ESET
REMOTE ADMINISTRATOR PLUG-IN For LabTech

Technical Setup and User Guide

Click here to download the latest version of this document

ESET REMOTE ADMINISTRATOR PLUG-IN FOR LabTech

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

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. 9/29/2015

1. Introduction

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

The ESET Remote Administrator Plug-in for LabTech is developed by ESET in cooperation with LabTech to deploy, manage and report on ESET endpoint products within your LabTech Console. With a host of new features built based on customer feedback, this solution allows LabTech users to more efficiently meet the needs of their customers.

Partner feedback 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 Glossary of terms

Agent —Typically used to refer to the LabTech Agent and the device the agent is installed on.

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.

ERAC —ESET Remote Administrator Console, sometimes referred to as the ESET Console.

- **Version 5**: A lightweight, portable frontend UI component that connects to the ERA server. The ERAC is the interface used to effect changes to devices managed by ESET Remote Administrator.

- **Version 6**: The ERA 6.x Web Console is accessed via your web browser. From the Web Console you can make changes to and manage your ESET products.

2. Prerequisites

LabTech RMM

- LabTech Server 2013 or later (Cloud or on-premise)

ESET Remote Administrator

- ESET Remote Administrator Server 6.2 or later

OR

- ESET Remote Administrator Server 5.2 or later
- (Optional - ERA 5.x only) ESET MSP Utilities - EMU

LabTech Server:

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

- LabTech2013 —Installation Prerequisites
- LabTech 10 —Installation Prerequisites

NOTE: Your LabTech server must have Internet access to download dependencies from http://ftp.nod.sk. To verify the connection, visit the following address: http://ftp.nod.sk/~esetmsp/RMM/LabTech/

ESET Remote Administrator Server Version 6.x:

Installing ESET Remote Administrator 6.x

You can download the latest Windows installers for ERA 6.x from 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 LabTech 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 optimal operation of the ERA Plug-in for LabTech, 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 LabTech server, or an instance of the LabTech 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

ESET Remote Administrator Server Version 5:

Installing or upgrading from ESET Remote Administrator 5.x or earlier

You can install or update your ERA Server to the latest LabTech supported version using the Smart Installer, or by downloading the latest ERA Server and ERAC versions from ESET.com using the links below. 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 LabTech server on the same computer.

- Download ESET Remote Administrator Server
- Download ESET Remote Administrator Console

For optimal operation of the ERA Plug-in for LabTech, make sure that the ESET Remote Administrator Server meets the minimum hardware and software requirements as described in the ESET Remote Administrator User Guide.

Network Configuration

The ESET Server should be accessible from a static IP address or hostname (recommended). If ESET endpoints, the LabTech server, or an instance of the LabTech 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 Console connection
TCP 2226 - ERA API / plug-in connection

ESET MSP Utilities (EMU)

This plug-in works independent of licenses—EMU is required to handle MSP licenses.

Follow the documentation available here to download and install ESET MSP Utilities. An ERA Key will be required and can be obtained by contacting LabTech.

3. Installation

Installation steps will differ slightly depending on the version of LabTech you are using:

- **LabTech 10**—Install from the LabTech Solution Center
- **LabTech 2013**—Install from Plugin Manager

3.1 Install from Solution Center

Solution Center can only be opened on your LabTech server. If you do not have access to your LabTech server, please contact LabTech support for assistance. Follow the steps below to install the ERA Plug-in for LabTech from Solution Center:

1. On your LabTech server, open a new instance of LabTech Control Center.

2. Click **Tools** > **Solution Center**.

3. Click **Security**.

4. Select **ESET Plugin v2** and click **Queue**.

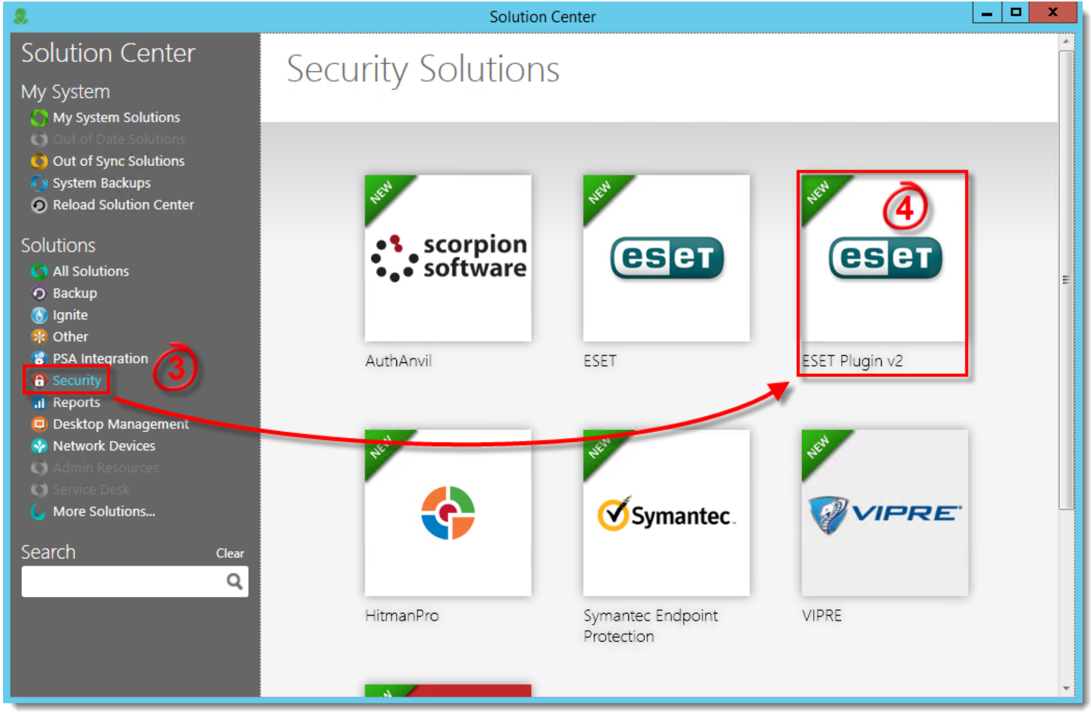


Figure 1-1

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 LabTech Control Center instances to allow the new plug-in to load.

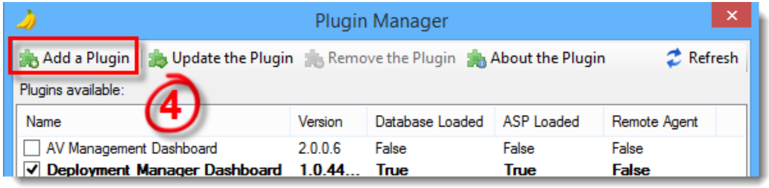
3.2 Install from Plugin Manager

1. Download the latest ESET Remote Administrator Plug-in for LabTech.

2. When your download finishes, extract the ZIP file to a safe location.

3. Open LabTech Control Center and click **Help** > **Plugin Manager**.

4. Click **Add a Plugin**.



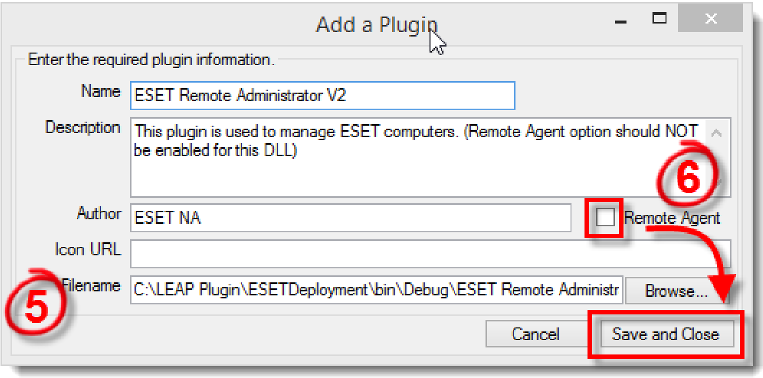
Plugins available:

	Name	Version	Database Loaded	ASP Loaded	Remote Agent
□	AV Management Dashboard	2.0.0.6	False	False	False
☑	**Deployment Manager Dashboard**	**1.0.44...**	**True**	**True**	**False**

Figure 1-2

5. Navigate to the files you downloaded in step 1, select **ESET Remote Administrator V2.dll** and click **OK**.

6. Make sure that the check box next to **Remote Agent** is deselected. Click **Save and Close** when you are finished.



Enter the required plugin information.

Name: ESET Remote Administrator V2

Description: This plugin is used to manage ESET computers. (Remote Agent option should NOT be enabled for this DLL)

Author: ESET NA □ Remote Agent

Icon URL:

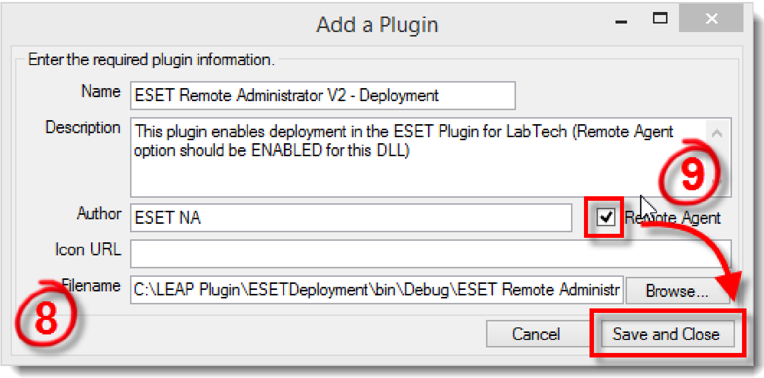
Filename: C:\LEAP Plugin\ESETDeployment\bin\Debug\ESET Remote Administr

Figure 1-3

7. Click **Add a Plugin**.

8. Navigate to the files you downloaded in step 1, select **ESET Remote Administrator V2 - Deployment.dll** and click **OK**.

9. Make sure the check box next to **Remote Agent** is selected. Click **Save and Close** when you are finished.



Enter the required plugin information.

