



# TOTAL SECURITY SUITE for BUSINESS

www.escanav.com

Product Version: 14.0. 1400.xxxx

sales@escanav.com





Copyright © 2020 by MicroWorld Software Services Private Limited. All rights reserved.

Any technical documentation provided by MicroWorld is copyrighted and owned by MicroWorld. Although MicroWorld makes every effort to ensure that this information is accurate, MicroWorld will not be liable for any errors or omission of facts contained herein. This user guide may include typographical errors, technical or other inaccuracies. MicroWorld does not offer any warranty to this user guide's accuracy or use. Any use of the user guide or the information contained therein is at the risk of the user. MicroWorld reserves the right to make changes without any prior notice. No part of this user guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MicroWorld Software Services Private Limited.

The terms MicroWorld, MicroWorld Logo, eScan, eScan Logo, MWL, and MailScan are trademarks of MicroWorld. Microsoft, MSN, Windows, and Windows Vista are trademarks of the Microsoft group of companies. All other product names referenced in this user guide are trademarks or registered trademarks of their respective companies and are hereby acknowledged. MicroWorld disclaims proprietary interest in the marks and names of others.

The software described in this user guide is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

| Document Number:                | 5BUG/04.05.2020/14.1                             |
|---------------------------------|--|
| <b>Current Software Version</b> | : 14.0.1400.xxxx                                 |
| Technical Support:              | support@escanav.com                              |
| Sales:                          | sales@escanav.com                                |
| Forums:                         | http://forums.escanav.com                        |
| eScan Wiki:                     | http://wiki.escanav.com/wiki/index.php/Main_Page |
| Live Chat:                      | http://www.escanav.com/english/livechat.asp      |
| Printed By:                     | MicroWorld Software Services Private Limited     |
| Date:                           | June, 2020                                       |





# Contents

| Introduction                      | 9  |
|-----------------------------------|----|
| Pre-requisites for eScan Server   | 9  |
| System Requirements               | 10 |
| Installing eScan TSS for Business | 11 |
| Installation Process              | 12 |
| Components of eScan Server        | 18 |
| Web Console Login                 | 19 |
| Main Interface                    | 22 |
| Navigation Panel                  | 24 |
| Dashboard                         | 28 |
| Deployment Status                 | 29 |
| eScan Status                      | 29 |
| License                           | 30 |
| Protection Status                 | 30 |
| Update Status                     | 30 |
| Scan Status                       | 31 |
| File Anti-Virus                   | 32 |
| Proactive                         | 32 |
| Mail Anti-Virus                   | 33 |
| Anti-Spam                         | 33 |
| Web Anti-Phishing                 | 34 |
| Mail Anti–Phishing                | 34 |
| Web Protection                    | 35 |
| Firewall                          | 35 |
| Endpoint Security                 | 36 |
| Privacy                           | 37 |
| Anti-Ransomware                   | 37 |
| Protection Statistics             | 38 |
| File Anti-Virus                   | 38 |
| Mail Anti-Virus                   | 40 |
| Anti-Spam                         | 40 |
| Web Protection                    | 41 |
| Endpoint Security-USB             | 41 |
| Endpoint Security-Application     | 42 |
| Summary Top 10                    | 42 |
| Asset Changes                     | 43 |
| Live Status                       | 44 |
| Configure Dashboard Display       | 45 |
| Managed Computers                 | 46 |
| Search                            | 47 |
| Update Agent                      | 47 |





| Adding an Update Agent                                   | 48  |
|--|-----|
| Deleting an Update Agent                                 | 49  |
| Action List  | 50  |
| Creating a Group   | 50  |
| Removing a Group   | 51  |
| Set Group Configuration                                  | 51  |
| Managing Installations                                   | 52  |
| Deploy/Upgrade Client                                    | 55  |
| Refresh Client   | 56  |
| Manual installation of eScan Client on network computers | 57  |
| Installing eScan Client Using Agent                      | 58  |
| Installing other Software (Third Party Software)         | 59  |
| Uninstall eScan Client                                   | 61  |
| Synchronize with Active Directory                        | 62  |
| Outbreak Prevention                                      | 63  |
| Create Client Setup                                      | 65  |
| Properties of a group                                    | 66  |
| Group Tasks  | 67  |
| Creating a Group Task                                    | 67  |
| Managing a Group Task                                    | 69  |
| Assigning a Policy to the group                          | 70  |
| Policy Template  | 72  |
| Defining Policies  | 72  |
| Creating Policy Template for a group/specific computer   | 74  |
| Editing a Policy Template                                | 75  |
| Assigning Policy Template to Group (s)                   | 153 |
| Assigning Policy Template to Computer(s)                 | 154 |
| Deleting Policy Template                                 | 155 |
| Copying a Policy Template                                | 155 |
| Parent Policy  | 156 |
| Policy Criteria Templates                                | 158 |
| Adding a Policy Criteria Template                        | 158 |
| Viewing Properties of a Policy Criteria template         | 163 |
| Deleting a Policy Criteria template                      | 164 |
| Client Action List                                       | 166 |
| Set Host Configuration                                   | 167 |
| Deploy/Upgrade Client                                    | 168 |
| Uninstall eScan Client                                   | 169 |
| Move to Group  | 170 |
| Remove from Group  |     |
| Connect to Client (RMM)                                  | 170 |
| Add to RMM License                                       |     |
| Manage I wo-FA License                                   |     |
| Export   |     |
| Show Installed Softwares                                 | 173 |





| Force Download                                    | 174 |
|---|-----|
| On Demand Scanning                                | 175 |
| Send Message                                      | 176 |
| Outbreak Prevention                               |     |
| Delete All Quarantine Files                       | 179 |
| Create OTP  |     |
| Pause Protection                                  |     |
| Resume Protection                                 |     |
| Properties of Selected Computer                   |     |
| Unmanaged Computers                               |     |
| Network Computers                                 |     |
| Creating a New Group from the Select Group window |     |
| IP Range  |     |
| Adding New IP Range                               |     |
| Moving an IP Range to a Group                     |     |
| Deleting an IP Range                              |     |
| Active Directory                                  |     |
| Adding an Active Directory                        |     |
| Moving Computers from an Active Directory         | 191 |
| New Computers Found                               |     |
| Filter Criteria                                   | 192 |
| Action List                                       | 193 |
| Report Templates                                  | 194 |
| Creating a Report Template                        | 195 |
| Creating Schedule for a Report Template           | 196 |
| Viewing Properties of a Report Template           | 196 |
| Deleting a Report Template                        | 196 |
| Report Scheduler                                  | 197 |
| Creating a Schedule                               | 197 |
| Viewing Reports on Demand                         | 199 |
| Managing Existing Schedules                       | 200 |
| Generating Task Report of a Schedule              | 200 |
| Viewing Results of a Schedule                     | 200 |
| Viewing Properties of a Schedule                  | 201 |
| Deleting a Schedule                               | 201 |
| Events and Computers                              | 202 |
| Events Status                                     | 202 |
| Computer Selection                                | 203 |
| Software/Hardware Changes                         | 204 |
| Violations  | 205 |
| Settings  | 205 |
| Event Status Setting                              | 206 |
| Computer Selection                                | 207 |
| Software/ Hardware Changes Setting                | 210 |
| Performing an action for computer                 | 211 |





| Tasks for Specific Computers           | 213 |
|--|-----|
| Creating a task for specific computers | 213 |
| Viewing Properties of a task           | 215 |
| Viewing Results of a task              | 215 |
| Deleting a task for specific computers | 216 |
| Asset Management                       | 217 |
| Hardware Report                        | 217 |
| Filtering Hardware Report              | 218 |
| Exporting Hardware Report              | 219 |
| Software Report                        | 219 |
| Filtering Software Report              | 220 |
| Exporting Software Report              | 220 |
| Software License                       | 221 |
| Filtering Software License Report      | 221 |
| Exporting Software License Report      | 222 |
| Software Report (Microsoft)            | 222 |
| Filtering Software Report (Microsoft)  | 223 |
| Exporting Software Report (Microsoft)  | 223 |
| Filtering Microsoft OS Report          | 224 |
| Exporting Microsoft OS Report          | 224 |
| User Activity                          | 225 |
| Print Activity                         | 225 |
| Viewing Print Activity Log             | 225 |
| Filtering Print Activity Log           | 226 |
| Exporting Print Activity Report        | 227 |
| Print Activity Settings                | 227 |
| Session Activity Report                | 228 |
| Viewing Session Activity Log           | 228 |
| Filtering Session Activity Log         | 228 |
| Exporting Session Activity Report      | 229 |
| File Activity Report                   | 230 |
| Viewing File Activity Log              | 230 |
| Filtering File Activity Log            | 230 |
| Exporting File activity Report         | 231 |
| Patch Report                           | 232 |
| Patch report                           | 232 |
| Filtering Patch Report                 | 232 |
| Exporting Patch Report                 | 233 |
| All Patch Report                       | 233 |
| Filtering All Patch Report             | 234 |
| Exporting All Patch Report             | 234 |
| Notifications                          | 235 |
| Outbreak Alert                         | 235 |
| Event Alert                            | 236 |
| Unlicensed Move Alert                  | 237 |





| New Computer Alert   | 237 |
|--|-----|
| SMTP Settings  | 238 |
| Settings   | 239 |
| EMC Settings   | 240 |
| Web Console Settings   | 242 |
| Update Settings  | 244 |
| General Config   | 245 |
| Update Notification  | 246 |
| Scheduling   | 247 |
| Auto-Grouping  | 247 |
| Excluding clients from auto adding under Managed Group(s)                    | 249 |
| Removing clients from the excluded list                                      | 249 |
| Defining a group and client selection criteria for auto adding under managed |     |
| computer(s)  | 250 |
| Two-Factor Authentication (2FA)  | 251 |
| Enabling 2FA login   | 252 |
| Disabling 2FA login  | 253 |
| Administration   | 255 |
| User Accounts  | 255 |
| Creating a User Account  | 255 |
| Adding a User from Active Directory  | 256 |
| Deleting a User Account  | 257 |
| User Roles   | 258 |
| Adding a User Role   | 258 |
| Role Properties  | 259 |
| Deleting a User Role   | 262 |
| Export & Import  | 262 |
| Export Settings  | 263 |
| Import Settings  | 263 |
| Scheduling   | 264 |
| Customize Setup  | 265 |
| Creating a customized setup for Windows                                      | 266 |
| Editing Setup Properties   | 266 |
| Deleting a Setup   | 267 |
| License  | 268 |
| Adding and Activating a License  | 268 |
| Moving Licensed Computers to Non-Licensed Computers                          | 269 |
| Moving Non-Licensed Computers to Licensed Computers                          | 271 |
| Graphical User Interface (GUI)   | 273 |
| Data Encryption  | 274 |
| How to Create a Vault?   | 274 |
| Identity protection  | 281 |
| Configuration  | 282 |
| Reports  | 283 |
| Help   | 284 |





| Quick Access Links   |  |
|----------------------|--|
| Rescue Mode          |  |
| eScan Remote Support |  |
| Tools                |  |
| Contact Us           |  |
| Chat Support         |  |
| Forum Support        |  |
| Email Support        |  |
|                      |  |





# Introduction

eScan Management Console is a web-based centralized management console that lets an administrator install and manage eScan client on the computers connected across the network. With this console, you can perform following activities–

- Install eScan client application on computers.
- Install third party applications and deploy patches.
- Monitor the security status of computers.
- Create and manage policies or tasks for computers.
- Create and view customized reports of the security status of the computers.
- Manage notifications for alerts and warnings for computers.

# Pre-requisites for eScan Server

Before installing eScan ensure that the following pre-requisites are met:

- Access to computer as an administrator.
- Uninstall the existing anti-virus software, if any.
- Check for free space on the hard disk/partition for installing eScan.
- Static IP address for eScan server.
- IP address of the mail server to which warning messages will be sent (optional).

**NOTE** If authentication for the mail server is mandatory for accepting emails, you will need a username and password to send emails.





# System Requirements

#### • Windows (Windows server & workstations) Platforms Supported:

Microsoft® Windows® 2019 / 2016 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 R2 / 2003 / 10 / 8.1 / 8 / 7 / Vista / XP SP 2 / 2000 Service Pack 4 and Rollup Pack 1

(For 32-bit and 64-bit Editions)

- Hardware for Clients and Server (Server):
  - CPU 2GHz Intel<sup>™</sup> Core<sup>™</sup> Duo processor or equivalent.
  - Memory 4 GB & above
  - Disk Space 8 GB & above
- Endpoints:
  - 1.4 Ghz minimum(2.0 Ghz recommended) Intel Pentium or equivalent
  - GB minimum (1.5 GB recommended )
  - Disk Space 1GB and more

#### • eScan Management Console can be accessed by using following browsers:

- Internet Explorer 9 and above
- Firefox 14 and above
- Google Chrome latest version
- Microsoft Edge latest version





# Installing eScan TSS for Business

#### • Installing eScan TSS for Business from CD/DVD

Installing eScan TSS for business from the CD/DVD is very simple, just insert the CD/DVD in the ROM and wait few seconds for the Autorun to run the installation wizard. In case the installation wizard does not run automatically, locate and doubleclick the twn4ksmk.exe on CD-ROM. This will run the installation wizard based setup of eScan TSS for business. To complete the installation, follow the instructions on screen.

• Downloading and installing eScan TSS for Business from internet

You can also download the setup file from <u>here</u>. For installing eScan Server from the setup file downloaded from the internet, just double click on the twn4ksmk.exe and follow the instructions on the screen to complete the installation process.





# **Installation Process**

To install the eScan TSS for business, follow the steps given below: The installation wizard displays following window:



- 1. Click the drop-down and select a desired language for installation.
- 2. Click **OK**.

**NOTE** The Default Language displayed in the drop-down menu is dependent on the Operating System's language installed on the computer.

- 3. The installation wizard welcomes you. To proceed, click on **Next**. **License Agreement** screen appears.
- 4. Select Destination Location for the installation of eScan TSS for Business. If you want to select a different installation location, click **Browse** and select the destination folder for installation.







| NOTE | Default Path for eScan installation on a 32-bit PC – C:\Program Files\eScan       |
|------|---|
| NOTE | Default path for eScan installation on a 64-bit PC – C:\Program Files (x86)\eScan |

 Please read the License Agreement completely. To proceed with the installation, select the option **I accept the agreement** and then click **Install**. The installation wizard initiates installation and displays the process.



After the installation, the wizard asks you to configure the settings for SQL Server hosting and Login settings for the eScan Management console.







6. To proceed, click **Next**. The configuration wizard requests you to select a computer for hosting SQL server.

| e Scan Management                | Console Configuration Wizard         |
|----------------------------------|--------------------------------------|
| Select computer hosting SQL S    | erver.                               |
| Use local instance               | <u> </u>                             |
| Install Microsoft SQL Server Exp | ress Edition (recommended)           |
| SQL Server Installation Path     | C:\Program Files (x86)\Micros Browse |
| Choose existing                  |                                      |
| SQL Server Name                  | Browse                               |
|                                  |                                      |
|                                  | Back Next                            |

The window displays following options:

• Use local instance

If you already have SQL instances running locally, click the drop-down and select a desired local instance.

• **Install Microsoft SQL Server Express Edition (recommended)** If the computer selected for eScan server installation doesn't have SQL server installed, it is recommended that you select this option. Click Browse and select an installation path for SQL server installation.

| NOTE | Default installation path for 32-bit PC – C:\Program Files\Microsoft SQL Server       |
|------|---|
|      | Default installation path for 64-bit PC – C:\Program Files (x86)\Microsoft SQL Server |

# Choose existing If an SQL server hosting computer exists on your LAN, select this option. Click Browse and select the SQL server hosting computer.

- Select this option if you have already created an instance for eScan Database on any SQL Server installed on any computer connected to the network. Click **Browse** to locate the server. This option is being used if you already have an instance running locally or in your local area network.
- 7. After selecting an option, click **Next** to proceed.

If you selected the recommended option, the configuration wizard will begin installation of the Microsoft SQL Server Express.





| 4 | eScan Management Console Configuration Wizard  |
|---|--|
|   | This wizard will install following prerequisites along with Microsoft SQL<br>Server Express: |
|   | Microsoft Windows Installer<br>Microsoft .Net Framework                                      |
|   | Microsoft SQL Server Express Edition   |
|   | Click "Install" to proceed.  |
|   | <u>B</u> ack Install   |

8. To proceed, click **Install**. After the successful installation, the wizard displays following window.

| C      | eScan Management Console Configuration Wizard                         |
|--------|---|
| Instal | ling Microsoft SQL Server Express                                     |
| Micro  | soft SQL Server Express has been installed successfully on your<br>m. |
| ~      | Microsoft Windows Installer   |
| ~      | Microsoft .Net Framework  |
| ~      | Microsoft SQL Server Express Edition                                  |
|        | Click "Next" to continue  |
|        | Back  |



9. To proceed, click **Next**. The wizard requests you to enter the login credentials for the root user.

**NOTE** The default username for web console is **root**.

| eScan Manag   | gement Console Configuration Wizard  |  |  |  |  |
|---|--|--|--|--|--|
| eScan Management Console login information                  |  |  |  |  |  |
| Enter the login credentials for<br>eScan Management Console | Enter the login credentials for the root user to give permission to manage the eScan Management Console. |  |  |  |  |
| User name:  | root   |  |  |  |  |
| Description:  | Administrator account created during installation  |  |  |  |  |
| Password:*  |  |  |  |  |  |
| Confirm Password:*  |  |  |  |  |  |
| Email address:*   |  |  |  |  |  |
|   | Click "Next" to continue   |  |  |  |  |
|   | <u>Back</u> <u>N</u> ext   |  |  |  |  |

10. After filling all the details, click **Next**. The wizard displays installation successful message.

| f#1   | e Scan Management Console Configuration Wiza<br>Completed.   | ard |
|-------|--|-----|
| eScan | You have successfully installed / configured Microsoft SQL<br>Server Express on your computer. Click "Finish" to proceed<br>with eScan installation. | 4   |

an





11. To exit the eScan Management Console Configuration Wizard, click **Finish**. After completing the installation process, the wizard asks you to restart your PC.

| eScan Install                                    |  |
|--|--|
| C POSTAL<br>WORLD                                | eScan<br>Reboot PC to complete eScan Installation? |
| eS@an<br>www.escanav.com<br>Copyright MicroWorld | Yes No   |

12. To restart PC, select option **Yes**, restart the computer now. After the computer restarts, launch the eScan TSS for Business and enter the license key for <u>activation</u>.

| NOTE | It is recommended that To run eScan services fully it is recommended that |
|------|---|
| NUTE | you restart the PC.   |





# Components of eScan Server

The eScan Server is comprised of following components:

#### • eScan Server

This is the core component that lets you manage, deploy and configure eScan client on computers. It stores the configuration information and log files about the computers connected across the network. Being the core component, it communicates with the following components.

#### • Agent

It manages the connection between the eScan server and the client computers.

#### • eScan Management Console

It is a Web-based application hosted on the eScan Server. With this application, administrators can manage and configure eScan on computers in the network.

#### • Microsoft SQL Server Express Edition

It is a database for storing events and logs already included in the eScan Setup file.

#### • Apache

It is an open source, cross-platform web server software essential for running eScan Management Console. It's included in the eScan Setup file.

For Windows 8 / 8.1 / 2008 / 2012 / 2016 / 2019 operating systems, the SQL 2008 Express edition will be installed.

**NOTE** For Windows 7 and below, SQL 2005 Express edition will be installed.

Uninstallation of eScan server won't remove SQL and APACHE from the endpoint. The user will have to uninstall these components manually.





## Web Console Login

The web console login page can be accessed via two methods.

To log in to the eScan Management Console, follow the steps given below:

- 1. Launch a web browser.
- 2. Enter the following URL: <IP address of the eScan Server installed system>:10443 Web console login page appears.

|                 | Lines many and Decemend to person the Web Concele |     |
|-----------------|---|-----|
| Please type you | User hame and Password to access the web console. |     |
| Username:*      |   |     |
|                 | For Active Directory account:                     |     |
|                 |   |     |
| Password:*      | Login   | 1   |
| You can provide | users the following link(s):                      |     |
| eScan Client S  | etup (Windows)                                    |     |
| http://         | /Setup/eScan Client.exe                           | [+] |
| eScan Agent S   | etup (Windows)                                    |     |
| nttp://         | /Setup/Agent_Setup.exe                            | [+] |

- 3. Enter the login credentials defined during installation.
- 4. Click Login.

The second method to go to login page is as follows:

1. In the taskbar, right-click the eScan Management Console icon **P**. A list of options appears.



2. Click Open Web Console.

Default browser launches and displays web console login page.





Rests of the options are explained below:

#### **Client Live Updater**

Clicking this option displays live event feeds from all computers on your network. This feed consists of IP Address, Username of the computers, Module Names and Client actions. This Live Feed list can be exported to Excel if required.

| K           |          |                      |                  |                    | Cli      | ent Live U  | pdate    |
|-------------|----------|----------------------|------------------|--------------------|----------|-------------|----------|
| Date        | Time     | Machine Na           | IP Address       | User Name          | Event ID | Module Name | Descri 🗸 |
| 28 May 2020 | 14:32:38 | 411.011.040          | 10.000.000       | 101001-001         | Endpoin  | IC1 eScan E | Execu    |
| 28 May 2020 | 14:32:19 |                      | 100100000000     | 101101100          | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:30:49 | - 40 - 51 - 141      | 1001000          | 1011-011-0201      | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:30:41 |                      | 1001000          | -411-011-0401      | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:30:20 |                      | 1001000          | - 40-01-020        | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:30:41 |                      | 10.000           |                    | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:30:55 | - 40.0 (0.0 (0.407)) | 10.1001-1-1      | 101101-011-0101    | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:30:02 |                      | 10010000000      | - 61-61-1-687      | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:31:17 |                      | 10010000000      | -61-61-627         | Endpoin  | [C] eScan E | Execu    |
| 28 May 2020 | 14:31:24 |                      | 1001000000000    | -814-811-1487      | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:30:14 |                      | 10.1001          | -61-61-1487        | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:30:59 |                      | 18-1 (BE11-1-1-) | -61-61-1487        | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:30:26 |                      | 100-1001         | -61-61-147         | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:31:26 | - 411 - 611 - 1421   | 10010000000      | -61-61-687         | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:31:27 |                      | 100100000000     | - 614-617-1487     | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:30:21 |                      | 100100000000     | -814-811-1487      | Endpoin  | [C] eScan E | Execu    |
| 8 May 2020  | 14:30:34 |                      | 101001-1-1       | - 611 - 611 - 1287 | Endpoin  | [C] eScan E | Execu v  |
| :           |          |                      |                  |                    |          |             | >        |
|             |          |                      |                  | _                  |          |             |          |

#### **Stop Announcement**

Clicking this option stops broadcast from and towards the server.

#### About eScan Management Console

Clicking this option displays Server Up Time and general information.

#### Shut Down

Clicking this option shuts down the eScan Management console.

|      | It is recommended that you do not shut down the server, as doing so will stop the communications between client and server. |
|------|---|
| NOTE |   |
|      | The "root" is the Superuser account created by eScan during Installation, see -   |
|      | Filling Login Credentials for eScan Management Console.   |





The web console login page displays following links:

#### • eScan Client Setup (Windows)

This link can be shared via email to the computer users where remote installation is impossible. By clicking this link users can download the eScan Client Setup and install it manually on their computers. Users can also directly access the eScan Management console from their desktop.

#### • eScan Agent Setup (Windows)

This link can be shared via email to the computer user where you are unable to get system information or communication is breaking frequently. After the eScan Agent Setup is downloaded and installed on the Managed Computer, it establishes the connection between the server and client computers.

