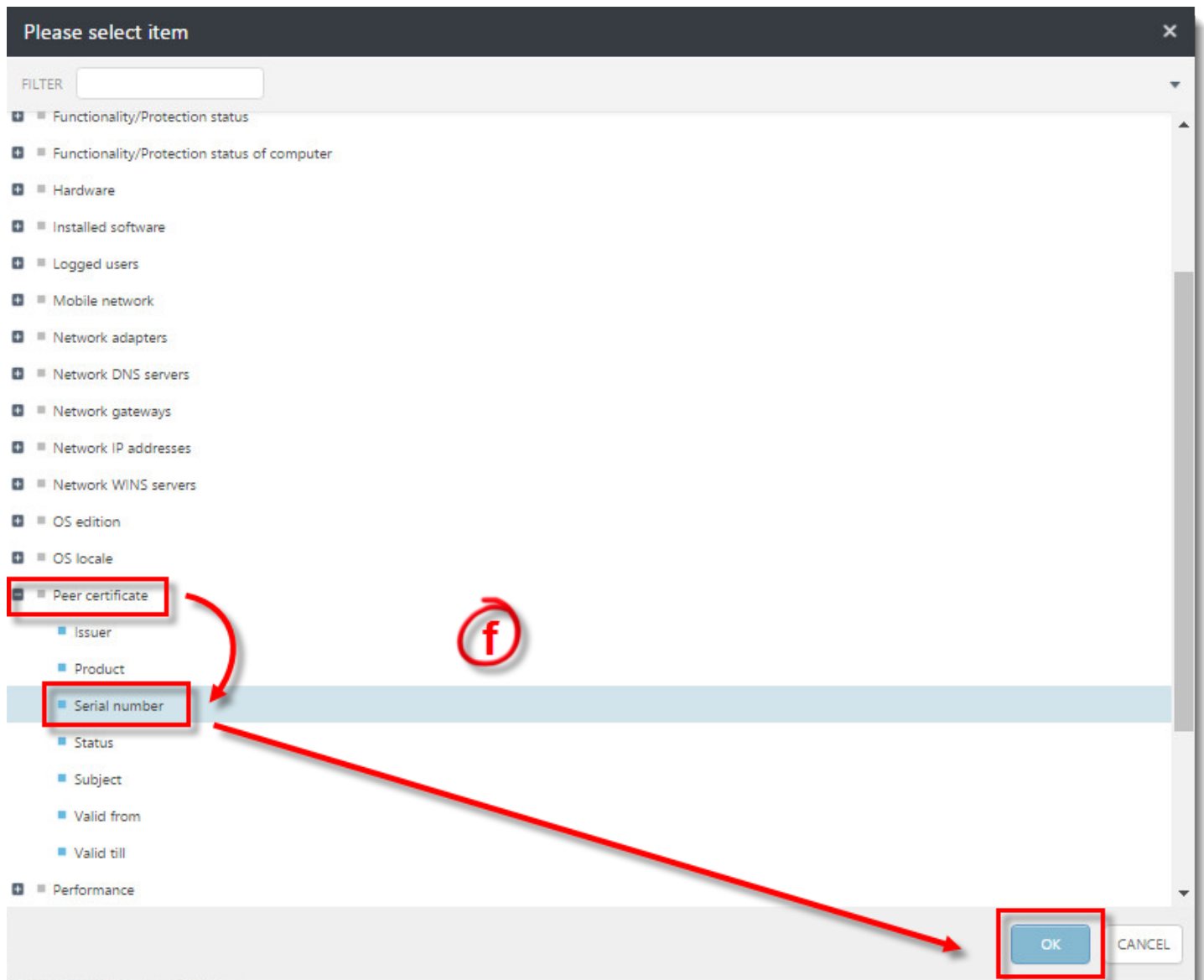


Figure 1-13

g. Paste the serial number you copied in step 2-g into its respective field and click **Finish**.

< BACK New Template - Expression

+ BASIC

- EXPRESSION

OPERATION AND (All conditions have to be true)

Peer certificate . Serial number = (equal) 01036b35c539944635a

+ ADD RULE

g

FINISH CANCEL

Figure 1-14

- h. Click **Finish**. Your new dynamic group will appear in the list of groups.

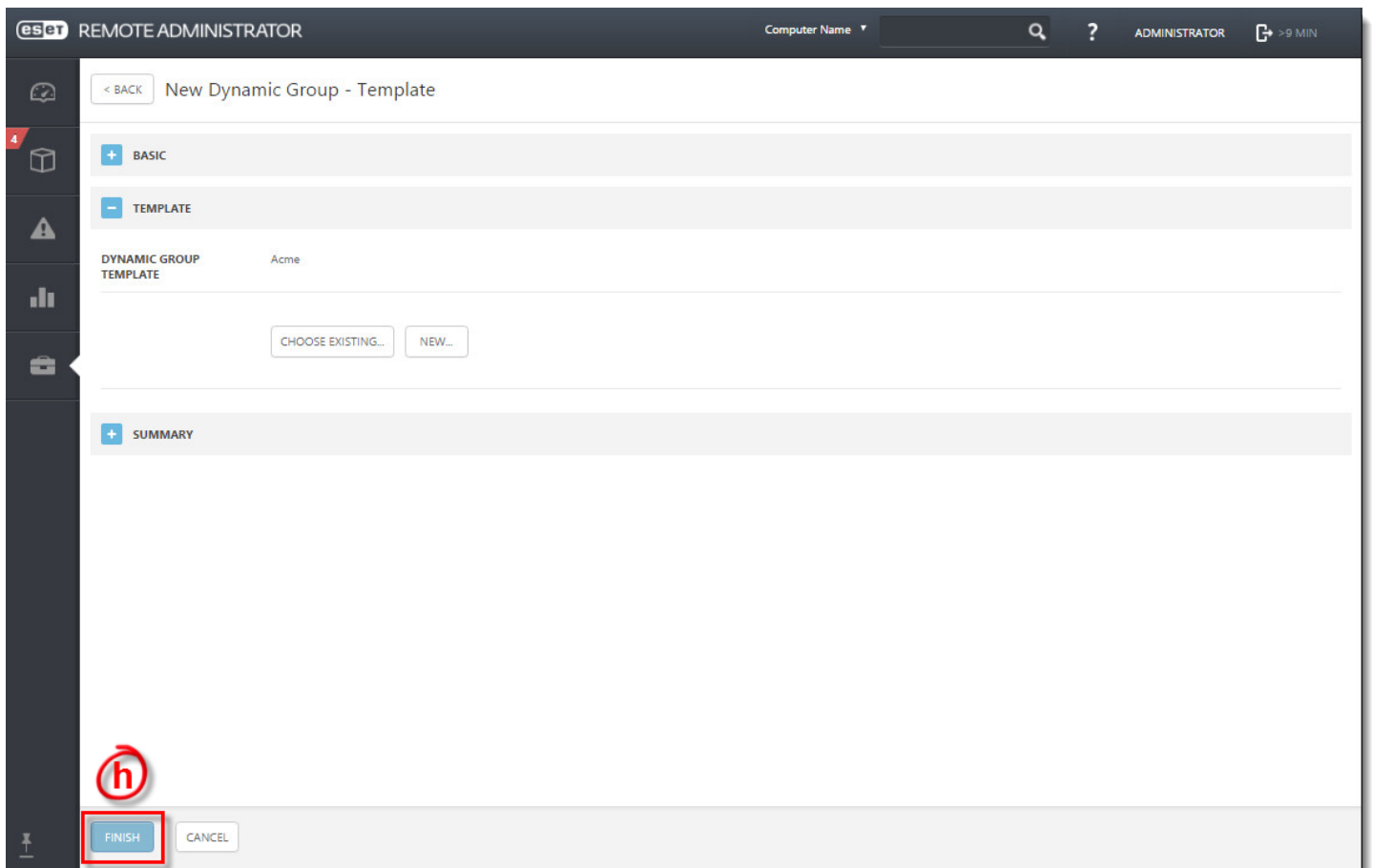


Figure 1-15

4. Create an Agent Live Installer for the Client Site.
 - a. In the **Quick Links** section, click **Deploy ERA Agent**.

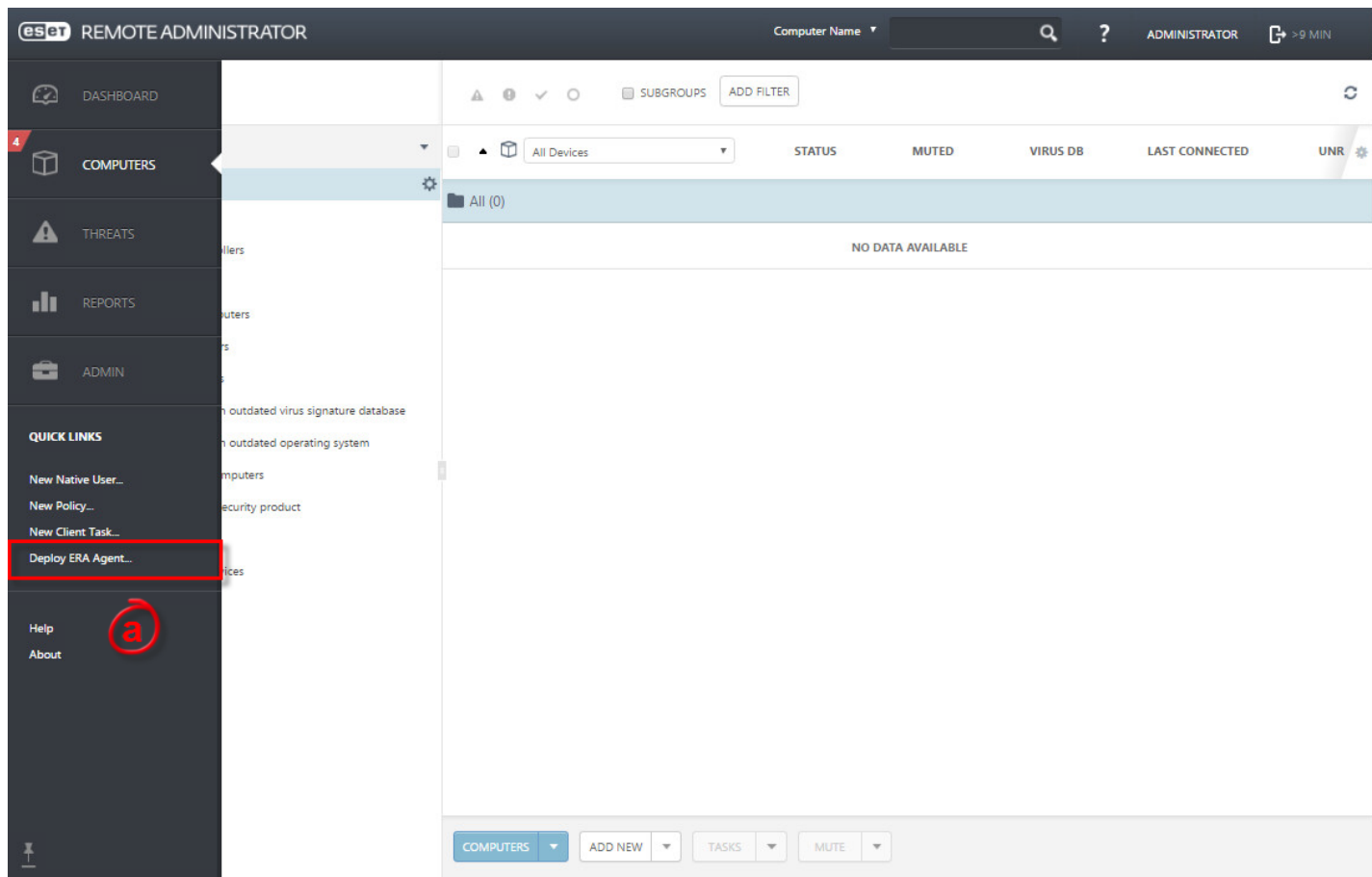


Figure 1-16

- b. In the **Local Deployment** section, under **Create Agent Live Installer**, click **Create Installer**.

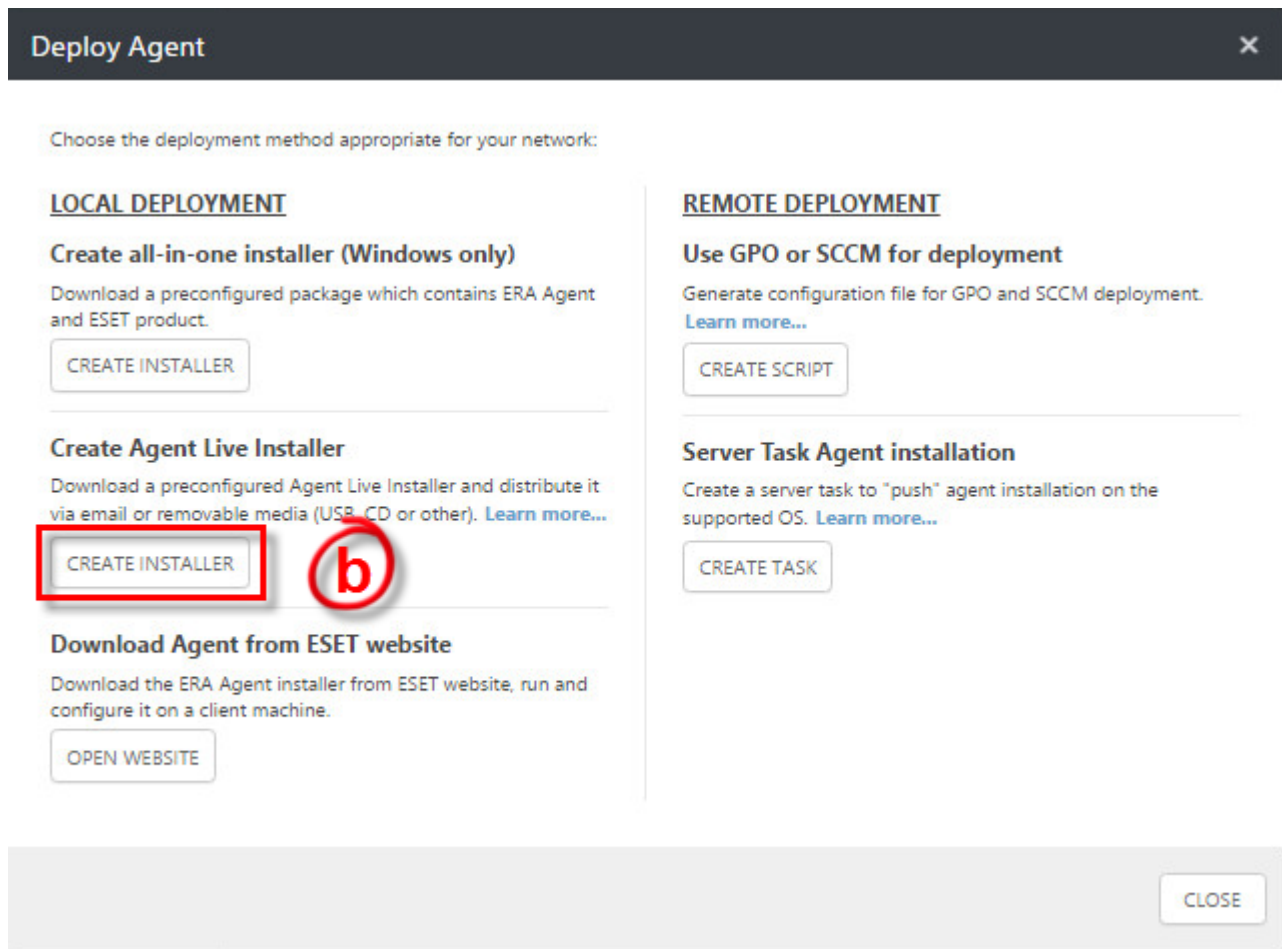


Figure 1-17

- c. Next to the **ERA Certificate**, click the link to select the appropriate Agent Certificate and then click **OK**.

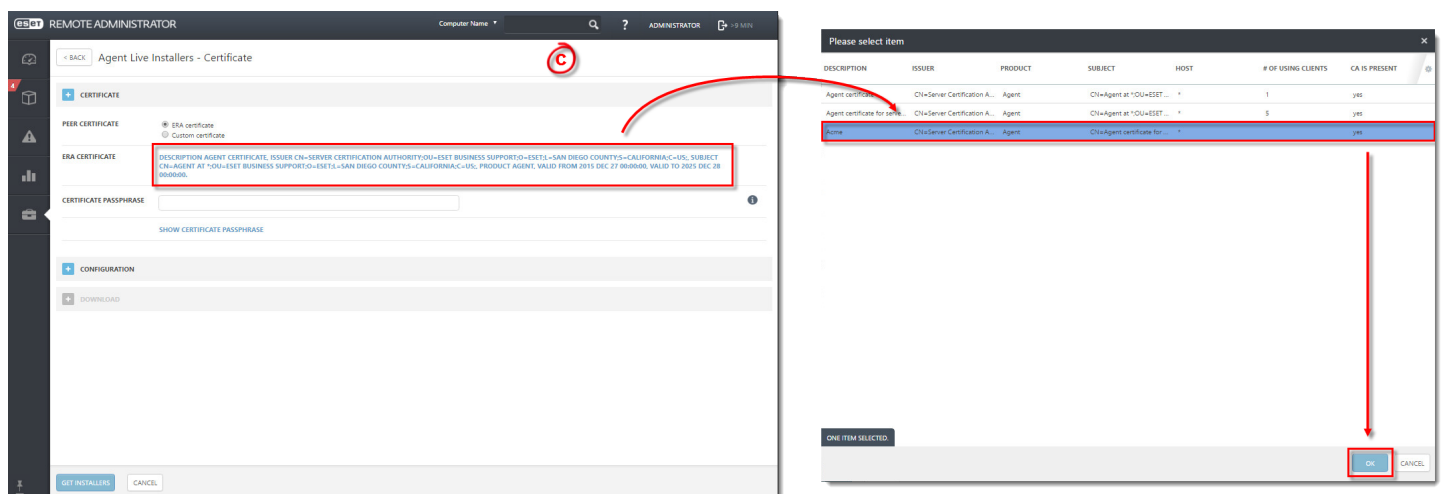


Figure 1-18

- d. Click **Get Installers**.

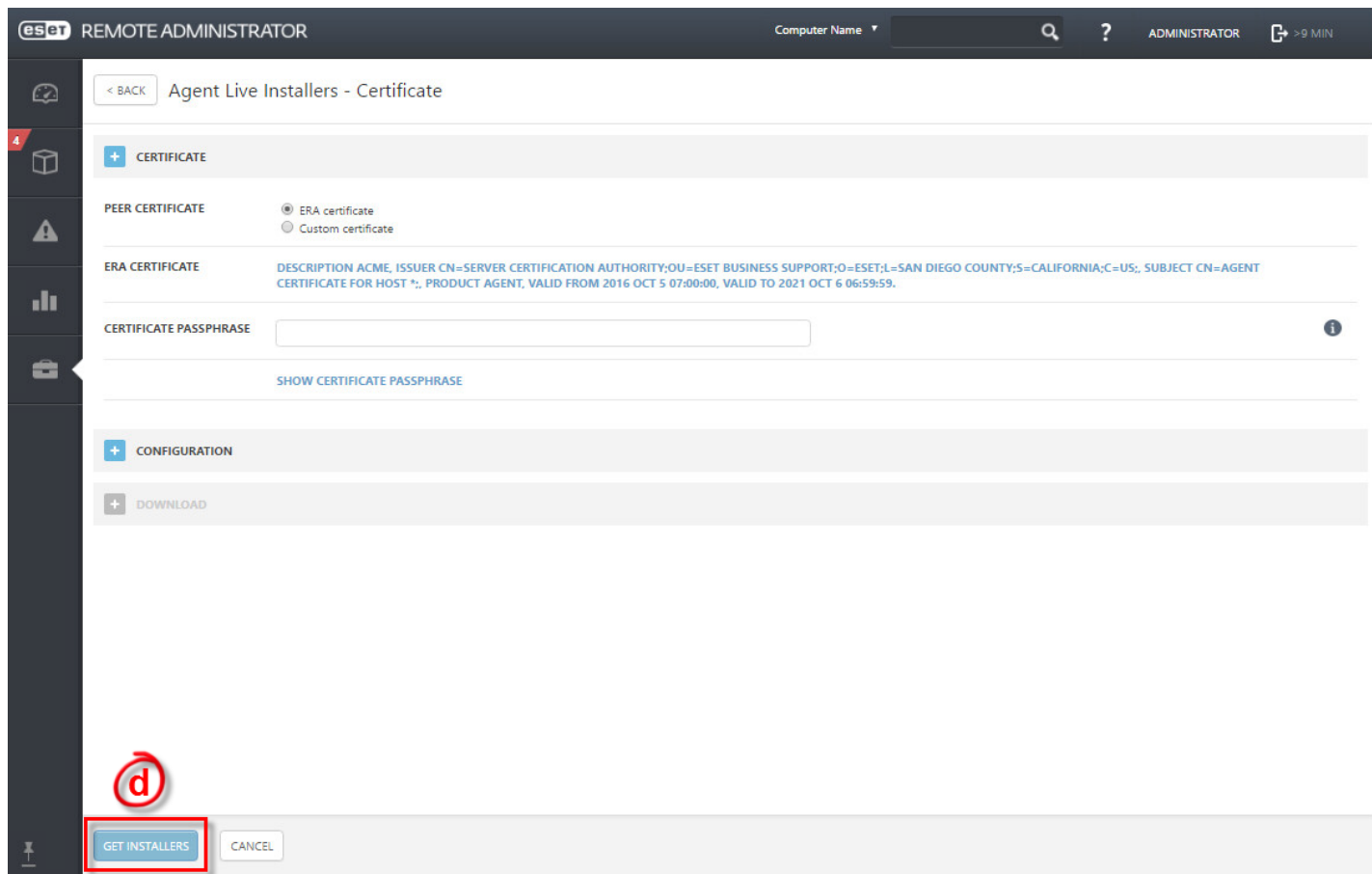


Figure 1-19

- e. Next to the installer file(s) applicable to this Client Site, click **Download**. Use the downloaded installer(s) on every Client Site device (for example, desktop, laptop or server). When installation is complete, each device will automatically check in to ERA and filter in to the dynamic group created in step 3.

