Copyright © 2017 by ESET, spol. s r.o.
ESET Remote Administrator 6 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: www.eset.com/support

REV. 3/28/2017
Contents

1. Preface .........................................................6
  1.1 About help......................................................6
      1.1.1 Offline help..................................................7
  1.2 Supported Web browsers and ESET security products........9
  1.3 Icon legend..................................................10

2. Getting started with ESET Remote Administrator Web Console........13
  2.1 Introduction to ESET Remote Administrator..........................13
  2.2 Opening the ERA Web Console.........................................14
  2.3 Using the Startup Wizard..............................................15
  2.4 ERA Web Console..................................................17
  2.5 How to manage Endpoint products from ESET Remote Administrator........20
  2.6 Following upgrade from an earlier version of ERA................21

3. Working with ERA Web Console ..................................23
  3.1 Login screen....................................................24
      3.1.1 Troubleshooting - Web Console..............................25
  3.2 Dashboard.........................................................25
      3.2.1 User settings..................................................27
      3.2.2 Dashboard settings...........................................28
      3.2.3 Drill down.......................................................29
      3.2.4 Edit report template..........................................31
  3.3 Computers.......................................................35
      3.3.1 Computer details...............................................37
      3.3.2 Import CSV......................................................39
  3.4 Threats..................................................................40
  3.5 Reports..................................................................42
      3.5.1 Create a new report template.................................44
      3.5.2 Generate report................................................47
      3.5.3 Schedule a report..............................................47
      3.5.4 Outdated applications.......................................48
      3.5.5 SysInspector log viewer.....................................49

4. ESET Remote Administrator initial configuration.....................51
  4.1 Status overview..................................................51
  4.2 New native user account...........................................52
  4.3 Certificates.......................................................53
  4.4 Licenses - add new license........................................54
  4.5 Deployment.......................................................58
      4.5.1 Add client computer to ERA structure.......................58
      4.5.1.1 Using Active Directory synchronization..................59
      4.5.1.2 Using RD Sensor..........................................60
      4.5.1.3 Add Computers.............................................62
      4.5.2 Agent deployment process...................................65
      4.5.2.1 Local deployment.........................................65
      4.5.2.1.1 Create an all-in-one Agent installer..................66
      4.5.2.1.2 Create Agent Live Installer............................67
      4.5.2.1.3 Download Agent from ESET website...............69
      4.5.2.1.3.1 Deploy Agent locally.................................70
      4.5.2.2 Remote deployment......................................72
      4.5.2.2.1 Agent deployment using GPO and SCCM............73
      4.5.2.2.1.1 Deployment steps - GPO.............................73
      4.5.2.2.1.2 Deployment steps - SCCM..........................78
      4.5.2.2.2 Deployment tool.........................................94
      4.5.2.3 ERA Agent settings........................................95
      4.5.2.3.1 Create a Policy for ERA Agent connection interval....96
      4.5.2.3.2 Create a Policy for ERA Agent to connect to the new ERA Server.................100
      4.5.2.3.3 Create a Policy to enable ERA Agent Password protection..........................103
      4.5.2.4 Agent protection..........................................104
      4.5.3 Troubleshooting - Agent connection........................105
      4.5.4 Troubleshooting - Agent deployment........................105
      4.5.5 Example scenarios of ERA Agent deployment..............108
      4.5.5.1 Example scenarios of ERA Agent deployment to targets not joined to domain...........108
      4.5.5.2 Example scenarios of ERA Agent deployment to targets joined to domain...............109
      4.5.6 Product installation.........................................111
      4.5.6.1 Product installation (command line).....................113
      4.5.6.2 List of problems when installation fails...............115
      4.5.7 Desktop Provisioning........................................115

4.6 Additional configuration........................................115

5. Mobile Device Management..........................................116
  5.1 Device Enrollment..............................................118
      5.1.1 Enrollment via email.........................................120
      5.1.2 Individual enrollment via link or QR code................122
      5.1.3 Device Enrollment Android ..................................123
      5.1.4 Device Enrollment iOS........................................132
      5.1.4.1 Device Enrollment iOS with DEP.........................135
  5.2 Create a Policy for iOS MDM - Exchange ActiveSync Account........138
  5.3 Create a Policy for MDC to activate APNS/DEP for iOS enrollment........143
  5.4 Create a Policy to enforce restrictions on iOS and add Wi-Fi connection........146
      5.4.1 MDM configuration profiles................................150

6. Admin.............................................................151
  6.1 Groups...........................................................151
      6.1.1 Create new Static Group......................................153
      6.1.2 Create new Dynamic Group..................................155
      6.1.3 Assign Task to a Group........................................157
      6.1.4 Assign a policy to a group....................................158
      6.1.5 Static Groups..................................................160
      6.1.5.1 Static Group Wizard........................................161
      6.1.5.2 Manage Static Groups.....................................162
### 6.2 User Management

- 6.2.1 Add New Users ................................................................. 186
- 6.2.2 Edit Users ............................................................................ 188
- 6.2.3 Create New User Group .................................................. 190

### 6.3 Installers ............................................................................. 190

### 6.4 Quarantine .......................................................................... 193

### 6.5 Policies .............................................................................. 194

- 6.5.1 Policies Wizard ................................................................. 195
- 6.5.2 Flags .................................................................................. 196
- 6.5.3 Manage Policies ................................................................. 197
- 6.5.4 How Policies are applied to clients ....................................... 198
- 6.5.4.1 Ordering Groups ............................................................... 198
- 6.5.4.2 Enumerating Policies ......................................................... 200
- 6.5.4.3 Merging Policies ............................................................... 201
- 6.5.4.3.1 Example scenario of merging policies ............................. 202
- 6.5.5 Configuration of a product from ERA ................................... 205
- 6.5.6 Assign a Policy to a Group .................................................. 205
- 6.5.7 Assign a Policy to a Client ................................................... 208
- 6.5.8 ERA Proxy policy settings ................................................. 209
- 6.5.9 ESET Rogue Detection Sensor policy settings .................... 209
- 6.5.10 How to use Override mode .................................................. 211

### 6.6 Client Tasks ...................................................................... 212

- 6.6.1 Client Tasks executions ....................................................... 213
- 6.6.1.1 Progress indicator ........................................................... 216
- 6.6.1.2 Status icon ..................................................................... 216
- 6.6.1.3 Drill down ........................................................................ 217
- 6.6.1.4 Trigger ........................................................................... 219
- 6.6.2 Shutdown computer ............................................................ 220
- 6.6.3 On-Demand Scan ............................................................... 221
- 6.6.4 Operating System Update .................................................. 223
- 6.6.5 Quarantine Management .................................................... 224
- 6.6.6 Rogue Detection Sensor Database Reset ............................. 226
- 6.6.7 Remote Administrator Components Upgrade .................... 227
- 6.6.8 Reset Cloned Agent ............................................................. 228
- 6.6.9 Run Command .................................................................... 229
- 6.6.10 Run SysInspector Script .................................................... 231
- 6.6.11 Server Scan ....................................................................... 232
- 6.6.12 Software Install ................................................................. 233
- 6.6.13 Software Uninstall .............................................................. 235
- 6.6.14 Product Activation .............................................................. 236
- 6.6.15 SysInspector Log Request (Windows only) .......................... 238
- 6.6.16 Upload Quarantined File ..................................................... 239
- 6.6.17 Modules Update ................................................................. 240
- 6.6.18 Modules Update Rollback .................................................. 241
- 6.6.19 Display Message ................................................................ 242
- 6.6.20 Anti-Theft Actions .............................................................. 243
- 6.6.21 Stop Managing (Uninstall ERA Agent) ............................... 245
- 6.6.22 Export Managed Products Configuration .......................... 247
- 6.6.23 Assign Task to Group .......................................................... 248
- 6.6.24 Assign Task to Computer(s) ............................................... 249
- 6.6.25 Triggers ............................................................................ 250

### 6.7 Server Tasks ...................................................................... 251

- 6.7.1 Server Task Types .............................................................. 252
- 6.7.1.1 Static Group Synchronization .......................................... 253
- 6.7.1.1.1 Synchronization mode - Active Directory ...................... 253
- 6.7.1.1.2 Synchronization mode - MS Windows Network ............. 254
- 6.7.1.1.3 Synchronization mode - VMware .................................. 255
- 6.7.1.1.4 Static Group Synchronization - Linux Computers ........ 256
- 6.7.1.2 User Synchronization ....................................................... 257
- 6.7.1.3 Agent Deployment ............................................................ 258
- 6.7.1.4 Generate Report ............................................................... 259
- 6.7.1.5 Rename computers .......................................................... 261
- 6.7.1.6 Delete Not Connecting Computers .................................... 262
- 6.7.2 Triggers ............................................................................ 263
- 6.7.2.1 Cron expression interval .................................................. 264
- 6.7.3 Advanced Settings - Throttling ............................................ 267
- 6.7.3.1 Throttling Examples .......................................................... 269

### 6.8 Notifications ..................................................................... 271

- 6.8.1 Manage Notifications .......................................................... 272
- 6.8.2 How to configure an SNMP Trap Service .............................. 274

### 6.9 Certificates ...................................................................... 276

- 6.9.1 Peer Certificates ................................................................. 277
- 6.9.1.1 Create a new Certificate ................................................... 278
- 6.9.1.2 Export Peer Certificate ...................................................... 279
- 6.9.1.3 APN/DEP certificate ........................................................... 279
- 6.9.1.4 Show revoked ................................................................. 282
- 6.9.1.5 Set new ERA Server certificate .......................................... 283
1. Preface

Welcome to the ERA Administration guide. This document explains how to manage ESET Business Solutions within your infrastructure. It also details changes in the latest version of ERA as well as scenarios for administrators and users who will be working with ERA Web Console.

1.1 About help

The Administration guide was written to help you get familiar with ESET Remote Administrator and provides instructions to use it.

For consistency and to help prevent confusion, terminology used throughout this guide is based on the ESET Remote Administrator parameter names. We also used a uniform set of symbols to highlight topics of particular interest or significance.

**NOTE**
Notes can provide valuable information, such as specific features or a link to some related topic.

**IMPORTANT**
This requires your attention and it should not be skipped. Usually, it provides non-critical but significant information.

**WARNING**
Critical information you should treat with increased caution. Warnings are placed specifically to deter you from committing potentially harmful mistakes. Please read and understand text placed in warning brackets, as it references highly sensitive system settings or something risky.

**EXAMPLE**
Example case which describes a user case relevant for the topic where it is included. Examples are used to explain more complicated topics.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold type</strong></td>
<td>Names of interface items such as boxes and option buttons.</td>
</tr>
<tr>
<td><strong>Italic type</strong></td>
<td>Placeholders for information you provide. For example, <em>file name or path</em> means you type the actual path or a name of file.</td>
</tr>
<tr>
<td><strong>Courier New</strong></td>
<td>Code samples or commands</td>
</tr>
<tr>
<td><strong>Hyperlink</strong></td>
<td>Provides quick and easy access to cross-referenced topics or external web location. Hyperlinks are highlighted in blue and may be underlined.</td>
</tr>
<tr>
<td><code>%ProgramFiles%</code></td>
<td>The Windows system directory which stores installed programs of Windows and others.</td>
</tr>
</tbody>
</table>

- **Online help** is the primary source of help content. The latest version of Online help will automatically be displayed when you have a working internet connection. The ESET Remote Administrator online help pages include three active tabs at the top navigation header: **Installation/Upgrade**, **Administration** and **VA Deployment**.
Topics in this guide are divided into several chapters and sub-chapters. You can find relevant information by browsing the **Contents** of the help pages. Alternatively, you can use the **Index** to browse by keywords or use full-text **Search**.

ESET Remote Administrator allows you to search help topics by keyword or by typing words or phrases to search for within the user guide. The difference between these two methods is that a keyword may be logically related to help pages which do not contain that particular keyword in the text. Searching by words and phrases will search the contents of all pages and display only those containing the searched word or phrase in the actual text.

**IMPORTANT**

Once you open a User Guide from the navigation bar at the top of the page, search will be limited to the contents of that guide. For example, if you open the Administrator guide, topics from the Installation/Upgrade and VA Deployment guides will not be included in search results.

- The **ESET Knowledgebase** contains answers to the most frequently asked questions, as well as recommended solutions for various issues. Regularly updated by ESET technical specialists, the Knowledgebase is the most powerful tool for resolving various types of problems.
- The **ESET Forum** provides ESET users with an easy way to get help and to help others. You can post any problem or question related to your ESET products.
- You can post your rating and/or provide a feedback on a particular topic in help, click the **Was this information helpful?** link or **Rate this article: Helpful / Not Helpful** in case of ESET Knowledgebase, underneath the help page.

### 1.1.1 Offline help

Offline help for ESET Remote Administrator is not installed by default. If you need ESET Remote Administrator help that you can use while you are offline (in case you do not have an internet access at times, or all the time), perform the steps below to add Offline help.

Click the language code to download Offline help for ESET Remote Administrator in your desired language. You even can have Offline help can be installed for multiple languages.

- **Offline help setup instructions for Windows**
  1. **Download** a .zip file by clicking a language code in the table below to download Offline help for your ESET Remote Administrator in your desired language.
  2. **Save** the .zip file (for example to a USB flash drive).
  3. **Create** a new folder named help on your server that runs ERA Web Console within the following location: `%ProgramFiles%\Apache Software Foundation\Tomcat 7.0\webapps\era\webconsole\` and **Copy** the .zip file to the help folder.
  4. **Extract** the contents of the .zip file, for example en-US.zip, to a folder with the same name, in this case **en-US** so that the folder structure looks like this: `%ProgramFiles%\Apache Software Foundation\Tomcat 7.0 \webapps\era\webconsole\help\en-US`
You can now open your ERA Web Console, select the language and log in. When you press the icon in the top right corner, an Offline help page will be displayed.

**NOTE**
You can add Offline help in multiple languages if required by following the same steps as above.

**IMPORTANT**
If your computer, or a mobile device you access ERA Web Console from, does not have an internet connection, you will need to change your setting in ERA Web Console to force ERA Offline help to open by default (instead of Online help). To do so, follow the instructions below the table.

### Offline help setup instructions for Linux

1. **Download** a .tar file by clicking a language code in the table below to download Offline help for your ESET Remote Administrator in desired language.
2. **Save** the .tar file (for example to a USB flash drive).
3. **Open terminal** and navigate to `/usr/share/tomcat/webapps/era/webconsole`
4. **Create** new folder named `help` by running `mkdir help` command.
5. **Copy** the .tar file to the `help` folder and extract it, for example by running `tar -xvf en-US.tar` command.

You can now open your ERA Web Console, select the language and log in. When you press the icon in the top right corner, an Offline help page will be displayed.

**NOTE**
You can add Offline help in multiple languages if required by following the same steps as above.

**IMPORTANT**
If your computer, or a mobile device you access ERA Web Console from, does not have an internet connection, you will need to change your setting in ERA Web Console to force ERA Offline help to open by default (instead of Online help). To do so, follow the instructions below the table.

<table>
<thead>
<tr>
<th>Supported Language</th>
<th>Offline HTML Help .zip</th>
<th>Offline HTML Help .tar</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>en-US.zip</td>
<td>en-US.tar</td>
</tr>
<tr>
<td>Arabic</td>
<td>ar-EG.zip</td>
<td>ar-EG.tar</td>
</tr>
<tr>
<td>Chinese Simplified</td>
<td>zh-CN.zip</td>
<td>zh-CN.tar</td>
</tr>
<tr>
<td>Chinese Traditional</td>
<td>zh-TW.zip</td>
<td>zh-TW.tar</td>
</tr>
<tr>
<td>Croatian</td>
<td>hr-HR.zip</td>
<td>hr-HR.tar</td>
</tr>
<tr>
<td>Czech</td>
<td>cs-CZ.zip</td>
<td>cs-CZ.tar</td>
</tr>
<tr>
<td>French</td>
<td>fr-FR.zip</td>
<td>fr-FR.tar</td>
</tr>
<tr>
<td>French Canadian</td>
<td>fr-FC.zip</td>
<td>fr-FC.tar</td>
</tr>
<tr>
<td>German</td>
<td>de-DE.zip</td>
<td>de-DE.tar</td>
</tr>
<tr>
<td>Greek</td>
<td>el-GN.zip</td>
<td>el-GR.tar</td>
</tr>
<tr>
<td>Italian</td>
<td>it-IT.zip</td>
<td>it-IT.tar</td>
</tr>
<tr>
<td>Japanese</td>
<td>ja-JP.zip</td>
<td>ja-JP.tar</td>
</tr>
<tr>
<td>Korean</td>
<td>ko-KR.zip</td>
<td>ko-KR.tar</td>
</tr>
<tr>
<td>Polish</td>
<td>pl-PL.zip</td>
<td>pl-PL.tar</td>
</tr>
<tr>
<td>Portuguese Brazilian</td>
<td>pt-BR.zip</td>
<td>pt-BR.tar</td>
</tr>
<tr>
<td>Russian</td>
<td>ru-RU.zip</td>
<td>ru-RU.tar</td>
</tr>
<tr>
<td>Spanish</td>
<td>es-ES.zip</td>
<td>es-ES.tar</td>
</tr>
</tbody>
</table>
1.2 Supported Web browsers and ESET security products

The following Operating Systems, Web browsers and ESET security products are supported by ESET Remote Administrator.

- **Windows**, **Linux** and **macOS**

- The ESET Remote Administrator Web Console can be run in the following web browsers:

<table>
<thead>
<tr>
<th>Web browser</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mozilla Firefox</td>
<td>20+</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>10+</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>25+</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>23+</td>
</tr>
<tr>
<td>Safari</td>
<td>6+</td>
</tr>
<tr>
<td>Opera</td>
<td>15+</td>
</tr>
</tbody>
</table>

**NOTE**
We recommend that you keep **Web browsers** up to date.

- ESET Remote Administrator is able to deploy, activate or manage the following ESET products

<table>
<thead>
<tr>
<th>Product</th>
<th>Product version</th>
<th>Activation method</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESET Endpoint Security for Windows</td>
<td>6.x &amp; 5.x</td>
<td>6.x - License Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.x - Username/Password</td>
</tr>
<tr>
<td>ESET Endpoint Antivirus for Windows</td>
<td>6.x &amp; 5.x</td>
<td>6.x - License Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.x - Username/Password</td>
</tr>
<tr>
<td>Product</td>
<td>Product version</td>
<td>Activation method</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>ESET Endpoint Security for OS X</td>
<td>6.x</td>
<td>License Key</td>
</tr>
<tr>
<td>ESET Endpoint Antivirus for OS X</td>
<td>6.x</td>
<td>License Key</td>
</tr>
<tr>
<td>ESET Endpoint Security for Android</td>
<td>2.x</td>
<td>License Key</td>
</tr>
<tr>
<td>ESET File Security for Windows Server</td>
<td>6.x</td>
<td>License Key</td>
</tr>
<tr>
<td>ESET File Security for Microsoft Azure</td>
<td>6.x</td>
<td>License Key</td>
</tr>
<tr>
<td>ESET Mail Security for Microsoft Exchange Server</td>
<td>6.x</td>
<td>License Key</td>
</tr>
<tr>
<td>ESET Security for Microsoft SharePoint Server</td>
<td>6.x</td>
<td>License Key</td>
</tr>
<tr>
<td>ESET Mail Security for IBM Domino Server</td>
<td>6.x</td>
<td>License Key</td>
</tr>
</tbody>
</table>

Older versions of ESET products manageable via ESET Remote Administrator 6:

<table>
<thead>
<tr>
<th>Product</th>
<th>Product version</th>
<th>Activation method</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESET File Security for Microsoft Windows Server</td>
<td>4.5.x</td>
<td>Username/Password</td>
</tr>
<tr>
<td>ESET NOD32 Antivirus 4 Business Edition for Mac OS X</td>
<td>4.x</td>
<td>Username/Password</td>
</tr>
<tr>
<td>ESET NOD32 Antivirus 4 Business Edition for Linux Desktop</td>
<td>4.x</td>
<td>Username/Password</td>
</tr>
<tr>
<td>ESET Mail Security for Microsoft Exchange Server</td>
<td>4.5.x</td>
<td>Username/Password</td>
</tr>
<tr>
<td>ESET Mail Security for IBM Lotus Domino</td>
<td>4.5.x</td>
<td>Username/Password</td>
</tr>
<tr>
<td>ESET Security for Microsoft Windows Server Core</td>
<td>4.5.x</td>
<td>Username/Password</td>
</tr>
<tr>
<td>ESET Security for Microsoft SharePoint Server</td>
<td>4.5.x</td>
<td>Username/Password</td>
</tr>
<tr>
<td>ESET Security for Kerio</td>
<td>4.5.x</td>
<td>Username/Password</td>
</tr>
<tr>
<td>ESET NOD32 Antivirus Business Edition</td>
<td>4.2.76</td>
<td>Username/Password</td>
</tr>
<tr>
<td>ESET Smart Security Business Edition</td>
<td>4.2.76</td>
<td>Username/Password</td>
</tr>
</tbody>
</table>

### 1.3 Icon legend

This is a collection of icons used throughout ERA Web Console with their description. Some of the icons depicts actions, item types or current status. Most icons are displayed in one of three colors to denote the accessibility of an element:

- Default icon - available action
- Blue icon - highlighted element when you hover with mouse pointer
- Gray icon - action not available

<table>
<thead>
<tr>
<th>Status icon</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>![i]</td>
<td><strong>Show Details</strong> <a href="#">detailed information</a> about the client device.</td>
</tr>
<tr>
<td>![i] ![i]</td>
<td><strong>Show Alerts</strong> <a href="#">detailed information</a> about alerts on target client device.</td>
</tr>
</tbody>
</table>
| ![+] ![+]  | **Add New** - add new devices  
**New Task** - add new task  
**New Notification** - add new notification  
**New Static/Dynamic groups** - add new groups |
<p>| ![edit] ![edit] | <strong>Edit</strong> - you can edit your created tasks, notifications, reports template, groups, policies, etc. |
| ![copy] ![copy] | <strong>Duplicate</strong> - lets you create a new policy based on the existing policy you’ve selected, a new name is required for the duplicate. |</p>
<table>
<thead>
<tr>
<th>Status icon</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Move icon" /></td>
<td><strong>Move</strong> - computers, policies, Static or Dynamic groups. <strong>Access Group</strong> - Move the item to a different static group.</td>
</tr>
<tr>
<td><img src="image" alt="Delete icon" /></td>
<td><strong>Delete</strong> - removes the selected client, group, etc completely.</td>
</tr>
<tr>
<td><img src="image" alt="Rename multiple items icon" /></td>
<td><strong>Rename multiple items</strong> - if you select multiple items you can rename them one by one in a list or use Regex search and replace multiple items at once.</td>
</tr>
<tr>
<td><img src="image" alt="Add New icon" /></td>
<td><strong>Add New</strong> - add new devices</td>
</tr>
<tr>
<td><img src="image" alt="Scan icon" /></td>
<td><strong>Scan</strong> - using this option will run the <a href="#">On Demand Scan</a> task on the client that reported the threat.</td>
</tr>
<tr>
<td><img src="image" alt="Update Modules icon" /></td>
<td><strong>Update Modules</strong> - using this option will run the <a href="#">Modules Update</a> task (triggers an update manually).</td>
</tr>
<tr>
<td><img src="image" alt="Run Task icon" /></td>
<td><strong>Run Task</strong> for mobile devices</td>
</tr>
<tr>
<td><img src="image" alt="Reenroll icon" /></td>
<td><strong>Reenroll</strong> - opens <a href="#">Add mobile device via email</a> window.</td>
</tr>
<tr>
<td><img src="image" alt="Unlock icon" /></td>
<td><strong>Unlock</strong> - device will be unlocked.</td>
</tr>
<tr>
<td><img src="image" alt="Lock icon" /></td>
<td><strong>Lock</strong> - device will be locked when suspicious activity is detected or the device is marked as missing.</td>
</tr>
<tr>
<td><img src="image" alt="Find icon" /></td>
<td><strong>Find</strong> - if you want to request the GPS coordinates of your mobile device.</td>
</tr>
<tr>
<td><img src="image" alt="Siren icon" /></td>
<td><strong>Siren</strong> - triggers a loud siren remotely, the siren will start even if your device is set to mute.</td>
</tr>
<tr>
<td><img src="image" alt="Wipe icon" /></td>
<td><strong>Wipe</strong> - all data stored in your device will be permanently erased.</td>
</tr>
<tr>
<td><img src="image" alt="Reboot icon" /></td>
<td><strong>Reboot</strong> - if you select a computer and press <strong>Reboot</strong> the device will be rebooted. <strong>Restore</strong> - restore <a href="#">quarantined</a> file to its original location.</td>
</tr>
<tr>
<td><img src="image" alt="Shutdown icon" /></td>
<td><strong>Shutdown</strong> - if you select a computer and press <strong>Shutdown</strong> the device will be shut down.</td>
</tr>
<tr>
<td><img src="image" alt="Run Task... icon" /></td>
<td><strong>Run Task...</strong> - select a task and configure trigger and <a href="#">throttling</a> (optional) for this task. The task will be queued according to the task settings. This option immediately triggers an existing <a href="#">task</a>, that you select from a list of available tasks.</td>
</tr>
<tr>
<td><img src="image" alt="Last used tasks icon" /></td>
<td><strong>Last used tasks</strong> - shows last used tasks. You can click on task to execute it again.</td>
</tr>
<tr>
<td><img src="image" alt="Assign User... icon" /></td>
<td><strong>Assign User...</strong> - assign user to a device. You can manage users in <a href="#">User management</a>.</td>
</tr>
<tr>
<td><img src="image" alt="Manage Policies icon" /></td>
<td><strong>Manage Policies</strong> - a policy can also be assigned directly to a client (multiple clients), not just a group. Select this option to assign the policy to selected client(s).</td>
</tr>
<tr>
<td><img src="image" alt="Send Wake-Up Call icon" /></td>
<td><strong>Send Wake-Up Call</strong> - ERA Server runs instant replication of the ERA Agent on a client machine. UDPv4 and UDPv6 ports are used with default port numbers 1237 and 1238. This is useful when you do not want to wait for the regular interval when the ERA Agent connects to the ERA Server. For example when you want a <a href="#">Client Task</a> to be run immediately on client(s) or if you want a <a href="#">Policy</a> to be applied right away.</td>
</tr>
<tr>
<td><img src="image" alt="Deploy Agent icon" /></td>
<td><strong>Deploy Agent</strong> - with this option, you can create a <a href="#">new Server Task</a>.</td>
</tr>
<tr>
<td><img src="image" alt="Deactivate product icon" /></td>
<td><strong>Deactivate product</strong> - removes license from all selected devices via ESET license server.</td>
</tr>
<tr>
<td><img src="image" alt="Connect icon" /></td>
<td><strong>Connect</strong> - generate and download a <code>.rdp</code> file that will let you connect to target device via Remote Desktop Protocol.</td>
</tr>
<tr>
<td><img src="image" alt="Mute icon" /></td>
<td><strong>Mute</strong> - if you select a computer and press <strong>Mute</strong>, the Agent of this client stops reporting to ERA; it will only aggregate the information. A muted icon will be displayed next to a computer name in the Muted column. Once muting is disabled by clicking <strong>Mute &gt; Un-mute</strong>, the muted computer will report again and communication between ERA and the client is restored.</td>
</tr>
<tr>
<td><img src="image" alt="Disable icon" /></td>
<td><strong>Disable</strong> - disable or remove a setting or selection.</td>
</tr>
<tr>
<td>Status icon</td>
<td>Descriptions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Assign</td>
<td>to assign a Policy to client or groups.</td>
</tr>
<tr>
<td>Import</td>
<td>select Reports, Policies or Public key you want to import.</td>
</tr>
<tr>
<td>Export</td>
<td>select Reports, Policies or Peer Certificate you want to export.</td>
</tr>
<tr>
<td>Desktop</td>
<td></td>
</tr>
<tr>
<td>Virtual Machine(Agentless)</td>
<td></td>
</tr>
<tr>
<td>Mobile</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>File Server</td>
<td></td>
</tr>
<tr>
<td>Mail Server</td>
<td></td>
</tr>
<tr>
<td>Gateway Server</td>
<td></td>
</tr>
<tr>
<td>Collaboration Server</td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Mobile Device Connector</td>
<td></td>
</tr>
<tr>
<td>Rouge Detection Sensor</td>
<td></td>
</tr>
<tr>
<td>Virtual Agent Host</td>
<td></td>
</tr>
<tr>
<td>Proxy</td>
<td></td>
</tr>
<tr>
<td>ERA Server</td>
<td></td>
</tr>
<tr>
<td>Shared Local Cache</td>
<td></td>
</tr>
<tr>
<td>Virtual Security Appliance</td>
<td></td>
</tr>
<tr>
<td>Enterprise Inspector Agent</td>
<td></td>
</tr>
<tr>
<td>Enterprise Inspector Server</td>
<td></td>
</tr>
</tbody>
</table>
2. Getting started with ESET Remote Administrator Web Console

ESET Remote Administrator can be configured and managed via Era Web Console. After you have successfully installed ESET Remote Administrator or deployed ERA VA, you can connect to your ERA Server using ERA Web Console.

The following sections detail ERA Web Console features and how to use it. You can create installers and deploy ERA Agent/ESET security product on client computers. After ERA Agent deployment, you can manage groups, create and assign policies, set up notifications and reports. Select a topic below to learn more:

- Opening the ERA Web Console
- Using the Startup Wizard
- ERA Web Console
- Status overview

2.1 Introduction to ESET Remote Administrator

Welcome to ESET Remote Administrator (ERA) version 6. ERA 6 allows you to manage ESET products on workstations, servers and mobile devices in a networked environment from one central location. Using the ESET Remote Administrator Web Console (ERA Web Console), you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or threats on remote computers. ERA is made up of the following components:

- **ESET Remote Administrator Server** - ERA Server can be installed on Windows as well as Linux servers and also comes as a Virtual Appliance. It handles communication with Agents, and collects and stores application data in the database.

- **ERA Web Console** - ERA Web Console replaces ESET Remote Administrator Console (ERAC) in older versions, and is the primary interface that allows you to manage client computers in your environment. It displays an overview of the status of clients on your network and allows you to deploy ESET solutions to unmanaged computers remotely. After you install ESET Remote Administrator Server (ERA Server), you can access the Web Console using your web browser. If you choose to make the web server available via the Internet, you can use ERA from any place and/or device with an Internet connection.

- **ERA Agent** - The ESET Remote Administrator Agent facilitates communication between the ERA Server and client computers. You must install the Agent on any client computer to establish communication between that computer and the ERA Server. Because it is located on the client computer and can store multiple security scenarios, use of the ERA Agent significantly lowers reaction time to new threats. Using ERA Web Console, you can deploy the ERA Agent to unmanaged computers that have been recognized via your Active Directory or ESET RD Sensor. You can also manually install the ERA Agent on client computers if necessary.

- **ERA Proxy** - While it is not required for the deployment of your ESET solution, the ERA Proxy provides scalability. You can deploy the Proxy server on large networks to optimize database queries, improve overall network performance, and distribute load on the ERA Server. The ERA Proxy is also responsible for distributing configuration data to client Agents. You must install the ERA Agent on the same computer as the ERA Proxy Server to facilitate communication between the ERA Server and the Proxy.

- **Rogue Detection Sensor** - ERA Rogue Detection Sensor detects unmanaged computers present on your network and sends their information to the ERA Server. This allows you to easily add new client computers to your secured network. RD Sensor remembers computers that have been discovered and will not send the same information twice.

- **HTTP Apache Proxy** - Is a service that can be used in combination with ESET Remote Administrator 6 and later to distribute updates to client computers and installation packages to the ESET Remote Administrator Agent.

- **Mobile Device Connector** - Is a component that allows for Mobile Device Management with ESET Remote Administrator, permitting you to manage mobile devices (Android and iOS) and administer ESET Endpoint Security for Android.
• **ERA VA Deployment** - The ERA Virtual Appliance (ERA VA) is available for users who want to run ESET Remote Administrator (ERA) in a virtualized environment.

• **ESET Remote Administrator Virtual Agent Host** - A component of the ESET Remote Administrator that virtualizes agent entities to allow for the management of agent-less virtual machines. This solution enables vMotion of virtual machines and thereby automation, dynamic group utilization and the same level of task management as ERA Agent on physical computers. The Virtual Agent collects information from virtual machines and sends it to the ERA Server.

• **Mirror Tool** - The mirror tool is necessary for offline modules updates. If your client computers do not have an internet connection and need modules updates, you can use the Mirror Tool to download update files from ESET update servers and store them locally.

• **Migration Tool** - For an upgrade or migration from an older generation of ESET Remote Administrator 5 to ESET Remote Administrator 6, you can use our Migration Tool to make the upgrade process easier. The Migration Tool is a standalone application that uses a wizard to provide straightforward migration of ERA 4.x / 5.x data into an intermediate database that can then be imported into ERA 6.x.

• **Standalone Deployment Tool** - This tool serves to deploy All-in-one packages created in the ERA Web Console. It is a convenient way to distribute ERA Agent together with an ESET product on computers over a network.

• **ESET License Administrator** - ESET License Administrator, a new licensing portal for ESET products, allows you to manage licenses as a license owner (renewal/purchasing privileges) or security admin (product admin privileges) and observe license events such as expiration, usage, and authorization. See the ESET License Administrator section of this document for instructions to activate your product, or see the ESET License Administrator User Guide for more information about using the ESET License Administrator. If you already have an ESET-issued Username and Password that you want to convert to a License Key, see the Convert legacy license credentials section.

2.2 Opening the ERA Web Console

ESET Remote Administrator Web Console is the main interface used to communicate with ERA Server. You can think of it as a control panel, a central place from which you can manage all ESET security solutions. It is a web-based interface that can be accessed using a browser from any place and any device with internet access.

There are multiple ways to open the ERA Web Console.

• On your **local server** (the machine hosting your Web Console) type this URL into the web browser: https://localhost/era/

• From **any place with internet access** to your web server, type the URL in following format: https://yourservername/era/
Replace "yourservername" with the actual name or IP address of your web server.

• To log into the **ERA Virtual appliance**, use following URL:
https://[IP address]/
Replace "[IP address]" with the IP address of your ERA VM. If you do not remember the IP address, see step 9 of Virtual appliance deployment instructions.
On your local server (the machine hosting your Web Console), click **Start > All Programs > ESET > ESET Remote Administrator > ESET Remote Administrator Web Console** - a login screen will open in your default web browser. This does not apply to the ERA Virtual appliance.

When web server (that runs ERA Web Console) is up, the following login screen is displayed.

![Login Screen](image)

1. **NOTE**
   If you experience problems logging in or receive error messages while trying to log in, see [Web Console Troubleshooting](#).

### 2.3 Using the Startup Wizard

When you log into the Web Console for the first time, a **Startup Wizard** for ESET Remote Administrator will appear. This wizard will give a basic explanation of important ERA Web Console sections, ERA Agent and ESET security products. You will read about **Computers**, **Groups**, **Client Tasks**, **ERA Agent** and **ESET Endpoint Security 6** or **ESET Endpoint Antivirus 6**.

The last step of the Startup Wizard called Deployment will help you Create all-in-one installer package (containing ERA Agent and ESET security product).

2. **IMPORTANT**
   The installer package comes as an `.exe` file and is valid for Windows only.

If you do not want to use the wizard, click **Close Startup Wizard**. ERA Web Console will open. The wizard will not show up the next time you log into the ERA Web Console. You can view the Startup wizard again by clicking **Help > Startup Wizard**.

Use of the Wizard is not required, you can **Create all-in-one Agent installer** by clicking **Deploy ERA Agent...** in the **Quick Links** section.
**IMPORTANT**

If you want to create an installer package, your user account must have the Agent Deployment permission assigned. If a user account does not have this permission, the Startup Wizard will be displayed without the Deployment step and the user will not have the option to create an installer package.

Follow the steps bellow to create an installer package:

1. **Language** - select a language for the installer from the drop-down list of supported languages.

2. **Product** - select an ESET security product installation file from the list. If you choose version 6.3 or older, automatic product activation will not work, you'll have to activate the product later. ESET security version 6.4 or newer will be automatically activated during the installation.

**NOTE**

If you do not see any product installation files, make sure you have repository set to AUTOSELECT, in the Advanced settings section of Server settings.

3. **Choose License** (Optional) - you can add a license using one of the methods described in the Licenses section. If you already have existing licenses in License Management, simply choose the license that will be used to activate the ESET security product during the installation. If you do not choose a license, you can create an installer without it and activate the product later. ESET security version 6.4 or newer will be automatically activated during the installation.

4. If you select the Advanced checkbox, you'll be able to choose an Agent certificate and enter Certificate passphrase if needed. For example if you've specified the passphrase during the installation of your ERA, or if you are using Custom certificate with a passphrase. Otherwise, leave the Certificate passphrase field blank.

5. Click Create Installer, all-in-one installation package files will be generated for 32-bit and 64-bit operating systems. Click the desired version to start downloading it. Once the download completes you will be prompted to specify location where to store the file (for example ERA_Installer_x32_en_US.exe or ERA_Installer_x64_en_US.exe), click Save file.

6. Run the all-in-one installation package file on a client computer. For step-by-step instructions, see All-in-one Agent setup wizard.
2.4 ERA Web Console

ESET Remote Administrator Web Console is the main interface used to communicate with ERA Server. You can think of it as a control panel, a central place where you can manage all of your ESET security solutions. It is a web-based interface that can be accessed using a browser (see Supported Web browsers) from any place and any device with internet access.

In the ERA Web Console standard layout:

- The current user is always shown in the upper right, where the timeout for his/her session counts down. You can click Logout to log out at any time. When a session times out (because of user inactivity), a user must log in again.
- To change User Settings, click your username in top right corner of ERA Web Console.
- You can click ? at the top of any screen to open the Help menu. The first link in this menu always links to Online Help for the current screen.
- The Menu is accessible on the left at all times except when using a wizard. Click the ☰ to expand the menu on the left side of the screen; you can collapse it by clicking ▼ Collapse menu.
- The ⚙ icon always denotes a context menu.
- Click ⌁ Refresh to reload/refresh displayed information.

Status Overview shows you how to get the most out of ESET Remote Administrator. This will guide you through the recommended steps.
Screens with trees have specific controls. The tree itself is on the left with actions below. Click an item from the tree to display options for that item.

Tables allow you to manage units from rows individually, or in a group (when more rows are selected). Click a row to display options for units in that row. Data in tables can be filtered and sorted.
Objects in ERA can be edited using wizards. All wizards share the following behaviors:
2.5 How to manage Endpoint products from ESET Remote Administrator

Administrator can perform variety of tasks from the ERA Console in order to install products and control client computers. Follow links below to read more about those topics.

Installation of ERA Agent and Endpoint security products

ESET Remote Administrator requires that the ERA Agent to be installed on each managed client computer. The ERA Agent can be installed in combination with your Endpoint security product using the deployment tool or all-in-one installer. Before installation, we recommend that you import your license into ESET Remote Administrator so it can be used for your consequent installations. There are two methods to install your Endpoint product:

- Use the deployment tool or all-in-one installer to install your Endpoint product and ERA Agent at the same time
- Install your ESET Endpoint product on clients where you have already installed ERA Agent using a client task

Managing the Endpoint security product from ESET Remote Administrator

All Endpoint security products can be managed from ERA Web Console. Policies are used to apply settings to single computers or groups. For example, you can create a policy to block access to certain web localities or change all other settings from in the product. Policies can be merged, as shown in our example. Policies set using ERA cannot be overwritten by a user on a client machine. However, the administrator can use the override feature to allow a user to make changes on a client temporarily. When you are finished making changes, you can request the final configuration from the client and save it as a new policy.
Client tasks can also be used to manage clients. Client tasks are deployed from the Web Console and executed on the client by the ERA Agent. The most common client tasks for Windows Endpoints are:

- **Update modules** (also updates the virus database)
- Run **On-Demand scan**
- Run custom **command**
- Request the computer and product **configuration**

### Reporting the computer status and getting information from clients to ESET Remote Administrator

Each client computer is connected to ESET Remote Administrator through ERA Agent. The Agent reports all requested information about the client machine and its software to the ERA Server. The connection between the agent and server is set by default to 1 minute, but it can be **changed** in your ERA Agent policy. All logs from Endpoints or other ESET security products are sent to the ERA Server.

Information about installed ESET products and other basic information about a client's OS and status can be found in **Admin > Computers**. Select a client and click **Show Details**. In the **Configuration** section of this window, a user can look up older configurations or request current configuration. In the **SysInspector** section, a user can request logs (from Windows computers only).

Web Console also allows you to access a list of all threats (navigate to **Threats**) from client devices. Threats from a single device can be viewed in **Admin > Computers**. Select a client and click **Show Details > Threats and Quarantine**.

You can generate custom **reports** on-demand or using a scheduled task to view data about clients in your network. Pre-defined report templates offer a quick way to gather important data, or you can create your own **new templates**. Examples of reports include aggregated information about computers, threats, quarantine and necessary updates.

<table>
<thead>
<tr>
<th>IMPORTANT</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user can only use report templates for which he has sufficient <strong>permissions</strong>. By default, all templates are stored in the group <strong>All</strong>. A report can only include information about computers and events within that user's permission scope. Even if a report template is shared among more users, each user's report will only contain information about devices for which that user has permission. See the list of permissions for more information on access rights.</td>
</tr>
</tbody>
</table>

### 2.6 Following upgrade from an earlier version of ERA

Updates to security in ESET Remote Administrator 6.5 make it necessary to review your network **users** settings, **permissions** and **server settings** following an upgrade from an earlier build of ERA.

#### Users and permission sets

The administrator should review all users and **permission sets**. The new security model is strongly based on static groups, so we recommend that you plan the structure of your groups and create permission sets afterward. The administrator can also create **new native users**.

<table>
<thead>
<tr>
<th>IMPORTANT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not forget to <strong>assign each user a home group</strong> and permission set that will give the user permissions over that group. All objects created by the user are always automatically contained in that user's home group.</td>
</tr>
</tbody>
</table>

Following an upgrade, users will be divided into two categories:

- Users who were not assigned a permission set for the **All** group in the older version of ERA will not have a home group in the new ERA. These users will not have permissions for **Groups and Computers** and therefore will not be able to see any devices.

- Users who were assigned a permission set for the **All** group in the older version of ERA will keep their permissions for the **All** group. Additionally, these users will gain a new permission for the **Groups and Computers** functionality.
Server tasks and triggers

ESET Remote Administrator 6.5 allows only one trigger for each server task. The number of server task triggers is automatically adjusted after an upgrade to match the number of server tasks. From Admin > Server Tasks select a task to see details about its trigger.

Reports, templates and all other objects

Following an upgrade all objects are contained in the static group All. The administrator can share objects among users in different ways:

- duplicate objects to make them available to non-admin users
- move objects to shared groups where more users can access them
- users can be assigned other permission sets that would grant them limited rights for certain objects (for example Policies) over the All group

Static and dynamic groups

Static groups are essential for the new security model in ESET Remote Administrator 6.5, each object is located in one static group. Following an upgrade, the structure of static and dynamic groups stays the same. Users must be assigned proper permissions for their group so that they can see and interact with other group members.
3. Working with ERA Web Console

All clients are managed through the ERA Web Console. You can access the ERA Web Console from any device using a compatible browser. The ERA Web Console is divided into three main sections:

1. At the top of the ERA Web Console, you can use the Quick Search tool. Type a Client name or IPv4/IPv6 Address and press Enter. You will be redirected to the Groups section where the relevant client(s) will be displayed.

<table>
<thead>
<tr>
<th>Quick links</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New Computer</td>
<td>Create New Policy</td>
</tr>
<tr>
<td>Add New Mobile Device</td>
<td>Assign Policy</td>
</tr>
<tr>
<td>Add New User</td>
<td></td>
</tr>
<tr>
<td>Generate Report</td>
<td></td>
</tr>
<tr>
<td>New Client Task</td>
<td>Open</td>
</tr>
<tr>
<td>Installers</td>
<td></td>
</tr>
<tr>
<td>Create New Installer</td>
<td></td>
</tr>
<tr>
<td>Deploy ERA Agent</td>
<td>Dynamic Group Templates</td>
</tr>
<tr>
<td></td>
<td>License Management</td>
</tr>
</tbody>
</table>

2. The menu on the left contains the main sections of ESET Remote Administrator and the following items:

- Dashboard
- Computers
- Threats
- Reports
- Admin

3. Buttons on the bottom of the page are unique for each section and function, and are described in detail in their respective chapters.

**NOTE**

One button is common for all new items: Mandatory Settings. This red button is displayed when mandatory settings have not been configured and are preventing completion of the item. This is also indicated by a red exclamation mark next to each section. Click Mandatory Settings to navigate to the section where the settings in question are located.

**General rules**

- Required (mandatory) settings are always marked with a red exclamation mark next to the section and the respective settings. To navigate to mandatory settings (if applicable), click Mandatory settings at the bottom of each page.
- If you need help when working with ESET Remote Administrator, click the ? icon in the top right corner and click <Current topic> - Help. The respective help window for the current page will be displayed.
- See Admin for more information.
3.1 Login screen

A user needs login credentials (username and password) to log into the Web Console. It is also possible to log in as a domain user by selecting the checkbox next to Log into domain (a domain user is not related to any mapped domain group).

NOTE
If you experience problems logging in or receive error messages while trying to log in, see Web Console Troubleshooting for suggestions to resolve your issue.

You can select your language by clicking the drop-down arrow next to currently selected language, for details see our Knowledgebase article.

Deselect Allow session in multiple tabs checkbox if you do not want to allow ERA Web Console to open in multiple tabs in your web browser.

Change Password / Use Different Account allows you to change password or switch back to the login screen.

Session management and security measures:

- Login IP address lockout
  After 10 unsuccessful login attempts from the same IP address, further login attempts from this IP address are blocked for approximately 10 minutes. The IP address ban on login attempts does not affect existing sessions.

- Wrong session ID address lockout
  After using an invalid session ID 10 times from the same IP address, all further connections from this IP address are blocked for approximately 10 minutes. Expired session IDs are not counted. If there is an expired session ID in the browser, it is not considered an attack. The 15 minute IP address ban is for all actions (including valid requests). The ban can be released by restarting Web Console (tomcat service).
3.1.1 Troubleshooting - Web Console

This section will help you with Web Console login error massages:

<table>
<thead>
<tr>
<th>Error message</th>
<th>Possible cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login failed: Invalid username or password</td>
<td>Carefully check that you entered your username and password correctly.</td>
</tr>
<tr>
<td>Login failed: Connection has failed with state 'Not connected'</td>
<td>Check to see, whether the ERA Server service and your database service are running, see our Knowledgebase article.</td>
</tr>
<tr>
<td>Login failed: Communication error</td>
<td>Verify that Apache Tomcat is running and working properly.</td>
</tr>
<tr>
<td>Login failed: Connection timeout</td>
<td>Check network connection and firewall settings to make sure ERA Web Console can reach ERA Server. Also, ERA Server may be overloaded, attempt to reboot it. This issue can also occur if you are using different versions of ERA Web Console and ERA Server.</td>
</tr>
<tr>
<td>Login failed: User has no access rights assigned</td>
<td>User does not have any access rights assigned. Log in as an administrator and edit user's account assigning at least one Permission Set to this user.</td>
</tr>
<tr>
<td>Using unencrypted connection! Please configure the webserver to use HTTPS</td>
<td>For security reasons, we recommend that you set up ERA Web Console to use HTTPS.</td>
</tr>
</tbody>
</table>

JavaScript is disabled. Please enable JavaScript in your browser.

You do not see the login screen or the login screen appears to be constantly loading.

You do not see the login screen or the login screen appears to be constantly loading. Restart the ESET Remote Administrator Server service. Once the ESET Remote Administrator Server service is up and running again, restart the Apache Tomcat service. After this, the ESET Remote Administrator Web Console login screen will load successfully.

"An unexpected error has occurred" or "An uncaught exception has occurred"

This error typically occurs when you are accessing the ESET Remote Administrator Web Console, see supported web browsers.

**NOTE**

Since the Web Console uses secure protocol (HTTPS), you might get a message in your web browser regarding a security certificate or untrusted connection (exact wording of the message depends on the browser you are using). This is because your browser wants you to verify the identity of the site you are trying to access. Click Continue to this website (Internet Explorer) or I Understand the Risks, click Add Exception... and then click Confirm Security Exception (Firefox) to allow access to the ERA Web Console. This only applies when you’re trying to access the ESET Remote Administrator Web Console URL.