#### • eScan AV Report

Clicking this link redirects you to the eScan AV Report webpage that displays Anti-Virus report for eScan installed computers. Select a group and then click **Get Details** > **Export**. A detailed .xls report will be downloaded to computer.





# Main Interface

Upon first login, console displays Setup Wizard that familiarizes you with the basic procedures. It is recommended that you follow the steps displayed, before proceeding to the other modules.

| e Scan                       | 😵 About eScan 💩 root 🗳 Log Off<br>eScan Management Console (14.0.1400. 🚥)  | )  |
|------------------------------|--|----|
| DashBoard                    | Setup Wizard   | р  |
| Setup Wizard                 |  | 1  |
| Managed Computers            | Welcome to the Setup Wizard  | 4. |
| Unmanaged Computers          | This Wizard helps to create Groups, select computers for respective Groups and installation of eScan on selected Groups. |    |
| Report Templates             |  |    |
| Report Scheduler             |  |    |
| Events & Computers           |  |    |
| Tasks For Specific Computers |  |    |
| Asset Management             | Cital Market to Descend  |    |
| User Activity                | CIICK Next to Proceed.   |    |
| Patch Report                 | Next >   |    |
| Notifications                |  | -  |
| ± Settings                   |  |    |
| Administration               |  |    |
| License                      |  |    |
|                              |  |    |
|                              |  |    |

| NOTE | The Setup Wizard is available in the navigation panel and can be accessed again as |
|------|--|
| NOTE | per your requirement.  |

The Navigation panel is found on the left of the main interface screen. The username of the login in user is displayed at the top right corner of the screen.

You will find a **Help** link at the top right corner of every screen that will take you to a quick online help guide for the features on that screen.

The description of different link found on the main interface of the eScan console is listed in the table below:

#### About eScan

Clicking this link redirects you to MircoWorld's homepage.

#### Username

Clicking Username lets you edit User Login details like Full name, Password and email address that you use to Login in the eScan Management Console.





#### Log off

Clicking Logoff logs you out of the eScan Management Console.

#### root

Clicking root lets you change root account's password.

| 📀 eScan Management (           | Console - Google Chrome                           |                      |
|--------------------------------|---|----------------------|
| (i) Not secure                 | :10443/ewconsole/ewconsole.dll/editUserName?usi   | rid=1&from=banner& 🔍 |
| Edit User                      |   | 👔 Help               |
| Enable this account            | nt  |                      |
| Account Type and               | Information                                       |                      |
| Custom Account<br>User's name: | root  |                      |
| Full Name*:                    | Administrator account created during installation |                      |
| New Password:                  |   |                      |
| Confirm Password:              |   |                      |
| Email Address:                 | a@b.com   |                      |
|                                | For Example: user@yourcompany.com                 |                      |
| Account Role                   |   |                      |
| Role*: Adminis                 | trator  | Ŧ                    |
| Save                           | Close   | (*) Mandatory Fields |
|                                |   |                      |
|                                |   |                      |
|                                |   |                      |
|                                |   |                      |

Enter the new password in **New Password** and **Confirm Password** fields and then click **Save**. The password for root account will be saved and updated.





# **Navigation Panel**

Navigation Panel on the left side displays accessible modules that let you manage, install, update and configure eScan client on the computers connected across the network.

| DashBoard                    |
|------------------------------|
| Setup Wizard                 |
| Managed Computers            |
| 🗄 Unmanaged Computers        |
| Report Templates             |
| Report Scheduler             |
| Events & Computers           |
| Tasks For Specific Computers |
| Asset Management             |
| 🗄 User Activity              |
| Patch Report                 |
| Notifications                |
| 🗄 Settings                   |
| + Administration             |
| License                      |

The navigation panel contains following modules:

- Dashboard
- Setup Wizard
- Managed Computers
- Unmanaged Computers
- Report Templates
- Report Scheduler
- Events & Computers
- Tasks for Specific Computers
- Asset Management
- User Activity
- Patch Report
- Notifications
- Settings
- Administration
- License





#### Dashboard

The Dashboard module displays charts showing Deployment status, Protection status, Protection Statistics, Summary Top 10, Asset Changes, Live Status and the monitoring done by Management Console of the computers for virus infections and security violations.

#### Setup Wizard

The Setup Wizard module guides you step-by-step in creation of groups, adding computers to respective groups, adding hosts from the network and installing client on the connected computer at a desired path/ location on that computer.

#### **Managed Computers**

The Managed Computers module lets you can define/configure Policies for computers. It provides various options for creating groups, adding tasks, deploying or uninstalling client application, moving computers from one group to the other and redefining properties of the computers from normal to roaming users and vice versa.

#### **Unmanaged Computers**

The Unmanaged Computers module displays information about the computers that have not yet been assigned to any group. This section also lets you set the host configuration, move computers to a group, view the properties of a computer, or refresh the information about a client computer with **Action List** menu.

#### **Report Templates**

The Report Templates module lets you create and view customized reports based on a given template, for a given period; sorted by date, computer, or action taken; and for a selected condition or target group. It also provides options for configuring or scheduling reports, viewing report properties, and refreshing or deleting existing reports.

#### **Report Scheduler**

The Report Scheduler module lets you schedule a new reporting task, run an already created reporting schedule or view its properties.

#### **Events and Computers**

The Events and Computers module lets you monitor various activities performed on client's computer. You can view log of all events based on Event Status, Computer Selection or Software/ Hardware Changes on that client computer. Using the Settings option on the screen you can define settings as desired.





#### **Tasks for Specific Computers**

The Tasks for Specific Computers module lets you create and run tasks like enable/disable protection(s) on specific computers, it also lets you schedule or modify created tasks for selected computers or groups. You can also easily re-define the settings of an already created task for a computer. It also lets you view results of the completed tasks.

#### **Asset Management**

The Asset Management module provides you the entire Hardware configuration and list of software installed on computers in a tabular format. Using this module, you can easily keep a track of all the Hardware as well as Software resources installed on all the Computers connected to the Network. Based on different Search criteria you can easily filter the information as per your requirement. It also lets you export the entire system information available through this module in PDF, Microsoft Excel or HTML formats.

#### **User Activity**

The User Activity module lets you monitor different tasks/activities like printing, session login time or actions on files in the client computers.

#### **Patch Report**

The Patch Report module displays the number of windows security patches installed and not installed on managed computers. This will help an administrator identify the number of vulnerable systems in the network and install the critical patches quickly.

#### Notifications

The Notifications module provides you options to enable different notifications when different actions/incidents occur on the server. You may choose to be notified or not to be notified based on the significance of these actions in your business.

#### Settings

The Settings module lets you configure FTP downloads settings, maintaining Logs, eScan Management Console timeout settings, update download settings along with Two-factor authentication login settings for eScan.

#### Administration

The Administration module lets you create User Accounts and allocate them Admin rights for using eScan Management Console. It is helpful in a large organization where installing eScan client on large number of computers in the organization may consume lot of time and efforts. Using this option, you can allocate rights to the other employees which will allow them to install eScan Client and implement Policies and tasks on other computers.





#### License

The License module lets you manage license of users. You can add, activate, and view the total number of licenses available for deployment, number of licenses deployed, and number of licenses remaining with their corresponding values. You can also move the licensed computers to non-licensed computers and non-licensed computers to licensed computers.





# Dashboard

The Dashboard module displays statistics and status of eScan Client installed on computers in pie chart format. It consists of following tabs:

- Deployment Status
- Protection Status
- Protection Statistics
- Summary Top 10
- Asset Changes
- Live Status

In the top right corner there are additional links that are explained below:

#### **Date of Virus Signatures**

It displays the last date on which the Virus signatures were updated. Click this link to update virus signatures.

#### Refresh

Clicking **Refresh** refreshes the Dashboard information.





# **Deployment Status**

This tab displays information about eScan Client installed on computers, active licenses and current eScan version number in use.



### eScan Status



Installed – It displays the number of computers on which eScan Client is installed.
Not Installed - It displays the number of computers on which eScan Client is not installed.
Unknown - It displays the number of computers on which Client installation status is unknown. (Server is unable to receive information from the computers for a long time)
Total – It displays the total number of computers connected across the network.





### License

| License |                    |                |       |
|---------|--------------------|----------------|-------|
|         | License in Use     | 385            |       |
|         | License Remaining  | 14620          |       |
|         | Total License Size | 15005          |       |
|         | 27 day(s) remaini  |                |       |
|         |                    |                |       |
|         |                    | [ Manage Licer | nse ] |

License in Use - It displays the number of licenses that are active. Licenses Remaining - It displays the number of remaining licenses. Total License Size - It displays the total number of licenses available.

## **Protection Status**

This tab displays the status of eScan Client's modules along with the Update and Scan status since last 7 days.

| Deployment Status Pro | otection Status Protection Stat                       | istics Summary Top 10                   | Asset Changes Live Status |   |   |
|-----------------------|---|---|---------------------------|---|---|
|                       |   | Since Las                               | t 7 Days                  |   |   |
|                       | Update Status   |   | Sca                       | n Status  |   |
| G                     | Updated<br>Not Updated<br>Total                       | 4<br>282<br>286                         |                           | Scanned<br>Not Scanned<br>Unknown<br>Total            | 0<br>0<br><u>286</u><br>286             |
|                       |   | Protectio                               | n Status                  |   |   |
|                       | File Anti-Virus                                       |   |                           | Proactive   |   |
|                       | Started<br>Stopped<br>Unavailable<br>Unknown<br>Total | 4<br>0<br>0<br><u>282</u><br><u>285</u> |                           | Started<br>Stopped<br>Unavailable<br>Unknown<br>Total | 2<br>0<br>0<br><u>383</u><br><u>385</u> |

### **Update Status**







**Updated** – It displays the number of computers on which virus signature database is updated.

**Not Updated** - It displays the number of computers on which virus signature database is not updated.

**Total** - It displays the total number of computers connected across the network.

Clicking **Groupwise Details** displays Groupwise Update Status window.

| e Scan                  |  |  |                   |                | eSca | n Ma      | nage      | emen      | t Co  | onsole       |
|-------------------------|--|--|-------------------|----------------|------|-----------|-----------|-----------|-------|--------------|
| Groupwise Update Status |  |  |                   |                |      | We        | edneso    | lay, O    | ctobe | r 23, 2019   |
| Hanaged Computers       | □ Include Sub Groups ☑<br>Group: Managed Compute | Groupwise Deta<br><b>:rs</b> (Include Su | ails<br>b Groups) |                |      |           |           |           |       | <u>Print</u> |
|                         | Group Name                                       | <u>Updated</u>                           | Not Updated       | License in Use | EP   | <u>E0</u> | <u>CP</u> | <u>co</u> | IL    | NA           |
|                         | Managed Computers                                | 0  | 382               | 382            | 0    | 0         | 1         | 0         | 0     | <u>381</u>   |
|                         | Sample Group                                     | 0  | 3                 | 3              | 1    | 0         | 1         | 0         | 0     | 1            |
|                         | Test   | 3  | 0                 | 3              | 2    | 0         | 1         | 0         | 0     | 0            |

It displays the number of computers on which virus database is Updated, Not Updated and Licenses in Use as per the group. Selecting **Include Sub Groups** checkbox will display the subgroups containing computers.

### Scan Status



**Scanned** - It displays the number of computers that have been scanned in last 30 days for viruses and malware infections.

**Not Scanned** - It displays the number of computers that have not been scanned in last 30 days for viruses and malware infections.

**Unknown** - It displays the number of computers on which the scan status is unknown. **Total** - It displays the total number of computers connected across the network.





### File Anti-Virus

| File An | ti-Virus                          |             |  |
|---------|-----------------------------------|-------------|--|
|         | Started<br>Stopped<br>Unavailable | 4<br>0<br>0 |  |
|         | Total                             | 386         |  |

**Started** – It displays the number of computers on which the File Anti-Virus module is in Started state.

**Stopped** – It displays the number of computers on which the File Anti-Virus module is in Stopped state.

**Unavailable** – It displays the number of computers where the File Anti-Virus module is unavailable.

**Unknown** – It displays the number of computers where the File Anti-Virus module status is unknown.

**Total** – It displays the total number of computers connected across the network.

### Proactive



**Started** - It displays the number of computers on which Proactive scanning service is running.

**Stopped** - It displays the number of computers on which Proactive scanning service is stopped.

**Unavailable** – It displays the number of computers where Proactive scanning service is unavailable. This module is available only in computers with Windows OS.

**Unknown** - It displays the number of computers on which the Proactive scanning service status is unknown.

**Total** - It displays the total number of computers connected across the network.





## Mail Anti-Virus

| Mail Ar | nti-Virus   |     |  |
|---------|-------------|-----|--|
|         | Started     | 0   |  |
|         | Stopped     | 3   |  |
|         | Unavailable | 0   |  |
|         | Unknown     | 383 |  |
|         | Total       | 386 |  |
|         |             |     |  |

**Started** – It displays the number of computers on which the Mail Anti-Virus module is in Started state.

**Stopped** – It displays the number of computers on which the Mail Anti-Virus module is in Stopped state.

**Unavailable** – It displays the number of computers on which the Mail Anti-Virus module is unavailable.

**Unknown** – It displays the number of computers on which the Mail Anti-Virus module status is unknown.

**Total** – It displays the total number of computers connected across the network.

### Anti-Spam



**Started** – It displays the number of computers on which the Anti-Spam module is in Started state.

**Stopped** – It displays the number of computers on which the Anti-Spam module is in Stopped state.

**Unknown** – It displays the number of computers on which the Anti-Spam module status is unknown.

**Unavailable** – It displays the number of computers on which the Anti-Spam module is unavailable.

**Total** – It displays the total number of computers connected across the network.





## Web Anti-Phishing

| Web A | nti-Phishing |     |
|-------|--------------|-----|
|       | Started      | 0   |
|       | Stopped      | 3   |
|       | Unavailable  | 0   |
|       | Unknown      | 383 |
|       | Total        | 386 |
|       |              |     |
|       |              |     |

**Started** – It displays the number of computers on which the web Anti-Phishing service is started.

**Stopped** – It displays the number of computers on which the web Anti-Phishing service is stopped.

**Unknown** – It displays the number of computers on which the web Anti-Phishing service status is unknown.

**Unavailable** - It displays the number of computers on which the web Anti-Phishing service is unavailable.

**Total** – It displays the total number of computers connected across the network.

### Mail Anti–Phishing



**Started** – It displays the number of computers on which the Mail Anti-Phishing service is enabled.

**Stopped** – It displays the number of computers on which the Mail Anti-Phishing service is disabled.

**Unknown** – It displays the number of computers on which the Mail Anti-Phishing service status is unknown.

**Unavailable** – It displays the number of computers on which the Mail Anti-Phishing service is unavailable.

**Total** – It displays the total number of computers connected across the network.





### Web Protection

| Web P | rotection   |   |
|-------|---|---|
|       | Started   | 1   |
|       | Stopped   | 2   |
|       | Unavailable   | ed <u>1</u><br>ed <u>2</u><br>ailable 0<br>own <u>383</u><br><u>386</u> |
|       | Web Protection  Started  Stopped  Unavailable  Unknown  Stopped  Total  O | 383   |
|       | Total   | 386   |
|       |   |   |

**Started** – It displays the number of computers on which the Web Protection module is in Started state.

**Stopped** – It displays the number of computers on which the Web Protection module is in Stopped state.

**Unavailable** – It displays the number of computers on which the Web Protection module is unavailable.

**Unknown** – It displays the number of computers on which the Web Protection module status is unknown.

**Total** – It displays the total number of computers connected across the network.

### **Firewall**



**Started** - It displays the number of computers on which the Firewall module is in Started state.

**Stopped** - It displays the number of computers on which the Firewall module is in Stopped state.

**Unavailable** - It displays the number of computers on which the Firewall module is unavailable.

**Unknown** - It displays the number of computers on which the Firewall module status is unknown.

**Total** – It displays the total number of computers connected across the network.





### Endpoint Security

| Endpoint | Security    |                 |            |
|----------|-------------|-----------------|------------|
|          | Started     | 4               |            |
|          | Stopped     | 0               |            |
|          | Unavailable | 0               |            |
|          | Unknown     | 382             |            |
|          | Total       | 386             |            |
|          |             | [ Other Devices | <u>.</u> ] |

**Started** - It displays the number of computers on which the Endpoint Security module is in Started state.

**Stopped** - It displays the number of computers on which the Endpoint Security module is in Stopped state.

**Unavailable** – It displays the number of computers on which the Endpoint Security module is unavailable.

**Unknown** - It displays the number of computers on which the Endpoint Security module status is unknown.

**Total** – It displays the total number of computers connected across the network.

Clicking **Other Devices** displays details about other devices.

| Other Devices     | Allowed  | Blocked  | Unavailable | Unknown | Tota |
|-------------------|----------|----------|-------------|---------|------|
| SD Card           | <u>6</u> | <u>0</u> | <u>0</u>    | 382     | 388  |
| Web Cam           | <u>6</u> | <u>0</u> | <u>0</u>    | 382     | 388  |
| Bluetooth         | <u>6</u> | <u>0</u> | <u>0</u>    | 382     | 388  |
| USB Modem         | <u>6</u> | 0        | <u>0</u>    | 382     | 388  |
| Composite Devices | <u>6</u> | 0        | <u>0</u>    | 382     | 388  |
| CD/DVD            | <u>6</u> | 0        | 0           | 382     | 388  |
| Imaging Devices   | 6        | 0        | <u>0</u>    | 382     | 388  |
| WI-FI             | 6        | 0        | <u>0</u>    | 382     | 388  |
| Printer           | 6        | <u>0</u> | <u>0</u>    | 382     | 388  |




# Privacy

| Started     | 0        |
|-------------|----------|
| _           |          |
| Stopped     | <u>4</u> |
| Unavailable | 0        |
| <br>Unknown | 382      |
| Total       | 386      |

**Started** - It displays the number of computers on which the Privacy Control module is in Started state.

**Stopped** - It displays the number of computers on which the Privacy Control module is in Stopped state.

**Unavailable** - It displays the number of computers on which the Privacy Control module of eScan is unavailable.

**Unknown** - It displays the number of computers on which the Privacy Control module status is unknown.

**Total** – It displays the total number of computers connected across the network.

### Anti-Ransomware



**Started** - It displays the number of computers on which the Anti-Ransomware module is in Started state.

**Stopped** - It displays the number of computers on which the Anti-Ransomware module is in Stopped state.

**Unknown** - It displays the number of computers on which the Anti-Ransomware module status is unknown.

**Total** – It displays the total number of computers connected across the network.





# **Protection Statistics**

This tab displays activity statistics and action taken by all modules of eScan Client since last seven days in pie chart format.



#### **Reset Counter**

Clicking **Reset Counter** resets all the statistics to zero. This option proves useful after you have taken an action on infected files and want to scan for residual infection presence.

# File Anti-Virus



**Disinfected** – It displays the number of files disinfected by File Anti-Virus module. **Quarantined** – It displays the number of files quarantined by File Anti-Virus module. **Deleted** - It displays the number of files deleted by File Anti-Virus module.

**Access Denied** - It displays the number of files to which access was denied by File Anti-Virus module.

**Total** – It displays the total number of files on which File Anti-Virus module took action since last seven days.





Clicking underlined numerical displays action taken on infected files amongst different computers and the group that computer belongs to.

| SeScan Management Console       | - Google Chrome           |   |
|---------------------------------|---------------------------|---|
| Not secure                      |                           | on the second |
| Be Scan                         |                           | eScan Management Console  |
|                                 |                           | Tuesday, September 10, 2019   |
| Protection Statistics >> File A | Anti-Virus >> Quarantined |   |
| Client OS Type All 🔻            |                           | <u>Print</u>  |
| Machine Name                    | Status                    | Group   |
| 0.110.00                        | Quarantined (78)          | Managed Computers   |
|                                 | Close                     |   |

Clicking the **Status** link further displays the detection date and time, file path, infection description and computer's username.

| eScan Management (       | nsole - Google Chrome                |   |                       |  |  |
|--------------------------|--------------------------------------|---|-----------------------|--|--|
| Not secure               |                                      |   |                       |  |  |
| eScan Management Consoli |                                      |   |                       |  |  |
|                          |                                      | Tuesda                                  | y, September 10, 2019 |  |  |
| Protection Statistics    | > File Anti-Virus >> Quarantined ( / |   |                       |  |  |
|                          |                                      |   |                       |  |  |
|                          |                                      |   | Print                 |  |  |
| Date/Time                | File Name                            | Description                             | User name             |  |  |
| 06/09/19 13:22:28        | C:\Users\                            | Infected by Virus: EICAR-Test-File (DB) | DIDDE TO SER          |  |  |
| 06/09/19 13:22:30        | C:\Users\                            | Infected by Virus: EICAR-Test-File (DB) | BING TOTAL            |  |  |
| 06/09/19 13:22:31        | C:\Users\                            | Infected by Virus: EICAR-Test-File (DB) | BIODE (BIODE)         |  |  |
| 06/09/19 13:22:33        | C:\Users\                            | Infected by Virus: EICAR-Test-File (DB) | 0100710100            |  |  |
| 06/09/19 13:22:33        | C:\Users\                            | Infected by Virus: EICAR-Test-File (DB) | DISE THE SEC          |  |  |
| 06/09/19 13:22:34        | C:\Users\                            | Infected by Virus: EICAR-Test-File (DB) | BINDE (BOND           |  |  |
| 06/09/19 13:22:38        | C:\Users\                            | Infected by Virus: EICAR-Test-File (DB) | BINEF (BINE)          |  |  |
| 06/09/19 13:22:39        | C:\Users\                            | Infected by Virus: EICAR-Test-File (DB) | BINEF DECK            |  |  |
| 06/09/19 13:22:40        | C:\Users\                            | Infected by Virus: EICAR-Test-File (DB) | ALCONT DUCK           |  |  |
| 06/09/19 13:22:41        | C:\Users\                            | Infected by Virus: EICAR-Test-File (DB) | COLUMN TO AND         |  |  |

Clicking [More] displays additional protection statistics.

| Malware URL Block           |  |
|-----------------------------|--|
| Autorun Block               |  |
| Executable Block USB        |  |
| Executable Block Network    |  |
| Executable Block User based |  |
| Proactive Statistics: Allow |  |
| Proactive Statistics: Block |  |
| Exploit Statistics Block    |  |
| Ransomware Statistics Block |  |
|                             |  |
| Total                       |  |





# Mail Anti-Virus



**Quarantined** – It displays the number of files/emails quarantined by Mail Anti-Virus module.

**Deleted** – It displays the number of files/emails deleted by Mail Anti-Virus module. **Disinfected** – It displays the number of files/emails disinfected by Mail Anti-Virus module. **Total** – It displays the total number of files/emails on which Mail Anti-Virus module took action since last seven days.

### Anti-Spam



**Deleted** – It displays the number of files deleted by Anti-Spam module.

**Quarantined** – It displays the number of files quarantined by Anti-Spam module. **Total** – It displays the total number of files on which Anti-Spam module took action since last seven days.





# Web Protection



**Allowed** – It displays the number of websites to which access was allowed by Web Protection module.

**Blocked** – It displays the number of websites to which access was blocked by Web Protection module.

**Total** – It displays the total number of websites allowed and blocked by Web Protection module since last seven days.

**Suspected Phishing Site** – It displays the number of systems on which suspected phishing sites were blocked. After clicking the numerical, Suspected Phishing Site window appears displaying System Name, Site Status and Computer Group. Clicking Site Status further displays Date, Time, Website name and action taken.

# **Endpoint Security-USB**



**USB Allowed** – It displays the number of USB access allowed by Endpoint Security-USB module.

**USB Blocked** – It displays the number of USB access blocked by Endpoint Security-USB module.

**Total** – It displays the total number of USB connections monitored by Endpoint Security-USB module since last seven days.