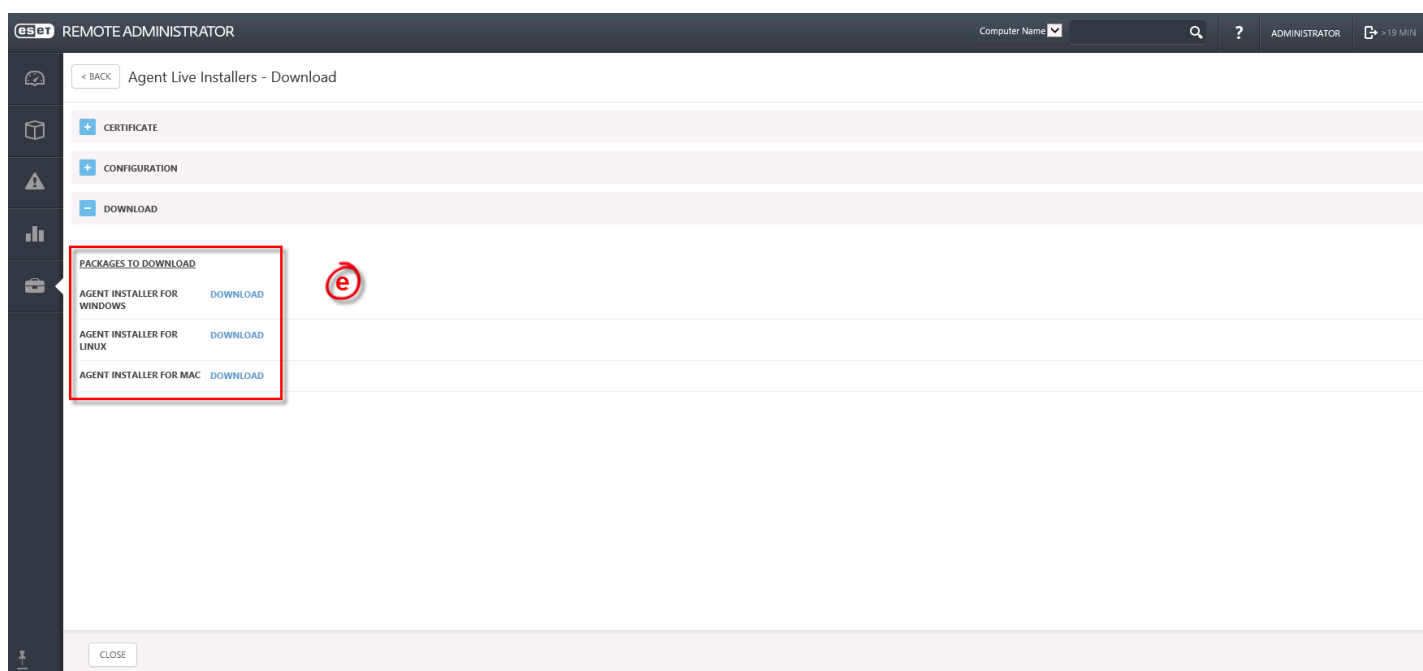


Figure 1-20

4.4 Managing ESET product deployments to ConnectWise Automate Agents

This section includes the following topics:

- [Deploy to a ConnectWise Automate group](#)
- [Deploy to a single agent, location, client or group from the context menu](#)
- [Monitor a Deployment task](#)

4.4.1 Deploy to a ConnectWise Automate group

To deploy an ESET product to a group of ConnectWise Automate Agents:

1. In the ConnectWise Automate plug-in Navigation menu, click **Deployment**.
2. Click **New Task**.

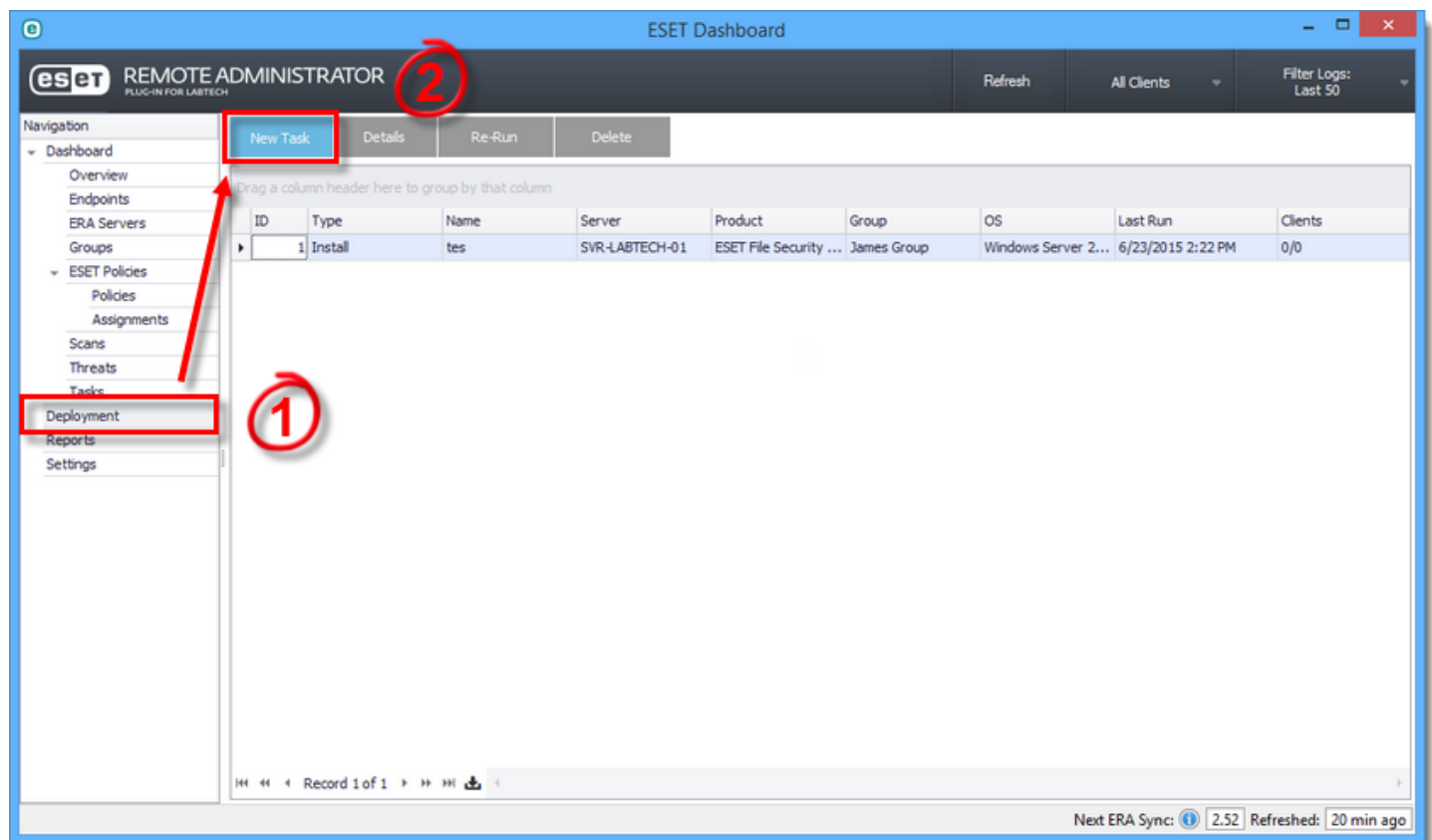


Figure 1-1

3. Select the ERA Server endpoints should connect to.
4. Select the ESET product to deploy.
5. Select the applicable ConnectWise Automate group.
6. Select the OS(s) you want to target.
7. **(Optional)** Select **Deploy to new agents that join the group** to have the ERA Plug-in for ConnectWise Automate attempt to deploy to any new agent that joins the group.
8. If more than one valid license or certificate is found for the product you selected, select the appropriate license or certificate. Click **Save** when you are finished.

The ERA Plug-in for ConnectWise Automate will immediately check ConnectWise Automate data to see if conflicting scanners are present on endpoints. If no conflicting scanners are present, deployment will begin. The ERA Plug-in for ConnectWise Automate will notify you when deployment is successful or in the case of a failed deployment, will report information about why deployment failed.

4.4.2 Deploy to a single agent, location, client or group from the context menu

To deploy an ESET product to a single agent, group, or location from the context menu:

1. Right-click the object in the ConnectWise Automate plug-in Navigation menu and select **Commands** >

ConnectWise Automate > ESET Deployment.

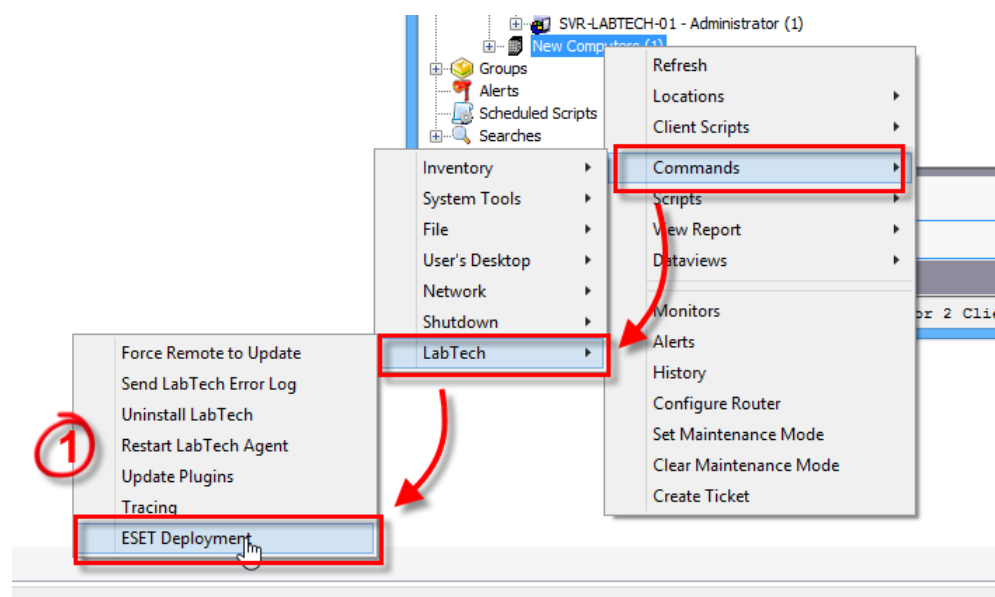


Figure 1-1

2. In the new deployment window, select the ESET server your endpoints should connect to and the ESET product to deploy.
3. Click **Submit**.

4.4.3 Monitor a Deployment task

To view the status or details of a Deployment task:

1. In the ConnectWise Automate plug-in Navigation menu, click **Deployment.z**
2. Select the applicable deployment task and click **Details**. You can resend a task if it has failed, or open the ConnectWise Automate Computer Window to diagnose a failed deployment.

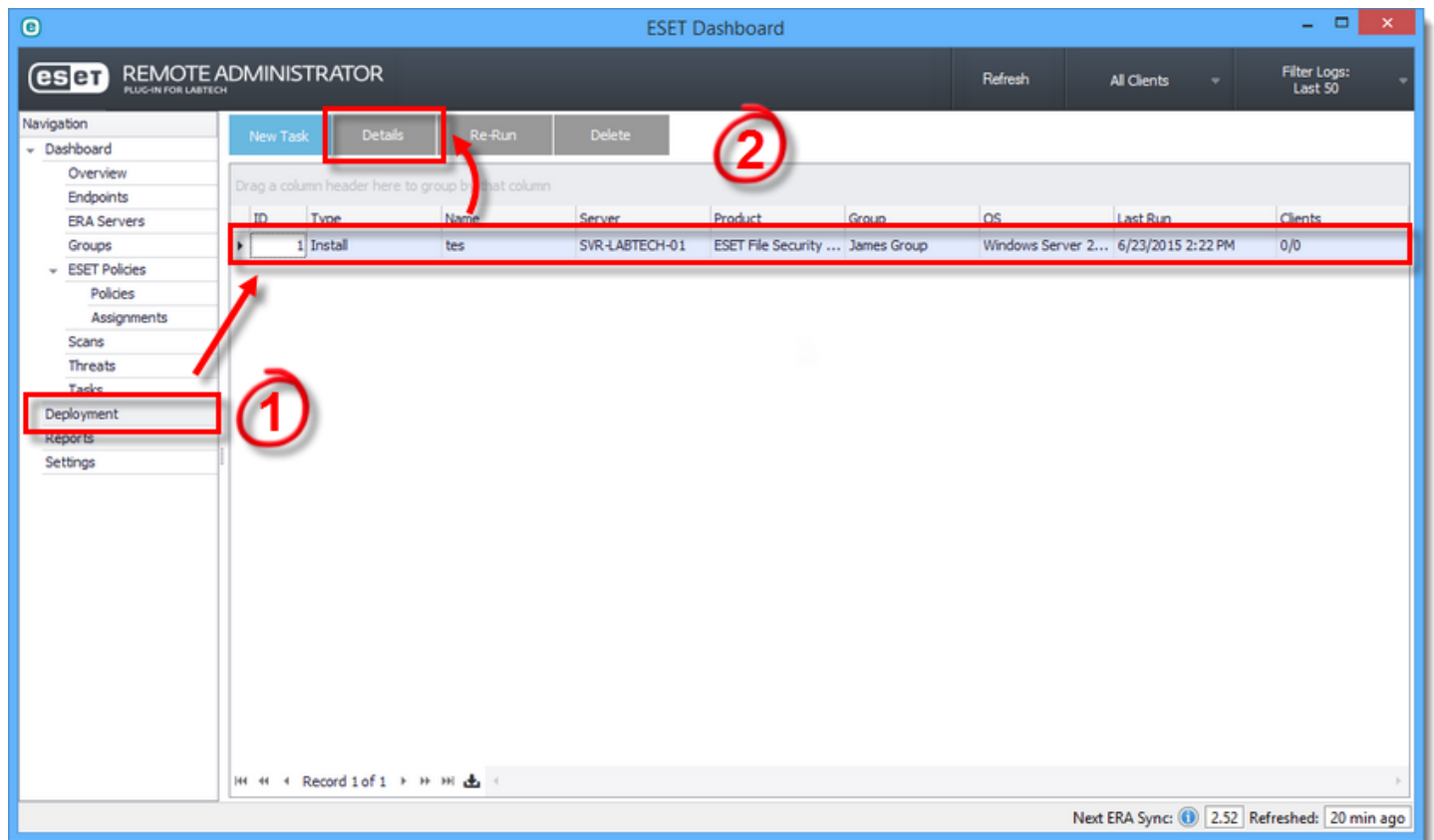


Figure 1-1

4.5 Managing ESET endpoints

The Endpoints module displays all endpoints for a selected client or for all clients.

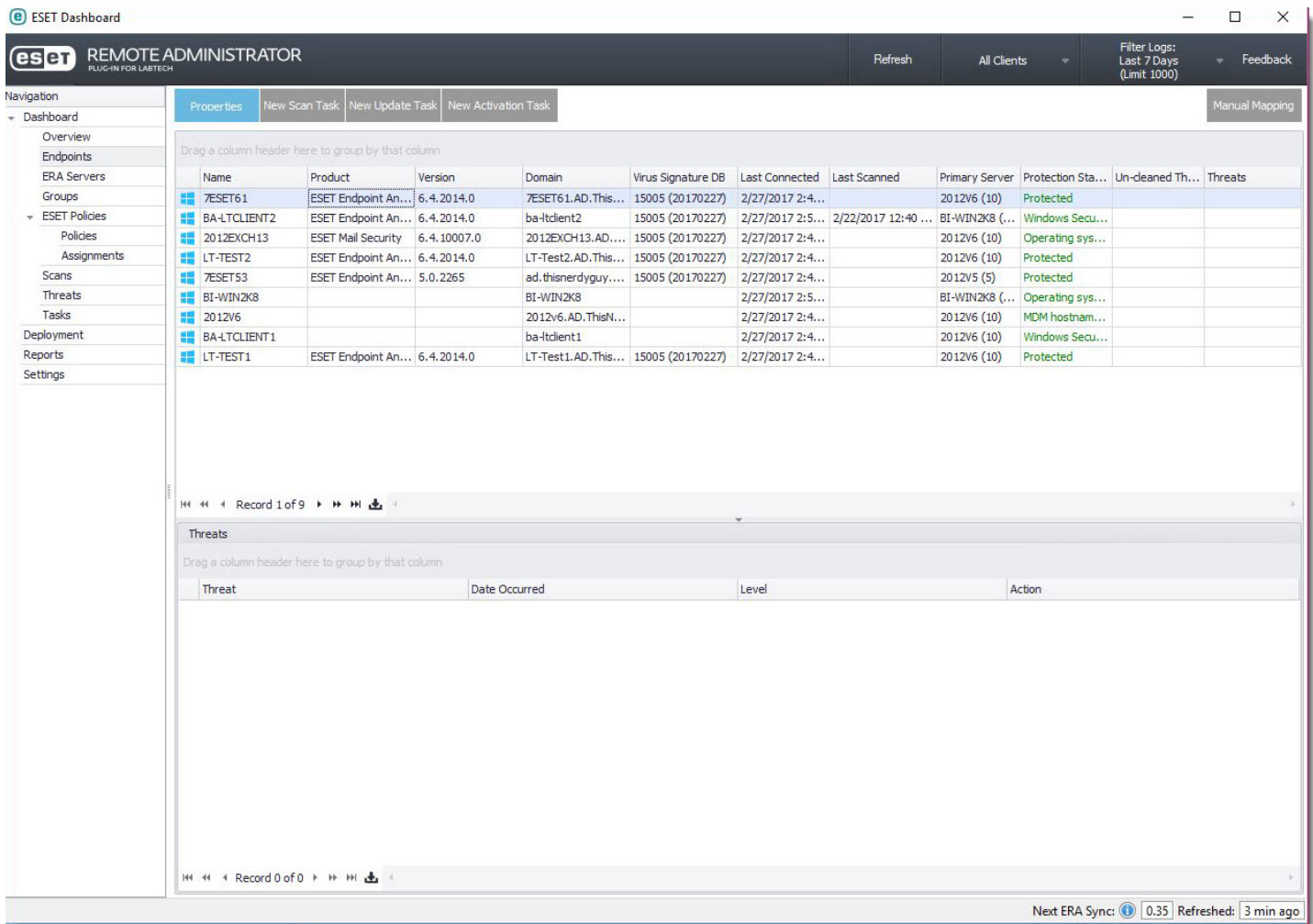


Figure 1-1

Issues with endpoints will be indicated by an orange or red indicator on the column where the issue exists. In the example shown below, the workstation is highlighted orange because it has out-of-date virus signature definitions.

Site	Dom...	Virus Signature DB	Las
BananaTech	work...	11887 (20150703)	7/3
Amazon	umb...	11887 (20140703)	7/3

Figure 1-2

This section includes the following topics:

- [Manually map an ESET endpoint to a ConnectWise Automate Agent](#)
- [Managing ESET tasks](#)
- [View endpoint properties](#)
- [Archive endpoint threats](#)

4.5.1 Manually map an ESET endpoint to a ConnectWise Automate Agent

The ERA Plug-in for ConnectWise Automate automatically maps ESET endpoints to ConnectWise Automate Agents on either of the following events:

- **New endpoints are synchronized from an ESET Server:** When new endpoints are synchronized from an ESET Server to ConnectWise Automate, the ERA Plug-in for ConnectWise Automate will search for all network adapters that belong to ConnectWise Automate agents not already matched to an endpoint and attempt to match the adapter's MAC addresses to MAC addresses that ERA has assigned to new endpoints.
- **When a new ConnectWise Automate agent is added:** During an hourly sync routine, the plug-in checks for previously synced endpoints that have not matched and checks to see if any new ConnectWise Automate agents have been added. If a new agent(s) is present, the plug-in searches all network adapters that belong to new agents and attempts to match the adapter's MAC addresses to MAC addresses that ERA has assigned to new endpoints.

If an endpoint has not found a match or is matched to the incorrect agent, you can manually create a new map to resolve the issue. Manual mappings always take priority over automatic matches.