Name: ESET Remote Administrator V2 - Deployment

Description: This plugin enables deployment in the ESET Plugin for LabTech (Remote Agent option should be ENABLED for this DLL)

Author: ESET NA ☑ Remote Agent

Icon URL:

Filename: C:\LEAP Plugin\ESETDeployment\bin\Debug\ESET Remote Administr

Figure 1-4

10. Click **Refresh** in LabTech Plugin Manager.

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

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

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

4. Initial Setup

Get started using the ERA Plug-in for LabTech by making sure you can detect your ERA Server(s) and access the ESET Dashboard.

4.1 Detect ESET Servers

Detect ESET Servers

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

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

1. Right-click the LabTech agent, client, location or group that contains an agent hosting your ESET Server.

2. Select **Commands** > **Inventory** > **Resend System info**.

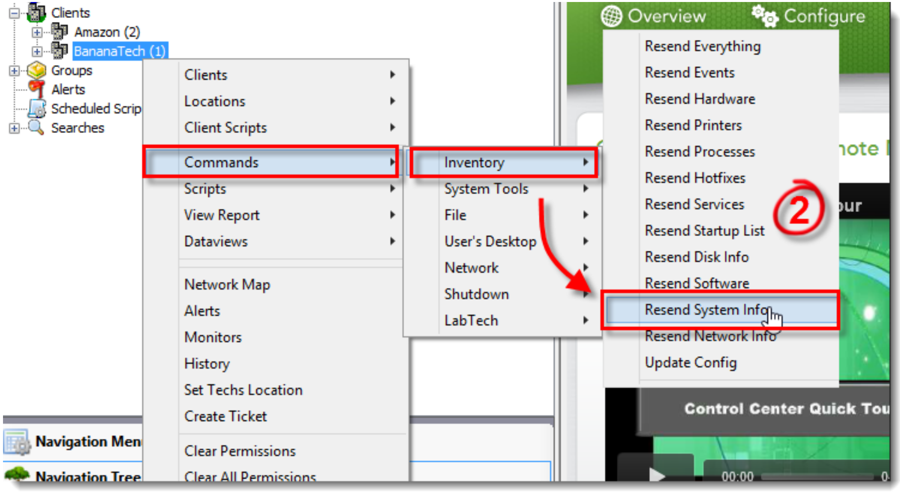


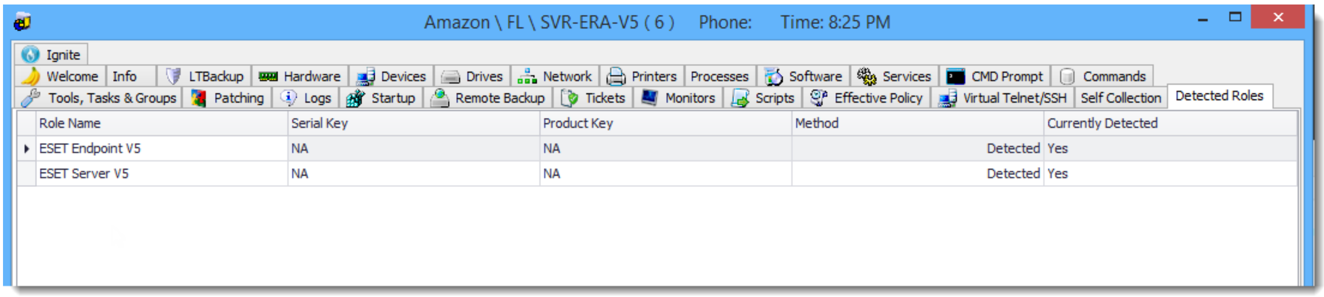
Figure 1-5

3. Repeat step 2 but select **Commands** > **Inventory** > **Update Config**.

Verify that ESET Servers are detected

1. Open the Computer Window of a LabTech agent and click the **Detected Roles** tab.

2. **ESET Server V5** or **ESET Server V6** should be displayed as a detected role.



Role Name	Serial Key	Product Key	Method	Currently Detected
ESET Endpoint V5	NA	NA	Detected	Yes
ESET Server V5	NA	NA	Detected	Yes

Figure 1-6

Force ESET Server detection

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

1. Open the Computer Window of a LabTech agent and click the **Detected Roles** tab.

2. Click **Overrides**.

3. Click **Add**.

4. Select **ESET Server V5** or **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.

4.2 The ESET Dashboard

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

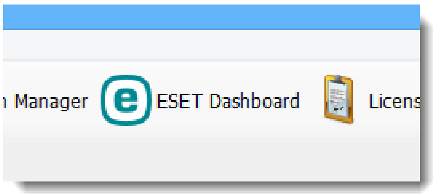
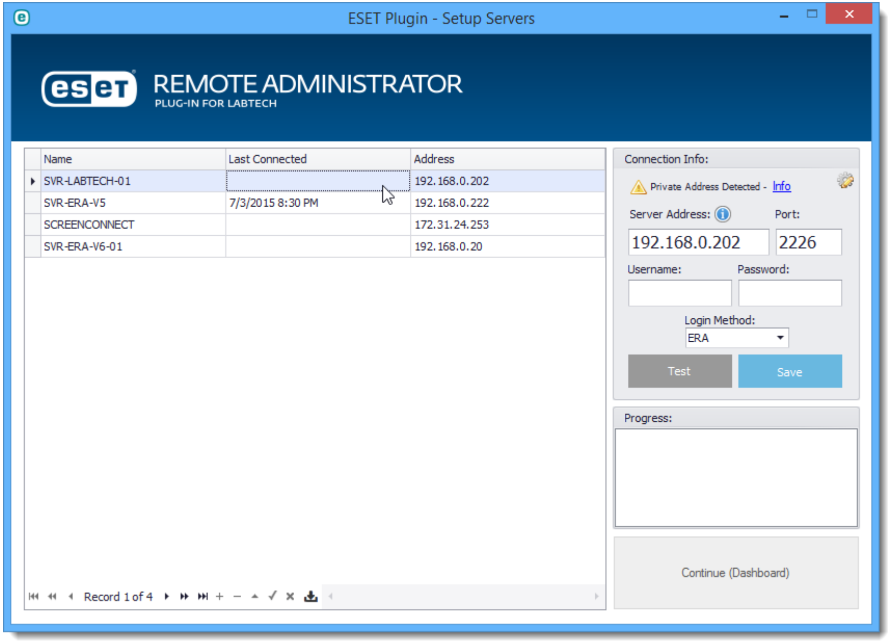


Figure 1-7

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, follow these instructions to resolve it.

ESET Dashboard Setup

The ESET Server setup screen will be displayed the first time that you open the ESET Dashboard.



ESET Plugin - Setup Servers

REMOTE ADMINISTRATOR
PLUG-IN FOR LABTECH

Name	Last Connected	Address
SVR-LABTECH-01		192.168.0.202
SVR-ERA-V5	7/3/2015 8:30 PM	192.168.0.222
SCREENCONNECT		172.31.24.253
SVR-ERA-V6-01		192.168.0.20

Record 1 of 4

Connection Info:

Private Address Detected - Info

Server Address: 192.168.0.202

Port: 2226

Username:

Password:

Login Method: ERA

Figure 1-8

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**.

4.2.1 Filtering 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.

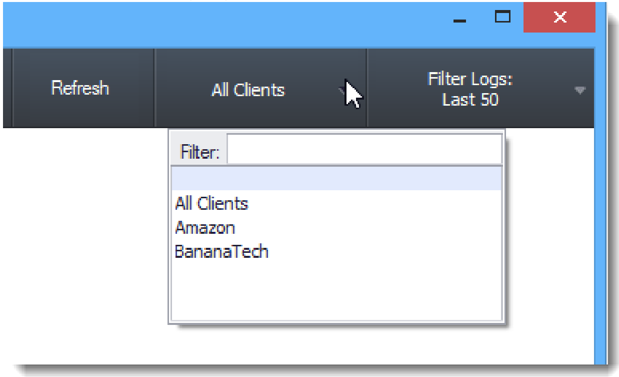


Figure 1-9

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

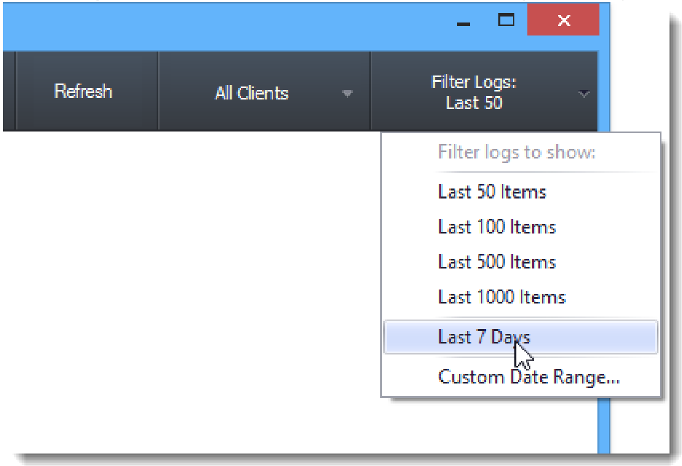
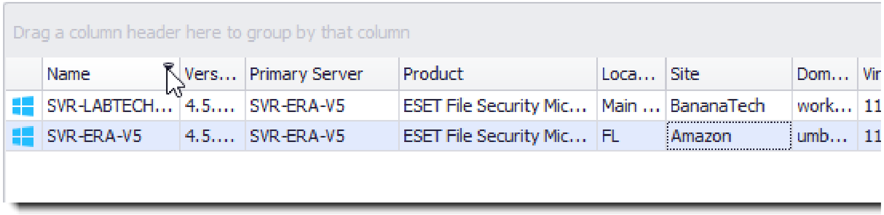


Figure 1-10

Filtering 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 1-11

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:

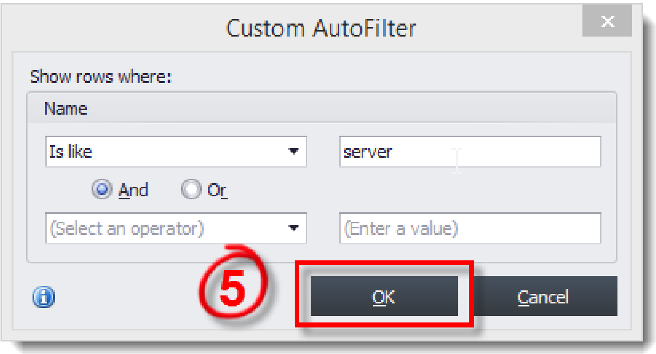
1. Hover over the **Name** column and click the filter icon.