# **Endpoint Security-Application**



**Applications Allowed** – It displays the number of applications allowed by Endpoint Security-Application module.

**Applications Blocked** – It displays the number of applications blocked by Endpoint Security-Application module.

**Total** – It displays the total number of applications monitored by Endpoint Security-Application module since last seven days.

# Summary Top 10

This tab displays top 10 Summary of various actions taken by eScan on all computers since last seven days along with bar chart and graph. This tab can be configured by clicking **Configure Dashboard Display**.

| Deployment Status | Protection Status Pr | otection Statistics Summary Top 10 | Asset Changes Live Status |  |  |  |  |
|-------------------|----------------------|------------------------------------|---------------------------|--|--|--|--|
| Since Last 7 Days |                      |                                    |                           |  |  |  |  |
|                   |                      | Top 10 Computer Infe               | ected Count               |  |  |  |  |
| Hits 1            |                      | Computer Name                      | Computer Infected in %    |  |  |  |  |
|                   | 610282018<br>MM-DD   | _                                  |                           |  |  |  |  |
|                   |                      | Top 10 USB Block                   | ked Count                 |  |  |  |  |
| Hits 0            | 9                    |                                    | No Record Found           |  |  |  |  |
|                   | MM-DD                |                                    |                           |  |  |  |  |

The tab displays the summary for following parameters:

- Top 10 Virus Blocked
- Top 10 Computer Infected Count
- Top 10 USB Blocked Count
- Top 10 Application Blocked Count by Application Name
- Top 10 Application Allowed Count by Application Name
- Top 10 Application Blocked Count by Computer Name
- Top 10 Application Allowed Count by Computer Name
- Top 10 Websites Blocked Count by Websites Name





- Top 10 Websites Allowed Count by Websites Name
- Top 10 Websites Blocked Count by Computer Name
- Top 10 Websites Allowed Count by Computer Name
- Top 10 Infected Emails (Mail AV)
- Top 10 Spam Emails (Anti-Spam) from
- Top 10 Websites Blocked Count by Username
- Top 10 Websites Allowed Count by Username
- Top 10 Exploit Blocked Count

# Asset Changes

This tab displays all hardware and software changes carried out on the server computer since last seven days.

| rotection Statistics   | Summary Top 10     | Asset Cha | nges  | Live Status      |  |  |  |
|--|--------------------|-----------|-------|------------------|--|--|--|
| Since Last 7 Days  |                    |           |       |                  |  |  |  |
| Hardware Changes   |                    |           |       |                  |  |  |  |
| Description Machine Count  |                    |           |       |                  |  |  |  |
| RAM  |                    |           |       | 0                |  |  |  |
| CPU  |                    |           |       | 0                |  |  |  |
| MOTHERBOARD 0  |                    |           |       |                  |  |  |  |
| HARD DISK 0  |                    |           |       |                  |  |  |  |
|  |                    |           |       |                  |  |  |  |
|  | Software Changes   |           |       |                  |  |  |  |
| Machine Name   | New Installed Soft | twares    | Unins | talled Softwares |  |  |  |
| Contraction of the local division of the loc | 1                  |           |       | 1                |  |  |  |
| and the second se  | 1                  |           |       | 1                |  |  |  |
|  |                    |           |       |                  |  |  |  |

Clicking the underlined machine names displays softwares installed on the computers since last seven days. Clicking the underlined numerical displays installed / uninstalled softwares on computers since last seven days.





# Live Status

| Protection Statistics | Summary Top 10 | Asset Changes     | Live Status     |  |
|-----------------------|----------------|-------------------|-----------------|--|
|                       | Live S         | Status            |                 |  |
|                       | Live Statu     | s                 |                 |  |
|                       |                | Online<br>Offline | <u>2</u><br>384 |  |
|                       |                | Total             | 386             |  |
|                       |                |                   |                 |  |

This tab displays the number of computers that are online and offline in a network.

Clicking the numerical displays the computer's username, status, eScan Client version number and the group under which it is categorized.





# Configure Dashboard Display

To configure the Dashboard display, follow the steps given below:

1. In the Dashboard screen, at the upper right corner, click **Configure Dashboard Display**.

Configure Dashboard Display window appears displaying tabs and their parameters.

| Configure Dashboard Display   |   |
|---|---|
| Deployment Status   |   |
| eScan Status  | eScan Version   |
| <ul> <li>License Summary</li> </ul>   |   |
| - Protection Status   |   |
| Update Status   | Scan Status   |
| File Anti-Virus   | Proactive   |
| Mail Anti-Virus   | Anti-Spam   |
| FireWall  | Mail Anti-Phishing  |
| Web Protection  | Web Anti-Phishing   |
| Endpoint Security   | Privacy   |
| Anti-Ransomware   |   |
| -Summary Top 10<br>Machine Infected<br>Application Allowed by Computer<br>Website Blocked by Computer<br>Application Blocked by App Name<br>Website Blocked by Sites<br>Website Blocked by Username<br>Infected Emails<br>Virus Blocked | <ul> <li>USB Blocked</li> <li>Application Blocked by Computer</li> <li>Website Allowed by Computer</li> <li>Application Allowed by App Name</li> <li>Website Allowed by Sites</li> <li>Website Allowed by Username</li> <li>Spam Emails</li> <li>Exploit Blocked</li> </ul> |
| -Live Status  |   |

2. Select the parameters' checkboxes to be displayed in the respective tabs.

#### 3. Click **OK**.

The tabs will be updated according to the changes.





# Managed Computers

To secure, manage and monitor computers, it is necessary to add them in a group. The **Managed Computers** module lets you create computer groups, add computers to a group, define policy templates for the created groups and computers, create policy criteria templates and tasks for specific groups.

Based on the departments, user roles and designations, you can create multiple groups and assign them different policies. This lets you secure and manage computers in a better way.

In the navigation panel, click **Managed Computers**. The Managed Computers screen appears on the right pane.

| Managed Computers                  |  |                | 💲 Refresh 🛛 👔 Help |
|------------------------------------|--|----------------|--------------------|
| P Search Supdate Agent             |  |                |                    |
| Action List 🔻 🚺 Client Action List | Policy Templates     Policy Criteria Templates |                | QR Code for 2FA    |
| 🖻 🥃 Managed Computers              | Name   |                |                    |
| 🔝 Policy                           | Policy   |                |                    |
| - 🔯 Group Tasks                    | Group Tasks                                    |                |                    |
| 😏 Client Computers (1)             | 🗊 Client Computers                             |                |                    |
| 🗄 🧫 Roaming Users                  | Group Information                              |                |                    |
| 🖻 🧮 sample                         | AD Sync  | Not Configured |                    |
| Policy                             | Total Subgroups                                | 2              |                    |
| Group Tasks                        | Total Computers                                | 1              |                    |
|                                    |  |                |                    |
|                                    |  |                |                    |
|                                    |  |                |                    |

The screen consists of following buttons:

- Search
- Update Agent
- Action List
- Client Action List
- Policy Templates
- Policy Criteria Templates





# Search

To search for specific computers, click **Search.** Search for Computers window appears. This is helpful for finding any computer added in Managed Computers.

| Filter Computer Name / IP: User's name: Find Now  | Search for Computers |                    |                        |                   |                     |                |                  | ĺ               | 👔 Helj    |
|---|----------------------|--------------------|------------------------|-------------------|---------------------|----------------|------------------|-----------------|-----------|
| Computer Name / IP:<br>User's name:<br>Find Now   | Filter               |                    |                        |                   |                     |                |                  |                 |           |
| Find Now  | Computer Name / IP:  |                    |                        |                   |                     |                |                  |                 |           |
|   | User a name.         | Find Now           |                        |                   |                     |                |                  |                 |           |
|   |                      |                    |                        |                   |                     |                |                  |                 |           |
| Client Action List -  | Client Action List 👻 |                    |                        |                   |                     |                |                  |                 |           |
| Computer Name Groups IP Address User name eScan Status Version Last Connection Installed Directory Monitor Status Anti-Spam Mail Anti-Virus Web | Computer Name Groups | IP Address User na | me eScan Status Versio | n Last Connection | Installed Directory | Monitor Status | <u>Anti-Spam</u> | Mail Anti-Virus | Web F     |
| There are no items to show in this  |                      |                    |                        |                   |                     |                | There are no     | o items to show | in this v |

The Filter section displays following fields:

#### Computer Name/IP

Enter a computer name or IP address.

#### Username

Enter a username.

#### Click Find Now.

The console will display the result.

# Update Agent

eScan lets you use a client computer as an update agent to deploy updates on groups of computers.

By default, eScan server distributes the virus definitions and policies to all the clients added in the web console. But, if you want to reduce server's workload, you can create an Update Agent for the respective group(s). The Update Agent will receive virus definitions and policies from server and distribute it to the assigned group(s). For more details, please see <u>eScan Update Agents</u>.

In Managed Computers screen, clicking **Update Agent** displays a list of computers that are acting as Update Agents for other computers in the group. The window also lets you **Add** or **Remove** Update Agents from this list. You can set an Update Agent for multiple groups.





# Adding an Update Agent

To add an Update Agent, follow the steps given below:

1. In Managed computers screen, click **Update Agent**. **Update Agent** window appears.

|                                    |            |                      | ×      |
|------------------------------------|------------|----------------------|--------|
| Update Agent                       |            |                      | 🝸 Help |
| Select Group Name and Update Agent |            |                      |        |
| Update Agent:                      |            |                      |        |
| Group Name:                        |            |                      |        |
|                                    |            | Add                  |        |
|                                    |            |                      |        |
| Update Agent                       | IP Address | Assigned to Group(s) |        |
|                                    |            |                      |        |

2. Click market to Update Agent field, to select the computer. Select Computer widow appears.

|                           |                       |                    | ×      |
|---------------------------|-----------------------|--------------------|--------|
| Select Computer           |                       |                    | 👔 Help |
| Anaged Computer           | 2                     |                    |        |
|                           |                       | Ok                 | Cancel |
| * Note: Update Agent cann | ot be set if Hostname | exceed 15 characte | rs.    |

- 3. Select a computer and click **OK.**
- 4. Click \_\_\_\_\_ next to Group Name field, to select the Group Name. This is the group to which the selected computer will act as an Update Agent and provide updates.
- 5. Select the Group and click **OK.**
- 6. Click **Add.** The Update Agent will be added for the selected group.





# **Deleting an Update Agent**

To delete an Update Agent, follow the steps given below:

1. In Managed computers screen, click **Update Agent**. Update Agent window appears.

| Update Agent                       |            |                                |  |  |  |  |
|------------------------------------|------------|--------------------------------|--|--|--|--|
| Select Group Name and Update Agent |            |                                |  |  |  |  |
| Update Agent:<br>Group Name:       |            | <br>Add                        |  |  |  |  |
|                                    |            |                                |  |  |  |  |
| Update Agent                       | IP Address | Assigned to Group(s)           |  |  |  |  |
| 1000                               | 10.10.01   | Managed Computers\Sample Group |  |  |  |  |
|                                    |            |                                |  |  |  |  |

2. In the Assigned to Group(s) column, click  $\widehat{\mathbf{m}}$ . A confirmation prompt appears.



3. Click **OK**. The Update Agent will be deleted.





# Action List

The Action List takes you action for a group. The drop-down contains following options:

- New Subgroup
- Set group Configuration
- Deploy/Upgrade Client
- Uninstall eScan Client
- Remove Group
- Synchronize with Active Directory
- Outbreak Prevention
- Create Client Setup
- Properties

### Creating a Group

To create a group, follow the steps given below:

 Click Action List > New Subgroup. Creating New Group window appears.

|                    |                      | ×      |
|--------------------|----------------------|--------|
| Creating New Group |                      | 🝸 Help |
| Create New Group   |                      |        |
| New Group Name :   |                      | ]      |
| Group Type :       | Normal User 🔻        | ]      |
| Policy Templates : | Group Default Policy | ]      |
| Ok Cancel          |                      |        |
|                    |                      |        |

- 2. Enter a name for the group.
- 3. Click the Group Type drop-down and select a type.
- 4. Click the Policy Templates drop-down and select a policy for the group.
- 5. Click **OK**.

A new group will be created under the Managed Computers.

|      | If the Group type is set to <b>Normal User</b> , then server will try to connect to the  |
|------|--|
|      | client computer using the hostname.  |
| NOTE | If the Group type is set to <b>Roaming User</b> , then server will try to connect to the |
|      | client computer using the IP address.  |
|      | Multiple groups can be created within a group.   |





# Removing a Group

To remove a group, follow the steps given below:

- 1. Select a group.
- 2. Click **Action List** > **Remove Subgroup**. A confirmation prompt appears.

| ×   |
|---|
| Remove Group  |
| Do you really want to remove the group "Sample Group" ? |
| Ok Cancel   |

3. Click **OK**. The group will be removed.

| NOTE | A group will be removed only if it contains no computers. |
|------|---|
|------|---|

# Set Group Configuration

With this option you can define single Username and Password to login for all the computers in the group.

To set a group configuration, follow the steps given below:

- 1. Select the group you want to configure.
- 2. Click **Action List** > **Set Group Configuration**. Set Group Configuration window appears.

| ogin Informati  | on                      |                   |                  |                |
|-----------------|-------------------------|-------------------|------------------|----------------|
| roup Name:      | Managed Computers       |                   |                  |                |
| emarks:         |                         |                   |                  |                |
| ser name:       | Administrator           |                   |                  |                |
| assword:        |                         |                   |                  |                |
|                 |                         |                   |                  |                |
| ote: If Host Na | me is in another Domain | Please mention Do | main Name Ex. Do | main1\HostName |

- 3. Enter Remarks and define Login credentials.
- 4. Click **Save**. The group configuration will be saved.





# Managing Installations

After grouping all computers in logical groups using eScan Management Console, you can now install eScan Client as well as other third party software on the computers connected to your network. [Conditions Apply]

This section will give you an overview on following activities:

#### Installing eScan Client

eScan client can be installed on computers connected to the network in the following ways:

- **Remote Installation**: It lets you install eScan Client on all the computers in a selected group at once. You can initiate and monitor eScan Client installation using eScan Management Console. For more click here.
- **Manual Installation**: In case remote installation fails, you can allow computer users to install eScan client manually on their computers. It does not require any remote assistance. For more click here.
- **Installing eScan using agent**: Installation of agent ensures that you have Administrator rights on the computer and you can now remotely install eScan Client on that computer. For more click here.
- Installing other Software (3<sup>rd</sup> Party software): eScan Management Console lets you install third party software on network computers remotely. <u>For more click</u> <u>here</u>.

|      | Conditions for third party software installation:   |
|------|---|
| NOTE | After starting the installation from eScan Management Console, no manual intervention should be required to complete the installation on Client computer. Only automated installations can be done through eScan Management Console.<br>Care should be taken that the installation file is not huge as it may impact internal network speed of your organization. |





### **Remote Installation of eScan Client**

#### **Pre-Installation**

To prepare a client computer for the remote deployment of eScan TSS for Business; begin with checking if the basic system requirements are in place.

Configure the settings on the client computer according to the OS installed on it

- Windows XP Professional systems
- Windows XP Home
- Windows Vista /Windows 7 /Windows 8 / Windows 8.1 / Windows 10

Configuring the settings on Windows XP Professional systems (Windows XP, 2000, 2003, all editions)

- 1. Click **Start** > **Control Panel**.
- 2. Double-click the **Administrative Tools** icon.
- 3. Double-click the **LocalSecurityPolicy** icon.
- 4. On the navigation pane, click **Local Policies** folder, and then click **Security Options** folder.
- 5. Double-click Network Access: Sharing and Security Model for Local accounts policy.
- 6. Select Classic Local user authenticate as themselves option from the drop-down list.
- 7. Click **Apply**, and then click **OK**.
- 8. Double-click the **Accounts**: **Limit local account use of blank passwords to console logon only policy**. The Accounts: Limit local account use of blank passwords to console logon only dialog box appears.
- 9. Click **Disabled** option.
- 10. Click **Apply**, and then click **OK**.

If Windows firewall is enabled on all locations, select **File and Printer Sharing** checkbox, under **Exceptions** tab (**Control Panel >> Windows Firewall >> Exception**). **For Windows XP Home** 

Since Windows XP Home has limitations with regards to remote deployment, MWAgent should be installed on your system. You can download MWAgent from the eScan web console.





# For Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10

- 1. Launch Run.
- 2. Enter **secpol.msc**, and then click **OK**. Local Security Settings window appears.
- 3. On the navigation pane, click **Local Policies** folder, and then double-click **Security Options** folder. The security policy appears.
- 4. Double-click **Network access: Sharing and security model for local accounts** policy.
- 5. Select Classic Local users authenticate as themselves option present in the dropdown.
- 6. Click **Apply** > **OK**.
- 7. Double-click Accounts: Limit local account use of blank passwords to console logon only policy.
- 8. Select **Disabled** option.
- 9. Click **Apply** > **OK**.
- 10. If the firewall is enabled, select **File and Printer Sharing** checkbox, under **Exceptions** tab.
- 11. On desktop, click **Start**, and right-click **My Computer**, click **Manage**. Computer Management window appears.
- On the navigation pane, click Local Users and Groups option, and then click Users folder, and double-click Administrator. Administrator Properties window appears.
- 13. Check Password never expires and uncheck Account is disabled checkbox.
- 14. Click **Apply** > **OK**.





# Deploy/Upgrade Client

To Deploy/Upgrade eScan client on all computers in a group or an individual computer, follow the steps given below:

### **Installing eScan Client on a Group**

- 1. Select the group on which you want to install eScan client.
- Click Action List > Deploy/Upgrade Client. Client Installation window appears.

| nt Installation  |            |     |   | <br>M nei |
|--|------------|-----|---|-----------|
| lect Application for Installation:                                   |            |     |   |           |
| Install eScan  |            |     |   |           |
| Select eScan Installation Options:                                   |            |     |   |           |
| Auto Reboot after Install  |            |     |   |           |
| Install Without Firewall   |            |     |   |           |
| Disable auto downloading of Windows patches                          | by eScan   |     |   |           |
| Installation Path  |            |     |   |           |
| <default></default>  | <b>~</b> [ | Add |   |           |
| Install Other Software   |            |     |   |           |
| Required files for Installation                                      |            |     |   |           |
| C:\PROGRA~2\eScan\Setup\Launchit.Exe,C:\PRO<br>eScan\Setup\Setup.exe | GRA~2\     | Add | J |           |
| Executable file  |            |     |   |           |
|  | $\sim$     |     |   |           |
| Parameters   |            |     |   |           |
| /Setupfile=Setup.exe   |            |     |   |           |
| Install Agent  |            |     |   |           |
| Install local client setup   |            |     |   |           |
| Required files for Installation                                      |            |     |   |           |
|  | (          | Add | ] |           |
| Executable file  |            |     |   |           |

3. Select Install eScan option.

By Default eScan is installed at the following Path on a Client computer. C:\Program Files\eScan (default path for 32-bit computer) OR

C:\Program Files (x86)\eScan (default path for 64-bit computers).

- 4. To define a different installation path, click **Add**. (Skip this step if default path chosen).
- 5. Click **Install**. A window displays File transfer progress. After Installation, the eScan status will be updated in Managed Computers list.





# **Refresh Client**

To refresh status of any client computer, follow the steps given below:

- 1. Under any group, click **Client Computers**. A list of computers appears on the right pane.
- 2. Select a computer.
- 3. Click **Refresh Client**. The Client will be refreshed.

### **Understanding the eScan Client Protection Status**

| Protected                  | This status is displayed when the File anti-virus module of eScan Client is enabled and eScan was updated in last 2 days.      |
|----------------------------|--|
| 📕 Not Installed / Critical | This status is displayed when either eScan is not installed<br>on any computer or File AV/Real Time Protection is<br>disabled. |
| 💻 Unknown status           | This status is displayed when communication is broken between Server and Client due to unknown reason.                         |
| 🤅 Update Agent             | This status is displayed when a computer is defined as an Update Agent for the group.  |
| RMM Enabled                | This status is displayed when a computer is added to<br>RMM license and the computer can be connected via RMM<br>service.      |
| Two-FA Enabled             | This status is displayed when a computer is added to 2FA license.  |





# Manual installation of eScan Client on network computers

If remote installation is not possible, you may manually install the eScan Management Console.

To install manually, the download links for manually installation of the **eScan Client** or **Agent** are displayed on the **Login Page** of eScan Management Console. Forward this link to the user of the Client computer on mail and guide the user through the installation process.

| Please type your            | User name and Password to access the Web Console. |      |
|-----------------------------|---|------|
| Username:*                  | For Active Directory account:<br>domain\username  |      |
| Password:*                  |   | ogin |
| You can provide u           | sers the following link(s):                       |      |
| eScan Client Set<br>http:// | up (Windows)<br>/Setup/eScan_Client.exe           | [+]  |
| eScan Agent Set             | up (Windows)                                      |      |





# Installing eScan Client Using Agent

You may install the eScan Client using an Agent in following ways:

- Remotely installing agent on Client computer(s)
- Manually installing agent on Client computer(s)

### **Remotely installing agent on Client computer(s)**

- 1. Click Managed Computers.
- 2. Select the computer(s) from a group.
- 3. Click Client Action List > Deploy/Upgrade Client.
- 4. Select **Install Agent** option and click **Install**. eScan Agent will be installed on selected computers.

|      | This option useful in case there are glitches in the network connectivity between   |
|------|---|
| NOTE | server and Client computer. It will overcome those glitches and speed up the client |
|      | installation on the selected computers.   |

### **Manually installing eScan Agent on Client computer(s)**

To manually install eScan Agent on computers, please send the link displayed on the **Login Page** of eScan Management Console to the users of the Client computer on mail.

| WEB CONSOLE LOGIN  |  |  |  |  |
|--|--|--|--|--|
| Please type your User name and Password to access the Web Console.               |  |  |  |  |
| Username:*   | For Active Directory account:<br>domain\username |  |  |  |
| Password:*   | Login  |  |  |  |
| You can provide users the  | e following link(s):                             |  |  |  |
| eScan Client Setup (Windows)<br>http:// /Setup/eScan Client.exe [+]              |  |  |  |  |
| eScan Agent Setup (Windows)<br>http:// /Setup/Agent Setup.exe<br>eScan AV Report |  |  |  |  |

Copyright © MicroWorld Technologies Inc. All rights reserved.