3.2 Dashboard

The dashboard is the default page displayed after you log into the ERA Web Console for the first time. It displays pre-defined reports about your network. You can switch between dashboards using the tabs in the top menu bar. Each dashboard consists of several reports. You can customize your dashboards by adding, modifying, resizing, moving and re-arranging reports. You can use Set as default to set your customized dashboard as a default for all new users. To revert these settings, click Reset to default (click the symbol next to the Dashboard title).

The following five dashboards come pre-configured in ESET Remote Administrator:

Computers
This dashboard gives you an overview of client machines, including their protection status, operating systems and update status.
Remote Administrator Server
In this dashboard, you can view information about the ESET Remote Administrator server itself, including server load, clients with problems, CPU load and database connections.

Antivirus threats
Here you can see reports from the antivirus module of client security products, including active threats, threats in the last 7/30 days, and so on.

Firewall threats
Firewall events of the connected clients arranged according to their severity, time of reporting, etc.

ESET applications
This dashboard lets you view information about installed ESET applications.

Dashboard functionality:

Permissions for Dashboard
A user must have the appropriate permission to work with Dashboards. Only report templates contained in a group where the user has access rights can be used in a Dashboard. If user has no rights assigned for Reports and Dashboard, he will see no data in the Dashboard section. Administrator can see all data by default.

IMPORTANT
Read - user can list report templates and their categories. User can also generate reports based on report templates. User is able to read his dashboard.
Use - user can modify his dashboard with available report templates
Write - create / modify / remove templates and their categories

All default templates are located in the All group.
3.2.1 User settings

In this section, you can customize your user settings. Click **User account** at the top right corner of the ERA Web Console (to the left of the **Logout** button) to display all active users. You can be logged into ERA Web Console from different web browsers, computers or mobile devices at the same time. You will see all your sessions here.

**NOTE**

User settings only apply to the user who is currently logged on. Each user can have their own preferred time settings for ERA Web Console. User-specific time settings are applied to that user regardless of where they access ERA Web Console.

- **Time Settings:**

  All information is stored internally in ESET Remote Administrator using the UTC (Coordinated Universal Time) standard. UTC time is automatically converted to the time zone used by ERA Web Console (taking daylight saving into account). ERA Web Console displays the local time of the system where ERA Web Console is running (not the internal UTC time). You can override this setting to set the time shown in ERA Web Console manually if you prefer.

  If you want to override the default **Use browser local time** setting, you can choose the **Select manually** option, then specify the console time zone manually and decide whether to use daylight saving time or not.

  **The changes will be applied after the next login.**

  ![TIME SETTINGS](image)

  **IMPORTANT**

  In some cases, the option to use a different time zone (for example, the local time of a client on which ERA is running) will be made available. This setting can be particularly pertinent when configuring triggers. When this option is available, it is indicated in ERA Web Console and you will be able to choose whether to **Use local time** or not.

  ![USE LOCAL TIME](image)

  Click **Save Time Settings** to confirm your changes.

- **Stored User State:**

  You can reset a stored user's UI state to default by clicking **Reset Stored User State**. This includes **Startup Wizard**, table column sizes, remembered filters, pinned side menu, etc.

  ![Reset stored user state](image)

  **Reset stored user state**

  Do you really want to reset stored user's UI state to default values?
  UI layout modifications (e.g. table column sizes, pinning side menu) and remembered filters will be reset.
  Some of the changes may require logout and login to be applied.

- **Active sessions**
Information about all active sessions of the current user contain:

- IP address of a client computer or a device from which a user is connected to ERA Web Console, and via IP address (in brackets) of a web server that runs ERA Web Console. In case ERA Web Console is running on the same machine as ERA Server, via 127.0.0.1 is displayed.
- Date and time when a user logged in.
- Selected language for ERA Web Console.

The current session is labeled This session. If you want to disconnect an active session, click Disconnect.

3.2.2 Dashboard settings

Use dashboard settings to manage pre-defined and newly created dashboards. The available options are described below:

- **Add a new dashboard** - Click the + symbol at the top of the dashboard header. Enter a name for the new dashboard and click OK to confirm. A new dashboard with nothing in the Reports field is created. Once you set up your dashboard, you can start adding reports to it.
- **Duplicate a dashboard** - Select the dashboard you want to duplicate and click the symbol next to the dashboard name. Select Duplicate from the list to create a duplicated dashboard.
- **Click Refresh page** to reload/refresh displayed information on selected dashboard.
- **Move a dashboard** - Click and drag the name of a dashboard to change its location relative to other dashboards.
- **Change the dashboard size (number of reports displayed)** - Click the symbol > Change layout. Select the number of reports you want to display in the dashboard and click them. The dashboard layout will change.
- **Rename a dashboard** - Click the symbol next to the dashboard name and click Rename. Enter a new name for the Dashboard and click OK.
- **Remove a dashboard** - Click the symbol next to the dashboard name, click Remove and then confirm the removal.
- **Resize** - Click the double-arrow symbol at the right of a report to resize it. More relevant reports are larger, while less relevant reports are smaller. You can also toggle full-screen mode to display any report full-screen.
Change Chart Type - Click the Chart symbol at the top left corner of a chart and select Pie Chart, Line Chart, etc. to change the chart type.

Click Refresh to refresh the displayed information inside the selected report.

Click Change to view a different report.

Click Edit report template to add or edit a template.

Click Set Refresh interval to define how often the data in a report is refreshed. The default refresh interval is 120 seconds.

Click Schedule to add/change the report schedule settings.

Click Rename/Remove the report.

### 3.2.3 Drill down

This dashboard functionality is useful for examining data in greater detail. It lets you interactively select specific items from a summary and view detailed data about them. Focus in on the item of interest by "drilling down" from summary information in order to get more information about this particular item. There are usually multiple levels you can drill down through.

There are four drill down types:

- **Show Detailed information** - Computer name and description, Static Group name, etc. Displays original (not aggregate) data for the clicked row.
- **Show Only 'value'** - Information, Critical, Security risk, Security notification, etc.
- **Expand column 'value'** - This will show aggregated information (usually for count or sum). For example, if there is just a number in the column and you click Expand column Computer, it will list all details about computers.
- **Show In Computers page (all)** - Redirects you to the Computers page (shows a result of 100 items only).

**NOTE**
The results you get using drill down of other reports will show the first 1000 items only.

Click the Generate and Download button if you want to generate and download the report. You can choose from .pdf, .ps or .csv (only table data).
3.2.4 Edit report template

This section details editing existing report templates (for information on how to create a new report template click here).

Click a blank square in the new dashboard. The Add Report window will be displayed. Select Installed applications and click Edit Template.

- Basic

Edit the Basic information about the Template. Review or change the Name, Description and a Category. This information is pre-defined according to the selected Report type.

- Chart

In the Chart section, select the Report type. In this example, we leave the Display Table option empty and select the Display Chart option.
NOTE
All selected chart types will be displayed in the Preview section. This way, you can see what the report will look like in real-time.

Selecting a Chart gives you multiple options. For a better overview, we select the Stacked Line Chart type. This chart type is used when you want to analyze data with different units of measure.

Optionally, you can define a title for the X and Y axis of the chart to make reading the chart and identifying trends easier.

Data
In the Data section, we enter the information to be displayed on the X and Y axis of the chart. Clicking the respective symbols opens a window with options. The choices available for the Y axis always depend on the information selected for the X axis and vice versa, because the chart displays their relation and the data must be compatible.

For the X axis, we select Computer > Computer name to determine what computers are sending spam. The Format will be set to Computer > Computer name. Color and Icons are set by the administrator.

For the Y axis, we select Installed software > Size in MB to determine the absolute number of the spam messages. The Format will be set to Installed software > Size in MB. Color and Icons are set by the administrator.

Sorting
Add sorting to define the relation between the selected data. Select the starting information and then the method, either Ascending or Descending. It is also possible to sort the data by both options (shown above).

Filter

Options displayed here depend on the settings configured earlier (information for the X and Y axis). Select an option and a mathematical function to determine how the data will be filtered. For this example, we selected Installed Software and Application name > is equal to > ESS and Installed Software. Size in MB > is greater than > 50.
In the **Summary**, review the selected options and information. If they are to your satisfaction, click **Finish** to create a **Report template**.

### 3.3 Computers

All client computers that were **added** to ESET Remote Administrator are shown here and are divided into **Groups**. Clicking on a group from the list (on the left) will display the members (clients) of this group in the right pane. You can filter the clients using the filters at the top of the page, there are also a few pre-defined filters that are quickly accessible:

- You can filter by severity using the status icons: ⚠ red - **Errors**, 🔴 yellow - **Warnings**, ✅ green - **OK** and ⚫ gray - **Unmanaged** computers. The severity icon represents the current status of your ESET product on a particular client computer. You can use a combination of these icons by turning them on or off. For example, to see only the computers with warnings, leave only the 🔴 yellow icon on (the rest of the icons must be turned off). To see both, 🔴 warnings and ⚠ errors, leave only these two icons on.

- To add multiple filtering criteria, click **Add filter** and select an item from the list. You can filter the results by **Computer Name**, **Description**, **Connected time**, **OS Version** or the **IPv4/IPv6 address**. Active filters are highlighted in blue.

**NOTE**

If you are not able to find a particular computer in the list and know it is in your ERA infrastructure, make sure that all filters are turned off.

- Click the 🌋 icon to choose from Actions. You can **Refresh** the list of computers, **Edit columns**, use **Auto-fit columns** feature, **Clear Selection**, or use **Table Sorting**.


• **Show Subgroups** check box - to show subgroups of the currently selected group.

• **Unmanaged** computers (clients on the network that do not have the ERA Agent or an ESET security product installed) usually appear in the **Lost & Found** group.

• You can **select** specific device or **deselect** specific entries when you clicked the **select all** checkbox at the top.

• You can **drag** and **drop** clients to move them between groups.

Using the **drop-down** menu below the filters, you can limit the displayed clients (computers/mobiles). There are a few categories:

• **All Devices** - select this option from the drop-down menu to see all the client computers again, without limiting (filtering) displayed clients. You can use a combination of all the above filtering options when narrowing down the view.

• **ESET Protected** (protected by an ESET product)

• **ESET Remote Administrator** (individual ERA components such as Agent, RD Sensor, Proxy, Server, etc.)

• **Other** (Shared Local Cache, Virtual Appliance, Enterprise Inspector Agent, Enterprise Inspector Server). When you make your selection, only the respective clients will be displayed.

• You can use the context menu (**icon**) next to an existing group to create a new **Static** or **Dynamic** group, create a **New task** or select from other available actions.

By clicking on a device you can open a new menu with actions available for particular device. You can also open this menu if you click on Actions button on the bottom bar.
• Click **Actions** to execute actions. Refer to [Icon legend](#) for details about different icon types and statutes.

### 3.3.1 Computer details

To find out details about a computer, select a client computer in a Static or Dynamic Group and click **Show Details**.

The information window consists of seven different parts:

1. **Overview:**
   - **Name** - Change the computer's name or description.
   - **Description** - Add a custom description or additional information about the device.
   - **Parent group** - Change parent Static group of the computer.
   - **Logged users** - Domain and username of last logged users on the device.
   - **Assigned users** - Change assigned users with current computer.
   - **Alerts** - Link to list of problems with current computer.
   - **Unresolved threats count** - Count of unresolved threats.
   - **Last connected and Scan time** - Time information with last connection or scan.
   - **Virus signature database** - Version of virus signature database on target device.
   - **ESET security products** - List of ESET components installed on the computer.

2. **Configuration:**
   - **Configuration** - Contains list of configurations of installed ESET products (ERA Agent, ERA Proxy, ESET endpoint, etc.). Open configuration via context menu and convert it to a policy. Click a configuration to see it in the viewer. Click **Request configuration** to create a task for ERA Agent to collect all the managed product configurations. After the task is delivered to ERA Agent, it is executed immediately and the results are delivered to ERA Server on the next connection. This will allow you to see the list of all managed product configurations. Click **Convert to Policy** to open a configuration and convert it to a policy.

   - **Applied Policies** - List of policies applied to the computer. Click **Manage Policies** to manage, edit, assign or delete a policy.
SysInspector:
Displays the most recent SysInspector results. Click Request log (Windows only) to run the SysInspector log request task on selected clients.

Task Executions:
A list of executed tasks. You can filter the view to narrow down the results, drill down, edit, duplicate, delete or run on/rerun the task.

Installed Applications:
Displays a list of programs installed on a client with details such as version, size, security status, etc. Select a program and click Uninstall to remove it. You will be asked to enter Uninstallation parameters. These are optional command line parameters for the installer (installation package). Uninstallation parameters are unique for each software installer. You can find more information in the documentation for the particular product.

Do you want to uninstall the selected item?
Uninstallation parameters

- Automatically reboot when needed

Alerts:
Shows a list of alerts and their details: Problem, Status, Product, Occurred, Severity, etc. This category can be accessed directly from Computers section by selecting Show Alerts. You can also execute some actions from Computers Details screen by clicking Actions in the lower left corner.

Threats and Quarantine:
All threat types are displayed, but you can filter by Anti-virus, Firewall and HIPS threats for a more specific view.
- Quarantine - A list of quarantined threats with details such as Threat name, Threat type, Object name, Size, First occurred, Count, User reason, etc.

Details:
- Basic - Information about device management. If the device is muted, managed, last time updated and number of applied policies.
- Device - Information about the manufacturer and model of computer.
- OS information - OS Name, Type, Version, etc.
- Network adapters - Information about networking, IPv4 and IPv6, Subnet, etc.
- Device identifiers - Serial number, FQDN name, etc.

Click Actions to execute actions. Refer to the Icon legend for details about actions.
3.3.2 Import CSV

- **Upload** - click Choose File and browse for the .csv file you would like to Upload.

- **Delimiter** - a delimiter is a character that is used to separate text strings. Select an appropriate delimiter (Semicolon, Comma, Space or Tab) to match what your .csv file uses. If your .csv file uses different character as delimiter, click the check box Other and enter the character. Data preview shows the contents of your .csv file which can help you identify the type of delimiter used to separate strings.

- **Column mapping** - once the .csv file has been uploaded and parsed, you can map each desired column in the imported CSV file to an ERA column (Name, Email Address, Device name, Description, etc.) displayed in the table. Use the drop-down lists to select which CSV column should be associated with a specific ERA column. If your .csv file does not have a header row, deselect the CSV Heading check box. See the Table preview to make sure the column mapping is set correctly and the import operation will work the way you want.

Once you have successfully mapped each of the columns and the table preview looks correct, click Import to begin the operation.
3.4 Threats

The Threats section gives you an overview of all threats found on devices that the target user account is managing. On the left side, the group structure is displayed. Here you can browse groups and view threats on members of a given group. Select the All group and use the All threats types filter to display all threats found on clients in all groups assigned to target user account.

Filtering threats
By default, all threat types from the last seven days are shown. To add multiple filtering criteria, click Add filter on the top bar and select an item from the list. You can filter the results by Computer Muted, Threat Resolved, Name (name of the threat), Cause (cause of the threat) or the IP Address of the client that reported this threat. By default, all threat types are displayed, but you can filter by Anti-virus, Firewall and HIPS threats for a more specific view.

On-demand scan
Using this option will run the On Demand Scan task on the client that reported the threat.

Mark as resolved / Marked as Not Resolved
Threats now can be marked as resolved in the threats section or under details for a specific client.

Move to Group
Move a computer to different static group. This will make it accessible for the local admin of the target group. Local admin has full access rights in his group.

Mute
Selecting mute on a specific threat mutes this threat (not the client). This report will no longer be displayed as active. You can also choose to mute the client (select Mute from the context menu on the threat) that reported this threat.

Click on a specific threat to execute actions on it. Refer to the Icon legend for details about different icon types and statutes.

Table columns:
Resolved, Object, Process Name, Description, User, Computer Description, Action details, Restart required, Scanner, Object type, Circumstances, Number of Occurrences, Source Address, Source Port, Target Address, etc.
3.5 Reports

Reports allow you to access and filter data from the database in a convenient way. Reports are divided into categories, and each category includes a short description. You can only see report templates that were moved by an administrator to your group. Click Generate Now at the bottom of the page to create a report based on a selected template and then display this report.

You can use pre-defined report templates from the list of Categories & Templates, or you can create a new report template with custom settings. Click Create a new report template to view settings for each report in detail and specify custom settings for a new report.

Select a report and click Report Templates to open the Actions context menu. The following options are available:

- **Generate now**
  The report will be generated and you can review the output data.

- **Schedule**
  **Schedule Report** - Template window will open, where you can modify the schedule trigger, throttling and report delivery. You can find all scheduled reports in the Scheduled reports tab.

- **New Category**
  Enter a **Name** and a **Description** to create a new report template category.

- **New Report Template**
  Create a new custom report template.

- **Edit**
  Edit an existing report template. The same settings and options used for creating a new report template apply.

- **Duplicate**
  Lets you create a new report based on the selected report (a new name is required for the duplicate).

- **Delete**
  Remove the selected report template completely.
Import
Click **Choose file** and then browse to the file you want to **Import**.

Export
Select report template you want to export from the list and click **Report Templates > Export**. The report template(s) will be exported to a .dat file. To export multiple report templates, change the select mode, (see **Modes** below). You can also export whole template category including all its report templates.

**Access Group** - Move the report template Category to a different static group. This will make it accessible for the local admin of target group. Local admin has full access rights in his group.

You can use **Modes** to change select mode (Single or Multiple). Click the ▼ arrow in upper right corner and choose from the context menu:
- Single select mode - you can select single item.
- Multiple item select mode - lets you use the check boxes to select multiple items.
- Refresh - reloads/refreshes displayed information.
- Expand All - Lets you display all information.
- Collapse All - Lets you hide all information.

**NOTE**
The **Export** feature exports the selected report template, which can then be imported to another ERA Server using **Import**. This is useful, for example, when you want to migrate your custom report templates to another ERA Server.

**IMPORTANT**
The **Import / Export** feature is designed for importing and exporting report templates only, not an actual generated report with data.

Download
Select a report template, click **Download** and choose a .pdf, .ps or .csv file format (.csv is suitable only for table data). The report will be generated and downloaded.

Permissions for Reports
Access Group Filter

![ACCESS GROUP Select](image)

The **Access Group** filter button enables users to select a static group and filter viewed objects according to the group where they are contained.

**IMPORTANT**
**Read** - user can list report templates and their categories. User can also generate reports based on report templates. User is able to read his dashboard.

**Use** - user can modify his dashboard with available report templates

**Write** - create / modify / remove templates and their categories

All default templates are located in the **All** group.
3.5.1 Create a new report template

Navigate to Reports and click Report templates inside Categories & Templates tab. From the pop up window, select New Report Template....

Basic

Edit the Basic information about the Template. Enter a Name, Description and Category. You can only choose from pre-defined Categories. If you want to create a new one use the New Category option (described in the previous chapter).
In the **Chart** section, select the **Report** type. Either a **Table**, where the information is sorted in rows and columns, or a **Chart**, that represents data using an X and Y axis.

**NOTE**
The selected chart type will be displayed in the **Preview** section. This way, you can see what the report will look like in real-time.

Selecting a **Chart** gives you multiple options:

- **Bar chart** - A chart with rectangular bars proportional to the values they represent.
- **Dots chart** - In this chart, dots are used to display quantitative values (similar to a bar chart).
- **Pie chart** - A pie chart is a circular chart divided into proportional sectors, representing values.
- **Doughnut chart** - Similar to a pie chart, but the doughnut chart can contain multiple types of data.
- **Line chart** - Displays information as a series of data points connected by straight line segments.
- **Simple line chart** - Displays information as a line based on values without visible data points.
- **Stacked line chart** - This chart type is used when you want to analyze data with different units of measure.
- **Stacked bar chart** - Similar to a simple bar chart, but there are multiple data types with different units of measure stacked in the bars.

Optionally, you can enter a title for the **X** and **Y** axis of the chart to make it easier to read the chart and recognize trends.
In the **Data** section, select the information you want to display:

a. **Table Columns**: Information for the table is added automatically based on the selected report type. You can customize the **Name**, **Label** and **Format** (see below).

b. **Chart Axes**: Select the data for the **X** and the **Y** axis. Clicking the respective symbols opens a window with options. The choices available for the **Y** axis always depend on the information selected for the **X** axis and vice versa, because the chart displays their relation and the data must be compatible. Select the desired information and click **OK**.

You can change the **Format** in which the data is displayed to any of the following:

- **Data Bar** (only for the bar charts) / **Value** / **Color** / **Icons**

**Sorting**

Add **Sorting** to define the relation between the selected data. Select the starting information (sorting value) and sorting method, either **Ascending** or **Descending**. This will define the outcome displayed in the chart.

**Filter**

Next, define the filtering method. Select the filtering method from the list and its value. This defines what information will be displayed in the chart.

**Summary**

In the **Summary**, review the selected options and information. If they are to your satisfaction, click **Finish** to create a new report template.

Every report in the dashboard has its own options for customization - click the wheel symbol in the upper right corner to view them. Here, you can **Refresh** the displayed information, **Change** to a different report, **Edit** the report template (see options above), set a new **Refresh** interval that defines how often the data in this report is refreshed or **Rename/Remove** the report. Using the arrows in the symbol below, you can customize the size of the report. You can make more relevant reports larger, less relevant reports smaller and so on. Click **Toggle fullscreen** to view a report in fullscreen mode.
3.5.2 Generate report

There are three ways to generate a report from report template:

1. Navigate to Quick Links on the top bar and click Generate Report. Select an existing report template and click Generate Now.

2. Click Reports > Categories & Templates tab. Select a report template from which you want to generate a report. (You can Edit a pre-defined report template or create a new report template, but you must save the report template before you generate a report from it.)
   - You can use Generate now to generate and show the report in the ERA Web Console or generate and download the report (the report will be saved to the device you are accessing the Web Console from).

3. Click Admin > Server Tasks > New to create a new Generate Report task.
   - The task is now created and displayed in the Task types list. Select this task and click Run Now on the bottom of the page. The task will be executed immediately.
   - Configure the settings (as described in the Generate Report task) and click Finish.

3.5.3 Schedule a report

There are two ways to schedule a report:

1. Navigate to Admin > Server Tasks. Select New to create a new Generate Report task.

2. Select a report template from which you want to generate a report. You can use and edit a pre-defined report template, or create a new report template.
   - You can either send this report in an e-mail (in a file format defined here) or save it to a file. Clicking either option displays the corresponding settings below.
   - You can choose multiple report templates for one report.
   - Configure the settings (as described in the Generate Report task). This time, we will create a Server Trigger for this task.
   - In the Trigger section, navigate to Settings. Select Scheduled trigger and the time when you want this task to run.
   - Click Finish. The task is created and will run at the period defined here (either one time, or repeatedly).
You can find your scheduled reports in Reports > Scheduled Reports tab.

- You can use **Schedule** to create a new schedule to already existing report.
- Click **Show Details** to see detailed information about selected schedule.
- You can choose multiple report templates for one report.
- You can execute the scheduled report by clicking on **Run now**.
- Click **Actions** to execute actions. Refer to [Icon legend](#) for details about different icon types and statutes.

### 3.5.4 Outdated applications

Use the **Outdated applications** report to see which ERA components are not up to date.

There are two methods to run this report:

1. Add a **New Dashboard**, click one of the tiles and a pop-up screen with **Report Templates** listed will be displayed. Select **Outdated applications** from the list and click **Add**.

2. Go to Reports, navigate to the **Computers** category, select **Outdated applications** from the list and then click **Generate now...** The report will be generated and you can review the output data.

To upgrade the components, use the Client Task [Administrator Components Upgrade](#).
3.5.5 SysInspector log viewer

Using SysInspector log viewer, you can view logs from SysInspector after it is run on a client computer. You can also open SysInspector logs directly from a SysInspector Log Request task after it has been successfully executed.

To do so, follow the steps below:

1. Add a New Dashboard. Click one of the tiles and a pop-up screen with report templates will be displayed.
2. Go to Reports, navigate to the Automation category, select the SysInspector snapshot history in last 30 days template from the list and then click Generate now. The report will be generated and you can review the output data.
3. Select a computer in a Static or Dynamic Group and click **Details**, click the SysInspector tab and then click **Open SysInspector log Viewer.**
4. ESET Remote Administrator initial configuration

Before you can start managing ESET Business Solutions you need to perform initial configuration. We recommend that you to use **Status overview** and go through the steps from top to bottom, especially if you have skipped the **Startup Wizard**.

The **Status overview** explains each section well, but you can also read next chapters for further details.

### 4.1 Status overview

Use the **Status Overview** to see usage statistics and a general status of your ESET Remote Administrator. It can also help you with initial configuration of ESET Remote Administrator. Click **Admin > Status Overview** to see detailed status information about ESET Remote Administrator in the following sections (use the buttons to perform tasks):

- **Help and support** - you can view our [instructional videos](#) and the [ESET Knowledgebase](#) for more information about ESET Remote Administrator.

- **Users** - you can create different [users](#) and configure their [permissions](#) to allow different levels of management in ESET Remote Administrator. The default ERA Administrator account was created during installation. We do not recommend that you use the default ERA Administrator account as a normal user account. Rather, create a [new native user account](#) and use that as the default account in ESET Remote Administrator.

- **Certificates** (optional) - if you want to use different certificates than the default ones provided by ERA, you can create [Certification Authorities](#) and [Peer certificates](#) for individual ESET Remote Administrator components to allow communication with ERA Server.

- **Licenses** - ESET Remote Administrator 6 uses a completely new [ESET licensing system](#), select the method you want to use to add [License(s)](#), which will be used when activating ERA components and ESET security products on client computers.

- **Computers** - you have a number of options when adding client computers, servers and mobile devices on your network to the ERA structure. You can [Add Computers](#) and [Mobile devices](#) manually or import a list of devices. You can automatically import computers detected using [ESET RD Sensor](#) or you can run [Static Group Synchronization](#) with Active Directory, LDAP, VMware, etc.

- **Agents** - there are multiple ways to [deploy ERA Agent](#) to client computers in your network. You can also create a [new policy for ERA Agent](#) to change the connection interval.

- **Products** - with the ERA Agent deployed, you can [install software](#) directly from the ESET repository or specify an installation package location (URL or a shared folder). You can create a new policy to change the configuration of the ESET security product installed on the client computers. Also, you can change [Server Settings](#) if necessary.

- **SMTP Settings** - ESET Remote Administrator can be configured to connect to your existing [SMTP server](#) which allows ERA to send email messages, for example [Notifications](#), mobile device enrollment emails, [Reports](#), etc.

- **Invalid objects** - Here you can find list of [client](#) and [server](#) tasks, [triggers](#) or [notifications](#) with references to unreachable or invalid objects. Click on any of the result fields to view a menu with the selected list of objects.
4.2 New native user account

After you log into ERA Web Console, create one or more Native user accounts and configure their Permission Sets to allow different levels of management in ESET Remote Administrator.

**IMPORTANT**

We do not recommend that you use the default ERA Administrator account as a normal user account. It serves as a backup in case something happens to normal user accounts or if you get locked out, etc. You can log in with the Administrator account to fix such issues.

To create a new native user, go to the Admin tab, click Access Rights > Users and then click New at the bottom of the page.

**NOTE**

In order to create the user properly, we recommend you follow these steps:

1. Decide which static group will be the user's home group. If needed, create the group.
2. Decide what permission set would be best for the user. If needed, create new permission set.
3. Follow this chapter and create the user.

![Image of ERA Web Console](image)

**Basic**

Enter a User name and an optional Description for the new user. Select Home Group. This is static group where all objects created by this user will be automatically contained.

**Set Password**

The password for the user should have at least 8 characters. The password should not contain the username.
Account

Enabled - Select this option unless you want the account to be inactive (you intend to use it later).

Have to change password - Select this option to force the user to change their password the first time they log into the ERA Web Console.

Password expiration - This option defines the number of days that the password is valid (it needs to be changed after that).

Autologout (min) - This option defines the idle time period (in minutes) after which the user is logged out of Web Console.

Full Name, Email contact and Phone contact can be defined to help identify the user.

Permission set

A user can be assigned multiple permission sets. You can select a pre-defined competence: Reviewer permission set (read-only rights for the All group) or Administrator permission set (full access to the All group) or Server assisted installation permission set (minimal access rights required for server assisted installation) or you can use a custom permission set. Each permission set provides permissions only for objects contained in the Static Groups selected in the permission set. Users without any permission set will not be able to log in to the Web Console.

**WARNING**

All pre-defined permission sets have the All group in the Static Groups section. Be aware of this when assigning it to a user. Users will have these permissions over all objects in ERA.

Summary

Review the settings configured for this user and click Finish to create the user.

4.3 Certificates

Certificates are an important part of ESET Remote Administrator, they are required for ERA components to communicate securely with ERA Server. All Peer Certificates need to be valid and signed by the same Certification Authority to ensure ERA components can communicate correctly.

**IMPORTANT**

You will see only those certificates located in your home group (assuming you have read permission for certificates). Certificates which are created during the ERA installation are located in the All group and only administrators have access to them.

You have a few options when it comes to certificates:

- You can use certificates that were automatically created during ERA installation.
- You can create new Certification Authority (CA) or Import Public Key which you will use to sign the Peer Certificate for each of the components (ERA Agent, ERA Proxy, ERA Server, ERA MDM or Virtual Agent Host).
- You can use your custom Certification Authority and certificates.

**NOTE**

If you plan to migrate from ERA Server to a new server machine, you must export/back up all Certification Authorities you are using, as well as ERA Server Certificate. Otherwise none of the ERA components will be able to communicate with your new ERA Server.
4.4  Licenses - add new license

ESET Remote Administrator has its own License Management which is accessible from the main menu under Admin > License Management.

You can use one of the three methods when adding a license, you can enter the License Key, provide Security Admin credentials, or upload an Offline license file.

**IMPORTANT**

A new security model in ERA 6.5 has changed license management. Only administrators whose home group is set to All, with Write permission on licenses in the home group, can add or remove licenses. Each license is identified by its Public ID and can contain one or more units. Licenses can be distributed only by an administrator to other users (lower Admins). A license is not reducible.

Type or copy and paste the License Key you received when you purchased your ESET security solution in to the License Key field. If you are using legacy license credentials (a Username and password), convert the credentials to a license key. If the license is not registered, it will trigger the registration process, which will be done on the ELA portal (ERA will provide the URL valid for registration based on the origin of the license).

Enter the Security Admin account credentials (ERA will display all delegate licenses in ERA License Manager).
Offline license file - copy a specific License file token and enter into ESET License Administrator portal and include the information about product(s) ERA is able to manage.

**NOTE**
For further instructions how to download Offline license file, see License Owner or Security Admin.
One you are logged in ESET License Administrator portal, select the check box next to *Allow management with Remote Administrator* and enter *Server Token* (License file token from ERA) into ESET License Administrator portal when generating an offline license file, otherwise the license file won’t be accepted by ESET Remote Administrator.

Go back to ERA License Management, select **Browse** for the offline license file you’ve exported in ELA, click **Upload** and then click **Add licenses** button.
List of licenses shown in categories (activated by) License Key, Offline license or Security Admin.

ADD LICENSES  CANCEL
Licenses can be distributed to ESET security products from ERA using two tasks:

- The Software installation task
- The Product activation task

### 4.5 Deployment

After a successful installation of ESET Remote Administrator, it is necessary to deploy the ERA Agent on the client computers in your network. This section describes all available methods you can use to deploy ERA Agent. It is very important because ESET security solutions running on client computers communicate with ERA Server exclusively through the Agent.

After the successful installation of ESET Remote Administrator and ESET Remote Administrator initial configuration deployment consists of following steps:

1. **Add client computers** to ERA group structure, it is necessary to deploy the ERA Agent and ESET Endpoint product to the computers in the network.
2. **Agent deployment process** - you can choose from Local deployment or Remote deployment.
3. **Create a policy to apply your custom settings** - this policy will be enforced by the Agent as soon as the software is installed. See step 4 for details.
4. **ESET Endpoint protection deployment** - allow you to use the software install task to install ESET security products.

Should you experience problems when deploying the ERA Agent remotely (the Server task Agent deployment fails) see the following ESET resources:

- Troubleshooting - Agent deployment
- Troubleshooting - Agent connection
- Example scenarios of ERA Agent deployment

#### 4.5.1 Add client computer to ERA structure

Before you can start managing client computers in your network, you need to add them to ESET Remote Administrator. Use one of the methods below to add them:

- Active Directory synchronization
- Using RD Sensor component
- Manually add new devices
- Install ERA Agent locally
4.5.1.1 Using Active Directory synchronization

AD synchronization is performed by running the Static Group Synchronization server task. It is a pre-defined default task that you can choose to execute automatically during ESET Remote Administrator installation. If the computer is in a domain, synchronization will be performed and computers from the AD will be listed in the default group All.

To start the synchronization process, click the task and choose Run now. If you need to create a new AD synchronization task, select a group to which you want to add new computers from the AD. Also select objects in the AD you want to synchronize from and what to do with duplicates. Enter your AD server connection settings and set the Synchronization mode to Active Directory/Open Directory/LDAP. Follow step-by-step instructions in this ESET Knowledgebase article.
4.5.1.2 Using RD Sensor

If you are not using AD synchronization, the easiest way to add a computer into the ERA structure is to use RD Sensor. The RD Sensor component is part of the installation bundle. You can easily drill down the report Rogue computers ratio, chart at the bottom of the Computers dashboard to view the rogue computers by clicking the red part of the graph.
The **Rogue computers** report on the Dashboard now lists computers found by the RD Sensor. Computers can be added by clicking the computer you want to **Add**, or you can **Add all displayed items**.

If you are adding a single computer, you can use a preset name or specify your own (this is a display name that will be used in ERA Web Console only, not an actual host name). You can also add a description if you want to. If this computer already exists in your ERA directory, you will be notified and can decide what to do with the duplicate. The available options are: **Deploy Agent**, **Skip**, **Retry**, **Move**, **Duplicate** or **Cancel**. Once the computer is added, a pop-up window will open with an option to **Deploy Agent**.
If you click **Add all displayed items** a list of computers to be added will be displayed. Click 🗄 next to the name of a specific computer if you do not want to include it in your ERA directory at this time. When you are finished removing computers from the list, click **Add**. After clicking **Add**, select the action to take when a duplicate is found (allow for a slight delay depending on the number of computers in your list): **Skip, Retry, Move, Duplicate** or **Cancel**. Once you have selected an option, a pop-up window listing all added computers will open with an option to **Deploy Agents** on those computers.

![Add Devices](image)

The results of the RD Sensor scan are written to a log file called **detectedMachines.log**. It contains a list of discovered computers on your network. You can find the **detectedMachines.log** file here:

- **Windows**
  
  C:\ProgramData\ESET\Rouge Detection Sensor\Logs\detectedMachines.log

- **Linux**
  
  /var/log/eset/RogueDetectionSensor/detectedMachines.log

### 4.5.1.3 Add Computers

This feature allows you to manually add **Computers** or **Mobile devices** that are not found or added automatically. The **Computers** or **Group** tab allows you to add new computers or mobile devices.

1. To add a new computer, click **Computers, Add New** and then select **Computers** (alternatively click the gear icon 🛠 next to existing **Static group** and then click **Add New**).

2. Use the **Conflict Resolution** drop-down menu to select the action to take if a computer you are adding already exists in ERA:
   - **Ask when conflicts are detected**: When a conflict is detected, the program will ask you to select an action (see the options below).
   - **Skip conflicting computers**: Duplicate computers will not be added.
   - **Move conflicting computers from other groups**: Conflicting computers will be moved from their original groups to the **All** group.
   - **Duplicate conflicting computers**: New computers will be added, but with different names.

3. **Parent group** - select an existing Parent group and then click **OK**.

4. Type the **IP address** or **host name** of a machine you want to add and ESET Remote Administrator will search for it on the network. Optionally, you can enter a **Description** of the computers.
4. Click + Add Device to add additional computers. If you want to delete a computer from the list of devices, click the Trashcan icon or click Remove All.

5. Alternatively, click Import CSV to upload a .csv file containing a list of computers to add. For more information, see Import CSV upload.

6. Click Add when you are finished making changes.

**NOTE**
Adding multiple computers may take a longer time (reverse DNS lookup may be preformed).

Once you click Add a pop-up window will open with a list of devices to be added. You can click OK or Deploy Agent.

7. If you've clicked Deploy Agent, choose the deployment type you want to perform:
Deploy Agent

Choose the deployment method appropriate for your network:

**LOCAL DEPLOYMENT**

Create all-in-one installer (Windows only)
Download a preconfigured package which contains ERA Agent and ESET product.
CREATE INSTALLER  SELECT EXISTING

Create Agent Live Installer
Download a preconfigured Agent Live Installer and distribute it via email or removable media (USB, CD or other). Learn more...
CREATE INSTALLER  SELECT EXISTING

Download Agent from ESET website
Download the ERA Agent installer from ESET website, run and configure it on a client machine.
OPEN WEBSITE

**REMOTE DEPLOYMENT**

Use GPO or SCCM for deployment
Generate configuration file for GPO and SCCM deployment. Learn more...
CREATE SCRIPT  SELECT EXISTING

Server Task Agent installation
Create a server task to "push" agent installation on the supported OS. Learn more...
CREATE TASK  SELECT TASK

Use the standalone Deployment Tool
Download the Deployment Tool and run it on any device in your network. It will find other devices in the network, synchronize with the Active Directory or use imported list. When you choose your targets list, you can remotely deploy the created all-in-one installers to your network. Learn more...
OPEN WEBSITE

CLOSE
4.5.2 Agent deployment process

ERA Agent deployment can be performed in a few different ways. You can deploy the Agent locally or remotely:

- **Local deployment** - using an all-in-one installation package (ERA Agent and ESET security product), Agent Live Installers or by downloading the ERA Agent from ESET.
- **Remote deployment** - we recommend that you use this method to deploy ERA Agent on large number of client computers.

### Deploy Agent

Choose the deployment method appropriate for your network:

#### LOCAL DEPLOYMENT

- **Create all-in-one installer (Windows only)**
  Download a preconfigured package which contains ERA Agent and ESET product.

  - [CREATE INSTALLER](#)
  - [SELECT EXISTING](#)

- **Create Agent Live Installer**
  Download a preconfigured Agent Live Installer and distribute it via email or removable media (USB, CD or other).

  - [CREATE INSTALLER](#)
  - [SELECT EXISTING](#)

- **Download Agent from ESET website**
  Download the ERA Agent installer from ESET website, run and configure it on a client machine.

  - [OPEN WEBSITE](#)

#### REMOTE DEPLOYMENT

- **Use GPO or SCCM for deployment**
  Generate configuration file for GPO and SCCM deployment.

  - [CREATE SCRIPT](#)
  - [SELECT EXISTING](#)

- **Server Task Agent installation**
  Create a server task to "push" agent installation on the supported OS.

  - [CREATE TASK](#)
  - [SELECT TASK](#)

- **Use the standalone Deployment Tool**
  Download the Deployment Tool and run it on any device in your network. It will find other devices in the network, synchronize with the Active Directory or use imported list. When you choose your targets list, you can remotely deploy the created all-in-one installers to your network.

  - [OPEN WEBSITE](#)

### 4.5.2.1 Local deployment

This deployment method is intended for on-premise installations. Create or download an installation package and allow access to it via shared folder or distribute the package using a USB drive (alternatively, email). The installer package must be installed by an Administrator or a user with Administrator privileges.

- **NOTE**
  We recommend that you only use local deployment if you have a small network (up to 50 computers). For larger networks, you can [Deploy ERA Agent using GPO or SCCM](#).

Local deployment can be performed in three ways:

- **Create an all-in-one Agent installer (Windows only)**
- **Create Agent Live Installer**
Local Deployment and permission

For more information on how to allow a user to deploy ERA Agent locally, follow the instructions in this [example](https://example.com).

**NOTE**
Keep in mind that the user will be able to work with Certificates when creating installers. A user must have **Use** permission for Certificates with access to the static group where certificates are contained. If a user wants to deploy ERA Agent, it is necessary to be assigned **Use** permission for Certification Authority that the actual server certificate is signed. For information on how to divide access to Certificates and Certification Authority, read this [example](https://example.com). See the list of permissions for more information on access rights.

### 4.5.2.1.1 Create an all-in-one Agent installer

The procedure of creating an all-in-one installer (including ERA Agent and an ESET product) package is similar to [Startup Wizard](https://example.com); however the all-in-one installer allows for advanced configuration options. These options include Policy settings for ERA Agent and ESET products, ERA Server **Hostname** and **Port**, and the ability to select a **Parent** Group.

**IMPORTANT**
The installer package comes in the form of an `.exe` file and is valid for Microsoft Windows operating systems only.

Click **Deploy ERA Agent** in the **Quick Links** section of the menu bar. In the **Deploy Agent** window, click **Create installer** under **Create all-in-one Installer (Windows only)**. The **Create all-in-one installer** window will open.

**Package creation**

- **Product** - Expand this section to choose an installation file from the list of available ESET products. If you choose version 6.3 or earlier, automatic product activation will not work—you’ll have to activate the product later. ESET products version 6.4 or later will be automatically activated during the installation.

If you agree with End User License Agreement, select the checkbox next the **I agree with application End User License Agreement**.

**NOTE**
If you do not see any product installation files, make sure you have the repository set to **AUTOSELECT**. For more information, see the **Advanced settings** section of **Server settings**.

1. **Language** - Select a supported language for the installer from the drop-down menu.
2. **License (Optional)** - You can use this option to add a license using one of the methods described in the **Licenses** section. If you already have existing licenses in **License Management**, simply choose the license that will be used to activate your ESET product during installation. If you do not choose a license, you can create an installer without it and **activate the product later**.

- **Certificate** - A Peer Certificate and ERA Certification Authority are chosen automatically based on the available certificates. If you want to use a different certificate than the one automatically selected, click **ERA Certificate** to see a list of available certificates and then select the one you want to use. If you want to use your own **Custom certificate**, click the radio button and upload a `.pfx` certificate file. See [Custom certificates with ERA](https://example.com) for further instructions.

Enter your **Certificate passphrase** if needed. Do so if, for example, you’ve specified the passphrase during the installation of ERA, or if you are using a Custom certificate with a passphrase. Otherwise, leave the **Certificate passphrase** field blank.

**IMPORTANT**
Be aware that it is possible to extract the **Certificate passphrase** because it is embedded in the `.exe` file.
Advanced - In this section, you can customize the all-in-one installer package:

3. Optionally, you can change the Name and enter Description for the package installer.

4. Parent group (optional) - Select the Parent group where the computer will be placed after the installation. If you want to create a new Parent Static group, click New Static group and use the wizard. The newly created group will automatically be selected.

5. ESET AV Remover will help you uninstall or completely remove other antivirus programs. Select the checkbox if you want to use it.

6. Initial installer configuration - Here, you can choose from the two configuration types:
   - Do not configure - Only the policies that are merged to a Parent Static group will be applied.
   - Select configuration from the list of policies - Use this option if you want to apply a configuration policy to ERA Agent and/or your ESET product. Click Select and choose from the list of available policies. If none of the predefined policies are suitable, you can create a new policy or customize your existing policy first. When you try selecting the policy again, your new policy will appear in the list.

7. If necessary, you can specify your ERA Server Hostname and Port number. Otherwise, leave the default values unchanged.

8. Click Create Package. All-in-one installation package files will be generated for 32-bit and 64-bit operating systems. Click Select and choose from the list of available policies. If none of the predefined policies are suitable, you can create a new policy or customize your existing policy first. When you try selecting the policy again, your new policy will appear in the list.


4.5.2.1.2 Create Agent Live Installer

This type of Agent deployment is useful when the remote and local deployment options do not suit you. In such cases, you can distribute the Agent Live Installer via email and let the user deploy it. You can also run the Agent Live Installer from removable media (a USB flash drive, for example).

NOTE
The client machine needs to have an internet connection to download the Agent installation package. Also, the client needs to be able to connect to the ERA Server.

Click Deploy ERA Agent in the Quick Links section of the menu bar. In the Deploy Agent window, click Create installer button under Create Agent Live Installer. The Agent Live installers window will open.

Package creation

Certificate - A Peer Certificate and ERA Certification Authority is chosen automatically based on the available certificates. If you want to use a different certificate than the one automatically selected, click the ERA Certificate description to select from a list of available certificates. If you want to use a Custom certificate, click the radio button and upload a .pfx certificate file. See Custom certificates with ERA for further details.

Enter a Certificate passphrase if needed. For example, if you’ve specified the passphrase during the installation of ERA, or if you are using a custom certificate with a passphrase. Otherwise, leave the Certificate passphrase field blank.

Configuration - In this section, you can customize the following settings for the Agent Live installer package:

1. Optionally, you can change the Name and enter Description for your package installer.

2. Server hostname - If necessary, you can specify the ERA Server Hostname and Port number. Otherwise, leave default values unchanged.
3. **Parent group (optional)**- Select the **Parent group** where the computer will be placed after the installation. If you want to create a new Parent Static group, click **New Static group** and use the wizard. The newly created group will automatically be selected.

4. Click **Get Installers** to generate links for Windows, Linux and MAC Agent installer files.

<table>
<thead>
<tr>
<th>PACKAGES TO DOWNLOAD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AGENT INSTALLER FOR WINDOWS</strong></td>
</tr>
<tr>
<td><strong>AGENT INSTALLER FOR LINUX</strong></td>
</tr>
<tr>
<td><strong>AGENT INSTALLER FOR MAC</strong></td>
</tr>
</tbody>
</table>

5. Click **Download** next to the installer file(s) that you want to download and save the **zip** file. Unzip the file on the client computer where you want to deploy ERA Agent and run **EraAgentOnlineInstaller.bat** (Windows) or **EraAgentOnlineInstaller.sh** script (Linux and MacOS) to run the installer. For instructions on how to deploy the ERA Agent on a client using the Agent Live Installer, see our **KB article**.

**NOTE**
If you are running the script on Windows XP SP2, you need to install **Microsoft Windows Server 2003 Administration Tools Pack**. Otherwise, the Agent Live Installer won't run properly. Once you have installed the Administration Pack, you can run the Agent Live Installer script.

**NOTE**
Check the status log on the client machine `C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html` to make sure ERA Agent is working properly. If there are problems with the Agent (for example, it is not connecting to the ERA Server), see **troubleshooting**.

To deploy the ERA Agent using Agent Live Installer from your local shared folder without the ESET Repository Download Server, follow these steps:

1. Edit the **EraAgentOnlineInstaller.bat** file (Windows) or **EraAgentOnlineInstaller.sh** script (Linux and Mac).

   Change lines 30 and 33 to point to the correct local download files. For example:

   ```
   30 set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.4.283.0/Agent_x64.msi
   31 set checksum=67e2c3c29633548daed2a8f6c59045d11d538b42
   32 if defined IsArch_x86 
   33 set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.4.283.0/Agent_x86.msi
   34 set checksum=0f80b4e5dc22ae4192601c335b6b6a76a79f5255
   ``

2. Use your own URL (local shared folder), instead of the one shown below:

   ```
   30 set url=\server\share\Agent_x64.msi
   31 set checksum=67e2c3c29633548daed2a8f6c59045d11d538b42
   32 if defined IsArch_x86 
   33 set url=\server\share\Agent_x86.msi
   34 set checksum=0f80b4e5dc22ae4192601c335b6b6a76a79f5255
   ``

**IMPORTANT**
Make sure that the user account under which the installation package is executed has write permission to the local shared folder. The path can contain spaces, for example `\server\shared folder\Agent_x64.msi` (do not use quotation marks `"`).

4. Edit line 76 to replace `

   `echo.packageLocation = DownloadUsingHTTPProxy("!url!", "!http_proxy_hostname!", "!http_proxy_port!", "!http_proxy_username!", "!http_proxy_password!")``

`with your actual URL and credentials if needed.
5. Save the file.

4.5.2.1.3 Download Agent from ESET website

Download the ERA Agent installation package from the ESET website. Select the appropriate package depending on the client computer’s OS:

- **Windows**
- **Linux**
- **macOS**

**Server assisted installation** - using the Agent installation package, this method downloads certificates from the ERA Server automatically (recommended for local deployment).

**NOTE**

If you decide to allow Server assisted installation by another user, make sure the following permissions are set:

- The user must have **Use** permission for the Certification Authority that signed the server’s peer certificate and **Use** permission for at least one peer certificate. If no such certificate exists, the user will need **Write** permission to create a new one.
- **Write** permission for the static group where the user wants to add the computer.

**Offline installation** - using the Agent installation package. You must manually export certificates and apply them in this deployment method.

If you encounter issues with the ERA Agent during installation, check the **status log** on the client machine to make sure ERA Agent is working properly. If there are problems with the Agent (for example, it is not connecting to the ERA Server), see **Troubleshooting - Agent deployment**.
4.5.2.1.3.1 Deploy Agent locally

To deploy the ERA Agent locally on a client computer using the installation wizard, follow the steps below:

**Server assisted installation:**

1. Make sure **Server assisted installation** is selected, specify your **Server host** (name or IP address) and the **Server port** of your ERA Server and then click **Next**. The default Server port is 2222, if you are using a different port, replace the default port with your custom port number.