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.



Custom AutoFilter

Show rows where:

Name

Is like ▾ server

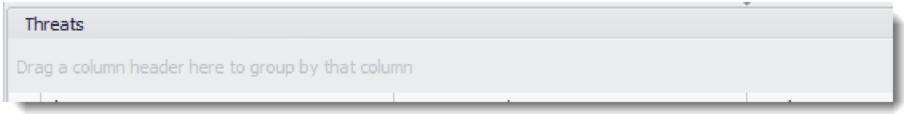
● And ○ Or

(Select an operator) ▾ (Enter a value)

Figure 1-12

Grouping 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."

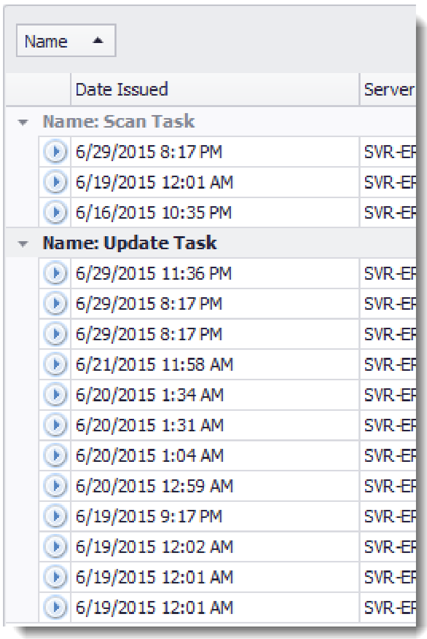


Threats

Drag a column header here to group by that column

Figure 1-13

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 ▲

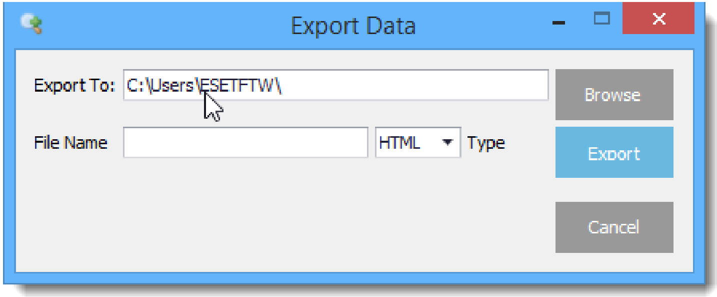
Date Issued	Server
Name: Scan Task	
6/29/2015 8:17 PM	SVR-EF
6/19/2015 12:01 AM	SVR-EF
6/16/2015 10:35 PM	SVR-EF
Name: Update Task	
6/29/2015 11:36 PM	SVR-EF
6/29/2015 8:17 PM	SVR-EF
6/29/2015 8:17 PM	SVR-EF
6/21/2015 11:58 AM	SVR-EF
6/20/2015 1:34 AM	SVR-EF
6/20/2015 1:31 AM	SVR-EF
6/20/2015 1:04 AM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

Figure 1-14

4.2.2 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.



Export Data

Export To: C:\Users\ESETFTW\

File Name

HTML Type

Figure 1-15

In the export data window:

1. Click **Browse** to choose a location to save your file.

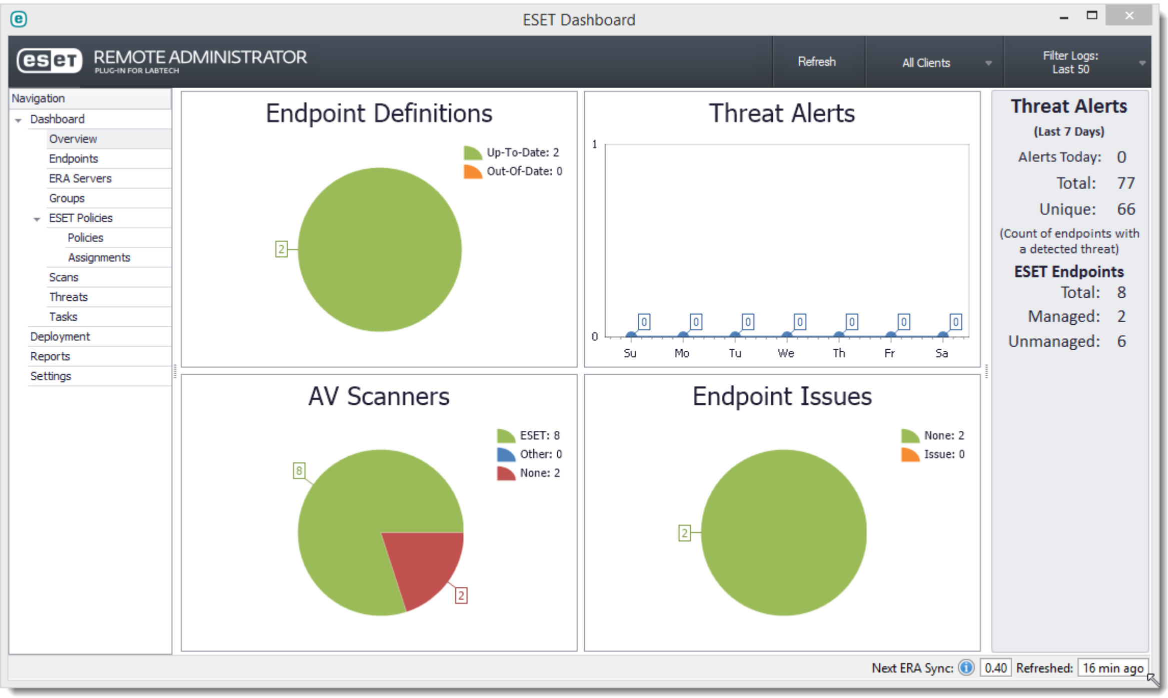
2. Type a name for the file in the **File Name** field.

3. Select the document type from drop-down menu.

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

4.2.3 Overview Module

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.



Filter Logs: Last 50

Threat Alerts
(Last 7 Days)
Alerts Today: 0
Total: 77
Unique: 66
(Count of endpoints with a detected threat)

ESET Endpoints
Total: 8
Managed: 2
Unmanaged: 6

Next ERA Sync: 0.40 Refreshed: 16 min ago

Figure 1-16

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 LabTech AV Scanners.
- **Endpoint Issues**: Displays the number of endpoints currently experiencing issues such as out-of-date system patches, disabled protection, uncleaned threats, etc.

The Details Panel

Threat Alerts

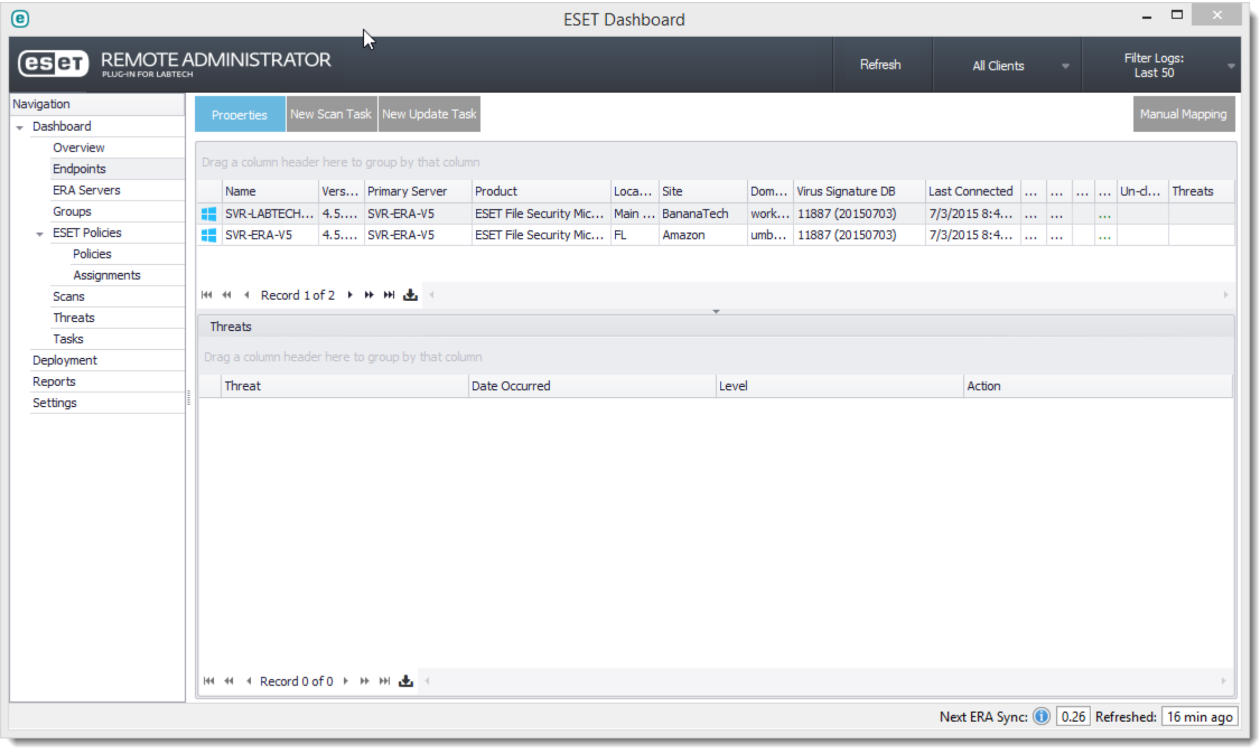
- **Alerts Today**: The number of endpoints that flagged threats today
- **Total**: The number of threats present on all endpoints
- **Unique**: The number of unique threats present on your network. For example, three machines with the same threat would be treated as one unique threat.

ESET Endpoints

- **Total**: Total number of endpoints with ESET solutions installed
- **Managed**: Total number of endpoints that can be manged 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.