# Installing other Software (Third Party Software)

To install third party software on computers, follow the steps given below:

- 1. Click Managed Computers.
- 2. Select a computer from a group.
- 3. Click **Client Action List** > **Deploy/Upgrade Client**. Client Installation window appears.
- 4. Select Install Other Software option.

| Select eScan Installation Options:  |                     |   |
|---|---------------------|---|
| Auto Reboot after Install   |                     |   |
| Install Without Firewall  |                     |   |
| Disable auto downloading of Window  | rs patches by eScan |   |
| Installation Path   |                     |   |
|   | Add                 |   |
| Install Other Software  |                     |   |
| Required files for Installation   |                     |   |
|   |                     |   |
|   | Add                 |   |
| Executable file   |                     |   |
|   | Edit Script         |   |
|   |                     | I |
| Parameters  |                     |   |
| Parameters  Install Agent Install local client setup Required files for Installation                              |                     |   |
| Parameters DInstall Agent Install local client setup Required files for Installation                              |                     |   |
| Parameters DInstall Agent DInstall local client setup Required files for Installation                             | Add                 |   |
| Parameters  Install Agent Install local client setup Required files for Installation Executable file              | Add                 |   |
| Parameters  Install Agent Install local client setup Required files for Installation Executable file              | Add                 |   |
| Parameters  Install Agent Install local client setup Required files for Installation  Executable file Parameters  | Add                 |   |
| Parameters  Install Agent Install local client setup Required files for Installation  Executable file  Parameters | Add                 |   |

#### 5. Click Add.

Add Files window appears.

| 😵 eScan Management Console - Google Chrome |        | x |
|--|--------|---|
| Not secure                                 | ?FOR=I | Q |
| Add Files                                  |        |   |
|  |        |   |
| Add Cancel                                 |        |   |
|  |        |   |
|  |        |   |
|  |        |   |
| 4  |        | • |





6. Enter the exact path of the EXE (on eScan Server) and click **Add**. The selected **EXE** will be added to the "Required files for Installation" list.

| Install Other Software             |             |
|------------------------------------|-------------|
| Required files for Installation    |             |
| C:\Users\QA\Downloads\twn4ksmk.exe | Add         |
| Executable file                    |             |
| twn4ksmk.exe 🗸 🗸                   | Edit Script |
| Parameters                         |             |
| [                                  | 1           |
| с                                  | ,           |

- 7. The Executable Filename will be displayed in the respective drop-down menu.
- 8. Define the command line parameters if required.
- 9. Click **Install** to initiate the installation process. A confirmation message appears.

| Client Ins | lient Installation                     |   |  |  |  |
|------------|--|---|--|--|--|
| 5/3/       | 11:09:02 AM : [                        | ]: Connecting to Computer                                 |  |  |  |
| 5/3/       | 11:09:02 AM : [                        | ]: Deploying other software files to host DANNY. Pls Wait |  |  |  |
| 5/3/       | 11:09:02 AM : [                        | ]: Copying file 1 of 1                                    |  |  |  |
| 5/3/       | 11:09:03 AM : [                        | j: Completed 100 %  |  |  |  |
| 5/3/       | ====================================== |   |  |  |  |
|            |  |   |  |  |  |
| Close      | Cancel                                 |   |  |  |  |





# Uninstall eScan Client

To uninstall eScan Client on all the computer from a group, follow the steps given below:

- 1. Select the group of computers for uninstallation.
- 2. Click **Action List** > **Uninstall eScan Client**. Client Uninstallation window appears.

| Client Uninstallation  |
|--|
| Ready to Start Uninstallation<br>Click "Uninstall" to Start Uninstallation |
| Uninstall Cancel   |

#### 3. Click Uninstall.

The Client Uninstallation window displays the progress.

| /26/2019 4:47:37 PM : [       ]: Reading Host Details         /26/2019 4:47:37 PM : [       ]: Version 14.0.1400.2220         /26/2019 4:47:37 PM : [       ]: Service Pack 2220         /26/2019 4:47:37 PM : [       ]: Task 'Uninstall eScan on Host(s)' successfully scheduled on |
|---|
| /26/2019 4:47:37 PM : [ ]: Version 14.0.1400.2220<br>/26/2019 4:47:37 PM : [ ]: Service Pack 2220<br>/26/2019 4:47:37 PM : [ ]: Task 'Uninstall eScan on Host(s)' successfully scheduled on   |
| /26/2019 4:47:37 PM : [ ]: Service Pack 2220<br>/26/2019 4:47:37 PM : [ ]: Task 'Uninstall eScan on Host(s)' successfully scheduled on  |
| /26/2019 4:47:37 PM : [ ]: Task 'Uninstall eScan on Host(s)' successfully scheduled on  |
|   |
|   |

After the uninstallation process is over, click **Close**.





# Synchronize with Active Directory

To synchronize a group with Active Directory, follow the steps given below:

- 1. In the Managed Computers folder tree, select a group for synchronization.
  - Click Action List > Synchronize with Active Directory. Synchronize with Active Directory window appears.

| Active Directory  Target Groups :  Managed Computers\Sample Group  Source Active Directory Organisation Unit :  Synchronization interval :  Synchronization interval :  Exclude From ADS Sync  Exclude From ADS Sync  Exclude ADS Sources  Add to Exclude  Delete  Pelete  Install eScan client automatically  Select eScan Installation Options:  Install without Firevall  Daync will not add the computers that are already present in any of the groups under Managed computers.Check  Sunce ADS Sync.  Sunce Install Without Firevall  Daync will not add the computers that are already present in any of the groups under Managed computers.Check  Computers.Check |   |                    |
|---|---|--------------------|
| Target Groups :         Managed Computers/Sample Group         Source Active Directory Organisation Unit :         Browse         Synchronization interval :         60       Minutes (Minimum 5 Minutes)         Exclude From ADS Sync         Exclude ADS Sources         Add to Exclude         Delete   | ynchronize with Active Directory  |                    |
| Target Groups :         Managed Computers'Sample Group         Source Active Directory Organisation Unit :         Browse         Synchronization interval :         60       Minutes (Minimum 5 Minutes)         Exclude From ADS Sync         Exclude ADS Sources         Add to Exclude         Delete   |   |                    |
| I arget Groups :         Managed Computers/Sample Group         Source Active Directory Organisation Unit :         Source Active Directory Organisation Unit :         Browse         Synchronization interval :         60       Minutes (Minimum 5 Minutes)         Exclude From ADS Sync         Exclude ADS Sources         Add to Exclude         Delete         Search Filter :         e.g.: (objectClass=*)         Install eScan client automatically         Select eScan Installation Options:         Install Without Firewall   |   |                    |
| Managed Computers/Sample Group       Browse         Source Active Directory Organisation Unit :       Browse         Synchronization interval :       Browse         60       Minutes (Minimum 5 Minutes)         Exclude From ADS Sync       Add to Exclude         Exclude ADS Sources       Add to Exclude         0       Browse         Search Filter :       e.g.: (objectClass=*)         0       Install eScan client automatically         Select eScan Installation Options:       Install Without Firewall         D sync will not add the computers that are already present in any of the groups under Managed computers.Check                               | Target Groups :   |                    |
| Surce Active Directory Organisation Unit :<br>Browse  Synchronization interval :<br>60 Minutes (Minimum 5 Minutes)  Exclude From ADS Sync  Exclude ADS Sources Add to Exclude Delete Delete   | Managed Computers\Sample Group  | Browse             |
| Source Active Directory Organisation Unit :  Source Active Directory Organisation Unit :  Synchronization interval :  Synchronization interval :  Succession ADS Sync  Exclude From ADS Sync  Exclude ADS Sources  Add to Exclude  Delete   Search Filter :  e.g.: (objectClass=*)  Install eScan client automatically  Select eScan Installation Options:  Install Without Firevall  D sync will not add the computers that are already present in any of the groups under Managed computers.Check  CanNogADSaync.log <sup>*</sup> for more details.   |   |                    |
| Synchronization interval :       Browse         60       Minutes (Minimum 5 Minutes)         Exclude From ADS Sync       Add to Exclude         Exclude ADS Sources       Add to Exclude         e.g.: (objectClass=*)       Delete         Install eScan client automatically       Select eScan Installation Options:         Install Without Firewall       Dayne will not add the computers that are already present in any of the groups under Managed computers.Check ican\U004ADSayne.log' for more details.   | - Source Active Directory Organisation Unit -   |                    |
| Synchronization interval :         60       Minutes (Minimum 5 Minutes)         Exclude From ADS Sync         Excluded ADS Sources         Add to Exclude         Delete         Search Filter :         e.g.: (objectClass=*)         Install eScan client automatically         Select eScan Installation Options:         Install Without Firewall   | Source Active Directory organisation onic .   |                    |
| Synchronization interval :<br>60 Minutes (Minimum 5 Minutes)<br>Exclude From ADS Sync<br>Exclude ADS Sources<br>Add to Exclude<br>Delete<br>Search Filter :<br>e.g.: (objectClass=*)<br>Install eScan client automatically<br>Select eScan Installation Options:<br>Install Without Firewall<br>D sync will not add the computers that are already present in any of the groups under Managed computers.Check<br>icanlog/ADSsync.log <sup>*</sup> for more details.   |   | Browse             |
| Synchronization interval :<br>60 Minutes (Minimum 5 Minutes)<br>Exclude From ADS Sync-<br>Exclude ADS Sources<br>Add to Exclude<br>Delete<br>Delete<br>Search Filter :<br>e.g.: (objectClass=*)<br>Install eScan client automatically<br>Select eScan Installation Options:<br>Install Without Firewall<br>D sync will not add the computers that are already present in any of the groups under Managed computers.Check<br>IcanVog/ADSsync.log" for more details.  |   |                    |
| 50       Minutes (Minimum 5 Minutes)         Exclude From ADS Sync       Add to Exclude         Excluded ADS Sources       Add to Exclude         Delete       Delete         Search Filter :   | Synchronization interval :  |                    |
| 60       Minutes (Minimum 5 Minutes)         Exclude From ADS Sync       Add to Exclude         Exclude ADS Sources       Add to Exclude         Delete       Delete         Search Filter :       e.g.: (objectClass=*)         Install eScan client automatically       Select eScan Installation Options:         Install Without Firewall       D sync will not add the computers that are already present in any of the groups under Managed computers.Check ican\log\ADSsync.log" for more details.   |   |                    |
| Exclude From ADS Sync<br>Exclude ADS Sources Add to Exclude Delete Delete   | 60 Minutes (Minimum 5 Minutes)  |                    |
| Exclude From ADS Sync<br>Exclude ADS Sources<br>Add to Exclude<br>Delete<br>Delete<br>Close<br>Search Filter :<br>e.g.: (objectClass=*)<br>Install eScan client automatically<br>Select eScan Installation Options:<br>Install Without Firewall<br>D sync will not add the computers that are already present in any of the groups under Managed computers.Check<br>ican\og\ADSsync.log" for more details.  |   |                    |
| Excluded ADS Sources     Add to Exclude     Delete      eete      eete      Search Filter :     ee.g.: (objectClass=*)      Install eScan client automatically      Select eScan Installation Options:     Install Without Firewall      D sync will not add the computers that are already present in any of the groups under Managed computers.Check     ican\log\ADSsync.log" for more details.     Chece  | Exclude From ADS Sync   |                    |
| Add to Exclude     Add to Exclude     Delete      Add to Exclude     Delete      Search Filter :     e.g.: (objectClass=*)      Install eScan client automatically      Select eScan Installation Options:     Install Without Firewall      D sync will not add the computers that are already present in any of the groups under Managed computers.Check     ican\log\ADSync.log" for more details.     Chece   | Evoluded ADS Sources  |                    |
| Search Filter :   |   | Add to Exclude     |
| Search Filter :  e.g.: (objectClass=*)  Install eScan client automatically  Select eScan Installation Options:  Install Without Firewall  D sync will not add the computers that are already present in any of the groups under Managed computers.Check :can\log\ADSsync.log" for more details.  Close  |   |                    |
| Search Filter :         e.g.: (objectClass=*)         Install eScan client automatically         Select eScan Installation Options:         Install Without Firewall         D sync will not add the computers that are already present in any of the groups under Managed computers.Check ican\log\ADSsync.log" for more details.         Close  |   | Delete             |
| Search Filter :<br>e.g.: (objectClass=*)<br>Install eScan client automatically<br>Select eScan Installation Options:<br>Install Without Firewall<br>D sync will not add the computers that are already present in any of the groups under Managed computers.Check<br>ican\log\ADSsync.log" for more details.  |   |                    |
| Search Filter :<br>e.g.: (objectClass=*)<br>Install eScan client automatically<br>Select eScan Installation Options:<br>Install Without Firewall<br>D sync will not add the computers that are already present in any of the groups under Managed computers.Check<br>ican\log\ADSsync.log" for more details.  |   |                    |
| Search Filter :<br>e.g.: (objectClass=*)<br>Install eScan client automatically<br>Select eScan Installation Options:<br>Install Without Firewall<br>D sync will not add the computers that are already present in any of the groups under Managed computers.Check<br>ican\log\ADSsync.log" for more details.  |   |                    |
| Search Filter :         e.g.: (objectClass=*)         Install eScan client automatically         Select eScan Installation Options:         Install Without Firewall         D sync will not add the computers that are already present in any of the groups under Managed computers.Check         ican\log\ADSsync.log" for more details.         Checa  |   |                    |
| e.g.: (objectClass=*)  Install eScan client automatically Select eScan Installation Options: Install Without Firewall  D sync will not add the computers that are already present in any of the groups under Managed computers.Check ican\log\ADSsync.log" for more details. Chece  |   |                    |
| e.g.: (objectClass=") Install eScan client automatically Select eScan Installation Options: Install Without Firewall D sync will not add the computers that are already present in any of the groups under Managed computers.Check ican\log\ADSsync.log" for more details. Checa  |   |                    |
| Install eScan client automatically Select eScan Installation Options: Install Without Firewall  D sync will not add the computers that are already present in any of the groups under Managed computers.Check ican\log\ADSsync.log" for more details. Checa   | e.g.: (objectClass=*)   |                    |
| Install eScan client automatically Select eScan Installation Options: Install Without Firewall  D sync will not add the computers that are already present in any of the groups under Managed computers.Check ican\log\ADSsync.log" for more details. Checa   |   |                    |
| Install eScan client automatically Select eScan Installation Options: Install Without Firewall  D sync will not add the computers that are already present in any of the groups under Managed computers.Check ican\log\ADSsync.log" for more details. Checa   |   |                    |
| Select eScan Installation Options: Install Without Firewall  D sync will not add the computers that are already present in any of the groups under Managed computers.Check ican\log\ADSsync.log" for more details.  Checa   | Tastall aSana diaat subaratically   |                    |
| Select eScan Installation Options:<br>Install Without Firewall<br>D sync will not add the computers that are already present in any of the groups under Managed computers.Check<br>ican\log\ADSsync.log" for more details.  |   |                    |
| Install Without Firewall D sync will not add the computers that are already present in any of the groups under Managed computers.Check ican\log\ADSsync.log" for more details.  | Select eScan Installation Options:  |                    |
| D sync will not add the computers that are already present in any of the groups under Managed computers.Check<br>ican\log\ADSsync.log" for more details.  |   |                    |
| D sync will not add the computers that are already present in any of the groups under Managed computers.Check<br>Scan\log\ADSsync.log" for more details.  | Install without Firewall  |                    |
| D sync will not add the computers that are already present in any of the groups under Managed computers.Check<br>Scan\log\ADSsync.log" for more details.  |   |                    |
| D sync will not add the computers that are already present in any of the groups under Managed computers.Check<br>ican\log\ADSsync.log" for more details.  |   |                    |
| k Close   | .D sync will not add the computers that are already present in any of the groups under Manag<br>Scan\log\ADSsync.log" for more details. | ed computers.Check |
|   | L Close   |                    |

#### Source Active Directory Organization Unit

Click **Browse** and select an Active Directory.

#### Synchronization Interval

Enter the preferred duration (in minutes).

#### **Exclude from ADS Sync**

This field displays a list of excluded Active Directory sources.

To delete a source, select the checkbox Excluded ADS Sources. Select a source(s) and then click **Delete**.

To exclude a source, select the source and then click **Add to Exclude**.





#### **Search Filter**

It lets you search an Active Directory for an object class.

#### Install eScan manually

Selecting this option lets you install eScan manually on the computers.

#### **Install without Firewall**

Selecting this option lets you install eScan without firewall.

3. After performing the necessary actions, click **OK**. The group will be synchronized with the Active Directory.

### **Outbreak Prevention**

Upon virus detection, eScan quarantines the virus and restricts it from spreading across the network. The Outbreak Prevention feature lets you configure policies for the network.

### **Deploying Outbreak Prevention**

To deploy Outbreak Prevention feature, follow the steps given below:

- 1. In the Managed Computers folder tree, select a group.
- 2. Click Action List > Outbreak Prevention.

Outbreak Prevention window appears.

| bepioy ou   |   | Restore outpre      |                    |        |       |
|---|---|---------------------|--------------------|--------|-------|
| utbreak Pre   | ention Policies   |                     |                    |        |       |
| Limit acce  | ess to shared folders (Allow  | v read access only) |                    |        |       |
| Deny writ   | e access to local files and   | folder              |                    |        |       |
| Block Spe   | cific Ports   |                     |                    |        |       |
| Block All   | Ports (Other than trusted (   | lient-server ports) |                    |        |       |
| Automaticall  | y restore outbreak prev   | ention after 1      | hours(s)           |        |       |
|   |   | an cause mator prob | lems with the comp | uters. |       |
| configuration   | vention Notification  |                     |                    |        |       |
| configuration   | vention Notification  |                     |                    |        |       |
| configuration<br>Outbreak Prev<br>Notify clie             | or these policies settings c<br>vention Notification<br>nt users when outbreak p  | revention starts    |                    |        |       |
| configuration<br>Outbreak Prev<br>Notify clie<br>Message: | or these policies settings c<br>rention Notification<br>int users when outbreak p | revention starts    |                    |        | 207/2 |

#### Limit access to shared folders

Select this checkbox to limit the infection's access to shared folders.

#### Deny write access to local files and folder

Select this checkbox to deny the infection write access for any file. Clicking the link displays another window that lets you specifically select folders and subfolders that should be denied and allowed access for modification.





#### **Block specific ports**

Select this checkbox to prevent infection from accessing specific ports. Clicking the link displays another window that lets you block incoming and outgoing data packets along with TCP and UDP ports.

#### Block All Ports (Other than trusted client-server ports)

Select this checkbox to block all ports other than trusted client server ports.

#### Automatically restore the outbreak prevention after hour(s)

This feature lets you restore outbreak prevention automatically after set duration (hours). Click the drop-down and select the preferred duration.

#### **Outbreak Prevention Notification**

To send a notification to client users after Outbreak Prevention is deployed, select the checkbox **Notify client users when outbreak prevention starts**. You can even write your own custom message for this feature in the Message field.

After making the necessary selections, click **Deploy**. The Outbreak Prevention feature will be deployed for the selected group.

### **Restore Outbreak Prevention**

In the Outbreak Prevention window, click **Restore Outbreak Prevention** tab.

| Itbreak Prevention              |   | Т      |
|---------------------------------|---|--------|
| Deploy Outbreak Prevention      | Restore Outbreak Prevention                                       |        |
| Restore Outbreak Prevention     |   |        |
| Notify client users after resto | ring the original settings  |        |
| Message:                        |   | 96/250 |
| eScan has stopped enforcing out | break prevention policies and has restored pre-outbreak settings. |        |
|                                 |   |        |
|                                 |   | ,      |
|                                 |   | //     |
|                                 |   |        |

To restore Outbreak Prevention manually, click **Restore**.

To notify clients about Outbreak Prevention restoration, select the checkbox **Notify client users after the original settings**.





# Create Client Setup

To create a Client setup, follow the steps given below:

- 1. In the Managed Computers folder tree, select a group.
- 2. Click **Action List** > **Create Client Setup**. Create Client Setup window appears.

| Create Client Setup | elp |
|---------------------|-----|
|                     |     |
| Setup Settings      |     |
| Add Policy          |     |
| Auto add to group   |     |
| Create Setup Cancel |     |

- 3. Select the necessary settings.
  - Add Policy: This option will let you add policy to the client setup.
  - **Auto add to group**: This option will add the endpoint(s) to the respective group automatically after endpoint installation.
- 4. Click **Create Setup**. The Client setup will be created and a download link will be displayed in right pane.

| Name               | Download Client Setup |                |
|--------------------|-----------------------|----------------|
| 🔃 Policy           |                       |                |
| 🔞 Group Tasks      |                       |                |
| 🗊 Client Computers |                       |                |
| Group Information  |                       |                |
| AD Sync            |                       | Not Configured |
| Total Subgroups    |                       | 1              |
| Total Computers    |                       | 3              |





# Properties of a group

To view the properties of a group, follow the steps given below:

- 1. Select a group.
- 2. Click Action List > Properties.

Properties window appears.

|   |                     |                        | × |
|---|---------------------|------------------------|---|
| 1 | Properties (sample) | 🝸 Help                 | ٠ |
|   | General             |                        |   |
|   | Name :              | sample                 |   |
|   | Parent Group :      | Managed Computers      |   |
|   | Group Type :        | Normal User 🗸          |   |
|   | Contains :          | 0 Groups , 0 Computers |   |
|   | Created :           | 28/05/20 5:59:37 PM    |   |
|   |                     |                        |   |

In Properties, General tab displays following details:

- Group Name
- Parent Group
- Group Type Normal or Roaming User
- Sub Groups or Number of Computers in that Group
- Creation date of the Group





# Group Tasks

With the **Group Tasks** option, you can create a task, start a task, select a task and view its properties, view task results as well as delete an already created task. Tasks can include the following.

- Enable/Disable desired Module
- Set Update Server
- Scheduling Scan on Networked Computers

# Creating a Group Task

To create a Group Task, follow the steps given below:

- 1. Select a group.
- 2. In group's folder tree, click **Group Tasks**.
- 3. In the Group Tasks pane, click **New Task**.

| Action List  Client Action List |   |        |  |  |
|---------------------------------|---|--------|--|--|
| 🖃 🧰 Managed Computer            | Group Tasks                                   | \$     |  |  |
| 🔃 Policy                        | •   |        |  |  |
| - 🔯 Group Tasks                 |   |        |  |  |
| 🗊 Client Computer:              | Telete New Task Start Task Properties Results |        |  |  |
| 🗄 🧰 Roaming Users               | Task Name Task Deferred Assisted To When      | Cabadu |  |  |
| 🖻 🧰 sample                      | Task Name Task Performed Assigned to whom     | Schedu |  |  |
| 🔃 Policy                        |   |        |  |  |
| 🔯 Group Tasks                   |   |        |  |  |
|                                 |   |        |  |  |





New Task Template window appears. This window lets you define Task Name, assign a task as well as schedule a task on computers.

| v Task Template   | ? |
|---|---|
| k Name  |   |
| Task Name:* security  |   |
| -inned Tacke  |   |
| כאכדו שאוואר  | 7 |
| File Anti-Virus Status  |   |
| Enabled   |   |
| Disabled  |   |
| Mail Anti-Virus Status  |   |
| Enabled   |   |
| Disabled  |   |
| Anti-Spam Status     Enabled  |   |
|   |   |
| Web Protection Status   |   |
| Enabled   |   |
| Disabled  |   |
| Endpoint Security Status  |   |
| Enabled   |   |
| Oisabled  |   |
| Firewall Status   |   |
| Disable Firewall  |   |
| Enable Limited Filter Mode of Firewall  |   |
| Enable Interactive Filter Mode of Firewall      Alternate Developed Status  |   |
|   |   |
| Disabled  |   |
| Start/Stop Another Server   |   |
| Start Server  |   |
| Stop Server   |   |
| Set Update Server   |   |
| Add Server Name/IP DESKTOP-3T473JA,192.168.0.117  |   |
| Remove Server Name/IP   |   |
| Scan  |   |
| Memory Scan   |   |
| System Folder Scan network drives   |   |
| Scan Local Drives Computer StartUp  |   |
| Scan System Drive   |   |
| Scan Data Drives  |   |
| Option  |   |
| Scan Archives   |   |
| Auto Shut Down After Scan Completion  |   |
| Scan Only   |   |
|   |   |
| Earce Cliept to Developed Lindate   |   |
| Force Client to Download Update Super Super Time with eScan Server  |   |
| <ul> <li>Force Client to Download Update</li> <li>Sync System Time with eScan Server</li> </ul>   |   |
| Force Client to Download Update     Sync System Time with eScan Server     Apply for Subgroups  |   |
| Force Client to Download Update     Sync System Time with eScan Server     Apply for Subgroups  |   |
| Force Client to Download Update     Sync System Time with eScan Server     Apply for Subgroups      KScheduling Settings      Force Client to Download Update     Manual Start  |   |
| Force Client to Download Update     Sync System Time with eScan Server     Apply for Subgroups      K Scheduling Settings   |   |
| Force Client to Download Update     Sync System Time with eScan Server     Apply for Subgroups      Scheduling Settings      O Enable Scheduler         Manual Start      O Daily   |   |
| Force Client to Download Update     Sync System Time with eScan Server     Apply for Subgroups      Scheduling Settings      O Enable Scheduler     Manual Start      O Daily     Weekly     Mon     Tue     Wed     Thu  |   |
|   |   |
| Force Client to Download Update Sync System Time with eScan Server Apply for Subgroups Sk Scheduling Settings Image: Scheduler |   |

- 4. Enter the Task Name and configure the desired task settings.
- 5. Click **Save**. The selected group will be assigned a task template.