2. Specify the method used for connection to Remote Administrator Server (ERA Server or ERA Proxy Server) in the **Server host** and **Web Console port** fields. Type your ERA Web Console login credentials into the **Username** and **Password** fields.
3. Select **Choose custom Static Group**, select the appropriate option for the client computer from the **Static Group** drop-down menu and then click **Next**.

![ESET Remote Administrator Agent Setup](image)

**Add computer to static group**

Please specify static group where computer will be added.

- Do not create computer (computer will be created automatically during the first connection)
- Choose custom static group

**Static group:**

- /All
- /All/Lost & found
- /All/San Diego
- /All/Singapore
- /All/Sydney
- /All/Tokyo

4. Choose destination folder and then click **Next**.

5. Click **Install** to begin the installation.

**Offline installation:**

1. To perform an **Offline installation**, enter **2222** into the **Server port** field, select **Offline installation** and then click **Next**.

![ESET Remote Administrator Agent Setup](image)

**Agent configuration**

Please enter agent configuration below.

**Network connection to ESET Remote Administrator**

- **Server host:** eraserver
- **Server port:** 2222

- Server assisted installation
- Offline installation
2. For this method, you must specify a Peer certificate and Certification Authority. For more information about how to export and use a Peer certificate and Certification Authority click here.

![Peer certificate setup](image)

NOTE
Check the status log on a client machine (located at C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html or C:\Documents and Settings\All Users\Application Data\Eset\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html) to verify ERA Agent is working properly. If there are problems with the Agent (for example, it is not connecting to the ERA Server), see section Troubleshooting - Agent deployment.

4.5.2.2 Remote deployment
Remote deployment can be performed in two ways:

- **Group Policy Object (GPO) and Software Center Configuration Manager (SCCM)** - we recommend this method for mass deployment of the ERA Agent on client computers.
- **Server task Agent deployment** - an alternative to GPO and SCCM.
- **Deployment tool** - this tool allows you to deploy All-in-one packages created in the ERA Web Console.

IMPORTANT
For remote deployments, verify all client computers have an internet connection.

Remote deployment and permissions
If you want to allow user to create GPO installers or SCCM scripts, set their permissions to match our example. The following permissions are necessary for Server task Agent deployment:

- **Write** permission for Groups & Computers where the deployment is executed
- **Use** permission for Certificates with access to static group where certificates are contained
- **Use** permission for Agent deployment in Server Tasks & Triggers section
4.5.2.2.1 Agent deployment using GPO and SCCM

Apart from local deployment or remote deployment using a Server task, you can also use management tools such as Group Policy Object (GPO), Software Center Configuration Manager (SCCM), Symantec Altiris or Puppet.

Click the appropriate link below to view step-by-step instructions for two popular ERA Agent deployment methods:

1. Deployment of ERA Agent using Group Policy Object (GPO)
2. Deployment of ERA Agent using Software Center Configuration Manager (SCCM)

4.5.2.2.1.1 Deployment steps - GPO

Follow the steps below to deploy the ERA Agent to clients using GPO:

Download the ERA Agent installer .msi file from ESET download page.

Click Deploy ERA Agent... in the Quick Links section of the menu bar, pop-up window will open where you can choose Use GPO or SCCM for deployment, click button Create Script configuration will be open.

Certificate - A Peer Certificate and ERA Certification Authority are chosen automatically based on the available certificates. If you want to use a different certificate than the one automatically selected, click ERA Certificate description to see a list of available certificates and choose the one you want to use. If you want to use your Custom certificate click the radio button and upload a .pfx certificate file. See Custom certificates with ERA for further details.

Enter Certificate passphrase if needed. For example if you've specified the passphrase during the installation of your ERA, or if you are using Custom certificate with a passphrase. Otherwise, leave the Certificate passphrase field blank.

Configuration - Lets you customize the all-in-one installer package:

1. Initial installer configuration - you can choose from the two configuration types:
   o Do not configure - only the policies that are merged to a Parent Static group will be applied.
   o Select configuration from the list of policies - use this option if you want to apply configuration policy to ERA Agent. Click Select and choose from the list of available policies. If none of the predefined policies are suitable, you can create new policy or customize existing first. When you try selecting the policy again, your new policy will appear in the list.

2. Other - if necessary, you can specify ERA Server Hostname and Port number. Otherwise, leave default values unchanged.

3. Parent group (optional) - you can either select existing Static group or create new one. Click Select to choose Parent Static group for the client machine on which you'll use the all-in-one installer package. If you want to create new Parent Static group, click New Static group button and use the wizard. Newly created group will automatically be selected.

4. Select Create Package and when a new popup window with install_config.ini file opens, click Save file.

5. Put the ERA Agent installer .msi file and created install_config.ini file in a shared folder that can be accessed by your target client(s).
IMPORTANT
Client computers will require read/execute access to this shared folder.
6. Use an existing Group Policy Object or create a new one (right-click GPO and click **New**). In the GPMC (Group Policy Management Console) tree, right-click the GPO you want to use and select **Edit**...

7. In **Computer Configuration**, navigate to **Policies > Software Settings**.

8. Right-click **Software installation**, select **New**, and click **Package**... to create a new package configuration.
9. Browse to the location of the ERA Agent .msi file. In the Open dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want to use. For example `\fileserver\share\filename.msi`

**NOTE**

Make sure that you use the UNC path of the shared installer package.

10. Click Open and choose the **Advanced** deployment method.
11. Confirm the package configuration and proceed with GPO deployment.
4.5.2.2.1.2 Deployment steps - SCCM

Follow the steps below to deploy the ERA Agent to clients using SCCM:

**Download** the ERA Agent installer `.msi` file from [ESET download page](#).

Click **Deploy ERA Agent...** in the **Quick Links** section of the menu bar, pop-up window will open where you can choose **Use GPO or SCCM for deployment**, click button **Create Script** configuration will be open.

**Certificate** - A Peer Certificate and ERA Certification Authority are chosen automatically based on the available certificates. If you want to use a different certificate than the one automatically selected, click **ERA Certificate** description to see a list of available certificates and choose the one you want to use. If you want to use your **Custom certificate** click the radio button and upload a `.pfx` certificate file. See [Custom certificates with ERA](#) for further details.

Enter **Certificate passphrase** if needed. For example if you've specified the passphrase during the installation of your ERA, or if you are using Custom certificate with a passphrase. Otherwise, leave the **Certificate passphrase** field blank.

**Configuration** - Lets you customize the all-in-one installer package:

1. **Initial installer configuration** - you can choose from the two configuration types:
   - Do not configure - only the policies that are merged to a Parent Static group will be applied.
   - Select configuration from the list of policies - use this option if you want to apply configuration policy to ERA Agent. Click **Select** and choose from the list of available policies. If none of the predefined policies are suitable, you can create **new policy** or customize existing first. When you try selecting the policy again, your new policy will appear in the list.

2. **Other** - if necessary, you can specify ERA **Server Hostname** and **Port** number. Otherwise, leave default values unchanged.

3. **Parent group (optional)** - you can either select existing Static group or create new one. Click **Select** to choose Parent Static group for the client machine on which you'll use the all-in-one installer package. If you want to create new Parent Static group, click **New Static group** button and use the wizard. Newly created group will be automatically selected.

4. Select **Create Package** and when a new popup window with `install_config.ini` file opens, click **Save file**.

5. Put the ERA Agent installer `.msi` files and `install_config.ini` file on a shared folder.
**IMPORTANT**

Client computers will require read/execute access to this shared folder.
1. Open SCCM console and click **Software Library**. In **Application Management** right-click **Applications** and choose **Create Application**. Choose **Windows Installer (*.msi file)**.
2. Specify all required information about the application and click **Next**.
3. Right-click the ESET Remote Administrator Agent Application, click the **Deployment Types** tab, select the only deployment there and then click **Edit**.
4. Click the **Requirements** tab and then click **Add**. Select **Operating system** from the **Condition** drop-down menu, select **One of** from the **Operator** drop-down menu and then specify the operating systems you will install to by selecting the appropriate check box(es). Click **OK** when you are finished and then click **OK** to close any remaining windows and save your changes.
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install this deployment type. Configuration Manager verifies that these requirements are met before content is deployed to the device.

Requirements:

<table>
<thead>
<tr>
<th>Requirement Type</th>
<th>Operator</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>One of</td>
<td>{All Windows 7 (64-bit)}</td>
</tr>
</tbody>
</table>
5. In the System Center Software Library, right-click your new application and select **Distribute Content** from the context menu. Follow the prompts in the Deploy Software Wizard to complete deployment of the application.
You have selected the following content for distribution:

Content: ESET Remote Administrator Agent (64-bit)

Some content might have associated dependencies that must be installed before the content can be installed.

- Detect associated content dependencies and add them to this distribution
6. Right-click the application and choose **Deploy**. Follow the wizard and choose the collection and destination where you want to deploy the agent.
Select distribution points that will host this content.

Software Update Packages are never distributed to Cloud Distribution Points.

Available distribution points:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>On-premises</td>
<td></td>
</tr>
</tbody>
</table>

Specify the content destination

Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collectors.

Content destination:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Associations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Distribution point</td>
</tr>
</tbody>
</table>

< Previous  Next >  Summary  Cancel
The Distribute Content Wizard completed successfully

Details:

- Content (1):
  - ESET Remote Administrator Agent (64-bit)
- Dependencies (1):
  - ESET Remote Administrator Agent (64-bit)
- Collections (0):
- Distribution point groups (0):
- Distribution points (1):

To exit the wizard, click Close.
Specify general information for this deployment

Software: ESET Remote Administrator Agent (64-bit)
Collection: Applications - Workstations BTS - ESET Remote Administration

- Use default distribution point groups associated to this collection
- Automatically distribute content for dependencies

Comments (optional):

< Previous  Next >  Summary  Cancel
Specify settings to control how this software is deployed

Action: Install
Purpose: Required

- Pre-deploy software to the user’s primary device
- Send wake-up packets
- Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
Specify the schedule for this deployment

This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. The deadline is when the application must be installed on the device, including a system restart if necessary.

Time based on: UTC

Schedule the application to be available at:

- 9.2.2015 12:32

Installation deadline:
- As soon as possible after the available time
- Schedule at:

- 9.2.2015 12:32
Specify the user experience for the installation of this software on the selected devices

Specify user experience setting for this deployment:

User notifications: Display in Software Center and show all notifications

When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:

- [ ] Software installation
- [ ] System restart (if required to complete the installation)

Write filter handling for Windows Embedded devices

- [x] Commit changes at deadline or during a maintenance window (requires restart)

If this option is not selected, content will be applied on the overlay and committed later.
4.5.2.2 Deployment tool

The deployment tool is a convenient way to distribute the ERA Agent together with an ESET product on computers over a network. The tool enables you to use custom created installers. It is available for free on the ESET website as a standalone ERA Component. The deployment tool is meant mainly for deployment on small to medium networks. It is available for Windows systems only.

For more details on prerequisites and usage of the tool see the Deployment tool chapter in the install guide.
4.5.2.3 ERA Agent settings

Configure specific settings for ERA Agent using a policy. There are predefined policies for the ERA Agent. For example, **Connection** - Connect every (Agent connection interval) or **Application reporting** - Report all installed applications (not only ESET applications). For more information on how to enforce location-based policy, read the example.

Click **Policies** and expand **Built-in Policies > ESET Remote Administrator Agent** to edit an existing policy or create a new one.

### Connection

- **Servers to connect to** - To add ERA Server connection details (hostname/IP and a port number), click Edit server list. Multiple ERA Servers can be specified. This can be useful if, for example, you've [changed the IP address of your ERA Server](#) or are doing a migration.
- **Data limit** - Choose the maximum number of bytes for sending data.
- **Connection interval** - Choose Regular interval and specify a time value for the connection interval (or you can use a [CRON expression](#)).
- **Certificate (requires restart!)** - You can manage Peer certificates for ERA Agent. Click **Change certificate** and select which ERA Agent certificate should be used by ERA Agent. For more information, see [Peer Certificates](#).

### Updates

- **Update interval** - Interval at which updates will be received. Select a Regular interval and configure the settings (or you can use a [CRON expression](#)).
- **Update server** - Update server from which the ERA Server receives updates for ESET products and ERA components.
- **Update type** - Select the type of updates you want to receive. Choose either Regular, Pre-release or Delayed update. We do not recommend that you select Pre-release updates for production systems, as this is a risk.

### Advanced Settings

- **HTTP Proxy** - Use a proxy server to facilitate internet traffic to clients on your network.
- **WakeUp** - ERA Server can run instant replication of the ERA Agent on a client machine. UDPv4 and UDPv6 ports are used with default port numbers 1237 and 1238. This is useful when you do not want to wait for the regular interval when the ERA Agent connects to the ERA Server. For example when you want a [Client Task](#) to be run immediately on client(s) or if you want a [Policy](#) to be applied right away.
- **Compatibility** - In order to allow for management of ESET products version 5 or earlier by ESET Remote Administrator Agent, a specific listening port must be set. Also, ESET products need to be configured to report to this port and ESET Remote Administrator Server address must be set to `localhost`.
- **Operating System** - Use the switches (enabled by default) to Report certain information or issues on the client computer.
- **Repository** - Location of the repository where all installation files are stored.

**NOTE**
The default repository is **AUTOSELECT**.

- **Diagnostics** - Enable or disable transmission of crash reports to ESET.
- **Logging** - Set the log verbosity to determine the level of information that will be collected and logged, from [Trace](#) (informational) to [Fatal](#) (most important critical information). The latest ERA Agent log file can be found on a client computer here: `C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs` or `C:\Documents and Settings\All Users\Application Data\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs`
- **Setup** - [Password protected setup](#) is a protection feature of ERA Agent (Windows only). [Set password](#) to enable ERA Agent Password protection. Once the policy is applied, ERA Agent cannot be uninstalled or repaired unless a password is provided.
IMPORTANT

If you forget this password, you will not be able to uninstall ERA Agent from the target machine.

Specify the clients that will receive this policy. Click Assign to display all Static and Dynamic Groups and their members. Select the computer that you want to apply a policy on and click OK.

Review the settings for this policy and click Finish.

4.5.2.3.1 Create a Policy for ERA Agent connection interval

In this example, we are going to create a new policy for the ERA Agent connection interval. We highly recommend doing this prior to testing mass deployment in your environment.

Create a New Static Group. Add a new policy by clicking Admin > Policies. Click Policies at the bottom and select New...
Basic

Enter a **Name** for the new policy (for example, "Agent Connection Interval"). The **Description** field is optional.

**Settings**

Select **ESET Remote Administrator Agent** from the **Product** drop-down menu.

**Connection**

Select a category in the tree on the left. In the right pane, edit settings as required. Each setting is a rule for which you can set a **flag**. Click **Change interval**.
In the **Regular interval** field, change the value to your preferred interval time (we recommend 60 seconds) and click **Save**.

**Interval**

- **Interval between connections**
  - Regular interval
  - CRON expression

- **Regular interval**
  
  - **Minutes**
  - CRON expression

- **Assign**

Specify the clients (individual computers/mobile devices or whole groups) that are the recipients of this policy.
Click **Assign** to display all Static and Dynamic Groups and their members. Select your desired clients and click **OK**.

### Select targets

<table>
<thead>
<tr>
<th>Groups</th>
<th>Computer Name</th>
<th>Status</th>
<th>Muted</th>
<th>Modules</th>
<th>Last Connected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last &amp; found (D)</td>
<td>computer.7CBAF8F5A1_</td>
<td>✔️</td>
<td></td>
<td></td>
<td>2016 Dec 14 02:46:46</td>
</tr>
<tr>
<td>Windows computers</td>
<td>era-latest-master</td>
<td>✔️</td>
<td></td>
<td>Unknown</td>
<td>2016 Dec 14 14:13:59</td>
</tr>
<tr>
<td>Linux computers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mac computers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computers with outdated modules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computers with outdated operating systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problematic computers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not activated security product</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Summary**
4.5.2.3.2 Create a Policy for ERA Agent to connect to the new ERA Server

This policy lets you change the behavior of ERA Agent by modifying its settings. The following is especially useful when migrating client machines to a new ERA Server.

Create new policy to set new ERA Server IP address and assign the policy to all client computers. Select Admin > Policies > create New.

**Basic**

Enter a Name for your policy. The Description field is optional.

**Settings**

Select ESET Remote Administrator Agent from the drop-down menu, expand Connection and click Edit server list next to Servers to connect to.
A window will open with a list of ERA Servers the ERA Agent can connect to. Click **Add** and type the IP address of your new ERA Server into the **Host** field. If you are using a different port than the default ERA Server port 2222, specify your custom port number.

Use the arrow buttons to change the priority of ERA Servers in case you have multiple entries in the list. Make sure your new ERA Server is at the top by clicking **double-up arrow** button and then click **Save**.

**Assign**

Specify the clients (individual computers/mobile devices or whole groups) that are the recipients of this policy.
Click **Assign** to display all Static and Dynamic Groups and their members. Select your desired clients and click **OK**.
Review the settings for this policy and click Finish.

4.5.2.3.3 Create a Policy to enable ERA Agent Password protection

Follow the steps below to create a new policy that will enforce a password to protect the ERA Agent. When Password protected setup is used, ERA Agent cannot be uninstalled or repaired unless a password is provided. See Agent protection for more details.

Basic

Enter a Name for this policy. The Description field is optional.

Settings

Select ESET Remote Administrator Agent from the drop-down list, expand Advanced settings, navigate to Setup and type the password into the Password protected setup field. This password will be required if someone is trying to uninstall or repair ERA Agent on a client computer.

IMPORTANT

Make sure to record this password in a safe place, it is essential to enter the password to allow ERA Agent uninstallation from the client computer. There is no other regular way of uninstalling ERA Agent without a correct password once Password protected setup policy is in place.

Assign

Specify the clients (individual computers/mobile devices or whole groups) that are the recipients of this policy.

Click Assign to display all Static and Dynamic Groups and their members. Select your desired clients and click OK.
Summary

Review the settings for this policy and click Finish.

4.5.2.4 Agent protection

The ERA Agent is protected by a built-in self-defense mechanism. This feature provides the following:

- Protection against modification of ERA Agent registry entries (HIPS)
- Files that belong to ERA Agent cannot be modified, replaced, deleted or altered (HIPS)
- ERA Agent process cannot be killed
- The ERA Agent Service cannot be stopped, paused, disabled, uninstalled or otherwise compromised

Some of the protection is covered by the HIPS feature included in your ESET product.

NOTE
To ensure full protection of the ERA Agent, HIPS must be enabled on a client computer.

Password-protected setup

In addition to self-defense, you can password-protect access to the ERA Agent (available for Windows only). When password-protection is configured, the ERA Agent cannot be uninstalled or repaired unless the correct password is provided. To set an ERA Agent password, you need to create the appropriate policy for ERA Agent.
4.5.3 Troubleshooting - Agent connection

When a client computer does not appear to be connecting to your ERA Server, we recommend that you perform ERA Agent troubleshooting locally on the client machine.

By default, the ERA Agent synchronizes with ERA Server every 20 minutes. You can change this setting by creating a new policy for the ERA Agent Connection Interval.

Check the latest ERA Agent log file. It can be found here:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Log File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs</td>
</tr>
<tr>
<td></td>
<td>C:\Documents and Settings\All Users\Application Data\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs</td>
</tr>
<tr>
<td>Linux</td>
<td>/var/log/eset/RemoteAdministrator/Agent/</td>
</tr>
<tr>
<td></td>
<td>/var/log/eset/RemoteAdministrator/EraAgentInstaller.log</td>
</tr>
<tr>
<td>OS X</td>
<td>/Library/Application Support/com.eset.remoteadministrator.agent/Logs/</td>
</tr>
<tr>
<td></td>
<td>/Users/%user%/Library/Logs/EraAgentInstaller.log</td>
</tr>
</tbody>
</table>

**NOTE**

To enable full logging, create a dummy file named traceAll without an extension in the same folder as a trace.log and then restart the ESET Remote Administrator Server service. This will enable full logging in the trace.log file.

- **last-error.html** – protocol (table) that displays the last error recorded while the ERA Agent is running.
- **software-install.log** – text protocol of the last remote installation task performed by the ERA Agent.
- **status.html** – a table showing the current state of communications (synchronization) of ERA Agent with ERA Server.
- **trace.log** – a detailed report of all ERA Agent activity including any errors that have been recorded.

The most common issues that can prevent the ERA Agent from connecting to the ERA Server are:

- Your Internal network is not configured properly. Make sure that the computer where ERA Server is installed can communicate with client computers where ERA Agent is installed.
- Your ERA server is not configured to listen on port 2222.
- DNS is not working properly, or ports are blocked by a firewall - check our list of ports used by ESET Remote Administrator, or see our KB article What addresses and ports on my third-party firewall should I open to allow full functionality for my ESET product?.
- An erroneously generated certificate containing false or limited features that do not match the public key of ERA Server Certification Authority is in place - create a new ERA Agent certificate to resolve this.

4.5.4 Troubleshooting - Agent deployment

You may encounter problems with ERA Agent deployment. If deployment fails, there are a number of things that might be the cause. This section will help you:

- Find out what caused ERA Agent deployment to fail
- Check for possible causes according to the table below
- Resolve the issue and perform a successful deployment

**Windows**

1. To find out why Agent deployment failed, navigate to Reports > Automation, select Agent Deployment task information in last 30 days and click Generate now.

A table will displayed deployment information. The Progress column displays error messages about why Agent deployment failed.

If you need even more details, you can change the verbosity of the ERA Server trace log. Navigate to Admin > Server Settings > Advanced Settings > Logging and select Error from the drop-down menu. Run the Agent deployment again and when it fails check the ERA Server trace log file for the latest log entries at the bottom of the file. The report will include suggestions about how to resolve the issue.
The latest file can be found here:

**ERA Server log**
C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\trace.log

**ERA Agent log**
C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs
C:\Documents and Settings\All Users\Application Data\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs

To enable full logging, create a dummy file named *traceAll* without an extension in the same folder as a trace.log. Restart the ESET Remote Administrator Server service, this will enable full logging into trace.log file.

**NOTE**
In case of ERA Agent connection problems, see Troubleshooting - Agent connection for more information.

**NOTE**
If the installation failed with error 1603, check *ra-agent-install.log* file. It can be found here: C:\Users\%user%\AppData\Local\Temp\ra-agent-install.log on the target computer.

2. The table below contains several reasons Agent deployment can fail:

<table>
<thead>
<tr>
<th>Error message</th>
<th>Possible cause(s)</th>
</tr>
</thead>
</table>
| **Could not connect**          | - Client is not reachable on the network, firewall blocks communication  
- Inbound ports 135, 137, 138, 139 and 445 are not open in firewall on the client or Windows Firewall: Allow inbound file and printer sharing exception is not used  
- Client's host name could not be resolved, use valid FQDN computer names |
| **Access denied**              | - When deploying from a server joined to a domain to a client joined to the domain, use credentials of an user that is member of Domain Admin group in format Domain\DomainAdmin  
- When deploying from a server joined to a domain to a client joined to the domain, you can temporarily elevate ERA Server service from network service to run under domain administrator account.  
- When deploying from a server to a client that are not in a same domain, **disable remote UAC filtering on target computer**.  
- When deploying from a server to a client that are not in a same domain, use credentials of a local user that is member of Administrators group in format Admin. Target computer name will be automatically prepended to the login.  
- No password set for administrator account  
- Insufficient access rights  
- ADMIN$ administrative share is not available  
- IPC$ administrative share is not available  
- Use simple file sharing is enabled |
| **Package not found in repository** | - Link to the repository is incorrect  
- Repository is unavailable  
- Repository does not contain required package |

3. Follow the appropriate troubleshooting steps according to the possible cause:

- **Client is not reachable on the network** - ping the client from the ERA Server, if you get a response, try to log on to the client machine remotely (for example, via remote desktop).

- **Firewall blocks communication** - check the firewall settings on both the server and the client, as well as any other firewall that exists between these two machines (if applicable).
• **Client’s host name could not be resolved** - possible solutions to DNS issues can include but are not limited to:
  - Using the `nslookup` command of the IP address and hostname of the server and/or the clients having Agent deployment issues. The results should match the information from the machine. For instance, an `nslookup` of a hostname should resolve to the IP address an `ipconfig` command shows on the host in question. The `nslookup` command will need to be run on the clients and the server.
  - Manually examining DNS records for duplicates.

• **Ports 2222 and 2223 are not open in firewall** - same as above, make sure that these ports are open on all firewalls between the two machines (client and server).

• **No password set for administrator account** - set a proper password for the administrator account (do not use a blank password)

• **Insufficient access rights** - try using the Domain Administrator's credentials when creating an Agent deployment task. If the client machine is in a Workgroup, use the local Administrator account on that particular machine.

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>After successful deployment, ports 2222 and 2223 are not open in firewall. Make sure that these ports are open on all firewalls between the two machines (client and server).</td>
</tr>
</tbody>
</table>

• **To activate** the Administrator user account:
  1. Open an administrative command prompt
  2. Enter the following command:
     ```
     net user administrator /active:yes
     ```

• **ADMIN$ administrative share is not available** - The client machine must have the shared resource ADMIN$ activated, make sure it is present among the other shares (Start > Control Panel > Administrative Tools > Computer Management > Shared Folders > Shares).

• **IPC$ administrative share is not available** - verify that the server can access IPC$ by issuing the following from a command prompt on the server:
  ```
  net use \clientname\IPC$ where clientname is the name of the target computer
  ```

• **Use simple file sharing is enabled** - if you are getting the Access denied error message and your environment is mixed (contains both a Domain and Workgroup), disable Use simple file sharing or Use Sharing Wizard on all machines that are having problems with Agent deployment. For example, in Windows 7 do the following:
  - Click Start, type folder into the Search box, and then click Folder Options. Click the View tab and in the Advanced settings box, scroll down the list and deselect the check box next to Use Sharing Wizard.

• **Link to the repository is incorrect** - In ERA Web Console, navigate to Admin > Server Settings, click Advanced settings > Repository and make sure the URL of the repository is correct.

• **Package not found in repository** - this error message usually appears when there is no connection to the ERA repository. Check your Internet connection.

**Linux and Mac OS**

If Agent deployment does not work on Linux or Mac OS, the issue is usually related to SSH. Check the client computer and make sure SSH daemon is running. Once fixed, run Agent deployment again.
4.5.5 Example scenarios of ERA Agent deployment

This section contains four verified scenarios for ERA deployment.

1. Deployment from ERA Server Appliance or Linux ERA Server to Windows targets not joined to a domain.
2. Deployment from Windows ERA Server from Windows source not joined to a domain to Windows targets not joined to the domain.
3. Deployment from ERA Server Appliance or Linux ERA Server to Windows targets joined to a domain.
4. Deployment from Windows ERA Server from Windows source joined to a domain to Windows targets joined to the domain.

4.5.5.1 Example scenarios of ERA Agent deployment to targets not joined to domain

1. Deployment from ERA Server Appliance or Linux ERA Server to Windows targets not joined to a domain.
2. Deployment from Windows ERA Server from Windows source not joined to a domain to Windows targets not joined to the domain.

Preconditions:

- Same local network.
- Working FQDN names, e.g.: desktop-win7.test.local maps to 192.168.1.20 and vice versa.
- Installed clean operating system from MSDN with defaults.

Targets:

Windows 10 Enterprise
Windows 8.1 Enterprise
Windows 7 Enterprise

1. Create a user with a password that is member of Administrators group, e.g.: "Admin". Open Microsoft Management Console by opening the Run console and typing the "mmc" into the field and clicking OK.
2. Add the Local Users and groups Snap-in from the File -> Add/Remove Snap-in. Add a new user into the Users folder and fill in the required information into the fields (do not forget to fill in the password). In the Groups section open the Properties of the Administrators group and add the new created user into the group by clicking on the Add... button. Fill in the login name of the new created user into the Enter the object names to select and verify it by clicking on the Check Names button.
3. In the Network and Sharing Center change the network setting from Public network to Private network by clicking on the Public network in the left side of the View your active networks section.
4. Disable Windows Firewall for Private Network by clicking on the Turn Windows Firewall on or off and selecting Turn off Windows Firewall in the Home or Work network location settings.
5. Check that File and printer sharing is enabled for Private network by clicking on the Change advanced sharing settings in the Network and Sharing center.
6. Open Registry editor by typing "regedit" into the Run console and locate HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
7. In the System file create a new DWORD Value with the name "LocalAccountTokenFilterPolicy", than open the created file and set the Value data to "1".
8. In the ESET Remote Administrator Web Console create "Agent Deployment" Server task assigned to FQDN name of the machine (you can find the FQDN name of the machine by right clicking in the Computer and selecting Properties. The FQDN name appears next to the Full computer name).
9. Set optional Server hostname to point to FQDN name or IP address of the ERA server.
10. Set username to just "Admin" (no domain name or computer name prefix) and his password.
11. Select Agent's certificate.
12. Execute the task.

For Windows XP Professional
1. Create a user with password that is member of Administrators group, e.g.: "Admin". Open Microsoft Management Console by opening the Run console and typing the "mmc" into the field and clicking OK.
2. Add the Local Users and groups Snap-in from the File -> Add/Remove Snap-in. Add a new user into the Users folder and fill in the required information into the fields (do not forget to fill in the password). In the Groups section open the Properties of the Administrators group and add the new created user into the group by clicking on the Add... button. Fill in the login name of the new created user into the Enter the object names to select and verify it by clicking on the Check Names button.
3. Disable Windows Firewall by selecting Off in the Windows Firewall -> General tab.
4. Check that File and printer sharing is enabled in Windows Firewall -> Exceptions tab.
5. Open the Run console and type in "secpol.msc" and press OK to open the Local Security Settings.
7. Set selected policy to Classic - local users authenticate as themselves.
8. In the ESET Remote Administrator Web Console create new "Agent Deployment" Server task assigned to FQDN name of the machine (you can find the FQDN name of the machine by right clicking in the Computer and selecting Properties. The FQDN name appears next to the Full computer name).
9. Set optional Server hostname to point to FQDN name or IP address of the ERA server.
10. Set username to just "Admin" (no domain name or computer name prefix) and his password.
11. Select Agent's certificate.
12. Execute the task.

4.5.5.2 Example scenarios of ERA Agent deployment to targets joined to domain
3. Deployment from ERA Server Appliance or Linux ERA Server to Windows targets joined to a domain.
4. Deployment from Windows ERA Server from Windows source joined to a domain to Windows targets joined to the domain.

Preconditions:

- Same local network.
- Working FQDN names, e.g.: desktop-win10.era.local maps to 10.0.0.2 and vice versa.
- Installed clean operating system from MSDN with defaults.
- Created domain "era.local" with netbios name "ERA".
- Created user "DomainAdmin" that is member of "Domain Admins" security group in domain controller.
- Each machine joined domain "era.local" with user "DomainAdmin" and this user is Administrator (Windows 10, 8.1, 7) or Standard user (power user on Windows XP).
- "DomainAdmin" is able to log into each machine and perform local administration tasks.
- Windows ERA Server service is temporarily running under "ERA\DomainAdmin" credentials. After deployment "Network Service" is enough. (no changes necessary in the appliance or Linux).

Targets:
Windows 10 Enterprise
Windows 8.1 Enterprise
Windows 7 Enterprise

1. Open **Network and Sharing Center**.
2. Check that network is **Domain network** in the **View your active networks** section.
3. Disable **Windows Firewall** for **Domain Network** by clicking the **Turn Windows Firewall on or off** and selecting **Turn off Windows Firewall in the Domain network location settings**.
4. Check that **File and printer sharing** in enabled for **Domain network** by clicking on the **Change advanced sharing settings** in the **Network and Sharing Center**.
5. In the ESET Remote Administrator Web Console create new "Agent deployment" Server task assigned to FQDN name of the machine (you can find the FQDN name of the machine by right clicking in the **Computer** and selecting **Properties**. The FQDN name appears next to the **Full computer name**).
6. Set **optional Server hostname** to point to FQDN name or IP address of the ERA server.
7. Set username to "ERA\DomainAdmin" (it is important to include the whole domain) and his password.
8. Select Agent's certificate.
9. Execute the task.

**For Windows XP Professional**

1. Disable **Windows Firewall** by selecting **Off** in the **Windows Firewall -> General** tab.
2. Check that **File and printer sharing** is enabled in the **Windows Firewall -> Exceptions** tab.
3. In the ESET Remote Administrator Web Console create new "Agent deployment" Server task assigned to FQDN name of the machine (you can find the FQDN name of the machine by right clicking in the **Computer** and selecting **Properties**. The FQDN name appears next to the **Full computer name**).
4. Set **optional Server hostname** to point to FQDN name or IP address of the ERA server.
5. Set username to "ERA\DomainAdmin" (it is important to include whole domain) and his password.
6. Select Agent's certificate.
7. Execute the task.
4.5.6 Product installation

ESET security products can be installed remotely by clicking the desired client computer and selecting New, or by creating a new Software Install task under Admin > Client Tasks. Click New... to begin setting up your new task.

The Client Task Execution display shows you the current status of Client Tasks and includes a Progress indicator for the selected task.

- Basic

Enter Basic information about the task, such as the Name, optional Description and the Task Type. The Task Type (see the list above) defines the settings and the behavior for the task.

- Target

IMPORTANT

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click Finish to create the task and then create a Trigger to specify Targets for the task.
Settings

Select the check box next to I agree with application End User License Agreement if you agree. See License Management or EULA for more information.

Click <Choose ESET License> and select the appropriate license for the installed product from the list of available licenses.

Click <Choose package> to select an installer package from the repository or specify a package URL. A list of available packages where you can select the ESET product you want to install (for example, ESET Endpoint Security) will be displayed. Select your desired installer package and click OK. If you want to specify a URL where the installation package is located, type or copy and paste the URL (for example file://\pc22\install\ees_nt64_ENU.msi) into the text field (do not use a URL that requires authentication).

http://server_address/ees_nt64_ENU.msi - If you are installing from a public web server or from your own HTTP server.
file://\pc22\install\ees_nt64_ENU.msi - if you are installing from network path.
file://C:\installs\ees_nt64_ENU.msi - if you are installing from local path.

NOTE

1. Both ERA Server and ERA Agent require access to the internet to access the repository and perform installations. If you do not have internet access, you can install the client software locally.

2. When performing Client Task > Operating System > Software Install on computers in a domain with ERA Agent running, it is necessary to provide read permission for the folder where the installers are stored. To do this, complete the following steps:
   a. Add an Active Directory computer account (for example NewComputer$)
   b. Grant Read permissions to NewComputer$ by right-clicking the folder with installers and selecting Properties > Sharing > Share from the context menu. Note that the "$" symbol needs to be present at the end of the computer name string.
If you need to, you can specify Installation parameters, otherwise leave this field empty. Select the check box next to Automatically reboot when needed to force an automatic reboot of the client computer after installation. Alternatively, you can leave this option deselected and the the client computer can be restarted manually.

**Summary**

Review the summary of configured settings and click Finish. The Client Task is now created and a pop-up window will open. We recommend you to click Create Trigger to specify when this Client Task should be executed and on what Targets. If you click Close, you can create a Trigger later on.

---

**4.5.6.1 Product installation (command line)**

The following settings are intended for use only with the reduced, basic and none user interface settings. See documentation for the msiexec version used for the appropriate command line switches.

**Supported parameters:**

**APPDIR=<path>**
- path - Valid directory path.
- Application installation directory.
  - For example: ees_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection

**APPDATADIR=<path>**
- path - Valid directory path.
- Application Data installation directory.

**MODULEDIR=<path>**
- path - Valid directory path.
- Module installation directory.

**ADDEXCLUDE=<list>**
- The ADDEXCLUDE list is a comma-separated list of all feature names not to be installed, as a replacement for the obsolete REMOVE.
- When selecting a feature not to install, then the whole path (i.e., all its sub-features) and related invisible features must be explicitly included in the list.
  - For example: ees_nt64_ENU.msi /qn ADDEXCLUDE=Firewall,Network

**NOTE**

The ADDEXCLUDE parameter cannot be used together with ADDLOCAL.

**ADDLOCAL=<list>**
- Component installation - list of non-mandatory features to be installed locally.
- Usage with ESET .msi packages: ees nt64 ENU.msi /qn ADDLOCAL=<list>

**Rules**
- The ADDLOCAL list is a comma separated list of all feature names to be installed.
- When selecting a feature to install, the whole path (all parent features) must be explicitly included in the list.
- See additional rules for correct usage.

Feature Presence
- **Mandatory** - the feature will always be installed.
- **Optional** - the feature can be deselected for install.
- **Invisible** - logical feature mandatory for other features to work properly.
- **Placeholder** - feature with no effect on the product, but must be listed with sub-features.

Feature tree of Endpoint is following:

<table>
<thead>
<tr>
<th>Feature tree</th>
<th>Feature Name</th>
<th>Feature Presence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
<td>Computer</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Computer / Antivirus and antispyware</td>
<td>Antivirus</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Computer / Antivirus and antispyware &gt; Real-time file system protection</td>
<td>RealtimeProtection</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Computer / Antivirus and antispyware &gt; Computer scan</td>
<td>Scan</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Computer / Antivirus and antispyware &gt; Document protection</td>
<td>DocumentProtection</td>
<td>Optional</td>
</tr>
<tr>
<td>Computer / Device control</td>
<td>DeviceControl</td>
<td>Optional</td>
</tr>
<tr>
<td>Network</td>
<td>Network</td>
<td>Placeholder</td>
</tr>
<tr>
<td>Network / Personal Firewall</td>
<td>Firewall</td>
<td>Optional</td>
</tr>
<tr>
<td>Web and e-mail</td>
<td>WebAndEmail</td>
<td>PlaceHolder</td>
</tr>
<tr>
<td>Web and e-mail / Protocol filtering</td>
<td>ProtocolFiltering</td>
<td>Invisible</td>
</tr>
<tr>
<td>Web and e-mail / Web access protection</td>
<td>WebAccessProtection</td>
<td>Optional</td>
</tr>
<tr>
<td>Web and e-mail / E-mail client protection</td>
<td>EmailClientProtection</td>
<td>Optional</td>
</tr>
<tr>
<td>Web and e-mail / E-mail client protection / MailPlugins</td>
<td>MailPlugins</td>
<td>Invisible</td>
</tr>
<tr>
<td>Web and e-mail / E-mail client protection / Antispam protection</td>
<td>Antispam</td>
<td>Optional</td>
</tr>
<tr>
<td>Web and e-mail / Web control</td>
<td>WebControl</td>
<td>Optional</td>
</tr>
<tr>
<td>Update mirror</td>
<td>UpdateMirror</td>
<td>Optional</td>
</tr>
<tr>
<td>Microsoft NAP support</td>
<td>MicrosoftNAP</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Additional rules

- If any of the WebAndEmail feature(s) is selected to be installed, the invisible ProtocolFiltering feature must be included in the list.
- If any of the EmailClientProtection sub-feature(s) is selected to be installed, the invisible MailPlugins feature must be explicitly included in the list.

Examples:

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
nees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

List of CFG_ properties:

- **CFG_POTENTIALLYUNWANTED_ENABLED=1/0**
  - 0 - Disabled, 1 - Enabled
  - PUA

- **CFG_LIVEGRID_ENABLED=1/0**
  - 0 - Disabled, 1 - Enabled
  - LiveGrid

- **FIRSTSCAN_ENABLE=1/0**
  - 0 - Disable, 1 - Enable
  - Schedule a new FirstScan after installation.

- **CFG_EPFW_MODE=0/1/2/3**
  - 0 - Automatic, 1 - Interactive, 2 - Policy, 3 - Learning

- **CFG_PROXY_ENABLED=0/1**
  - 0 - Disabled, 1 - Enabled
CFG_PROXY_ADDRESS=<ip>
  • Proxy IP address.

CFG_PROXY_PORT=<port>
  • Proxy port number.

CFG_PROXY_USERNAME=<user>
  • User name for authentication.

CFG_PROXY_PASSWORD=<pass>
  • Password for authentication.

4.5.6.2 List of problems when installation fails
  • Installation package not found.
  • Required newer version of the Windows Installer Service.
  • Another version or conflicting product is already installed.
  • Another installation is already in progress. Complete that installation before proceeding with this install.
  • Installation or uninstallation finished successfully but computer restart is required.
  • Task failed - there was an error, you need to look at the Agent trace log and check the return code of the installer.

4.5.7 Desktop Provisioning
See Supported Desktop Provisioning Environments for details.

4.6 Additional configuration
Once you have completed initial configuration, there are some additional actions you can consider doing:

Create/edit groups
We recommend that you sort clients into Groups, either Static or Dynamic, based on various criteria. This makes managing clients easier and helps you keep an overview of your network.

Create a new policy
Policies are used to distribute a specific configuration for ESET products running on client computers. They allow you to avoid configuring ESET products on each client manually. Once you have created a new policy with your custom configuration, you can assign it to a group (either static or dynamic) to apply your settings to all the computers in that group.

Assign a policy to a group
As explained above, a policy must be assigned to a group to take affect. Computers that belong to the group will have this policy applied to them. The policy is applied and updated every time an Agent connects to ERA Server.

Set up Notifications and create Reports
We recommend that you use notifications and reports to monitor the status of client computers in your environment. For example, if you want to be notified that a certain event occurred or want to view or download a report.
5. Mobile Device Management

The following diagram demonstrates communication between ESET Remote Administrator components and a mobile device:

ERSA <-> MDC <-> Device communication

NOTE
Direct upgrade from ESET Mobile Device Connector version 6.1 (all releases) to version 6.5 is not possible. It is necessary to first upgrade MDM from version 6.1 to version 6.4 and then you can upgrade to version 6.5.

In order to take advantage of the Mobile Device Management feature in ESET Remote Administrator, perform the following steps to install, enroll, configure and apply policies.

1. Install Mobile Device Connector (MDC) using the All-In-one installer or perform a component installation for Windows or Linux. Make sure that you have met the prerequisites prior to the installation.

   NOTE
   If you are installing MDC using the All-in-one installer, HTTPS certificates signed by ERA CA are created during the installation process. (this certificate is not visible in Admin > Certificates > Peer Certificates)

   To install ERA with the All-in-one installer and use a 3rd party HTTPS certificate, install ESET Remote Administrator first, then change your HTTPS certificate using Policy (in the ESET Remote Administrator mobile Device Connector Policy > General > Change certificate > Custom certificate).

   If you are installing the MDC component by itself, you can use:
   a) certificate signed by ERA CA (Basic > Product: Mobile Device Connector; Host: Hostname/IP Adress of MDC; Sign > Sign Method: Certification Authority; Certification Authority: ERA Certification Authority)
   b) 3rd party HTTPS certificate chain signed by a CA trusted by Apple (list of CA trusted by Apple).

2. Import the HTTPS certificate chain for MDM into the certificate store on the MDM device.

3. Activate ERA MDC using a Product Activation Client Task. The procedure is the same as when activating any ESET security product on a client computer (a license unit will not be used).

4. Run a User Synchronization Server Task (Recommend). This lets you automatically synchronize users with Active Directory or LDAP for the purpose of User Management.
5. Create an APN/DEP certificate. This certificate is used by ERA MDM for iOS device Enrollment.

**WARNING**
Certificates that will be added to your enrollment profile must be also added to your DEP profile.

6. Create a new policy for ESET Mobile Device Connector in order to activate APNS.

**NOTE**
If you are performing iOS Device enrollment with the Apple Device Enrollment Program (DEP) continue [here](#).

7. Enroll mobile devices using a Device Enrollment task. Configure the task to enroll devices for Android and/or iOS. This can also be done from Computers or Group tab by clicking Add new > Mobile devices while having selected a Static Group (Add new cannot be used in Dynamic Groups).

8. If you have not provided license during Device Enrollment, activate Mobile devices using a Product Activation Client Task - choose an ESET Endpoint Security license. A license unit will be used for each Mobile device.

9. You can edit Users in order to configure Custom attributes and Assign Mobile devices if you've not assigned users during Device Enrollment.

10. Now you can start applying policies and managing mobile devices. For example, Create a Policy for iOS MDM - Exchange ActiveSync Account which will automatically configure your Mail account, Contacts and Calendar on iOS devices. You can also apply restrictions on an iOS device and/or add a Wi-Fi connection.

11. You can use Reenroll on a mobile device which was corrupted or wiped. Re-enroll link will be sent via email.

12. Stop Managing (Uninstall ERA Agent) task will cancel MDM enrollment of a mobile device and remove it from ERA.
5.1 Device Enrollment

Mobile devices can be managed via ERA and an ESET security product running on the mobile device. To start managing mobile devices, you need to enroll them in ERA (it is no longer necessary to enter IMEI or other identification numbers into the mobile device).

The diagram below illustrates how a Mobile Device communicates with Mobile Device Connector during the enrollment process:

Device Enrollment

This diagram explains when enrollment, reenrollment and deenrollment can be used and explains the difference between managed and unmanaged devices.
• **Enrollment**: Enrollment can only be used when the device is not managed by MDM. In this case, the device doesn't exist in the **Computers** section. Deleting a device from the webconsole doesn't make it unmanaged and the device will appear in the webconsole after a successful replication. Only the deenrollment process can remove a device from managed status. Each enrollment token is unique and one-time-only so it can be used only once. Once the token is used it can't be used again.

• **Reenrollment**: Reenrollment can only be used if the device is managed. The reenrollment token is always different from the enrollment token and it can also be used only once. To reenroll a device, open the **Computers** section and select the mobile device you want to reenroll. Open the **Actions** menu and select **Mobile > Reenroll**.

• **Deenrollment**: Deenrollment is the correct way to stop managing a device. Deenrollment is performed using a **Stop managing client task**. If the device is not responding it can take up to 3 days until the device is actually removed. If you want to remove the device just to enroll it again, use reenrollment instead.

You can enroll mobile devices in the **Computers** section or under **Admin > Groups**. Select the **Static Group** that you want to add mobile devices to, click **Add new > Mobile devices** and then select one of the following enrollment methods:

• **Enrollment via email** - mass enrollment of mobile devices via email. This option is best suited if you need to enroll a large number of mobile devices or if you have existing mobile devices which you do not have physical access to. Using this option requires active participation from the user/owner of the mobile device.

• **Individual enrollment via link or QR code** - single mobile device enrollment. You will be able to enroll one mobile device at a time and will need to repeat the same process for each device. We recommend that you use this option only when you have a smaller number of mobile devices to enroll. This option is suitable if you do not want users/mobile device owners to do anything and must perform all enrollment tasks yourself. Also, you can use this option if you have new mobile devices which will be handed over to users once the devices are all set up.

**Troubleshooting:**

1. What should I do if I get error message: "The Enrollment token is already being used or is not valid."?

   It is likely that you are attempting to reenroll with an old enrollment token. Create a new reenrollment token in the webconsole and use that one instead. It is also possible that you are attempting a second reenrollment too soon after the first one. Verify that the reenrollment token is different from the first one. If it is not, then wait a few minutes and try to generate a new reenrollment token again.

2. What should I do if I get error message: "service certificate validation failed"?

   This error message indicates that there is a problem with your APNS or GCM service certificate. This is announced in ERA Web Console as one of the following warnings under MDM Core alerts:

   • **GCM service certificate validation failed** (0x0000000100001002)
   • **APNS service certificate validation failed** (0x0000000100001000)
   • **APNS Feedback service certificate validation failed** (0x0000000100001004)

   Make sure you have the correct certificate authority available on your system:

   • APNS certificate authority: **Entrust Certification Authority**, need to validate certificate from gateway.push.apple.com:2195;
   • APNS Feedback certificate authority: **Entrust Certification Authority**, need to validate certificate from feedback.push.apple.com:2196;
   • GCM certificate authority: **GeoTrust Global CA**, need to validate certificate from android.googleapis.com:443.

**NOTE**

If you are performing iOS Device enrollment with the Apple Device Enrollment Program (DEP) continue [here](#).
The desired certificate authority should be included in the certificate store on the MDM host machine. In a Windows system, you can search for "Manage Trusted Root Certificates". In a Linux system, the certificate location is dependent on the distribution you are using. Some examples of certificate store destinations include:

- on Debian, Cent OS: /usr/lib/ssl/cert.pem, /usr/lib/ssl/certs;
- on RedHat: /usr/share/ssl/cert.pem, /usr/share/ssl/certs;
- command openssl version -d usually returns desired path.

If the desired certification authority is not installed on the system the MDM Core is running on, install it. Following installation, restart the ERA MDC service.

**WARNING**

Use caution, certificate validation is a security feature, so if the warning occurs in web console it could also indicate a security threat.