1. In the ConnectWise Automate plug-in Navigation menu, click **Endpoints**.
2. Click **Manual Mapping**.

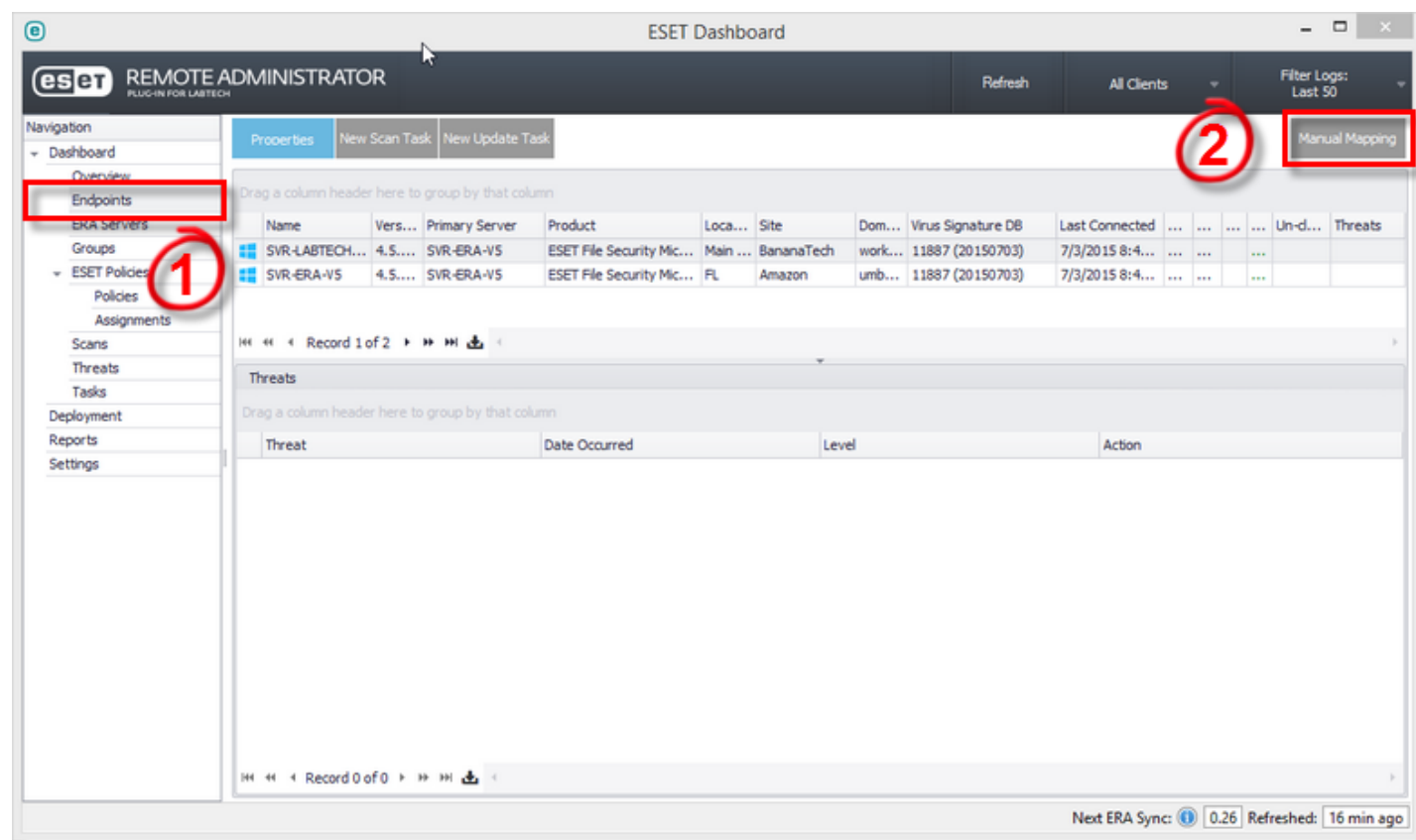


Figure 1-1

4. Click **New Match**.
5. Select **ESET Endpoints** from the **Search For** field and enter a search term for the device (for example, computer name, domain, MAC address, etc.) in the **Search query** field, or leave the **Search query** field blank to find all endpoints. You also have the option to display only unmatched devices by selecting the appropriate check box. Click **Search** when you are finished.

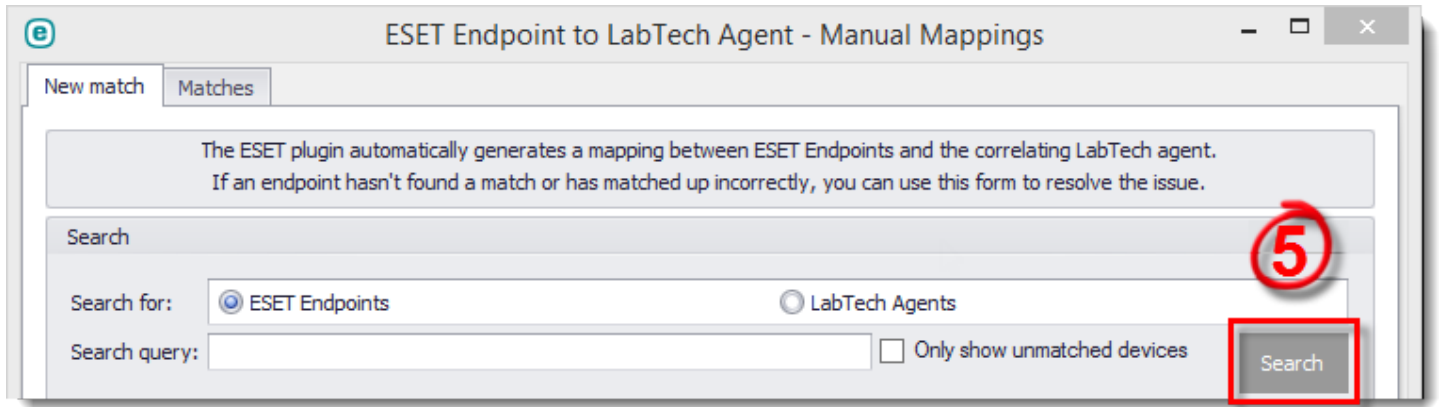


Figure 1-2

6. The table will display devices returned by your query.
7. Identify the device you want to match and select its corresponding check box. Data about the selected endpoint will be displayed in the **Selected ESET Endpoint** field.
8. Select **ConnectWise Automate Agents** from the **Search for** field.
9. Repeat steps 2 through 4. ConnectWise Automate agent data will be displayed in the **Selected ConnectWise Automate Agent** field.
10. Click **Confirm match & save** when you have confirmed that the agent and endpoint are a match. You can add more matches or close the Manual Mappings dialog.

4.5.2 Managing ESET tasks

In the Endpoints module, you can initiate new [on-demand scans](#) and force [definition updates](#) as tasks.

4.5.2.1 Initiate a New Scan Task

To initiate a new scan task:

1. In the ConnectWise Automate plug-in Navigation menu, click **Endpoints** and select the applicable endpoint(s).
2. Click **New Scan Task**. The **Scan Task** dialog will be displayed.

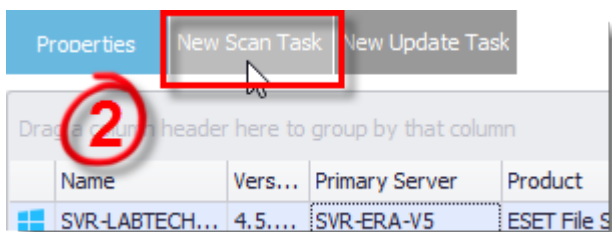


Figure 1-1

3. Select your scan targets from the **Targets** menu. You have the option to specify **Scan without cleaning** or enter a description for the task.
4. Click **Submit**. If the ERA Server is accessible the task will be sent immediately. If it is not, the task will be sent the next time that the ERA Plug-in synchronizes with the ERA Server. All tasks you create can be monitored from the Task log module.

4.5.2.2 Initiate a New Update Task

To initiate a new update task:

1. In the ConnectWise Automate plug-in Navigation menu, click **Endpoints** and select the applicable endpoint(s).
2. Click **New Update Task**. If the ERA Server is accessible the task will be sent immediately. If it is not, the task will be sent the next time that the ERA Plug-in synchronizes with the ERA Server. All tasks you create can be monitored from the Task log module.

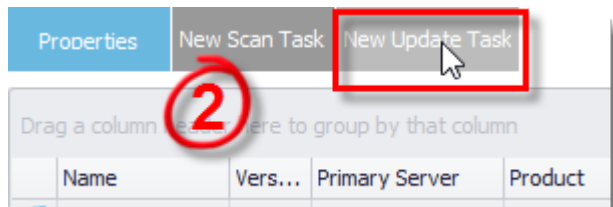


Figure 1-1

4.5.2.3 Initiate a New Activation Task

To initiate a new activation task:

1. In the ConnectWise Automate plug-in Navigation menu, click **Endpoints** and select the applicable endpoint.
2. Click **New Activation Task**.
3. In the **Activation License** drop-down menu, select the appropriate license and then click **Create Task**.

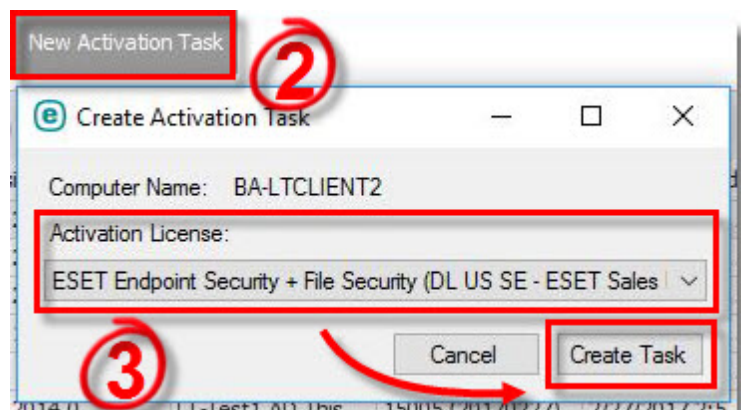


Figure 1-1

The activation task will be created on the ERA server the next time the ERA plug-in synchronizes with the server.

4.5.3 View endpoint properties

To view endpoint properties:

1. In the ConnectWise Automate plug-in Navigation menu, click **Endpoints**.
2. Select the applicable endpoint and then click **Properties**.

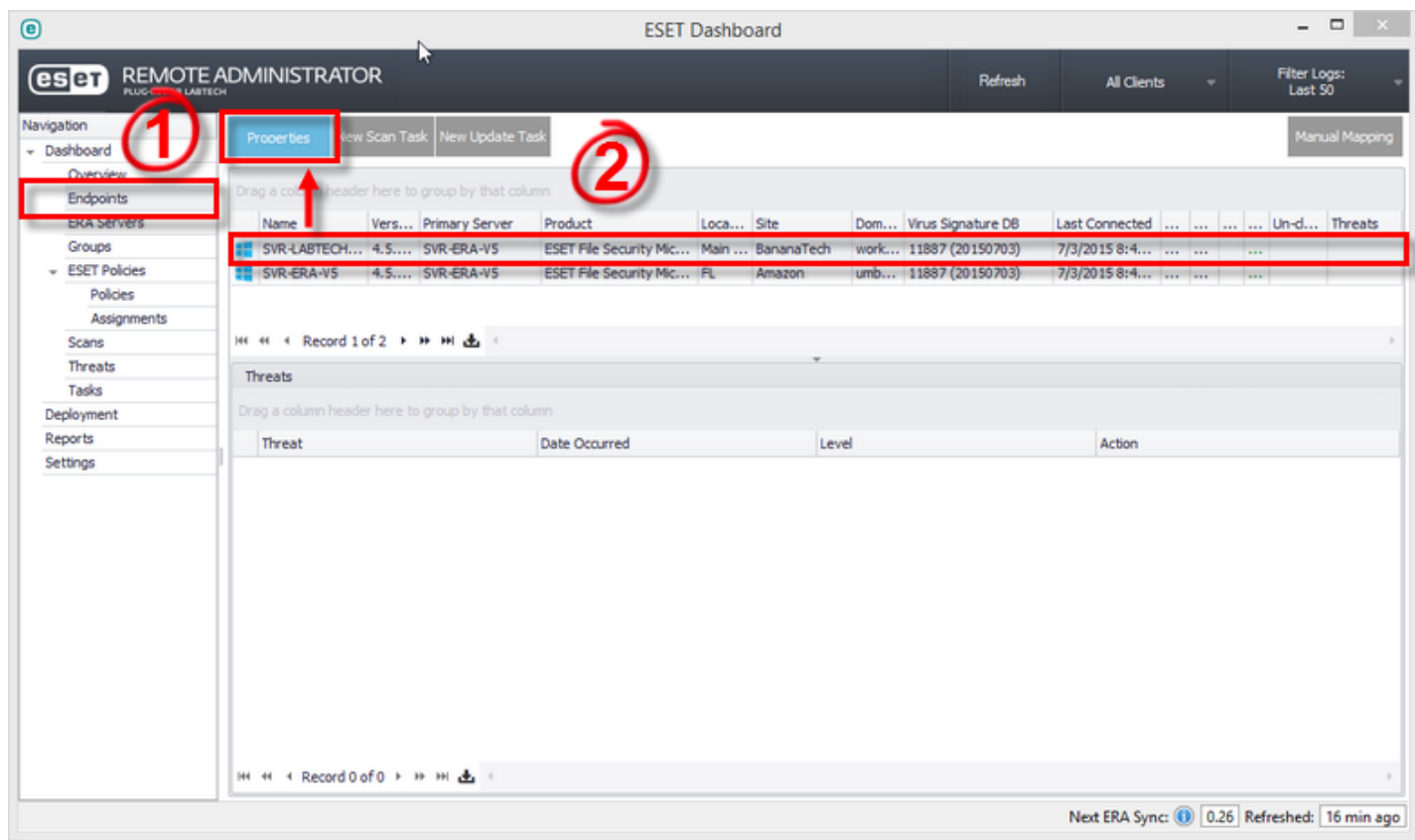


Figure 1-1

3. From this window, you can view or export data about ESET solutions and ConnectWise Automate. To open the ConnectWise Automate Computer window for this agent, click **Computer**. Other information, such as ESET policies applied and the protection status of this endpoint, is also available.

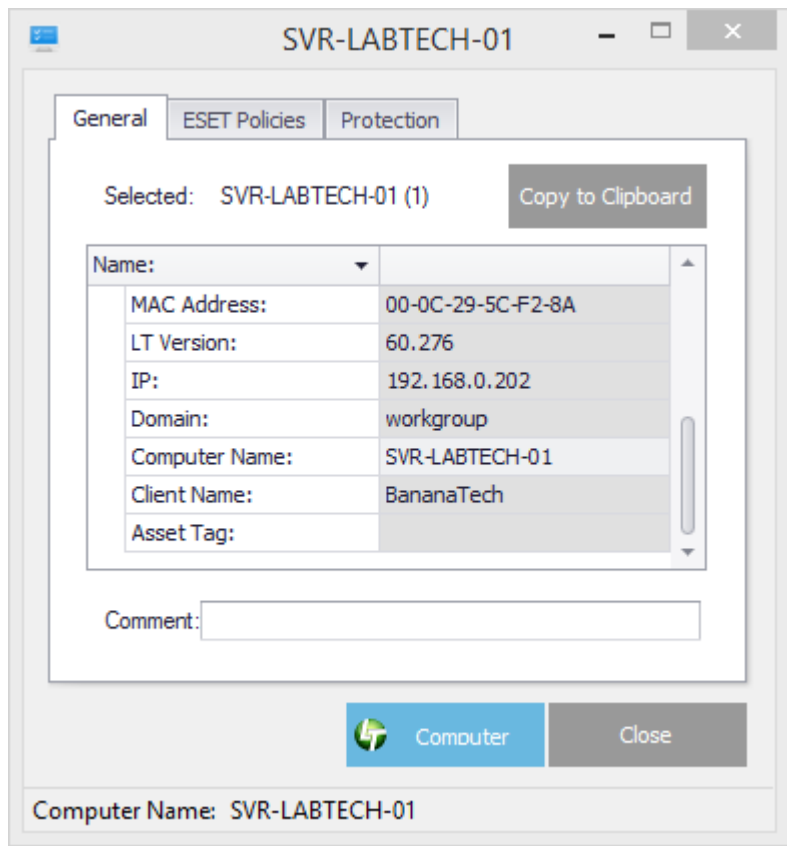


Figure 1-2

4.5.4 Archive endpoint threats

To archive an endpoint threat:

1. In the ConnectWise Automate plug-in Navigation menu, click **Endpoints**.
2. Select the applicable endpoint.

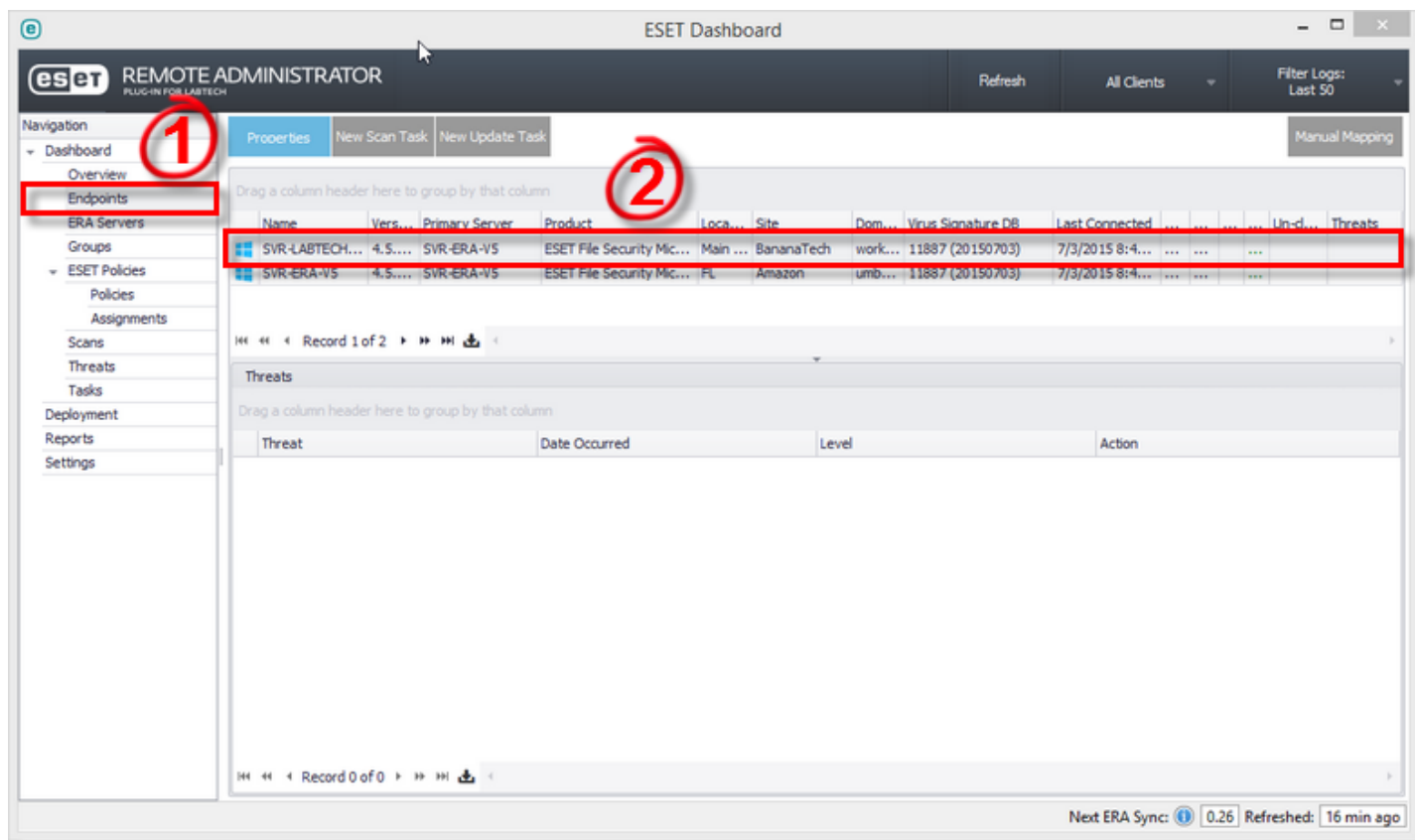


Figure 1-1

3. In the **Threats** table below, right-click a threat and select **Archive Threat**.

4.6 Managing ESET policies

This section includes the following topics:

- [ESET policy FAQ](#)
- [Create a policy](#)
- [Assigning policies](#)
- [Remove a policy from a group](#)
- [Hide groups without policies](#)
- [Import an existing policy from ERA](#)
- [Inherit/Merge Exclusions and Schedules](#)

4.6.1 ESET policy FAQ

Why don't I see my new policy in ERA?

Policies don't get created in ERA until they are assigned to ConnectWise Automate agents. If a policy isn't assigned to a ConnectWise Automate group or is assigned to a ConnectWise Automate group with no ESET agents, the policy won't show up in ERA until the policy is assigned to a group and an ESET agent joins the group.

What policy are endpoints assigned upon initial installation of the ERA Plug-in for ConnectWise Automate?

The ERA Plug-in for ConnectWise Automate doesn't modify any computer policy settings until a policy is created and assigned to a group. Computers will keep all their previous settings until a new policy is applied from the plug-in.

How do I assign global / default policies?

The recommended method to create a default policy is to create a new ESET policy from the ERA Plug-in for ConnectWise Automate and assign it to the "All Agents" group in ConnectWise Automate.

Alternatively, you can edit the "ConnectWise Automate Policies" policy and all parent policies to create policies that are inherited by plug-in managed policies.

Can I change policies from the ERA server?

You cannot modify any policies created by the plug-in from the ERA console. Changes will be overwritten by the plug-in during a maintenance cycle.

Why do I still see a deleted policy in ERA?

Deleted policies are not removed from ERA. It is ok to leave these and let the plug-in clean up policies if needed.

What happens to computers when their policy has been deleted?

If all policies that once applied to a computer are deleted, the computer will be assigned to the "ConnectWise Automate Policies" parent policy until a new policy is assigned to the computer.

How long does it take for a newly added computer to get its ESET Policy?


If the newly added computer has ESET software installed and is managed by an ERA server with the ERA Plug-in for ConnectWise Automate, it will receive policy settings within approximately 6 minutes of joining any group with ESET policies assigned to it.

What happens when a computer's group(s) are changed or is moved into a new group?