# Managing a Group Task

Selecting a Group Task enables Start Task, Properties, Results and Delete buttons.

| 6 | Group Tasks 😵 Refresh 👔 Help                            |                   |                     |                     |                    |
|---|---|-------------------|---------------------|---------------------|--------------------|
|   | 🚺 New Task 🛐 Start Task 📴 Properties 🕞 Results 👔 Delete |                   |                     |                     |                    |
|   | <u>Task Name</u>  | Task Performed    | Assigned To Whom    | Schedule Type       |                    |
| [ | security  | Not Performed Yet | 'Managed Computers' | Automatic Scheduler | <u>Task Status</u> |

#### Start Task

To start a task manually, select a task and then click **Start Task**.

#### **Delete Task**

To delete a task, select a task and then click **Delete**.

#### **Properties**

To view the properties of a task, select a task and then click **Properties**. It also lets you modify or redefine the entire settings configured. After making the necessary changes, click **Save**. The properties for the group task will be saved and updated.

| security                  | 👔 Help                 |
|---------------------------|------------------------|
|                           |                        |
| General Schedule Settings |                        |
|                           |                        |
| Tack Name                 | secustu                |
|                           | secondy                |
| Task Creation Time:       | 05/28/20 06:10:59 PM   |
| Status:                   | Task not performed yet |
| Last Run:                 |                        |
|                           |                        |
|                           |                        |
|                           |                        |
|                           |                        |
| Save Close                |                        |

#### Results

To view the results of a completed task, select a task and then click **Results**.

| Task Results (Sample Task)              |                                |               |                      |  |
|---|--------------------------------|---------------|----------------------|--|
| Group Tasks > Task Results              |                                |               |                      |  |
| Client Computers                        | Group                          | <u>Status</u> | Time                 |  |
| 100110000000000000000000000000000000000 | Managed Computers\Sample Group | Completed     | 09/24/19 11:52:29 AM |  |





#### Task Status

To view the status, select a task and then click **Task Status**. A brief task summary is displayed.



### Assigning a Policy to the group

To assign a Policy to the group, follow the steps given below:

- 1. In the Managed Computers folder tree, select a group.
- 2. Under the group name, click **Policy**. Policy pane appears on the right side.

| Action List 🕶 🛐 Client Action List  | Policy Templates Policy Criteria   | ia Templates   |  |  |
|---|--|--|--|--|
| Managed Computers     Policy     Group Tasks     Group Tasks     Group Client Computers (1) | Policy   | 🗢 Refresh 👔 Help   |  |  |
| ⊞· 🔤 Roaming Users<br>⊟· 🥃 sample<br>🔃 Policy   | Assigned Template<br>Group Default Policy                                  | Date And Time of Assigned Template May 28 2020 02:29:54 PM |  |  |
| - 🧐 Group Tasks<br>- 🞲 Client Computers   | Select Criteria Change Criteria (*) Criteria to be set in case of conflict | eria 🔐 Remove  |  |  |
|   | Criteria Assigned Policy Temp  | plate Date And Time of Assigned Criteria                   |  |  |

3. To assign a Policy Template to group, click **Select Template**. New policy window appears.

| New Policy   | 🝸 Help |
|--|--------|
| Policy Template Selection                                  |        |
| Group Default Policy<br>File ACt<br>Sample Policy Template | •      |
| Select Cancel  |        |

4. Select a policy template and then click **Select**.





5. To assign criteria to group, click **Select Criteria**. Select Policy Criteria window appears.

| Select Policy Criteria                                      | 🝸 Help   |
|---|----------|
| Set this criteria as a default criteria in case of conflict |          |
| Policy Template Selection                                   |          |
| Group Default Policy<br>File ACt<br>Sample Policy Template  | •        |
|   | Ŧ        |
| Criteria Template Selection                                 |          |
| aaa<br>cr1  |          |
|   | <b>*</b> |
| Select Cancel   |          |

- If a computer falls under both conditions created by you, it will create a conflict. To avoid such conflict, select the checkbox Set this criteria as a default criteria in case of conflict. Then select the Policy Template and Criteria Template to be used in case of conflict.
- 7. Click **Select**. The default Policy Template and Criteria Template for group will be saved and updated.





# **Policy Template**

This button allows you to add different security baseline policies for specific computer or group.

# **Defining Policies**

Following OS policies can be defined for eScan Client modules:

#### **File Anti-virus**

The File Anti-Virus module scans all the existing files and folders for any infection. It also lets you report/disinfect/quarantine/delete infected objects. Moreover, it saves a copy of report file for future reference, and displays attention messages.

#### **Mail Anti-Virus**

The Mail Anti-Virus module scans all the incoming emails. It scans the emails by breaking it into three sections the header, subject and the body. After scanning, the module combines the sections and sends it to your mailbox.

#### Anti-Spam

The Anti-Spam module blocks spam emails by checking the content of outgoing and incoming mails and quarantines advertisement emails.

#### **Web Protection**

The Web Protection module lets you block websites. You can allow/block websites on timebased access restriction.

#### Firewall

The Firewall module lets you put up a restriction to incoming and outgoing traffic and hacking. You can define the firewall settings here. You can define the IP range, permitted applications, trusted MAC addresses and local IP addresses.

#### **Endpoint Security**

The Endpoint Security module monitors the application on client computers. It allows/ restricts USB, Block list, White list, and defines time restrictions for applications.

#### **Privacy Control**

The Privacy Control module lets you schedule an auto-erase of your cache, ActiveX, cookies, plugins, and history. You can also secure delete your files and folders where the files will be deleted directly without any traces.

#### **Administrator Password**

Administrator Password lets you create and change password for administrative login of eScan protection center and Two-Factor Authentication.

#### **ODS/Schedule Scan**




ODS (On Demand Scanning)/Schedule Scan provides you with various options like – checking for viruses, and making settings for creating logs and receiving alerts. You can also create task in the scheduler for automatic virus scanning.

### **MWL Inclusion List**

MWL (MicroWorld WinSock Layer) Inclusion List contains the name of all executable files which will bind itself to MWTSP.DLL. All other files are excluded.

### **MWL Exclusion List**

MWL (MicroWorld WinSock Layer) Exclusion List contains the name of all executable files which will not bind itself to MWTSP.DLL.

### **Notifications & Events**

Notifications & Events lets you configure the notification settings. It lets you send emails to specific recipients when malicious code is detected in an email or email attachment. It also lets you send alerts and warning messages to the sender or recipient of an infected message. The Events tab lets you configure settings to allow/restrict clients from sending alert for specific events.

### **Schedule Update**

The Schedule Update lets you schedule eScan database updates.

### Tools

The Tools lets you configure eBackup and RMM (Remote Monitoring Management) Settings.

Priority will be given to Policy assigned through Policy Criteria first, then the
 policy given to a specific computer and lastly given to policy assigned to the group to which the computer belongs.





# Creating Policy Template for a group/specific computer

To create a Policy template for a group, follow the steps given below:

- 1. Click Managed Computers.
- 2. Select the desired group and then click **Policy Template**. Policy Template window appears.

| Policy Templates |               |                   |                                  | 📚 Refresh 🛛 👔 Help      |
|------------------|---------------|-------------------|----------------------------------|-------------------------|
| Properties       | Parent Policy | 👕 Delete 📑 Assign | to Group(s) Assign to Computer(s | i) Copy Template        |
| Name of Template | Created On    | Modified On       | Assigned to Group(s)             | Assigned to Computer(s) |
|                  |               |                   |                                  |                         |

3. Click **New Template**. New Template window appears.

| -Sets                                     |   |      |  |
|---|---|------|--|
| Enter Template Name:*                     |   |      |  |
| File Anti-Virus Assign From Select Policy | ~ | Edit | Mail Anti-Virus     Edit     Assign From Select Policy   |
| Anti-Spam<br>Assign From Select Policy    | ~ | Edit | Web Protection     Edit Assign From Select Policy        |
| Assign From Select Policy                 | ~ | Edit | EndPoint Security     Edit     Assign From Select Policy |
| Privacy Control Assign From Select Policy | ~ | Edit |  |

- 4. Enter a name for Template.
- 5. To edit a module, select it and then click **Edit**.
- 6. Click **Save**. The Policy Template will be saved.





## Editing a Policy Template

Each module of a policy template can be further configured according to your preferences.

To edit a Policy Template, follow the steps given below:

1. Select a Policy Template and then click **Properties**. Properties window appears.

| icy Details   |   |
|---|---|
|   |   |
| File Anti-Virus     Edit       Assign From Select Policy        - | Mail Anti-Virus Edit Assign From Select Policy    |
| Anti-Spam     Edit Assign From Select Policy                      | Web Protection Edit Assign From Select Policy     |
| Edit Edit Assign From Select Policy                               | EndPoint Security Edit Assign From Select Policy  |
| Privacy Control Edit Assign From Select Policy                    |   |
| Administrator Password Edit Assign From Select Policy             | ODS/Schedule Scan Edit Assign From Select Policy  |
| MWL Inclusion List Edit Assign From Select Policy                 | MWL Exclusion List Edit Assign From Select Policy |
| Notifications & Events     Edit Assign From Select Policy         | Schedule Update Edit Assign From Select Policy -  |
| Tools Edit Assign From Select Policy                              |   |

- 2. Select a module and click **Edit** to configure it.
- 3. After making changes, click **OK**. The Policy Template gets updated.





### **File Anti-Virus**

Editing File Anti-Virus module displays following tabs:

- Objects
- Options
- Blocked Files
- Folder Protection
- File Rights
- TSPM

### **Objects**

The Objects tab lets you configure following options.

| Objects      | Options                | Block Files        | Folder Prote | ction File | Rights 1 | rspm |
|--------------|------------------------|--------------------|--------------|------------|----------|------|
| Actions      | in case of virus       | detection          |              |            |          |      |
| - 0          | <u>Report only</u>     |                    |              |            |          |      |
| ₽° ● 1       | <u>Disinfect</u>       |                    |              |            |          |      |
| - Og         | <u>Quarantine obje</u> | <u>ect</u>         |              |            |          |      |
| - O I        | <u>Delete object</u>   |                    |              |            |          |      |
| 🕑 <u>s</u>   | Scan local remo        | vable disk drives  | 1            |            |          |      |
| 🕑 g          | Scan local hard        | <u>disk drives</u> |              |            |          |      |
| 🕑 g          | Scan network dr        | rives              |              |            |          |      |
| <u> Scar</u> | n files of followin    | <u>ig types</u>    |              |            |          |      |
| 🕂 🕑          | Exclude by masl        | <u>k</u>           |              |            |          |      |
| ±            | Not a Virus List       |                    |              |            |          |      |
| ÷ 🖌          | Exclude Files / F      | olders             |              |            |          |      |
|              | Scan compound          | objects            |              |            |          |      |
| L. 🗆         | Enable code ana        | lyser              |              |            |          |      |
|              |                        | _                  |              |            |          |      |
|              |                        |                    |              |            |          |      |

### Actions in case of virus detection

This section lists the different actions that File Anti-Virus can perform when it detects virus infection.

### **Report Only**

Upon virus detection, eScan will only report the virus and won't take any action.

Disinfect and If disinfection is impossible it will Quarantine Object or Delete Object"

Out of these, the **Disinfect** option is selected by default. By default, the quarantined files are saved in **C:\Program Files\eScan\Infected folder.** You can select the **Make** 





**backup file before disinfection** option if you would like to make a backup of the files before they are disinfected.

### Scan local removable disk drives [Default]

Select this option if you want eScan to scan all the local removable drives attached to the computer.

### Scan local hard disk drives [Default]

Select this option if you want eScan to scan all the local hard drives installed on the computer.

### Scan network drives [Default]

Select this option if you want eScan to scan all the network drives, including mapped folders and drives connected to the computer.

### Scan files of following types

Select this option if you want eScan to scan all files, only infectable files, and files by extension (Scan by mask). eScan provides you a list of default files and file types that it scans by extension. You can add more items to this list or remove items as per your requirements by clicking **Add/Delete**.

### Exclude by mask [Default]

Select this checkbox if you want File Anti-Virus monitor to exclude all the objects in the Exclude by mask list during real-time monitoring or scanning. You can add/delete a file or a particular file extension by clicking **Add/Delete**.

### Not a virus list [Default]

File Anti-Virus is capable of detecting riskware. Riskware refers to software originally not intended to be malicious but somehow can pose as a security risk to critical operating system functions. You can add the names of riskware, such as remote admin software, to the riskware list in the **Not a virus list** dialog box by clicking **Add/Delete** if you are certain that they are not malicious. The riskware list is empty by default.

### Exclude Files/Folders [Default]

Select this checkbox if you want File Anti-Virus to exclude all the listed files, folders, and sub folders while it is monitoring or scanning folders. The files/folders added to this list will be excluded from only real-time scan as well as on demand scan. You can add or delete files/folders from the list of by clicking **Add/Delete**.

### Scan compound objects [Default]

Select this checkbox if you want eScan to scan archives and packed files during scan operations. By default, **Packed** is selected.





### **Enable code Analyzer**

Select this checkbox if you want eScan to scan your computer for suspicious objects or unknown infections by using the heuristic analyzer. After selection, File Anti-Virus not only scans and detects infected objects, but also checks for suspicious files stored on computer.

### Options

The Options tab lets you configure following options:

| le Anti-Virus |  |  |                   |             | 🝸 Hel |
|---------------|--|--|-------------------|-------------|-------|
| Objects       | Options  | Block Files  | Folder Protection | File Rights | TSPM  |
|               | a report file<br>Show pack info i<br>Show clean obje<br>imit size to (KB<br>imit file size to<br>Proactive Behavi<br>Display attention<br>Snable Malware<br>Snable Ransomy | n the report<br>ct info in the rep<br>)_(avpM.rpt)<br>kup / Restore<br>(KB)<br>iour Monitor<br>n messages<br>URL Filter<br>vare Protection | ort               |             |       |
| Default       | Advanced   | Setting  | ОК Са             | ncel        |       |

### Save report file [Default]

Select this checkbox if you want eScan to save the reports generated by the File Anti-Virus module. The report file logs information about the scanned files and the action taken by File Anti-Virus when an infected file was found during the scan.

### Show pack info in the report [Default]

Select this checkbox if you want File Anti-Virus to add information regarding scanned compressed files, such as .zip and .rar files to the Monvir.log file.

### Show clean object info in the report

Select this checkbox if you want File Anti-Virus to add information regarding uninfected files found during a scan operation to the Monvir.log file. You can select this option to find out which files are not infected.





### Limit size to (Kb) (avpM.rpt)

Select this checkbox if you want File Anti-Virus to limit the size of the Monvir.log file and avpM.rpt file. To modify the limit, enter the log file size in field.

### Enable Auto backup/Restore [Default]

Selecting this checkbox lets you back up the critical files of the Windows® operating system and then automatically restores the clean files when eScan finds an infection in any of the system files that cannot be disinfected. You can do the following settings:

- **Do not backup files above size (KB) [Default]**: This option lets you prevent File Anti-Virus from creating backup of files that are larger than the file size that you have specified.
- **Minimum disk space (MB) [Default]**: The Auto-backup feature will first check for the minimum available space limit defined for a hard disk drive. If the minimum defined space is available then only the Auto-backup feature will work, if not it will stop without notifying. You can allot the Minimum disk space to be checked from this option. By default, the minimum disk space is 500 MB.

### Limit file size to (KB) [Default]

This checkbox lets you set a limit size for the objects or files to be scanned. The default value is set to **20480 Kb**.

### **Proactive Behavior Monitor**

Selecting this checkbox enables File Anti-Virus to monitor computer for suspicious applications and prompts you to block such applications when they try to execute.

• Whitelist Option: Whitelisting lets you mark the files in the database that you want to exclude from being blocked. To whitelist a file/folder, click Whitelist and then click Add from DB.

### Display attention messages [Default]

When this option is selected, eScan displays an alert consisting the path and name of the infected object and the action taken by the File Anti-Virus module.

### **Enable Malware URL Filter**

This option lets you enable a Malware URL filter where eScan blocks all URLs that are suspected to be malwares. You can exclude specific websites by whitelisting them from the eScan pop up displayed when you try to access the site.

### **Enable Ransomware Protection**

This option lets you enable Ransomware Protection on the system where eScan blocks any suspected ransomware activities performed on system. With the technology called PBAE (Proactive Behavioral Analysis Engine) eScan monitors the activity of all processes on the local computer and when it encounters any activity or behavior that matches a ransomware, it raises a red flag and blocks the process.





### **Block Files**

The Block Files tab lets you configure settings for preventing executables and files, such as autorun.inf on network drives, USB drives, and fixed drives from accessing your computer.

| bjects Options Block Files Folder Protection File Rights TSPM  | nti-Vir | us                                     |                                 |                   |             |      |                            |
|--|---------|--|---------------------------------|-------------------|-------------|------|----------------------------|
| Disable Autoplay on USB and Fixed Drives         Deny access of executables on USB Drives         User defined whitelist         Add         Deny access of executables from Network         User defined whitelist         Folder Name         Include Subfolder         Add         Delete         RemoveAll   | jects   | Options                                | Block Files                     | Folder Protection | File Rights | TSPM |                            |
| □ Deny access of executables on USB Drives         User defined whitelist         □ File Name         □ Deny access of executables from Network         User defined whitelist         □ Folder Name         □ Deny Access of following files         □ Quarantine Access-denied files         □ file Name         □ Add         □ Deny Access of following files         □ Quarantine Access-denied files   | Dis     | able Autoplay on                       | USB and Fixed D                 | rives             |             |      |                            |
| File Name       Add         Delete       RemoveAll         Deny access of executables from Network       User defined whitelist         Folder Name       Include Subfolder         Output       Add         Delete       RemoveAll         Deny Access of following files       Quarantine Access-denied files         file Name       Add         %sysdir%\*.EXE@       Add         Delete       RemoveAll | User    | Deny access of ex<br>defined whitelist | ecutables on USE                | B Drives          |             |      |                            |
| RemoveAll         Deny access of executables from Network         User defined whitelist         Folder Name         Include Subfolder         Add         Delete         RemoveAll  |         | <u>File Name</u>                       |                                 |                   |             |      | Add<br>Delete              |
| □       Deny access of executables from Network         User defined whitelist       Add         □       Folder Name       Add         □       Delete       RemoveAll         ☑       Deny Access of following files       Quarantine Access-denied files         □       %sysdir%\*.EXE@       Add         □       %sysdir%\*.EXE@       Add  |         |  |                                 |                   |             |      | RemoveAll                  |
| <ul> <li>Deny Access of following files</li> <li>Quarantine Access-denied files</li> <li><u>File Name</u></li> <li>%sysdir%\*.EXE@</li> </ul>  | User    | Folder Name                            |                                 | Include Subfol    | <u>der</u>  |      | Add<br>Delete<br>RemoveAll |
| File Name     Add            %sysdir%\*.EXE@      Delete   |         | Deny Access of fo<br>Quarantine Acces  | llowing files<br>s-denied files |                   |             |      |                            |
| RemoveAll  |         | File Name                              |                                 |                   |             |      | Add<br>Delete              |
|  |         |  |                                 |                   |             |      |                            |
|  |         | %sysdir%\*.EX                          | E@                              |                   |             |      | <br>Removeali              |
|  |         | %sysdir%\*.EXI                         | E@                              |                   |             |      | RemoveAll                  |

You can configure the following settings:

### Disable AutoPlay on USB and Fixed Drives [Default]

Selecting this option will disable AutoPlay when a USB/Fixed Drive is connected.

### Deny access of executables on USB Drives

Select this checkbox if you want eScan to prevent executables stored on USB drives from being accessed.

### Deny access of executable from Network

Select this checkbox if you want eScan to prevent executables on the client computer from being accessed from the network.





### User defined whitelist

This option gets enabled after selecting the **Deny access of executable from Network** checkbox. You can use this option to enter the folders that need to be whitelisted so that executables can be accessed in the network from the folders mentioned under this list. To add files, click **Add**.

| Add Folder | •                         |             |  |
|------------|---------------------------|-------------|--|
| C:\Docum   | ents and Settings\Remya\M | y Documents |  |
| 🗹 Indu     | de Subfolder              |             |  |
| Add Ca     | ancel                     |             |  |

Enter the complete path of the folder to be whitelisted on the client systems. You can either whitelist only the parent folder or select the **Include subfolder** option to whitelist the subfolders as well.

### Deny Access of following files [Default]

Select this checkbox if you want eScan to prevent the files in the list from running on the computers.

### **Quarantine Access-denied files**

Select this checkbox if you want eScan to quarantine files to which access is denied.

- You can prevent specific files from running on the eScan client computer by adding them to the Block Files list. By default, this list contains the value %sysdir%\\\*.EXE@. Click Add.
- 2. Enter the full name of the file to be blocked from execution on the client systems.





### **Folder Protection**

The Folder Protection tab lets you protect specific folders from being modified or deleted by adding them to the Folder Protection list. It lets you configure the following setting:

| le Anti-Virus   |  | 褶 He                       |
|-----------------|--|----------------------------|
| Objects Options | Block Files Folder Protection File Rights TSPM |                            |
| Folder Name     | Include Subfolder                              | Add<br>Delete<br>RemoveAll |
| Default Advar   | iced Setting OK Cancel                         |                            |

### Protect files in following folders from modification and deletion [Default]

This option is selected by default. Selecting this check box enables File Anti-Virus module to protect files in specific folders from being modified or deleted on the client systems.

- 1. To protect files from modification, click **Add**.
- 2. Enter the complete path of the folder to be protected on the client systems.
- 3. You can either protect only the parent folder or select the **Include subfolder** option to protect the subfolders as well.
- 4. Click Add.





### **File Rights**

The File Rights tab restricts or allows for remote or local users from modifying folders, subfolders, files or files with certain extensions.

| bjects | Options Block Files        | Folder Protection        | File Rights TSPM  |         |       |
|--------|----------------------------|--------------------------|-------------------|---------|-------|
| E      | nable eScan Remote File    | Rights                   |                   |         |       |
| Do n   | ot allow remote users to   | modify the following l   | ocal files        |         |       |
|        | <u>File / Folder Name</u>  | Includ                   | e Subfolder       | A Ad    | d     |
|        | *.EXE                      |                          |                   | Remo    | veAll |
|        | *.COM                      |                          |                   |         |       |
| Allow  | Modification for following | Files                    |                   | <b></b> |       |
|        | <u>File / Folder Name</u>  | ,                        | Include Subfolder | ∧ Ad    | Ь     |
|        | %TEMP%\                    |                          | v                 | Del     | ete   |
|        | %WINDIR%\TEMP\             |                          | v                 |         |       |
|        |                            |                          |                   | ¥       |       |
|        |                            |                          |                   |         |       |
| E Er   | nable eScan Local File Rig | ihts                     |                   |         |       |
| Don    | ot allow local users to mo | dify the following file: | 5                 | A       | d     |
|        | File / Folder Name         |                          | Include Subfolder | Del     | ete   |
|        | smss.exe                   |                          |                   | Remo    | veAll |

### **Enable eScan Remote File Rights**

Select this checkbox to allow/restrict the remote users to make any modifications to the files and folders.

### Do not allow remote users to modify the following local files

The files/folders added to this list cannot be modified by the remote users.