5.1.1 Enrollment via email

This method is ideal for mass enrollment of mobile devices. You can send an enrollment link to any number of devices via email. Each mobile device will receive a unique one-time token based on the email address.

**IMPORTANT**

It is mandatory to configure an SMTP server for mass enrollment via email. Go to Server Settings, expand Advanced Settings and specify the SMTP server details.

1. To add new mobile devices, go to the Computers section or Admin > Groups. Select the Static Group that you want to add mobile devices to and click Add new > Mobile devices > Enrollment via email.

Add mobile devices

- **Enrollment via email**
  
  Send enrollment link to any number of devices via email. To use this option an SMTP server must be configured in the server settings.

  Configure server settings

- Individual enrollment via link or QR code

  Enroll devices one at a time. You need physical access to the devices. Not recommended for large numbers of devices.

2. Mobile Device Connector - will automatically be selected. If you have more than one MDC, select the FQDN of the MDC you want to use. If you do not have Mobile Device Connector installed yet, refer to the Mobile Device Connector installation - Windows or Linux chapters for installation instructions.

3. License (optional) - click Select and choose the license that will be used for activation. A Product Activation client task will be created for the mobile device. A license unit will be taken (one per each mobile device).

4. Parent group - if you do not have a specific Static group for mobile devices, we recommend that you create a New Static Group (called Mobile Devices, for example ). If you already have an existing group, click the /All/Lost & Found, a pop-up window will open where you can choose the Static group.

5. List of Devices - specify mobile devices for enrollment, you can use the following functions to add mobile devices:
• **Add device** - single entry, you need to manually type an email address associated with the mobile device to which the enrollment email will be sent. If you also assign a user to the mobile device by clicking Pair and selecting the user, the email address will be overwritten with the one specified within User Management. If you want to add another mobile device, click **Add device** again submit the required information.

• **Select User** - you can add devices by selecting the appropriate user check boxes listed in **User Management**. Click Unpair to make corrections to the list of mobile devices for enrollment. Once you've unpaired an assigned user, that user will be noted as not paired. Click Pair to select the desired user for an unpaired device. Click the Trash can icon to delete an entry.

• **Import CSV** - a method that makes it easy to add a large number of mobile devices. Upload a .csv file containing a list of devices to add, see **Import CSV** for more details.

**NOTE**
We recommend that you specify a **Device name** in each entry when using the Import CSV method. This is the device name shown in the **Computers** section. If you leave the **Device name** field empty, email address will be used instead and appear as Device name in **Computers** and **Groups**. This may cause some confusion, especially in case you use the same email address to enroll multiple devices. This email address will appear multiple times and prevent you from being able to distinguish between the devices.

**IMPORTANT**
We recommend that you assign at least one user to a mobile device. If you want to use personalized policies on **iOS** a user must be assigned to a device.

6. **Enrollment email message** - a predefined message template contains details that are usually sufficient, but you can customize **Subject** and **Content** by including further information for your users. **Instructions** are shown below the **Content** in the enrollment email and will contain a **Device name** (or an email address) with enrollment link (URL). If you use one email address to enroll multiple mobile devices, a list of devices will be shown, each with its own enrollment link (URL) assigned. There are also instructions that mobile device (iOS and Android) user must perform in order to complete enrollment.

7. When you click **Enroll**, an email will be sent to each email address with appropriate enrollment link(s) and instructions.

8. To complete mobile device enrollment, follow these steps or let the users/owners of the mobile devices perform the steps themselves:
   - **Device Enrollment Android**
   - **Device Enrollment iOS**
5.1.2 Individual enrollment via link or QR code

When enrolling a mobile device using an enrollment link or QR code, you will need physical access to the device. Also, in order to use the QR code, you will need to have QR code Reader/Scanner application installed on the mobile device.

**NOTE**
For large numbers of mobile devices, we recommend you to use Enrollment via email.

1. To add a new mobile device, go to Computers section or Admin > Groups. Select Static Group that you want to add mobile device to and click Add new > Mobile devices > Individual enrollment via link or QR code.

Add mobile devices

- **Enrollment via email**
  - Send enrollment link to any number of devices via email. To use this option an SMTP server must be configured in the server settings.
  - Configure server settings

- **Individual enrollment via link or QR code**
  - Enroll devices one at a time. You need physical access to the devices. Not recommended for large numbers of devices.

2. **Device name** - type the Name of the mobile device (this name will be shown in the list of Computers), optionally enter a Description.

3. **User (optional)** - we recommend you to assign a user with mobile device, it is required for iOS devices, but optional for Android.

4. **Mobile Device Connector** - will automatically be selected. If you have more than one MDC, choose from the list by clicking the FQDN. If you do not have Mobile Device Connector installed yet, refer to the Mobile Device Connector installation - Windows or Linux chapters for installation instructions.

5. **License (optional)** - click Select and choose license that will be used for activation. A Product Activation client task will be created for the mobile device. A license unit will be taken (one per each mobile device).

6. **Parent group** - if you do not have a specific Static group for mobile devices, we recommend you to create a New Static Group (called Mobile Devices for example). If you already have an existing group, click the /ALL/LOST & FOUND, a pop-up window will open where you can choose the Static group.

7. After you click Next, the enrollment Link (URL) and QR code will be displayed. Type the whole URL into the mobile device's web browser manually (for example https://eramdm:9980/token, the token will be different for each mobile device), or send this URL to the mobile device by other means. Alternatively, you can use provided QR Code, which might be more convenient than typing the URL, but requires QR code Reader/Scanner on the mobile device.
8. To add another mobile device, click **Enroll Another**. A new Add mobile device page will open which remembers previous selections in the General section, you will only need to enter Device name and assign a User, click **Next** and follow instructions in step 7. Once you have completed generating enrollment URLs and QR codes, click **Close** to return to the previous window.

9. To perform the actual enrollment of the mobile devices, follow these step-by-step instructions:
   - [Device Enrollment Android](#)
   - [Device Enrollment iOS](#)

### 5.1.3 Device Enrollment Android

There are two scenarios for enrollment when ESET Endpoint Security for Android (EESA) is activated on the mobile device. You can activate EESA on the mobile device using a Product Activation task (recommended). The other scenario is for mobile devices with the ESET Endpoint Security for Android app already activated.

**EESA already activated** - follow the steps below to enroll your device:

1. Tap the enrollment link URL (including the port number) received via email, or type it into the browser manually (for example, `https://eramdm:9980/<token>`). You might be asked to accept an SSL certificate, click **Accept** if you agree and then click **Connect**.
IMPORTANT
If you do not have ESET Endpoint Security installed on the mobile device, you will automatically be redirected to the Google Play store, where you can download the app.

NOTE
If you receive the notification *Couldn’t find an app to open this link*, try opening the enrollment link in the default Android web browser.

2. Check your connection details (Mobile Device Connector server address and port) and click **Connect**.

To connect a device to Remote Administrator:
- In Remote Administrator add a new mobile device to the “Computers” list.
- Enter Mobile Device Connector (MDC) server address.

**MDC SERVER ADDRESS**

https://[server_address]

**Requirements**: Remote Administrator 6 or newer with Mobile Device Connector.

3. Type the ESET Endpoint Security admin mode password into the blank field and tap **Enter**.
4. This mobile device is now being managed by ERA, tap Finish.

**EESA not activated yet** - Follow the steps below to activate the product and enroll your Device:

1. Tap the enrollment link URL (including the port number) and type it into the browser manually (for example, `https://eramdm:9980/<token>`) or you can use provided QR Code. You might be asked to accept an SSL certificate, click Accept if you agree and then click Connect.
If you do not have ESET Endpoint Security installed on the mobile device, you will automatically be redirected to the Google Play store, where you can download the app.

If you receive the notification * Couldn’t find an app to open this link *, try opening the enrollment link in the default Android web browser.

2. Enter the name of the mobile device user.
Enter your name

Your name helps the administrator identify your device if it is lost or stolen.

3. Tap **Enable** to enable uninstall protection.
Enable uninstall protection

Enable uninstall protection to ensure ESET Endpoint Security cannot be uninstalled if your device is lost or stolen.

You will be required to set ESET Endpoint Security as device administrator.

4. Tap **Activate** to activate device administrator.
5. At this point, you can exit the ESET Endpoint Security for Android app on the mobile device and open ERA Web Console.
6. In ERA Web Console, go to Admin > Client Tasks > Mobile > Product Activation and click New.

It might take some time for the Product Activation client task to run on the mobile device. Once the task is successfully executed, the ESET Endpoint Security for Android app is activated and the mobile device can be managed by ERA. The user will now be able use the ESET Endpoint Security for Android app. When the ESET Endpoint Security for Android app is open, the main menu will be displayed:
5.1.4 Device Enrollment iOS

**NOTE**
If you are performing iOS Device enrollment with Apple Device Enrollment Program (DEP) continue here.

1. Tap the enrollment link URL (including the port number) and type it into the browser manually (for example, https://eramdm:9980/<token>) or you can use the provided QR Code.

2. Tap Install to continue at the MDM Enrollment Install Profile screen.

3. Tap Trust to allow installation of the new profile.
4. After installing the new profile, the Signed by field will display that the profile is Not Signed. This is standard for MDM enrollment. The profile is actually signed with a certificate, despite this it is shown as “not signed”. This is because iOS does not yet recognize the certificate.
5. This enrollment profile allows you to configure devices and set security policies for users or groups.

**IMPORTANT**
Removing the enrollment profile removes all company settings (Mail, Calendar, Contacts, etc.) and the iOS mobile device will not be managed. If a user removes the enrollment profile, ERA will not be aware of this and the device's status will change to ![warning](https://example.com/warning.png) and then to ![error](https://example.com/error.png) after 14 days because the device is not connecting. No other indication that the enrollment profile has been removed will be given.
5.1.4.1  Device Enrollment iOS with DEP

The Apple Device Enrollment Program (DEP) is Apple's new method for enrolling corporate iOS devices. With DEP you can enroll the iOS devices without any direct contact with the device and also with minimal interaction from the user. The Apple DEP enrollment provides administrators the option to customize the complete device setup process. It also provides the option to prevent users from removing the MDM profile from the device. You can enroll your existing iOS devices (if they meet the iOS devices DEP requirements) and all iOS devices that you will buy in the future. For further information about Apple DEP see the Apple DEP Guide and Apple DEP Documentation.

Connect your ERA MDM Server with Apple DEP server:

1. Verify that all Apple DEP Requirements are met for both account requirements and device requirements.
   - DEP Account:
     - The program is only available in certain countries. Visit the Apple DEP webpage to see if DEP is available in your country.
     - Apple DEP Account requirements can be found on these websites: Apple deployment program requirements and Apple Device Enrollment Program requirements.
     - Detailed DEP device requirements can be found here.

2. Log in to your Apple DEP Account (If you do not have an Apple DEP account you can create one here).
3. From the **Device Enrollment Program** section on the left side select **Manage Servers**.

4. Click **Add MDM Server** to open the Add MDM Server window.

5. Enter your **MDM Server Name**, for example: "ERA MDM Server," and then click Next.

6. Upload your public key into the DEP portal. Click **Choose File** and select the public key file (this is the APNS certificate you downloaded from Apple Push Certificate Portal) and click Next.
7. Now you can download your Apple DEP Token. This file will be uploaded into the ERA MDC policy under Apple Device Enrollment Program (DEP) -> Upload authorization token.

Add iOS Device into Apple DEP:

The next step is to assign iOS devices to your virtual MDM Server inside Apple DEP portal. You can assign your iOS devices by serial number, order number or by uploading a list of Serial numbers for target devices in CSV format. Either way, you must Assign the iOS device to the virtual MDM Server (you created in the previous steps).
WARNING
Once a device is removed from the DEP portal, it is removed permanently, you cannot add it back.

After that you can leave the Apple DEP portal and continue in ERA Web Console.

WARNING
If you are enrolling iOS devices that are currently in use (and that meet the device requirements) new policy settings will be applied to them after a factory reset of target device.

In order to complete the enrollment process you need to upload the APNS certificate into the MDC Policy that will be assigned to the MDM Server. (This MDC Policy will fulfill the role of MDM Server Settings).

NOTE
If your iOS device displays the message that it is not able to download the profile from ESET during enrollment, verify that the MDM server inside DEP is correctly configured (has the correct certificates) and that you assigned the correct iOS device to your selected ERA MDM Server inside Apple DEP.

5.2 Create a Policy for iOS MDM - Exchange ActiveSync Account

This policy governs all settings for iOS device. These settings apply for both DEP and non-DEP iOS devices.

- The DEP-only settings are denoted with a DEP icon  
  These settings will only apply to iOS devices enrolled in the Apple DEP portal. We recommend that you do not customize these DEP-only settings when creating a policy for non-DEP iOS devices.

- Some settings can only be applied to an iOS device with a certain version of iOS. These settings are marked by an icon representing the iOS version.

  - iOS version 9.0 and higher  

iOS version 9.3 and higher

iOS version 8.1.3 and higher

- If both of the icons (DEP icon and iOS version icon) are present next to a specific setting, the device must meet both requirements or management of the setting will fail.

See the sample scenario below which explains how to use the iOS MDM policy when you want to set up a Microsoft Exchange Mail account:

You can use this policy to configure a Microsoft Exchange Mail account, Contacts and Calendar on user's iOS mobile devices. The advantage of using such a policy is that you only need to create one policy which you can then apply to many iOS mobile devices without the need to configure each separately. This is possible using Active Directory user attributes. You need to specify a variable, for example \$\{exchange_login/exchange\} and this will be replaced with a value from the AD for a particular user.

If you do not use Microsoft Exchange or Exchange ActiveSync, you can manually configure each service (Mail Accounts, Contacts Accounts, LDAP Accounts, Calendar Accounts and Subscribed Calendar Accounts).

The following is an example of how to create and apply a new policy to automatically set up Mail, Contacts and Calendar for each user on iOS mobile device using Exchange ActiveSync (EAS) protocol to synchronize these services.

**NOTE**
Before you begin setting this policy up, make sure you've already performed the steps described under Mobile Device Management.

**Basic**

Enter a Name for this policy. The Description field is optional.

**Settings**

Select ESET Mobile Device Management for iOS from the drop-down list, click Others to expand categories and then click Edit next to Exchange ActiveSync Accounts.
Click **Add** and specify the details of your Exchange ActiveSync account. You can use variables for certain fields (select from the drop-down list), such as User or Email Address. These will be replaced with actual values from **User Management** when a policy is applied.
- **Account name** - Enter the name of the Exchange account.
- **Exchange ActiveSync Host** - Specify the Exchange Server hostname or its IP address.
- **Use SSL** - This option is enabled by default. It specifies whether the Exchange Server uses Secure Sockets Layer (SSL) for authentication.
- **Domain** - This field is optional. You can enter the domain this account belongs to.
- **User** - Exchange login name. Select the appropriate variable from the drop-down list to use attribute from your Active Directory for each user.
- **Email Address** - Select the appropriate variable from the drop-down list to use an attribute from your Active Directory for each user.
- **Password** - Optional. We recommend that you leave this field empty. If it is left empty users will be prompted to create their own passwords.
- **Past Days of Mail to Sync** - Select the number of past days of mail to sync from the drop-down list.
- **Identity certificate** - Credentials for connection to ActiveSync.
- **Allow messages to be moved** - If enabled, messages can be moved from one account to another.
- **Allow recent addresses to be synced** - If this option is enabled, the user is allowed to sync recently used addresses across devices.
- **Use Only in Mail** - Enable this option if you want to allow only the Mail app to send outgoing email messages from this account.
- **Use S/MIME** - Enable this option to use S/MIME encryption for outgoing email messages.
- **Signing Certificate** - Credentials for signing MIME data.
- **Encryption Certificate** - Credentials for encryption MIME data.
- **Enable per-message encryption switch** - Allow the user to choose whether to encrypt each message.

**NOTE**
If you do not specify a value and leave the field blank, mobile device users will be prompted to enter this value. For example a **Password**.

- **Add certificate** - You can add specific Exchange certificates (User Identity, Digital Signature or Encryption Certificate) if required.
**NOTE**
Using the steps above, you can add multiple Exchange ActiveSync Accounts, if desired. This way, there will be more accounts configured on one mobile device. You can also edit existing accounts if necessary.

**Assign**

Specify the clients (individual computers/mobile devices or whole groups) that are the recipients of this policy.

Click **Assign** to display all Static and Dynamic Groups and their members. Select your desired clients and click **OK**.
5.3 Create a Policy for MDC to activate APNS/DEP for iOS enrollment

This is an example of how to create a new policy for ESET Mobile Device Connector to activate APNS (Apple Push Notification Services) and iOS device Enrollment feature. This is required for iOS device Enrollment. Before configuring this policy, create a new APN certificate and have it signed by Apple on the Apple Push Certificates Portal so that it becomes a signed certificate or APNS Certificate. For step-by-step instructions see the APN certificate section.

Basic

Enter a Name for this policy. The Description field is optional.

Settings

Select ESET Remote Administrator Mobile Device Connector from the drop-down list.

IMPORTANT

If you installed MDM Server with All-in-One Installer (Not as a standalone and not as a component) the HTTPS certificate will be generated automatically during the installation. This only applies for ERA 6.5 Installer and later. For all the other cases you need to apply a custom HTTPS certificate. You can find more information annotated following step one of Mobile Device Management topic.

You can use the ERA certificate (signed by ERA CA) or your custom certificate. You can also specify the date for Force certificate change. Check the tooltip next to this setting for more information.

Summary

Review the settings for this policy and click Finish.
Under General, go to Apple Push Notification Service and upload the APNS Certificate and a APNS Private Key.

**NOTE**
Type your actual organization's name over the Organization string. This is used by the enrollment profile generator to include this information in the profile.
APNS Certificate (signed by Apple) - click the folder icon and browse for the APNS Certificate to upload it. (This is the file you downloaded from Apple Push Certificates Portal.)

APNS Private Key - click the folder icon and browse for the APNS Private Key to upload it. (This is the file you downloaded during APN/DEP Certificate creation.)

![APNS Certificate (signed by Apple)](image)

![APNS Private Key](image)

Diagnostics - Enable or disable the submission of anonymous crash report statistics to ESET for the improvement of customer experience.

Logging - Set the log verbosity to determine the level of information that will be collected and logged, from Trace (informational) to Fatal (most important critical information).

If you are creating this policy for iOS enrollment with Apple DEP, navigate to the Apple Device Enrollment Program (DEP).

Apple Device Enrollment Program (DEP) - these settings are DEP-only.

⚠️ WARNING
After the initial configuration, if any of these settings will be changed, in order to apply the changes, you will need to factory-reset and reenroll all the affected iOS devices.

Upload authorization token - click the folder icon and browse for the DEP server token. (This is the file you downloaded when you created the virtual MDM server on the Apple DEP portal)

Supervised mode - supervised mode is mandatory for most of the device policy options.

Mandatory Installation - the user will not be able to use the device without the installation of MDM profile.

Allow user to remove MDM profile - device must be in supervised mode to disallow the user to remove the MDM profile.

Skip Setup Items - this setting allows you to choose which of the initial setup steps during the initial iOS setup will be skipped. You can find more information about each of these steps in the Apple Knowledgebase Article.

Assign
Select the device that is hosting the MDM server the policy is targeted on.
Click **Assign** to display all Static and Dynamic Groups and their members. Select the Mobile Device Connector instance that you want to apply the policy on and click **OK**.

**Summary**

Review the settings for this policy and click **Finish**.

### 5.4 Create a Policy to enforce restrictions on iOS and add Wi-Fi connection

You can create a policy for iOS mobile devices to enforce certain restrictions. You can also define multiple Wi-Fi connections so that, for example, users will automatically be connected to the corporate Wi-Fi network at different office locations. The same applies to **VPN connections**.

Restrictions that you can apply to iOS mobile device are listed in categories. For example, you can disable FaceTime and the use of camera, disable certain iCloud features, fine-tune Security and Privacy options or disable selected applications.

**NOTE**

Restrictions that can or cannot be applied depend on the version of iOS used by client devices. iOS 8.x and newer are supported.
The following is an example of how to disable the **camera** and **FaceTime** apps and add Wi-Fi connection details to the list in order to have the iOS mobile device connect to a Wi-Fi network whenever the network is detected. If you use the auto Join option, iOS mobile devices will connect to this network by default. The policy setting will override a user’s manual selection of a Wi-Fi network.

**Basic**

Enter a **Name** for this policy. The **Description** field is optional.

**Settings**

Select **ESET Mobile Device Management for iOS**, click **Restrictions** to see categories. Use the switch next to **Allow use of camera** to disable it. Since the camera is disabled, FaceTime will automatically be disabled as well. If you wish to disable FaceTime only, leave the camera enabled and use the switch next to **Allow FaceTime** to disable it.
After you've configured **Restrictions**, click **Others** and then click **Edit** next to **Wi-Fi connection list**. A window with the list of Wi-Fi connections will open. Click **Add** and specify connection details for the Wi-Fi network you want to add. Click **Save**.

- **Service Set Identifier (SSID)** - SSID of the Wi-Fi network to be used.
- **Auto Join** - Optional (enabled by default), device automatically joins this network.

**Security settings:**
- **Encryption Type** - Select appropriate encryption from the drop-down list, make sure this value exactly matches the capabilities of the Wi-Fi network.
- **Password** - Enter the password that will be used to authenticate when connecting to the Wi-Fi network.

**Proxy settings** - Optional. If your network uses a Proxy, specify values accordingly.

**Assign**

Specify the clients (individual computers/mobile devices or whole groups) that are the recipients of this policy.
Click **Assign** to display all Static and Dynamic Groups and their members. Select your desired clients and click **OK**.
Review the settings for this policy and click **Finish**.

### 5.4.1 MDM configuration profiles

You can configure the profile to impose policies and restrictions on the managed mobile device.

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Passcode</strong></td>
<td>Requires end-users to protect their devices with passcodes each time they return from idle state. This ensures that any sensitive corporate information on managed devices remains protected. If multiple profiles enforce passcodes on a single device, the most restrictive policy is enforced.</td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
<td>Restriction profiles limit the features available to users of managed devices by restricting the use of specific permission related to Device functionality, Application, iCloud, Security and Privacy.</td>
</tr>
<tr>
<td><strong>Wi-Fi connection list</strong></td>
<td><strong>Wi-Fi profiles</strong> push corporate Wi-Fi settings directly to managed devices for instant access.</td>
</tr>
<tr>
<td><strong>VPN connection list</strong></td>
<td>VPN profiles push corporate virtual private network settings to corporate devices so that users can securely access corporate infrastructure from remote locations. <strong>Connection Name</strong> - View the name of the connection displayed on the device. <strong>Connection type</strong> - Choose the type of connection enabled by this profile. Each connection type enables different capabilities. <strong>Server</strong> - Enter the hostname or IP address of the server being connected to.</td>
</tr>
<tr>
<td><strong>Mail Accounts</strong></td>
<td>Allows the administrator to configure IMAP/POP3 email accounts.</td>
</tr>
<tr>
<td><strong>Exchange ActiveSync</strong></td>
<td><strong>Exchange ActiveSync</strong> profiles allow end-users to access corporate push-based email infrastructure. Please note that there are pre-populated look-up value fields and options that only apply to iOS 5+.</td>
</tr>
<tr>
<td><strong>CalDAV - Calendar</strong></td>
<td>CalDAV provides configuration options to allow end-users to sync wirelessly with the enterprise CalDAV server.</td>
</tr>
<tr>
<td><strong>CardDAV - Contacts</strong></td>
<td>This section allows for specific configuration of CardDAV services.</td>
</tr>
<tr>
<td><strong>Subscribed Calendars</strong></td>
<td>Subscribed Calendars provides calendar configuration.</td>
</tr>
</tbody>
</table>
6. Admin

The Admin section is the main configuration component of ESET Remote Administrator. This section contains all the tools that administrator can use to manage client security solutions, as well as the ERA Server settings. You can use Admin tools to configure your network environment in such a way that it won't require a lot of maintenance. Also, you can configure notifications and dashboards which will keep you aware of the status of your network.

In this section

- Status Overview
- Dynamic Group Templates
- Groups
- User Management
- Installers
- Quarantine
- Policies
- Client tasks
- Server tasks
- Notifications
- Certificates
- Access Rights
- Server Settings
- License Management

6.1 Groups

Groups can be understood as folders where computers and other objects are categorized. Security model since ERA 6.5 uses groups to contain objects and assign permissions. Objects are not only computers but also all tasks, notifications, policies, certificates, installers or permission sets. See the list of permissions for more information on access rights.

For computers and devices, you can use pre-defined groups and group templates, or create new ones. Client computers can be added to groups. This helps you keep the computers structured and arranged to your liking. You can add computers to either a Static or Dynamic Group.

Static Groups are managed manually, while Dynamic Groups are arranged automatically based on specific criteria in a template. Once the computers are in groups, you can assign policies, tasks or settings to these groups. The policy, task or setting is then applied to all the members of the group. There are two types of client groups:

**Static Groups**

Static Groups are groups of selected client computers and other objects. Group members are static and can only be added/removed manually, not based on dynamic criteria. An object can only be present in one Static Group. A static group can be deleted only if there are no objects contained in it.

**Dynamic Groups**

Dynamic Groups are groups of devices (not other objects like tasks or policies) where membership in the group is determined by specific criteria. If a client device does not fulfill that criteria, it will be removed from the group. Computers that satisfy the criteria will be added to the group automatically (hence the name “dynamic”).
The **Groups** window is divided into three sections:

1. A list of all groups and their subgroups is displayed on the left. You can select a group and an action for this group from the context menu (next to the group name). The options are the same as those described below (group actions button).

2. The following details for the selected group are shown on the right pane (you can switch between tabs):
   - **Computers** that are members of the group.
   - **Policies** assigned to this group.
   - **Tasks** assigned to this group.
   - **Summary** basic description of the group.

3. **Group** and **Computers** let you perform all the following actions:

   **Group** actions button:
   - **New Static Group...**
     This option becomes available if you click a **Group** in the list on the left. This group will be the default parent group, but you can change the parent group later when you [create a new Static Group](#).
   - **New Dynamic Group...**
     This option becomes available if you click a **Group** in the list on the left. This group will be the default parent group, but you can change the parent group later when you [create a new Dynamic Group](#).
   - **Edit...**
     Allows you to edit the selected Group. The same settings apply as when you create a new Group (static or dynamic).
   - **Move...**
     You can select a group and move it as a subgroup of another group.
   - **Delete**
     Removes the selected group completely.

   **Import...**
   You can import a list (usually a text file) of computers, as members of the selected group. If the computers already exist as a members of this group, the conflict will be solved based on the selected action:
   - **Skip conflicting computers** (conflicting computers will not be added)
   - **Move conflicting computers from other groups** (conflicting computers will be moved here from other groups they belong to)
   - **Duplicate conflicting computers** (conflicting computers will be added, but with different names).

   **Export...**
   Export the members of the group (and subgroups, if selected) in a list (.txt file). This list can be used for review, or imported later.

   **Add New...**
   With this option, you can add a [new device](#).

   **Scan**
   Using this option will run the **On Demand Scan** task on the client that reported the threat.

   **Update Modules**
   Using this option will run the **Modules Update** task (triggers an update manually).
Mobile

- Reenroll... with this option, you can create new client task.
- Find - if you want to request the GPS coordinates of your mobile device.
- Lock - device will be locked when suspicious activity is detected or the device is marked as missing.
- Unlock - device will be unlocked.
- Siren - triggers a loud siren remotely, the siren will start even if your device is set to mute.
- Wipe - all data stored in your device will be permanently erased.

New task...
You can create a new Client Task. Select a task and configure the throttling (optional) for this task. The task will be queued according to the task settings.
This option immediately triggers an existing task, that you select from a list of available tasks. The trigger is not available for this task, because it will be executed immediately.

Manage Policies...
Assign a Policy for the selected group.

6.1.1 Create new Static Group
There are three ways to create a New Static Group:

1. Click Computers > Groups and select New Static Group...
2. Click Admin > Groups > New Static Group...
3. Click **Admin > Groups** > select a Static Group and click **Group**.
6.1.2 Create new Dynamic Group

Dynamic Groups are groups of clients selected based on specific criteria. If a client computer does not fulfill the criteria, it will be removed from the group. If it fulfills the defined conditions, it will be added to the group. Group selection happens automatically based on configured settings, except for in the case of Static Groups.

There are three ways to create a New Dynamic Group:

1. Click **Computers > Groups >** and select **New Dynamic Group...**

2. Click **Admin > Groups >** and select **New Dynamic Group...**
3. Click Admin > Groups > Click the Group button and click New Dynamic Group...

A New Dynamic Group Wizard will appear. For more use cases how to create new Dynamic Group based on a Dynamic Group template with rules, see examples.

The Dynamic Group Templates section contains both pre-defined and custom templates based on different criteria. All templates are displayed in a list. Clicking an existing template allows you to edit it. To create a New Dynamic Group template, click New Template.
6.1.3 Assign Task to a Group

Click Admin > Groups > select Static or Dynamic group > next to the selected group, or click Group > + New task

The same can be done from Computers, select Static or Dynamic and click + New task. A New Client task wizard window will open.
6.1.4 Assign a policy to a group

After a policy is created, you can assign it to a Static or Dynamic Group. There are two ways to assign a policy:

1. Under Admin > Policies > select a policy and click Assign Group(s). Select a Static or Dynamic Group and click OK.

Select Group from the list.
2. Click **Admin > Groups > Group** or click the **icon next to the group name and select Manage Policies.**
In the **Policy application order** window click **Add Policy**. Select the check box next to the policy that you want to assign to this group and click **OK**. Click **Close**. To see what policies are assigned to a particular group, select that group and click the **Policies** tab to view a list of policies assigned to the group.

**NOTE**
For more information about policies, see the **Policies** chapter.

### 6.1.5 Static Groups

Static Groups are used to:

- Organize devices and create hierarchy of groups and subgroups
- Organize objects
- Serve as Home Groups for users

Static Groups can only be **created** manually. Devices can be moved manually into groups. Each computer or mobile device can belong only to one Static Group.

There are two default Static Groups:

- **All** - This is a main group for all devices in the ERA Server network. All objects created by the administrator are (by default) contained in this group. It is always displayed and cannot be renamed. Access to this group gives users access to all subgroups; therefore it should be distributed carefully.

- **Lost & Found** - A child group of group **All**. Each new computer that connects to the ERA Server for the first time is automatically displayed in this group. The group can be renamed or copied, but it can't be deleted or moved.

**IMPORTANT**
A static group can be deleted only if:

- The user has write permission on this group
- The group is empty
If there are still some objects in the static group, the delete operation will fail. There is an **Access Group** filter button located in each menu (for example, **Admin > Installers**) with objects.

Click **Select** to choose a static group—only objects contained in this group will then be listed in the view. With this filtered view, the user can easily manipulate objects from one group.

### 6.1.5.1 Static Group Wizard

Under **Computers > Groups** select one of the Static Groups, click the ☒ and then select **New Static Group**. You can create Static Groups in the **Group** section of the **Admin** tab, click the **Group** button or the ☒ next to the Static Group name.

#### Basic

Enter a **Name** and a **Description** for the new group. Optionally, you can change the **Parent group**. By default, the parent group is the group you selected when you started creating the New Static Group. If you want to change its parent group, click **Change Parent Group** and select a parent group from the tree. The parent of the New Static Group must be a Static Group. This is because it is not possible for a Dynamic Group to have Static Groups. Click **Finish** to create the New Static Group.
6.1.5.2 Manage Static Groups

Navigate to Admin > Groups and select the Static Group you want to manage. Click the Group button or the next to the Static Group name. A popover menu will open with available options:

**Static Group** actions:

- **New Static Group...** - This option becomes available if you click a Group in the list on the left. This group will be the default parent group, but you can change the parent group later when you create a new Static Group.

- **New Dynamic Group...**
  This option becomes available if you click a Group in the list on the left. This group will be the default parent group, but you can change the parent group later when you create a new Dynamic Group.

- **Edit...**
  Allows you to edit the selected Group. The same settings apply as when you create a new Group (static or dynamic).

- **Move...**
  You can select a group and move it as a subgroup of another group.

- **Delete**
  Removes the selected group completely.

- **Import**
  You can import a list (usually a text file) of computers as members of the selected group.

- **Export**
  Export members of the group (and subgroups, if selected) to a list (.txt file). This list can be used for review or imported later.

- **Add New...**
  Adds a computer to a Static Group.

- **Scan**
  Use this option to run the On Demand Scan task on the client that reported the threat.
Update Modules
Use this option will run the **Modules Update** task (triggers an update manually).

Mobile
- **Reenroll** - with this option, you can create new client task.
- **Find** - if you want to request the GPS coordinates of your mobile device.
- **Lock** - device will be locked when suspicious activity is detected or the device is marked as missing.
- **Unlock** - device will be unlocked.
- **Siren** - triggers a loud siren remotely, the siren will start even if your device is set to mute.
- **Wipe** - all data stored in your device will be permanently erased.

Run Task
Use this option to select **client tasks** to be executed on devices in this group.

New task...
This option immediately triggers an existing **task**, that you select from a list of available tasks. The trigger is not available for this task, because it will be executed immediately.

Last used tasks
List of last used **client tasks** for all groups and computers.

Manage Policies... - Assign a **policy** for the selected group.

6.1.5.3  Move Static Group
Click the symbol next to the group name and select **Move**. A pop-up window will be displayed showing the groups tree structure. Select the target group (static or dynamic) into which you want to move the selected group. The target group will become a parent group. You can also move groups by dragging and dropping a group into the target group of your choice.

**NOTE**
You cannot move a Static Group into a Dynamic Group. Also, it is not possible to move pre-defined Static Groups (for example, Lost & found) to any other group. Other groups can be moved freely. A Dynamic Group can be a member of any other group including Static Groups.

The following methods can be used when moving groups:

**Drag and drop** - click and hold the group you want to move and release it above new parent group.

- **Move** > select a new parent group from the list and click **OK**.
6.1.5.4 Import clients from Active Directory

To import clients from AD, create a new Server Tasks Static Group Synchronization.

Select a group to which you want to add new computers from the AD. Also select objects in the AD you want to synchronize from and what to do with duplicates. Enter your AD server connection settings and set the Synchronization mode to Active Directory/Open Directory/LDAP.
### 6.1.5.5 Export Static Groups

Exporting a list of computers that are in the ERA structure is simple. You can export the list and store it as a backup so that you can import the list back in the future, for example if you want to restore the group structure.

**NOTE**

Static groups need to contain at least one computer. Exporting empty groups is not possible.

1. Go to **Admin > Groups** > select a Static Group you want to export.

2. Click the **Group** button at the bottom (a context menu will pop-up).

3. Select **Export**.

4. The file will be saved in **.txt** format.

**NOTE**

Dynamic Groups cannot be exported because Dynamic Groups are only links to computers according to the criteria defined in Dynamic Group Templates.
6.1.5.6 Import Static Groups

Exported files from Static Groups can be imported back into ERA Web Console and included in your existing group structure.

1. Click **Group** (a context menu will pop-up).
2. Select **Import**.
3. Click **Browse** and navigate to the .txt file.
4. Select the group file and click **Open**. The file name is displayed in the text box.
5. Select one of the following options to resolve conflicts:
   - **Skip conflicting computers**
     If static Groups exist and computers from the .txt file already exist in this group, those computers are skipped and are not imported. Information about this is displayed.
   - **Move conflicting computers from other groups**
     If Static Groups exist and computers from the .txt file already exist in this group, it is necessary to move computers to other Static Groups prior to the import, after the import, these computers will be moved back into original groups where from they had been moved.
   - **Duplicate conflicting computers**
     If Static Groups exist and computers from the .txt file already exist in this group, duplicates of these computers are created in the same Static Group. The original computer is displayed with full information and the duplicate is displayed with its Computer name only.
5. Click **Import**, Static Groups and computers within will be imported.
6.1.6 Dynamic Groups

Dynamic Groups are in essence custom filters defined in Templates. Computers are filtered on the Agent side, so no extra information needs to be transferred to server. The Agent decides on its own which Dynamic Groups a client belongs to, and only notifies the server about this decision. Dynamic Groups have their rules defined in the Dynamic Group Template.

**NOTE**

If the client device is not connected (for example, it is turned off), its position in dynamic groups is not updated. After the device is connected again, its position in dynamic groups will be updated.

There are some pre-defined Dynamic Groups available after you have installed ESET Remote Administrator. If you need to, you can create custom Dynamic Groups. There are two way how to do that:

- create a template first and then create a Dynamic Group
- create a new Dynamic Group and new template on the fly

More than one Dynamic Group can be created from one template.

A user can use Dynamic Groups in other parts of ERA. It is possible to assign policies to them or prepare a task for all computers therein.

Dynamic Groups can be under Static Groups or Dynamic Groups. However, the topmost group is always static.

All the Dynamic Groups under a certain Static Group only filter computers of that Static Group no matter how deep they are in the tree. Moreover, for nested Dynamic Groups, a deeper Dynamic Group filters the results of the superior one.

Policies are applied as described here. However, once created, they can be moved freely across the tree.

**Dynamic Group actions**

Navigate to Admin > Groups and select the Dynamic Group you want to manage. Click the Group button or the next to the Dynamic Group name. A popover menu will open with available options:

- New Dynamic Group...
  This option becomes available if you click a Group in the list on the left. This group will be the default parent group, but you can change the parent group later when you create a new Dynamic Group.

- Edit...
  Allows you to edit the selected Group. The same settings apply as when you create a new Group (static or dynamic).

- Move...
  You can select a group and move it as a subgroup of another group.

- Delete
  Removes the selected group completely.

- New notification...
  With this option, you can create a new notification.

- Scan
  Use this option to run the On Demand Scan task on the client that reported the threat.

- Update Modules
  Use this option will run the Modules Update task (triggers an update manually).
Mobile
- **Reenroll** - with this option, you can create new client task.
- **Find** - if you want to request the GPS coordinates of your mobile device.
- **Lock** - device will be locked when suspicious activity is detected or the device is marked as missing.
- **Unlock** - device will be unlocked.
- **Siren** - triggers a loud siren remotely, the siren will start even if your device is set to mute.
- **Wipe** - all data stored in your device will be permanently erased.

Run Task

Use this option to select client tasks to be executed on devices in this group.

**New task...**

This option immediately triggers an existing task, that you select from a list of available tasks. The trigger is not available for this task, because it will be executed immediately.

**Last used tasks**

List of last used client tasks for all groups and computers.

**Manage Policies...** - Assign a policy for the selected group.

Use the **Apply sooner** and **Apply later** options to change priorities of Dynamic Groups according your needs.
6.1.6.1 Rules for a Dynamic Group template

When you set rules for a Dynamic Group template, you can use different operators for different conditions to achieve your desired scenario.

The following chapters explain rules and operations used in Dynamic Group templates:

- When does a computer become a member of a Dynamic Group?
- Operation description
- Rules and logical connectors
- Template Rules Evaluation
- How to create automation in ESET Remote Administrator
- Dynamic Group Templates
- Use cases - create a specific Dynamic Group template

### 6.1.6.1.1 When a computer is in Dynamic Group?

For a computer to become a member of a specific Dynamic Group, it must meet certain conditions. These conditions are defined in a Dynamic Group Template. Each template consists of one or several Rules. You can specify these rules when creating a new Template.

- Certain information about the current condition of a client computer is stored by the Agent. The computer's condition is evaluated by the Agent according to template rules.
- The set of conditions required for a client to join a Dynamic Group are defined in your Dynamic Group Templates, and clients are evaluated for inclusion in Dynamic Groups each time they check in to ESET Remote Administrator. When a client meets the values specified in a Dynamic Group template, it is automatically assigned to this group.
- Dynamic Groups can be seen as filters based on computer status. One computer may apply for more than one filter and, therefore, be assigned to more than one Dynamic Group. This makes Dynamic Groups different from Static Groups, because a single client cannot belong to more than one static group.

### 6.1.6.1.2 Operation description

If you specify multiple rules (conditions), you must select which operation should be used to combine the rules. Depending on the result, a client computer will or will not be added to a Dynamic Group which uses this Template.

**AND** - All defined conditions have to be true.
Checks if all conditions are evaluated positively – computer must meet all required parameters.

**OR** - At least one condition has to be true.
Checks if one of the conditions is evaluated positively – computer must meet one of the required parameters.

**NAND** - At least one condition has to be false.
Checks if one of the conditions cannot be evaluated positively – computer must not meet at least one parameter.

**NOR** - All conditions have to be false.
Checks if all conditions cannot be evaluated positively – computer doesn't meet all of required parameters.

**NOTE**
It is not possible to combine operations. Only one operation is used per Dynamic Group Template and applies to all its rules.
6.1.6.1.3 Rules and logical connectors

A rule consists of an item, logical connector (logical operator) and defined value.

When you click + Add rule a pop-up window will open with a list of items divided into categories. For example:

Installed software > Application name
Network adapters > MAC address
OS edition > OS name

To create a rule, select an item, choose a logical operator and specify a value. The rule will be evaluated according to the value you've specified and the logical operator used.

Acceptable value types include number(s), string(s), enum(s), IP address(es), product masks and computer IDs. Each value type has different logical operators associated with it and ERA Web Console will automatically show only supported ones.

- "= (equal)" - Symbol value and template value must match. Strings are compared without case sensitivity.
- "\ne (not equal)" - Symbol value and template value must not match. Strings are compared without case sensitivity.
- "> (greater than)" - Symbol value must be greater than template value. Can also be used to create a range comparison for IP address symbols.
- "\ge (greater or equal)" - Symbol value must be greater or equal to template value. Can also be used to create a range comparison for IP address symbols.
- "< (less than)" - Symbol value must be less than template value. Can also be used to create a range comparison for IP address symbols.
- "\le (less or equal)" - Symbol value must be less than or equal to template value. Can also be used to create a range comparison for IP address symbols.
- "contains" - Symbol value contains template value. Search is done without case sensitivity.
- "has prefix" - Symbol value has the same text prefix as template value. Strings are compared without case sensitivity. Set the first characters from your search string, for example, for "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", the prefix is "Micros" or "Micr" or "Microsoft" etc.
- "has suffix" - Symbol value has same text suffix as template value. Strings are compared without case sensitivity. Set the first characters from your search string, for example, for "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", the suffix is "319" or "0.30319", etc.
- "has mask" - Symbol value must match a mask defined in a template. Mask formatting allows any characters, the special symbols '*' - zero, one or many characters and '?' exactly one character, e.g.: "6.2." or "6.2.2033.2".
- "regex" - Symbol value must match the regular expression (regex) from a template. Regex must be written in Perl format.
- "in" - Symbol value must match any value from a list in a template. Strings are compared without case sensitivity.
- "in (string mask)" - Symbol value must match any mask from a list in a template.

Negative rules:

IMPORTANT
Negated operators must be used with care, because in the case of multiple line logs such as "Installed application", all lines are tested against these conditions. Please consult the included examples to see how negated operators or negated operations must be used to get expected results.

- "doesn't contain" - Symbol value does not contain template value. Search is done without case sensitivity.
- "doesn't have prefix" - Symbol value does not have the same text prefix as template value. Strings are compared without case sensitivity.
- "doesn't have suffix" - Symbol value does not have text suffix as template value. Strings are compared without case sensitivity.
- "doesn't have mask" - Symbol value must not match a mask defined in a template.
- "not regex" - Symbol value must not match a regular expression (regex) from a template. Regex must be written in Perl format. Negation operation is provided as a helper to negate matching regex-es without rewrites.
- "not in" - Symbol value must not match any value from the list in a template. Strings are compared without case sensitivity.
- "not in (string mask)" - Symbol value must not match any mask from a list in a template.
6.1.6.1.4 Template rules evaluation

Template rules evaluation is handled by ERA Agent, not ERA Server (only the result is sent to ERA Server). The evaluation process is happens according to the rules that are configures in a Template. The following is an explanation of the evaluation process with a few examples.

Status is a cluster of various information. Some sources provide more than one dimensional status per machine (for example, Operating System, RAM size, etc.), others provide multidimensional status information (for example, IP Address, Installed Application, etc).

Below is a visual representation of the status of a client:

<table>
<thead>
<tr>
<th>Network Adapters - IP Address</th>
<th>Network Adapters - MAC Address</th>
<th>OS Name</th>
<th>OS Version</th>
<th>HW - RAM size in MB</th>
<th>Installed Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>4A-64-3F-10-FC-75</td>
<td>Windows 7</td>
<td>6.1.7601</td>
<td>2048</td>
<td>ESET Endpoint Security</td>
</tr>
<tr>
<td>10.1.1.11</td>
<td>2B-E8-73-BE-81-C7</td>
<td></td>
<td></td>
<td></td>
<td>PDF Reader</td>
</tr>
<tr>
<td>124.256.25.25</td>
<td>52-FB-E5-74-35-73</td>
<td></td>
<td></td>
<td></td>
<td>Office Suite</td>
</tr>
</tbody>
</table>

Status is made of information groups. One group of data always provides coherent information organized into rows. The number of rows per group may vary.

Conditions are evaluated per group and per row - if there are more conditions regarding the columns from one group, only the values on the same row are considered.

**Example 1:**
For this example consider the following condition:

Network Adapters.IP Address = 10.1.1.11 AND Network Adapters.MAC Address = 4A-64-3F-10-FC-75

This rule matches no computer, as there is no such row where both conditions hold true.

<table>
<thead>
<tr>
<th>Network Adapters - IP Address</th>
<th>Network Adapters - MAC Address</th>
<th>OS Name</th>
<th>OS Version</th>
<th>HW - RAM size in MB</th>
<th>Installed Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>4A-64-3F-10-FC-75</td>
<td>Windows 7 Enterprise</td>
<td>6.1.7601</td>
<td>2048</td>
<td>ESET Endpoint Security</td>
</tr>
<tr>
<td>10.1.1.11</td>
<td>2B-E8-73-BE-81-C7</td>
<td></td>
<td></td>
<td></td>
<td>PDF Reader</td>
</tr>
<tr>
<td>124.256.25.25</td>
<td>52-FB-E5-74-35-73</td>
<td></td>
<td></td>
<td></td>
<td>Office Suite</td>
</tr>
</tbody>
</table>

**Example 2:**
For this example consider the following condition:

Network Adapters.IP Address = 192.168.1.2 AND Network Adapters.MAC Address = 4A-64-3F-10-FC-75

This time, both conditions matched cells on the same row and therefore, the rule as a whole is evaluated to TRUE. A computer is selected.
### Example 3:

For conditions with the OR operator (at least one condition must be TRUE), such as:

\[
\text{Network Adapters.IP Address = 10.1.1.11 OR Network Adapters.MAC Address = 4A-64-3F-10-FC-75}
\]

The rule is TRUE for two rows, as only either of the conditions must be satisfied. A computer is selected.

### 6.1.6.1.5 How to automate ESET Remote Administrator

By using techniques like the example shown below, you can automate a variety of actions, from product and OS updates, scanning, and automatic activations of newly added products with preselected licenses, to solving sophisticated incidents.

**WARNING**

This example should be performed only on clients without third-party security software or ESET security software from home segment (e.g. ESET Smart Security). The installation of ESET products on clients with third-party security software is not recommended. You can use ESET AV Remover to remove other antivirus programs from your computer.

**EXAMPLE**: How to automatically deploy ESET products on newly connected Windows desktops

1. **Create a Dynamic Group**, called *Without security product*.
   a. Make it a child group of the pre-defined group *Windows computers > Windows (desktops)*.
   b. Click **New Template**.
   c. Add the following rule: **Computer > Managed product mask**.
   d. As operator select **not equal**.
   e. Select the mask **ESET protected: Desktop**.
   f. Click **Finish** to save the group.

2. Navigate to **Admin > Client tasks > ESET Security Product > Software Install**.
a. Click **New** and give the task a **Name**.
b. Choose the package in the **Settings** section and set other parameters if needed.
c. Click **Finish > Create Trigger**.
d. In the **Target** section, click **Add Groups** and select **Without security product**.
e. In the **Trigger** section, select **Joined Dynamic Group Trigger**.
f. Click **Finish** to save the task and the trigger.

This task will be executed on clients connected to the dynamic group since this moment. You will need to execute this task manually on clients which were in the dynamic group before the task was created.

**EXAMPLE: How to enforce location-based policy**

1. **Create a Dynamic Group** called *Subnetwork 120*.
   a. Make it a child group of the *All* group.
   b. Click **New Template**.
   c. Add rule: **Network IP addresses > IP subnetwork**.
   d. As operator select **equal**.
   e. Enter the subnetwork you want to filter, for example, 10.1.120.0 (the last number has to be 0 to filter all the IP addresses from the 10.1.120. subnetwork).
   f. Click **Finish** to save the group.