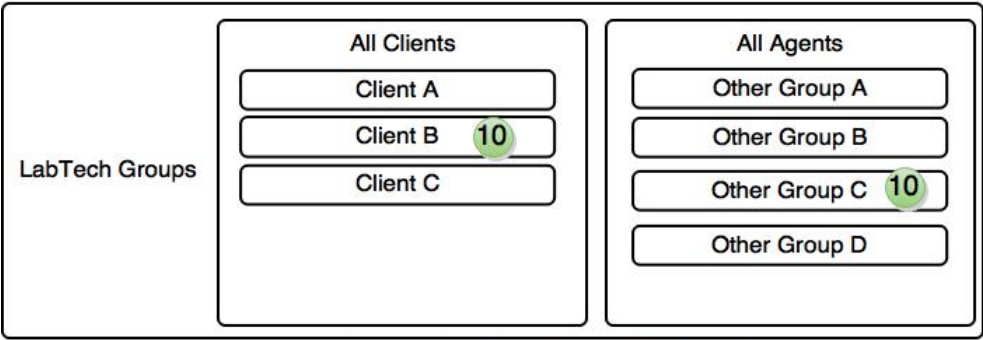
If the new group contains ESET policies it will get its new expected policy from the ERA Plug-in for ConnectWise Automate. If it is moved out of all groups with ESET policies assigned, it will retain its previous settings until a new policy is assigned to it.

What is policy inheritance?

Policy inheritance in the ERA Plug-in for ConnectWise Automate works similarly to ConnectWise Automate templates. Inheritance exhibits parent-child behavior down the ConnectWise Automate group tree. Because a ConnectWise Automate agent can be present in any number of groups (branches of the tree), priority is used to select the policy that will be applied. See the examples below:

-  ESET Policy w/ priority
-  ESET Policy w/ priority - Allow merging enabled

(1) SIMPLE CONFLICTING POLICIES

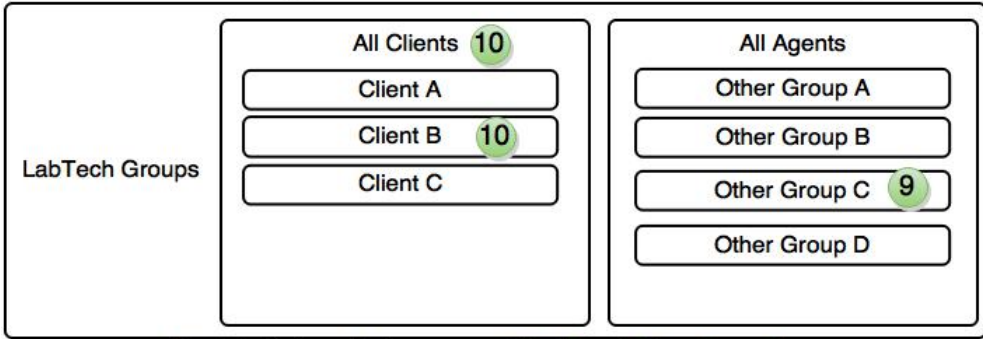


Endpoint belongs to two groups, Client B and Other Group C.
Both groups have an ESET policy with a priority 10.

Policies will merge together. If the policies have a conflicting setting one will win based on which group has the higher ID (You have no control over this). This is a case where you would modify the policy priority and set the more important policy with a lower priority (1 is the highest)

This could also be resolved by using the "Assignments" tab in the ESET Dashboard. Assignments let you resolve conflicts between policies with the same priority. You can move policies with the same priority up or down to assign a "sub-priority"

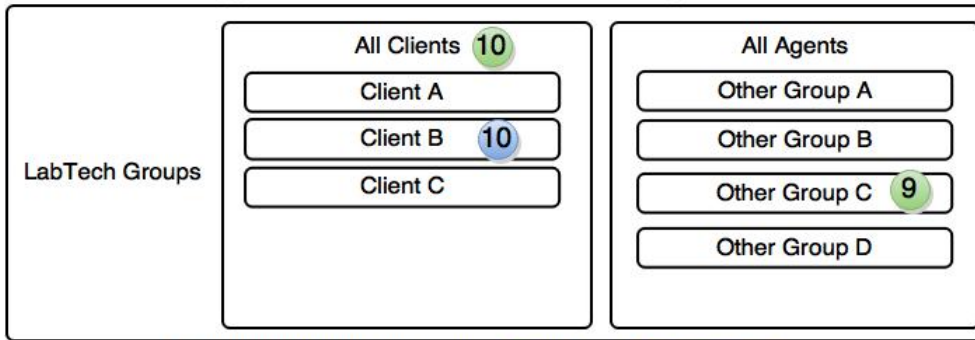
(2) SIMPLE POLICY INHERITANCE - NO CONFLICT



Endpoint belongs to two groups, Client B and Other Group C.
Client B is a child of All Clients which also has a policy assigned.

Policies will merge together. If a conflicting setting existed between the policy assigned to All Clients and the policy assigned to Client B, Client B's policy would win because it is the lowest child. Since Other Group C has a higher priority (lower number) it would trump any conflicts in the other policies.

(3) SIMPLE POLICY INHERITANCE - Merge enabled

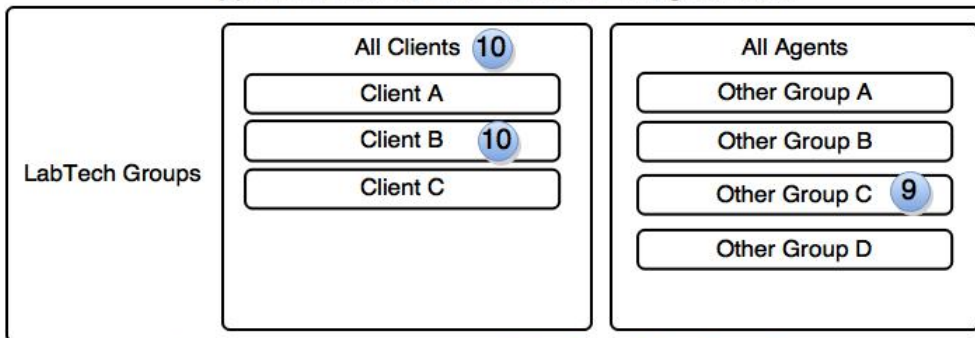


Endpoint belongs to two groups, **Client B** and **Other Group C**.
Client B is a child of **All Clients** which also has a policy assigned.

Policies will merge together. If a conflicting setting existed between the policy assigned to **All Clients** and the policy assigned to **Client B**, **Client B's** policy would win because it is the lowest child. Since **Other Group C** has a higher priority (lower number) it would trump any conflicts in the other policies.

Since **Client B** is set to allow merging, specific settings (ie: exclusions) will merge instead be overwritten by any settings assigned to **All Clients**. Since **Other Group C** does not have merge enabled, it will still take priority and overwrite any conflicting settings. (Not merge them further)

(4) SIMPLE POLICY INHERITANCE - Merge enabled



Endpoint belongs to two groups, **Client B** and **Other Group C**.
Client B is a child of **All Clients** which also has a policy assigned.

Policies will merge together. If a conflicting setting existed between the policy assigned to **All Clients** and the policy assigned to **Client B**, **Client B's** policy would win because it is the lowest child. Since **Other Group C** has a higher priority (lower number) it would trump any conflicts in the other policies.

Since all policies are set to allow merging, specific settings (ie: exclusions) will merge instead be overwritten. The final policy would have exclusions from all 3 policies.

Figure 1-1

4.6.2 Create a policy

To create a policy:

1. In the ConnectWise Automate plug-in Navigation menu, click **Policies** > **New**. In this example, we will create a policy bundle for all installed ERA 6.x products at Client Site “Acme”.

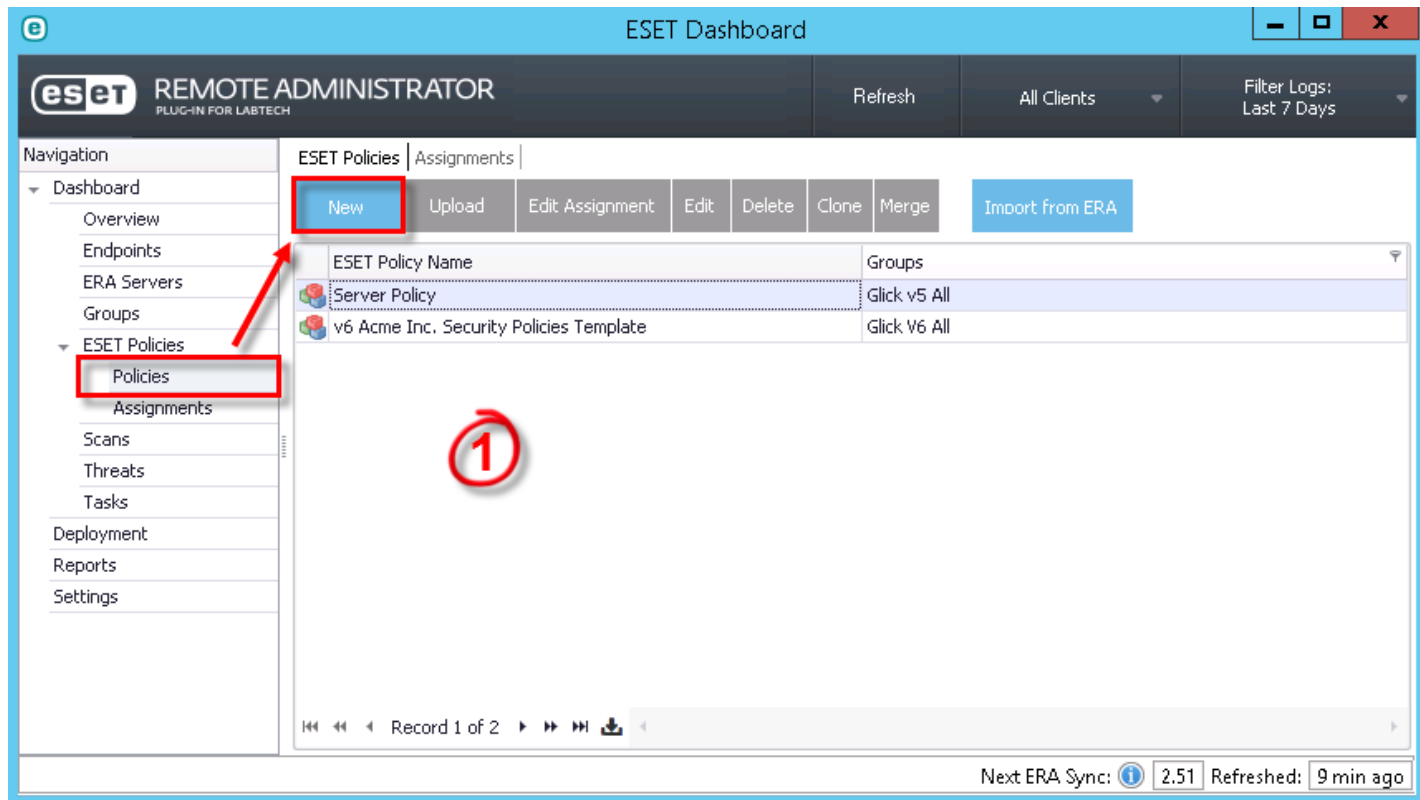


Figure 1-1

2. In the **ESET Policy Name** field, type a name for your policy. Click the **ERA V6** tab. In the **Add Product** drop-down menu, select the applicable security products managed for the client. Click **Save**.

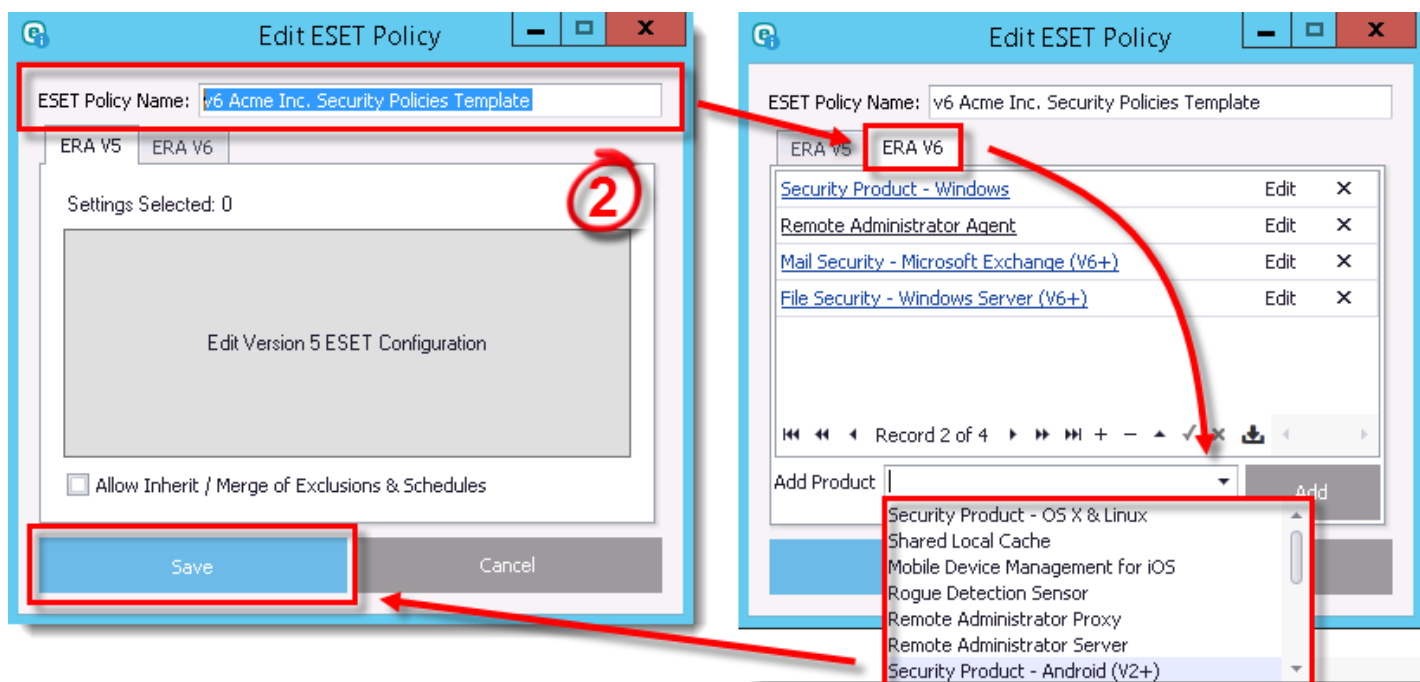


Figure 1-2

4.6.3 Assigning policies

An ESET policy can be assigned two different ways. This section includes the following topics:

- [Assign a policy from the Policies window](#)
- [Assign a policy from the Groups window](#)

4.6.3.1 Assign a policy from the Policies window

To assign a policy to a group from the Policies window of the plug-in:

1. In the ConnectWise Automate plug-in Navigation menu, click **Policies**.
2. Select the applicable policy and click **Edit Assignment**.

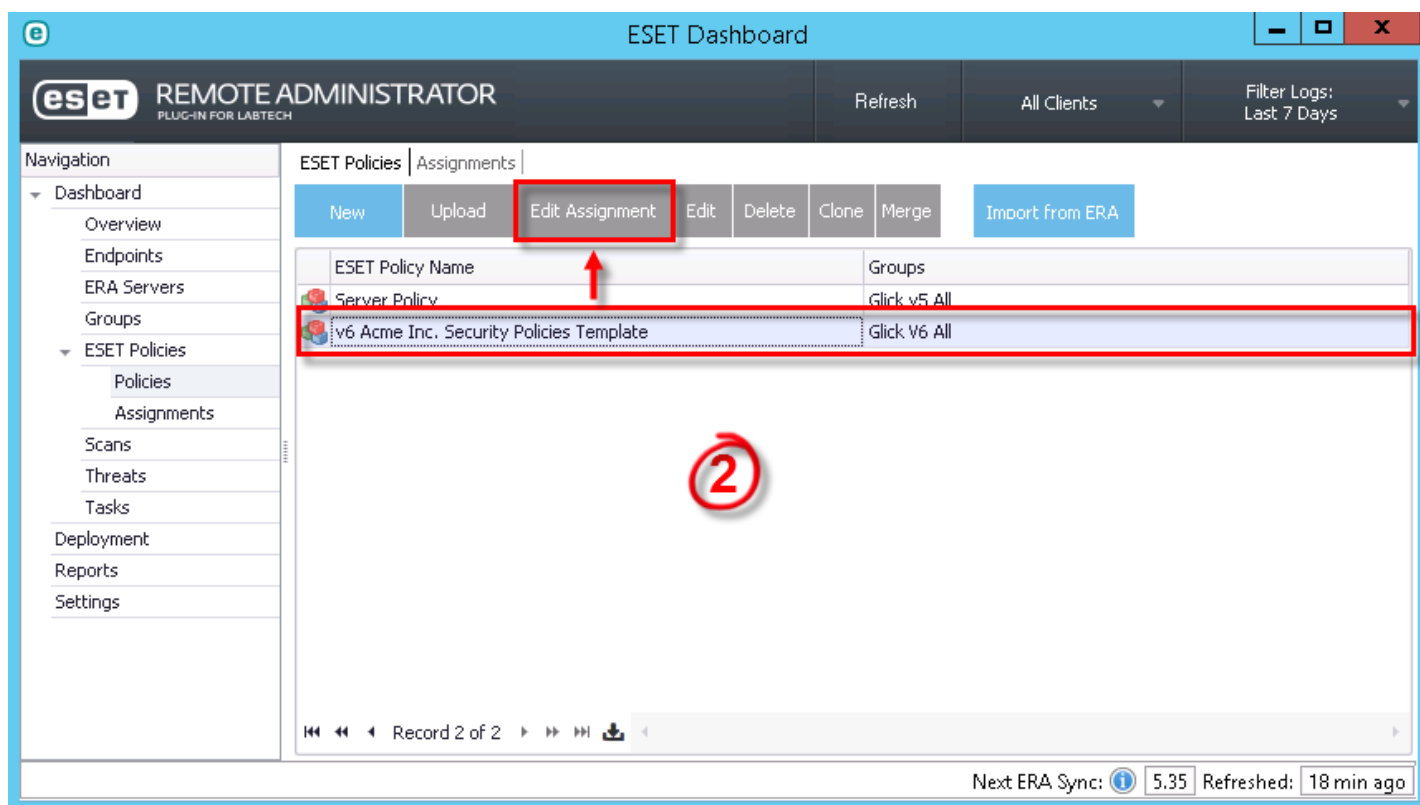


Figure 1-1

3. Select the appropriate group and click **Save**.

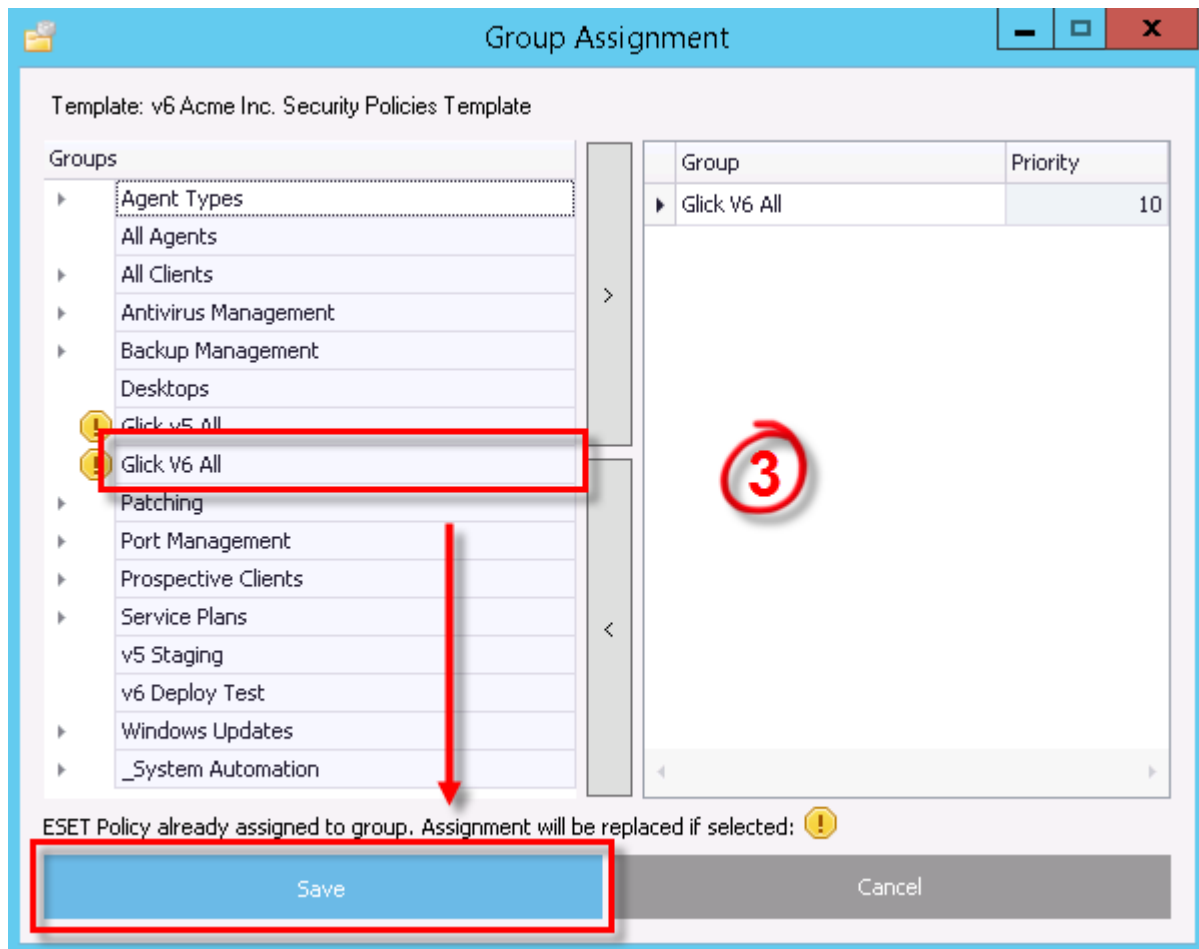


Figure 1-2

4.6.3.2 Assign a policy from the Groups window

To assign a policy to a group from the Groups window of the plug-in:

1. In the ConnectWise Automate plug-in Navigation menu, click **Groups**.
2. Select a group and click **Assign ESET Policy**.