### Allow modification for following files

The files added to this list can be modified by the remote user.

### Enable eScan local file rights

Select this checkbox to allow/restrict the local users to make any modifications to the files/folders.

### Do not allow local users to modify the following files

The files/folders added to this list cannot be modified by the local users.

### Allow modification for files

The files/folders added to this list can be modified by the local users.





### TSPM

eScan's Terminal Services Protection Module (TSPM) detects brute force attempts, identifies suspicious IP addresses/hosts and blocks any access attempts from them to prevent future attacks. The IP addresses and hosts from the attacks are banned from initiating any further connections to the system. It also detects and stops attempts of attackers who try to uninstall security applications from systems and alerts administrators about the preventive measures initiated by TSPM.

| File Anti-Virus  | 褶 Help        |
|--|---------------|
| Objects         Options         Block Files         Folder Protection         File Rights         TSPM <ul></ul> |               |
| WhiteListed IPs  | Add<br>Delete |
| Default Advanced Setting OK Cancel   |               |

- 1. Select the checkbox **Enable Terminal Service Protection Module** to activate TSPM module.
- 2. To add a list of IP addresses to be excluded from being blocked by TSPM, click **Add**. Add IP window appears.

|              | ×                    |
|--------------|----------------------|
| Add IP       |                      |
|              |                      |
|              |                      |
| IP Address*: |                      |
|              |                      |
|              |                      |
| Ok Cancel    | (*) Mandatory Fields |

3. Enter the IP address and then click **OK**.





### **Advanced Settings**

Clicking Advanced Settings lets you configure advanced settings for console.

| Adv | dvanced Setting |  |              |  |  |  |  |  |
|-----|-----------------|--|--------------|--|--|--|--|--|
|     | _               |  |              |  |  |  |  |  |
|     |                 | Name   | <u>Value</u> |  |  |  |  |  |
|     |                 | Disable Reload Password (2=Disable/1=Enable)             | 1 .          |  |  |  |  |  |
|     |                 | Display Print Job events                                 | 1 .          |  |  |  |  |  |
|     |                 | IPAddress Change Allowed (2=Disable/1=Enable)            | 1 .          |  |  |  |  |  |
|     |                 | Enable Time Syncronization                               | 1 .          |  |  |  |  |  |
|     |                 | Clear Quarantine folder after Days specified             | 28           |  |  |  |  |  |
|     |                 | Clear Quarantine Folder after Size Limit specified in MB | 0            |  |  |  |  |  |
|     |                 | Exclude System PID from Scanning                         | 0 🔻          |  |  |  |  |  |
|     |                 | Disable Virtual Key Board Shortcut key                   | 0 .          |  |  |  |  |  |
|     |                 | Show eScan Tray Menu                                     | 1 .          |  |  |  |  |  |
|     |                 | Show eScan Tray Icon                                     | 1 .          |  |  |  |  |  |
|     |                 | Show eScan Desktop Protection Icon                       | 1 .          |  |  |  |  |  |
|     |                 | Enable eScan Remote Support in Non-Administrator mode    | 0 .          |  |  |  |  |  |
|     |                 | Define Virus Alert Time (in seconds)                     | 20           |  |  |  |  |  |
|     |                 | Show Malware URL Warning                                 | 1 .          |  |  |  |  |  |
|     |                 |  |              |  |  |  |  |  |
|     | Ok              |  |              |  |  |  |  |  |

### Disable Reload Password (2=Disable/1=Enable)

This option lets you enable or disable password for reloading eScan. After enabling, the user will be asked to enter reload password if user attempts to reload eScan. This is the administrator password for eScan Protection Center.

### Display Print Job events (1 = Enable/0 = Disable)

This option lets you capture events for the Print Jobs from Managed Computers.

### IP Address Change Allowed (2 = Disable/1 = Enable)

This option lets you enable/disable IP Address Change by the user on their computer.

### Enable Time Synchronization (1 = Enable/0 = Disable)

This option lets you enable/disable time synchronization with internet. Active internet connection is mandatory for this feature.

### **Clear Quarantine folder after Days specified**

This option lets you specify number of days after which the Quarantine folder should be cleared on Managed Computers.





### **Clear Quarantine Folder after Size Limit specified in MB**

This option lets you specify size limit for the Quarantine folder. If the defined size limit exceeds, the Quarantine folder will be cleared on Managed Computers.

### Exclude System PID from Scanning (1 = Enable/0 = Disable)

This option lets you exclude system process ID (Microsoft assigned System PIDs) from scanning on Managed Computers.

### Disable Virtual Key Board Shortcut key (1 = Enable/0 = Disable)

This option lets you disable shortcut for using Virtual Keyboard on Managed Computers.

### Show eScan Tray Menu (1 = Show/0 = Hide)

This option lets you Hide or Show eScan Tray menu on Managed Computers.

#### Show eScan Tray Icon (1 = Show/0 = Hide)

This option lets you hide or show eScan Tray Icon on Managed Computers.

### Show eScan Desktop Protection Icon (1 = Show/0 = Hide)

This option lets you hide or show eScan Protection icon on Managed Computers.

## Enable eScan Remote Support in Non-Administrator mode (1 = Enable/0 = Disable)

This option lets you enable/disable eScan Remote Support in Non-Administrator Mode. eScan will not prompt for entering Administrator Password to start eScan Remote Support from Managed Computers.

### **Define Virus Alert Time (in seconds)**

This option lets you define time period in seconds to display Virus Alert on Managed Computers.

### Show Malware URL Warning (1 = Show/0 = Hide)

This option lets you show or hide Malware URL warning messages on Managed Computers.

### Protect Windows Hosts File (1 = Allow/0 = Block)

Use this option to Allow/Block modifications to Windows Host Files.

### Search for HTML Scripts (1 = Allow/0 = Block)

Use this option to Allow/Block search for html script (infection) in files. This option will have impact on system performance.

### Show Network Executable block alert (1 = Show/0 = Hide)

This option lets you show/hide Network executable block alerts on Managed Computers.





### Show USB Executable Block Alert (1 = Show/0 = Hide)

This option lets you show/hide USB executable block alerts on Managed Computers.

### Show eScan Tray Icon on Terminal Client (1 = Show/0 = Hide)

This option lets you show/hide eScan Tray Icon on Terminal Clients on Managed Computers.

### Enable eScan Self Protection (1 = Enable/0 = Disable)

This option lets you Enable/Disable eScan Self Protection on Managed Computers, if this feature is enabled, no changes or modifications can be made in any eScan File.

### Enable eScan Registry Protection (1 = Enable/0 = Disable)

This option lets you Enable/Disable eScan Registry Protection. User cannot make changes in protected registry entries if it is enabled on Managed Computers.

### Enable backup of DLL files (1 = Enable/0 = Disable)

This option lets you Enable/Disable backup of DLL files on Managed Computers.

## Integrate Server Service dependency with Real-time monitor (1 = Enable/0 = Disable)

This option lets you Integrate Server Service dependency with real-time monitor.

### Send Installed Software Events (1 = Enable/0 = Disable)

This option lets you receive Installed Software Events from Managed Computers.

### Enable Winsock Protection (Require Restart) (1 = Enable/0 = Disable)

This option lets you Enable/Disable protection at the Winsock Layer.

### Enable Cloud (1 = Enable/0 = Disable)

This option lets you Enable/Disable eScan Cloud Security Protection on Managed Computers.

### Enable Cloud Scanning (1 = Enable/0 = Disable)

This option lets you Enable/Disable Cloud Scanning on Managed Computers.

### Remove LNK (Real-Time) (1 = Enable/0 = Disable)

This option lets you Enable/Disable Removal of LNK on real-time basis.

### Whitelisted AutoConfigURL

This option lets you whitelist AutoConfigURLs. Enter comma separated URLs that need to be whitelisted.

### Disable Add-ons/Extension blocking (1 = Enable/0 = Disable)

Selecting this option disables Add-ons and Extension blocking.

### Include files to scan for archive (Eg: abc\*.exe)

This option lets you add file types that needs to be when archive scanning enabled.

### Block Date-Time Modification (1 = Enable/0 = Disable)

This option lets you block the modification of the system date and time.





## Allow CMD-Registry for Date-Time blocking (Depends upon Block Date-Time Modification) (1 = Enable/0 = Disable)

Selecting this option lets you block date-time modification from the CMD-Registry.

### Domain list for exclusion of Host file scanning (e.g. abc.mwti)

Selecting this option lets you add the list of domains to be excluded from host file scanning.

## Disable Pause Protection and Open Protection center on Right Click (Set 192 for disable)

This option disables Pause Protection and Open Protection center on Right Click if you set it to 192.

### Enable Share Access Control (1 = Enable/0 = Disable)

## (Note:- Only if it is enabled the setting "NetworkSharesReadOnlyAccess" and "NetworkSharesNoAccess" will be referred)

It enables Share Access Control. Network Shares ReadOnly Access and Network Shares NoAccess options will work only if this option is selected.

# List of comma-separated servers and/or shares and/or wildcards which needs to be given NO ACCESS e.g. \\192.168.1.1\temp or \\192.168.1.1\temp\\*.doc or \*.doc (Work only when "Enable Share Access Control" is set)

Selecting this option lets you add the List of comma-separated servers and/or shares and/or wildcards that should not be accessible.

## List of comma-separated servers and/or shares and/or wildcards which needs to be given READ ONLY ACCESS e.g. $\192.168.1.1\$ temp or

## \\192.168.1.1\temp\\*.doc or \*.doc (Work only when "Enable Share Access Control" is set)

Selecting this option lets you add the List of comma-separated servers and/or shares and/or wildcards that should be given only view access and not be editable.

### Include files to scan for archive (eg:abc\*.exe)

Selecting this option lets you add file types that should be scanned.

### Whitelist IP Address (Depends on IP Address Change Allowed) (E.G 192.168.1.\* You can put comma-separated list)

Selecting this option lets you add the list of IP addresses separated by commas to whitelist them.

### Block Access to Control Panel (1 = Enable/0 = Disable)

Selecting this option lets you block the user from accessing the control panel.

### Disable COPY/PASTE (1 = Enable/0 = Disable)

Selecting this option lets you disable Copy/Paste actions.

## Enable logging of sharing activity from suspected malware system (WSmbFilt.log on client system) (1 = Enable/0 = Disable)

Enabling this option directs eScan to log any sharing activity performed by suspected malware system. By default, this feature is enabled.





### Block all RDP Session except Whitelisted under TSPM

Selecting this option lets you block all RDP sessions excluding the ones you have Whitelisted under TSPM.

## Allow RDP (1=Block Foreign IP and allow Local IP/0 =Block Local & Foreign IP but allow Whitelisted IP)

This option lets you allow or block the foreign and local IP addresses excluding the whitelisted ones.

### **PowerShell Exclusion list**

Selecting this option lets you add a PowerShell script file path manually to exclude files and folders from real-time scan.

### Allow Uninstallers (1 = Enable/0 = Disable)

Selecting this option lets you enable/disable use of third party uninstallers.

### Block Renaming of Hostname (1 = Enable/0 = Disable)

Selecting this option lets you enable/disable block Hostname renaming.

### Restricted Environment enabled (1 = Enable/0 = Disable)

Selecting this option lets you enable/disable restrict environment settings.

### Block eternal blue (wannacry) exploits (1 = Enable/0 = Disable)

Selecting this option lets you block eternal blue (wannacry) exploits. By default, this option is enabled.

### Send Windows Security Patch Events (1-KB patches;2-Security Update;4-Hotfix;8-Update;16-Service Pack;31-All)

By selecting this option, you enable eScan to send events for the windows security patches installed in the system.

### **Block Renaming of Hosts file**

Selecting this option lets you block renaming of host files on managed computers.

### Block Gmail (except corporate ones)

Selecting this option lets you block users from accessing personal Gmail accounts on managed computers.

### **Mail Anti-Virus**

Mail Anti-Virus is a part of the Protection feature of eScan. This module scans all incoming and outgoing emails for viruses, spyware, adware, and other malicious objects. It lets you send virus warnings to client computers on the Mail Anti-Virus activities. By default, Mail Anti-Virus scans only the incoming emails and attachments, but you can configure it to scan outgoing emails and attachments as well. Moreover, it lets you notify the sender or system administrator whenever you receive an infected email or attachment. This page provides you with options for configuring the module.





| Mail Antivirus Settings   | 🝸 Help |
|---|--------|
| Start Stop  |        |
| Scan Options          Block Attachments Types       Action         PRETTY*.EXE       Add         NAVI*.EXE       Delete         KAK.HTA       Advanced         EIX200* EVE       Advanced |        |
| PIX200*.EXE<br>MINE.*<br>TRY*.EXE<br>SUPP*.EXE<br>THE_FLY.*<br>Y2K.EXE  |        |
| Port Settings for eMail Outgoing Mail(SMTP) Incoming Mail(POP3) Scan Outgoing Mails   |        |
| Default Ok Cancel   |        |





### **Scan Options**

This tab lets you select the emails to be scanned and action that should be performed when a security threat is encountered during a scan operation. This tab lets you configure following settings:

- **Block Attachments Types**: This section provides you with a predefined list of file types that are often used by virus writers to embed viruses. Any email attachment having an extension included in this list will be blocked or deleted by eScan at the gateway level. You can add file extensions to this list as per your requirements. As a best practice, you should avoid deleting the file extensions that are present in the **Block Attachments Types** list by default. You can also configure advanced settings required to scan emails for malicious code.
- **Action**: This section lets you configure the actions to be performed on infected emails. These operations are as follows:
  - **Disinfect [Default]**: Select this option if you want Mail Anti-Virus to disinfect infected emails or attachments.
  - **Delete**: Select this option if you want Mail Anti-Virus to delete infected emails or attachments.
  - Quarantine Infected Files [Default]: Select this option if you want Mail Anti-Virus to quarantine infected emails or attachments. The default path for storing quarantined emails or attachments is – C:\Program Files\eScan\QUARANT.

However, you can specify a different path for storing quarantined files, if required.

- **Port Settings for email**: You can also specify the ports for incoming and outgoing emails so that eScan can scan the emails sent or received through those ports.
  - **Outgoing Mail (SMTP) [Default: 25]**: You need to specify a port number for SMTP.
  - **Incoming Mail (POP3) [Default: 110]**: You need to specify a port number for POP3.
  - **Scan Outgoing Mails**: Select this option if you want Mail Anti-Virus to scan outgoing emails as well.





### Advanced

Clicking **Advanced** displays Advanced Scan Options dialog box. This dialog box lets you configure the following advanced scanning options:

| vanced Scan Options         Delete all Attachments in eMail if Disinfection is not possible         Delete entire eMail if Disinfection is not possible         Delete entire eMail if any Virus is found         Quarantine Blocked Attachments         Delete entire eMail if any Blocked Attchement is found         Quarantine eMail if Attachments are not Scanned         Quarantine Attachments if they are Scanned         Exclude Attchements (White List)         Add |
|---|
| <ul> <li>Delete all Attachments in eMail if Disinfection is not possible</li> <li>Delete entire eMail if Disinfection is not possible</li> <li>Delete entire eMail if any Virus is found</li> <li>Quarantine Blocked Attachments</li> <li>Delete entire eMail if any Blocked Attchement is found</li> <li>Quarantine eMail if Attachments are not Scanned</li> <li>Quarantine Attachments if they are Scanned</li> <li>Exclude Attchements (White List)</li> <li>Add</li> </ul> |
| <ul> <li>Delete entire eMail if Disinfection is not possible</li> <li>Delete entire eMail if any Virus is found</li> <li>Quarantine Blocked Attachments</li> <li>Delete entire eMail if any Blocked Attchement is found</li> <li>Quarantine eMail if Attachments are not Scanned</li> <li>Quarantine Attachments if they are Scanned</li> <li>Exclude Attchements (White List)</li> <li>Add</li> <li>Delete</li> </ul>  |
| <ul> <li>Delete entire eMail if any Virus is found</li> <li>Quarantine Blocked Attachments</li> <li>Delete entire eMail if any Blocked Attachment is found</li> <li>Quarantine eMail if Attachments are not Scanned</li> <li>Quarantine Attachments if they are Scanned</li> <li>Exclude Attachments (White List)</li> <li>Add</li> <li>Delete</li> </ul>   |
| <ul> <li>Quarantine Blocked Attachments</li> <li>Delete entire eMail if any Blocked Attachment is found</li> <li>Quarantine eMail if Attachments are not Scanned</li> <li>Quarantine Attachments if they are Scanned</li> <li>Exclude Attachments (White List)</li> <li>Add</li> <li>Delete</li> </ul>  |
| <ul> <li>Delete entire eMail if any Blocked Attchement is found</li> <li>Quarantine eMail if Attachments are not Scanned</li> <li>Quarantine Attachments if they are Scanned</li> <li>Exclude Attchements (White List)</li> <li>Add</li> <li>Delete</li> </ul>  |
| Quarantine eMail if Attachments are not Scanned Quarantine Attachments if they are Scanned Exclude Attchements (White List) Add Delete  |
| Quarantine Attachments if they are Scanned<br>Exclude Attchements (White List)<br>Add<br>Delete   |
| Exclude Attchements (White List) Add Delete   |
| Add Delete  |
| Delete  |
| Delece  |
|   |
|   |
|   |
|   |
| Save  |
|   |

### Delete all Attachment in email if disinfection is not possible

Select this option to delete all the email attachments that cannot be cleaned.

### Delete entire email if disinfection is not possible [Default]

Select this option to delete the entire email if any attachment cannot be cleaned.

### Delete entire email if any virus is found

Select this option to delete the entire email if any virus is found in the email or the attachment is infected.

### Quarantine blocked Attachments [Default]

Select this option to quarantine the attachment if it bears extension blocked by eScan.

### Delete entire email if any blocked attachment is found [Default]

Select this option to delete an email if it contains an attachment with an extension type blocked by eScan.

### Quarantine email if attachments are not scanned

Select this checkbox to quarantine an entire email if it contains an attachment not scanned by Mail Anti-Virus.





### Quarantine Attachments if they are scanned

Select this checkbox if you want eScan to quarantine attachments that are scanned by Mail Anti-Virus.

#### **Exclude Attachments (White List)**

This list is empty by default. You can add file names and file extensions that should not be blocked by eScan. You can also configure eScan to allow specific files even though if the file type is blocked. For example, if you have listed \*.PIF in the list of blocked attachments and you need to allow an attachment with the name ABC, you can add abcd.pif to the Exclude Attachments list. Add D.PIFing \*.PIF files in this section will allow all \*.PIF to be delivered. MicroWorld recommends you to add the entire file name like ABCD.PIF.





### **Anti-Spam**

Anti-Spam module filters junk and spam emails and sends content warnings to specified recipients. Here you can configure the following settings.

| Anti-Spam  | Help |
|--|------|
| Start Stop   |      |
| Advanced   |      |
| Send Original Mail to User   |      |
| Do not check content of Replied or Forwarded Mails   |      |
| Check Content of Outgoing mails  | ses  |
| Spam Filter Configuration  |      |
| Check for Mail Phishing  |      |
| Treat Mails with Chinese/Korean character set as SPAM  |      |
| Treat Subject with more than 5 whitespaces as SPAM   |      |
| Check content of HTML mails  |      |
| ✓ Quarantine Advertisement mails Advar   | nced |
| Mail Tagging Options   |      |
| Do not change email at all.  |      |
| Both subject and body is changed. [Spam] tag is added in Subject. Actual spam content is embed<br>in Body. | lded |
| "X-MailScan-Spam: 1" header line is added. Actual spam content is embedded in Body.                        |      |
| Only [Spam] tag is added in Subject. Body is left unchanged.   |      |
| "X-MailScan-Spam: 1" header line is added. Body and subject both remain unchanged.                         |      |
| Default OK Cancel  |      |

### Advanced

This section provides you with options for configuring the general email options, spam filter configuration, and tagging emails in Anti-Spam.

### Send Original Mail to User [Default]

This checkbox is selected by default. eScan delivers spam mail to your inbox with a spam tag. When an email is tagged as SPAM, it is moved to this folder. Select this checkbox, if you want to send original email tagged as spam to the recipient as well.

### Do not check content of Replied or Forwarded Mails

Select this checkbox, if you want to ensure that eScan does not check the contents of emails that you have either replied or forwarded to other recipients.





### **Check Content of Outgoing mails**

Select this checkbox, if you want Anti-Spam to check outgoing emails for restricted content.

### Phrases

Click **Phrases** to open the **Phrases** dialog box. This dialog box lets you configure additional email related options. In addition, it lets you specify a list of words that the user can either allow or block.

|   |                |        |      |                            |  |   |                                 | × |
|---|----------------|--------|------|----------------------------|--|---|---------------------------------|---|
| P | hrases to Cheo | :k     |      |                            |  |   |                                 |   |
|   |                |        | <br> |                            |  |   |                                 | _ |
|   |                |        |      | User s<br>User s<br>User s | pecified white<br>pecified List o<br>pecified word | elist of words/<br>of Blocked wor<br>s/phrases disa | phrases<br>:ds/phrases<br>abled |   |
|   | Action Lis     | t 🕶    |      |                            |  |   |                                 |   |
|   | Sr. No.        | Phrase |      |                            |  | Quarantine  | Delete                          |   |
|   |                |        |      |                            |  |   |                                 |   |
|   |                |        |      |                            |  |   |                                 |   |
|   |                |        |      |                            |  |   |                                 |   |
|   |                |        |      |                            |  |   |                                 |   |
|   |                |        |      |                            |  |   |                                 |   |
|   |                |        | <br> |                            |  |   |                                 |   |
|   |                | Canad  | <br> |                            |  |   |                                 |   |
|   | UK             | Cancel |      |                            |  |   |                                 |   |

### User specified whitelist of words/phrases (Color Code: GREEN)

This option indicates the list of words or phrases that are present in the whitelist. A phrase added to the whitelist cannot be edited, enabled, or disabled.

### User specified List of Blocked words/phrases: (Color Code: RED)

This option indicates the list of words or phrases that are defined in block list.

### User specified words/phrases disabled: (Color Code: GRAY)

This option indicates the list of words or phrases that are defined to be excluded during scans. The options in the **Phrases to Check** dialog box are disabled by default.

### **Action List**

- Add Phrase: Option to add phrase to quarantine or delete the mail.
- Edit Phrase: To modify existing phrase added in list.
- **Enable Phrase:** By default, it is enabled. After being disabled, you can use this option to enable it.
- Disable Phrase: Disable existing phrase added in list.
- Whitelist: This will allow email to deliver to inbox when phrase is found in the email.
- Block list: This will delete email when it contains the phrase.
- **Delete:** Delete the phrase added in list.





### **Spam Filter Configuration**

This section provides you with options for configuring the spam filter. All options in this section are selected by default.

### Check for Mail Phishing [Default]

Select this option if you want Anti-Spam to check for fraudulent emails and quarantine them.

### Treat Mails with Chinese/Korean character set as SPAM [Default]

When this option is selected, emails are scanned for Chinese or Korean characters. This check is based on the research data conducted by MicroWorld's various spam email samples collected from around the globe. From these samples, it was observed that spammers often use Chinese or Korean characters in their emails.

### Treat Subject with more than 5 whitespaces as SPAM [Default]

In its research, MicroWorld found that spam emails usually contain more than five consecutive white spaces. When this option is selected, Anti-Spam checks the spacing between characters or words in the subject line of emails and treats emails with more than five whitespaces in their subject lines as spam emails.

### Check content of HTML mails [Default]

Select this option if you want Anti-Spam to scan emails in HTML format along with text content.

### **Quarantine Advertisement mails [Default]**

Select this option if you want Anti-Spam to check for advertisement types of emails and quarantine them.