2. Navigate to **Admin > Policies**.
   a. Click **New policy** and give the policy a **Name**.
   b. In the **Settings** section, select **ESET Remote Administrator Agent**.
   c. Make the policy change; for example, change the **Connection interval** to 5 minutes.
   d. In the **Assign** section, click **Assign** and select the check box next to your group *Subnetwork 120* and click **OK** to confirm.
   e. Click **Finish** to save the policy.

This policy will be applied on clients connected to the dynamic group since this moment.

**WARNING**

When the client machine leaves the dynamic group (conditions matching the dynamic group membership are not valid anymore) settings will stay applied unless there is another policy applied on the same set of settings.

### 6.1.6.2 Dynamic Group Wizard

Every Dynamic Group uses a Template to filter client computers. Once defined, a template can be used in other Dynamic Group to filter clients. ERA includes several default Dynamic Group templates out-of-the-box to make it easy to categorize client computers.

**NOTE**

A user needs access permissions to be able to work with Dynamic Group templates. All pre-defined templates are located in static group *All* and are by default available only to the administrator. Other users need to be **assigned with additional permissions**; otherwise, the templates can be moved to a group where the users have permissions.

You can create Dynamic Groups using an existing Template or a new template (which will then be used for this Dynamic Group).

**Basic**

Enter a **Name** and **Description** (optional) for the new Dynamic Group. By default, the parent group is the group you selected when you started creating the new static group. If you want to change its parent group, you can still do so by clicking **Change Parent Group** and selecting one from the tree. The parent of the New Dynamic Group can be Dynamic or Static. Click **Finish** to create the new Dynamic Group.
You can either select an existing Dynamic Group template or create a new Dynamic Group template.

Review the configuration to make sure it is correct (if you need to make changes, you can still do so) and click Finish.

6.1.6.3 Dynamic Group Templates

Dynamic group templates establish the criteria computers must meet to be placed in a Dynamic group. When these criteria are met by a client, a client will automatically be moved into the appropriate Dynamic Group.

- Create New Dynamic Group Template
- Manage Dynamic Group Template
- Rules for a Dynamic Group Template
- Dynamic Group Template - examples
6.1.6.3.1 New Dynamic Group Template

Click New Template under Admin > Dynamic Group Templates.

**Basic**

Enter a Name and a Description for the new Dynamic Group template.

**Expression**

See our examples with illustrated step-by-step instructions for samples of how to use Dynamic Groups on your network.

**Summary**

Review the configured settings and click Finish to create the template. This new template will be added to the list of all templates, and can be used later to create a new Dynamic Group.
6.1.6.3.2 Create Dynamic Group

To create a new Dynamic Group, follow the steps below:

1. Click the next to the Dynamic Group name and then click **New Dynamic Group**. Alternatively, the **New Dynamic Group** is accessible from **Admin > Groups**. Select a group (in the **Groups** pane) and click **Group** at the bottom.

2. A **Dynamic Group Wizard** will appear. Enter a name and description (optional) for the new template.

3. You can change the parent group by clicking **Change Parent Group**.
4. Expand **Template**.

- If you want to create the group from pre-defined template, or from a template you have *already created*, click **Choose existing** and select the appropriate template from the list.
- If you have not created any templates and none of the pre-defined templates in the list suit you, click **New** and follow the steps to create a **new template**.
6.1.6.3 Manage Dynamic Group Templates

Templates can be managed from Admin > Dynamic Group Templates. You can either create a New Template or edit an existing one. To edit, select the template you want to edit and a wizard will open. Alternatively, you can select a template by selecting the check box next to it and then clicking Edit Template. Duplicate lets you create new Dynamic Group Templates based on the selected templates. A new name will be required for the duplicate task.

**IMPORTANT**
Due to the new security model in ESET Remote Administrator 6.5, managing Dynamic Group Templates requires sufficient permissions. All pre-defined templates are stored by default in the All static group. For duplication of a template, the user has to be assigned write permissions (for Dynamic Group templates) for the group where the source template is located and for the user’s home group (where the duplicate will be stored). See the similar example.

![Dynamic Group Templates screenshot]

Click Save as if you want to keep your existing template and create a new one based on the template you are editing. When prompted, specify the name for your new template.

**Save dynamic group template as**

New dynamic group template’s name

```
Operating system is MS Windows
```
6.1.6.3.4 Move Dynamic Group

Click the symbol next to the group name and select Move. A pop-up window will be displayed showing the groups tree structure. Select the target group (static or dynamic) into which you want to move the selected group. The target group will become a parent group. You can also move groups by dragging and dropping a group into the target group of your choice.

**NOTE**
You cannot move a Static Group into a Dynamic Group. Also, it is not possible to move pre-defined Static Groups (for example, Lost & found) to any other group. Other groups can be moved freely. A Dynamic Group can be a member of any other group including Static Groups.

The following methods can be used when moving groups:

**Drag and drop** - click and hold the group you want to move and release it above new parent group.

![Drag and drop example](image)

**> Move** > select a new parent group from the list and click OK.

![Select new parent group](image)

**> Edit** > select Change parent group.

![Edit example](image)

**NOTE:** The Dynamic Group in a new position starts to filter computers (based on the template) without any relation to its previous location.
6.1.6.3.5  Dynamic Group template - examples

The sample Dynamic Group templates in this guide demonstrate some of the ways you can use Dynamic Groups to manage your network:

- **Dynamic Group that detects if a security product is installed**
- **Dynamic Group that detects if a specific version of a software is installed**
- **Dynamic Group that detects if a specific version of software is not installed**
- **Dynamic Group that detects if a specific version of software is not installed but another version exists**
- **Dynamic Group that detects if a computer is in a specific subnet**
- **Dynamic Group that detects installed but not activated versions of server security products**

There are, of course, many other objectives that can be achieved using Dynamic Groups Templates with a combination of rules. The possibilities are almost endless.

6.1.6.3.5.1  Dynamic Group - a security product is installed

This Dynamic Group can be used to execute task immediately after ESET security product is installed on a machine: Activation, Custom scan, etc.

**NOTE**

It is also possible to specify `operator "not in"` or `operation NAND` to negate the condition. As the Manage product mask itself is one line log, both will work.

You can create a **New Template** under **Admin > Dynamic Group Templates** and create a **new Dynamic Group with template** or create a **new Dynamic Group** using an existing or new template.

- **Basic**
  
  Enter a **Name** and a **Description** for the new Dynamic Group template.

- **Expression**
  
  Select a logical operator in the **Operation** menu: **AND** (All conditions have to be true).

  - Click + **Add Rule** and select a **condition**. Select **Computer > Managed products mask > in > ESET protected: Desktop**. You can also choose different ESET products.

- **Summary**
  
  Review the configured settings and click **Finish** to create the template. This new template will be added to the list of all templates, and can be used later to create a new Dynamic Group.
6.1.6.3.5.2 Dynamic Group - a specific software version is installed

This Dynamic Group can be used to detect installed ESET security software on a machine. Then you will be able to execute for example upgrade task or run custom command on those machines. Different operators like "contains" or "has prefix" can be used.

Click New Template under Admin > Dynamic Group Templates.

- Basic
  - Enter a Name and a Description for the new Dynamic Group template.
  - Expression
    - Select a logical operator in the Operation menu: AND (All conditions have to be true).
    - Click + Add Rule and select a condition:
      - Installed software > Application name > = (equal) > ESET Endpoint Security
      - Installed software > Application version > = (equal) > 6.2.2033.0
  - Summary
    - Review the configured settings and click Finish to create the template. This new template will be added to the list of all templates, and can be used later to create a new Dynamic Group.

6.1.6.3.5.3 Dynamic Group - a specific version of a software is not installed at all

This Dynamic Group can be used to detect missing ESET security software on a machine. The settings from this example will include machines that do not contain the software at all or machines with different versions than one specified.

This group is useful because you will be able to execute software installation task on those computers to either install or upgrade. Different operators like "contains" or "has prefix" can be used.

Click New Template under Admin > Dynamic Group Templates.

- Basic
  - Enter a Name and a Description for the new Dynamic Group template.
  - Expression
    - Select a logical operator in the Operation menu: NAND (At least one condition has to be false).
    - Click + Add Rule and select a condition:
      - Installed software > Application name > = (equals) > "ESET Endpoint Security"
      - Installed software > Application version > = (equals) > "6.2.2033.0"
  - Summary
    - Review the configured settings and click Finish to create the template. This new template will be added to the list of all templates, and can be used later to create a new Dynamic Group.
6.1.6.3.5.4 Dynamic Group - a specific version of a software is not installed but other version exists

This Dynamic Group can be used to detect software that is installed but with different version than you are requesting. This group is useful because you will be able to execute upgrade tasks on those machines where the required version is missing. Different operators can be used but make sure that version testing is done with negated operator.

Click New Template under Admin > Dynamic Group Templates.

Basic

Enter a Name and a Description for the new Dynamic Group template.

Expression

- Select a logical operator in the Operation menu: AND (All conditions have to be true).

- Click + Add Rule and select a condition:
  - Installed software > Application name > = (equals) > "ESET Endpoint Security"
  - Installed software > Application version > ≠ (not equal) > "6.2.2033.0"

Summary

Review the configured settings and click Finish to create the template. This new template will be added to the list of all templates, and can be used later to create a new Dynamic Group.

6.1.6.3.5.5 Dynamic Group - a computer is in specific subnet

This Dynamic Group can be used to detect specific subnet. Then it can be used to apply custom policy for web control or update. You can specify different ranges.

Click New Template under Admin > Dynamic Group Templates.

Basic

Enter a Name and a Description for the new Dynamic Group template.

Expression

- Select a logical operator in the Operation menu: AND (All conditions have to be true).

- Click + Add Rule and select a condition:
  - Network IP addresses > Adapter IP address > ≥ (greater or equal) > "10.1.100.1"
  - Network IP addresses > Adapter IP address > ≤ (less or equal) > "10.1.100.254"
  - Network IP addresses > Adapter subnet mask > = (equal) > "255.255.255.0"

Summary

Review the configured settings and click Finish to create the template. This new template will be added to the list of all templates, and can be used later to create a new Dynamic Group.
This Dynamic Group can be used to detect inactive server products. Once these products are detected, you can assign a Client Task to this group to activate client computers with proper license. In this example only EMSX is specified, but you can specify multiple products.

Click **New Template** under **Admin > Dynamic Group Templates**.

**Basic**

Enter a Name and a Description for the new Dynamic Group template.

**Expression**

- Select a logical operator in the **Operation** menu: AND (All conditions have to be true).
- Click + Add Rule and select a condition:
  - Computer > Managed products mask > in > "ESET protected: Mail Server"
  - Functionality/Protection problems > Source > = (equals) > "Security product"
  - Functionality/Protection problems > Problem > = (equals) > "Product not activated"

**Summary**

Review the configured settings and click **Finish** to create the template. This new template will be added to the list of all templates, and can be used later to create a new Dynamic Group.

### 6.2 User Management

This section allows you to manage Users and User Groups for the purpose of iOS Mobile Device Management. Mobile Device Management is conducted with the use of policies assigned to iOS devices. However, we recommend that you synchronize Users with Active Directory first. Then you can modify users or add Custom Attributes.

**IMPORTANT**

User Management is different from **Access Rights**. To manage ERA users and permission sets navigate to **Admin > Access Rights**.

- User highlighted in orange have no device assigned to them. Click the user, select Edit... and click Assigned Computers to view details for that user. Click Add computers to assign computers or device(s) to this user.

<table>
<thead>
<tr>
<th>USER NAME</th>
<th>USER DESCRIPTION</th>
<th>EMAIL ADDRESS</th>
<th>PHONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amanda</td>
<td></td>
<td><a href="mailto:amanda@company.com">amanda@company.com</a></td>
<td></td>
</tr>
</tbody>
</table>

No computers assigned. Please assign some computers to this user in order to use personalized iOS policies.
- You can also add or remove **Assigned users** from within Computers details. When you are in Computers or Groups, select a computer or mobile device and click **Show Details**. The user can be assigned to more than one computer/mobile device. You can also use 🏷 Assign User... to assign a user directly to selected device/s.

- You can filter the users using the filter at the top of the page, click **Add Filter** and select an item from the list.

**User management actions:**
Show Details
The user details menu displays information such as Email Address, Office or Location, Custom Attributes and Assigned Computers. The user can have more than one assigned computer/mobile device. You can change the user’s Name, Description or Parent group. Custom Attributes shown here are the ones that can be used when creating policies.

Click on the user to open drop-down menu to execute actions. Refer to Icon legend for details about actions.
6.2.1 Add New Users

Click Admin > User Management > Add Users... to add users that were not found or added automatically during User Synchronization.
Type the name of the User you want to add into the User Name field. Use the Conflict Resolution drop-down menu to select the action to take if a user you are adding already exists in ERA:

- **Ask when conflicts are detected**: When a conflict is detected, the program will ask you to select an action (see the options below).
  - **Skip conflicting users**: Users with the same name will not be added. This also ensures that existing user's custom attributes in ERA will be preserved (not overwritten with the data from Active Directory).
  - **Overwrite conflicting users**: Existing user in ERA is overwritten by the user from Active Directory. If two users have the same SID, the existing user in ERA is removed from its previous location (even if the user was in a different group).

Click + Add to add additional users. If you want to add multiple users at once, click Import CSV to upload a csv file containing a list of users to be added. Optionally, you can enter a Description of the users for easier identification.

Click Add when you are finished making changes. Users will appear in the parent group that you specified.
6.2.2 Edit Users

You can modify a user's details such as Basic information, Custom Attributes and Assigned Computers.

**NOTE**

When performing a User synchronization task for users that have custom attributes defined, set User creation collision handling to Skip. If you do not, user data will be overwritten by data from your Active Directory.

#### Basic

If you have used a User synchronization task to create the user and some fields are blank, you can specify these manually as required.

#### Custom Attributes

You can edit existing Custom Attributes or add new attributes. To add new ones, click Add New and select from the categories:

- **Wi-Fi Accounts**: Profiles can be used to push corporate Wi-Fi settings directly to managed devices.
- **VPN Accounts**: You can setup a VPN along with the credentials, certificates, and other required information to make the VPN readily accessible for users.
- **Email Accounts**: This is used for any email account that uses IMAP or POP3 specifications. If you use an Exchange server, use the Exchange ActiveSync settings below.
- **Exchange Accounts**: If your company utilizes Microsoft Exchange, you can create all the settings here to minimize the setup time for your users' access to mail, calendar, and contacts.
- **LDAP (Attribute Alias)**: This is especially useful if your company utilizes LDAP for contacts. You can map the contact fields to the corresponding iOS contact fields.
- **CalDAV**: This contains the settings for any calendar that uses the CalDAV specifications.
- **CardDAV**: For any contacts that are synced through the CardDAV specification, the information for syncing can be established here.
- **Subscribed Calendars**: If any CalDAV calendars are setup, this is where you can define read-only access to others' calendars.
Some of the fields will become an attribute which can then be used when creating a policy for iOS mobile device as a variable (placeholder). For example, Login ${exchange_login/exchange} or Email Address ${exchange_email/exchange}.

**Assigned Computers**

Here you can select individual Computers/Mobile devices. To do so, click **Add Computers** - all Static and Dynamic Groups with their members will be listed. Use check boxes to make your selection and click **OK**.
6.2.3 Create New User Group

Click Admin > User Management > + New User Group...

**Basic**

Enter a Name and Description (optional) for the new User Group. By default, the parent group is the group you selected when you started creating the new User Group. If you want to change its parent group, click Change Parent Group and select a parent group from the tree. Click Finish to create the new User Group.

You can assign specific permissions to this User Group from within Access Rights using Permission Sets (see User Groups section). This way, you can specify which specific ERA Console users can manage which specific User Groups. You can even restrict access for such users to other ERA functions, if desired. These users will then manage User Groups only.

6.3 Installers

This section allows you to create Agent installer packages to deploy ERA Agent on client computers. The installer packages are saved in ERA Web Console and you can edit and download them again when necessary.

1. Click Admin > Installers > Create installer.
2. Select the installer type you want to create. The options are as follows:

   - **All-in-one installer package**
     Follow the steps from Package creation to configure the All-in-one installer, which allows advanced configuration options. These options include Policy settings for ERA Agent and ESET products, ERA Server Hostname and Port, and the ability to select a Parent Group.

     **NOTE**
     After creating and downloading the All-in-one installer package, there are two options for deploying the ERA Agent:
     - Locally on a client computer
     - Using the Deployment tool to deploy ERA Agents to multiple client computers at the same time.
Agent live installer

Follow the steps from Package creation to configure the installer. This type of Agent deployment is useful when the remote and local deployment options do not suit you. In such cases, you can distribute the Agent Live Installer via email and let the user deploy it. You can also run the Agent Live Installer from removable media (a USB flash drive, for example).

GPO or SCCM

Access Group Filter

The Access Group filter button enables users to select a static group and filter viewed objects according to the group where they are contained.

Installers and permissions

A user can create or edit installers contained in groups where the user has Write permission for Stored Installers.

**NOTE**

- Keep in mind that the user will be able to work with Certificates when creating installers. A user must be assigned Use permission for Certificates with access to the static group where certificates are contained. If a user wants to deploy ERA Agent, that user must have Use permissions for the Certification Authority that the actual server certificate is signed by. For information on how to divide access to Certificates and Certification Authority, read this example.

- A user needs to be assigned Use permission for Policies that are selected in Advanced > Initial installer configuration > Configuration type when creating an All-in-one installer, GPO installer or SCCM script.

- A user needs to be assigned Use permission for Licenses if the license for static group is specified.

**EXAMPLE: How to allow user to create installers**

Administrator wants to allow user John to create or edit new installers in John’s Group. Administrator has to follow these steps:

1. Create new Static Group called John’s Group

2. Create a new Permission set
   
   a. name it Permissions for John - Create Installers
   
   b. add the group John’s Group in the section Static Groups
   
   c. in the Functionality section, select
      
      - Write for Stored Installers
      
      - Use for Certificates
      
      - Write for Groups & Computers
      
   d. click Finish to save the permission set

3. Create a new Permission set
   
   a. name it Permissions for John - Certificates
   
   b. add the group All in the section Static Groups
   
   c. in Functionality section select Use for Certificates.

   d. click Finish to save the permission set

These permissions are the minimal requirements for full (create and edit) installer usage.

4. Create a new User
a. name it John
b. in the Basic section select John’s Group as the Home Group
c. set the password to user John
d. in Permission Sets section select Permissions for John - Certificates and Permissions for John - Create Installers
e. click Finish to save the user

---

How to download installers from the installers menu

1. Click Admin > Installers.
2. Select the check box next to the installer you want to download.
3. Click Download and choose the correct version of installation package.

How to edit installers from the installers menu

1. Click Admin > Installers.
2. Select the check box next to the installer you want to edit.
3. Click Actions > Edit to modify the installer package.
6.4 Quarantine

This section shows all files quarantined on client devices. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them, or if they are being falsely detected by an ESET product.

You can Delete the quarantined file or Restore it to its previous location. You can use Restore with Exclusion to prevent the file to be reported by the ESET product again.

There are two ways to access Quarantine:

1. Admin > Quarantine.
2. Computer details > Threats and quarantine > Quarantine tab.

If you click on an item in the Quarantine section you will open Quarantine Management menu.

- **Show Details** - Displays the source device, threat name and type, object name with full file path, hash, size, etc.
- **Computers** - Opens Computers section with filtered devices connected with the quarantined file.
- **Delete** - Removes the file from quarantine and the affected device.
- **Restore** - Restores the file to its original location.
- **Restore and Exclude** - Restores the file to its original location and excludes it from scanning.
- **Upload** - Opens Upload Quarantined File task.

**IMPORTANT**

The Upload function is recommended only for experienced users. If you want to investigate the quarantined file more, you can Upload it to a shared directory.
6.5 Policies

Policies are used to push specific configurations to ESET products running on client computers. This allows you to avoid configuring each client’s ESET product manually. A policy can be applied directly to individual Computers as well as groups (Static and Dynamic). You can also assign multiple policies to a computer or a group, unlike in ESET Remote Administrator 5 and earlier where it was only possible to apply one policy to one product or component.

Policies and permissions

The user must have sufficient permissions to create and assign policies. Permissions needed for certain Policies actions:

- To read the list of policies and their configuration a user needs Read permission.
- To assign policies to targets, a user needs Use permission.
- To create, modify or edit policies, a user needs Write permission.

See the list of permissions for more information on access rights.

**EXAMPLE**

- If user John needs only to read policies created by himself, Read permission for Policies are needed.
- If user John wants to assign certain policies to computers, he needs Use permission for Policies and Use permission for Groups and Computers.
- To allow John full access for policies, Administrator must set Write permission for Policies.

Policy application

Policies are applied in the order that Static Groups are arranged. This is not true for Dynamic Groups, where child Dynamic Groups are traversed first. This allows you to apply policies with greater impact at the top of the Group tree and apply more specific policies for subgroups. Using flags, an ERA user with access to groups located higher in the tree can override the policies of lower groups. The algorithm is explained in detail in How Policies are applied to clients.

Merging policies

A policy applied to a client is usually the result of multiple policies being merged into one final policy.

**NOTE**

We recommend that you assign more generic policies (for example, the update server) to groups that are higher within the group tree. More specific policies (for example, device control settings) should be assigned deeper in the group tree. The lower policy usually overrides the settings of the upper policies when merged (unless defined otherwise using policy flags).

**NOTE**

When you have a policy in place and decide to remove it later on, the configuration of the client computers will not automatically revert back to their original settings once the policy is removed. The configuration will remain according to the last policy that was applied to the clients. The same thing happens when a computer becomes a member of a Dynamic Group to which a certain policy is applied that changes the computer’s settings. These settings remain even if the computer leaves the Dynamic Group. Therefore, we recommend that you create a policy with default settings and assign it to the root group (All) to have the settings revert to defaults in such a situation. This way, when a computer leaves a Dynamic Group that changed its settings, this computer will revert to default settings.
6.5.1 Policies Wizard

Policies are grouped/categorized by ESET product. Click to expand a category and see available policies. Built-in policies contain predefined policies and custom policies list categories of all the policies you’ve manually created.

Use policies to configure your ESET product the same way you would from within the Advanced setup window of the product GUI. Unlike policies in Active Directory, ERA policies cannot carry any script or series of commands. Type to search for an item in Advanced setup (for example, HIPS). All HIPS settings will be displayed. When you click the icon in the upper right corner, an Online Help page for the particular setting will be displayed.

Access Group Filter

The Access Group filter button enables users to select a static group and filter viewed objects according to the group where they are contained.

Create new policy

1. Click Admin > Policies > New Policy.
2. Enter basic information about the policy, such as a name and description (optional).
3. Select the correct product in the Settings section.
4. Use flags to add settings that will be handled by the policy.
5. Specify the clients that will receive this policy. Click Assign to display all Static and Dynamic Groups and their members. Select the computer that you want to apply a policy on and click OK.
6. Review the settings for this policy and click Finish.
6.5.2 Flags

When merging policies, you can change the behavior by using policy flags. Flags define how a setting will be handled by the policy.

For each setting, you can select one of the following flags:

- **Not apply** - Any setting with this flag is not set by policy. Because the setting is not forced, it can be changed by other policies later on.

- **Apply** - Settings with this flag will be sent to the client. However, when merging policies, it can be overwritten by a later policy. When a policy is applied to a client computer and a particular setting has this flag, that setting is changed regardless of what was configured locally on the client. Because the setting is not forced, it can be changed by other policies later on.

- **Force** - Settings with the Force flag have priority and cannot be overwritten by a later policy (even if the later policy has a Force flag). This assures that this setting won't be changed by later policies during merging.

To make navigation easier, all rules are counted. The number of rules you have defined in a particular section will be displayed automatically. Also, you'll see a number next to the category names in the tree on the left. This shows a sum of rules in all its sections. This way, you'll quickly see where and how many settings/rules are defined.

You can also use the following suggestions to make policy editing easier:

- Use to set the Apply flag to all items in a current section
- Use to delete rules applied to the items in the current section

**EXAMPLE: How can Administrator allow users to see all policies**

Administrator wants to allow user John to create or edit policies in his home group and allow John to see policies that are created by Administrator. Policies created by Administrator include Force flags. User John can see all policies, but cannot edit policies created by Administrator because Read permission for Policies with access to Static Group All is set. User John can create or edit policies in his Home Group San Diego. Administrator has to follow these steps:

**Create environment**
1. Create a new Static Group called San Diego.
2. Create new Permission set called Policy - All John with access to Static Group All and with Read permission for Policies.
3. Create a new Permission set called Policy John with access to Static Group San Diego, with functionality access Write permission for Group & Computers and Policies. This permission set allows John to create or edit policies in his Home Group San Diego.

**Create policies**
5. Create new policy All- Enable Firewall, expand Settings section, select ESET Endpoint for Windows, navigate to Personal Firewall > Basic and apply all settings by Force flag. Expand the Assign section and select Static Group All.
6. Create new policy John Group- Enable Firewall, expand Settings section, select ESET Endpoint for Windows, navigate to Personal Firewall > Basic and apply all settings by Apply flag. Expand the Assign section and select Static Group San Diego.

**Result**

Policies created by Administrator will be applied first because of Force flag usage. Settings with the Force flag have priority and cannot be overwritten by a later policy. Then policies created by user John will be applied.
Navigate to Admin > Groups > San Diego, click the computer and select Show details. In Configuration > Applied policies is the final policy application order.

<table>
<thead>
<tr>
<th>POLICY ORDER</th>
<th>POLICY PRODUCT</th>
<th>POLICY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (applied first)</td>
<td>ESET Endpoint for Windows</td>
<td>All - Enable firewall</td>
</tr>
<tr>
<td>2</td>
<td>ESET Endpoint for Windows</td>
<td>San Diego - Enable firewall</td>
</tr>
</tbody>
</table>

The first policy is created by Administrator and the second created by user John.

6.5.3 Manage Policies

Policies are grouped/categorized by ESET product. Click to expand a category and see available policies. Built-in policies contain predefined policies and custom policies list categories of all the policies you've manually created or modified.

Actions available for policies:

- **New**
  Function used to create a new policy.

- **Edit**
  Function used to modify an existing policy.

- **Duplicate**
  Function used to create a new policy based on an existing policy you have selected. Duplicate policy requires a new name.

- **Assign**
  Function used to assign a policy to a group or a client.

- **Delete**
  Function used to delete a policy.

- **Import**
  Click Policies > Import, click Choose File and browse for the file you want to import. To select multiple policies, see Modes below.

- **Export**
  Select a policy you want to export from the list and click Policies > Export. The policy will be exported to a .dat file. To export multiple policies, change the select mode (see Modes below).

- **Access group**
  Function used to move a policy to another group.

You can use Modes to change select mode (Single or Multiple). Click the ▾ arrow in upper right corner and choose from the context menu:

- Single select mode - you can select single item.
- Multiple item select mode - lets you use the check boxes to select multiple items.
- Refresh - reloads/refreshes displayed information.
- Expand All - Lets you display all information.
- Collapse All - Lets you hide all information.
6.5.4 How Policies are applied to clients

Groups and Computers can have several policies assigned to them. Moreover, a Computer can be in a deeply nested Group, the parents of which have their own policies.

The most important thing for the application of policies is their order. This is derived from the Group order and order of policies assigned to the Group.

Follow the steps below to determine the active policy for any client:

1. Find the order of groups in which the client resides
2. Replace groups with assigned Policies
3. Merge Policies to get final settings

6.5.4.1 Ordering Groups

Policies can be assigned to groups, and are applied in a specific order. Rules written below determine in which order policies are applied to clients.

1. Rule 1: Static Groups are traversed from the root Static Group (All).
2. Rule 2: On every level, the Static Groups of that level are traversed first in the order they appear in the tree (this is also called "breadth-first" search).
3. Rule 3: After all Static Groups at a certain level are accounted for, Dynamic Groups are traversed.
4. Rule 4: In every Dynamic Group, all its children are traversed in the order that they appear in the list.
5. Rule 5: At any level of a Dynamic Group, any child will be listed and searched for its children. When there are no more children, the next Dynamic Groups at the parent level are listed (this is also called "depth-first" search).

IMPORTANT
The policy is applied to the computer. This means that traversal ends at the computer which you want to apply the policy on.
Using the rules written above, the order in which policies will be applied on individual computers would be as follows:

<table>
<thead>
<tr>
<th>PC1</th>
<th>PC2</th>
<th>PC3</th>
<th>PC4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ALL</td>
<td>1. ALL</td>
<td>1. ALL</td>
<td>1. ALL</td>
</tr>
<tr>
<td>2. SG1</td>
<td>2. SG1</td>
<td>2. SG2</td>
<td>2. SG2</td>
</tr>
<tr>
<td>3. PC1</td>
<td>3. DG1</td>
<td>3. SG3</td>
<td>3. SG3</td>
</tr>
<tr>
<td></td>
<td>4. PC2</td>
<td>4. PC3</td>
<td>4. PC3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5. DG4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5. DG5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5. DG6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6. PC4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7. PC4</td>
</tr>
</tbody>
</table>
6.5.4.2 Enumerating Policies

Once the order of Groups is known, the next step is to replace each group with the policies assigned to it. Policies are listed in the same order as they are assigned to a Group. It is possible to edit the priority of policies for a group with more policies assigned. Each policy configures only one product (ERA Agent, ERA Proxy, EES, etc.).

**NOTE**
A group without a policy is removed from the list.

We have 3 policies applied to both static and Dynamic Groups (see picture below):

![Diagram showing policy assignments to groups]

The order in which policies will be applied on the Computer. The list below displays groups and policies applied on them:

1. All -> removed, no Policy here
2. SG 2 -> Policy 1, Policy 2
3. SG 3 -> removed for no Policy
4. DG 1 -> Policy 1, Policy 2
5. DG 3 -> removed, no Policy
6. DG 2 -> Policy 3
7. DG 4 -> removed, no Policy
8. DG 5 -> removed, no Policy
9. DG 6 -> removed, no Policy
10. Computer -> removed, no Policy

The final list of policies is:

1. Policy 1
2. Policy 2
3. Policy 1
4. Policy 2
5. Policy 3
6.5.4.3 Merging Policies

Policies are merged one by one. When merging policies, the general rule is that the later policy always replaces the settings set by the former one. To change this behavior, you can use policy flags (available for every setting). Some settings have another rule (replace / append / prepend) you can configure.

Keep in mind that the structure of the groups (their hierarchy) and the sequence of the policies determines how the policies are merged. Merging of any two policies may have different results depending on their order.

When creating policies, you will notice that some settings have additional rules that you can configure. These rules allow you to arrange the same settings in various policies.

- **Replace**: The default rule which is used when merging policies. It replaces the settings set by the former policy.
- **Append**: When applying the same setting in more than one policy, you can append the settings with this rule. The setting will be placed at the end of the list that was created by merging policies.
- **Prepend**: When applying the same setting in more than one policy, you can prepend the settings with this rule. The setting will be placed at the beginning of the list that was created by merging policies.

**NOTE**
- In ERA version 6.4 and earlier, Replace is the default and only available rule.
- In ERA version 6.5, settings which do not allow you to select one of the rules listed above have the default rule Replace.
6.5.4.3.1 Example scenario of merging policies

This example describes:

- Instructions on how to apply policy settings to ESET Endpoint security products
- How policies are merged when applying flags and rules

In situations where the Administrator wants to:

- Allow access for Marketing department to the websites www.forbidden.uk, www.deny-acces.com

...the Administrator has to follow these steps:

1. Create a new static group San Diego office and then Marketing department as a subgroup of static group San Diego office.
2. Navigate to Admin > Policy and create a new policy as follows:
   a) Called San Diego office
   b) Expand Settings and select ESET Security Product for Windows
   c) Navigate to Web and Mail > Web access protection > URL Address Management
   d) Click the button to Apply policy and edit Address list by clicking Edit
   e) Click List of blocked addresses and select Edit.
   g) Expand Assign and assign the policy to San Diego office and its subgroup Marketing department
   h) Click Finish to save the policy

This policy will be applied to San Diego office and Marketing department and will block the websites as shown below.
3. Navigate to Admin > Policy and create new policy:
   a) Called Marketing department
   b) Expand Settings and select ESET Security Product for Windows
   c) Navigate to Web and Mail section > Web access protection > URL Address Management
   d) Click the button to Apply policy, select the Append rule and then edit the Address list by clicking Edit. Rule Append causes that the Address list will be placed at the end when merging policies.
   e) Click List of allowed addresses > Edit.
   f) Add the following web addresses: www.forbidden.uk, www.deny-acces.com. Save the list of blocked addresses and then address list.
   g) Expand Assign and assign the policy to Marketing department
   h) Click Finish to save the policy

This policy will be applied to Marketing department and will allow access to the websites as shown below.
4. The final policy will include both policies applied to *San Diego office* and *Marketing Department*. Open **Endpoint Security product** and navigate to **Setup > Web and email > Advanced setup**, select the **Web and email** tab > **Web access protection** and expand **URL address management**. The final Endpoint product configuration will be shown.

The final configuration includes:

1. Address list of *San Diego office* policy
2. Address list of *Marketing department* policy
6.5.5 Configuration of a product from ERA

You can use policies to configure your ESET product the same way you would from within the Advanced setup window of the product GUI. Unlike policies in Active Directory, ERA policies cannot carry any script or series of commands.

For ESET security products of version 6+ there are options under **User Interface > User Interface Elements > Statuses** with two properties:

- **Show** - status is reported on the client GUI
- **Send** - status is reported to ERA

Examples of policy usage to configure ESET products:

- ERA Agent policy settings
- ERA Proxy policy settings
- ESET Rogue Detection Sensor policy settings
- Create a Policy for iOS MDM - Exchange ActiveSync Account
- Create a Policy for MDC to activate APNS for iOS enrollment

6.5.6 Assign a Policy to a Group

After a policy is created, you can assign it to a **Static or Dynamic Group**. There are a two ways to assign a policy:

1. Under **Admin > Policies** > select a policy and click **Assign Group(s)**. Select a Static or Dynamic Group and click **OK**.

   ![Policy Assignment](image)

   Select **Group** from the list.
2. Click Admin > Groups > Group or click the gear icon next to the group name and select Manage Policies.
In the **Policy application order** window click **Add Policy**. Select the check box next to the policy that you want to assign to this group and click **OK**. Click **Close**. To see what policies are assigned to a particular group, select that group and click the **Policies** tab to view a list of policies assigned to the group.

**NOTE**
For more information about policies, see the **Policies** chapter.
6.5.7 Assign a Policy to a Client

To assign a policy to a client workstation, click **Admin > Policies** select the **Clients** tab and click **Assign client(s)**.

Select your target client computer(s) and click **OK**. The policy will be assigned to all computers you have selected.
6.5.8   ERA Proxy policy settings
It is possible to change the behavior of ERA Proxy machines via policy. This is mostly used to change settings like connection interval or the server to which the proxy is connected.

Click Policies and expand Custom Policies to edit an existing policy or create a new one.

_connection_

Remote Administrator port - This is the port for the connection between the ESET Remote Administrator Server and Proxy. Changing this option requires that you restart the ERA Server service for the change to take effect.

Servers to connect to - To add ERA Server connection details (hostname/IP and a port number), click Edit server list. Multiple ERA Servers can be specified. This can be useful if, for example, you've changed the IP address of your ERA Server or are performing a migration.

Data limit - Specify the maximum number of bytes for sending data.

Connection interval - Select Regular interval and specify a time value for the connection interval (or you can use a CRON expression).

Certificate - You can manage peer certificates for ERA Proxy. Click Change certificate and select which ERA Proxy certificate should be used by ERA Proxy. For more information, see Peer Certificates.

_advanced settings_

Diagnostics - Enable or disable the submission of anonymous crash report statistics to ESET for the improvement of customer experience.

Logging - Set the log verbosity to determine the level of information that will be collected and logged, from Trace (informational) to Fatal (most important critical information).

Assign
Specify the clients that will receive this policy. Click Assign to display all Static and Dynamic Groups and their members. Select the computer that you want to apply a policy on and click OK.

Summary
Review the settings for this policy and click Finish.

6.5.9   ESET Rogue Detection Sensor policy settings
It is possible to change the behavior of ESET RD Sensor using a policy. This is mostly used to change the filtering of addresses. You can, for example, include certain addresses in the blacklist so they are not detected.

Click Policies and expand Custom Policies to edit an existing policy or create a new one.

_filters_

IPv4 Filter

Enable IPv4 address filtering - By enabling filtering, only computers whose IP addresses are part of the Whitelist in the IPv4 filter list will be detected, or only those that are not part of the Blacklist.

Filters - Specify whether the list will be a Whitelist or Blacklist.

IPv4 address list - Click Edit IPv4 list to add or remove addresses from the list.

MAC address prefix filter

Enable MAC address prefix filtering - By enabling filtering, only computers whose MAC address prefix (xx:xx:xx) addresses are part of the MAC address list will be detected, or only those that are not part of the Blacklist.

Filtering mode - Specify whether the list will be a Whitelist or Blacklist.
MAC address prefix list - Click Edit MAC prefix list to add or remove a prefix from the list.

Detection

Active detection - Enabling this option will allow the RD Sensor to search the local network for computers actively. This can improve search results but it can also trigger firewall warnings on some machines.

OS detection ports - RD Sensor uses a pre-configured list of ports to search the local network for computers. This list can be added by changing lists below.

Advanced Settings

Diagnostics - Enable or disable the submission of anonymous crash report statistics to ESET for the improvement of customer experience.

Assign

Specify the clients that will receive this policy. Click Assign to display all Static and Dynamic Groups and their members. Select the computer that you want to apply a policy on and click OK.

Summary

Review the settings for this policy and click Finish.
6.5.10 How to use Override mode

Users with ESET Endpoint products (version 6.5 and above) for Windows installed on their machine can use the Override feature. Override mode allows users on the client-computer level to change settings in the installed ESET product, even if there is a policy applied over these settings. Override mode can be enabled for certain AD users, or it can be password-protected. The function can not be enabled for more than four hours at once.

⚠️ WARNING

Override mode can not be stopped from the ERA Web Console once it is enabled. Override is disabled only after the time of override expires, or after it is turned off on the client itself.

To set the Override mode:

1. Navigate to **Admin > Polices > New Policy**.
2. In the **Basic** section, type in a **Name** and **Description** for this policy.
3. In the **Settings** section, select **ESET Endpoint for Windows**.
4. Click **Override mode** and configure rules for override mode.
5. In the **Assign** section, select the computer or group of computers on which this policy will be applied.
6. Review the settings in the **Summary** section and click **Finish** to apply the policy.

**EXAMPLE**

If John has a problem with his endpoint settings blocking some important functionality or web access on his machine, the Administrator can allow John to override his existing endpoint policy and tweak the settings manually on his machine. Afterward, these new settings can be requested by ERA so the Administrator can create a new policy out of them.

To do so, follow the steps below:
1. Navigate to Admin > Policies > New Policy.
2. Complete the Name and Description fields. In the Settings section, select ESET Endpoint for Windows.
3. Click Override mode, enable the override mode for one hour and select John as the AD user.
4. Assign the policy to John’s computer and click Finish to save the policy.
5. John has to enable the Override mode on his ESET endpoint and change the settings manually on his machine.
6. On the ERA Web Console, navigate to Computers, select John’s computer and click Show Details.
7. In the Configuration section, click Request configuration to schedule a client task to get the configuration from the client ASAP.
8. After short time, the new configuration will appear. Click on the product which settings you want to save and then click Open Configuration.
9. You can review settings and then click Convert to policy.
10. Complete the Name and Description fields.
11. In the Settings section, you can modify the settings if needed.
12. In the Assign section, you can assign this policy to John’s computer (or others).
13. Click Finish to save the settings.
14. Do not forget to remove the override policy once it is no longer needed.

6.6 Client Tasks

You can use Client Tasks to manage client computers and their ESET products. There is a set of pre-defined tasks that cover the most common scenarios, or you can create a custom client task with specific settings. Use client tasks to request an action from client computers. To run a client task successfully, it is required to have sufficient access rights for the task and for the objects (devices) that task uses. See the list of permissions for more information on access rights.

Client tasks can be assigned to groups or individual computers. Once created, a task is executed using a Trigger. Client tasks are distributed to clients when the ERA Agent on a client connects to the ERA Server. For this reason, it may take some time for task execution results to be communicated to the ERA Server. You can manage your ERA Agent connection interval to reduce task execution times. The following pre-defined tasks are available for your convenience (each Task Category contains Task Types):

All Tasks

- ESET Security Product
  - Export Managed Products Configuration
  - On-Demand Scan
  - Product Activation
  - Quarantine Management
  - Run SysInspector Script
  - Server scan
  - Software Install
  - SysInspector Log Request (Windows only)
  - Upload Quarantined File
  - Modules Update
  - Modules Update Rollback

- ESET Remote Administrator
  - Remote Administrator Components Upgrade
Reset Cloned Agent
Rogue Detection Sensor Database Reset
Stop Managing (Uninstall ERA Agent)

Operating System
Display Message
Operating System Update
Run Command
Shutdown computer
Software Install
Software Uninstall
Stop Managing (Uninstall ERA Agent)

Mobile
Anti-Theft Actions
Display Message
Export Managed Products Configuration
On-Demand Scan
Product Activation
Software Install
Stop Managing (Uninstall ERA Agent)
Modules Update

6.6.1 Client Tasks executions
The current status of each Client Task can be tracked under Admin > Client Tasks. For each task, a Progress indicator bar and Status icon is displayed. You can Drill down to view further details of a given Client Task and even take further actions such as Run on or Rerun on failed.

IMPORTANT
You must create a Trigger to execute all Client Tasks.

NOTE
A lot of data is re-evaluated during this process, it may require more time for execution than in previous versions (depending on Client Task, Client Trigger and overall Computers count).
Refer to Status icon for details about different icon types and statutes.

- **Client Task** action (click the Client Task to see context menu):
  
  1. **Show Details**
  The Client Task Detail displays **Summary** information about the Task, click the **Executions** tab to switch view to see each execution result. You can **Drill down** to view details for a given Client Task. If there are too many executions, you can filter the view to narrow down the results.

  **NOTE**
  When installing older ESET products, the Client Task report will display: Task delivered to the managed product.

  2. **Edit**
  Allows you to edit the selected **Client Task**. Editing existing tasks is useful when you only need to make small adjustments. For more unique tasks, you might prefer to create a new task from scratch.

  3. **Duplicate**
  Lets you create a new task based on the selected task, a new name is required for the duplicate.

  4. **Delete**
  Removes the selected task(s) completely.

  5. **Run on**
  Add a **new Trigger** and select Target computers or groups for this task.

  6. **Rerun on failed**
  Creates a new Trigger with all computers that failed during previous Task execution set as targets. You can edit the task settings if you prefer, or click **Finish** to rerun the task unchanged.

  7. **Access Group** - Move the client task to a different static group.
• **Execution** action (use the ⚡ sign to expand the Client Task to see its Executions/Triggers, click the Trigger to get context menu):

ritic Edit...

Allows you to edit the selected **Trigger**.

♂ **Rerun ASAP**

You can run the Client Task again (ASAP) using an existing **Trigger** straight away with no modification.

┊ **Delete**

Removes the selected trigger completely.

┊ **Duplicate...**

Lets you create a new Trigger based on the selected one, a new name is required for the duplicate.

**Access Group Filter**

The **Access Group** filter button enables users to select a static group and **filter viewed objects** according to the group where they are contained.
6.6.1.1 Progress indicator

The progress indicator is a color bar that shows the execution status of a Client Task. Each Client Task has its own indicator (shown in the Progress row). The execution status of a Client Task is shown in different colors, and includes the number of computers in that state for a given task:

- **Running** (blue)
  - ![Running Color Bar](Image)
  - 1

- **Successfully finished** (green)
  - ![Successfully finished Color Bar](Image)
  - 2

- **Failed** (orange)
  - ![Failed Color Bar](Image)
  - 2

Newly created Client Task (white) – it might take some time for the indicator to change color, ERA Server must receive a response from an ERA Agent to show the execution status. The progress indicator will be white if there is no Trigger assigned.

A combination of the above

- ![Combination Color Bar](Image)
  - 1

When you click the color bar, you can select from execution results and take further actions if necessary, see Drill down for more details.

Refer to Icon legend for details about different icon types and statutes.

### IMPORTANT

The progress indicator shows the status of a Client Task when it was last executed. This information comes from the ERA Agent. The progress indicator shows exactly what the ERA Agent is reporting from client computers.

6.6.1.2 Status icon

The icon next to Progress indicator provides additional information. It shows whether there are any planned executions for a given Client Task as well as the result of executions that were completed. This information is enumerated by ERA Server. The following statuses can be indicated:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Image" alt="Running" /></td>
<td>Client Task is being executed on at least one target, there are no scheduled and no failed. This applies even if the Client Task has already finished on some targets.</td>
</tr>
<tr>
<td><img src="Image" alt="Success" /></td>
<td>Client Task has finished successfully on all targets, there are no scheduled or running executions.</td>
</tr>
<tr>
<td><img src="Image" alt="Error" /></td>
<td>Client Task has run on all targets, but has failed on at least one. No further executions are planned (scheduled).</td>
</tr>
<tr>
<td><img src="Image" alt="Planned" /></td>
<td>Client Task is planned for execution, but no executions are running.</td>
</tr>
<tr>
<td><img src="Image" alt="Planned/Running" /></td>
<td>Client Task has scheduled executions (from the past or in the future). No executions have failed and at least one execution is currently running.</td>
</tr>
<tr>
<td><img src="Image" alt="Planned/Successful" /></td>
<td>Client Task still has some scheduled executions (from the past or in the future), no failed or running executions and at least one execution has finished successfully.</td>
</tr>
<tr>
<td>Status</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Running</td>
<td>Client Task is being executed on at least one target, there are no scheduled and no failed. This applies even if the Client Task has already finished on some targets.</td>
</tr>
<tr>
<td>Planned/Error</td>
<td>Client Task still has some executions scheduled (from the past or in the future), no running executions and at least one execution has failed. This applies even if some executions have completed successfully.</td>
</tr>
</tbody>
</table>

### 6.6.1.3 Drill down

When you click the color progress indicator bar, you can select from the following:

- Show all
- Show planned
- Show running
- Shown successful
- Show failed

An Executions window will display a list of computers with your selected result (using a filter). Computers with a result other than the one selected will not be shown. You can modify the filter or turn it off to see all computers regardless of their last status.

You can also drill down deeper, for example by selecting **History** to see details about the Client Task execution including the time when it **Occurred**, current **Status**, **Progress** and **Trace message** (if available). You can click **Computer name** or **Computer description** and take further actions if necessary, or view **Computer Details** for a specific client.
NOTE
If you do not see any entries in the Executions history table, try setting the Occurred filter to longer duration.
6.6.1.4 Trigger

A Trigger must be assigned to a Client Task for it to be executed. To define a Trigger, select the Target computers or groups on which a Client task should be executed. With your target(s) selected, set the trigger conditions to execute the task at a particular time or event. Additionally, you can use Advanced settings - Throttling to further fine-tune the Trigger, if required.

**Basic**

Enter basic information about the Trigger in the Description field and then click Target.

**Target**

The Target window allows you to specify the clients (individual computers or groups) that are the recipients of this task. Click Add Targets to display all Static and Dynamic Groups and their members.

Select clients, click OK and proceed to the Trigger section.

**Trigger** - Determines what event triggers the task.

- **As Soon As Possible** - Executes the task as soon as the client connects to ESET Remote Administrator Server and receives the task. If the task cannot be performed until the Expiration date, the task will be removed from the queue - the task will not be deleted, but it will not be executed.
- **Scheduled Trigger** - Executes the task at a selected time. You can schedule this task once, repeatedly or using a CRON expression.
- **Event Log Trigger** - Executes the task based on events specified here. This trigger is invoked when a certain event occurs in logs. Define the log type, logical operator and filtering criteria that will trigger the task.
- **Joined Dynamic Group Trigger** - This trigger executes the task when a client joins the Dynamic Group selected in the target option. If a Static Group or individual client(s) have been selected, this option will not be available.
NOTE
For more information about triggers, proceed to the Triggers chapter.

Advanced settings - Throttling - Throttling is used to restrict a task from being executed if a task is triggered by a frequently occurring event, for example the Event Log Trigger or the Joined Dynamic Group Trigger (see above). For more information, see the Throttling chapter.

Click Finish when you have defined the recipients of this task and the triggers that execute the task.

6.6.2 Shutdown computer
You can use the Shutdown computer task to shutdown or reboot client computers. Click New... to begin setting up your new task.

Basic
Enter Basic information about the task, such as the Name, optional Description and the Task Type. The Task Type (see the list above) defines the settings and the behavior for the task. In this case you can use the Shutdown computer task.