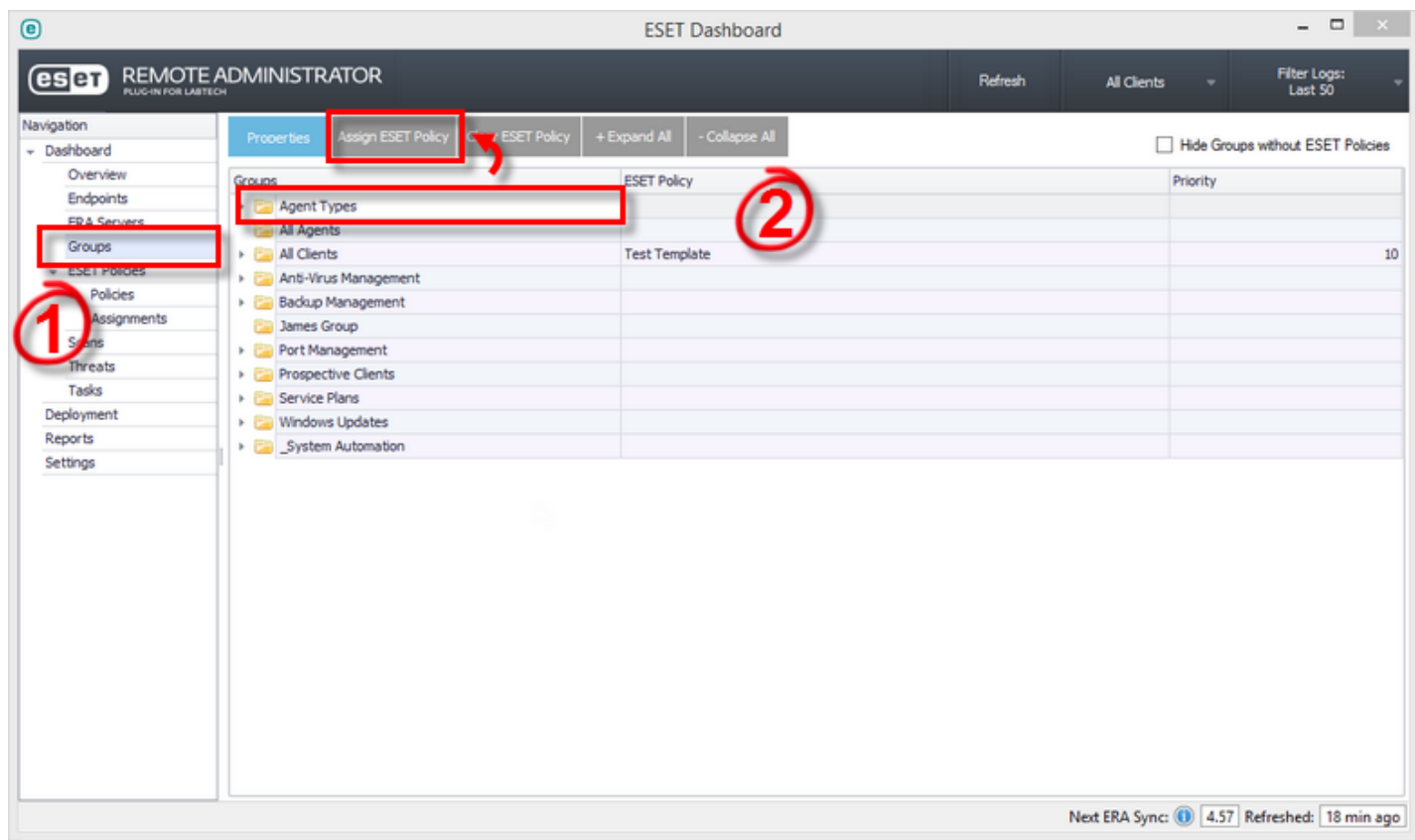


Figure 1-1

3. Select the policy you want to assign to the group, select the priority level you want to use from the drop-down menu (1 is the highest priority and 10 is the lowest) and then click **Save**.

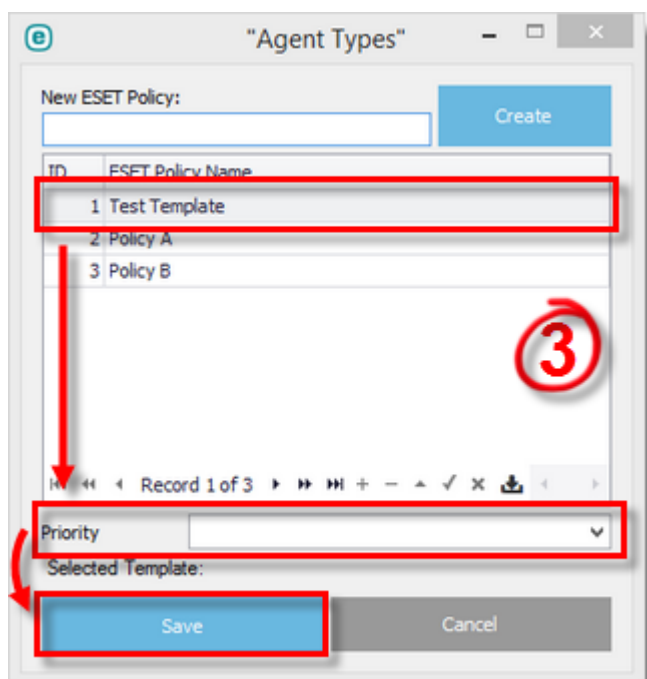


Figure 1-2

4.6.4 Remove a policy from a group

To remove a policy from a group in the plug-in:

1. In the ConnectWise Automate plug-in Navigation menu, click **Groups**.
2. Select a group and click **Clear ESET Policy**.

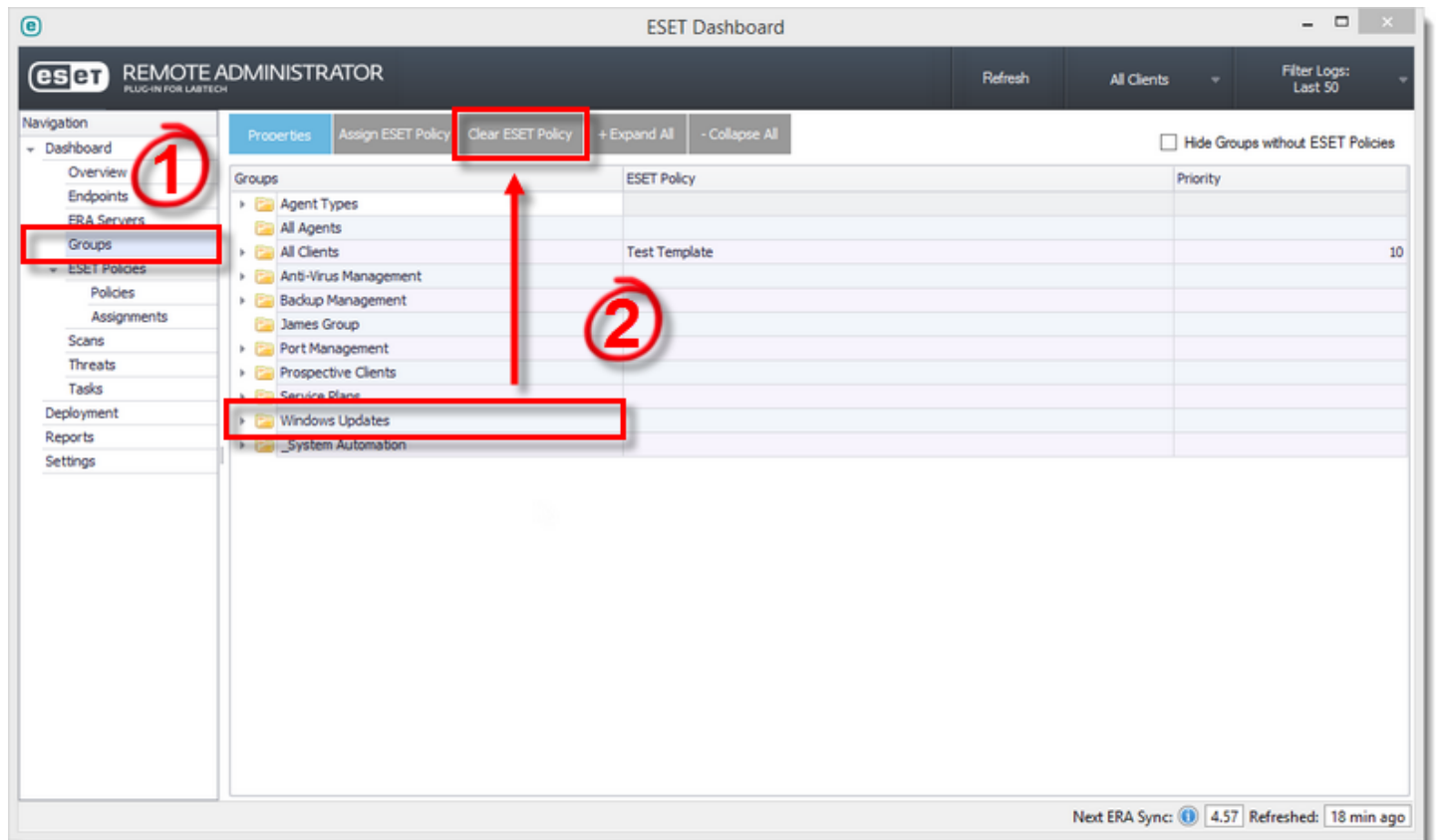


Figure 1-1

3. Select the policy you want to remove from the group and then click **Save**.

4.6.5 Hide groups without policies

To hide groups in the plug-in without corresponding ESET policies:

1. In the ConnectWise Automate plug-in Navigation menu, click **Groups**.
2. Select the check box next to **Hide Groups without ESET policies**. The dashboard will display only groups that have ESET policies assigned to them.

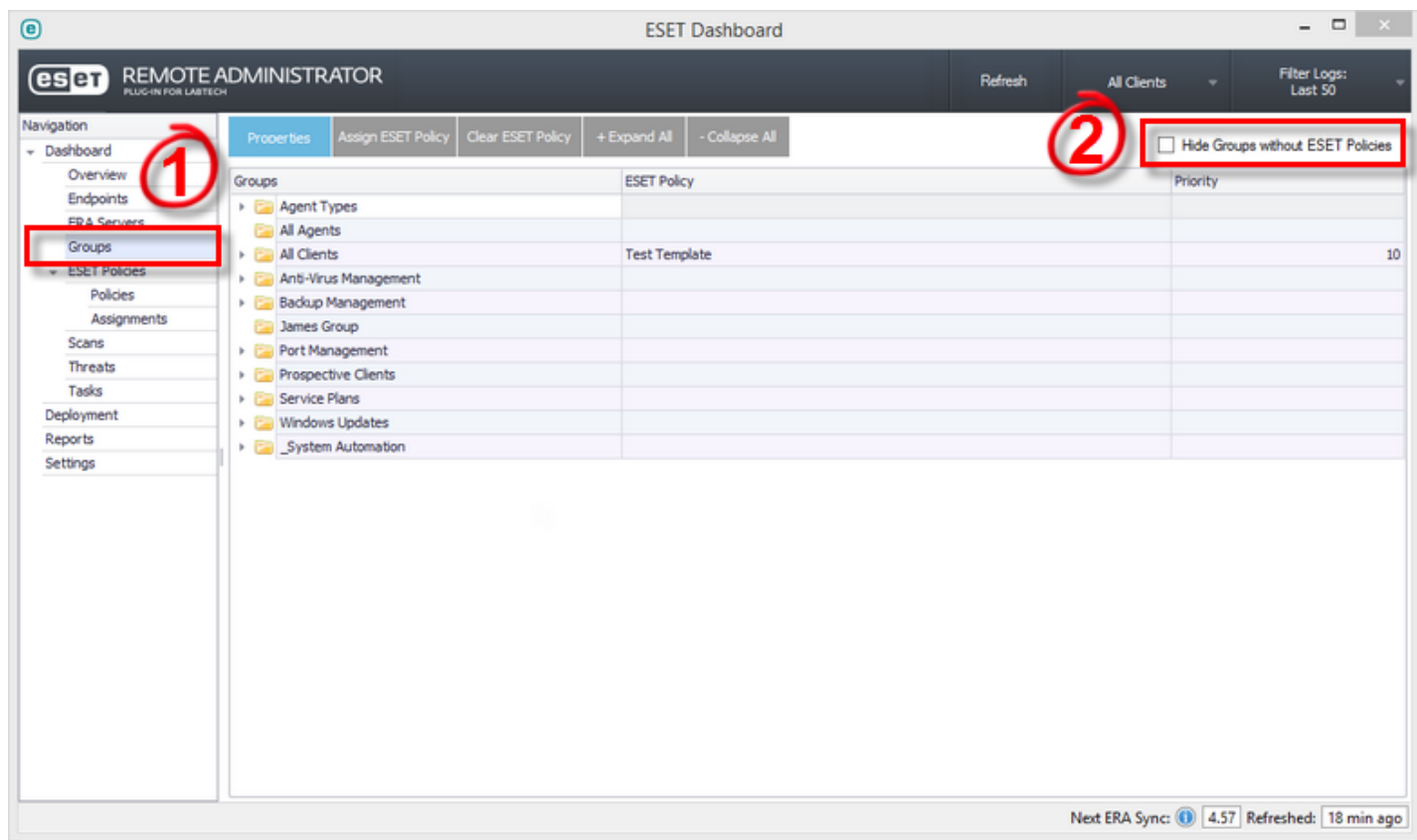


Figure 1-1

4.6.6 Import an existing policy from ERA

You must import policies into the ERA Plug-in for ConnectWise Automate to allow for their management using the plug-in. To do so, follow the steps below:

1. In the ConnectWise Automate plug-in Navigation menu, click **Policies**.
2. Click **Import from ERA**.

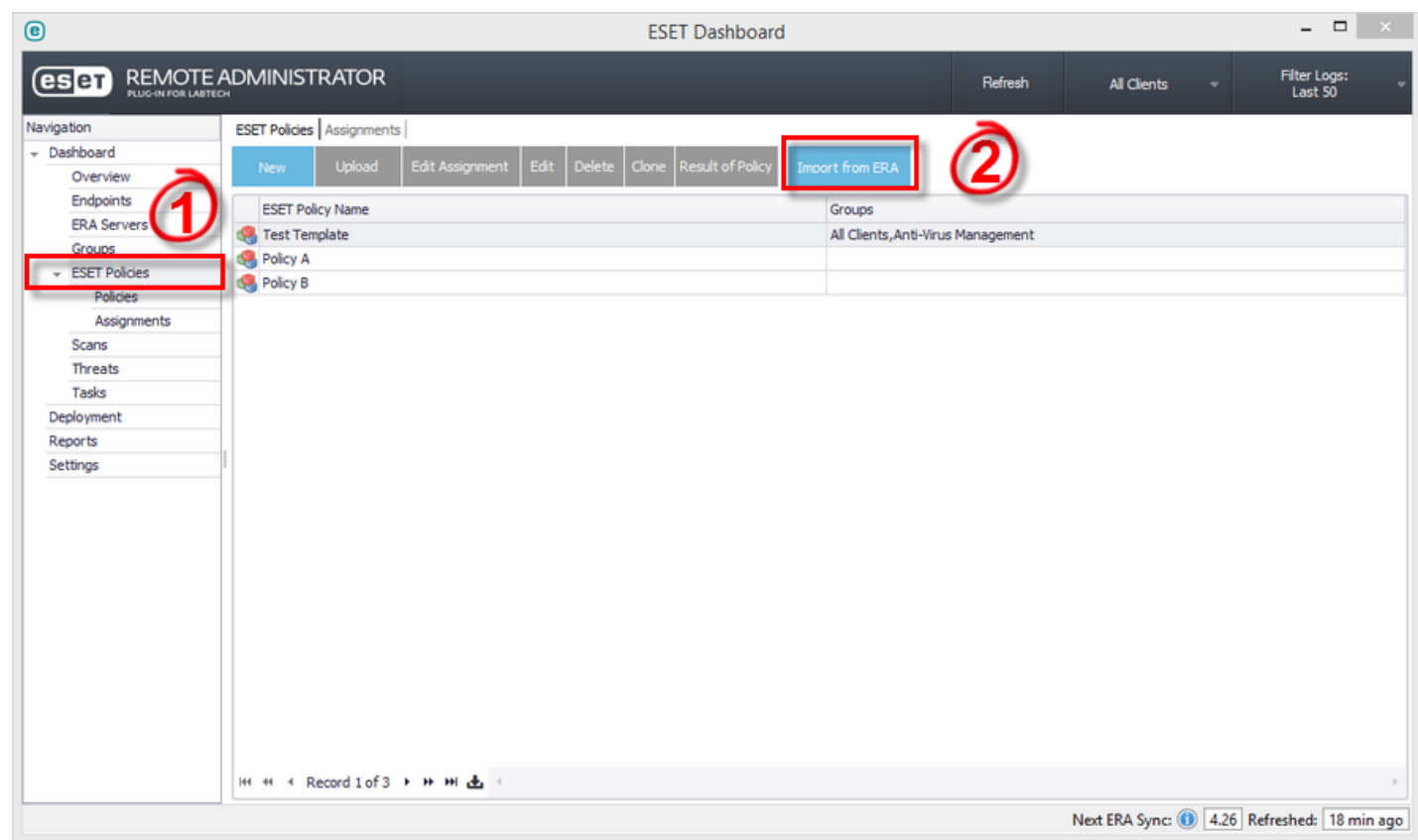


Figure 1-1

3. Select an ERA server.
4. Select the applicable policies, click > to add them to the **Selected** list and then click **Import**.

When a policy is imported from ERA, the plug-in copies all settings from the policy and adds it to a new policy in the ERA Plug-in for ConnectWise Automate. No changes will be made to the policy on the ERA server unless **Delete from ERA** is selected.

NOTE: Imported policies will not take effect until they are assigned to a ConnectWise Automate group.

4.6.7 Inherit/Merge Exclusions and Schedules

The ERA Plug-in for ConnectWise Automate will allow you to merge exclusions and schedules down the ConnectWise Automate group tree. Select **Allow Inherit/Merge of Exclusions & Schedules** when editing policy configurations to allow a policy to merge with its parent policy.

4.7 Managing ESET servers

This section includes the following topics:

- [Detect a server](#)
- [Force server detection](#)
- [Verify server detection](#)
- [Synchronize a server](#)
- [Update server connection settings](#)

4.7.1 Detect a server

The ERA Plug-in for ConnectWise Automate adds new role detection rules to the ConnectWise Automate database. Your ESET Server(s) should automatically be detected the first time that your Agents run their inventory schedules as defined in ConnectWise Automate.

You can expedite this process to detect your ESET Server(s) immediately. To do so, follow the steps below:

1. Right-click the ConnectWise Automate Agent, client, location or group that contains an agent hosting your ESET Server.
2. Select **Commands > Inventory > Resend System info**.

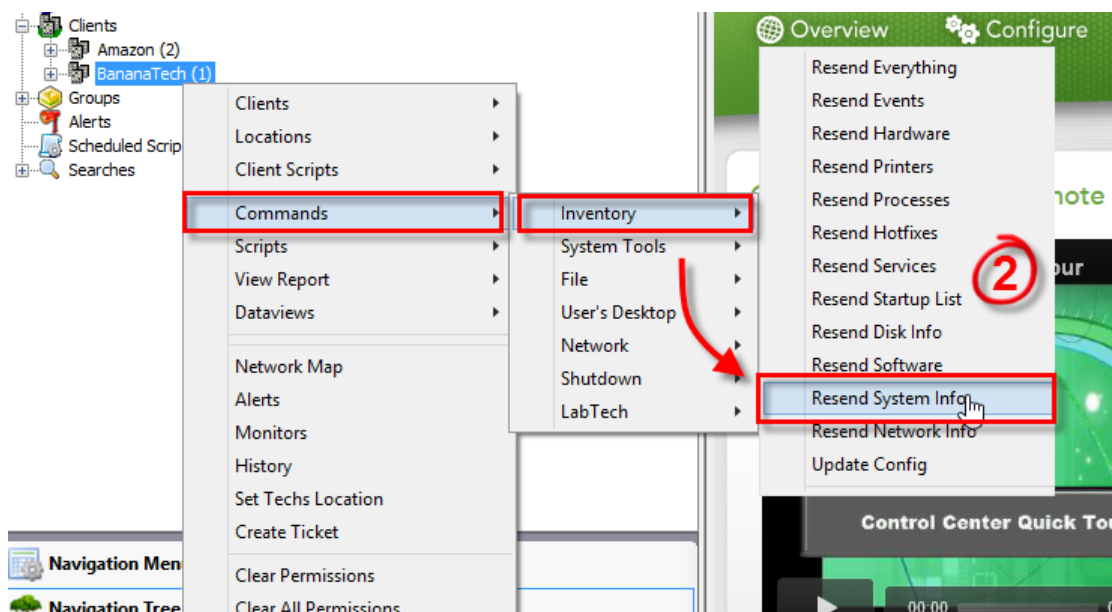


Figure 1-5

3. Select **Commands > Inventory > Update Config**.

4.7.2 Force server detection

While it is not recommended, you can force a ConnectWise Automate agent to be found as an ESET Server using the steps below:

1. Open the Computer Window of a ConnectWise Automate Agent and then click **Detected Roles**.

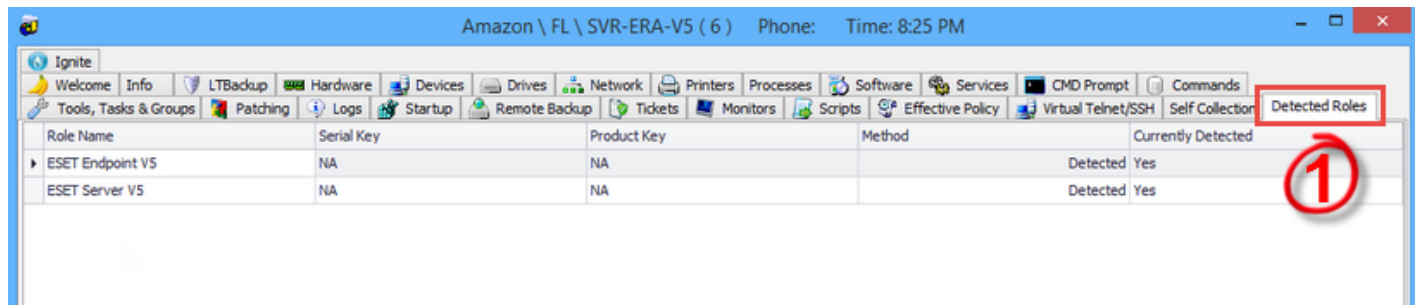


Figure 1-1

2. Click **Overrides**.
3. Click **Add**.
4. Select **ESET Server V6** as the Role Template.
5. Select **Apply** as the method.
6. Click **Add > Add**. The agent will now be detected as an ESET Server.