4.2.4 Endpoint Module

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

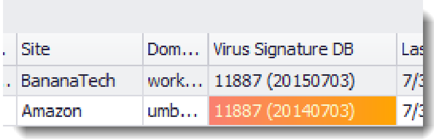


	Name	Vers…	Primary Server	Product	Loca…	Site	Dom…	Virus Signature DB	Last Connected	…	…	…	…	Un-cl…	Threats
	SVR-LABTECH…	4.5.…	SVR-ERA-V5	ESET File Security Mic…	Main …	BananaTech	work…	11887 (20150703)	7/3/2015 8:4…	…	…		…		
	SVR-ERA-V5	4.5.…	SVR-ERA-V5	ESET File Security Mic…	FL	Amazon	umb…	11887 (20150703)	7/3/2015 8:4…	…	…		…		

Threat	Date Occurred	Level	Action

Figure 1-17

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

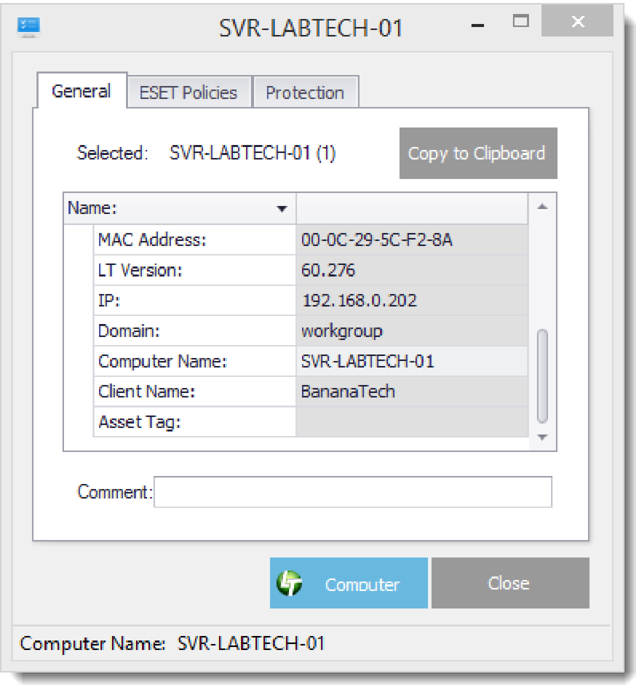
Figure 1-18

Displaying Endpoint Threats

Select an endpoint to display un-archived threats for those endpoints in the table below. Right-click a threat and select **Archive Threat** to remove it from the table.

Displaying Endpoint Properties

Double-click an endpoint row or select an endpoint and click **Properties** to display the Endpoint Properties window.



SVR-LABTECH-01

General | ESET Policies | Protection

Selected: SVR-LABTECH-01 (1)

Name:	
MAC Address:	00-0C-29-5C-F2-8A
LT Version:	60.276
IP:	192.168.0.202
Domain:	workgroup
Computer Name:	SVR-LABTECH-01
Client Name:	BananaTech
Asset Tag:	

Comment:

Computer Name: SVR-LABTECH-01

Figure 1-19

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

Creating new Scan/Update tasks

see Scan / Update tasks

4.2.4.1 Scan / Update tasks

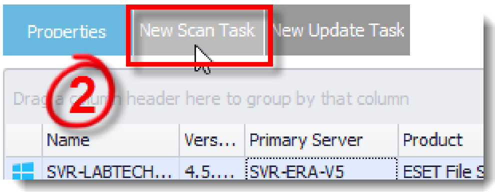
From the Endpoints module you can initiate new on-demand scans and force definition updates as tasks.

Scan Tasks

To initiate a new scan task:

1. Select target the endpoint(s) from the endpoint table.

2. Click **New Scan Task**. The **Scan Task** dialog will be displayed.



Name	Vers...	Primary Server	Product
SVR-LABTECH...	4.5....	SVR-ERA-V5	ESET File S

Figure 1-20

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.

Update Task

To initiate a new update task:

1. Select the endpoint(s) you want to update from the endpoint table.

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.

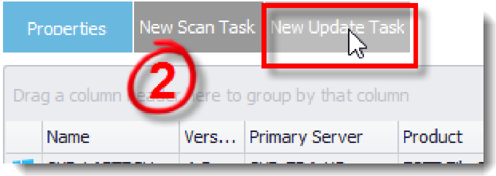


Figure 1-21

4.2.4.2 Endpoint to Agent Mapping

The ERA Plug-in for LabTech automatically generates a map of ESET endpoints the their corresponding LabTech agent. 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.

Automatic Mapping

The ERA Plug-in for LabTech automatically maps ESET endpoints to LabTech 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 LabTech, the ERA Plug-in for LabTech will search for all network adapters that belong to LabTech 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 LabTech 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 LabTech 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.

Manual Mapping

If automatic mapping fails to find a match, or finds the incorrect match for an endpoint, you can create a manual mapping. Manual mappings always take priority over automatic matches.

Open the Manual Mapping dialog

1. Click the ESET icon in the LabTech navigation bar to open the ESET Dashboard.

2. Click **Endpoints** on the navigation panel to display the Endpoints module.

3. Click **Manual Mapping** in the top right.

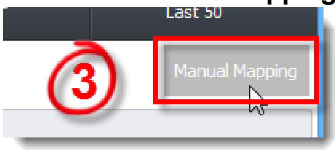
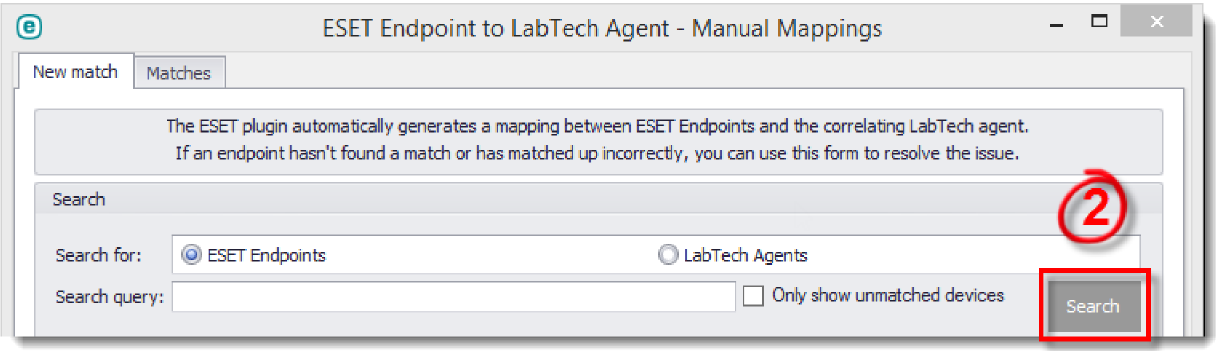


Figure 1-22

Create a manual mapping

1. Click **New Match**.

2. 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.



The ESET plugin automatically generates a mapping between ESET Endpoints and the correlating LabTech agent. If an endpoint hasn't found a match or has matched up incorrectly, you can use this form to resolve the issue.

Search for: ● ESET Endpoints ○ LabTech Agents

Search query: □ Only show unmatched devices

Search

Figure 1-23

3. The table will display devices returned by your query.

4. 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.

5. Select **LabTech Agents** from the **Search for** field.

6. Repeat steps 2 through 4. LabTech agent data will be displayed in the **Selected LabTech Agent** field.

7. 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.

Diagnosing Mapping Issues

Automatic matching
Matching is based predominantly on device MAC addresses and takes into account the most recent information. If two agents report the same MAC address, the agent added most recently will be saved as a match.

By default, the ESET Server only saves the first valid MAC address that was used to connect the endpoint to the ESET server. If this causes an issue, we recommend that you enable **MAC address renaming** on your ERA server. For instructions to do so, see our Knowledgebase article.

To reset endpoint to agent matching
All matches are stored in the table **plugin_eset_ra_endpoint_weight** in the LabTech database. This table will recreate itself and automatically be rebuilt if it is cleared or deleted.

5. ERA Server Module

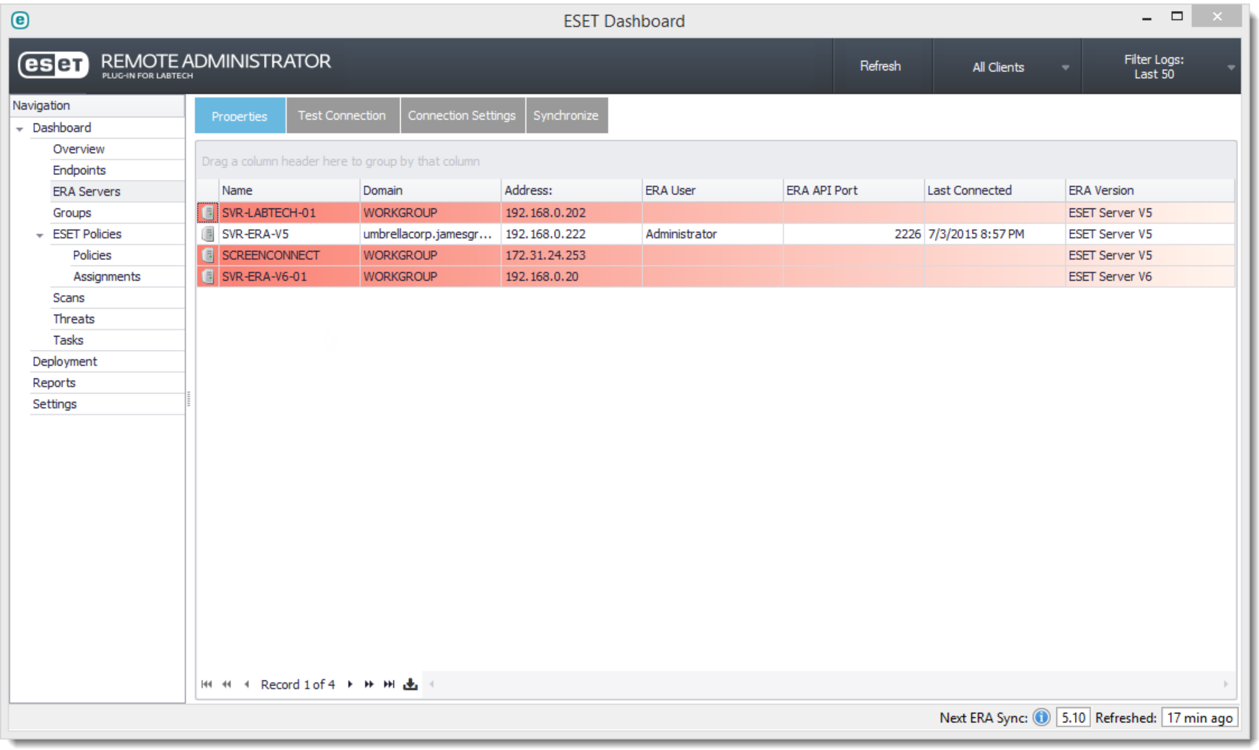
Information about all detected ERA servers is displayed here; disconnected ERA servers are highlighted in red.