Target

IMPORTANT
It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click Finish to create the task and then create a Trigger to specify Targets for the task.

Settings
- Reboot computer(s)- select this check box if you want to reboot following task completion. If you want to shutdown computer(s), leave it deselected.

Summary
Review the summary of configured settings and click Finish. The Client Task is now created and a pop-up window
will open. We recommend you to click Create Trigger to specify when this Client Task should be executed and on what Targets. If you click Close, you can create a Trigger later on.

Client task has been created. Do you want to add trigger now?

6.6.3 On-Demand Scan
The On-Demand Scan task lets you manually run a scan on the client computer (separate from a regular scheduled scan). Click New... to begin setting up your new task.

Basic
Enter Basic information about the task, such as the Name, optional Description and the Task Type. The Task Type (see the list above) defines the settings and the behavior for the task. In this case you can use the On-Demand Scan task.

Target

IMPORTANT
It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click Finish to create the task and then create a Trigger to specify Targets for the task.

Settings

Shutdown after scan - If you select this check box, the computer will shut down after scanning is finished
Scan profile - You can select the profile you want from the drop-down menu:

- **In-depth Scan** - This is a pre-defined profile on the client, it is configured to be the most thorough scan profile and checks the whole system but also requires the most time and resources.
- **Smart scan** - Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. The advantage of Smart scan is it is easy to operate and does not require detailed scanning configuration. Smart scan checks all files on local drives and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value.
- **Scan From Context Menu** - Scans a client using a pre-defined scan profile, you can customize the scan targets.
- **Custom Profile** - Custom scan lets you specify scanning parameters such as scan targets and scanning methods. The advantage of a Custom scan is the ability to configure the parameters in detail. Configurations can be saved to user-defined scan profiles, which make it easy to repeat the scan using the same parameters. A profile must be created prior to running the task with the custom profile option. Once you select a custom profile from the drop-down menu, type the exact name of the profile into the **Custom profile** field.

Cleaning

By default, **Scan with cleaning** is selected. This means that when infected objects are found, they are cleaned automatically. If this is not possible, they will be quarantined.

Scan Targets

This option is also selected by default. Using this setting, all targets specified in the scan profile are scanned. If you deselect this option, you need to manually specify scan targets in the **Add Target** field. Type the scan target into the text field and click **Add**. The target will be displayed in the **Scan targets** field below. A scan target can be a file, location or you can run a pre-defined scan using any of the following strings as a **Scan target**:

<table>
<thead>
<tr>
<th>Scan target</th>
<th>Scanned localities</th>
</tr>
</thead>
<tbody>
<tr>
<td>${DriveRemovable}</td>
<td>All removable drives and devices.</td>
</tr>
<tr>
<td>${DriveRemovableBoot}</td>
<td>Boot sectors of all removable drives.</td>
</tr>
<tr>
<td>${DriveFixed}</td>
<td>Hard drives (HDD, SSD).</td>
</tr>
<tr>
<td>${DriveFixedBoot}</td>
<td>Boot sectors of hard drives.</td>
</tr>
<tr>
<td>${DriveRemote}</td>
<td>Network drives.</td>
</tr>
<tr>
<td>${DriveAll}</td>
<td>All available drives.</td>
</tr>
<tr>
<td>${DriveAllBoot}</td>
<td>Boot sectors of all drives.</td>
</tr>
<tr>
<td>${DriveSystem}</td>
<td>System drives.</td>
</tr>
<tr>
<td>${Share}</td>
<td>Shared drives (only for server products).</td>
</tr>
<tr>
<td>${Boot}</td>
<td>Main boot sector.</td>
</tr>
<tr>
<td>${Memory}</td>
<td>Operating memory.</td>
</tr>
</tbody>
</table>

**EXAMPLE: Scan targets**

Below are some examples of how to use **On-Demand Scan** target parameters:

- **File**: C:\Users\Data.dat
- **Folder**: C:\MyFolder
- **Unix path or file**: /usr/data
### Summary

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed and on what Targets. If you click **Close**, you can create a **Trigger** later on.

---

**6.6.4  Operating System Update**

The **System Update** task is used to update the operating system of the client computer. This task can trigger the operating system update on Windows, OS X and Linux operating systems.

#### Basic

Enter basic information about the task, such as a **Name** and **Description** and then select the **Operating System Update** task. The **Task Type** (see the list of **Client Task types**) defines the settings and behavior for the task.

#### Target

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a **Trigger** to specify Targets for the task.
Settings

- **Automatically Accept EULA** - select this check box if you want to accept the EULA automatically. No text will be displayed to the user.

- **Install Optional Updates** - this option applies to Windows operating systems only, updates that are marked as optional will also be installed.

- **Allow Reboot** - this option applies to Windows operating systems only and causes the client computer to reboot once the updates are installed.

Summary

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed and on what Targets. If you click **Close**, you can create a **Trigger** later on.

Client task has been created. Do you want to add trigger now?

![Create Trigger/Close Button](image)

6.6.5 Quarantine Management

The **Quarantine management** task is used to manage objects in the ERA Server quarantine - infected or suspicious objects found during the scan.

**Basic**

Enter Basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task. In this case you can use the **Quarantine Management** task.

**Target**

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a **Trigger** to specify Targets for the task.
**Settings**

**Quarantine management settings**

**Action** - Select the action to be taken with the object in Quarantine.
- **Restore Object(s)** (restores the object to its original location, but it will be scanned and if the reasons for the Quarantine persist, the object will be quarantined again)
- **Restore Object(s) and Exclude in Future** (restores the object to its original location and it will not be quarantined again).
- **Delete Object(s)** (deletes the object completely).

**Filter type** - Filter the objects in the Quarantine based on the criteria defined below. Either based on the Hash string of the object or Conditions.

**Conditional filter settings:**
- **Hash filter settings** - Add hash items into the field. Only known objects can be entered, for example, an object that has already been quarantined.
- **Occurred from/to** - Define the time range, when the object has been quarantined.
- **Minimal/maximal size (bytes)** - Define the size range of the quarantined object (in bytes).
- **Threat name** - Select a threat from the quarantined items list.
- **Object name** - Select an object from the quarantined items list.

**Summary**

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed and on what Targets. If you click **Close**, you can create a **Trigger** later on.

Client task has been created. Do you want to add trigger now?
6.6.6 Rogue Detection Sensor Database Reset

The Rogue Detection Sensor Database Reset task is used to reset the RD Sensor search cache. The task deletes the cache and the search results will be stored again. This task does not remove detected computers. This task is useful when detected computers are still in the cache and are not reported to the server.

**NOTE**
Settings are not available for this task.

**Target**

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click Finish to create the task and then create a Trigger to specify Targets for the task.

**Summary**

Review the summary of configured settings and click Finish. The Client Task is now created and a pop-up window will open. We recommend you to click Create Trigger to specify when this Client Task should be executed and on what Targets. If you click Close, you can create a Trigger later on.
6.6.7 Remote Administrator Components Upgrade

The **Remote Administrator Components Upgrade** task is used to upgrade ERA components (ERA Agent, ERA Proxy, ERA Server, Webconsole and MDM). For example, when you want to upgrade from ERA version 6.1.28.0, 6.1.33.0, 6.2.x, 6.3.x 6.4.x to ERA version 6.5.x

**NOTE**
See [Components upgrade](#) for detailed instructions. For another how to upgrade ESET Remote Administrator to the latest version (6.x) guide, see our [Knowledgebase article](#).

**Basic**

Enter Basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task. In this case you can use the **Remote Administrator Components Upgrade** task.

**Target**

**IMPORTANT**
It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a **Trigger** to specify Targets for the task.

**Settings**

Select the check box next to **I agree with application End User License Agreement** if you agree. See [License Management](#) or EULA for more information.

- **Reference Remote Administrator Server** - Select ERA Server version from the list. All ERA components will be upgraded to versions compatible with the selected server.
- **Automatically reboot when needed** - You can force a reboot of the client operating system, if the installation requires so.
Review the summary of configured settings and click Finish. The Client Task is now created and a pop-up window will open. We recommend you to click Create Trigger to specify when this Client Task should be executed and on what Targets. If you click Close, you can create a Trigger later on.

Client task has been created. Do you want to add trigger now?

### 6.6.8 Reset Cloned Agent

The **Reset Cloned Agent** task can be used to distribute the ESET Agent in your network via a pre-defined image. Cloned Agents have the same SID, which can cause problems (multiple Agents with the same SID), to resolve this, use the **Reset Cloned Agent** task to reset the SID and assigns Agents a unique identity.

**NOTE**
Settings are not available for this task.

### Target

**IMPORTANT**
It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click Finish to create the task and then create a Trigger to specify Targets for the task.
will open. We recommend you to click Create Trigger to specify when this Client Task should be executed and on what Targets. If you click Close, you can create a Trigger later on.

Client task has been created. Do you want to add trigger now?

6.6.9 Run Command

The Run command task can be used to execute specific command line instructions on the client. The administrator can specify the command line input to run.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Command will run as user</th>
<th>Default working directory</th>
<th>Accessible network locations</th>
<th>Command will be run in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Local System</td>
<td>C:\Windows \Temp</td>
<td>only locations in the current domain and available to user Local System</td>
<td>Command prompt (cmd.exe)</td>
</tr>
<tr>
<td>Linux or macOS</td>
<td>root</td>
<td>/tmp</td>
<td>only if location is mounted and available to root user</td>
<td>Console</td>
</tr>
</tbody>
</table>

**Basic**

Enter Basic information about the task, such as the Name, optional Description and the Task Type. The Task Type (see the list above) defines the settings and the behavior for the task. In this case you can use the Run Command task.

**Target**

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click Finish to create the task and then create a Trigger to specify Targets for the task.
**Settings**

- **Command line to run** - Enter a command line you want to run on the client(s).
- **Working directory** - Enter a directory where the command line above will be executed.

**EXAMPLE: How to run local script**

To run a local script located on a client at `C:\Users\user\script.bat` follow these steps:

1. Create a new Client Task and select **Run Command**.
2. In the **Settings** section enter:
   - **Command line to run**: `script.bat`
   - **Working Directory**: `C:\Users\user`
3. Click **Finish**, create a trigger and choose target clients.

**Summary**

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed and on what Targets. If you click **Close**, you can create a **Trigger** later on.

Client task has been created. Do you want to add trigger now?
6.6.10 Run SysInspector Script

The Run SysInspector Script task is used to remove unwanted objects from the system. A SysInspector Script needs to be exported from ESET SysInspector prior to using this task. After you export the script, you can mark objects you want to remove and run the script with the modified data - the marked objects will be deleted.

**Basic**

Enter Basic information about the task, such as the Name, optional Description and the Task Type. The Task Type (see the list above) defines the settings and the behavior for the task. In this case you can use the **Run SysInspector Script** task.

**NOTE**
Once the task is finished, you can review the results in a report.

**Target**

**IMPORTANT**
It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click **Finish** to create the task and then create a **Trigger** to specify Targets for the task.

**Settings**

- **SysInspector Script** - Click **Browse** to navigate to the service script. The service script needs to be created prior to running this task.
- **Action** - You can either **Upload** to, or **Download** a script from the ERA Console.

**Summary**

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed and on what Targets. If you click **Close**, you can create a **Trigger** later on.
6.6.11 Server Scan

You can use the Server Scan task to scan clients with ESET Server solutions installed (currently ESET File Security 6, ESET Mail Security 6, ESET Mail Security for IBM Domino and ESET Security for Microsoft SharePoint Server).

- **Scanned Server** - click Select to choose a server for scanning. Only one server can be selected.

- **Scan Targets** - displays resources on the selected server that are available for scanning.

**NOTE**
The first time that you use Generate target list, allow about half the duration of specified Update period to pick it up. For example, if the Update period is set to 60 minutes, allow 30 minutes to receive the list of scan targets. For more information see ERA scan targets.

**NOTE**
You can use the Server Scan task scan to perform a Hyper-V scan on ESET File Security 6, as well as On-demand mailbox database scan and Hyper-V scan on ESET Mail Security 6. Other scan methods are currently not available.
6.6.12 Software Install

The **Software Install** task is used to install software on your client computers. It is primarily intended to install ESET products, but you can use it to install any software you like.

**Basic**

Enter Basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task. In this case you can use the **Software Install** task.

**Target**

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a **Trigger** to specify Targets for the task.

**Settings**

Select the check box next to **I agree with application End User License Agreement** if you agree. See **License Management** or EULA for more information.

Click **Choose ESET License** and select the appropriate license for the installed product from the list of available licenses.

Click **Choose package** to select a installer package from the repository or specify a package URL. A list of available packages where you can select the ESET product you want to install (for example, ESET Endpoint Security) will be displayed. Select your desired installer package and click **OK**. If you want to specify a URL where the installation package is located, type or copy and paste the URL (for example `file://\pc22\install\ees_nt64_ENU.msi`) into the text field (do not use a URL that requires authentication).
http://server_address/ees_nt64_ENU.msi - If you are installing from a public web server or from your own HTTP server.
file://\pc22\install\ees_nt64_ENU.msi - if you are installing from network path.
file://C:\installs\ees_nt64_ENU.msi - if you are installing from local path.

**NOTE**

1. Both ERA Server and ERA Agent require access to the internet to access the repository and perform installations. If you do not have internet access, you can install the client software locally.

2. When performing **Client Task > Operating System > Software Install** on computers in a domain with ERA Agent running, it is necessary to provide **read permission** for the folder where the installers are stored. To do this, complete the following steps:
   a. Add an Active Directory computer account (for example *NewComputer$*)
   b. Grant **Read** permissions to *NewComputer$* by right-clicking the folder with installers and selecting **Properties > Sharing > Share** from the context menu. Note that the "$" symbol needs to be present at the end of the computer name string.

If you need to, you can specify **Installation parameters**, otherwise leave this field empty. Select the check box next to **Automatically reboot when needed** to force an automatic reboot of the client computer after installation. Alternatively, you can leave this option deselected and the client computer can be restarted manually.

**NOTE**

The Software Install task can be used to upgrade ESET Security Products. Run the task using the latest installer package to install the latest version over your existing solution.

**Summary**

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed and on what Targets. If you click **Close**, you can create a **Trigger** later on.

**NOTE**

When installing ESET Endpoint Antivirus or ESET Endpoint Security version 6.5 and later with the install parameter **CFG_LIVEGRID_ENABLED**, the behavior of the product after the install will be following:

<table>
<thead>
<tr>
<th>Feature</th>
<th>CFG_LIVEGRID_ENABLED=0</th>
<th>CFG_LIVEGRID_ENABLED=1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESET LiveGrid® reputation system (recommended)</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>Submit anonymous statistics</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Submit sample</td>
<td>Off</td>
<td>On</td>
</tr>
</tbody>
</table>

**IMPORTANT**

The product upgrade for version 4.x (ESET Security for Microsoft SharePoint) using **Software Task** will be aborted and return a general installation error (0x643). For upgrade instructions for ESET Security for Microsoft SharePoint using ERA, see the following **Online help**.
6.6.13 Software Uninstall

The **Software Uninstall** task is used to uninstall ESET security product from client computers when they are no longer wanted/needed. Once you uninstall the ERA Agent from the client computer, ESET security product may retain some settings after the ERA Agent has been uninstalled.

1. **IMPORTANT**
   We recommend that you reset some settings (for example, password protection) to default settings using a policy before the device is removed from management. Also, all tasks running on the Agent will be abandoned. The **Running**, **Finished** or **Failed** execution status of this task may not be displayed accurately in ERA Web Console depending on replication.

2. **Basic**
   Enter basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task.

3. **Target**
   **IMPORTANT**
   It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a **Trigger** to specify Targets for the task.
Settings

Software Uninstallation Settings

- **Uninstall - Application from list:**
  - **Package name** - Select an ERA component, a client security product or a 3rd-party application. All packages that can be uninstalled from the selected client(s) are displayed in this list.
  - **Package version** - You can either remove a specific version (sometimes, a specific version can cause problems) of the package, or **uninstall all versions of a package**.
  - **Automatically reboot when needed** - You can force a reboot of the client operating system if it is required for uninstallation.

- **Uninstall - Third party antivirus software (Built with OPSWAT)** - For a list of compatible AV Software, see our Knowledgebase article. This removal is different from the Add or Remove Programs uninstallation. It uses alternative methods to remove third party antivirus software thoroughly including any residual registry entries or other traces.

Follow the step-by-step instructions in this article [How do I remove third-party antivirus software from client computers using ESET Remote Administrator? (6.x)](6.6.14) to send a task to remove third-party antivirus software from client computers.

- If you want to allow uninstallation of password-protected applications see our Knowledgebase article. (see step 12.)

Summary

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed and on what Targets. If you click **Close**, you can create a **Trigger** later on.

Client task has been created. Do you want to add trigger now?

**NOTE**

In case the ESET security product uninstallation does not finish successfully, for example if you get **Product: ESET Endpoint Security -- Error 5004. Enter a valid password to continue uninstallation. error** message, this is because there is a password protection setting enabled in ESET security product. Apply a policy to the client computer(s) you want to uninstall ESET security product from in such a way, that the password protection is disabled, which otherwise prevents the uninstallation.

6.6.14 Product Activation

Follow the steps below to activate an ESET security product on a client computer or a mobile device.

**Basic**

Enter basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task.

**Target**

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a **Trigger** to specify Targets for the task.
**Settings**

**Product activation settings** - Select a license for the client from the list. This license will be applied to products already installed on the client. If you do not see any licenses listed, go to [Licenses - add new license](#).

**Summary**

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed and on what Targets. If you click **Close**, you can create a **Trigger** later on.

Client task has been created. Do you want to add trigger now?
6.6.15 SysInspector Log Request (Windows only)

The **SysInspector Log Request** task is used to request the SysInspector log from a client security product, that has this function.

### Basic

Enter Basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task. In this case you can use the **SysInspector Log Request** task.

### Target

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a **Trigger** to specify Targets for the task.

#### Settings

- **Store log on client** - Select this if you want to store the SysInspector log on the client as well as on the ERA Server. For example, when a client has ESET Endpoint Security installed, the log is usually stored under `C:\Program Data\ESET\ESET Endpoint Antivirus\SysInspector`.

#### Summary

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed and on what Targets. If you click **Close**, you can create a **Trigger** later on.
6.6.16 Upload Quarantined File

The Upload Quarantined File task is used to manage files quarantined on clients.

**Basic**

Enter basic information about the task, such as the Name, optional Description and the Task Type. The Task Type (see the list above) defines the settings and the behavior for the task. In this case you can use the Upload Quarantined File task.

**Target**

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click Finish to create the task and then create a Trigger to specify Targets for the task.

**Settings**

- **Quarantined object** - Select a specific object from the quarantine.
- **Object password** - Enter a password to encrypt the object for security reasons. Please note that password will be displayed in the corresponding report.
- **Upload path** - Enter a path to a location where you want to upload the object.
- **Upload username/password** - In case the location requires authentication (network share, etc.), enter the credentials to access this path.
Review the summary of configured settings and click Finish. The Client Task is now created and a pop-up window will open. We recommend you to click Create Trigger to specify when this Client Task should be executed and on what Targets. If you click Close, you can create a Trigger later on.

Client task has been created. Do you want to add trigger now?

6.6.17 Modules Update

The Modules Update task forces the update of all modules of the security product installed on a target device. This is a general task for all security products on all systems. You can find the list of all modules of the target security product in the About section of the security product.

Target

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click Finish to create the task and then create a Trigger to specify Targets for the task.

Settings

- **Clear Update Cache** - This option deletes the temporary update files in the cache on the client, and can often be used to repair module update errors.
6.6.18 Modules Update Rollback

In cases where a module update causes issues, or you do not want to apply the update to all clients (for example, for testing, or when using pre-release updates), you can use the Modules Update Rollback task. When you apply this task, the modules will be reset to the previous version.

**Target**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click Finish to create the task and then create a Trigger to specify Targets for the task.

**Settings**

Expand this section to customize module update rollback settings.

**Action**
- **Enable Updates** - Updates are enabled and the client will receive the next module update.
- **Rollback and Disable Updates for Next** - Updates are disabled for the specific time period in the **Disable interval** drop-down menu (24, 36, 48 hours, or until revoked). Be careful when using the **Until revoked** option, as this presents a security risk.

### Summary

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed and on what Targets. If you click **Close**, you can create a **Trigger** later on.

Client task has been created. Do you want to add trigger now?

---

### 6.6.19 Display Message

This functionality lets you send a message to any device (client computer, tablet, mobile, etc.). The message will be displayed on-screen to inform the user. The message is displayed differently to recipients on Windows and Unix (Linux, macOS) systems:

- Windows users will see a notification
- On macOS and Linux the message is displayed only in a console, but if one is opened.

#### Basic

Enter Basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task. In this case you can use the **Display Message** task.

#### Target

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a **Trigger** to specify Targets for the task.
Settings

You can enter a Title and type in your Message.

Summary

Review the summary of configured settings and click Finish. The Client Task is now created and a pop-up window will open. We recommend you to click Create Trigger to specify when this Client Task should be executed and on what Targets. If you click Close, you can create a Trigger later on.

Client task has been created. Do you want to add trigger now?

CREATE TRIGGER
CLOSE

6.6.20 Anti-Theft Actions

The Anti-Theft feature protects a mobile device from unauthorized access. If a mobile device (enrolled and managed by ERA) is lost or gets stolen, there are some actions that take place automatically and some actions can be performed using a client task. If an unauthorized person replaces a trusted SIM card with an untrusted SIM, the device will automatically be locked by ESET Endpoint Security for Android and an alert SMS will be sent to the user-defined phone number(s). This message will include the phone number of the SIM card currently in use, the IMSI (International Mobile Subscriber Identity) number and the phone's IMEI (International Mobile Equipment Identity) number. The unauthorized user will not be aware that this message has been sent because it will automatically be deleted from the device's messaging threads. You can also request the GPS coordinates of the lost mobile device or remotely erase all data stored on the device using a client task.
**Target**

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a **Trigger** to specify Targets for the task.

### Settings

- **Find** - The device will reply with a text message containing its GPS coordinates. If a more precise location is available after 10 minutes, the device will re-send the message. Received information is displayed in the **Computer details**.

- **Lock** - The device will be locked. The device can be unlocked using the Administrator password or the unlock command.

- **Unlock** - The device will be unlocked so it can be used again. The SIM card currently in the device will be saved as a Trusted SIM.

- **Siren** - The device will be locked and it will play a very loud sound for 5 minutes (or until unlocked).

- **Wipe** - All accessible data on the device will be erased (files will be overwritten). ESET Endpoint Security will remain on the device. This can take up to several hours.

- **Enhanced Factory Reset** - All accessible data on the device will be erased (file headers will be destroyed) and the device will be reset to its default factory settings. This can take several minutes.
Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed and on what Targets. If you click **Close**, you can create a **Trigger** later on.

---

**6.6.21  Stop Managing (Uninstall ERA Agent)**

- **Desktop** - This task will remove the Agent installed on the machine where MDM is installed.
- **Mobile** - This task will cancel MDM enrollment of your mobile device.

After the device is no longer managed (Agent is removed), some settings may remain in the managed products.

**IMPORTANT**

We recommend that you reset some settings (for example, password protection) to default settings using a policy before the device is removed from management. Also, all tasks running on the Agent will be abandoned. The **Running**, **Finished** or **Failed** execution status of this task may not be displayed accurately in ERA Web Console depending on replication.

1. If the device has some special settings that you do not want to maintain, set a device policy that returns unwanted settings to default values (or values which are desirable).
2. Before performing this step, we recommend that you to wait long enough to be certain that policies from point 1 have finished replication on the target computer before deleting the computer from the list in ERA.
3. Before performing this step, we recommend that you to wait long enough to be certain that policies from point 2 have finished replication on the target computer.
NOTE

Settings are not available for this task.

Target

IMPORTANT

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click Finish to create the task and then create a Trigger to specify Targets for the task.

Summary

Review the summary of configured settings and click Finish. The Client Task is now created and a pop-up window will open. We recommend you to click Create Trigger to specify when this Client Task should be executed and on what Targets. If you click Close, you can create a Trigger later on.

Client task has been created. Do you want to add trigger now?
6.6.22  Export Managed Products Configuration

The Export Managed Products Configuration task is used to export the settings of individual ERA components or ESET security products installed on the client(s).

**Basic**

Enter Basic information about the task, such as the Name, optional Description and the Task Type. The Task Type (see the list above) defines the settings and the behavior for the task. In this case you can use the Export Managed Products Configuration task.

**Target**

**IMPORTANT**

It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure Settings for the task and click Finish to create the task and then create a Trigger to specify Targets for the task.

**Settings**

Export managed products configuration settings

- **Product** - Select an ERA component or a client security product for which you want to export the configuration.

**Summary**

Review the summary of configured settings and click Finish. The Client Task is now created and a pop-up window will open. We recommend you to click Create Trigger to specify when this Client Task should be executed and on what Targets. If you click Close, you can create a Trigger later on.
6.6.23 Assign Task to Group

Click Admin > Groups > select Static or Dynamic group > next to the selected group, or click Group > + New task.

The same can be done from Computers, select Static or Dynamic and click > + New task. A New Client task wizard window will open.
6.6.24 Assign Task to Computer(s)
There are three ways to assign a task to computer(s).

1. Dashboard > Computers with problems > select + New Task...

2. Computer > select computer(s) using check boxes > select + New task...
A New Client task wizard window will open.

6.6.25 Triggers

Triggers are essentially sensors that react to certain events in a pre-defined way. They are used to execute the client task they are assigned to. They can be activated by the scheduler (time events) or when a certain system event occurs.

**IMPORTANT**

It is not possible to reuse a trigger. Each client task must be triggered with a separate trigger. Each trigger can run only one client task.

The trigger does not run newly assigned tasks immediately (except the ASAP trigger)—the task is run as soon as the trigger is fired. Trigger sensitivity to events can be reduced further using throttling.

Client trigger types:

- **As soon as possible** - This trigger is invoked right after you click Finish. The Expiration date value specifies the date after which the task will no longer be executed.

Scheduled

- **Schedule Once** - This trigger is invoked once on the scheduled time. Can be delayed by random interval.
- **Daily** - This trigger is invoked every selected day. You can set the start and end of the interval. For example, you can run a server task for ten consecutive weekends.
- **Weekly** - This trigger is invoked on a selected day of the week. For example, run a client task every Monday and Friday between 1. July and 31. August.
- **Monthly** - This trigger is invoked on selected days in the selected week of a month, for the selected period of time. The Repeat on value sets the weekday in the month (for example, the second Monday) on which the task should run.
- **Yearly** - This trigger is invoked every year (or more years, if so configured) on the specified start date.
**NOTE**

**Random delay interval** is available to be set for scheduled type triggers. It defines the range of maximal delay for task execution. Randomizing can prevent overloading the server.

**EXAMPLE**

If John set the **Client Task** to trigger **Weekly** on **Monday** and **Start** on **2017 Feb 10 8:00:00**, with **Random delay interval** set to **1 hour** and **end by** set to **2017 Apr 6 00:00:00**, the task would run with a randomized one-hour delay between 8:00 and 9:00 every Monday until the specified end date.

Other

- **Joined Dynamic Group Trigger** - This trigger is invoked when a device joins the dynamic group.
- **Event Log Trigger** - This trigger is invoked when a certain event occurs in logs. For example, if there is a threat in the **Scan** log. This type of trigger provides a set of special settings in the **Throttling settings**.
- **CRON Expression** - This trigger is invoked at a certain time and date.

**NOTE**

**Joined Dynamic Group Trigger** is available only if a dynamic group is selected in the **Target** section. The trigger will run the task only on devices that join the dynamic group after the trigger is created. For all the devices already in the dynamic group, you will have to execute the task manually.

Scheduled Trigger will run the task based on date and time settings. Tasks can be scheduled to **run once**, on a recurring basis, or on **CRON expression**.

### 6.7 Server Tasks

Server tasks can automate routine jobs. Each server task can have one **trigger** configured. If the task needs to be run with various events, there has to be separate server task for each trigger. ERA includes six predefined **Server Task types**.

**NOTE**

Server tasks cannot be assigned to any specific client or client group.

Server tasks and permissions

The task and trigger both need an executing user. This is the user who modifies the task (and trigger). This user must have sufficient permissions for the chosen action. During execution, the task always takes the executing user from the trigger. If the task is run using the **Run task immediately after finish** setting, the executing user is the user logged into the ERA Web Console. A user has permissions (Read, Use, Write) for the selected server task instance if it has those permissions selected in its permission set (**Admin > Access Rights > Permission Sets**) and has these permissions set for that Static Group where the server task is located. See the **list of permissions** for more information on access rights.

**EXAMPLE**

*John*, whose home group is **John’s Group**, wants to remove **Server Task 1: Generate Report**. The task was originally created by **Larry**, therefore the task is automatically contained in Larry's home group, **Larry's Group**. The following conditions must be met for **John** to remove the task:

- **John** must be assigned a permission set with write permissions for **Server Tasks & Triggers - Generate Reports**.
- The permission set must contain **Larry's Group** under **Static Groups**.

Permissions needed for certain server task actions

- To create a new server task, the user needs write permission for the selected task type and proper access rights for the referenced objects (computers, licenses, groups).
To modify a server task, the user needs write permission for the selected server task instance and proper access rights for the referenced objects (computers, licenses, groups).

To remove a server task, the user needs write permission for the selected server task instance.

To run a server task, the user needs use permission for the selected server task instance.

**Create a new server task**

1. Click **Admin > Server Tasks > New**.
2. Enter basic information about the task, such as a name, description (optional) and the task type. The task type defines the settings and the behavior of the task.
3. You can decide if you want to:
   - **Run task immediately after finish** - Select this check box to have the task run automatically after you click Finish.
   - **Configure trigger** - Select the check box and expand the **Trigger** section to configure the trigger settings.
   - Set the trigger later (select no check box).
4. Configure the task settings in the **Settings** section.
5. Set the trigger in the **Trigger** section, if it is available.
6. Verify all the settings for this task in the **Summary** section and then click **Finish**.

**Access Group Filter**

The **Access Group** filter button enables users to select a static group and **filter viewed objects** according to the group where they are contained.

**NOTE**

It is recommended for users who are regularly using Server tasks to create their own tasks rather than sharing them with other users. Each time the task is run it uses the permissions of the executing user. This can confuse some users.

### 6.7.1 Server Task Types

The following Server Tasks are predefined:

- **Agent Deployment** - distributes the Agent to client computers.
- **Delete Not Connecting Computers** - deletes clients that no longer connect to ESET Remote Administrator from Web Console.
- **Generate Report** - used to generate reports as they are needed.
- **Rename Computers** - this task will periodically rename computers in groups using FQDN format.
- **Static Group Synchronization** - updates group information to display current data.
- **User Synchronization** - updates User or User Group.
6.7.1.1 Static Group Synchronization

The Static Group Synchronization task will search your network (Active Directory, Open Directory, LDAP, local network or VMware) for computers and put them into a Static group. If you select Synchronize with Active Directory during Server Installation, found computers will be added to the All group. To synchronize Linux computers joined to Windows domain, follow these detailed instructions.

There are 3 Synchronization modes:

- **Active Directory/Open Directory/LDAP** - Type in the basic Server connection information. Click here for detailed instructions.
- **MS Windows Network** - Enter a Workgroup to be used, along with the appropriate user credentials. Click here for detailed instructions.
- **VMware** - Type in the VMware vCenter Server connection information. Click here for detailed instructions.

6.7.1.1.1 Synchronization mode - Active Directory

Click Admin > Server Task > Static Group Synchronization > New.

**Basic**

In this section, you can enter basic information about a task, such as a Name and Description (optional). You can also select from the following task trigger settings:

- **Run task immediately after finish** - Select this option to have the task run automatically after you click Finish.
- **Configure trigger** - Select this option to enable the Trigger section, where you can configure trigger settings.
- **To set the trigger later, leave this check box deselected.**

**Settings**

**Common Settings**

Click **Select** under **Static Group Name** - by default, the executing user's home group will be used for synchronized computers. Alternatively, you can create a New Static Group.

- **Object to synchronize** - Either Computers and Groups, or Only Computers.
- **Computer creation collision handling** - If the synchronization adds computers that are already members of the Static Group, you can select a conflict resolution method:
  - **Skip** (synchronized computers will not be added)
  - **Move** (new computers will be moved to a subgroup)
  - **Duplicate** (new computer is created with modified name)
- **Computer extinction handling** - If a computer no longer exists, you can either Remove this computer or Skip it.
- **Group extinction handling** - If a group no longer exists, you can either Remove this group or Skip it.

**Synchronization mode** - Active Directory / Open Directory / LDAP

**Server connection settings**

- **Server** - Type the Servername or IP address of your domain controller.
- **Login** - Type the login credentials for your domain controller in the format DOMAIN\username.
- **Password** - Type the password used to log onto your domain controller.

- **Use LDAP Parameters** - If you want to use LDAP, select the check box next to Use LDAP instead of Active Directory and enter specific attributes to match your server. Or, you can select Presets by clicking Custom. The following attributes will be populated automatically:
- **Active Directory** - Click **Browse** next to **Distinguished Name**. Your Active Directory tree will be displayed. Select the top entry to sync all groups with ERA, or select only the specific groups that you want to add. Click **OK** when you are finished.
- **Mac OS X Server Open Directory (Computer Host Names)**
- **Mac OS X Server Open Directory (Computer IP Addresses)**
- **OpenLDAP with Samba computer records** - For setting up the parameters **DNS name in Active Directory**.

**Synchronization settings**

- **Distinguished name** - Path (Distinguished Name) to the node in the Active Directory tree. Leaving this option empty will synchronize the entire AD tree.
- **Excluded distinguished name(s)** - You can choose to exclude (ignore) specific nodes in the Active Directory tree.
- **Ignore disabled computers (only in active directory)** - You can choose to ignore computers disabled in active directory (the task will skip these computers).

**Trigger**

The **Trigger** section contains information about the trigger(s) which would run a task. Each Server Task can have up to one trigger. Each trigger can run only one Server Task. If **Configure trigger** is not selected in the **Basic** section, a trigger is not created. A task can be created without trigger. Such a task can be run afterward manually or a trigger can be added later.

**Advanced Settings - Throttling**

By setting **Throttling**, you can set advanced rules for the created trigger. Setting throttling is optional.

**Summary**

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

**6.7.1.1.2 Synchronization mode - MS Windows Network**

Click **Admin > Server Task > Static Group Synchronization > New...**

**Basic**

In this section, you can enter basic information about a task, such as a Name and Description (optional). You can also select from the following task trigger settings:

- **Run task immediately after finish** - Select this option to have the task run automatically after you click Finish.
- **Configure trigger** - Select this option to enable the **Trigger** section, where you can configure trigger settings.
- To set the trigger later, leave this check box deselected.

**Settings**

**Common Settings**

Click **Select** under **Static Group Name** - by default, the executing user's home group will be used for synchronized computers. Alternatively you can create a **New Static Group**.

- **Object to synchronize** - Either **Computers and Groups**, or **Only Computers**.
- **Computer creation collision handling** - If the synchronization adds computers that are already members of the Static Group, you can select a conflict resolution method:
  - **Skip** (synchronized computers will not be added)
  - **Move** (new computers will be moved to a subgroup)
  - **Duplicate** (new computer is created with modified name)
- **Computer extinction handling** - If a computer no longer exists, you can either **Remove** this computer or **Skip** it.
- **Group extinction handling** - If a group no longer exists, you can either **Remove** this group or **Skip** it.
Synchonization mode - MS Windows Network

In the **Microsoft Windows Network synchronization settings** section type the following information:

- **Workgroup** - Type the domain or workgroup that contains the computers that will be synced. If you do not specify a workgroup, all visible computers will be synchronized.
- **Login** - Type the login credentials used for synchronization in your Windows network.
- **Password** - Type the password used to log on to your Windows network.

**Trigger**

The **Trigger** section contains information about the trigger(s) which would run a task. Each Server Task can have up to one trigger. Each trigger can run only one Server Task. If **Configure trigger** is not selected in the **Basic** section, a trigger is not created. A task can be created without trigger. Such a task can be run afterward manually or a trigger can be added later.

**Advanced Settings - Throttling**

By setting **Throttling**, you can set advanced rules for the created trigger. Setting throttling is optional.

**Summary**

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

6.7.1.1.3 Synchronization mode - VMware

It is possible to synchronize virtual machines running on VMware vCenter Server.

Click **Admin > Server Task > Static Group Synchronization > New.**

**Basic**

In this section, you can enter basic information about a task, such as a Name and Description (optional). You can also select from the following task trigger settings:

- **Run task immediately after finish** - Select this option to have the task run automatically after you click Finish.
- **Configure trigger** - Select this option to enable the **Trigger** section, where you can configure trigger settings.
  - To set the trigger later, leave this check box deselected.

**Settings**

**Common Settings**

Click **Select** under **Static Group Name** - by default, the executing user's home group will be used for synchronized computers. Alternatively you can create a **New Static Group**.

- **Object to synchronize** - Either **Computers and Groups**, or **Only Computers**.
- **Computer creation collision handling** - If the synchronization adds computers that are already members of the Static Group, you can select a conflict resolution method:
  - **Skip** (synchronized computers will not be added)
  - **Move** (new computers will be moved to a subgroup)
  - **Duplicate** (new computer is created with modified name)
- **Computer extinction handling** - If a computer no longer exists, you can either **Remove** this computer or **Skip** it.
- **Group extinction handling** - If a group no longer exists, you can either **Remove** this group or **Skip** it.
• **Synchronization mode** - VMWare

**Server connection settings**

• **Server** - Type in the DNS or IP address of the VMware vCenter Server.
• **Login** - Type in the login credentials for the VMware vCenter Server.
• **Password** - Type in the password used to log onto your VMware vCenter Server.

**Synchronization settings**

• **Structure view** - Select the type of structure view, either **Folders** or **Resource pool**.
• **Structure path** - Click **Browse** and navigate to the folder you want to synchronize. If the field is left empty, the entire structure will be synchronized.
• **Computer view** - Select whether to display computers by **Name**, **Host Name** or **IP Address** following synchronization.

**Trigger**

The **Trigger** section contains information about the trigger(s) which would run a task. Each Server Task can have up to one trigger. Each trigger can run only one Server Task. If **Configure trigger** is not selected in the **Basic** section, a trigger is not created. A task can be created without trigger. Such a task can be run afterward manually or a trigger can be added later.

**Advanced Settings - Throttling**

By setting **Throttling**, you can set advanced rules for the created trigger. Setting throttling is optional.

**Summary**

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

**6.7.1.1.4 Static Group Synchronization - Linux Computers**

Linux computer joined to Windows domain does not display any text in Active Directory Users and Computers (ADUC) in Computer properties, therefore it is necessary to insert text manually.

Check the **Server prerequisites** and the following prerequisites:

• The Linux computers are in Active Directory.
• Domain controller has a DNS server installed.
• **ADSI Edit** is installed.

1. Open a command prompt and run `adsiedit.msc`
2. Navigate to **Action > Connect to**. The connection settings windows will be displayed.
3. Click **Select a well known Naming context**.
4. Expand the combo box below and select **Default** naming context.
5. Click **OK** - the ADSI value on the left should be the name of your domain controller - Default naming context (your domain controller).
6. Click the **ADSI** value and expand its subgroup.
7. Click the **subgroup** and navigate to the CN (Common Name) or OU (Organizational Unit) where Linux computers are displayed.
8. Click the **hostname** of the Linux computer and select **Properties** from the context menu. Navigate to the **dNSHostName** parameter and click **Edit**.
9. Change the value `<not set>` to valid text (for example, `ubuntu.TEST`).
10. Click OK > OK. Open ADUC and select the properties of the Linux computer - the new text should be displayed here.

### 6.7.1.2 User Synchronization

This Server Task synchronizes the Users and User Group information from a source such as Active Directory, LDAP parameters, etc. To run this task, click Admin > Server Task > User Synchronization > New...

#### Basic

In this section, you can enter basic information about a task, such as a Name and Description (optional). You can also select from the following task trigger settings:

- **Run task immediately after finish** - Select this option to have the task run automatically after you click Finish.
- **Configure trigger** - Select this option to enable the Trigger section, where you can configure trigger settings.
- To set the trigger later, leave this check box deselected.

#### Settings

**Common settings**

- **User Group name** - by default, the root for synchronized users will be used (by default, this is the All group). Alternatively, you can create a new User Group.

- **User creation collision handling** - two types of conflict that might occur:
  - There are two users with the same name in the same group.
  - There is an existing user with the same SID (anywhere in the system).

You can set collision handling to:

- **Skip** - user is not added to ERA during synchronization with Active Directory.
- **Overwrite** - existing user in ERA is overwritten by the user from Active Directory, in the case of an SID conflict the existing user in ERA is removed from its previous location (even if the user was in a different group).

- **User extinction handling** - If a user no longer exists, you can either Remove this user or Skip it.

- **User group extinction handling** - If a user group no longer exists, you can either Remove this user group or Skip it.

#### Server connection settings

- **Server** - Type the Server name or IP address of your domain controller.
- **Login** - Type the login credentials for your domain controller in the format **DOMAIN\username**.
- **Password** - Type the password used to log on to your domain controller.

- **Use LDAP Parameters** - If you want to use LDAP, select the check box next to Use LDAP instead of Active Directory and enter the information for your server. Alternatively you can select Presets by clicking Custom... and the attributes will be populated automatically:
  - **Active Directory**
  - **Mac OS X Server Open Directory (Computer Host Names)**
  - **Mac OS X Server Open Directory (Computer IP Addresses)**
  - **OpenLDAP with Samba computer records** - setting up the parameters DNS name in Active Directory.

### Synchronization settings

- **Distinguished name** - Path (Distinguished Name) to the node in the Active Directory tree. Leaving this option empty will synchronize the entire AD tree.
User group and user attributes - User's default attributes are specific to the directory to which the user belongs. If you want to synchronize Active Directory attributes, select the AD parameter from the drop-down menu in the appropriate fields or enter a custom name for the attribute. Next to each synchronized field is an ERA placeholder (for example: ${display_name}) that will represent this attribute in certain ERA policy settings.

Advanced user attributes - If you want to use advanced custom attributes select Add New. These fields will inherit the user's information, which can be addressed in a policy editor for iOS MDM as a placeholder.

Trigger

The Trigger section contains information about the trigger(s) which would run a task. Each Server Task can have up to one trigger. Each trigger can run only one Server Task. If Configure trigger is not selected in the Basic section, a trigger is not created. A task can be created without trigger. Such a task can be run afterward manually or a trigger can be added later.

Advanced Settings - Throttling

By setting Throttling, you can set advanced rules for the created trigger. Setting throttling is optional.

Summary

All configured options are displayed here. Review the settings and click Finish if they are ok. The task is now created and ready to be used.

6.7.1.3 Agent Deployment

Remote deployment of the ERA Agent is performed from the Admin section. Click Server Task > Agent Deployment > New to start configuring your new task.

**NOTE**

We recommend you to first test mass Agent deployment in your environment. Once it's working fine, then you can begin with actual deployment on users client computers. Also, before you start testing mass deployment, change Agent connection interval.

Basic

In this section, you can enter basic information about a task, such as a Name and Description (optional). You can also select from the following task trigger settings:

- Run task immediately after finish - Select this option to have the task run automatically after you click Finish.
- Configure trigger - Select this option to enable the Trigger section, where you can configure trigger settings.
- To set the trigger later, leave this check box deselected.

Settings

Automatic resolution of suitable Agent - If you have multiple operating systems (Windows, Linux, Mac OS) in your network, select this option and this task will automatically find the appropriate server-compatible Agent installation package for each system.

Targets - Click this to select the clients that will receive this task.

Server hostname (optional) - You can enter a server hostname if it is different on the client side and the server side.

Username / Password - The username and the password for the user with sufficient rights to perform a remote installation of the agent.

Peer certificate:

- ERA Certificate - This is the security certificate and certification authority for the Agent installation. You can select the default certificate and certification authority, or use custom certificates.
- Custom certificate - If you use a custom certificate for authentication, navigate to the certificate and select it when installing the Agent. For more information, see the Certificates chapter.

Certificate Passphrase - Password for the certificate, either the password you entered during ERA Server installation (in the step where you created a certification authority) or the password for your custom certificate.
NOTE

- ERA Server can select the appropriate Agent installation package for operating systems automatically. To choose a package manually, deselect Automatic resolution of suitable Agent and then choose the package you want to use from the list of available Agents in ERA repository.

- For installation on Linux or Mac machine, make sure the target machine has SSH daemon enabled and running on the port 22 and a firewall is not blocking this connection. Use the following command (replace the IP address with the IP of your ERA Server) to add an exception in Linux firewall:
  
  
  ```
  iptables -A INPUT -s 10.0.0.1 -p tcp --dport 22 --state NEW -j ACCEPT
  ```

- For installation on Linux, choose a user with permission to use the `sudo` command or `root` user. If `root` is used, the `ssh` service must allow you to log-in as `root`.

### Trigger

The **Trigger** section contains information about the trigger(s) which would run a task. Each Server Task can have up to one trigger. Each trigger can run only one Server Task. If **Configure trigger** is not selected in the **Basic** section, a trigger is not created. A task can be created without trigger. Such a task can be run afterward manually or a trigger can be added later.

### Advanced Settings - Throttling

By setting **Throttling**, you can set advanced rules for the created trigger. Setting throttling is optional.

### Summary

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

### 6.7.1.4 Generate Report

The **Generate Report** task is used to generate reports from previously created or pre-defined Report templates.

#### Basic

In this section, you can enter basic information about a task, such as a Name and Description (optional). You can also select from the following task trigger settings:

- **Run task immediately after finish** - Select this option to have the task run automatically after you click Finish.
- **Configure trigger** - Select this option to enable the **Trigger** section, where you can configure trigger settings.
- To set the trigger later, leave this check box deselected.

#### Settings

**Report templates** - Click **Add Report Template** to choose a report template from the list. User creating the task will be able to see and choose only from Report Templates which are available in his group. You can choose multiple report templates for one report.

Select **Send email** or **Save to file** to get the generated report.

**Report delivery**

**Send email**

To send/receive mail messages, you must configure SMTP settings under [Server Settings > Advanced Settings](#).
Send to - Enter the email address(-es) of recipients for report emails. Separate multiple addresses with a comma (,). It is also possible to add CC and BCC fields; these work exactly as they do for mail clients.

Subject - Subject of the report message. Enter a distinctive subject, so that incoming messages can be sorted. This is an optional setting, but we recommend that you do not leave it empty.

Message contents - Define the body of the report message.

Send mail if report is empty - use this option if you want the report to be sent even though there is no data in it.

Print options

Click Show print options to display the following settings:

- **Output format** - Select the appropriate file format. The generated report will be attached to the message and can be printed later.
- **Output language** - Select the language for the message. The default language is based on the language selected for the ERA Web Console.
- **Page size/Resolution/Paper orientation/Color format/Margin units/Margins** - These options are relevant if you want to print the report. Select the appropriate options based on your print preferences. These options only apply to the PDF and PS format, not to the CSV format.

**NOTE**
The Generate report task allows you to select from several output file formats. Selecting CSV results in the date and time values in your report to be stored in the UTC format. When you select either of the two remaining output options (PDF, PS) the report will use the local server time.

Save to file

File options

Relative file path - The report will be generated in a specific directory, for example:

For Windows, report are typically placed in `C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Data\GeneratedReports`

In older Windows systems, the path may be `C:\Users\All Users\ESET\RemoteAdministrator\Server\EraServerApplicationData\Data\GeneratedReports`

For Linux, report are typically placed in `/var/opt/eset/RemoteAdministrator/Server/GeneratedReports/`

Save file if report is empty - use this option if you want the report to be saved even though there is no data in it.

Print options

Click Show print options to display the following settings:

- **Output format** - Select the appropriate file format. The generated report will be attached to the message and can be printed later.
- **Output language** - Select the language for the message. The default language is based on the language selected for the ERA Web Console.
- **Page size/Resolution/Paper orientation/Color format/Margin units/Margins** - These options are relevant if you want to print the report. Select the appropriate options based on your print preferences. These options only apply to the PDF and PS format, not to the CSV format.

**NOTE**
The Generate report task allows you to select from several output file formats. Selecting CSV results in the date and time values in your report to be stored in the UTC format. When you select either of the two remaining output options (PDF, PS) the report will use the local server time.
**Trigger**

The **Trigger** section contains information about the trigger(s) which would run a task. Each Server Task can have up to one trigger. Each trigger can run only one Server Task. If **Configure trigger** is not selected in the **Basic** section, a trigger is not created. A task can be created without trigger. Such a task can be run afterward manually or a trigger can be added later.

**Advanced Settings - Throttling**

By setting **Throttling**, you can set advanced rules for the created trigger. Setting throttling is optional.