4.7.3 Verify server detection

To verify server detection:

1. Open the Computer Window of a ConnectWise Automate agent and click **Detected Roles**.

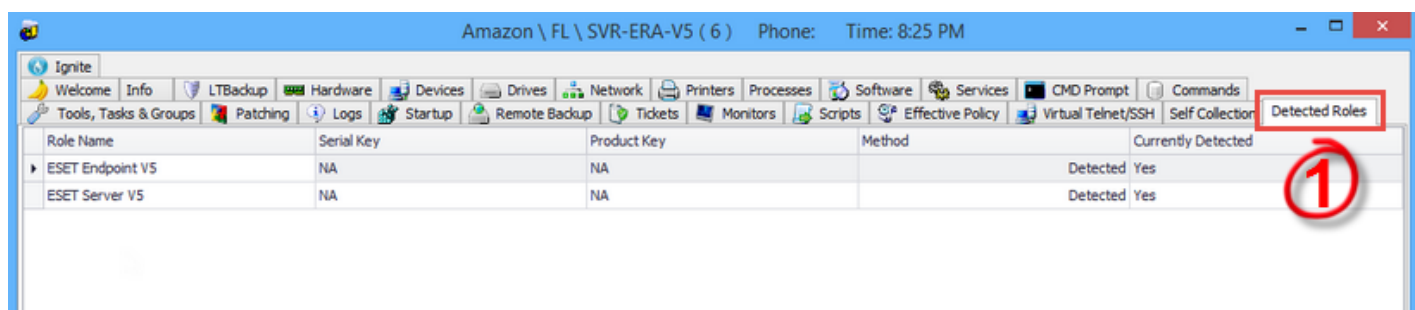


Figure 1-1

2. In the **Role Name** field, **ESET Server V5** or **ESET Server V6** will be displayed.

4.7.4 Synchronize a server

The ERA Plug-in for ConnectWise Automate will synchronize data automatically with the ERA server approximately every 6 minutes. The Next ERA Sync indicator at the bottom of the dashboard displays time until the next synchronization. To immediately force synchronization:

1. In the ConnectWise Automate plug-in Navigation menu, click **ERA Servers**.
2. Select a server and click **Synchronize**.

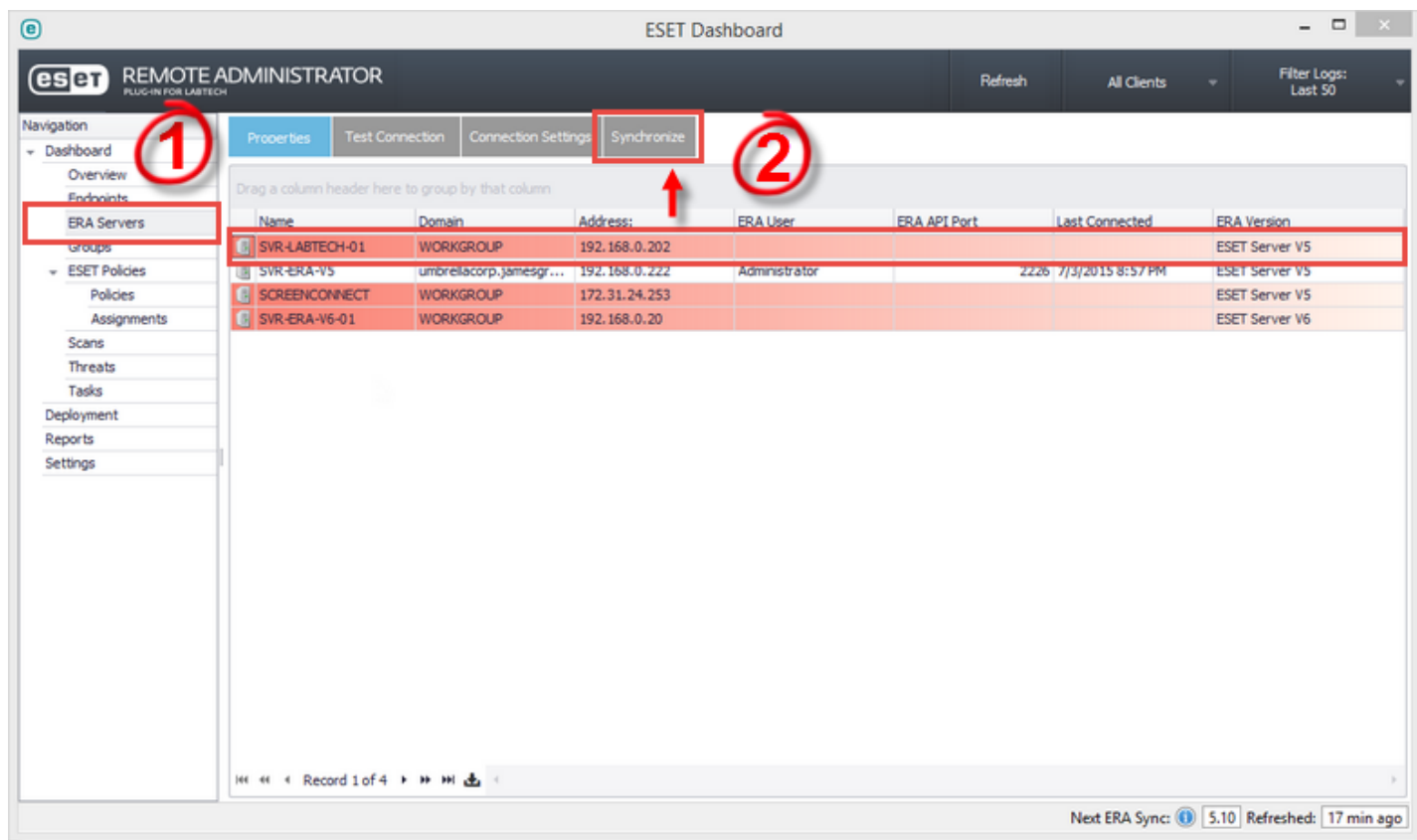


Figure 1-1

4.7.5 Update server connection settings

To update connection settings for a server:

1. In the ConnectWise Automate plug-in Navigation menu, click **ERA Servers**.
2. Select a server and click **Connection Settings**.

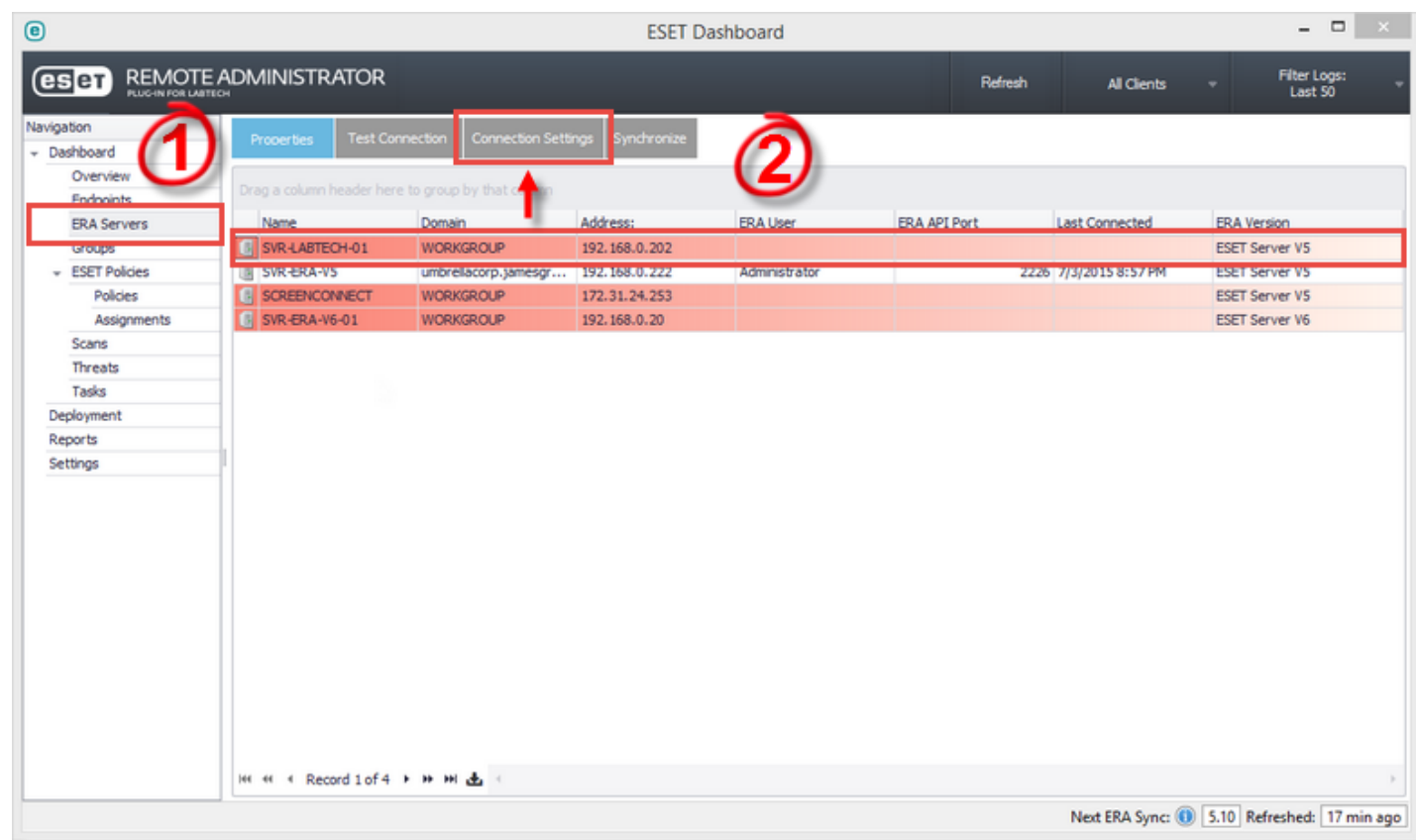


Figure 1-1

4.8 Using the ESET Dashboard

This section includes the following topics:

- [Access and setup the ESET Dashboard](#)
- [Filter data in the Dashboard](#)
- [Navigate the Overview window](#)
- [Viewing reports](#)

4.8.1 Access and setup the ESET Dashboard

Access the ESET Dashboard

Once the ESET Server has been detected by ConnectWise Automate, you can access the ESET Dashboard. Click **ESET Dashboard** to do so.

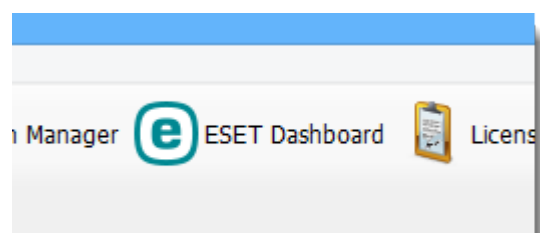


Figure 1-1

NOTE: If you receive a notification about your server downloading dependencies, this is expected within the first few minutes of installing or updating the plug-in. Close the notification and retry a few minutes later. If the notification still appears, refer to [Support and Troubleshooting](#) for what to do to resolve this issue.

ESET Dashboard Setup

The ESET Server setup screen will be displayed the first time you open the ESET Dashboard. To set up a connection to a detected ESET Server:

1. Select the ESET Server you want to connect to from the table.
2. Enter the following connection parameters into the appropriate fields:
 - a. **Server Address:** FQDN (Recommended), IP address or host name that all endpoints can use to access the server.
 - b. **Port:** ESET Server API port (TCP 2226 in ERA 5.x or TCP 2223 in ERA 6.x).
 - c. **Username / password:** Credentials used to connect to your ESET Server (the same credentials used to access ERAC).
 - d. **Login Method:** ERA by default. If your server has been set up to authenticate using Windows credentials, select **Windows Authentication**.

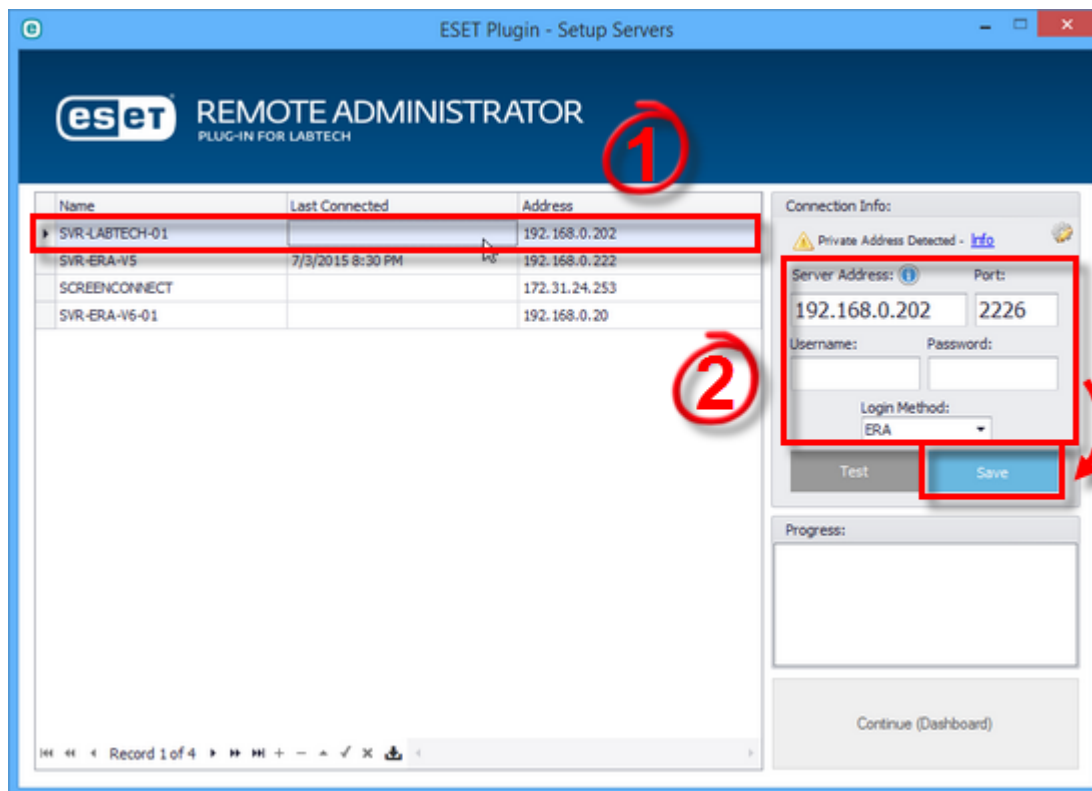


Figure 2-1

4.8.2 Filter data in the Dashboard

Information in the dashboard can be filtered by a number of criteria. Selecting a client will load ESET data relevant for endpoints belonging to that particular client. Click **All Clients** to display data for all clients you have permissions to view.

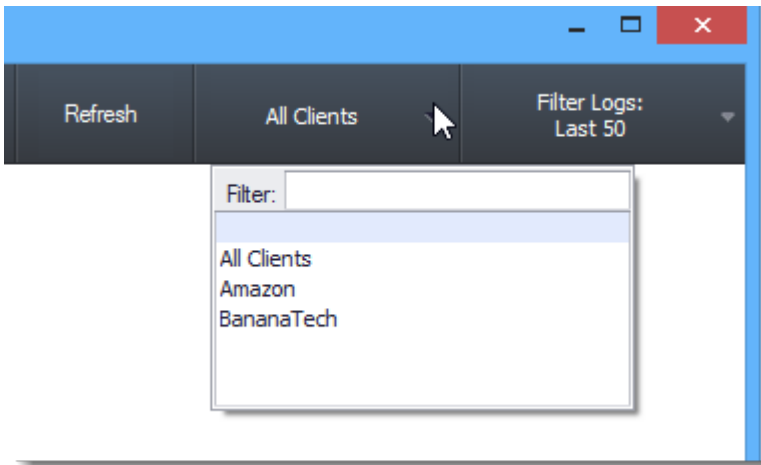


Figure 1-1

Filter Logs will set the maximum number of logs displayed or change the date range for which logs are displayed.

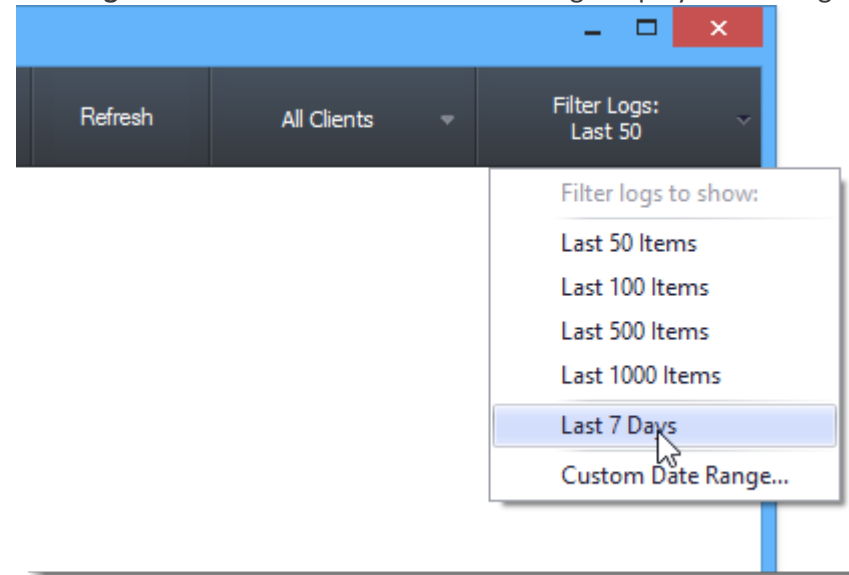


Figure 1-2

Filter Table Data

All tables in the dashboard can be filtered and sorted by any column.

Drag a column header here to group by that column

	Name	Vers...	Primary Server	Product	Loca...	Site	Dom...	Vir
	SVR-LABTECH...	4.5...	SVR-ERA-V5	ESET File Security Mic...	Main ...	BananaTech	work...	11
	SVR-ERA-V5	4.5...	SVR-ERA-V5	ESET File Security Mic...	FL	Amazon	umb...	11

Figure 2-1

Click the filtering icon displayed when you hover over a cell to view filtering options. For example, to find all endpoints with "Server" in the name:

1. Hover over the **Name** column and click the filter icon.
2. Click **Custom** to bring up the custom filter options.
3. Select **Is like** from the condition drop-down menu.
4. Type **Server** into the value field.
5. Click **OK** to view filtered results.

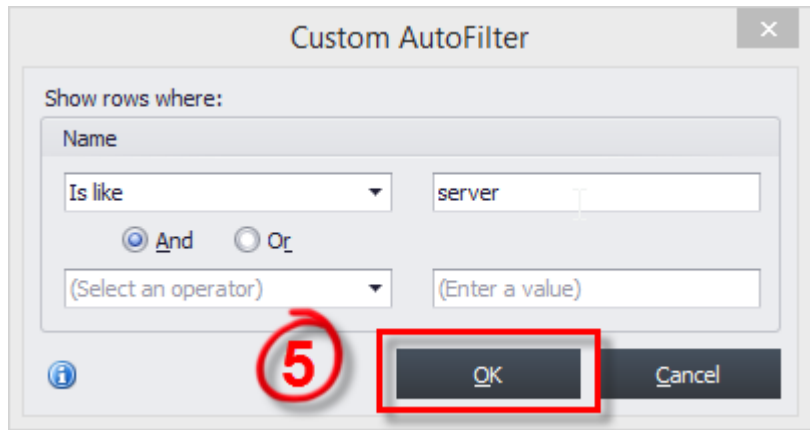


Figure 2-2

Group Table Data

You can use grouping to sort data. Tables that allow grouping will display a group box and the notification "drag a column header here to group by that column."

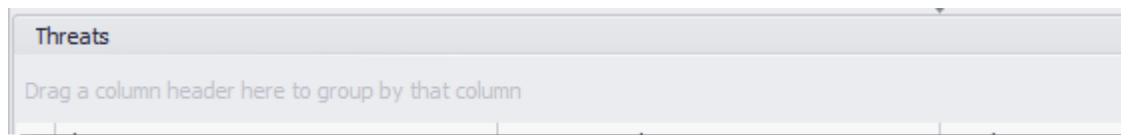


Figure 3-1

To group by a column, drag any column into the group box and drop it. The table will update instantly. The example below shows a table grouped by Task Name.