Synchronization

The ERA Plug-in for LabTech 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. Select a server from the table and click **Synchronize** to force it to synchronize immediately.

Update connection settings

Select a server from the table and click **Connection Settings** to update connection settings for that server.



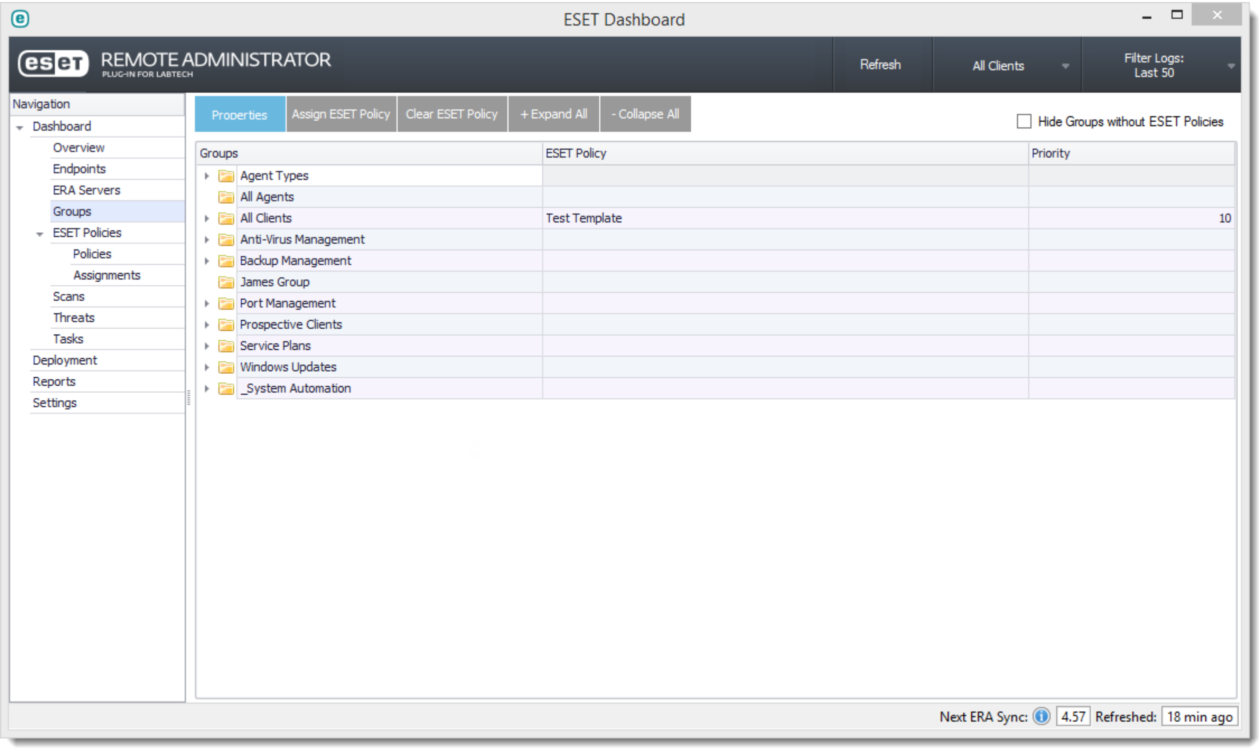
Name	Domain	Address:	ERA User	ERA API Port	Last Connected	ERA Version
SVR-LABTECH-01	WORKGROUP	192.168.0.202				ESET Server V5
SVR-ERA-V5	umbrellacorp.jamesgr...	192.168.0.222	Administrator	2226	7/3/2015 8:57 PM	ESET Server V5
SCREENCONNECT	WORKGROUP	172.31.24.253				ESET Server V5
SVR-ERA-V6-01	WORKGROUP	192.168.0.20				ESET Server V6

Next ERA Sync: 5.10 Refreshed: 17 min ago

Figure 1-24

6. Groups Module

All LabTech groups and their associated ESET policies are displayed here.



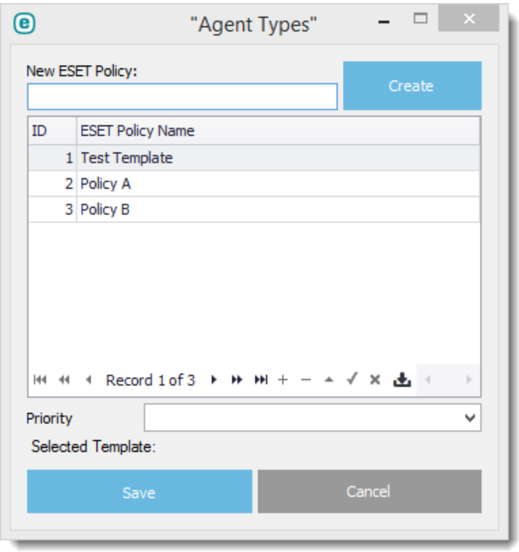
Groups	ESET Policy	Priority
Agent Types		
All Agents		
All Clients	Test Template	10
Anti-Virus Management		
Backup Management		
James Group		
Port Management		
Prospective Clients		
Service Plans		
Windows Updates		
_System Automation		

Next ERA Sync: 4.57 Refreshed: 18 min ago

Figure 1-25

Assigning ESET policies to groups

Select a group and click **Assign ESET Policy** to assign a policy to a group. The assignment window will be displayed. 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**.



ID	ESET Policy Name
1	Test Template
2	Policy A
3	Policy B

Figure 1-26

Clearing ESET policies from a group

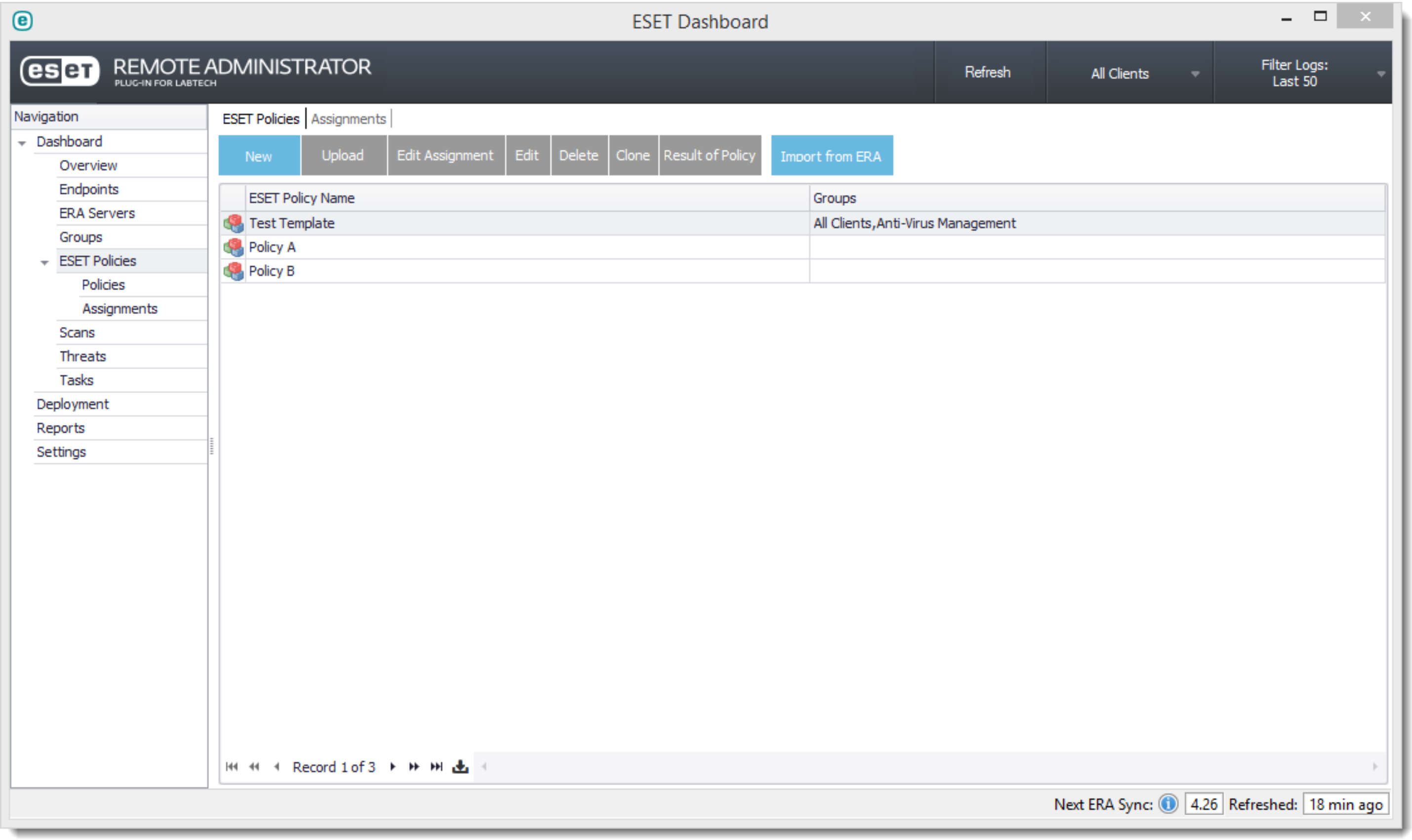
Select a group and click **Clear ESET Policy** to remove any policy assigned to that group.