### Advanced

Clicking **Advanced** displays Advanced Spam Filtering Options dialog box. This dialog box lets you configure the following advanced options for controlling spam.

| Advanced Spam Filtering Options  |  |
|--|--|
| <ul> <li>Enable Non Intrusive Learning Pattern (NILP) check</li> <li>Enable eMail Header check</li> <li>Enable X-Spam Rules check</li> <li>Enable Sender Policy Framework (SPF) check</li> </ul> | :k   |
| <ul> <li>Enable Spam URI Realtime Blacklist (SURBL) check</li> <li>Enable Real-time Blackhole List (RBL) check</li> </ul>  | k  |
| RBL Servers Add bl.spamcop.net b.barracudacentral.org Remove All   | Auto-Spam Whitelist Add  *@analytics.bounces.googl @Delete *@irctc.co.in *@sourcenext.co.jp *@sourcenext.com *@courcenext.infe |
| Save Cancel  |  |

### Enable Non- Intrusive Learning Pattern (NILP) check [Default]

Non-Learning Intrusive Pattern (NILP) is MicroWorld's revolutionary technology that uses Bayesian Filtering and works on the principles of Artificial Intelligence (AI) to analyze each email and prevents spam and phishing emails from reaching your inbox. It has self-learning capabilities and it updates itself by using regular research feeds from MicroWorld servers. It uses an adaptive mechanism to analyze each email and categorize it as spam or ham based on the behavioral pattern of the user.

### Enable email Header check [Default]

Select this option if you want to check the validity of certain generic fields likes From, To, and CC in an email and marks it as spam if any of the headers are invalid.

### Enable X Spam Rules check [Default]

X Spam Rules are rules that describe certain characteristics of an email. It checks whether the words in the content of emails are present in eScan's database. This database contains a list of words and phrases, each of which is assigned a score or threshold. The Spam Rules Check technology matches X Spam Rules with the mail header, body, and attachments of each email to generate a score. If the score crosses a threshold value, the mail is considered as spam. Anti-Spam refers to this database to identify emails and takes action on them.





### Enable Sender Policy Framework (SPF) check

SPF is a world standard framework adopted by eScan to prevent hackers from forging sender addresses. It acts as a powerful mechanism for controlling phishing mails. Select this checkbox if you want Anti-Spam to check the SPF record of the sender's domain. However, your computer should be connected to the Internet for this option to work.

### Enable Spam URI Real-time Blacklist (SURBL) check

Select this option if you want Anti-Spam to check the URLs in the message body of an email. If the URL is listed in the SURBL site, the email will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.

### Enable Real-time Blackhole List (RBL) check

Select this option if you want Anti-Spam to check the sender's IP address in the RBL sites. If the sender IP address is blacklisted in the RBL site, the email will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.

### **RBL Servers**

RBL is a DNS server that lists IP addresses of known spam senders. If the IP of the sender is found in any of the blacklisted categories, the connection is terminated. The RBL Servers list contains addresses of servers and sites that maintain information regarding spammers. You can add or delete address in the list as per your requirement.

### **Auto Spam Whitelist**

Unlike normal RBLs, SURBL scans emails for names or URLs of spam websites in the message body. It terminates the connection if the IP of the sender is found in any of the blacklisted categories. This contains a list of valid email addresses that can bypass the above Spam filtering options. It thus allows emails from the whitelist to be downloaded to the recipient's inbox. You can add or delete address in the list as per your requirement.

### **Mail Tagging Options**

Anti-Spam also includes some mail tagging options, which are described as follows:

### Do not change email at all

Select this option if you want to prevent Anti-Spam from adding the [Spam] tag to emails that have been identified as spam.





## Both subject and body are changed: [Spam] tag is added in Subject: Actual spam content is embedded in Body

This option lets you identify spam emails. When you select this option, Anti-Spam adds a [Spam] tag in the subject line and the body of the email that has been identified as spam.

### "X MailScan Spam: 1" header line is added: Actual spam content is embedded in Body

This option lets you add a [Spam] tag in the body of the email that has been identified as spam. In addition, it adds a line in the header line of the email.

### Only [Spam] tag is added in Subject: Body is left unchanged [Default]

This option lets you add the [Spam] tag only in the subject of the email, which has been identified as spam.

## "X MailScan Spam: 1" header line is added: Body and subject both remain unchanged

This option lets you add a header line to the email. However, it does not add any tag to the subject line or body of the email.





### **Web Protection**

Web Protection module scans the website content for specific words or phrases. It lets you block websites containing pornographic or offensive content. Administrators can use this feature to prevent employees from accessing non-work related websites during preferred duration.

| We | Protection                        |                |               |            |             |                |                        | 🝸 Help         |
|----|-----------------------------------|----------------|---------------|------------|-------------|----------------|------------------------|----------------|
| ۲  | Start Stop                        |                |               |            |             | Start Phishing | ) Filter 🔲 Start Malwa | are URL Filter |
| ſ  | Filtering Options Scanning Option | ons Define     | Time-Restrict | ion        |             |                |                        |                |
|    | Status     Active                 |                |               |            |             | O Block Web A  | Access                 |                |
| Γ  | Filter Categories                 | Allow          | Block         |            | Site Names  |                |                        |                |
|    | Category Name                     | <u>Type</u>    | <u>Status</u> |            | playboy.con | n              |                        | <b>^</b>       |
|    | Pornography                       | Block 🔻        | Customize     |            |             |                |                        |                |
|    | Gambling                          | Block <b>T</b> | Customize     |            |             |                |                        |                |
|    | Alcohol                           | Block V        | Customize     |            |             |                |                        |                |
|    | Violence                          | Block <b>T</b> | Customize     |            |             |                |                        |                |
|    | Drugs                             | Block V        | Customize     |            |             |                |                        |                |
|    | Ratings block category            | Block V        | Customize     | <b>]</b> • |             |                |                        | -              |
|    | Add Delete                        |                |               |            | Add         | Delete         | Save                   |                |
|    | Filtering Options                 | k category     |               |            |             |                |                        |                |
|    | Default Advanced Setting          | ОК             | Cancel        |            |             |                |                        |                |

You can configure the following settings.

### **Filtering Options**

This tab has predefined categories that help you control access to the Internet.

### Status

This section lets you allow or block access to specific websites based on Filter Categories. You can set the status as **Active** or **Block** web access. Select the **Block Web Access** option if you want to block all the websites except the ones that have been listed in the **Filter Categories**. When you select this option, only **Filtering Options** and **Pop-up Filter** tabs are available.





### **Filter Categories**

This section uses the following color codes for allowed and blocked websites.

### Green

It represents an allowed websites category.

### Red

It represents a blocked websites category.

The filter categories used in this section include categories like Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings\_block\_category, Websites Allowed, etc. You can also add or delete filter categories depending on your requirement.

### **Category Name**

This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category. You can also add or delete filter categories depending on your requirement.

### **Filter Options**

This section includes the **Add sites rejected by the filter to Block category checkbox**. Select this option if you want eScan to add websites that are denied access to the Block category database automatically.

### **Scanning Options**

This tab lets you enable log violations and shutdown program if it violates policies. It also lets you specify ports that need monitoring.

| Web Protection   | 👔 Help   |
|--|--|
| Start     Stop   | 🔲 Start Phishing Filter 🔲 Start Malware URL Filter                       |
| Filtering Options       Scanning Options       Define Time-Restriction         Actions       Image: Construction of the second s | Port Setting<br>Internet Access (HTTP Port)<br>80,8080,3128,6588,4480,88 |
| Default Advanced Setting OK Cancel   |  |

### Actions

This section lets you select the actions that eScan should perform when it detects a security violation.





### Log Violations [Default]

This checkbox is selected by default. Select this option if you want Web Protection to log all security violations for your future reference.

### Shutdown Program in 30 Secs

Select this option if you want Web Protection to shut down the browser automatically in 30 seconds when any of the defined rules or policies is violated.

### **Port Setting**

This section lets you specify the port numbers that eScan should monitor for suspicious traffic.

### **Internet Access (HTTP Port)**

Web browsers commonly use the port numbers 80, 8080, 3128, 6588, 4480, and 88 for accessing the Internet. You can add port numbers to the **Internet Access (HTTP Port)** box to monitor the traffic on those ports.

### **Define Time Restriction**

This section lets you define policies to restrict access to the Internet.



### **Enable Time Restrictions for Web Access**

Select this option if you want to set restrictions on when a user can access the Internet. By default, all the fields appear dimmed. The fields are available only when you select this option.

The time restriction feature is a grid-based module. The grid is divided into columns based on the days of the week vertically and the time interval horizontally.





### Active

Click **Active** and select the appropriate grid if you want to keep web access active on certain days for a specific interval.

### Inactive

Select this option if you want to keep web access inactive on certain days for a specific interval.

### **Block Web Access**

Select this option if you want to block web access on certain days for a specific interval.

### **Phishing and Malware URL Filter**

Under Web Protection eScan also provides options to enable Phishing and Malware filters which will detect and prevent any phishing attempts on the system and block all malware attacks.

To enable the filters, select **Start** and then select the respective checkboxes.

| Web Protection | 👔 Help                |
|----------------|-----------------------|
| Start Stop     | Start Phishing Filter |

### **Advanced Settings**

Clicking **Advanced** displays Advanced Settings.

|     | Name  | Value |
|-----|---|-------|
| (m) | Ignore IP address from Web-scanning   |       |
| -   | Enable Unknown Browsers detection   | 1 -   |
|     | Enable allowing of WhiteListed Site during BlockTime                        | 1 -   |
|     | Enable Online Web-Scanning Module   | 2 👻   |
| 1   | Disable Web Warning Page  | 0 -   |
|     | Enable HTTPS Popup  | 1 -   |
|     | Show External Page for Web blocking (Page to be define under External Page) | 0 🗸   |
|     | External Page Link for Web blocking (Depends on Show External Page)         |       |
|     | Force inclusion of Application into Layer scanning (MW Layer)               |       |
|     | Enable HTTP Popup   | 0 🗸   |
|     | Ignore Reference of sub-link  | 0 💌   |
|     | Allow access to SubDomain for Whitelisted sites(Only HTTP Sites)            | 1 -   |
|     | Allow access to SubDomain for Whitelisted sites(Only HTTPS Sites)           | 1 -   |
| -   | Enable logging of visited websites  | 1 -   |
|     | Block EXE download from HTTP Sites  | 0     |

### Ignore IP address from Web-scanning

Select this option to enable/disable to ignore IP address from web-scanning

### Enable Unknown Browsers detection (1 = Enable/0 = Disable)

Select this option to enable/disable enable unknown browsers detection

### Enable allowing of WhiteListed Site during BlockTime (1 = Enable/0 = Disable)

Select this option to enable/disable enable allowing of whitelisted site during blocktime





### Enable Online Web-Scanning Module (1 = Enable/0 = Disable)

Select this option to enable/disable enable online web-scanning module

### Disable Web Warning Page (1 = Enable/0 = Disable)

Select this option to enable/disable to disable web warning page

### Enable HTTPS Popup (1 = Enable/0 = Disable)

Select this option to enable/disable HTTPS pop-ups.

### Show External Page for Web blocking (Page to be define under External Page)

Select this option to enable/disable to show external page for web blocking

### External Page Link for Web blocking (Depends on Show External Page)

Select this option to enable/disable external page link for web blocking

### Force inclusion of Application into Layer scanning (MW Layer)

Select this option to enable/disable the force inclusion of application into layer scanning.

### Enable HTTP Popup (1 = Enable/0 = Disable)

Select this option to enable/disable HTTP pop-ups.

### Ignore Reference of sub-link(1 = Enable/0 = Disable)

Select this option to enable/disable ignore the reference of sublink.

## Allow access to SubDomain for Whitelisted sites(Only HTTP Sites) (1 = Enable/0 = Disable)

Select this option to enable/disable acess to the subdomain for whitelisted sites for HTTP sites

## Allow access to SubDomain for Whitelisted sites(Only HTTPS Sites) (1 = Enable/0 = Disable)

Select this option to enable/disable acess to the subdomain for whitelisted sites for HTTPS sites

### Enable logging of visited websites (1 = Enable/0 = Disable)

Select this option to enable/disable the logging of visited websites.

### Block EXE download from HTTP Sites (1 = Enable/0 = Disable)

Select this option to enable/disable block download of .exe files from HTTP websites.

### **Block HTTP Traffic only on Web Browser**

Select this option to enable/disable block the HTTP Traffic on web browers.

### Allow website list (Depends on "Block HTTP Traffic only on Web Browser")

Select this option to enable/disable to allow the website list. This depends on **Block HTTP Traffic only on Web Browser** option.

### Block Microsoft EDGE Browser (1 = Enable/0 = Disable)

Select this option to enable/disable blocking Microsoft Edge broser.

### Enable Web Protection using Filter driver (1 = Enable/0 = Disable)





Select this option to enable/disable web protection using filter driver.

### Force Disable Web Protection using Filter driver (1 = Enable/0 = Disable)

Select this option to force enable/disable web protection using filter driver.

### WFP Exclude IP List (1 = Enable/0 = Disable)

Select this option to enable/disable excluding IP list from Web Filter Protection.





### **Firewall**

Firewall module is designed to monitor all incoming and outgoing network traffic and protect your computer from all types of network based attacks. eScan includes a set of predefined access control rules that you can remove or customize as per your requirements. These rules enforce a boundary between your computer and the network. Therefore, the Firewall feature first checks the rules, analyzes network packets, and filters them on the basis of the specified rules. When you connect to the Internet, you expose your computer to various security threats.

| Fir | e Wall  |                                |          | <sub>?</sub> Help |
|-----|---|--------------------------------|----------|-------------------|
| ۲   | Allow All   O Limited Filter   O Interactive Filter   |                                |          |                   |
|     | Zone Rule Expert Rule Trusted MAC Address   | Local IP List Application Rule |          |                   |
|     | Name  | IP Address/Host Name           | Туре     | Zone              |
|     | Allow Local Network 192.168.*.*   | 192.168.0.1-192.168.254.254    | IP Range | Trusted           |
|     | Add Host Name       Add IP       Add IP Ran         Show Application Alert         Default Rules       Advanced Setting       OK       Ca | ge Modify Remove               |          |                   |

The Firewall feature of eScan protects your data when you:

- Connect to Internet Relay Chat (IRC) servers and join other people on the numerous channels on the IRC network.
- Use Telnet to connect to a server on the Internet and then execute the commands on the server.
- Use FTP to transfer files from a remote server to your computer.
- Use Network Basic Input Output System (NetBIOS) to communicate with other users on the LAN connected to the Internet.
- Use a computer that is a part of a Virtual Private Network (VPN).
- Use a computer to browse the Internet.
- Use a computer to send or receive email.





By default, the firewall operates in the **Allow All** mode. However, you can customize the firewall by using options like **Limited Filter** for filtering only incoming traffic and **Interactive Filter** to monitor incoming and outgoing traffic. The eScan Firewall also lets you specify different set of rules for allowing or blocking incoming or outgoing traffic. These rules include Zone Rules, Expert Rules, Trusted Media Access Control (MAC) Address, and Local IP list. This page provides you with options for configuring the module. You can configure the following settings to be deployed to the eScan client systems.

**Allow All** – Clicking **Allow All** disables the eScan Firewall i.e. all the incoming and outgoing network traffic will not be monitored/filtered.

**Limited Filter** – Clicking **Limited Filter** enables eScan Firewall in limited mode which will monitor all incoming traffic only and will be allowed or blocked as per the conditions or rules defined in the Firewall.

**Interactive** - Clicking **Interactive** enables eScan Firewall to monitor all the incoming and outgoing network traffic and will be allowed or blocked as per the conditions or rules defined in the Firewall.

Following tabs are available:

- Zone Rule
- Expert Rule
- Trusted MAC Address
- Local IP List
- Application Rule

### **Zone Rule**

This is a set of network access rules to make the decision of allowing/blocking of the access to the system. This will contain the source IP address or source Host name or IP range either to be allowed or blocked.

Buttons (to configure a zone rule)

**Add Host Name** – This option lets you add a "host" in the zone rule. After clicking **Add Host Name**, enter the HOST name of the system, select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the zone rule.

**Add IP** – This option lets you add an IP address of a system to be added in the zone rule. After clicking **Add IP**, enter the IP address of the system, select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the Zone Rule.

**Add IP Range** – This option lets you add an IP range to be added in the zone rule. After clicking **Add IP Range**, add the IP Range (i.e. a range of IP that the zone rules should be applied), select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the zone rule.

**Modify** – To modify/change any listed zone rule (s), select the zone rule to be modified and click **Modify**.

Remove - To remove any listed zone rule (s), select the zone rule and click Remove.





### **Expert Rule**

This tab lets you specify advanced rules and settings for the eScan firewall. You can configure expert rules on the basis of the various rules, protocols, source IP address and port, destination IP address and port, and ICMP types. You can create new expert rules. However, configure these rules only if you are familiar with firewalls and networking protocols.

- Source IP Address/Host Name
- Source Port Number
- Destination IP Address/Host Name
- Destination Port Number

### Buttons (to configure an Expert Rule)

1. Add – Click Add to create a new Expert Rule. In the Add Firewall Rule Window:

| General Source       | Destination | Advanced      |  |
|----------------------|-------------|---------------|--|
| Rule Name            |             |               |  |
| Rule1                |             |               |  |
| Rule Action          |             |               |  |
| Permit Packet        | (           | 🔍 Deny Packet |  |
| Apply Rule on Interf | ace         |               |  |
|                      |             |               |  |
|                      |             |               |  |
|                      |             |               |  |
|                      |             |               |  |




#### **General tab**

In this section, specify the Rule settings

Rule Name – Provide a name to the Rule.

Rule Action – Action to be taken, whether to Permit Packet or Deny Packet.

**Protocol** – Select the network protocol (e.g. TCP, UDP, ARP) on which the Rule will be applied.

**Apply rule on Interface** – Select the Network Interface on which the Rule will be applied.

#### Source tab

In this section, specify/select the location from where the outgoing network traffic originates.

**My Computer** – The rule will be applied for the outgoing traffic originating from your computer.

**Host Name** – The rule will be applied for the outgoing traffic originating from the computer as per the host name specified.

**Single IP Address** – The rule will be applied for the outgoing traffic originating from the computer as per the IP address specified.

**Whole IP Range** – To enable the rule on a group of computers in series, you can specify a range of IP address. The rule will be applied for the outgoing traffic from the computer(s) which is within the defined IP range.

**Any IP Address** – When this option is selected, the rule will be applied for the traffic originating from ANY IP address.

**Any** – When this option is selected, the rule gets applied for outgoing traffic originating from any port.

**Single Port** – When this option is selected, the rule gets applied for the outgoing traffic originating from the specified/defined port.

**Port Range** – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the outgoing traffic originating from the port which is within the defined range of ports.

**Port List** – A list of port can be specified. The rule will be applied for the outgoing traffic originating from the ports as per specified in the list.

**NOTE** The rule will be applied when the selected Source IP Address and Source Port matches together.





#### **Destination tab**

In this section, specify/select the location of the computer where the incoming network traffic is destined.

#### **Destination IP Address –**

**My Computer** – The rule will be applied for the incoming traffic to your computer.

**Host Name** – The rule will be applied for the incoming traffic to the computer as per the host name specified.

**Single IP Address** – The rule will be applied for the incoming traffic to the computer as per the IP address specified.

**Whole IP Range** – To apply the rule on a group of computers in series, you can specify a range of IP address. The rule will be applied for the incoming traffic to the computer(s) which is within the defined IP range.

**Any IP Address** – When this option is selected, the rule will be applied for the incoming traffic to ANY IP Addresses.

**Any** – After selecting this option, the rule will be applied for the incoming traffic to ANY port.

**Single Port** – After selecting this option, the rule will be applied for the incoming traffic to the specified/defined port.

**Port Range** – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the incoming traffic to the port which is within the defined range of ports.

**Port List** – A list of port can be specified/added. The rule will be applied for incoming traffic originating from the ports as per specified in the list.

NOTEThe rule will be applied when the selected Destination IP Address and DestinationNOTEPort matches together.





#### Advanced tab

This tab contains advance setting for Expert Rule.

| I     I       Destination Unreachable     I       Echo Reply (ping)     I       Echo Request (ping)     I       Information Reply     I | in | Out |
|---|----|-----|
| Destination Unreachable Echo Reply (ping) Echo Request (ping) Information Reply Information Reply Information Reply Information Reguest |    |     |
| Echo Reply (ping) Echo Request (ping) Information Reply Information Reply   | _  |     |
| Echo Request (ping)   |    |     |
| Information Reply   |    |     |
| Information Request   |    |     |
| information Request   |    |     |
| Parameter Problem   |    |     |
| Redirect  |    |     |
| Source Quench   |    |     |
| TTL Exceeded  |    |     |

**Enable Advanced ICMP Processing -** This is activated when the ICMP protocol is selected in the **General** tab.

**The packet must be from/to a trusted MAC address** – When this option is selected, the rule will only be applied on the MAC address defined/listed in the Trusted MAC **Address** tab.

**Log information when this rule applies** – This will enable to log information of the Rule when it is implied.

Modify – Clicking Modify lets you modify any Expert Rule.

**Remove** – Clicking **Remove** lets you delete a rule from the Expert Rule.

**Shift Up and Shift Down**– The UP and DOWN arrow button will enable to move the rules up or down as required and will take precedence over the rule listed below it.

**Enable Rule / Disable Rule** – These buttons lets you enable or disable a particular selected rule from the list.





### **Trusted MAC Address**

This section contains the information of the MAC address of the system. A MAC address is a hardware address that uniquely identifies each node of a network. The Trusted MAC address list will be checked along with the Expert Rule only when "The packet must be from/to a trusted MAC address" option is checked and the action will be as per specified in the rule. (Refer to the Advance Tab of the Expert Rule). Buttons (to configure the Trusted MAC Address)

**Add** – To add a MAC address click on this button. Enter the MAC address to be added in the list for e.g. 00-13-8F-27-00-47

Edit – To modify/change the MAC Address, click Edit.

Remove – To delete the MAC Address, click Remove.

Clear All – To delete the entire listed MAC Address, click Clear All.

### Local IP List

This section contains a list of Local IP addresses.

| one Rule Expe    | rt Rule Trusted MAC Ad  | Idress Local IP Lis | Application Rule |  |  |
|------------------|-------------------------|---------------------|------------------|--|--|
| 0000:0000:0000:0 | 000:0000:0000:0000:0001 |                     |                  |  |  |
| 127.*.*.*        |                         |                     |                  |  |  |
| 192.168.*.*      |                         |                     |                  |  |  |
|                  |                         |                     |                  |  |  |
|                  | Remove                  | Clear All           |                  |  |  |

Add – To add a local IP address, click Add.

**Remove –** To remove a local IP address, click **Remove**.

Clear All – To clear all local IP addresses, click Clear All.

Default List – To load the default list of IP addresses, click Default List.





# **Application Rule**

In this section you can define the permissions for different application. The application can be set to Ask, Permit or Deny mode.

| Zone Rule Expert Rule Tr       | usted MAC Address Local IP List | Application Rule |        |
|--------------------------------|---------------------------------|------------------|--------|
| Application                    | Description                     | Path             | Access |
|                                |                                 |                  |        |
|                                |                                 |                  |        |
|                                |                                 |                  |        |
|                                |                                 |                  |        |
|                                |                                 |                  |        |
|                                |                                 |                  |        |
|                                |                                 |                  |        |
| Add Rem                        | Clear All                       |                  |        |
| Show Application Alert         |                                 |                  |        |
| Default Rules Advanced Setting | OK Cancel                       |                  |        |

#### Defining permission for an application

To define permission for an application, follow the steps given below:

1. Click Add. Add New Application window appears.

| Add New Applicatio | n         |        |
|--------------------|-----------|--------|
| Application name   | with path |        |
| Ask                | Permit    | O Deny |
| OK Can             | icel      |        |

- 2. Enter the application name with path and select a permission.
- 3. Click **OK**.