Name	Date Issued	Server
Name: Scan Task		
6/29/2015 8:17 PM	SVR-EP	
6/19/2015 12:01 AM	SVR-EP	
6/16/2015 10:35 PM	SVR-EP	
Name: Update Task		
6/29/2015 11:36 PM	SVR-EP	
6/29/2015 8:17 PM	SVR-EP	
6/29/2015 8:17 PM	SVR-EP	
6/21/2015 11:58 AM	SVR-EP	
6/20/2015 1:34 AM	SVR-EP	
6/20/2015 1:31 AM	SVR-EP	
6/20/2015 1:04 AM	SVR-EP	
6/20/2015 12:59 AM	SVR-EP	
6/19/2015 9:17 PM	SVR-EP	
6/19/2015 12:02 AM	SVR-EP	
6/19/2015 12:01 AM	SVR-EP	
6/19/2015 12:01 AM	SVR-EP	

Figure 3-2

4.8.3 Navigate the Overview window

The Overview module displays high-level information about your network. The client and log filters at the top of the display can be used to customize which data is shown.



Figure 1-1

Charts

The following charts are shown in the default Overview:

- **Endpoint Definitions:** Displays the number of clients that have up-to-date AV definitions in green and those that do not in orange.

- **Threat Alerts:** A line graph that displays the number of endpoints flagged with threats in the past week.
- **AV Scanners:** Displays the type of security software in place on clients based on data from your ConnectWise Automate AV Scanners.
- **Endpoint Issues:** Displays the number of endpoints currently experiencing issues such as out-of-date system patches, disabled protection, uncleaned threats, etc.

Threat Alerts

- **Alerts Today:** The number of endpoints that flagged threats today
- **Total:** The number of threats present on all endpoints
- **Unique:** The number of unique threats present on your network. For example, three machines with the same threat would be treated as one unique threat.

ESET Endpoints

- **Total:** Total number of endpoints with ESET solutions installed
- **Managed:** Total number of endpoints that can be managed from the plugin
- **Unmanaged:** Total endpoints minus the managed endpoints. This number can be used to identify endpoints that haven't matched up correctly, or endpoints connecting to an ERA server that hasn't been configured in the plug-in.

4.8.4 Viewing reports

The Reports module displays custom reports in the ERA Plug-in for ConnectWise Automate. Other ESET reports are available in ConnectWise Automate Report Manager.

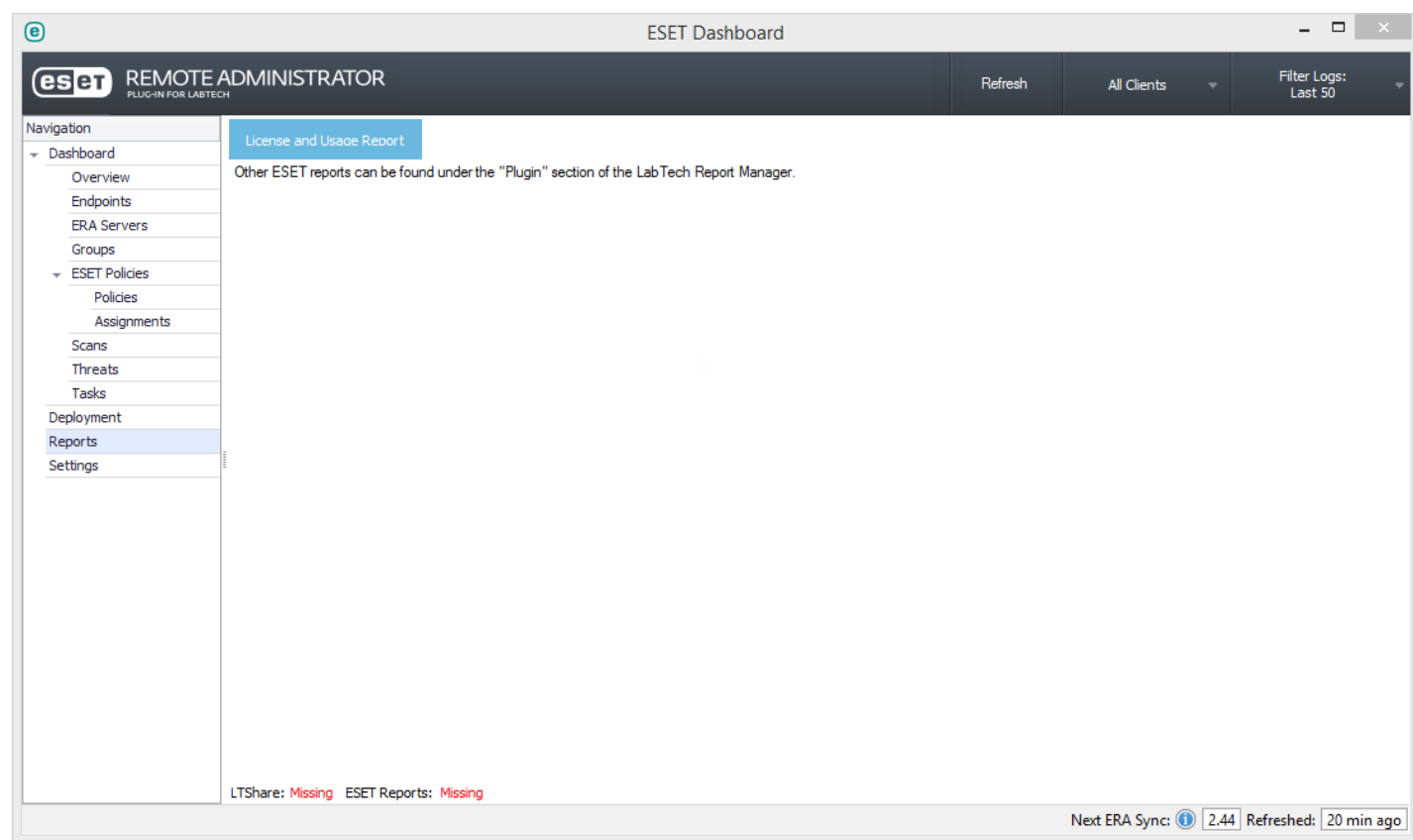


Figure 1-1

This section includes the following topics:

- [View the License and Usage report](#)
- [View the Client/Location Usage report](#)

4.8.4.1 View the License and Usage report

This report contains important licensing information such as total license count, licenses in use, etc.

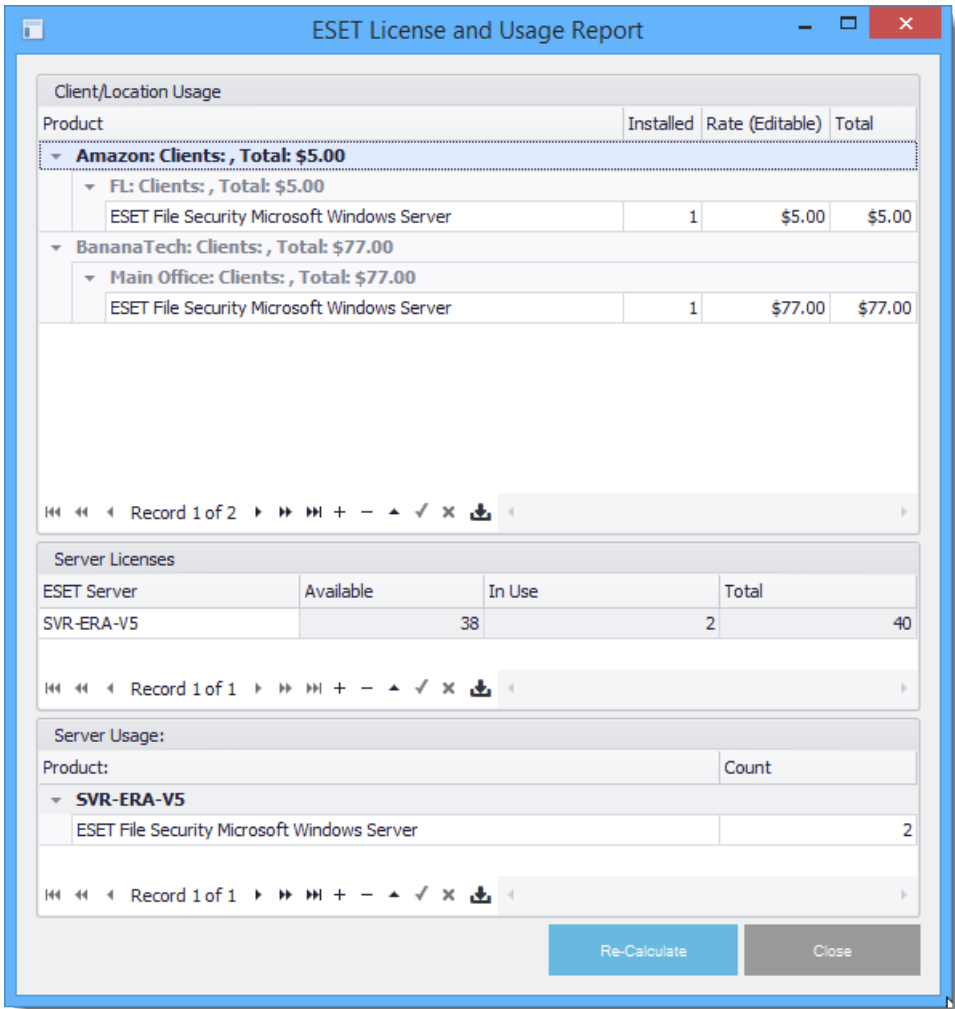


Figure 1-1

4.8.4.2 View the Client/Location Usage report

This report displays a breakdown of ESET product usage by client and location. Additionally, you can type a rate into the **Rate** column and click **Calculate** to update totals. You will be prompted to save your information when you save this report.

5. MSP and Licensing

ConnectWise Automate Partners contact their ConnectWise Automate representative to purchase licenses and to adjust product license quantities.

The two most important components for an ESET ConnectWise Automate MSP/Plug-in user are the **ESET Licensing Administrator (ELA)** and **Security Admin** accounts. See the table below for an overview of the ConnectWise Automate MSP components:

Important components	Description
ERA Plug-in for ConnectWise Automate	The ESET Remote Administrator Plug-in for ConnectWise Automate is developed by ESET in cooperation with ConnectWise Automate to deploy, manage and report on ESET endpoint products within your ConnectWise Automate Console. See Platform Overview for more information.
ESET Licensing Administrator (ELA) https://ela.eset.com/	A version 6 business product licensing management system for ESET licenses. Using ELA, a ConnectWise Automate MSP uses a Security Admin to manage and distribute licenses. After accepting their role, the Security Admin can manage the license (make changes, associate seats, etc.) and can assign licenses to computers (licenses include both MSP and pre-paid/non-MSP).
Agent (ERA)	The ERA Agent is required for the remote management of client computers using ERA version 6. ESET endpoint clients do not communicate with the ERA server directly, and the ESET Remote Administrator Agent facilitates this communication instead. See the section ESET version 6 system architecture overview for more information about the ERA Agent.
ESET Remote Administrator 6 (ERA 6)	ERA allows you to manage ESET products on workstations, servers and mobile devices in a networked environment from one central location. The deployment capability of ERA was originally designed to be used in a contiguous LAN. Since most MSPs connect to their clients over a WAN across the open Internet, a third-party tool is needed to install the ESET clients remotely. Using a Remote Monitoring and Management (RMM) tool is the ideal way to distribute software. However, it is now possible to download the installer directly from the ERA server and with version 6, you can distribute the ERA Agent via Active Directory.
Security Admin	<p>The ERA Plug-in for ConnectWise Automate connects to ELA using the Security Admin account to retrieve license credentials.</p> <p>ConnectWise Automate will associate the Security Admin account to a client site and the ConnectWise Automate MSP manages client sites using unique client certificates. After purchasing or modifying licenses, the ConnectWise Automate MSP uses the plug-in to Synchronize Licenses from an ESET Server to ConnectWise Automate, and the endpoint counts will be updated.</p>
V6 Swap Agreement	A ConnectWise Automate V6 Swap Agreement is required to be in place by ConnectWise Automate before any V6 migrations can commence. Once complete, a signed V6 Swap Agreement will signify to ConnectWise Automate that a Security Admin account is needed. V6 Migrations cannot be completed until a V6 Swap Agreement is signed by the Partner for ConnectWise Automate.

To view license utilization

Log into ELA using your Security Admin credentials. From ELA, you can view activated endpoints and total license utilization, download a license file or offline license file and deactivate endpoints if necessary.

NOTE: ConnectWise Automate MSPs cannot increase license count within ELA. You must contact your ConnectWise Automate representative to adjust license quantities.

6. Support and Troubleshooting

See below for known issues and information to diagnose common issues.

Known Issues

For an up-to-date list of known issues, see [ConnectWise Automate Plug-in Known Issues](#).

Server is downloading dependencies

It is normal for this notification to be displayed within the first few minutes following installation/update of the ERA Plug-in for ConnectWise Automate. Close the notification and attempt your operation again in a few minutes. If the notification continues to appear, restart the ConnectWise Automate database agent (**Control Center > Help > Server Status > Restart Database Agent**). If the issue persists, it is likely that the server cannot access the ESET resource server to download Plug-in dependencies. Test your ConnectWise Automate server to verify that it can access <http://ftp.nod.sk>.

Getting help

If you require assistance with the ERA Plug-in for ConnectWise Automate, please contact ConnectWise Automate support through your regular support channels and review the support procedure below:

1. Partner (ConnectWise Automate customer) contacts ConnectWise Automate support for initial (Level 1) support.
2. If necessary, ConnectWise Automate submits an escalation case to ESET and includes all necessary Partner contact information (for example, name, phone number, email and desired appointment window).
3. ESET Agent schedules an appointment with an ESET MSP Agent.
4. The ESET MSP Agent makes two attempts to reach the Partner. Each call attempt is separated by a 5-10 minute wait and a voicemail is left at each attempt.
5. After two failed attempts, the ESET MSP Agent sends an outbound email from the NetSuite case to ConnectWise Automate support and the Partner requesting a new appointment window. ConnectWise Automate support or the Partner must reply to the case email with the requested information.

To submit feedback or feature requests to ESET, use the [ConnectWise Automate Plug-in Feedback form](#).

Changelog

For an up-to-date list of changes, see the [ERA 6 Plug-in for ConnectWise Automate Changelog](#).

6.1 Database

All endpoint and log data is synchronized with the ConnectWise Automate database. This data can be used to create your own custom reports, monitors and scripts.

With the exception of Role Detection rules, all data from the ERA Plug-in for ConnectWise Automate is contained in tables with the prefix **plugin_eset_ra**. For example, all endpoint threat data is contained in the table **plugin_eset_ra_threat**. See below for a complete list of tables containing plug-in data:

plugin_eset_ra_deployment
plugin_eset_ra_deployment_details
plugin_eset_ra_endpoint
plugin_eset_ra_endpoint_weight

plugin_eset_ra_era
plugin_eset_ra_group
plugin_eset_ra_license
plugin_eset_ra_license_calc
plugin_eset_ra_policy_data
plugin_eset_ra_property
plugin_eset_ra_queue
plugin_eset_ra_scan
plugin_eset_ra_task
plugin_eset_ra_task_detail
plugin_eset_ra_template
plugin_eset_ra_template_config
plugin_eset_ra_template_meld
plugin_eset_ra_template_product
plugin_eset_ra_threat

To use the endpoint-to-agent matches that the plug-in creates and manages, you can use a SQL JOIN statement on the plugin_eset_ra_endpoint_weight table using the primary keys (era_id, client_name, and ComputerID).

Database Maintenance

Truncating log tables such as threats and scans will not have a negative affect on the ERA Plug-in for ConnectWise Automate's performance, but data will not be re-synchronized with the database. Logs use datetime values to determine which data should be requested from the ERA Server. These datetime values are stored in the table **plugin_eset_ra_era** for each ERA server, for example **last_threat** and **last_scan**. These columns can be modified in the event that a backlog sync is required.

6.2 Exporting to Common Formats

All tables can be exported to common formats including CSV, XLS, XLSX, HTML and PDF.

Click **Export** from any table to export its contents.

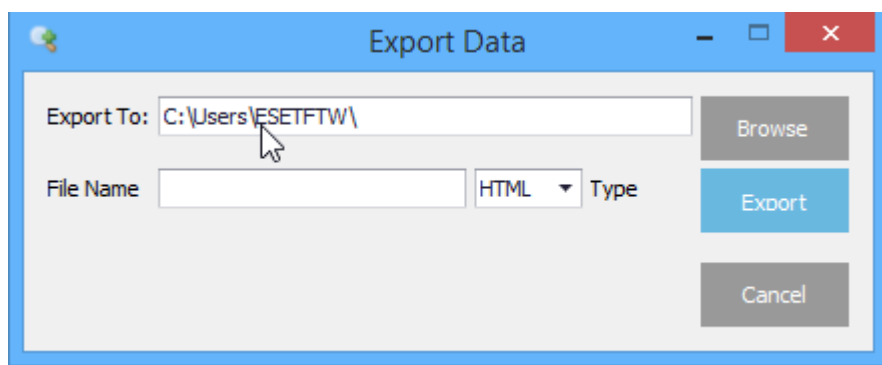


Figure 1-1

In the export data window:

1. Click **Browse** to choose a location to save your file.
2. Type a name for the file in the **File Name** field.
3. Select the document type from drop-down menu.

4. Click **Export**. Your file will automatically be saved with the correct file extension appended.

6.3 Development tickets

To generate an SQL dump for ConnectWise Automate Plug-in development:

1. On a ConnectWise Automate Server, open SQLyog and expand **ConnectWise Automate > Tables**.

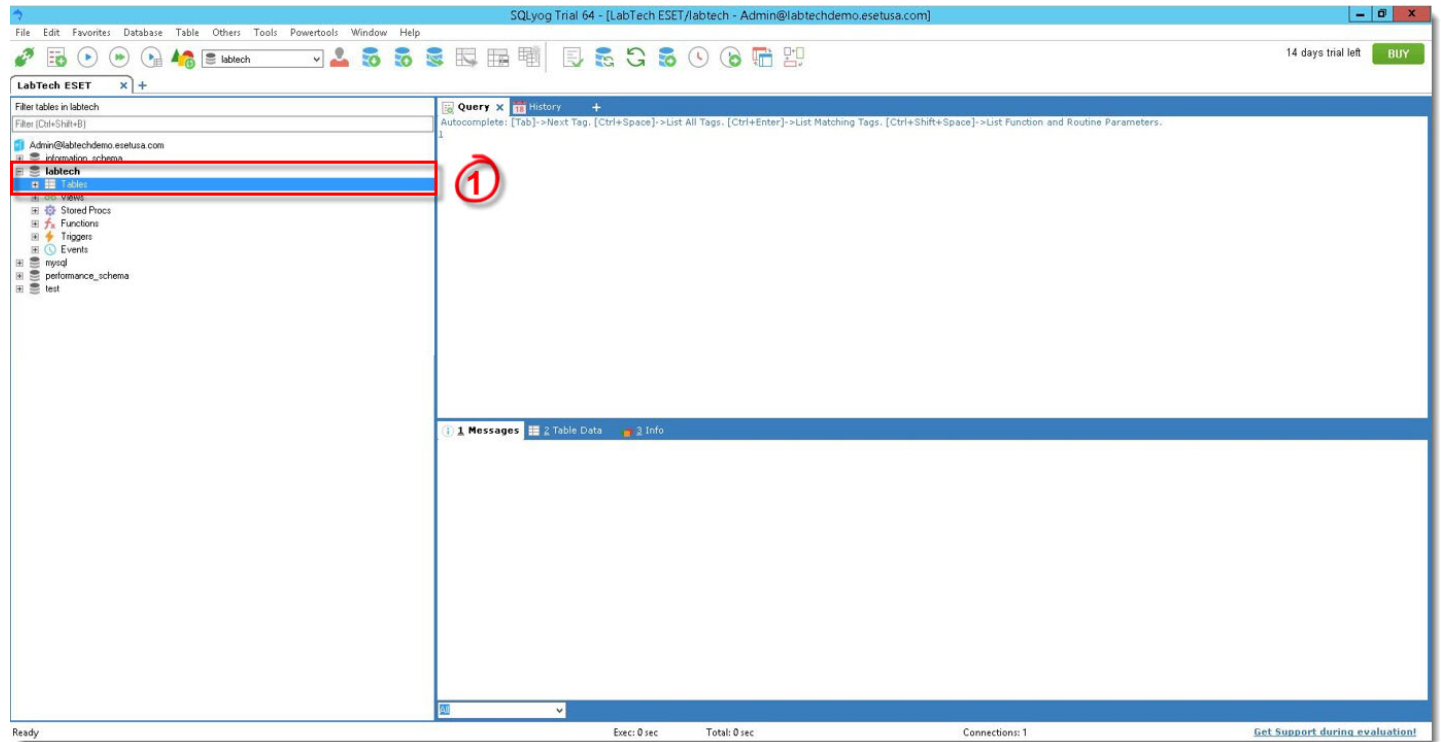


Figure 1-1

2. Select a **plugin_eset_*** table, right-click and then select **Backup/Export > Backup Table(s) As SQL Dump** from the context menu.