Hiding groups without policies

Select **Hide Groups without ESET policies** to have the dashboard display only groups that have ESET policies assigned to them.

7. ESET Policies Module

You can create new policies and review existing policies in this module.



ESET Policy Name	Groups
Test Template	All Clients,Anti-Virus Management
Policy A	
Policy B	

Next ERA Sync: 4.26 Refreshed: 18 min ago

Figure 1-27

Creating ESET policies

1. Click **New** and type a name for your new policy in the **Policy Name** field.

   a. ERA 5 Policies: Select the **V5** tab and click **Configuration Editor** to make changes to your policy configuration. Click **Save** when you are finished.

   b. ERA 6 Policies: Select the **V6** tab and select the products you want to create a configuration for. Click **Edit** next to a specific product to make changes to the policy for that product. Click **Save** when you are finished making changes.

Assigning ESET policies

1. Select the policy you want to assign to LabTech groups and click **Edit Assignment**.

2. Select the LabTech groups you want to import from the left panel and click **>** to add them to the selected panel. Click **Save** when you are finished.

Inheriting and Merging Exclusions and Schedules

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

7.1 Importing Existing Policies

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

1. Click **ESET Policies** > **Import from ERA**.

2. Select an ERA server to import policies from.

3. Select the policies you want to import and click **>** to add them to the **Selected** list. Click **Import** when you are finished.

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 LabTech. 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 LabTech group.

7.2 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 LabTech agents. If a policy isn't assigned to a LabTech group or is assigned to a LabTech 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 LabTech?
The ERA Plug-in for LabTech 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 Labtech and assign it to the "All Agents" group in LabTech.
Alternatively, you can edit the "LabTech 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 "LabTech 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 LabTech, it will receive policy settings within approximately 6 minutes of joining any group with ESET policies assigned to it.

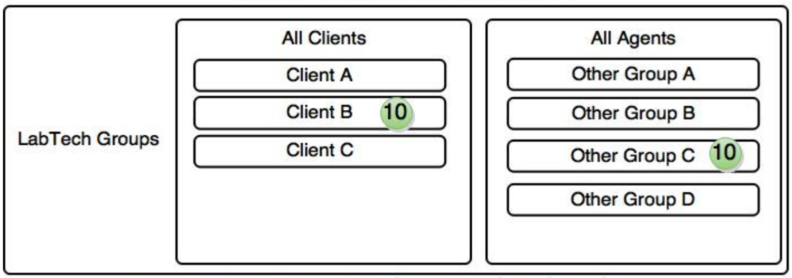
What happens when a computer's group(s) are changed or is moved into a new group?
If the new group contains ESET policies it will get its new expected policy from the ERA Plug-in for LabTech. If it is moved out of all groups with ESET policies assigned, it will retain its previous settings until a new policy is assigned to it.

7.3 Policy Inheritance

Policy inheritance in the ERA Plug-in for LabTech works similarly to LabTech templates. Inheritance exhibits parent-child behavior down the LabTech group tree. Because a LabTech 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

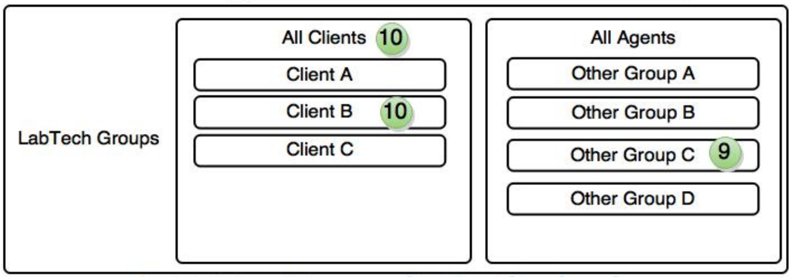


Endpoint belongs to two groups, Client B and Other Group C.
Both groups have an ESET policy with a priority 10.

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"

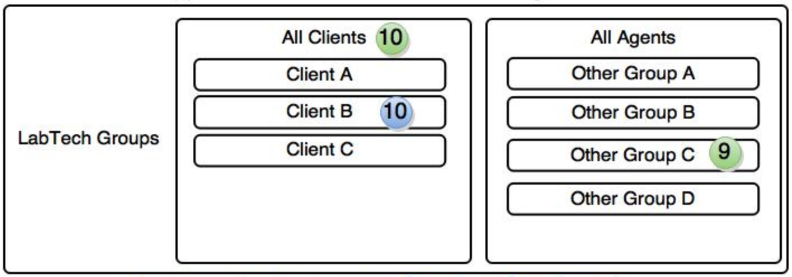
(2) SIMPLE POLICY INHERITANCE - NO CONFLICT



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

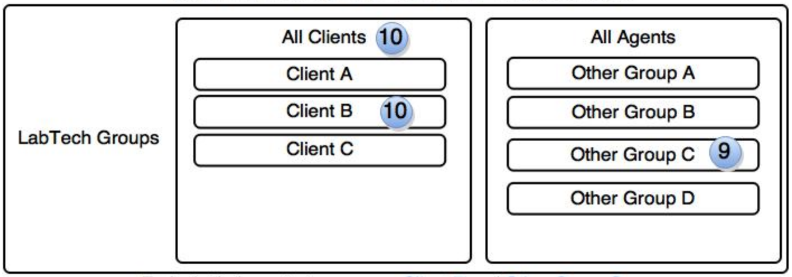


Endpoint belongs to two groups, Client B and Other Group C.
Client B is a child of All Clients which also has a policy assigned.

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 have merge enabled, it will still take priority and overwrite any conflicting settings. (Not merge them further)

(4) SIMPLE POLICY INHERITANCE - Merge enabled



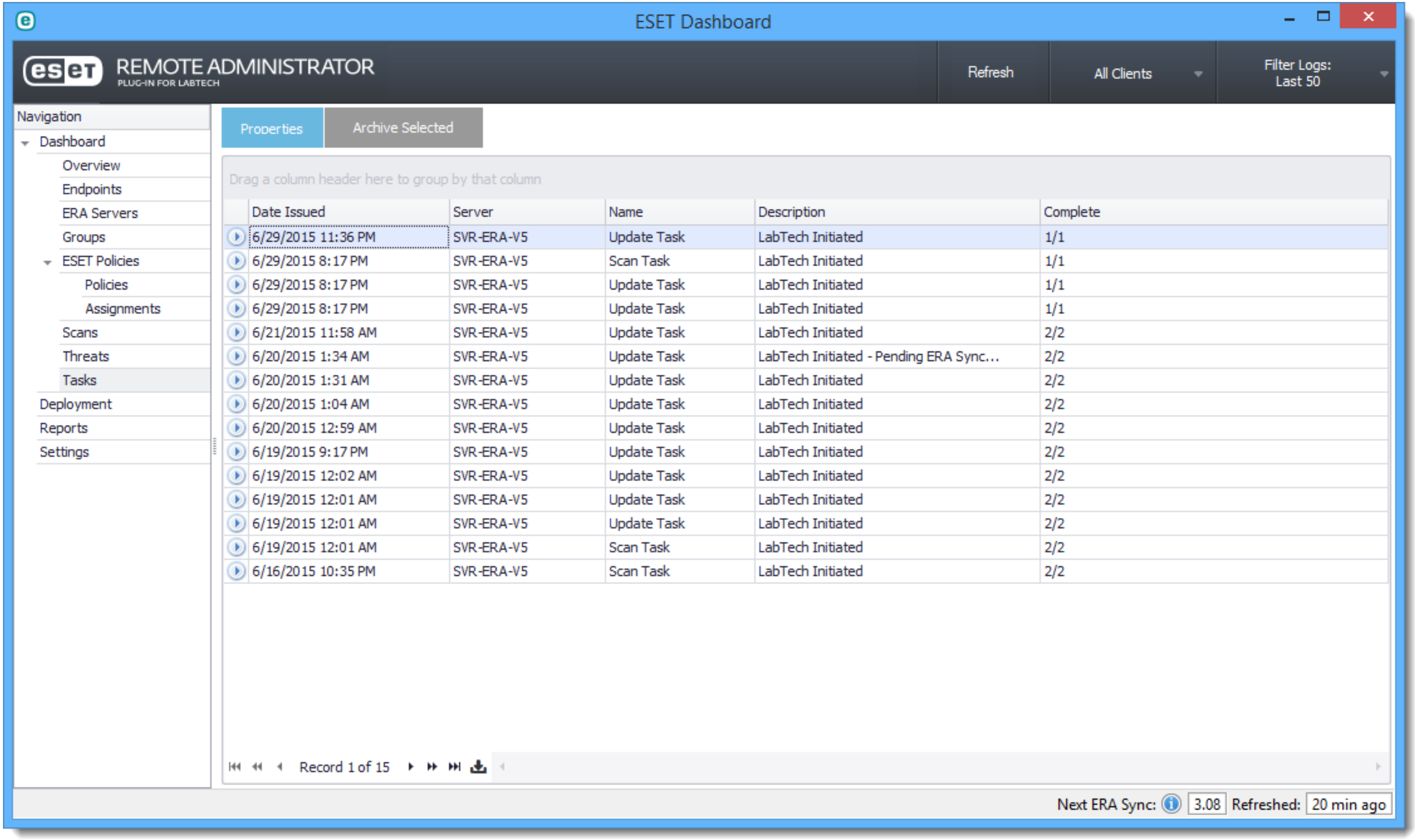
Endpoint belongs to two groups, Client B and Other Group C.
Client B is a child of All Clients which also has a policy assigned.

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.

8. Threats / Scans / Tasks Modules

These three modules use a similar layout but display different types of data. Logs for the data present in the dashboard can be filtered using the client and log filters. Select any log and click **Properties** to view more detailed information on the log and the endpoint associated with it.