**Summary**

All configured options are displayed here. Review the settings and click **Finish** if they are ok. The task is now created and ready to be used.

**NOTE**
The Ubuntu Server Edition requires **X Server** and **xinit** installed for the correct function of the Report Printer (PDF Reports).

```
sudo apt-get install server-xorg
sudo apt-get install xinit
startx
```

6.7.1.5 Rename computers

You can use the **Rename Computers** task to rename computers to FQDN format in ERA. You can use existing server task that came default with your ERA installation. This task automatically renames synchronized computers located in the **Lost & found** group every hour. To create a new task, click **Server Task > Rename computers > New**.

**Basic**

In this section, you can enter basic information about a task, such as a Name and Description (optional). You can also select from the following task trigger settings:

- **Run task immediately after finish** - Select this option to have the task run automatically after you click **Finish**.
- **Configure trigger** - Select this option to enable the **Trigger** section, where you can configure trigger settings.
- **To set the trigger later**, leave this check box deselected.

**Settings**

**Group name** - Select a Static or Dynamic Group or create a **New Static** or **Dynamic Group** for the renamed computers.

**Rename based on:**

- **Computer name** - Each computer is identified on the local network by its unique computer name

- **Computer FQDN (Fully Qualified Domain Name)** - This starts with hostname and continues with domain names all the way up to top-level domain name.

Resolution of name conflicts will be performed for computers already present in ERA (computer name must be unique) and those added via synchronization. Checks only apply to the names of computers outside the subtree being synchronized.
**Trigger**

The Trigger section contains information about the trigger(s) which would run a task. Each Server Task can have up to one trigger. Each trigger can run only one Server Task. If Configure trigger is not selected in the Basic section, a trigger is not created. A task can be created without trigger. Such a task can be run afterward manually or a trigger can be added later.

**Advanced Settings - Throttling**

By setting Throttling, you can set advanced rules for the created trigger. Setting throttling is optional.

**Summary**

All configured options are displayed here. Review the settings and click Finish if they are ok. The task is now created and ready to be used.

### 6.7.1.6 Delete Not Connecting Computers

The Delete not connecting computers task lets you remove computers according to specified criteria. For example, if the ERA Agent on a client computer has not connected for 30 days, it can be removed from ERA Web Console.

**Basic**

In this section, you can enter basic information about a task, such as a Name and Description (optional). You can also select from the following task trigger settings:

- **Run task immediately after finish** - Select this option to have the task run automatically after you click Finish.
- **Configure trigger** - Select this option to enable the Trigger section, where you can configure trigger settings.
- To set the trigger later, leave this check box deselected.

**Settings**

- **Group name** - select a Static or Dynamic Groups or create new a Static or Dynamic Group for renamed computers.

- **Number of days the computer has not been connected** - type number of days after which computers will be removed.

- **Deactivate License** - use this option if you also want to deactivate licenses of removed computers.

- **Remove Unmanaged Computers** - if you select this check box, unmanaged computers will also be removed.

**Trigger**

The Trigger section contains information about the trigger(s) which would run a task. Each Server Task can have up to one trigger. Each trigger can run only one Server Task. If Configure trigger is not selected in the Basic section, a trigger is not created. A task can be created without trigger. Such a task can be run afterward manually or a trigger can be added later.

**Advanced Settings - Throttling**

By setting Throttling, you can set advanced rules for the created trigger. Setting throttling is optional.

**Summary**

All configured options are displayed here. Review the settings and click Finish if they are ok. The task is now created and ready to be used.
6.7.2 Triggers

Triggers are essentially sensors that react to certain events in a pre-defined way. They are used to execute the Server Task they are assigned to. They can be activated by the scheduler (time events) or when a certain system event occurs.

**IMPORTANT**

It is not possible to reuse a trigger. Each Server Task must be triggered with a separate trigger. Each trigger can run only one Server Task.

The trigger does not run newly assigned tasks immediately—the task is run as soon as the trigger is fired. Trigger sensitivity to events can be reduced further using throttling.

Server Trigger types:

**Scheduled**

- **Scheduled Once** - This trigger is invoked once on the scheduled time. Can be delayed by random interval.
- **Daily** - This trigger is invoked every selected day. You can set the start and end of the interval. For example, you can run a Server Task for ten consecutive weekends.
- **Weekly** - This trigger is invoked on a selected day in week. For example, run Server Task every Monday and Friday between 1. July and 31. August.
- **Monthly** - This trigger is invoked on selected days in the selected week of a month, for the selected period of time. The Repeat on value sets on which of selected weekday in the month (eg. second monday) should the task run.
- **Yearly** - This trigger is invoked every year (or more years, if so configured) on the specified start date.

**NOTE**

Random delay interval is available to be set for Scheduled type triggers. It defines the range of maximal delay for task execution. Randomizing can prevent overloading the server.

**EXAMPLE**

If John set the Server Task to trigger Weekly on Monday and Start on 2017 Feb 10 8:00:00, with Random delay interval set to 1 hour and end by set to 2017 Apr 6 00:00:00, the task would run with randomized 1 hour delay between 8:00 and 9:00 every Monday until the specified end date.

Dynamic Group

- **Dynamic Group Members Changed** - This trigger is invoked when the contents of a Dynamic Group change. For example, if clients join or leave a specific Dynamic Group.
- **Dynamic Group Size Changed According to Threshold** - This trigger is invoked when the number of clients in a Dynamic Group becomes higher or lower than the specified threshold. For example, if more than 100 computers are in a given group.
- **Dynamic Group Size Changed Over the Time Period** - This trigger is invoked when the number of clients in a Dynamic Group changes over a defined time period. For example, if the number of computers in a given group increases by 10% in an hour.
- **Dynamic Group Size Changed According to Compared Group** - This trigger is invoked when the number of clients in an observed Dynamic Group change according to a compared group (static or dynamic). For example, if more than 10% of all computers are infected (the group All compared to the group Infected).
Other

- **Server Started** - Is invoked when the server starts. For example, this trigger is used for the Static Group Synchronization task.
- **Event Log Trigger** - This trigger is invoked when a certain event occurs in logs. For example, if there is a threat in the Scan log. This type of trigger provides a set of special settings in the Throttling settings.
- **CRON Expression** - This trigger is invoked at a certain time and date.

Scheduled Trigger will run the task based on date and time settings. Tasks can be scheduled to run once, on a recurring basis, or on CRON expression.

### 6.7.2.1 Cron expression interval

A CRON expression is used to configure specific instances of a trigger. Mostly for scheduled repetitive triggering. It is a string consisting of 6 or 7 fields that represent individual values of the schedule. These fields are separated by space and contain any of the allowed values in various combinations.

CRON expression can be as simple as this: `* * * * ? *` or more complex, like this: `0/5 14,18,3-39,52 * ? JAN,MAR,SEP MON-FRI 2012-2020`

List of values you can use in the CRON expression:

<table>
<thead>
<tr>
<th>Name</th>
<th>Required</th>
<th>Value</th>
<th>Allowed Special Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seconds</td>
<td>Yes</td>
<td>0-59</td>
<td>, - * / R</td>
</tr>
<tr>
<td>Minutes</td>
<td>Yes</td>
<td>0-59</td>
<td>, - * / R</td>
</tr>
<tr>
<td>Hours</td>
<td>Yes</td>
<td>0-23</td>
<td>, - * / R</td>
</tr>
<tr>
<td>Day of the month</td>
<td>Yes</td>
<td>1-31</td>
<td>, - * / ? L W</td>
</tr>
<tr>
<td>Month</td>
<td>Yes</td>
<td>1-12 or JAN-DEC</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day of the week</td>
<td>Yes</td>
<td>0-6 or SUN-SAT</td>
<td>, - / ? L #</td>
</tr>
<tr>
<td>Year</td>
<td>Yes</td>
<td>1970-2099</td>
<td>, - * /</td>
</tr>
</tbody>
</table>

CRON expression syntax is following:

```
+---------- Seconds (0 - 59)
¦  +---------- Minutes (0 - 59)
¦  ¦  +---------- Hours (0 - 23)
¦  ¦  ¦  +---------- Day of the month (1 - 31)
¦  ¦  ¦  ¦  +---------- Month (1 - 12 or JAN-DEC)
¦  ¦  ¦  ¦  ¦  +---------- Day of the week (0 - 6 or SUN-SAT)(for example, 0 is the same as SUN)
¦  ¦  ¦  ¦  ¦  ¦  +---------- Year
¦  ¦  ¦  ¦  ¦  ¦  ¦
* * * * * ? *
```

- The `0 0 0` means midnight (seconds, minutes, hours).
- Use `?` when a value cannot be defined because it was defined in other field (day of the month or day of the week).
- The `*` means every (seconds, minutes, hours, day of the month, month, day of the week, year).
- The SUN means on Sunday.

**NOTE**

The names of months and days of the week are not case sensitive. For example, MON is equal to mon, or JAN is equal to jan.

**Special characters:**
Comma (,)
Commas are used to separate items of a list. For example, using "MON,WED,FRI" in the 6th field (day of the week) means Mondays, Wednesdays and Fridays.

Hyphen (-)
Defines ranges. For example, 2012-2020 indicates every year between 2012 and 2020, inclusive.

Wildcard (*)
Used to select all possible values within a field. For example, * in the minute field means every minute. The wildcard cannot be used in day of the week field.

Question mark (?)
When choosing a specific day, you can specify either day of the month or day of the week. You cannot specify both. If you specify day of the month, you must use ? for day of the week and vice versa. For example, if you want the trigger to fire on a particular day of the month (say, the 10th), but don’t care what day of the week that happens to be, put 10 in the day of the month field and ? in the day of the week field.

Hash (#)
Used to specify “the nth” day of the month. For example, the value of 4#3 in the day of the week field means the third Thursday of the month (day 4 = Thursday and #3 = the 3rd Thursday in the month). If you specify #5 and there isn’t 5th of the given day of the week in the month, then the trigger will not fire that month.

Slash (/)
Describes increments of a range. For example 3-59/15 in the 2nd field (minutes) indicate the third minute of the hour and every 15 minutes thereafter.

Last (L)
When used in the day of the week field, it allows you to specify constructs such as the last Friday (5L) of a given month. In the day of the month field, it specifies the last day of the month. For example, day 31 for January, day 28 for February on non-leap years.

Weekday (W)
The W character is allowed for the day of the month field. This character is used to specify the weekday (Monday-Friday) nearest the given day. As an example, if you specify 15W as the value for day of the month field, the meaning is the nearest weekday to the 15th of the month. So, if the 15th is a Saturday, the trigger fires on Friday the 14th. If the 15th is a Sunday, the trigger fires on Monday the 16th. However, if you specify 1W as the value for day of the month, and the 1st is a Saturday, the trigger fires on Monday the 3rd, as it does not jump over the boundary of a month’s days.

**NOTE**
The L and W characters can also be combined in the day of the month field to result in LW, which translates to last weekday of the month.

Random (R)
The R is a special ERA CRON expression character that allows you to specify randomized time moments. For example, R 0 0 * * ? * trigger fires every day at 00:00 but at a random second (0-59).

**IMPORTANT**
We recommend you to use randomized time moments to prevent all ERA Agents from connecting at the same time to your ERA Server.

Real examples that illustrate some variations of the CRON expression:

<table>
<thead>
<tr>
<th>CRON expression</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 12 ** ? *</td>
<td>Fire at 12pm (noon) every day.</td>
</tr>
<tr>
<td>R 0 0 ** ? *</td>
<td>Fire at 00:00 but at random second (0-59) every day.</td>
</tr>
<tr>
<td>CRON expression</td>
<td>Meaning</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------</td>
</tr>
<tr>
<td>R R R 15W * ? *</td>
<td>Fire at 15th every month at random time (seconds, minutes, hours). If the 15th is a Saturday, the trigger fires on Friday the 14th. If the 15th is a Sunday, the trigger fires on Monday the 16th.</td>
</tr>
<tr>
<td>0 15 10 ** ? 2016</td>
<td>Fire at 10:15am every day during the year 2016.</td>
</tr>
<tr>
<td>0 * 14 * ? *</td>
<td>Fire every minute starting at 2pm and ending at 2:59pm, every day.</td>
</tr>
<tr>
<td>0 0/5 14 * ? *</td>
<td>Fire every 5 minutes starting at 2pm and ending at 2:55pm, every day.</td>
</tr>
<tr>
<td>0 0/5 14,18 * ? *</td>
<td>Fire every 5 minutes starting at 2pm and ending at 2:55pm, and fire every 5 minutes starting at 6pm and ending at 6:55pm, every day.</td>
</tr>
<tr>
<td>0 0-5 14 * ? *</td>
<td>Fire every minute starting at 2pm and ending at 2:05pm, every day.</td>
</tr>
<tr>
<td>0 10,44 14 ? 3 WED *</td>
<td>Fire at 2:10pm and at 2:44pm every Wednesday in March.</td>
</tr>
<tr>
<td>0 15 10 ? * MON-FRI</td>
<td>Fire at 10:15am every weekday (Monday, Tuesday, Wednesday, Thursday and Friday).</td>
</tr>
<tr>
<td>0 15 10 15 * ? *</td>
<td>Fire at 10:15am on the 15th day of every month.</td>
</tr>
<tr>
<td>0 15 10 ? * 5L</td>
<td>Fire at 10:15am on the last Friday of every month.</td>
</tr>
<tr>
<td>0 15 10 ? * 5L 2016-2020</td>
<td>Fire at 10:15am on every last Friday of every month from the year 2016 to 2020, inclusive.</td>
</tr>
<tr>
<td>0 15 10 ? * 5#3</td>
<td>Fire at 10:15am on the 3rd Friday of every month.</td>
</tr>
<tr>
<td>0 0 * * ? *</td>
<td>Fire every hour, every day.</td>
</tr>
</tbody>
</table>
6.7.3 Advanced Settings - Throttling

Throttling is used to restrict a task from being executed. Usually throttling is used when a task is triggered by a frequently occurring event. Under certain circumstances, throttling may prevent a trigger from being fired. Each time the trigger is triggered, it is evaluated according to the schema below. Only those triggers which meet the specified conditions would then make the task execute. If no throttling conditions are set, all trigger events would run the task.

There are two types of conditions for Throttling: time-based and statistical. For a task to be executed:

- It has to pass both types of conditions
- Conditions must be set; if a condition is empty, it is omitted
- All time-based conditions must pass, as they are evaluated with the AND operator
- All statistical conditions evaluated with the AND operator must pass; at least one statistical condition with the OR operator must pass
- Statistical and time conditions set together must pass, as they are evaluated with the AND operator—only then is the task executed

If any of the defined conditions are met, stacked information for all observers is reset (the count starts over from 0). This holds for time-based as well as statistical conditions. This information is also reset if the Agent or ERA Server is restarted. All modifications made to a trigger reset its status. We recommend that you only use one statistical condition and multiple time-based conditions. Multiple statistical conditions can cause unnecessary complications, and can alter trigger results.

**Time-based criteria**

All of the configured conditions must be fulfilled in order to trigger the task.
Aggregate invocations during time period (T2) - Allow triggering once during the specified time period. If for example, this is set to ten seconds and during this time ten invocations occur, only the first would trigger the event.

Time ranges (T1) - Allows triggering only within the defined time period. You can add multiple time ranges to the list—they will be sorted chronologically.

Statistical criteria

Statistical criteria application - Statistical conditions can be combined using either the AND logical operator (all conditions must be fulfilled) or the OR logical operator (the first condition fulfilled triggers the action).

Triggered every No of occurrences (S1) - Allows only every x-th trigger hit. For example, if you enter ten, only each tenth triggering will be counted.

No of occurrences within a time period (S2) - Allows only triggering within the defined time period. This will define the minimal frequency of events to trigger the task. For example, you can use this setting to allow the execution of the task if the event is detected 10x in an hour. Firing of the trigger causes a counter reset.

• Time period - Define the time period for the option described above.

A third statistical condition is available only for certain trigger types. See: Trigger > Trigger type > Event Log Trigger.

Event log criteria

This criteria are evaluated by ERA as third statistical criteria (S3). The Statistical criteria application operator (AND / OR) is applied to evaluate all three statistical conditions together. It is recommended to use event log criteria in combination with the Generate Report task. All three fields are required for the criteria to work. The buffer of symbols is reset if the trigger is fired and there is a symbol already in buffer.

Symbol - According to Log type, which is set in the Trigger menu, you can choose a symbol in the log which you can then search for. Click Change to display the menu. You can remove the selected symbol by clicking Remove.

Number of events with symbol - Enter the integer number of distinct events with selected symbol to run the task.

Applies when number of events - This sets what type of events would trigger the condition. The available options are:

• Received in a Row - Selected number of events must occur in a row. These events must be distinctive.
• Received Since Last Trigger Execution - The condition is triggered when the selected number of distinctive events is reached (since last task execution).

NOTE

When in use with a Server Task, all client computers are considered. It is unlikely to receive higher number of distinctive symbols in a row. Use the Received in a Row setting only for reasonable cases. A missing value (N/A) is considered as "not unique" and therefore the buffer is reset in this point.

Additional properties

As stated above, not every event will cause a trigger to fire. Actions taken for non-firing events can be:

• If there is more than one event skipped, group the last N events into one (store data of suppressed ticks) [N <= 100]
• For N == 0, only the last event is processed (N means history length, where the last event is always processed)
• All non-firing events are merged (merging the last tick with N historical ticks)

If the trigger fires too often or you want to be notified less often, consider the following suggestions:
• If the user wants to react only if there are more events, not a single one, see statistical condition S1
• If the trigger should fire only when a cluster of events occur, follow statistical condition S2
• When events with unwanted values are supposed to be ignored, refer to statistical condition S3
• When events from outside relevant hours (for example, working hours) should be ignored, see time-based condition T1
• To set a minimum time between trigger firings, use time-based condition T2

**NOTE**
The conditions can also be combined to form more complex throttling scenarios. See the [throttling examples](#) for more details.

### 6.7.3.1 Throttling Examples

Throttling examples explain how the throttling conditions (T1, T2, S1, S2, S3) are combined and evaluated.

**NOTE**
"Tick" means impulse from the trigger. "T" stands for time-based criteria, "S" stands for statistical criteria. "S3" stands for event log criteria.

#### S1: Criterion for occurrences (allow every third tick)

<table>
<thead>
<tr>
<th>Time</th>
<th>00</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>trigger is modified</th>
<th>07</th>
<th>08</th>
<th>09</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticks</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### S2: Criterion for occurrences within time (allow if three ticks occur within four seconds)

<table>
<thead>
<tr>
<th>Time</th>
<th>00</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>trigger is modified</th>
<th>07</th>
<th>08</th>
<th>09</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticks</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

#### S3: Criterion for unique symbol values (allow if three unique values are in a row)

<table>
<thead>
<tr>
<th>Time</th>
<th>00</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>trigger is modified</th>
<th>07</th>
<th>08</th>
<th>09</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>A</td>
<td>B</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>G</td>
<td>H</td>
<td></td>
<td>J</td>
<td>K</td>
<td>n/a</td>
<td>L</td>
<td>M</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>S3</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

#### S3: Criterion for unique symbol values (allow if three unique values are since the last tick)

<table>
<thead>
<tr>
<th>Time</th>
<th>00</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>07</th>
<th>trigger is modified</th>
<th>08</th>
<th>09</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>A</td>
<td>B</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>G</td>
<td>H</td>
<td>I</td>
<td></td>
<td>J</td>
<td>K</td>
<td>n/a</td>
<td>L</td>
<td>M</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>S3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

#### T1: Allow a tick in certain time ranges (allow every day starting at 8:10, duration 60 seconds)

<table>
<thead>
<tr>
<th>Time</th>
<th>8:09:50</th>
<th>8:09:59</th>
<th>8:10:00</th>
<th>8:10:01</th>
<th>trigger is modified</th>
<th>8:10:59</th>
<th>8:11:00</th>
<th>8:11:01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticks</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

This criterion has no state; therefore trigger modifications have no effect on the results.
### T2: Allow a single tick in a time interval (allow at most once every five seconds)

<table>
<thead>
<tr>
<th>Time (00-13)</th>
<th>00</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>trigger modified</th>
<th>07</th>
<th>08</th>
<th>09</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticks</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>T2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### S1+S2 combination
- S1: every fifth tick
- S2: three ticks within four seconds

<table>
<thead>
<tr>
<th>Time (00-16)</th>
<th>00</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>07</th>
<th>08</th>
<th>09</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticks</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>S1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Result</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The result is enumerated as: S1 (logical or) S2

### S1+T1 combination
- S1: Allow every third tick
- T1: Allow every day starting at 8:08, duration 60 seconds

<table>
<thead>
<tr>
<th>Time: 8:07:50-8:09:01</th>
<th>8:07:50</th>
<th>8:07:51</th>
<th>8:07:52</th>
<th>8:07:53</th>
<th>8:08:10</th>
<th>8:08:11</th>
<th>8:08:19</th>
<th>8:08:54</th>
<th>8:08:55</th>
<th>8:09:01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticks</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>S1</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Result</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

The result is enumerated as: S1 (logical and) T1

### S2+T1 combination
- S2: three ticks within ten seconds
- T1: Allow every day starting at 8:08, for a duration of 60 seconds

<table>
<thead>
<tr>
<th>Time: 8:07:50-8:09:01</th>
<th>8:07:50</th>
<th>8:07:51</th>
<th>8:07:52</th>
<th>8:07:53</th>
<th>8:08:10</th>
<th>8:08:11</th>
<th>8:08:19</th>
<th>8:08:54</th>
<th>8:08:55</th>
<th>8:09:01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticks</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>S2</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Result</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

The result is enumerated as: S2 (logical and) T1.

Note that the state of S2 is reset only when the global result is 1.
S2+T2 combination

- S2: three ticks within ten seconds
- T2: Allow at most once every 20 seconds

<table>
<thead>
<tr>
<th>Time</th>
<th>00</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>07</th>
<th>...</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticks</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>S2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Result</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The result is enumerated as: S2 (logical and) T2.
Note that the state of S2 is reset only when the global result is 1.

6.8 Notifications

Notifications are essential for keeping track of the overall state of your network. When a new event occurs (based on your configuration), you will be notified using a defined method (either an SNMP Trap or email message), and you can respond accordingly.

- All notification templates are displayed in the list and can be filtered by Name or Description.
- Click Add Filter to add filtering criteria and/or enter a string into the Name/Notification field.
- Select an existing notification to edit or delete it.
- To create a new notification, click New notification on the bottom of the page.
- Click Duplicate to create a new notification based on the selected notification (a new name is required for the duplicate task).
- A user can see only notifications that are contained in a group for which he has Read permissions.

Notifications, users and permissions

Similar to Server Tasks, the use of Notifications is restricted by the permissions of the current user. Every time the notification is executed, there is an executing user whose permissions are taken into account. The executing user is always the one who edited the notification last.

IMPORTANT

For a notification to work well, it is necessary that the executing user has sufficient permissions for all referenced objects (devices, groups, templates.). Typically, Read and Use permissions are required. If the user does not have these permissions, or he loses them afterward, the notification will fail. Failed notifications are highlighted with orange and will trigger an email to notify the user.

Create notification - To create a notification the user must have Write permissions for notifications on his home group. A new notification is created in the user's home group.

Modify notification - To be able to modify a notification, the user must have Write permissions for notifications on a group where the notification is located.

Remove notification - To be able to delete a notification, the user must have Write permissions for notifications on a group where the notification is located.

Access Group Filter

The Access Group filter button enables users to select a static group and filter viewed objects according to the group where they are contained.
EXAMPLE

John, whose Home Group is John’s Group, wants to remove (or modify) Notification 1. The notification was originally created by Larry, therefore it is automatically contained in Larry's Home group, Larry’s Group. The following conditions must be met for John to remove (or modify) Notification 1:

- John must be assigned a permissions set with Write permissions for notifications
- The permissions set must contain Larry’s Group under Static Groups

6.8.1 Manage Notifications

Notifications are managed in the Admin tab. Select a notification and click Edit Notification or Duplicate.

Basic

You can edit the Notification Name and Description fields to make it easier to filter between different notifications.

Notification template

Existing Dynamic Group - An existing Dynamic Group will be used to generate notifications. Select a Dynamic Group from the list and click OK.

Dynamic Group Size Changed According to Compared Group - If the number of clients in a Dynamic Group changes according to a compared group (either static or dynamic), the notification will be invoked.

NOTE

You can assign a notification only to a Dynamic Group where you have sufficient permissions. Dynamic Groups that are out of your home group will not be visible.

Other Event Log Template

This option is used for notifications not associated with a Dynamic Group, but based on system events filtered out from the event log. Select a log type on which the notification will be based and a logical operator for filters.

Tracked State - This option notifies you of object state changes in relation to your user-defined filters.
NOTE
You can change the tracked state and + Add Filter or Logical operator for filters.

Configuration

Notify every time the Dynamic Group content changes - Enable this to be notified when members of a Dynamic Group are added, removed or changed. ERA checks the Dynamic Group once every 20 minutes.

Notification time period - Define the time period (in minutes, hours or days) for the comparison with the new state. For example, seven days ago the number of clients with outdated security products was ten and the threshold (see below) was set to 20. If the number of clients with an outdated security product reaches 30, you will be notified.

Threshold - Define a threshold that will trigger the sending of a notification. You can either define a number of clients, or a percentage of clients (members of the Dynamic Group).

Generated message - This is a pre-defined message that will appear in the notification. It contains configured settings in text form.

Message - Beside the pre-defined message, you can add a custom message that will appear at the end of the pre-defined message above. This is optional, but it is recommended for better filtering of notifications and overview.

NOTE
Available options depend on the notification template you select.

Advanced settings - Throttling

Aggregation
Aggregation condition is available only for the following notification templates:

- Other Event Log Template
- Existing Dynamic Group

Number of ticks to aggregate - This will define how many ticks (trigger hits) are needed in order to activate the trigger. For more specific information, see the Throttling chapter.

Time-based criteria
All of the configured conditions must be fulfilled in order to trigger the task.

Aggregate invocations during time period (T2) - Allow triggering once during the specified time period. If for example, this is set to ten seconds and during this time ten invocations occur, only the first would trigger the event.

Time ranges (T1) - Allows triggering only within the defined time period. You can add multiple time ranges to the list—they will be sorted chronologically.

Statistical criteria

Statistical criteria application - Statistical conditions can be combined using either the AND logical operator (all conditions must be fulfilled) or the OR logical operator (the first condition fulfilled triggers the action).

Triggered every No of occurrences (S1) - Allows only every x-th trigger hit. For example, if you enter ten, only each tenth triggering will be counted.

No of occurrences within a time period (S2) - Allows only triggering within the defined time period. This will define the minimal frequency of events to trigger the task. For example, you can use this setting to allow the execution of the task if the event is detected 10x in an hour. Firing of the trigger causes a counter reset.

- Time period - Define the time period for the option described above.

A third statistical condition (Event log criteria) is available only for Other Event Log Template, which can be set in the Notification template section.
Event log criteria

This criteria are evaluated by ERA as third statistical criteria (S3). The Statistical criteria application operator (AND / OR) is applied to evaluate all three statistical conditions together. It is recommended to use event log criteria in combination with the Generate Report task. All three fields are required for the criteria to work. The buffer of symbols is reset if the trigger is fired and there is a symbol already in buffer.

Symbol - According to Log type, which is set in the Trigger menu, you can choose a symbol in the log which you can then search for. Click Change to display the menu. You can remove the selected symbol by clicking Remove.

Number of events with symbol - Enter the integer number of distinct events with selected symbol to run the task.

 Applies when number of events - This sets what type of events would trigger the condition. The available options are:

• Received in a Row - Selected number of events must occur in a row. These events must be distinctive.
• Received Since Last Trigger Execution - The condition is triggered when the selected number of distinctive events is reached (since last task execution).

Distribution

Subject - The subject of a notification message. This is optional, but also recommended for better filtering, or when creating rules to sort messages.

Distribution

• Send SNMP Trap - Sends an SNMP Trap. The SNMP Trap notifies the Server using an unsolicited SNMP message. For more information, see How to configure an SNMP Trap Service.
• Send email - Sends an email message based on your email settings.
• Send syslog - You can use ERA to send notifications and event messages to your Syslog server. Also, it is possible to export logs from a client's ESET product and send them to the Syslog server.

Email addresses - Enter the email addresses of the recipients of the notification messages, separate multiple addresses with a comma (",").

Syslog severity - Choose the severity level from the drop-down menu. Notifications will then appear with such severity on the Syslog server.

Click Finish to create a new template based on the template you are editing. You will be required to enter a name for the new template.

6.8.2 How to configure an SNMP Trap Service

To successfully receive SNMP messages, the SNMP trap service needs to be configured. Configuration steps according to operating system:

WINDOWS

Prerequisites

• The Simple Network Management Protocol service must be installed on the machine where ERA Server is installed, as well as the machine where the SNMP trap software will be installed.
• Both computers (above) should be in the same subnet.
• The SNMP Service must be configured on the ERA Server computer.
SNMP Service configuration (ERA Server)

1. Press the Windows key + R to open a run dialog box, type Services.msc into the Open field and press Enter. Search for the SNMP Service.
2. Open the Traps tab, type public into the Community name field and click Add to list.
3. Click Add, type the Host name, IP or IPX address of the computer where the SNMP trapping software is installed into the appropriate field and click Add.
4. Proceed to the Security tab. Click Add to display the SNMP Service Configuration window. Type public into the Community name field and click Add. Rights will be set to READ ONLY, this is ok.
5. Make sure that Accept SNMP packets from any hosts is selected and click OK to confirm. The SNMP service is not configured.

SNMP Trap Software configuration (Client)

1. The SNMP Service is installed and doesn’t need to be configured.
2. Install AdRem SNMP Manager or AdRem NetCrunch.
3. AdRem SNMP Manager: Start the application and select Create New SNMP Node List. Click Yes to confirm.
4. Check the network address of your subnet (displayed in this window). Click OK to search your network.
5. Wait for the search to finish, the search results will be displayed in the Discovery results window. The IP address of the ERA Server should be displayed in this list.
6. Select the IP address of the server and click OK. Your server address is displayed in the Nodes section.
7. Click Trap Receiver Stopped and select Start. Trap Receiver Started will be displayed. Now you can receive SNMP messages from your ERA Server.

LINUX and ERA Virtual Appliance

1. ERA VA already contains needed package. On other Linux systems, install the snmpd package by running one of the following commands:
   - apt-get install snmpd snmp (Debian, Ubuntu distributions)
   - yum install net-snmp (Red-Hat, Fedora distributions)
2. Open the /etc/default/snmpd file and make the following attribute edits:
   - SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
   - Adding # will disable this line completely.
   - SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -c /etc/snmp/snmpd.conf'
   - Add this line to the file.
   - TRAPDRUN=yes
   - Change the trapdrun attribute to yes.
3. Create a backup of the original snmpd.conf file. The file will be edited later.
   - mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original
4. Create a new snmpd.conf file and add these lines:
   - rocommunity public
   - syslocation "Testing ERA6"
   - syscontact admin@ERA6.com
5. Open the /etc/snmp/snmptrapd.conf file and add the following line at the end of the file:
   - authCommunity log,execute,net public
6. Type the following command to start the SNMP manager services and logging of incoming traps:
   - /etc/init.d/snmpd restart
   - or
   - service snmpd restart
7. To check if the trap is working and catching the messages, run the following command:
   - tail -f /var/log/syslog | grep -i TRAP
6.9 Certificates

Certificates are an important part of ESET Remote Administrator, they are required for ERA components to communicate with ERA Server. To make sure all components can communicate correctly, all Peer Certificates need to be valid and signed by the same Certification Authority.

You can create a new **Certification Authority** and **Peer Certificates** in ERA Web Console, follow the instructions in this guide to:

- **Create a new Certification Authority**
  - Import a Public Key
  - Export a Public Key
  - Export a Public Key in BASE64 format

- **Create a new Peer Certificate**
  - Create a Certificate
  - Export a Certificate
  - Create an APN certificate
  - Revoke a certificate
  - Certificate usage
  - Set new ERA Server certificate
  - Custom certificates with ESET Remote Administrator
  - Expiring Certificate - reporting and replacement

**IMPORTANT**
macOS / OS X does not support Certificates with expiry date January 19, 2038 and later. ERA Agent running on macOS / OS X will not be able to connect to ERA Server.

**NOTE**
For all Certificates and Certification Authorities created during installation of ERA components, the Valid from value is set to 2 days before certificate creation.

For all Certificates and Certification Authorities created in the ERA Web Console, the Valid from value is set to 1 day before certificate creation. The reason for this is to cover all possible time discrepancies between affected systems.

For example, a Certification Authority and Certificate, created 2017 Jan 12 during installation will have a pre-defined Valid from value of 2017 Jan 10 00:00:00, and a Certificate Authority and Certificate created 2017 Jan 12 in ERA Web Console will have a pre-defined Valid from value of 2017 Jan 11 00:00:00.
6.9.1 Peer Certificates

If a Certification Authority is present on your system, you should create a peer certificate for individual ESET Remote Administrator components. Each component (ERA Agent, ERA Proxy and ERA Server) requires a specific certificate.

촉 New...
This option is used to create a new certificate. These certificates are used by the ERA Agent, ERA Proxy and ERA Server.

APN/DEP Certificate
This option is used to create a new APN/DEP certificate. This certificate is used by the MDM. This action requires a valid license.

Certificate usage
You can also check which clients are using this ERA certificate.

Edit...
Select this option to edit an existing certificate from the list. The same options apply as when you create a new certificate.

Export...
This option is used to export a certificate as a file. This file is necessary if you install the ERA Agent locally on a computer or when installing MDM.

Export as Base64...
This option is used to export a certificate as a .txt file.

Revoke...
If you no longer want to use a certificate, select Revoke. This option invalidates the certificate. Invalid certificates will not be accepted by ESET Remote Administrator.

IMPORTANT
The revoke action is irreversible, you will not be able to use a certificate that has been revoked. Make sure there are no ERA Agents left using this certificate before you revoke it. This will prevent loss of connection to client computers or servers (ERA Server, ERA Proxy, Mobile Device Connector, Virtual Agent Host).

Access Group
A certificate or a authority can be moved to other group. Then it becomes available to users who have sufficient rights for this group. To easily find a certificate's home group select the certificate and click Access Group in the drop down menu. The home group of the certificate is displayed in the first line of the pop up menu (for example, / All/San Diego. See our sample scenario to learn more about sharing certificates).

IMPORTANT
You will see only those certificates located in your home group (assuming you have read permission for certificates). Certificates which are created during the ERA installation are located in the All group and only administrators have access to them.

Show Revoked - shows you all revoked certificates.

Agent certificate for server assisted installation - This certificate is generated during server installation if you select the Generate certificates option.

Access Group Filter

The Access Group filter button enables users to select a static group and filter viewed objects according to the group where they are contained.
6.9.1.1 Create a new Certificate

As part of the installation process, ESET Remote Administrator requires that you create a Peer certificate for Agents. These certificates are used to authenticate products distributed under your license.

**NOTE**
There is one exception, an Agent certificate for server assisted installation cannot be created manually. This certificate is generated during server installation, provided that Generate certificates is selected.

To create a new certificate in the ERA Web Console, navigate to Admin > Certificates and click Actions > New.

**Basic**

- **Description** - Enter description for the certificate.
- **Product** - Select the type of certificate you want to create 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 that you leave this field blank, but you can set a passphrase for the certificate that will be required when clients attempt to activate.

**Attributes (subject)**

These fields are not mandatory, but you can use them to include more detailed information about this certificate.

- **Common name** - This value should contain the string "Agent", "Proxy" or "Server", according to the selected Product. If you want, you can enter descriptive information about the certificate.

Enter the **Valid from** and **Value to** values to ensure that the certificate is valid.

**NOTE**
For all Certificates and Certification Authorities created during installation of ERA components, the Valid from value is set to 2 days before certificate creation.

For all Certificates and Certification Authorities created in the ERA Web Console, the Valid from value is set to 1 day before certificate creation. The reason for this is to cover all possible time discrepancies between affected systems.

For example, a Certification Authority and Certificate, created 2017 Jan 12 during installation will have a pre-defined Valid from value of 2017 Jan 10 00:00:00, and a Certificate Authority and Certificate created 2017 Jan 12 in ERA Web Console will have a pre-defined Valid from value of 2017 Jan 11 00:00:00.

**Sign**

Select from two signing methods:

- **Certification authority** - If you would like to sign using the ERA Certification Authority (created CA during ERA installation).
  - Select the ERA Certification Authority from the list of certification authorities
  - Create a new certification authority
- **Custom pfx file** - To use a custom .pfx file, click Browse, navigate to your custom .pfx file and click OK. Select Upload to upload this certificate to the Server.

**NOTE**
If you would like to sign a new certificate using the ERA CA (created during ERA installation) in ERA Virtual Appliance, it is necessary to enter a Certification Authority Passphrase. This is the password you specified during ERA VA configuration.
Review the certificate information you entered and click Finish. The certificate is now successfully created and will be available in the Certificates list to use when installing the Agent. The certificate will be created in your home group.

NOTE
As an alternative to creating a new certificate, you can Import a Public Key, Export a Public Key or Export a Peer Certificate.

6.9.1.2 Export Peer Certificate

Export a Peer Certificates

1. Select the Peer Certificates you want to use from the list and select the check box next to it.
2. From the context menu select Export. The certificate will be exported (including private key) as a .pfx file. Type a name for your public key and click Save.

Export as Base64 from Peer Certificates:

Certificates for ERA components are available in Web Console. To copy the contents of a certificate in Base64 format, click Admin > Peer Certificates, select a certificate and then select Export as Base64. You can also download the Base64 encoded certificate as a file. Repeat this step for other component certificates as well as for your Certification Authority.

6.9.1.3 APN/DEP certificate

An APN (Apple Push Notification) / DEP (Device Enrollment Program) certificate is used by ERA MDM for iOS device enrollment. You must create an Apple-provided push certificate and get it signed by Apple before you can enroll iOS devices in ERA. Also make sure you have a valid license for ERA.

Click the Admin tab > Certificates > Peer Certificates, click New and then select APN/DEP Certificate.

NOTE
To acquire an APN certificate, you will need an Apple ID. This ID is required for Apple to sign the certificate.

To acquire a DEP enrollment token, you will need an Apple DEP Account.
Specify the certificate attributes (Country code, Organization name, etc.) and click **Submit request**.

1. Open the [Apple Push Certificates Portal](https://example.com) and log in using your **Apple ID**.

2. Click **Create a Certificate**.

3. Fill in the note (optional). Click on Choose File and upload the CSR file you downloaded in previous step and click **Upload**.

4. After a while you will see a new confirmation screen with the information that your APNS certificate for ESET Mobile Device Management server was successfully created.

5. Proceed by clicking on **Download** button and save the `.pem` file to your computer.


Download your **CSR** (Certification Signing Request) and **Private Key**.

Certificate

1. Open the [Apple Push Certificates Portal](https://example.com) and log in using your **Apple ID**.

2. Click **Create a Certificate**.

3. Fill in the note (optional). Click on Choose File and upload the CSR file you downloaded in previous step and click **Upload**.

4. After a while you will see a new confirmation screen with the information that your APNS certificate for ESET Mobile Device Management server was successfully created.

5. Proceed by clicking on **Download** button and save the `.pem` file to your computer.

Important

APNS certificate is required for both DEP and non-DEP MDC policy.

If you are creating a DEP Enrollment certificate, continue here.

Apple Push Certificates Portal

Certificates for Third-Party Servers

<table>
<thead>
<tr>
<th>Service</th>
<th>Vendor</th>
<th>Expiration Date*</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Device Management</td>
<td>ESET, spol. s.r.o.</td>
<td>Dec 16, 2017</td>
<td>Active</td>
<td>Renew</td>
</tr>
</tbody>
</table>

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

Upload

Once you have completed the steps above, you can create a Policy for MDC to activate APNS for iOS enrollment. You can then Enroll any iOS device by visiting https://<mdmcore>:<enrollmentport>/unique_enrollment_token from the device’s browser.
6.9.1.4 Show revoked

This list displays all certificates that have been created and then invalidated by the ERA Server. Revoked certificates will automatically be removed from the main Peer certificate screen. Click Show Revoked to view certificates that have been revoked from the main window.

To revoke a certificate, follow the steps below:

1. Go to Admin > Certificates > Peer Certificates > select a certificate and click Revoke...

2. Specify the Reason for revocation and click Revoke.

3. Click OK. The certificate will disappear from the list of Peer Certificates. To see previously revoked certificates, click Show revoked button.
6.9.1.5  Set new ERA Server certificate

Your ERA Server certificate is created during installation and distributed to ERA Agents and other components to allow communication to the ERA Server. If necessary, you can configure ERA Server to use a different peer certificate. You can use ERA Server certificate (generated automatically during installation) or a Custom certificate. The ERA Server certificate is required for a secure TLS connection and authentication. The Server certificate is used to make sure that ERA Agents and ERA Proxies do not connect to an illegitimate server. Click Tools > Server Settings to edit certificate settings.

1. Click Admin > Server Settings > expand section Connection, select Change certificate.

2. Choose from the two Peer certificate types:
   - Remote Administrator certificate - click Open certificate and select the certificate to use.
   - Custom certificate - browse to your custom certificate. If you are performing a migration, select the exported certificate from your old ERA Server.
3. Select **Custom certificate**, select the ERA Server certificate .pfx file you exported from the old server and then click **OK**.

4. **Restart** the ERA Server service, see our Knowledgebase article.

### 6.9.1.6 Custom certificates with ESET Remote Administrator

If you have your own PKI (public key infrastructure) within your environment and want ESET Remote Administrator to use your custom certificates for communication between its components, the following steps will guide you through the process of setting it all up. The example shown below was performed on a Windows Server 2012 R2. In case you are using different version of Windows Server, some screens may slightly vary for you, buy the objective of the procedure remains the same.

**NOTE**

An easier way to create a custom certificate is to use keytool, which is included in Java. For more information, read our Knowledgebase article.

**Required server roles:**

- Active Directory Certificate Services (AD CS).
- Active Directory Domain Services.

1. **Open** Management Console and add Certificates Snap-ins:

   - Log on to the server as a member of the local Administrator group.
   - **Run** mmc.exe to open Management Console.
   - Click **File** in the top menu and select **Add/Remove Snap-in...** (or press CTRL+M).
   - Select Certificates in the left pane and click **Add** button.
Select **Computer Account** and click **Next**.

Make sure **Local Computer** is selected (default) and click **Finish**.

Click **OK**.

2. Create **Custom Certificate Request**:

- Double-click **Certificates (Local Computer)** to expand it.
- Double-click **Personal** to expand it. Right-click **Certificates** and select **All Tasks > Advanced Operations** and choose **Create Custom Request**...
- Certificate Enrollment wizard window will open, click **Next**.
- Select the **Proceed without enrollment policy** option and click **Next** to continue.

- **Choose (No Template) Legacy Key** from the drop-down list and make sure that **PKCS #10** Request format is selected. Click **Next**.
• Expand **Details** section by clicking the arrow pointing down, then click **Properties** button.

• In the **General** tab, type in **Friendly name** for your certificate, you can also type **Description** (optional).
• In the **Subject** tab, do the following:
In **Subject name** section, choose **Common Name** from the drop-down list under **Type** and enter **era server** into the **Value** field, then click **Add** button. **CN=era server** will appear in the information box on the right. If you are creating certificate request for ERA Agent or ERA Proxy, type **era agent** or **era proxy** to the value field of Common name.

**NOTE**

Common Name must contain one of these strings: "server", "agent" or "proxy", depending on which Certificate Request you want to create.

In **Alternative name** section, choose **DNS** from the drop-down list under **Type** and enter * (asterisk) into the **Value** field, then click **Add** button.

- In the **Extensions** tab, expand **Key usage** section by clicking the arrow pointing down. Add the following from the Available options: **Digital signature**, **Key agreement**, **Key encipherment**. Deselect **Make these key usages critical** option using the checkbox.
In the Private Key tab, do the following:

Expand Cryptographic Service Provider section by clicking the arrow pointing down. You'll see a list of all cryptographic service providers (CSP). Make sure that only Microsoft RSA SChannel Cryptographic Provider (Encryption) is selected.

NOTE
Deselect all other CSPs (except the Microsoft RSA SChannel Cryptographic Provider (Encryption) which must be selected).
Expand **Key Options** section. In the **Key size** menu, select a value of at least **2048**. Select **Make private key exportable**.

Expand **Key Type** section, select **Exchange** option. Click **Apply**, and check your settings.

Click **OK** button. Certificate information will be displayed, and click then **Next** button to continue. Click on **Browse** button to select the location where the certificate signing request (CSR) will be saved. Type the file name and make sure the **Base 64** is selected.
Click **Finish** button, your **CSR** now has been generated.

3. Import **Custom Certificate Request** and Issue **Custom Certificate** from Pending Requests.
   - Open **Server Manager**, click **Tools > Certification Authority**.
   - In the **Certification Authority (Local)** tree, select **Your Server (usually FQDN) > Properties > Policy Module** tab, click **Properties**... button. Make sure you have **Set the certificate request status to pending**. The administrator **must explicitly issue the certificate** option selected. If not, use the radio button to select this option. Otherwise, it will not work properly. In case you've changed this setting, restart Active Directory certificate services.
In the Certification Authority (Local) tree, select Your Server (usually FQDN) > All Tasks > Submit new request... and navigate to previously generated CSR file in step 2.

Certificate will be added into Pending Requests. Select the CSR in the right navigation pane. In the Action menu, select All Tasks > Issue.

• Click **Issued** Certificates in the left pane. Right-click the certificate you want to export, click **All Tasks > Export Binary Data**...

• In the Export Binary Data dialog, choose **Binary Certificate** from the drop-down list and in Export options, click **Save binary data to a file** and then click **OK**.

![Export Binary Data dialog](image.png)

• In the Save Binary Data dialog box, move to the file location where you want to save the certificate, and then click **Save**.

5. **Import created .tmp file.**

• Go to **Certificate (Local Computer) > right-click Personal**, select **All Tasks > Import...**

• Click **Next**...

• Locate previously saved .tmp binary file using **Browse...** click **Open**. Select Place all certificates in the following store > **Personal**. Click **Next**.

• The certificate will be imported after you click **Finish**.

6. **Export Certificate including private key to .pfx file.**

• In the **Certificates (Local Computer)** expand **Personal** and click **Certificates**, select created certificate that you want to export, on the **Action** menu, point to **All Tasks > Export...**

• In the **Certificate Export Wizard**, click **Yes, export the private key**. (This option will appear only if the private key is marked as exportable and you have access to the private key.)

• Under Export File Format, select **To include all certificates in the certification path**, select the **Include all certificates in the certification path if possible** check box and then click **Next**.
- **Password**, type a password to encrypt the private key you are exporting. In Confirm password, type the same password again, and then click **Next**.
• **File name**, type a file name and path for the `.pfx` file that will store the exported certificate and private key. Click **Next**, and then click **Finish**.

7. Once you have your custom .pfx certificate file created, you can configure ERA components to use it.

   **NOTE**
   The above example shows you how to create ERA Server certificate. Repeat the same steps for ERA Agent and ERA Proxy certificates. ERA Proxy certificate can be used by ERA MDM.

Configure ERA Server to [start using custom .pfx certificate](#).
To get ERA Agent or ERA Proxy, ERA MDM to use custom `.pfx` certificate, run repair of the appropriate component. Navigate to Start > Program and Features, right-click ESET Remote Administrator Agent and select Change. Click Next button and run Repair. Click Next leaving Server host and Server port as they were. Click Browse button next to Peer certificate and locate custom `.pfx` certificate file. Type in the certificate's password you've specified in step 6. Click Next and complete the repair. ERA Agent is now using custom `.pfx` certificate.

![ESET Remote Administrator Agent Setup](image)

### 6.9.1.7 Expiring Certificate - reporting and replacement

ERA is able to notify you about a Certificate or a Certification Authority that is going to expire. There are predefined Notifications for both ERA Certificate and ERA Certification Authority in the Notifications tab. To activate this feature, click Edit Notification and specify details in the Distribution section, such as email address or SNMP trap. Each user is able to see notifications only for those certificates which are in his home group (given he has assigned Read permissions for Certificates).

**NOTE**

Make sure you have configured SMTP connection settings in Server settings first. Once done, you can edit notification to add Distribution email address.

If a computer has a certificate which is about to expire, its status information will automatically change. The status will be reported to Dashboard, Computers list, Status Overview and Certificate tab:
To replace an expiring Certification Authority or Certificate, follow these steps:

1. **Create new Certification Authority** with new validity period (in case the old one is going to expire), ideally making it valid immediately.