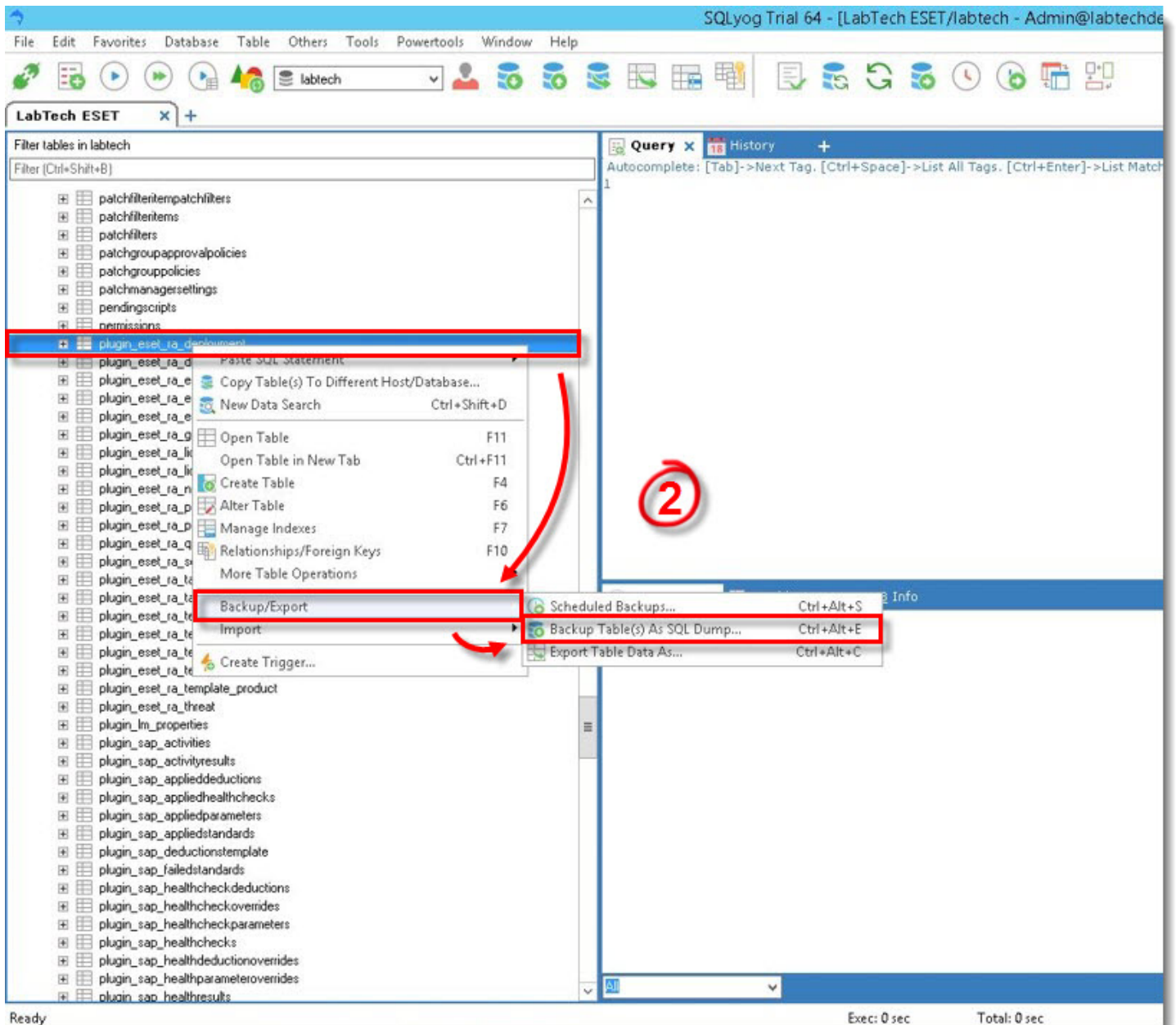


Figure 1-2

3. In the **SQL Dump** window, de-select the checkbox next to **Tables**.

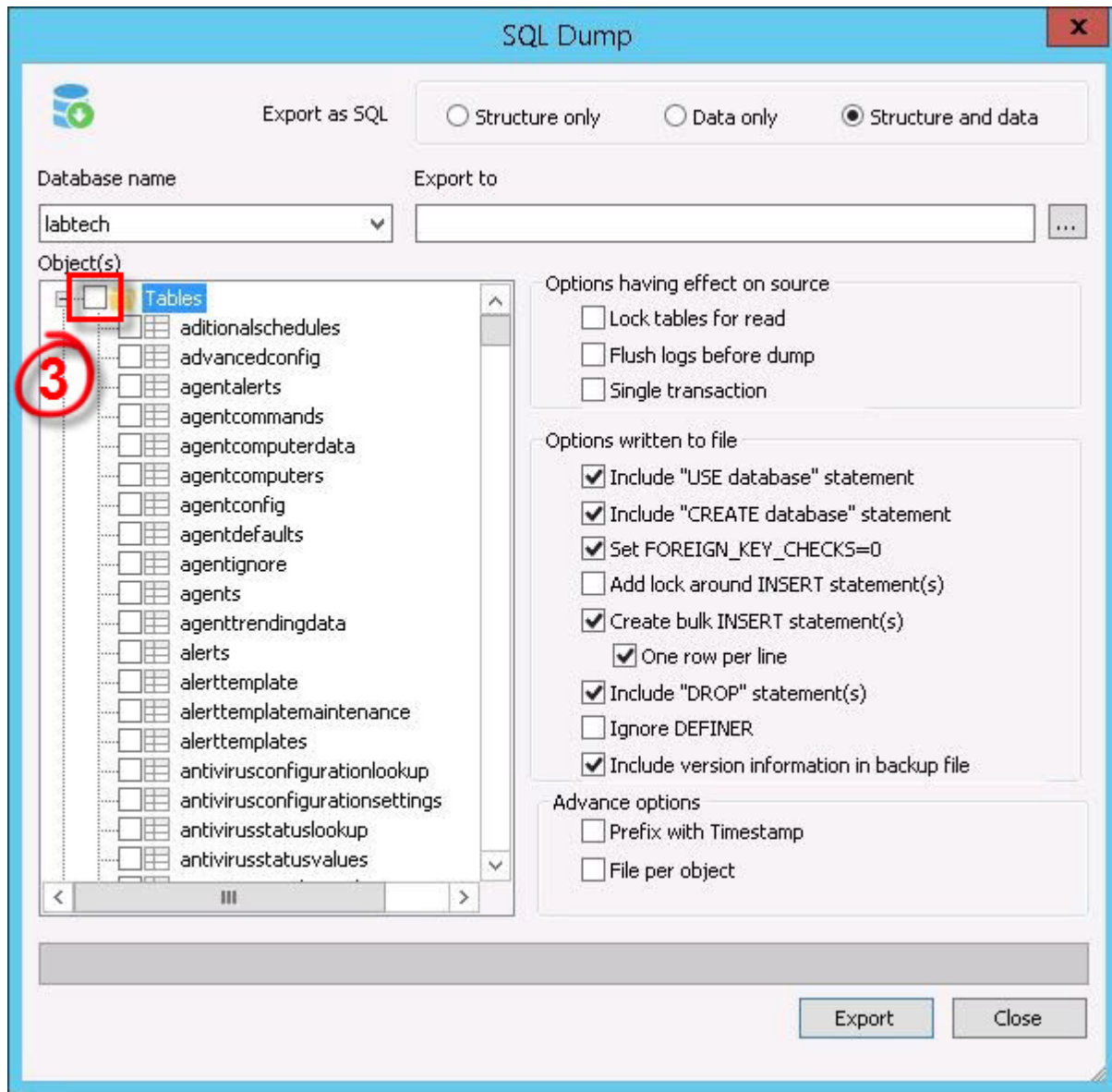


Figure 1-3

4. Select the **plugin_eset_*** tables (or tables specified by support/development). In the **Export to** field, browse to the appropriate file and then click **Export**.

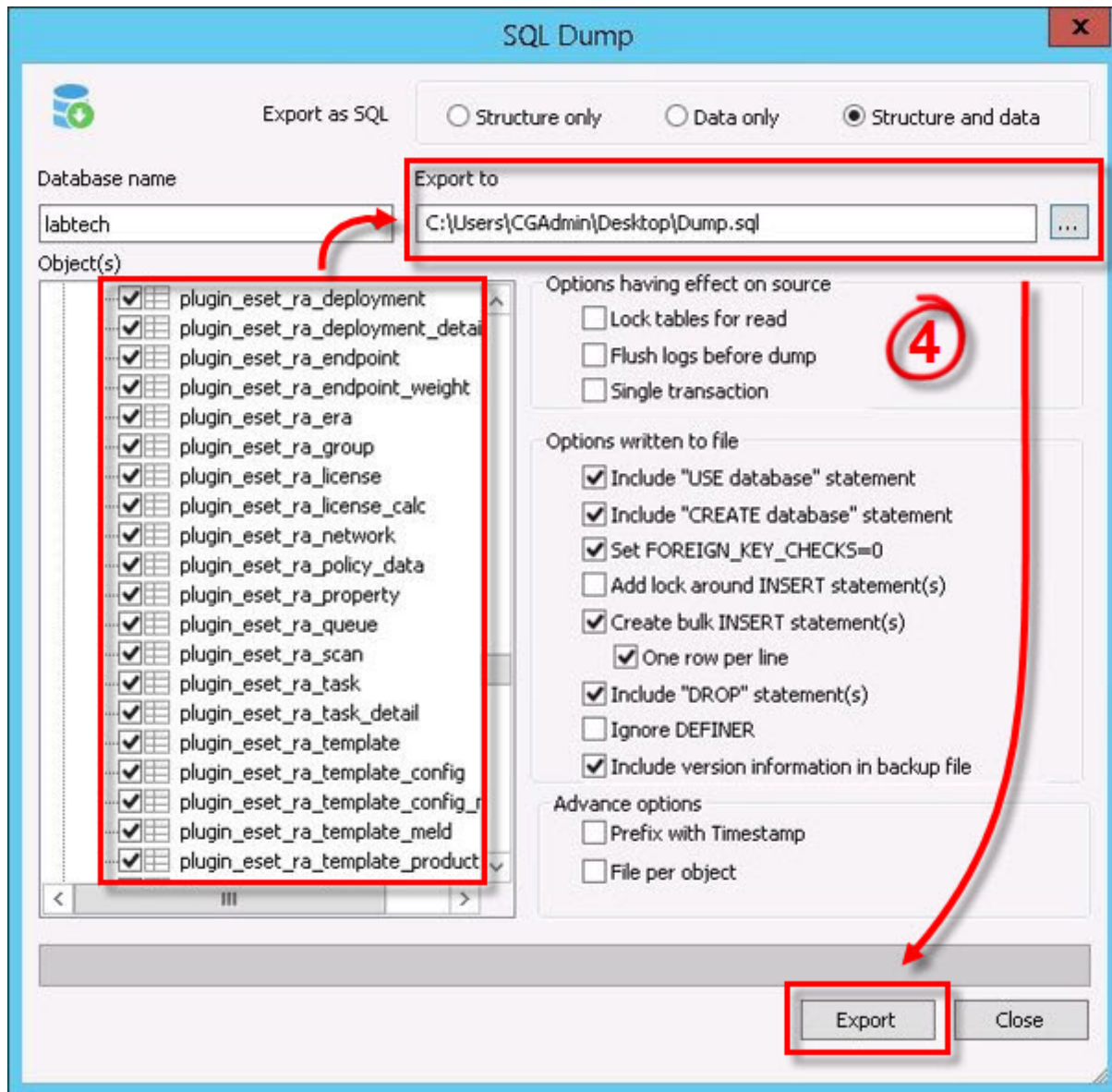


Figure 1-4

5. When the export is complete, upload the saved .sql to support.

6.4 ConnectWise Automate Plug-in Feedback

Additionally, you can submit feedback, make feature requests and send comments about the ERA Plug-in for ConnectWise Automate to our development team using the ESET feedback form. From the ConnectWise Automate Control Center click the ESET menu item and then click **Feedback** to access the form. Your feedback is greatly appreciated, and we encourage you to provide a contact number and email if you'd like to hear from our team.

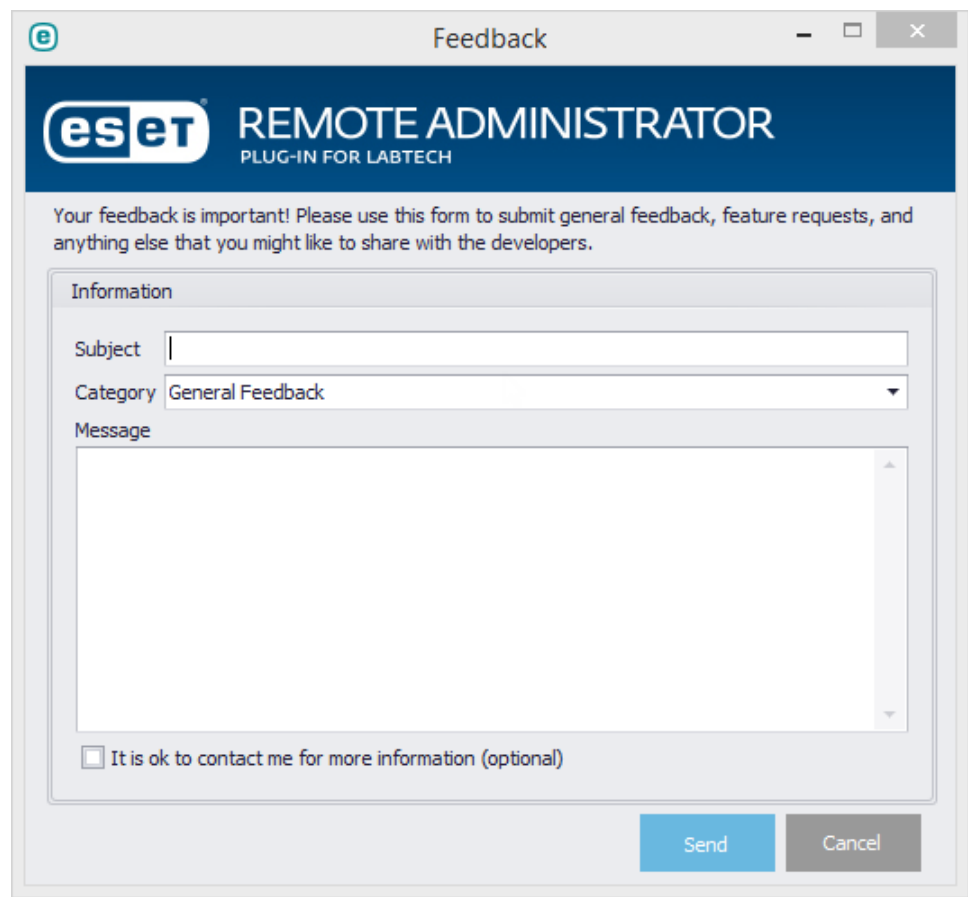
The image shows a window titled "Feedback" with the ESET logo and "REMOTE ADMINISTRATOR PLUG-IN FOR LABTECH" header. Below the header, a message states: "Your feedback is important! Please use this form to submit general feedback, feature requests, and anything else that you might like to share with the developers." The form contains an "Information" section with a "Subject" text box, a "Category" dropdown menu set to "General Feedback", and a "Message" text area. At the bottom of the form is a checkbox labeled "It is ok to contact me for more information (optional)". Two buttons, "Send" and "Cancel", are located at the bottom right of the window.

Figure 1-1

6.5 ConnectWise Automate Plug-in Known Issues

The following Known Issues list is for the ERA Plug-in for ConnectWise Automate version 2.0.4.8:

Version 6 Policy Editor window opens but is blank/unable to load content.

This is due to an older version of the JQuery library not being properly updated. On the ConnectWise Automate server, navigate to `C:\LTShare\Transfer\Software\ESET\V6CfgEdit` and open the "j" folder, and rename the file `001_jquery-1.11.3.min.js` to `001_jquery-1.10.2.min.js` close the plug-in and reopen it.

Version 6 Policy Editor gives an error saying the hostname could not be resolved but the ERA connection test is successful.

There is a new field under **Settings** for "Server Address," in some instances this gets populated with the "http://" in front of the hostname, causing a conflict. Ensure this field only contains the hostname, without any protocol (http/https) or other data (example: hostname.com).

Also found in **Settings** is a "Use SSL for v6 Configuration Editor" check box, this is for cases where your server is using SSL and potentially port 80 is blocked. This will tell the configuration editor to instead use SSL over port 443.

Under 'Deployment', a 'Migration' task will not allow the 'Activate Endpoints' button to become active.

If the migration has already been performed for a given group or endpoint(s), a workaround is to create an identical task, but as "Deploy ESET Software" instead of "Migrate," this task will fail because all detected endpoints already have ESET, but will allow an activation to be performed to the same group of endpoints.

Unable to "force" install/uninstall task to endpoints.

Due to the nature of detection, sometimes a task will fail thinking ESET is already installed. This should be exercised with extreme caution, but in the Deployment task steps, there is an "Advanced" menu where you select the ERA, selecting "Override Status" will ignore ESET detection and attempt the task regardless.

For an up-to-date list of changes, see the [ERA 6 Plug-in for ConnectWise Automate Changelog](#).

Devices with multiple MAC addresses will not automatically populate the ConnectWise Automate Plug-in.

Multiple MAC addresses can be identified in ESET Remote Administrator by selecting the device, left-clicking and from the context menu selecting **Details**. Scroll down to **Network Adapters** and you should see only one or two entries. You should see two entries per NIC—one for IPv4 and one for IPv6. If more than two NICs are seen, multiple MAC addresses will be an issue.

Solution: [Manually map an ESET endpoint to a ConnectWise Automate Agent](#).

6.6 ERA 6 Plug-in for ConnectWise Automate Changelog

Version 2.5.0.x

- **Added:** Several ConnectWise Automate Monitors. For example:
 - Protection Disabled
 - Product Not Activated
 - Out of Date Modules
 - Unhandled Threat Detection
 - If the real time scanner detects a threat and the threatlog reports a status containing the word "critical" or "error", an entry to this threat will be added to a newly designed table representing active threats. These active threats will be cleared on two conditions. An AV scan for the machine in question returns 0 infected files, or the threat is "Archived" in the plug-in.
- **Added:** Ability to "Delete" an ERA server from the ERA Server page of the plug-in.
Note: If a server with a ConnectWise Automate agent and ESET role is detected, it will be re-added.
- **Added:** "Site" (ConnectWise Automate Client) and ConnectWise Automate "Location" columns to Scans, Threats and Tasks. These are hidden by default but may be enabled by using the column chooser on the respective page.
- **Added:** the ability to click on a graph in the Dashboard. This will take you to the related page and group the data by the appropriate column.
- **Added:** ERA Actual and Requested policy info to client properties. This should make it easier to track down the policy on the ERA server itself.
- **Added:** Ability to create an activation task via the "Endpoints" section of the plug-in.
- **Improved:** Uninstalling clients via deployment will now remove their record from the ERA server.
- **Improved:** Creating a new policy will now refresh the policies table.

- **Improved:** Overview graphs and data should now provide a more accurate representation of the status of your environment.
- **Improved:** Deployment has been re-written to be more reliable, for example:
 - **Added:** The ability to "Override Status" when performing an uninstall deployment.
 - **Changed:** When running an ESET deployment on a specific ConnectWise Automate computer via the Control Center the "override status" option will be automatically enabled.
 - **Changed:** Upon successful deployment, a ConnectWise Automate task will be created to refresh system information. This should help reduce the number of false-positives and false-negatives regarding current AV status.
 - **Changed:** When creating a deployment task, "override status" and "persistent" options are now mutually exclusive.
 - **Changed:** Migration deployment tasks can now be used to move ESETv5 Clients to v6 as well as move v6 clients from one server to another v6 server (can be used to fix broken ERA agent installs).
 - **Changed:** When deploying to a v6 server, version 6 products will now populate at the top of the product selection drop-down list.
 - **Changed:** When creating an "install" deployment, the OS selection dialog will now appropriately display only OSs compatible with the product being deployed.
 - **Fixed:** Typo that caused the review panel of deployment to show a group as the target for a one-off deployment task.
- **Improved:** Endpoint matching now properly takes last connected time into account upon finding duplicate ERA endpoint records.
- **Improved:** Moved many of the data queries into views.
- **Improved:** Added several indexes to ESET tables in the database to improve performance of the plug-in.
- **Changed:** V6 Role Definition for clients updated with new regex that should be compatible all the way up to 6.x.
- **Fixed:** Minor Text and grammatical errors.
- **Fixed:** V6 Configuration editor will now properly request pages from the ERA server in the correct order.
- **Fixed:** V6 Configuration editor should be more obvious to configure for ConnectWise Automate servers using SSL.
- **Fixed:** V6 Mac address/IP Address mapping issue should be resolved (Rare case where client machine had many, many Mac addresses due to VMWare).
- **Fixed:** An issue that could occur if a policy had special characters in the description field.
- **Fixed:** An issue where an invalid SSL cert could prevent the v6 policy editor from loading.
- **Fixed:** An issue that could cause multiple persistent deployment tasks to run on the same machine if they took longer than six minutes to run.
- **Fixed:** An issue that was causing computers removed from a ConnectWise Automate group to retain their previous groups' policy.
- **Fixed:** An issue that was causing the "Hide Groups without ESET Policies" to cause an error.

Version 2.0.4.8

- **Added:** Support for ERA 6.4.
- **Added:** Linux ERA 6.4 Role support.
- **Added:** Support for migrations from version 5 to 6.
- **Added:** Settings page includes a ConnectWise Automate server hostname field.
- **Added:** Settings page includes checkbox to use SSL for v6 configuration editor.
- **Added:** Option for custom v6 Agent Port during deployment.
- **Fixed:** Policy sync would break when assigning too many groups, extended amount of groups assignable per group.
- **Fixed:** Issue with endpoints being moved to incorrect policies during sync, particularly with very long policy names. Policy name length was being cut too short, length extended.
- **Fixed:** Client Filtering not working on Endpoints page. Filtering now works across all pages.
- **Fixed:** User Permissions for groups and sites, users should only see groups and sites they have permissions for.
- **Fixed:** Endpoint Properties "Effective Policy" button shows incorrect policy.

- **Fixed:** Bug causing language section under deployment to select the wrong default language.
- **Fixed:** Protection page under Endpoint Properties now displays multiple status messages separated by new line.
- **Fixed:** Issue with V6 Policy Editor pointing to wrong server in certain cases.
- **Fixed:** Issue with older threat data not being properly deleted.
- **Fixed:** Issue with deployment flags for reboot and conflicts not being properly detected.