Date Issued	Server	Name	Description	Complete
6/29/2015 11:36 PM	SVR-ERA-V5	Update Task	LabTech Initiated	1/1
6/29/2015 8:17 PM	SVR-ERA-V5	Scan Task	LabTech Initiated	1/1
6/29/2015 8:17 PM	SVR-ERA-V5	Update Task	LabTech Initiated	1/1
6/29/2015 8:17 PM	SVR-ERA-V5	Update Task	LabTech Initiated	1/1
6/21/2015 11:58 AM	SVR-ERA-V5	Update Task	LabTech Initiated	2/2
6/20/2015 1:34 AM	SVR-ERA-V5	Update Task	LabTech Initiated - Pending ERA Sync…	2/2
6/20/2015 1:31 AM	SVR-ERA-V5	Update Task	LabTech Initiated	2/2
6/20/2015 1:04 AM	SVR-ERA-V5	Update Task	LabTech Initiated	2/2
6/20/2015 12:59 AM	SVR-ERA-V5	Update Task	LabTech Initiated	2/2
6/19/2015 9:17 PM	SVR-ERA-V5	Update Task	LabTech Initiated	2/2
6/19/2015 12:02 AM	SVR-ERA-V5	Update Task	LabTech Initiated	2/2
6/19/2015 12:01 AM	SVR-ERA-V5	Update Task	LabTech Initiated	2/2
6/19/2015 12:01 AM	SVR-ERA-V5	Update Task	LabTech Initiated	2/2
6/19/2015 12:01 AM	SVR-ERA-V5	Scan Task	LabTech Initiated	2/2
6/16/2015 10:35 PM	SVR-ERA-V5	Scan Task	LabTech Initiated	2/2

Next ERA Sync: 3.08 Refreshed: 20 min ago

Figure 1-29

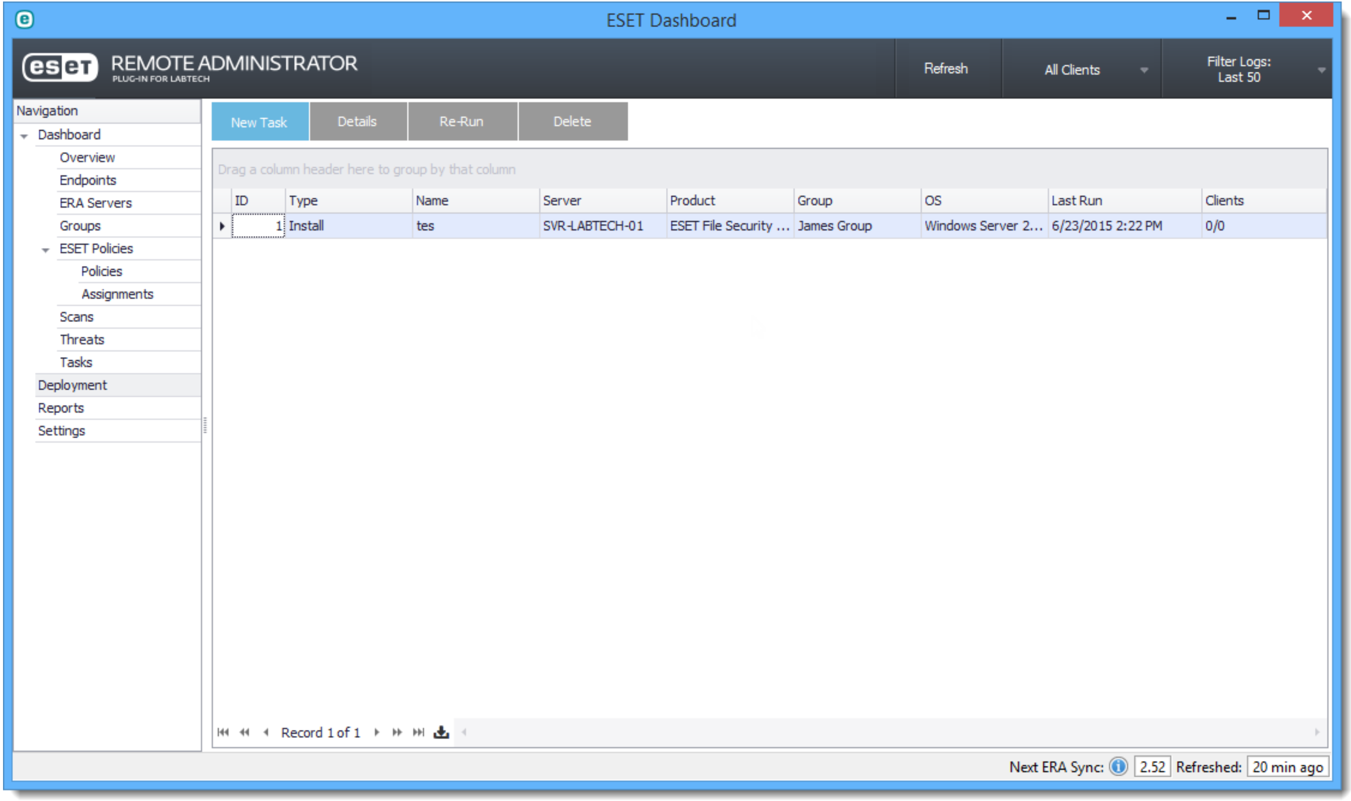
Archiving Logs

We recommend that you archive older logs that aren't pertinent to the current status of your network. Select one or more logs from the dashboard and click **Archive Selected** to archive them. Archived logs will be hidden immediately after they are archived.

NOTE: Archived data is still accessible in the database until a database cleanup is run on the interval specified under settings.

9. Deployment Module

The Deployment module allows you to create and view deployment tasks. The ERA Plug-in for LabTech uses its own module on the remote agent to deploy ESET products to LabTech agents, however earlier ESET deployment scripts created by LabTech are supported and functional.



ID	Type	Name	Server	Product	Group	OS	Last Run	Clients
1	Install	tes	SVR-LABTECH-01	ESET File Security ...	James Group	Windows Server 2...	6/23/2015 2:22 PM	0/0

Next ERA Sync: 2.52 Refreshed: 20 min ago

Figure 1-30

Deploying to a LabTech Group

1. Click **New Task**.

2. Select the ERA Server endpoints should connect to.

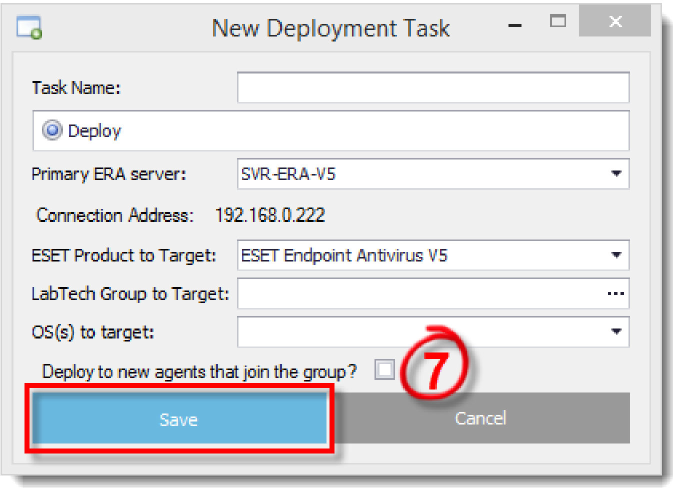
3. Select the ESET product to deploy.

4. Select the LabTech group you want to deploy to.

5. Select the OS(s) you want to target.

6. (**Optional**) Select **Deploy to new agents that join the group** to have the ERA Plug-in for LabTech attempt to deploy to any new agent that joins the group.

7. 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.



New Deployment Task

Task Name:

● Deploy

Primary ERA server: SVR-ERA-V5

Connection Address: 192.168.0.222

ESET Product to Target: ESET Endpoint Antivirus V5

LabTech Group to Target: ...

OS(s) to target:

Deploy to new agents that join the group? □

Figure 1-31

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

Monitoring a Deployment Task
Select any deployment task and click **Details** to view its status and details. You can resend a task if it has failed, or open the LabTech Computer Window to diagnose a failed deployment.

Deploying to a single agent, location, client or group

You can deploy to a single agent, group, or location from the context menu. To do so, follow the steps below:

1. Right-click the object in LabTech navigation and select **Commands** > **LabTech** > **ESET Deployment**.

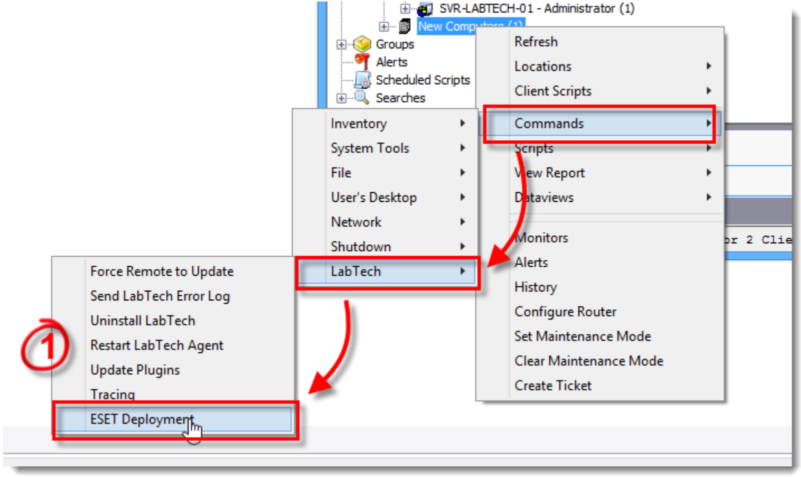
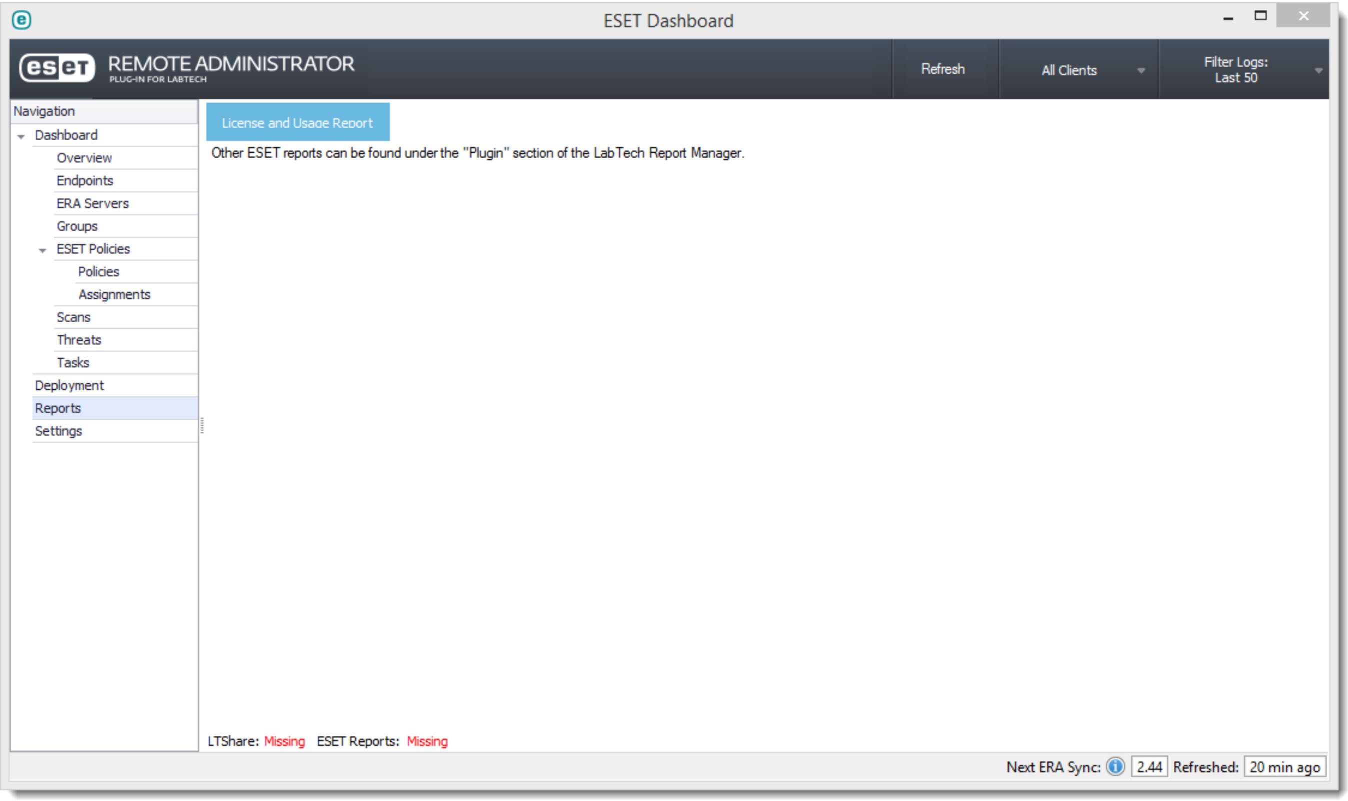


Figure 1-32

2. In the new deployment window, select the ESET Server your endpoints should connect to and the ESET product to deploy. Click **Submit** when you are ready to deploy.

10. Reports Module

The Reports module dispays custom reports in the ERA Plug-in for LabTech. Other ESET reports are avialable in LabTech Report Manager.



Other ESET reports can be found under the "Plugin" section of the LabTech Report Manager.

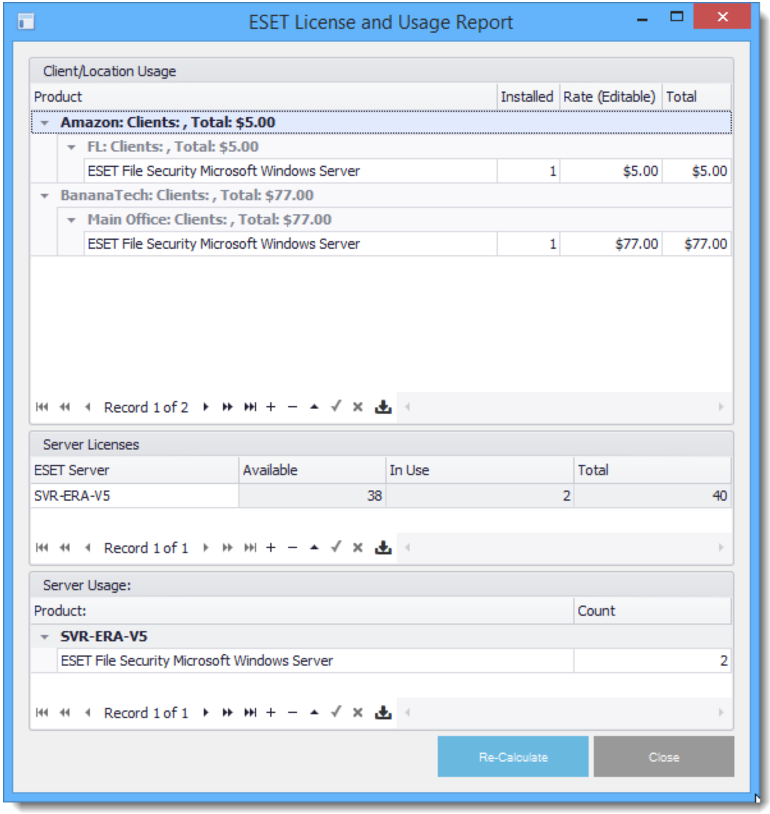
LTShare: Missing ESET Reports: Missing

Next ERA Sync: 2.44 Refreshed: 20 min ago

Figure 1-33

10.1 License and Usage Report

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



Client/Location Usage

Product	Installed	Rate (Editable)	Total
Amazon: Clients: , Total: $5.00			
FL: Clients: , Total: $5.00			
ESET File Security Microsoft Windows Server	1	$5.00	$5.00
BananaTech: Clients: , Total: $77.00			
Main Office: Clients: , Total: $77.00			
ESET File Security Microsoft Windows Server	1	$77.00	$77.00

Server Licenses

ESET Server	Available	In Use	Total
SVR-ERA-V5	38	2	40

Server Usage:

Product:	Count
SVR-ERA-V5	
ESET File Security Microsoft Windows Server	2

Figure 1-34

Client / Location Usage

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.

11. Settings

The following settings for the ERA Plug-in for LabTech 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.

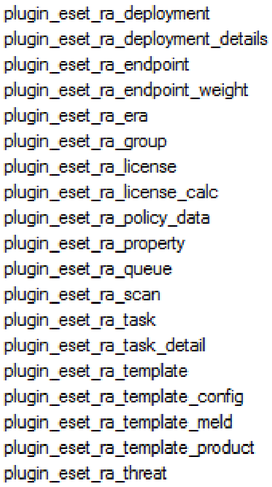
Maintenance

- **Run manual ERA Sync**: Runs a synchronization similar to the sync that occurs on the LabTech 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.

12. Database

All endpoint and log data is synchronized with the LabTech 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 LabTech 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 Labtech'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.

13. MSP Licenses

The ERA Plug-in for LabTech works independent of licenses; any license type will work.

ESET MSP Utilities (EMU) is available from ESET to manage MSP licenses. Click here to visit the ESET MSP Utilities Hub. EMU uses ERA Keys to generate and update licenses as needed. All licenses should appear in ERA with an expiration date approximately three months away. This value updates automatically, and should always appear to be approximately three months.

How does EMU affect the plug-in?

When EMU is installed on an ERA server it automatically creates and manages a special policy called **BaseUP** along with a few other policies. If the ERA Plug-in for LabTech detects the BaseUP policy, it will automatically create all plug-in managed policies under the BaseUP policy.

If EMU is not used to manage licenses, server licenses can optionally be installed through the ERA Plug-in for LabTech.

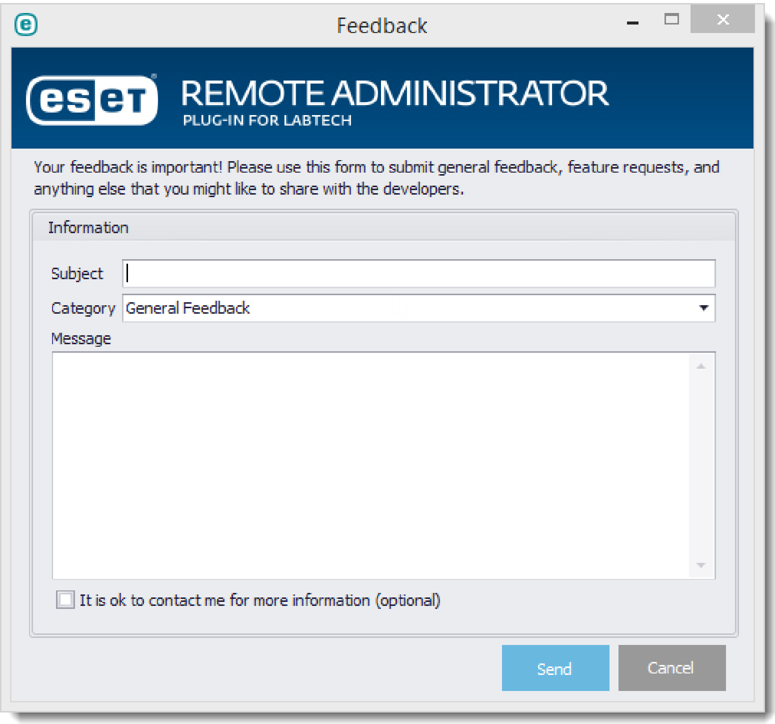
14. Support

Diagnosing Common 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 LabTech. Close the notification and attempt your operation again in a few minutes. If the notification continues to appear, restart the LabTech 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 LabTech server to verify that it can access http://ftp.nod.sk.

Getting help

If you require assistance with the ERA Plug-in for LabTech, please contact LabTech support through conventional channels. Additionally, you can submit feedback, make feature requests and send comments about the ERA Plug-in for LabTech to our development team using the ESET feedback form. From the LabTech 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.



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.

Information

Subject

Category: General Feedback

Message

□ It is ok to contact me for more information (optional)

Figure 1-35