2. Create new **Peer Certificates** for ERA Server and other components (Agent/Proxy/MDM) within the validity period of your new Certification Authority.

3. Create policies to set new Peer Certificates. Apply the policies to ERA components, ERA Proxy, MDM and to ERA Agent on all client computers in your network.

4. Wait until the new Certification Authority and Peer Certificates are applied and the clients were replicated.

   **NOTE**
   
   Ideally, wait 24 hours or check if all of your ERA components (Agents/Proxy) have replicated at least twice.

5. Replace **Server certificate in ERA Server Settings** so that clients are able to authenticate using their new Peer Certificates.

6. Once you have completed all the steps above, every client is connecting to ERA and all is working as expected, revoke old Peer Certificates and delete the old Certification Authority.
6.9.2 Certification Authorities

Certification Authorities are listed and managed in the Certification Authorities section. If you have multiple Certification Authorities, you can apply a filter to sort them.

**NOTE**

Certification Authorities and certificates are accessed using the same permissions for the Certificates function. Certificates and authorities created during installation, and those created afterward by the administrator, are contained in the All static group. See the list of permissions for more information on access rights.

Actions > ✦ New - Create a new Certification Authority

Actions > ✕ Delete - Delete the selected certification authority

Actions > 🟢 Import Public Key

Actions > 🟢 Export Public Key

Actions > 🟢 Access Group - A certification authority can be moved to another group to become available to users who have sufficient rights for this group.

**Access Group Filter**

The Access Group filter button enables users to select a static group and filter viewed objects according to the group where they are contained.

**EXAMPLE: How to divide access to certificates and authorities**

If Administrator does not want to allow the user John to access ERA Certification Authorities, but needs him to be able to work with certificates, the administrator has to follow these steps:

1. Create a new Static Group called Certificates.
2. Create new Permission set.
   a. Name this permission set Permissions for certificates.
   b. Add a group named Certificates in section Static Groups.
   c. In the Functionality section, select Write for Certificates.
   d. In the Users section, click Native Users and select John.
   e. Click Finish to save the permission set.
3. Move certificates from the All group to the newly created Certificates group:
   a. Navigate to Admin > Certificates > Peer Certificates.
   b. Select the check boxes ✅ next to the certificates you want to move.
   c. Click Actions > 🟢 Access Group, select the Certificates group and then click OK.

Now, John is able to modify and use moved certificates. However, Certification Authorities are safely stored out of this user's reach. John will not be able even to use existing authorities (from group All) for signing any certificates.
6.9.2.1 Create a new Certification Authority

To create a new authority, navigate to Admin > Certificates > Certification Authority and click Action > + New at the bottom of the page.

Certification Authority

Enter a Description of the Certification Authority and select a Passphrase. This Passphrase should contain at least 12 characters.

Attributes (Subject)

1. Enter a Common name (name) of the Certification Authority. Select a unique name to differentiate multiple Certificate Authorities. Optionally, you can enter descriptive information about the Certification Authority.
2. Enter the Valid from and Valid to values to ensure that the certificate is valid.

**NOTE**

For all Certificates and Certification Authorities created during installation of ERA components, the Valid from value is set to 2 days before certificate creation.

For all Certificates and Certification Authorities created in the ERA Web Console, the Valid from value is set to 1 day before certificate creation. The reason for this is to cover all possible time discrepancies between affected systems.

For example, a Certification Authority and Certificate, created 2017 Jan 12 during installation will have a pre-defined Valid from value of 2017 Jan 10 00:00:00, and a Certificate Authority and Certificate created 2017 Jan 12 in ERA Web Console will have a pre-defined Valid from value of 2017 Jan 11 00:00:00.

3. Click Save to save your new Certification Authority. It will now be listed in the Certification Authority list under Admin > Certificates > Certification Authority, and is ready to be used. Certification authority is created in the home group of the user who has created it.

To manage the Certification Authority, select the check box next to the Certification Authority in the list and use the context menu (left-click the Certification Authority) or the Action button on the bottom of the page. Available options are Import Public Key and Export a Public key or Edit the Certification Authority.
6.9.2.2   Export a Public Key

Export a public key from a Certification Authority:

1. Select the Certification Authority you want to use from the list and select the check box next to it.
2. Select Actions > Export Public Key. The public key will be exported as a .der file. Type a name for the public key and click Save.

**NOTE**

If you delete the default ERA Certification Authority and create a new one, it will not work. You also need to change Server certificate in Server Settings and then restart the ERA Server service.

Export a public key as Base64 from a Certification Authority:

1. Select the Certification Authority you want to use from the list and select the check box next to it.
2. Select Actions > Export Public Key as Base64. You can also download the Base64 encoded certificate as a file. Repeat this step for other component certificates as well as for your Certification Authority.

**NOTE**

- If you are using custom certificates that are not in Base64 format, they will need to be converted to Base64 format (alternatively, you can export these certificates as described above). This is the only format accepted by ERA components to connect to ERA Server. For more details about how to convert certificates see [http://linux.die.net/man/1/base64](http://linux.die.net/man/1/base64) and [https://developer.apple.com/library/mac/documentation/Darwin/Reference/ManPages/man1/base64.1.html](https://developer.apple.com/library/mac/documentation/Darwin/Reference/ManPages/man1/base64.1.html). For example:

  'cat ca.der | base64 > ca.base64.txt''
  'cat agent.pfx | base64 > agent.base64.txt'

- To export a certificate a user is required to have Use rights over Certificates. See the full list of access rights for more information.

6.9.2.3   Import a Public Key

To import a 3rd party Certification Authority, click Admin > Certificates > Certification Authorities.

1. Click Actions button and then select Import Public Key.
2. Choose file to upload: click Browse and navigate to the file you want to import.
3. Enter a Description for the certificate and click Import. The Certification Authority is now successfully imported.
6.10 Access Rights

Access rights let you manage ERA Web Console users and their permissions. There are two types:

1. **Native Users** - User accounts created and managed from the ERA Web Console.

Optionally, you can set up **Two-Factor Authentication** for Native Users and Mapped Domain Security Groups. This will increase security when logging into and accessing ERA Web Console.

Access to items from either category must be granted (using **Permission Sets**) to every ERA Web Console user.

**IMPORTANT**

The administrator native user whose home group is **All** has access to everything. We do not recommend using this account on a regular basis. We strongly advise that you create another 'admin' account or use Administrators from Mapped Domain Security Groups with the Administrator Permission Set assigned to them. This way you have a fallback should anything happen to the admin account. Also, you can create additional accounts with narrower access rights based on your desired competences. Use the default administrator account only as a backup option.

Users are managed in the **users** area of the **Admin** section. **Permission sets** define the level of access to different items for different users. See the **list** of all access rights and their functions for more details.

**List of Access Rights related examples**

There are various examples across Administration guide concerning access rights. This is list of them:

- How to duplicate policies
- Difference between Use and Write
- How to create a solution for branch office admins
- How to share objects via duplication
- How to divide access to certificates and authorities
- How to allow user to create installers
- How to remove notifications
- How to create policies
- Allow users to see all policies
- Share licenses among branch admins

### 6.10.1 Users

User management is part of the **Admin** section of the ERA Web Console.

**New security model in ESET Remote Administrator 6.5**

There is an improved security model for users and permission sets in the ESET Remote Administrator 6.5. These are key terms used in the new model:

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Group</td>
<td>Home Group is the group where all objects (devices, tasks, templates, etc.) a user creates are automatically stored. Each user must only have one home group.</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Object</td>
<td>Objects are located in Static Groups. Access to objects is by groups, not users (providing access by group makes it easy to accommodate multiple users, for example, if one user is on holiday). Server tasks and notifications are exceptions that require an “executing” user.</td>
</tr>
<tr>
<td>Access Group</td>
<td>Access Group functions as a static group which allows users to filter the location of the object based on access rights.</td>
</tr>
<tr>
<td>Administrator</td>
<td>A user that has home group All with a full Permission Set over the group is effectively an administrator.</td>
</tr>
<tr>
<td>Access Right</td>
<td>The right to access an object or to execute a task is assigned with a Permission Set.</td>
</tr>
<tr>
<td>Permission Set</td>
<td>A Permission Set represents the permissions for users that access ERA Web Console. They define what the user can see or do in ERA Web Console. A user can be assigned multiple Permission Sets. Permission sets are applied only over objects in defined groups. These Static Groups are set in the Static Groups section when creating or editing a permission set.</td>
</tr>
<tr>
<td>Functionality</td>
<td>A functionality is one type of object or action. Typically, functionalities get these values: Read, Write, Use. The combination of functionalities applied to an Access Group is called a Permission Set.</td>
</tr>
</tbody>
</table>

**Access Group Filter**

The Access Group filter button enables users to select a static group and filter viewed objects according to the group where they are contained.

**EXAMPLE: Branch office admins solution**

If a company has two offices, each with local admins, they need to be assigned with more permission sets for different groups.

Let’s say there are admins John in San Diego and Larry in Sydney. Both of them need to take care only of their local computers, use Dashboard, Policies, Reports and Dynamic Groups Templates with their machines. The main Administrator has to follow these steps:
2. Create new Permission sets:
   a. Permission set called Sydney permission set, with Static Group Sydney office, and with full access permissions (exclude Server Settings).
   b. Permission set called San Diego permission set, with Static Group San Diego office, and with full access permissions (exclude Server Settings).
   c. Permission set called All Group / Dashboard, with Static Group All, with the following permissions:
      - Read for Client Tasks
      - Use for Dynamic Group Templates
      - Use for Reports and Dashboard
      - Use for Policies
      - Use for Send Email
      - Use for Send SNMP Trap
      - Use for Export report to file
      - Use for Licenses
      - Write for Notifications
3. Create new user John with home group San Diego office, assigned with the permission sets San Diego permission set and All Group / Dashboard.
4. Create new user Larry with home group Sydney office, assigned with the permission sets Sydney permission set and All Group / Dashboard.

If permissions are set like this, John and Larry can use same tasks and policies, reports and dashboard, use dynamic group templates without restrictions; however each can only use templates for machines contained in their home groups.

Domain Security Groups
To ease usage in Active Directory, users from Domain Security Groups can be allowed to log into ERA. Such users can exist next to ERA Native Users; however, the permission sets are set for the Active Directory security group (instead of for individual users, as in the Native User case).

Sharing objects
If an Administrator wants to share objects, such as dynamic group templates, report templates, or policies, the following options are available:

- Move those objects into shared groups
- Create duplicate objects and move them into static groups which are accessible to other users (see the example below)

**EXAMPLE: Sharing via duplication**
For an object duplication the user needs to have Read permission on the original object and Write permission on his Home Group for this type of action.

Administrator, whose home group is All, wants to share Special Template with user John. The template was originally created by Administrator, therefore it is automatically contained in the group All. Administrator will follow these steps:

1. Navigate to Admin > Dynamic Group Templates.
2. Select the Special Template and click Duplicate, if needed, set name and description and click Finish.
3. The duplicated template will be contained in the home group of Administrator, group All.
4. Navigate to Admin > Dynamic Group Templates and select the duplicated template, click Access Group > Move and select the destination static group (where John has permission). Click OK.
How to share objects among more users via Shared Group

To better understand how the new security model works, see the scheme below. There is a situation where there are two users created by the administrator. Each user has his own home group with objects he has created. San Diego permission set gives John rights to manipulate Objects in his home group. The situation is similar for Larry. If these users need to share some objects (for example, computers), these objects should be moved to Shared Group (a static Group). Both users should be assigned with Shared permission set which has Shared Group listed in the Static Groups section.

**NOTE**
A fresh ERA installation has the Administrator (Native User with home group All) as the only account.

ERA access rights explained in logical model (click to expand)
6.10.1.1 Create a Native User

To create a new native user, go to the Admin tab, click Access Rights > Users and then click New at the bottom of the page.

**NOTE**

In order to create the user properly, we recommend you follow these steps:

1. Decide which static group will be the user's home group. If needed, create the group.
2. Decide what permission set would be best for the user. If needed, create new permission set.
3. Follow this chapter and create the user.
Basic

Enter a User name and an optional Description for the new user. Select Home Group. This is static group where all objects created by this user will be automatically contained.

Set Password

The password for the user should have at least 8 characters. The password should not contain the username.

Account

Enabled - Select this option unless you want the account to be inactive (you intend to use it later).

Have to change password - Select this option to force the user to change their password the first time they log into the ERA Web Console.

Password expiration - This option defines the number of days that the password is valid (it needs to be changed after that).

Autologout (min) - This option defines the idle time period (in minutes) after which the user is logged out of Web Console.

Full Name, Email contact and Phone contact can be defined to help identify the user.

Permission set

A user can be assigned multiple permission sets. You can select a pre-defined competence: Reviewer permission set (read-only rights for the All group) or Administrator permission set (full access to the All group) or Server assisted installation permission set (minimal access rights required for server assisted installation) or you can use a custom permission set. Each permission set provides permissions only for objects contained in the Static Groups selected in the permission set. Users without any permission set will not be able to log in to the Web Console.

WARNING

All pre-defined permission sets have the All group in the Static Groups section. Be aware of this when assigning it to a user. Users will have these permissions over all objects in ERA.
Review the settings configured for this user and click **Finish** to create the user.

### 6.10.1.2 Map Group to Domain Security Group

You can map a domain security group to the ERA Server and allow existing users (members of these domain security groups) to become ERA Web Console users.

**NOTE**

This feature is only available for systems with Active Directory. It cannot be used with LDAP.

To access the **Mapped Domain Security Group Wizard**, navigate to **Admin > Access Rights > Mapped domain security groups > New**, or simply click **New** when the mapped domain security group is selected in the tree.

#### Basic

**Domain group**

Enter a **Name** for the group. You can also enter a group **Description**. Select **Home Group**. This is static group where all objects created by users from this domain group will be automatically contained. This domain group will be defined by a **Group SID** (security identifier). Click **Select** to select a group from the list and then click **OK** to confirm.

**Account**

**Enabled** - Select this option unless you want the account to be inactive (if you intend to use it later).

**Autologout (min)** - This option defines the idle time period (in minutes), after which the user is logged out of Web Console.

**Email contact** and **Phone contact** can be defined to help identify the group.

#### Permission set

Assign competences (rights) for the users from this group. One or more permission sets can be assigned. You can use a pre-defined competence:
Review the settings configured for this user and click Finish to create the group.

Users will appear in the Domain Users tab after they first log in.

6.10.1.3 Assign User a Permission Set

Admin > Access rights > Permission Sets and then click Edit to assign a user to a specific permission set. See Manage Permission Sets for more details.

In the Users section, edit a specific user by clicking Edit... and select the check box next to a specific permission set in the Unassigned (Available) Permission Sets section.
6.10.1.4 Two Factor Authentication

Two-Factor Authentication (2FA) provides a more secure method to log into and access ERA Web Console.

- To enable 2FA for other user's account, one needs to have Write permission over that user. Once enabled, a user needs to configure 2FA themselves before they can log in. Users will receive a link via text message (SMS), which they can open in their phone's web browser to view instructions for configuring 2FA.

- Two-Factor Authentication is provided by ESET and its ESET Secure Authentication technology. You do not need to deploy or install ESET Secure Authentication within your environment, as ERA automatically connects to ESET servers to authenticate users who log into your ERA Web Console.

- Users with 2FA enabled will be required to log into ESET Remote Administrator using ESET Secure Authentication.

**NOTE**
You cannot use users with 2FA for Server Assisted installations.

6.10.2 Permission Sets

A permission set represents the permissions for users that access ERA Web Console. They define what the user can do or see in the Web Console. Native users have their own permissions while domain users have the permissions of their Mapped security group. Each permission set has its domain of application (static groups). Permissions which are selected in the Functionality section will apply over objects in the groups which are set in the Static Groups section for each user assigned by this permission set. Having access to certain Static Group automatically means access to every one of its subgroups. With proper setting of static groups it is possible to build separated branches for local admins (see the example).

A user can be assigned a permission set even without being able to see it. A permission set is also an object which is automatically stored in the home group of the user who created it. When a user account is created, the user is stored as object in the home group of the creating user. Usually the Administrator creates users, so they are stored in the group All.
The **Access Group** filter button enables users to select a static group and **filter viewed objects** according to the group where they are contained.

### IMPORTANT

**Good practice for working with permissions:**

- Never give access to **Server Settings** to inexperienced users - only Administrator should have this access.
- Consider restricting access to **Client Tasks > Run Command** - it is a very powerful task that could be abused.
- Non-admin level users should not have permissions for **Permission Sets**, **Native Users**, **Server Settings**.
- If a more complicated model of permissions is needed, do not hesitate to create more permission sets and assign them accordingly.

Next to permissions to ERA functionality, there can be given **Read**, **Use**, **Write** access to **User Groups**.

#### EXAMPLE: Duplication

For an object duplication the user needs to have **Read** permission on the original object and **Write** permission on his **Home Group** for this type of action.

*John*, whose home group is **John's Group**, wants to duplicate **Policy 1**, which was originally created by **Larry**, therefore the policy is automatically contained in Larry's home group, **Larry's Group**. This is the recommended way of achieving it:
1. Create a new static group. Name it, for example, *Shared policies*.
2. Assign both *John* and *Larry* with Read permissions for *Policies* in the group *Shared policies*.
3. *Larry* moves Policy 1 to the *Shared policies* group.
4. Assign *John* with Write permissions for *Policies* in his home group.
5. *John* can now Duplicate the Policy 1 - duplicate will appear in his home group.

**EXAMPLE: Difference between Use and Write**

If *Administrator* does not want to allow user *John* to modify policies in the *Shared policies* group, he would create a permission set with:

- **Functionality** Policies: **Read** and **Use** permissions selected
- **Static Groups**: *Shared Policies*

With these permissions assigned to *John*, *John* is able to run those policies but he can not edit them, create new, nor delete them. If an administrator were to add **Write** permission, *John* could create new, duplicate, edit and delete policies within the selected static group (*Shared policies*).

### 6.10.2.1 Manage Permission Sets

To make changes to a specific permissions set, click it and then click **Edit**. Click **Duplicate** to create a duplicate permission set which you can modify and assign to a specific user. The duplicate will be stored in the home group of the user who duplicated it.

#### Basic

Enter a **Name** for the set (mandatory setting), you can also enter a set **Description**.

#### Static Groups

You can add a **Static Group** (or multiple Static Groups) that will take this competence. Permissions which are checked in the **Functionality** section will apply over objects contained in groups selected in this section.

#### Functionality

Select individual modules for which you want to grant access. The user with this competence will have access to these specific tasks. It is also possible to set different permissions for each type of server task and client task. There are available pre-defined competences for the **All** group.

- **Administrator competence** (full access)
- **Reviewer competence** (read only)

Granting **Write** permission automatically grants **Use** and **Read** rights; granting **Use** rights automatically grants **Read** rights.

**WARNING**

All pre-defined permission sets have the **All** group in the **Static Groups** section. Be aware of this when assigning it to a user. Users will have these permissions over all objects in ERA.

#### User Groups

You can add a **User Group** (or multiple User Groups) of ESET Mobile Device Management for iOS.

#### Users

Choose a user to be assigned by this permission set. All available **users** are listed on the left. Select specific users or select all users using the **Add All** button. Assigned users are listed on the right. It is not mandatory to assign a user, you can do it later.

#### Summary

Review the settings configured for this competence and click **Finish**. The permission set is stored in the Home Group of the user who created it.
Click **Save as** to create a new template based on the template you are editing. You will be required to enter a name for the new template.

6.10.2.2 List of permissions

Permission types

When creating or editing a permission set in **Admin > Access Rights > Permission Sets > New / Edit > Functionality** there is a list of all available permissions. ERA Web Console permissions are divided into categories; for example, **Groups & Computers, Native Users, Certificates, Policies** and so on. A given permissions set can allow for **Read, Use** or **Write** access. In general:

**Read** permissions are good for auditing users. They can view data but cannot make changes.
**Use** permissions allow users to use objects, run tasks, but not modify or delete.
**Write** permissions allow users to either modify respective objects and/or duplicate them.

Certain types of permissions (listed below) control a process, not an object. That is why they work on a global level, so it does not matter which static group is the permission applied on, it will work regardless. If the process is allowed to a user he can use it only over objects for which he has sufficient permissions. For example, the **Export report to file** permission enables the exporting functionality, however data contained in the report are determined by other permissions.

Users can be assigned permissions for the following processes:

- **Enterprise Inspector Administrator**
- **Enterprise Inspector User**
- **Agent Deployment**
- **Reports and Dashboard** (only the functionality of the Dashboard will be available, the usable report templates are still dependent on accessible static groups)
- **Send Email**
- **Send SNMP Trap**
- **Export report to file**
- **Server Settings**

**IMPORTANT** When assigning (or un-assigning) a permission set to a user, **Use** permission is required for **Permission Sets** and **Native Users**.

---

### Functionality types:

**Groups & Computers**

- **Read** - List computers, groups and computers within a group.
- **Use** - Use a computer/group as a target for a policy or task.
- **Write** - Create, modify and remove computers. This also includes renaming a computer or a group.

**Enterprise Inspector Administrator**

- **Write** - Perform administrative functions in Enterprise Inspector.

**Enterprise Inspector User**

- **Read** - Read only access to Enterprise Inspector.
- **Write** - Read and write access to Enterprise Inspector.

**Permission Sets**

- **Read** - Read the list of permission sets and the list of access rights within them.
- **Use** - Assign/remove existing permission sets for users.
- **Write** - Create, modify and remove permission sets.
Domain Groups
Read - List domain groups.
Use - Allows granting/revoking of permission sets.
Write - Create/modify/remove domain groups.

Native Users
Read - List native users.
Use - Allows granting and revoking of permission sets.
Write - Create/modify/remove native users.

Agent Deployment
Use - Allow access to deploy Agent via Quick Links or to add client computers manually in ERA Web Console.

Stored Installers
Read - List stored installers.
Use - Export stored installer.
Write - Create/modify/remove stored installers.

Certificates
Read - Read the list of peer certificates and Certification Authorities.
Use - Export Certification Authorities and peer certificates and use them in installers or tasks.
Write - Create new peer certificates or Certification Authorities and revoke them.

Server Tasks & Triggers
Read - Read the list of tasks and their settings (except of sensitive fields like passwords).
Use - Execute an existing task with Run Now (as the user currently logged to the Web Console).
Write - Create, modify and remove server tasks.

Categories can be expanded by clicking the plus sign and single or multiple types of server tasks can be selected.

Client Tasks
Read - Read the list of tasks and their settings (except of sensitive fields like passwords).
Use - Schedule execution of existing Client tasks or cancel their execution. Note that for assignment of tasks (or assignment cancellation) to targets (computers or groups) additional Use access is required for the affected targets.
Write - Create, modify or remove existing Client tasks. Note that for assignment of tasks (or assignment cancellation) to targets (computers or groups) additional Use access is required for the affected target objects.

Categories can be expanded by clicking the plus sign and single or multiple types of client tasks can be selected.

Dynamic Groups Templates
Read - Read the list of Dynamic Groups templates.
Use - Use existing templates for dynamic groups.
Write - Create, modify and remove Dynamic Group templates.

Reports and Dashboard
Read - List report templates and their categories. Generate reports based on report templates. Read your own dashboards based on default dashboards.
Use - Modify your own dashboards with available report templates.
Write - Create, modify, remove existing report templates and their categories. Modify default dashboards.
Policies
Read - Read the list of policies and configuration within them.
Use - Assign existing policies to targets (or cancel their assignment). Note, that for the affected targets additional Use access is necessary.
Write - Create, modify and remove policies.

Send Email
Use - Send emails. (Useful for Notifications and Generate Report server tasks.)

Send SNMP Trap
Use - Allows to send SNMP trap. (Useful for Notifications.)

Export report to file
Use - Allows you to store reports on the ERA Server machine file system. Useful with the Generate Report server tasks.

Licenses
Read - Read the list of licenses and their usage statistics.
Use - Use the license for activation.
Write - Add and remove licenses. (The user must have home group set to All. By default only the Administrator can do it.)

Notifications
Read - Read the list of notifications and their settings.
Write - Create, modify, remove notifications. For proper notification handling additional Use access rights may be required for Send SNMP Trap or Send Email depending on the notification configuration.

Server Settings
Read - Read server settings.
Write - Modify server settings.

6.11 Server Settings
In this section, you can configure specific settings for the ESET Remote Administrator Server itself.

Connection
Remote Administrator port (requires restart!) - This is the port for the connection between the ESET Remote Administrator Server and Agent(s). Changing this option requires restarting the ERA Server service for the change to take effect.
Web Console port (requires restart!) - Port for the connection between the ERA Web Console and the ERA Server.
Advanced security - Use this setting to have ERA Server use newest TLS and newly created certification authorities and certificates to use SHA-2. Enabling advanced security may break compatibility with older systems.
Certificate (requires restart!) - Here you can manage ERA Server certificates. Click Change certificate and select which ERA Server certificate should be used by your ERA Server. For more information, see Peer Certificates.

IMPORTANT
These changes require restart of the ESET Remote Administrator Server service. See our Knowledgebase article for instructions.
Updates

**Update interval** - Interval at which updates will be received. You can select a regular interval and configure the settings or you can use a CRON expression.

**Update server** - Update server from which the ERA Server receives updates for ESET products and ERA components.

**Update type** - Select the type of updates you want to receive. You can choose either **Regular**, **Pre-release** or **Delayed update**. We do not recommend that you select Pre-release updates for production systems as this is a risk.

Advanced Settings

**HTTP Proxy** - Use a proxy server to facilitate internet traffic to clients on your network. If the ERA Server was installed from the All-in-one installer, the HTTP Proxy is enabled automatically.

**WakeUp** - ERA Server can run instant replication of the ERA Agent on a client machine. UDpv4 and UDpv6 ports are used with default port numbers 1237 and 1238. This is useful when you do not want to wait for the regular interval when the ERA Agent connects to the ERA Server. For example when you want a **Client Task** to be run immediately on client(s) or if you want a **Policy** to be applied right away.

**SMTP server** - Use an **SMTP Server** to let ERA Server send email messages (for example email notifications or reports). Specify details of your SMTP server.

**Syslog server** - You can have ERA send notifications and event messages to your **Syslog server**. Also, it is possible to **export logs** from a client computer's ESET product and send them to the Syslog server.

**Static Groups** - Enables **automatic pairing of found computers** to computers already present in Static Groups. Pairing works on reported hostname by ERA Agent and if it can not be trusted then it should be disabled. If pairing fails, the computer will be placed into the Lost and Found group.

**Repository** - Location of the repository where all installation files are stored.

NOTE
The default repository is set to **AUTOSELECT**. It is possible to create and use **offline repository**.

Diagnostics - Enable or disable the submission of anonymous crash report statistics to ESET for the improvement of customer experience.

Logging - Set the log verbosity to determine the level of information that will be collected and logged, from **Trace** (informational) to **Fatal** (most important critical information).

The latest ERA Server log file can be found here:
- **Windows**: `C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs`
- **Linux**: `/var/log/eset/RemoteAdministrator/Server/`

You can setup **exporting logs to Syslog** here.

Database cleanup - To prevent a database overload, you can use this option to regularly clean logs.

Customization

**Customize UI** - It is possible to add a custom logo to the ERA Web Console and the reports generated via **Server Task**.

- **None** - Basic design, no custom logo
- **Co-branding** - Allows custom logo for Web Console and in the footer of reports
- **White-labeling** - Allows custom logo for Web Console and in the footer or header of reports

**Company logo**
- **Dark background logo (Web Console header)** - This logo will be displayed in the top left corner of Web Console.
- **Light background logo** - This logo will be displayed in the header (for MSP license owners) or footer (co-branding setting) of reports generated via **Server Task**.

Click 📦 to select a logo. Click ⏰ to download current logo. Click ✗ to remove current logo.

**Reports** - If enabled, you can add text into **Report footer text** field which will be added to the right bottom corner of reports generated in PDF format.
IMPORTANT

A custom logo can not be used together with custom footer text. Logo has the same position as footer text. If logo and footer are used simultaneously, only logo will be visible. When using the White-labeling setting, the custom logo will appear in the upper left corner of the report; a smaller ESET logo is placed in bottom right corner, instead of footer text.

6.11.1 SMTP server

ESET Remote Administrator can automatically send email reports and notification. Enable Use SMTP server, navigate to Admin > Server Settings > Advanced Settings > SMTP Server and specify the following:

- **Host** - Hostname or an IP address of your SMTP server.
- **Port** - SMTP uses port 25 by default, but you can change it in case your SMTP server uses different port.
- **Username** - If your SMTP server requires authentication, specify the SMTP user account name (do not include the domain as this will not work).
- **Password** - The password associated with the SMTP user account.
- **Connection security type** - Specify connection type, the default is Not secured, but if your SMTP server allows for secure connections, choose TLS or STARTTLS. So if you want to make your connection more secure, it's a good choice to use a STARTTLS or SSL/TLS extension, that employ a separate port for encrypted communication.
- **Authentication type** - The default is set to No authentication, however, you can select appropriate Authentication type from the drop-down list (for example Login, CRAM-MD5, CRAM-SHA1, SCRAM-SHA1, NTLM or Automatic).
- **Sender address** - Specify the sender address that will be displayed in the header of notification emails (From:).
- **Test SMTP server** - This is to make sure the SMTP settings are correct, press Send test email button and a pop-up window will open. Enter recipient's email address and the test email message will be sent via SMTP server to this address. Check the recipient's mailbox to verify the test email was delivered.

6.11.2 Automatically pair found computers

If there is an occurrence of multiple instances of the same computer in ERA (for example if ERA Agent is reinstalled on a client computer that is already managed), Automatically pair found computers feature takes care of this and pairs these instances into one. This should eliminate the need for manual verification and sorting of found computers.

Pairing works on reported hostname by ERA Agent and if it can not be trusted, we recommend you to disable Automatically pair found computers. If pairing fails a computer will be placed into Lost and Found group. The idea is that whenever ERA Agent is reinstalled on an already managed computer, it would be automatically paired and thus correctly placed into ERA without your intervention. Also, new ERA Agent will immediately get its policies and tasks.

- When **disabled**, computers that should be placed into Lost & found group will be paired with the first found unmanaged computer (placeholder, circle icon) located anywhere in ERA tree. If there isn't any placeholder with the same name, the computer would be placed into Lost & found.

- When **enabled (default)**, computers that should be placed into Lost & found will be paired with the first found unmanaged computer (placeholder, circle icon) located anywhere in ERA tree. If there isn't any placeholder with the same name, the computer will be paired to the first found managed computer (alert or check icon) located anywhere in ERA tree. If this pairing also fails, the computer will be placed into Lost & found.

**NOTE**

If you consider automatic pairing unwanted, disable it. You can always verify and sort computers manually.
6.11.3 Syslog server

If you have a Syslog server running in your network, you can configure ERA Server to send Notifications to your Syslog server. You can also enable Export logs to Syslog in order to receive certain events (Threat Event, Firewall Aggregated Event, HIPS Aggregated Event, etc.) from client computers running ESET Endpoint Security, for example.

To enable Syslog server:

1. Navigate to Admin > Server Settings > Advanced Settings > Syslog Server and click the slider bar next to Use Syslog server.

2. Specify the following mandatory settings:
   a. **Host** (IP address or hostname of the destination for Syslog messages)
   b. **Port** number (default value is 514).
   c. **Format** of the log: BSD (specification), Syslog (specification)
   d. **Transport** protocol for sending messages to Syslog (UDP, TCP, TLS)

After making changes, click **Save**.

NOTE
The regular application log file is constantly being written to. Syslog only serves as a medium to export certain asynchronous events, such as notifications or various client computer events.
6.11.4 Export logs to Syslog

ESET Remote Administrator is able to export certain logs/events and send them to your [Syslog server](#). Events such as ThreatEvent, Firewall Aggregated Event, HIPS Aggregated Event etc. are generated on any managed client computer running an ESET product (for example, ESET Endpoint Security). These events can be processed by any Security Information and Event Management (SIEM) solution capable of importing events from a Syslog server. Events are written to the Syslog server by ESET Remote Administrator.

1. To enable Syslog server, click **Admin > Server Settings > Advanced Settings > Syslog server > Use Syslog server**.

2. To enable exporting, click **Admin > Server Settings > Advanced Settings > Logging > Export logs to Syslog**.

3. Choose one of the following formats for event messages:
   a. [JSON (JavaScript Object Notation)](#)
   b. [LEEF (Log Event Extended Format)](#) - format used by IBM's application QRadar

6.11.4.1 Events exported to JSON format

JSON is a lightweight format for data exchange. It is built on collection of name / value pairs and an ordered list of values.

**Exported events**

This section contains details on the format and meaning of attributes of all exported events. The event message is in the form of a JSON object with some mandatory and some optional keys. Each one exported event will contain the following key:

<table>
<thead>
<tr>
<th>event_type</th>
<th>string</th>
<th>Type of exported events: Threat_Event, FirewallAggregated_Event, HipsAggregated_Event.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>string</td>
<td>IPv4 address of the computer generating the event.</td>
</tr>
<tr>
<td>ipv6</td>
<td>string</td>
<td>IPv6 address of the computer generating the event.</td>
</tr>
<tr>
<td>source_uuid</td>
<td>string</td>
<td>UUID of the computer generating the event.</td>
</tr>
<tr>
<td>occurred</td>
<td>string</td>
<td>UTC time of occurrence of the event. Format is %d-%b-%Y %H:%M:%S</td>
</tr>
<tr>
<td>severity</td>
<td>string</td>
<td>Severity of the event. Possible values (form least severe to most severe) are: Information Notice Warning Error Critical Fatal</td>
</tr>
</tbody>
</table>

Custom keys according to **event_type**:

1. **ThreatEvent**

All Threats events generated by managed endpoints will be forwarded to Syslog. Threat event specific key:

<table>
<thead>
<tr>
<th>threat_type</th>
<th>string</th>
<th>optional</th>
<th>Type of threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>threat_name</td>
<td>string</td>
<td>optional</td>
<td>Name of threat</td>
</tr>
<tr>
<td>threat_flags</td>
<td>string</td>
<td>optional</td>
<td>Threat related flags</td>
</tr>
<tr>
<td>scanner_id</td>
<td>string</td>
<td>optional</td>
<td>Scanner ID</td>
</tr>
<tr>
<td>scan_id</td>
<td>string</td>
<td>optional</td>
<td>Scan ID</td>
</tr>
<tr>
<td>engine_version</td>
<td>string</td>
<td>optional</td>
<td>Version of the scanning engine</td>
</tr>
<tr>
<td>object_type</td>
<td>string</td>
<td>optional</td>
<td>Type of object related to this event</td>
</tr>
<tr>
<td>object_uri</td>
<td>string</td>
<td>optional</td>
<td>Object URI</td>
</tr>
</tbody>
</table>
2. FirewallAggregated_Event

Event logs generated by ESET Personal Firewall are aggregated by the managing ESET Remote Administrator Agent to avoid wasting bandwidth during ERA Agent/ERA Server replication. Firewall event specific key:

- **event**: Event name
- **source_address**: Address of the event source
- **source_address_type**: Type of address of the event source
- **source_port**: Port of the event source
- **target_address**: Address of the event destination
- **target_address_type**: Type of address of the event destination
- **target_port**: Port of the event destination
- **protocol**: Protocol
- **account**: Name of the user account associated with the event
- **process_name**: Name of the process associated with the event
- **rule_name**: Rule name
- **rule_id**: Rule ID
- **inbound**: Whether or not the connection was inbound
- **threat_name**: Name of the threat
- **aggregate_count**: How many exact same messages were generated by the endpoint between two consecutive replications between ERA Server and managing ERA Agent

3. HIPSAggregated_Event

Events from Host-based Intrusion Prevention System are filtered on **severity** before they are sent further as Syslog messages. Only events with **severity** levels **Error**, **Critical** and **Fatal** are sent to Syslog. HIPS specific attributes are as follows:

- **application**: Application name
- **operation**: Operation
- **target**: Target
- **action**: Action
- **rule_name**: Rule name
**application** | string | optional | Application name
---|---|---|---
**rule_id** | string | optional | Rule ID
**aggregate_count** | number | optional | How many exact same messages were generated by the endpoint between two consecutive replications between ERA Server and managing ERA Agent

### 4. Audit Event

ERA 6.5 forwards Server’s internal audit log messages to Syslog. Specific attributes are as follows:

<table>
<thead>
<tr>
<th>attribute</th>
<th>type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>string</td>
<td>Audit log domain</td>
</tr>
<tr>
<td>action</td>
<td>string</td>
<td>Action taking place</td>
</tr>
<tr>
<td>target</td>
<td>string</td>
<td>Target action is operating on</td>
</tr>
<tr>
<td>detail</td>
<td>string</td>
<td>Detailed description of the action</td>
</tr>
<tr>
<td>user</td>
<td>string</td>
<td>Security user involved</td>
</tr>
<tr>
<td>result</td>
<td>string</td>
<td>Result of the action</td>
</tr>
</tbody>
</table>

### 5. Enterprise Inspector Alert Event

ERA 6.5 forwards ESET Enterprise Inspector Alerts to Syslog. Specific attributes are as follows:

<table>
<thead>
<tr>
<th>attribute</th>
<th>type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>processname</td>
<td>string</td>
<td>Name of the process causing this alert</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>Owner of the process</td>
</tr>
<tr>
<td>rulename</td>
<td>string</td>
<td>Name of the Enterprise Inspector rule triggering this alert</td>
</tr>
<tr>
<td>count</td>
<td>number</td>
<td>Number of alerts of this type generated since last alert</td>
</tr>
</tbody>
</table>

### 6.11.4.2 Events exported to LEEF format

LEEF format is a customized event format for IBM® Security QRadar®. Events have standard and custom attributes. ERA uses some of standard attributes described in [official IBM documentation](https://www.ibm.com/support/pages/qradar). Custom attributes are the same as in JSON format. There are five categories of events:

- Threat
- Firewall
- HIPS
- Audit
- Enterprise Inspector Alerts

**NOTE**

More information about Log Event Extended Format (LEEF) can be found at [official IBM website](https://www.ibm.com/support/pages/qradar).
7. License Management

ESET Remote Administrator uses a completely new ESET licensing system. You can easily manage your licenses via ESET Remote Administrator. By purchasing licensing for any ESET business product, you automatically receive access to ESET Remote Administrator.

**NOTE**
You can activate your ESET product using ESET Remote Administrator. This applies to earlier versions as well.

If you already have an ESET-issued Username and Password that you want to convert to a License Key, see Convert legacy license credentials. The Username and the Password have been replaced by a License Key/Public ID. A License Key is a unique string used to identify the license owner and the activation itself. A Public ID is a short string used to identify the license to a third party (for example, the Security Admin responsible for the Unit distribution).

The Security Admin can be used to manage specific licenses and is different from a License Owner. The license owner can delegate a license to a security admin, authorizing that person to manage specific licenses. If they accept, they receive license management privileges. We recommend that all license owners also create Security Admin accounts for themselves.

Licenses can be managed from this section, online by clicking Open ELA (ESET License Administrator), or using the ESET License Administrator web interface (see the Security Admin section).

Permissions for license management

Each user can be assigned a permission for Licenses. Permissions are valid only for license contained in the static group where that permission set is assigned. Each type of permission allows user for different actions.

**IMPORTANT**
A new security model in ERA 6.5 has changed license management. Only administrators whose home group is set to All, with Write permission on licenses in the home group, can add or remove licenses. Each license is identified by its Public ID and can contain one or more units. Licenses can be distributed only by an administrator to other users (lower Admins). A license is not reducible.

Working in Web Console

The License Management section in ESET Remote Administrator is accessible from the main menu under Admin > License Management.

Licenses can be identified by their Public ID. In ESET License Administrator and ERA, each license is identified by Public ID, License Type and Flags:

- **License Type** can be Full_Paid (paid license), Trial (trial license) and NFR (license Not For Resale).
- **Flags** include MSP, Business and a Consumer.

The list of licenses is shown in categories (activated by) Offline license, License Key or Security Admin. You can use Modes to change select mode (Single or Multiple). Click the ▼ arrow in upper right corner and choose from the context menu:

- Single select mode - you can select single item.
- Multiple item select mode - lets you use the check boxes to select multiple items.
- Refresh - reloads/refreshes displayed information.
- Expand All - Lets you display all information.
- Collapse All - Lets you hide all information.
The security **Product name** for which its license is intended.

The overall **Status** of the license (if the license is expired, overused, or at risk of expiration or overuse, a warning message will be displayed here).

The number of **Units** that can be activated with this license and number of offline units.

The number of **Subunits** of ESET server products (mailboxes, gateway protection, connections).

The license **Expiration** date.

The license **Owner name** and **Contact**.

**License Status** is displayed for the active menu item.

- **Green** - Your license is activated successfully.
- **Red** - The license is not registered via ESET License Administrator, or the license has expired.
- **Orange** - Your license is still depleted or is about to expire (expiration is due in 30 days).

**Synchronize licenses**

ESET License Administrator automatically syncs once a day. Click **Synchronize licenses** to refresh license information in ERA immediately.

**Access Group Filter**

The **Access Group** filter button enables users to select a static group and filter viewed objects according to the group where they are contained.

**Add License or License key**

Click **Add Licenses** and then select the method you want to use to add your new license(s):

1. **License Key** - Enter a license key for a valid license and click **Add License**. The license key will be verified against the activation server and added to the list.
2. **Security Admin Credentials** - Connect a security admin account and all its licenses to the License Management section.

3. **License File** - Add a license file (.lf) and click Add License. The license file will be verified and the license added to the list.

**Remove Licenses**

Select a license from the list above and click this to remove it completely. You will be asked to confirm this action. Removal of the license does not trigger deactivation of the product. Your ESET product will remain activated even after the license has been deleted in ERA License Management.

**Licenses can be distributed to ESET products from ERA using two tasks:**

- The software installation task
- The product activation task

**EXAMPLE: How can Administrator share licenses among branch admins**

There are three users and Administrator, each user has his own home group:

- John, San Diego
- Larry, Sydney
- Makio, Tokyo

Administrator imports 3 licenses. These are contained in static group *All* and other users can not use them.

Administrator can click the cogwheel next to license which he wants to assign to other user. Click Access Group > Move and chose group where user has permission. For user John, click group San Diego. John needs to have Use permission for Licenses in group San Diego.

When the user John logs in, he can see and use only the license which was moved to his group. Administrator should repeat the process analogically for other users (Larry and Makio), afterward, users can see only their license, while Administrator can see them all.
7.1 Add License - License Key

ESET Remote Administrator has its own License Management which is accessible from the main menu under Admin > License Management.

You can use one of the three methods when adding a license, you can enter the License Key, provide Security Admin credentials, or upload an Offline license file.

**IMPORTANT**

A new security model in ERA 6.5 has changed license management. Only administrators whose home group is set to All, with Write permission on licenses in the home group, can add or remove licenses. Each license is identified by its Public ID and can contain one or more units. Licenses can be distributed only by an administrator to other users (lower Admins). A license is not reducible.

Type or copy and paste the License Key you received when you purchased your ESET security solution in to the License Key field. If you are using legacy license credentials (a Username and password), convert the credentials to a license key. If the license is not registered, it will trigger the registration process, which will be done on the ELA portal (ERA will provide the URL valid for registration based on the origin of the license).

Enter the Security Admin account credentials (ERA will display all delegate licenses in ERA License Manager).
**Offline license file** - copy a specific **License file token** and enter into [ESET License Administrator portal](#) and include the information about product(s) ERA is able to manage.

**NOTE**
For further instructions how to download Offline license file, see [License Owner](#) or [Security Admin](#).
One you are logged in ESET License Administrator portal, select the check box next to *Allow management with Remote Administrator* and enter *Server Token* (License file token from ERA) into ESET License Administrator portal when generating an offline license file, otherwise the license file won’t be accepted by ESET Remote Administrator.

Go back to ERA License Management, select **Browse** for the offline license file you’ve exported in ELA, click **Upload** and then click **Add licenses** button.
List of licenses shown in categories (activated by)

License Key, Offline license or Security Admin.
Licenses can be distributed to ESET security products from ERA using two tasks:

- The Software installation task
- The Product activation task
8. FAQ

Q: Version 5 has a Custom Client Info field. This is helpful for our MSPs to determine which client belongs to each of their customers. Does this exist in v6?
A: Dynamic Groups, which are little bit different (evaluated on agent level) do not allow for the creation of “custom parameters / tagging”. You can, however, generate a report to display custom client data.

Q: How do you resolve the error Login Failed, Connection has failed with the state of 'Not connected'?
A: Check if ERA Server service is running or MS SQL Server service. If not, start it. If it is running, restart the service, refresh web console and then try to log in again. For more information see Troubleshooting login.

Q: What is the group "Lost and Found" used for?
A: Each computer that connects to ERA server and is not a member of any static group is automatically displayed in this group. You can work with the group and the computers inside it as with computers in any other static group. The group can be renamed or moved under another group but it can't be deleted.

Q: How do you create a dual update profile?
A: See our ESET Knowledgebase article for step-by-step instructions.

Q: How do you refresh the information on a page or in a section of the page without refreshing the entire browser window?
A: Click Refresh in the context menu at the top right of a section of the page.

Q: How do you perform a silent installation of the ERA Agent?
A: You can use a GPO as a Startup script to achieve this. At this time it is not possible to perform a silent installation from Web Console.

Q: RD Sensor does not detect all clients on network.
A: RD sensor passively listens to network communication on the network. If PCs are not communicating, they are not listed by RD Sensor. Check your DNS settings to make sure that issues with DNS lookup are not preventing communication.

Q: How do I reset the Active threats count shown in ERA after cleaning threats?
A: To reset the number of active threats, a full (in-depth scan) needs to be started via ERA on the target computer(s). If you have cleaned a threat manually, you can mute the appropriate alert.

Q: How do I set up CRON expression for the ERA Agent connection interval?
A: P_REPLICATION_INTERVAL accepts a CRON expression. Default is "R R/20 * * * ? *" which means connecting at random second (R=0-60) every random 20th minute (for example 3, 23, 43 or 17,37,57). Random values should be used for load balancing in time. So every ERA Agent is connecting in different random time. If an accurate CRON is used, for example "0 * * * * ? *", all Agents with this setting will connect at the same time (every minute at :00 second) there will be load peaks on server in this time. For more information see Cron expression interval.

Q: How do I create new Dynamic Group for automatic deployment?
A: See our Knowledgebase article for step-by-step instructions.

Q: When importing a file containing a list of computers to add to ERA, what is the format required for the file?
A: File with following lines:
   All\Group1\GroupN\Computer1
   All\Group1\GroupM\ComputerX
All is the required name of root group.

Q: Which 3rd party certificates can be used to sign ERA certificates?
A: The certificate has to be CA (or intermediate CA) certificate with the 'keyCertSign' flag from 'keyUsage' constraint. This means that it can be used for signing other certificates.

Q: How do I reset the Administrator password for Web Console (The password entered during set up on Windows Operating Systems)?
A: It is possible to reset the password by running the server installer and choosing Repair. Note that you may require the password for the ERA database if you did not use Windows Authentication during creation of the database.
Q: How do I reset the Administrator password for Web Console (Linux, entered during set up)?
A: If you have another user in ERA with sufficient rights, you should be able to reset the administrator account password. However, if administrator is the only account (as it is created upon installation) in the system, you cannot reset this password.
You reinstall ERA, search for the DB entry for the Administrator account, and update the old DB according to this entry. In general the best practice is to back up credentials for “Administrator” in a safe location and create new users with desired set of privileges. The Administrator account should ideally not be used for purposes other than creating other users or resetting their accounts.

Q: How do I troubleshoot if RD Sensor is not detecting anything?
A: If your OS is detected as a network device, it won’t be sent to ERA as a computer. Network devices (printers, routers) are filtered out. RD Sensor was compiled with libpcap version 1.3.0, please verify that you have this version installed on your system. The second requirement is a bridged network from your virtual machine where RD Sensor is installed. If these requirements are met, run nmap with OS detection (http://nmap.org/book/osdetect-usage.html) to see whether it can detect the OS on your computer.

Q: I can not see items in the Dynamic Groups Templates window—why?
A: Most likely, your users do not have sufficient permissions. Users can see templates only if they are contained in a static group where the user has been assigned at least Read permissions for Dynamic Group Templates.

Q: I can not see any information in the Dashboard window—why?
A: Most likely, your users do not have sufficient permissions. Users need to have permissions over computers and also for Dashboard to have the data displayed. See the example permission set.
9. About ESET Remote Administrator

To open the About window, navigate to Help > About. This window provides details about the installed version of ESET Remote Administrator and the list of installed program modules. The top of the window contains information about your operating system and system resources. Also, you'll see a license which is used by ERA to download module updates (the same license used to activate ERA).

**NOTE**

For instructions to find out which version an ERA component is, see our [Knowledgebase article](#).