The permission for the application will be defined.

#### Removing permission of an application

Select an application and click **Remove**. The application will no longer have the permission.





#### **Other Buttons**

- **Clear All** This option will clear/delete all the information stored by the Firewall cache.
- **Show Application Alert** Selecting this option will display an eScan Firewall Alert displaying the blocking of any application as defined in the Application Rule.
- **Default Rules** This button will load/reset the rules to the Default settings present during the installation of eScan. This will remove all the settings defined by user.





# **Endpoint Security**

Endpoint Security module protects your computer or Computers from data thefts and security threats through USB or FireWire® based portable devices. It comes with Application Control feature that lets you block unwanted applications from running on your computer. In addition, this feature provides you with a comprehensive reporting feature that lets you determine which applications and portable devices are allowed or blocked by eScan.

| ication Control Device Control          | DLP (Attachment Control) |        |
|---|--------------------------|--------|
| Reach List White List Define            | Time Destrictions        |        |
| Enter Application to Block              | The Restretons           |        |
|   |                          |        |
| List of Blocked Applications            |                          | Block  |
| + Custom Group                          | Allow This Group         | Import |
| + Computer Game                         | Allow This Group         | Delete |
| + Instant Messengers                    | Allow This Group         |        |
| <ul> <li>Music Video Players</li> </ul> | Allow This Group         |        |
| + P2P Applications                      | Allow This Group         |        |
|   |                          |        |
|   |                          |        |
|   |                          |        |
|   |                          |        |
|   |                          |        |
|   |                          |        |

This page provides you with information regarding the status of the module and options for configuring it.

• **Start/Stop:** It lets you enable or disable Endpoint Security module. Click the appropriate option.

There are two tabs – Application Control and USB Control, which are as follows:

# **Application Control**

This tab lets you control the execution of programs on the computer. All the controls on this tab are disabled by default. You can configure the following settings.

#### **Enable Application Control**

Select this option if you want to enable the Application Control feature of the Endpoint Security module.

#### **Block List**

**Enter Application to Block:** It indicates the name of the application you want to block from execution. Enter the full name of the application to be blocked.





#### **List of Blocked Applications**

This list contains blocked executables of applications that are predefined by MicroWorld. Each of the applications listed in the predefined categories are blocked by default. In addition, you can also add executables that you need to block only to the Custom Group category. If you want, you can unblock the predefined application by clicking the **UnBlock** link. The predefined categories include computer games, instant messengers, music & video players, and P2P applications.

#### White List

#### **Enable White Listing**

Select this checkbox to enable the whitelisting feature of the Endpoint Security module.

#### **Enter Application to whitelist**

Enter the name of the application to be whitelisted.

#### White Listed Applications

This list contains predefined whitelisted applications. Each of the applications listed in the predefined categories are allowed by default. If you want to block the predefined categories, select the block option.

#### **Define Time Restrictions**

This option lets you enable/disable application control feature. This feature lets you define time restriction when you want to allow or block access to the applications based on specific days and between pre-defined hours during a day.

For example, the administrator can block computer games, instant messengers, for the whole day but allow during lunch hours without violating the Application Control Policies.

#### **Datewise Restrictions**

This feature lets you define datewise restrictions when you want to allow or block access to the applications based on specific dates and between pre-defined hours during that date.





# **Device Control**

The Endpoint Security module protects your computer from unauthorized portable storage devices prompting you for the password whenever you plug in such devices. The devices are also scanned immediately when connected to prevent any infected files running and infecting the computer.

| EndPoint Security   | 👔 Help |
|---|--------|
| Start     Stop  |        |
| Application Control Dury (Attachment Control)   |        |
|   |        |
|   |        |
| Block USB Ports Ask for Password  |        |
| Use eScan Administrator Password     Use Other Password   |        |
| Do Virus Scan     Allow user to cancel scan     Read Only - USB     Disable AutoPlay  |        |
| Record Files Copied To USB / CD     Record Files Copied To USB / CD     Record Files Copied To USB / CD     Ignore System Drive                   |        |
| Serial No.         Device Name         Description           Import         Edit           Delete         RemoveAll           Print         Print |        |
| Disable Web Cam     Disable Bluetooth     Disable SD Cards  |        |
| CD / DVD Settings<br>Block CD / DVD Read Only - CD / DVD  |        |
| Default Advanced Setting OK Cancel  |        |

You can configure the following settings:

#### Enable Device Control [Default]

Select this option if you want to monitor all the USB storages devices connected to your endpoint. This will enable all the options on this tab.





#### **USB Settings**

This section lets you customize the settings for controlling access to USB storage devices.

#### **Block USB Ports**

Select this option if you want to block all the USB storage devices from sharing data with endpoints.

#### **Ask for Password**

Select this option, if you want eScan to prompt for a password whenever a USB storage device is connected to the computer. You have to enter the correct password to access USB storage device. It is recommended that you always keep this checkbox selected.

#### **Use eScan Administrator**

This option is available only when you select the **Ask for Password** checkbox. Click this option if you want to assign eScan Administrator password for accessing USB storage device.

#### **Use Other Password**

This option is available only when you select the **Ask for Password** checkbox. Click this option if you want assign a unique password for accessing USB storage device.

#### Do Virus Scan [Default]

When you select this option, the Endpoint Security module runs a virus scan if the USB storage device is connected. It is recommended that you always keep this checkbox selected.

#### Allow user to cancel scan

Select this option to allow the user to cancel the scanning process of the USB device.

#### Disable AutoPlay [Default]

When you select this option, eScan disables the automatic execution of any program stored on a USB storage device when you connect the device.

#### **Read Only USB**

Select this option if you want to allow access of the USB device in read-only mode.

#### **Record Files Copied To USB**

Select this option if you want eScan to create a record of the files copied from the system to USB drive.

#### **Record Files Copied To Network**

Select this option if you want eScan to create a record of the files copied from managed computers to the network drive connected to it.

#### **Record Files Copied To Local**

Select this option if you want eScan to create a record of the files copied from the one drive to another drive of the system. Please note that if you have selected "Ignore System Drive" along with this option no record will be captured if the files are copied from system drive (the drive in which OS is installed) to another drive.





#### **Ignore System Drive**

Select this option in case of you do not want eScan to record files that are copied from system drive of managed computers to either network drive or any local drive.

#### Whitelist

eScan provides a greater level of endpoint security by prompting you for a password whenever you connect a USB drive. To disable password protection for a specific device, you can add it along with its serial number to the whitelist. The next time you connect the device it will not ask for a password but will directly display the files or folders stored on the device. This section displays the serial number and device name of each of the whitelisted devices in a list. You can add devices to this list by clicking **Add**. The Whitelist section displays the following button.

#### Scan Whitelisted USB Devices

By default, eScan does not scan whitelisted USB devices. Select this option, if you want eScan to scan USB devices that have been added to the whitelist.

#### Add

Click Add to whitelist USB devices. USB Whitelist window appears.

| USB W | hitelist          |          |             |        |           |                                       |             |
|-------|-------------------|----------|-------------|--------|-----------|---------------------------------------|-------------|
| -     | <u>Serial No.</u> | <u>]</u> | Device Name |        | Host Name | <u>Client Date and</u><br><u>Time</u> | Description |
| No Re | cord Found        |          |             |        |           |                                       |             |
|       |                   |          |             |        |           |                                       |             |
|       |                   |          |             |        |           |                                       |             |
|       |                   |          |             |        |           |                                       |             |
|       |                   |          |             |        |           |                                       |             |
|       |                   |          |             |        |           |                                       |             |
|       |                   |          |             |        |           |                                       |             |
|       |                   |          |             |        |           |                                       |             |
|       |                   |          |             |        |           |                                       |             |
|       |                   |          |             |        |           |                                       |             |
|       |                   | OK       | Cancel      | Custom | Edit      |                                       |             |

To whitelist a USB device, its details are required. If a USB device is connected to any eScan installed endpoint, the USB details are sent to the server. The administrator will have to manually whitelist the USB device.





To manually add a USB device in USB Whitelist without connecting to an endpoint, click **Custom**.

|               | × |
|---------------|---|
| USB Whitelist |   |
| Serial No.    |   |
| Device Name   |   |
| Description   |   |
| OK Cancel     |   |

Enter the USB details and click **OK**. The USB device will be added and whitelisted.

#### Import

To whitelist USB devices from a csv file, click **Import**. Click **Choose File** to import the file with the list. The list should be in following format: Serial No 1, Device Name 1, Device Description 1(Optional) Serial No 2, Device Name 2 **Eg:** SDFSD677GFQW8N6CN8CBN7CXVB, USB Drive 2.5, Whitelist by xyzDFRGHHRS54456HGDF347OMCNAK, Flash Drive 2.2

**Disable Web Cam**: Select this option to disable Webcams. **Disable SD Cards**: Select this option to disable SD cards. **Disable Bluetooth**: Select this option to disable Bluetooth.

**Block CD / DVD:** Select this option to block all CD/DVD access. **Read Only - CD / DVD:** Select this option to allow read-only access for CD/DVD.

**NOTE** Click **Default** to apply default settings done during eScan installation. It loads and resets the values to the default settings.





# **DLP (Attachment Control)**

The DLP (Attachment Control) tab lets you control attachment flow within your organization. You can block/allow all attachments the user tries to send through specific processes that can be defined. You can exclude specific domains/subdomains that you trust, from being blocked even if they are sent though the blocked processes mentioned before.

| Арр | ication Control Device Control DLP (Attachment Control)                         |
|-----|---|
|     |   |
|     | Attachment Allowed  |
|     | Attachment Blocked  |
|     | Enter Process Name : <b>Eg.</b> Thunderbird.exe                                 |
|     |   |
|     | Add Delete  |
|     | Blacklisted Process   |
|     |   |
|     |   |
|     | • • • • • • • • • • • • • • • • • • •   |
|     |   |
|     | Attachments will be allowed from below sites irrespective of the above settings |
|     | Enter Site Name - En Gmail com Yahoo  |
|     |   |
|     | Add Delete  |
|     | Whitelisted sites   |
|     |   |
|     |   |
|     |   |
|     |   |

You can configure the following settings:

#### **Attachment Allowed**

Select this option if you want attachments to be allowed through all processes except a specific set of processes mentioned below.

#### **Attachment Blocked**

Select this option if you want attachments to be blocked through all processes except a specific set of processes mentioned below.





#### **Enter Process Name**

Enter the name of the processes that should be excluded from the above selection.

#### **Blacklisted Process**

This will display a list of process you excluded when you selected the **Attachment Allowed** option. eScan will block all attachments through this process.

#### **Whitelisted Process**

This will display a list of process you excluded when you selected the **Attachment Blocked** option. eScan will allow all attachments through this process.

#### **Enter Site Name**

Enter the name of the websites through which attachments should be allowed irrespective of the above settings.

#### **Whitelisted Sites**

The websites added above to be whit listed are displayed in this list.

### **Advanced Settings**

| Name  | Value |  |
|---|-------|--|
| Allow Composite USB Device                                    | 1 .   |  |
| Allow USB Modem   | 1 .   |  |
| Enable Predefined USB Exclusion for Data Outflow              | 1 .   |  |
| Enable CD/DVD Scanning  | 1.    |  |
| Enable USB Whitelisting option on prompt for eScan clients    | 0 🔻   |  |
| Enable USB on Terminal Client                                 | 1.    |  |
| Enable Domain Password for USB                                | 0 .   |  |
| Show System Files Execution Events                            | 0 🔻   |  |
| Allow mounting of Imaging device                              | 1 .   |  |
| Block File Transfer from IM                                   | 1 .   |  |
| Allow WIFI Network  | 1 .   |  |
| Whitelisted WIFI SSID (Comma Separated)                       |       |  |
| Allow Network Printer   | 1 .   |  |
| Whitelisted Network Printer list(Comma Separated)             |       |  |
| Disable Print Screen  | 0 .   |  |
| Allow eToken Devices  | 1     |  |
| Include File Extension for File Activity Monitoring (e.g EXE) |       |  |

#### Allow Composite USB Device (1 = Enable/0 = Disable)

Select this option to allow/block use of composite USB devices.

#### Allow USB Modem (1 = Enable/0 = Disable)

Select this option to allow/block use of USB modem.

#### Enable USB on Terminal Client (1 = Enable/0 = Disable)

Select this option to enable/disable USB on terminal client.





Allow mounting of Imaging device (1 = Enable/0 = Disable) Select this option to allow/block mounting of imaging devices.

**Block File Transfer from IM (1 = Enable/0 = Disable)** Select this option to allow/block file transfer from Instant Messengers.

**Allow Wi-Fi Network (1 = Enable/0 = Disable)** Select this option to allow/block use of Wi-Fi networks.

Allow Network Printer (1 = Enable/0 = Disable) Select this option to allow/block use of network printers.

Allow eToken Devices (1 = Enable/0 = Disable) Select this option to allow/block use of eToken devices.





# **Privacy Control**

Privacy Control module protects your confidential information from theft by deleting all the temporary information stored on your computer. This module lets you use the Internet without leaving any history or residual data on your hard drive. It erases details of sites and web pages you have accessed while browsing. This page provides you with options for configuring the module.

| ivacy Control  |  | <b>?</b>                        |
|--|--|---------------------------------|
| General Advanced   |  |                                 |
| Scheduler Options  |  |                                 |
| You can set to run this Tool Automatically<br>Options Below. | at Various times. Select the times you would | like Auto Erase to run from the |
| Run at System Startup  | Run Everyday at 0:00 am                      | 0-                              |
| Auto Erase Options   | Clear Last Search Menu                       | Clear Carbe                     |
| Clear Last Run Menu  | Clear Recent Documents                       | Clear Cookies                   |
| Clear Temporary Folders                                      | Clear Files & Folders                        | Clear Plugins                   |
| Clear Last Find Computer                                     | Clear Open/Save Dialog Box History           | Clear ActiveX                   |
| Clear Browser Address Bar History                            | Empty Recycle Bin                            | Clear History                   |
|  |  | Select All                      |
|  |  |                                 |
|  |  |                                 |
| Default OK Capaci  |  |                                 |
| Default OK Califee   |  |                                 |

It consists following tabs:

- General
- Advanced

### **General tab**

This tab lets you specify the unwanted files created by web browsers or other installed software that should be deleted. You can configure the following settings:

#### **Scheduler Options**

You can set the scheduler to run at specific times and erase private information, such as your browsing history from your computer. The following settings are available in the **Scheduler Options** section.

#### **Run at System Startup**

It auto executes the Privacy Control module and performs the desired auto-erase functions when the computer starts up.





#### Run Every day at

It auto-executes the Privacy Control module at specified times and performs the desired auto erase functions. You can specify the time within the hours and minutes boxes.

#### **Auto Erase Options**

The browser stores traceable information of the websites that you have visited in certain folders. This information can be viewed by others. eScan lets you remove all traces of websites that you have visited. To do this, it auto detects the browsers that are installed on your computer. It then displays the traceable component and default path where the temporary data is stored on your computer. You can select the following options based on your requirements.

#### **Clear Auto Complete Memory**

Auto Complete Memory refers to the suggested matches that appear when you enter text in the Address bar, the Run dialog box, or forms in web pages. Hackers can use this information to monitor your surfing habits. When you select this checkbox, Privacy Control clears all this information from the computer.

#### **Clear Last Run Menu**

When you select this option, Privacy Control clears this information in the Run dialog box.

#### **Clear Temporary Folders**

When you select this option, Privacy Control clears files in the Temporary folder. This folder contains temporary files installed or saved by software. Clearing this folder creates space on the hard drive of the computer and boosts the performance of the computer.

#### **Clear Last Find Computer**

When you select this option, Privacy Control clears the name of the computer for which you searched last.

#### **Clear Browser Address Bar History**

When you select this checkbox, Privacy Control clears the websites from the browser's address bar history.

#### **Clear Last Search Menu**

When you select this option, Privacy Control clears the name of the objects that you last searched for by using the Search Menu.

#### **Clear Recent Documents**

When you select this checkbox, Privacy Control clears the names of the objects found in Recent Documents.

#### **Clear Files & Folders**

When you select this checkbox, Privacy Control deletes selected Files and Folders. Use this option with caution as it permanently deletes unwanted files and folders from the computer to free space on the computer.





#### Clear Open/Save Dialog box History

When you select this checkbox, Privacy Control clears the links of all the opened and saved files.

#### **Empty Recycle Bin**

When you select this checkbox, Privacy Control clears the Recycle Bin. Use this option with caution as it permanently clears the recycle bin.

#### **Clear Cache**

When you select this checkbox, Privacy Control clears the Temporary Internet Files.

#### **Clear Cookies**

When you select this checkbox, Privacy Control clears the Cookies stored by websites in the browser's cache.

#### **Clear Plugins**

When you select this checkbox, Privacy Control removes the browser plug-in.

#### **Clear ActiveX**

When you select this checkbox, Privacy Control clears the ActiveX controls.

#### **Clear History**

When you select this checkbox, Privacy Control clears the history of all the websites that you have visited. In addition to these options, the **Auto Erase Options** section has many options.

#### Select All/ Unselect All

Click this button to select/unselect all the auto erase options.





# Advanced tab

This tab lets you select unwanted or sensitive information stored in MS Office, other Windows files and other locations that you need to clear.

| - MS Office   | k Temp Files Others Windows Media Player Play List |
|---|--|
| MS PowerPoint     Start Menu Order Hist       MS FrontPage     Registry Streams MRL       MS Access     Application Log | (Most recently used)                               |
|   | Select All   |

#### **MS Office**

The .msi extension files will be cleared if these options are selected.

#### Windows

The respective unwanted files like temp files will be cleared.

#### Others

The unwanted files in the Windows media player will be cleared.

**NOTE** Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.





# **Administrator Password**

Administrator Password lets you create and change password for administrative login of eScan protection center and Two-Factor Authentication.

### eScan Password

It also lets you keep the password as blank, wherein you can login to eScan protection center without entering any password for read-only access.

| Add/Change Password               | 🝸 Help         |
|-----------------------------------|----------------|
| eScan Password Two-Factor Authent | ication        |
| Set Password                      | Blank Password |
| Enter new Password                |                |
| Confirm new Password              |                |
| Password is case-sensitive        |                |
| Use separate uninstall password   |                |
| Enter uninstall password          |                |
| Confirm uninstall password        |                |
|                                   |                |
|                                   |                |
| Derault Advanced Setting OK       | Cancel         |

There is also an option to set a uninstall password. An uninstallation password prevents personnels from uninstalling eScan client from their endpoint. Upon selecting Uninstall option, eScan asks them for uninstall password. To set an uninstall password, select checkbox **Use separate uninstall password**.





# **Two-Factor Authentication**

Your default system authentication (login/password) is Single-Factor Authentication which is considered insecure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your basic system logon. The 2FA feature requires personnel to enter an additional passcode after entering the system login password. So, even if an unauthorized person knows your system credentials, the 2FA feature secures a system against unauthorized logons.

With the 2FA feature enabled, the system will be protected with basic system login and eScan 2FA. After entering the system credentials, eScan Authentication screen (as shown below) will appear. The personnel will have to enter the 2FA passcode to access the system. A maximum of three attempts are allowed to enter the correct passcode. If the 2FA login fails, the personnel will have to wait for 30 seconds to log in again. Read about <u>managing</u> <u>2FA license</u>.

| <b>C</b> eSca | n Authentication          |
|---------------|---------------------------|
|               | Two-Factor Authentication |
| Copyright M   |                           |

To enable the Two-Factor Authentication feature, follow the steps given below:

- 1. In the eScan web console, go to **Managed Computers**.
- 2. Click Policy Templates > New Template.

**NOTE** You can enable the 2FA feature for existing Policy Templates by selecting a Policy Template and clicking **Properties**. Then, follow the steps given below:

- 3. Select Administrator Password check box and then click Edit.
- 4. Click **Two-Factor Authentication** tab.

Following window appears.





| р |
|---|
|   |
|   |
|   |
|   |
|   |
|   |
|   |
|   |
|   |
|   |

5. Select the check box **Enable Two-Factor Authentication**. The Two-Factor Authentication feature gets enabled.

#### **Login Scenarios**

The 2FA feature can be used for following all login scenarios:

#### RDP

RDP stands for Remote Desktop Protocol. Whenever someone takes remote connection of a client's system, the personnel will have to enter system login credentials and 2FA passcode to access the system.

#### Safe Mode

After a system is booted in Safe Mode, the personnel will have to enter system login credentials and 2FA passcode to access the system.

#### Local Logon

Whenever a system is powered on or restarted, the personnel will have to enter system login credentials and 2FA passcode to access the system.

#### Unlock

Whenever a system is unlocked, the personnel will have to enter login credentials and 2FA passcode to access the system.





### **Password Types**

If the policy is applied to a group, the 2FA passcode will be same for all group members. The 2FA passcode can also be set for specific computer(s). You can use following all password types to log in:

#### **Use eScan Administrator Password**

You can use the existing eScan Administrator password for 2FA login. This password can be set in **eScan Password** tab besides the **Two-Factor Authentication** tab.

#### **Use Other Password**

You can set a new password which can be combination of uppercase, lowercase, numbers, and special characters.

#### **Use Online Two-Factor Authentication**

To use this feature, follow the steps given below:

- 1. Install the Authenticator app from Play Store for Android devices or App Store for iOS devices.
- 2. Open the Authenticator app and tap **Scan a barcode**.
- 3. Select the check box **Use Online Two-Factor Authentication**.
- 4. Go to **Managed Computers** and below the top right corner, click **QR code for 2FA**.

A QR code appears.

- 5. Scan the onscreen QR code via the Authenticator app.
  - A Time-based One-Time Password (TOTP) appears on smart device.
- 6. Forward this TOTP to personnel for login.

After selecting the appropriate Login Scenarios and Password Types, click **OK**. The Policy Template gets saved/updated.





# **Advanced Setting**

Clicking **Advanced Setting** displays Advance setting.

| _ |  |              |
|---|--|--------------|
|   | Name   | <u>Value</u> |
|   | Enable Automatic Download  | 1 .          |
|   | Enable Manual Download   | 1 .          |
|   | Enable Alternate Download  | 1 .          |
|   | Set Alternate Download Interval(In Hours)                        | 6            |
|   | Disable download from Internet for Update<br>Agents              | 0 .          |
|   | Stop Auto change for download from Internet for<br>Update Agents | 1 .          |
|   | Enable Download of AntiSpam update first on<br>clients           | 1 .          |
|   | No password for pause protection                                 | 0 •          |

#### Enable Automatic Download (1 = Enable/0 = Disable)

It lets you Enable/Disable Automatic download of Antivirus signature updates.

#### Enable Manual Download (1 = Enable/0 = Disable)

It lets you Enable/Disable Manual download of Antivirus signature updates

#### Enable Alternate Download (1 = Enable/0 = Disable)

It lets you Enable/Disable download of signatures from eScan (Internet) if eScan Server is not reachable.

#### Set Alternate Download Interval (In Hours)

It lets you define time interval to check for updates from eScan (Internet) and download it on managed computers.

#### Disable download from Internet for Update Agents (1 = Enable/0 = Disable)

Selecting this option lets you disable Update Agents from downloading the virus signature from internet.





# Stop Auto change for download from Internet for Update Agents (1 = Enable/0 = Disable)

This option is used when an Update Agent didn't find the primary server to download virus signature, then it tries to get virus signature from internet, so to stop Update Agent from downloading from internet this option is to be set to 1(one).

#### Enable Download of Anti-Spam update first on clients (1 = Enable/0 = Disable)

Normally while updating a system for virus signatures, we first download the anti-virus signature and then anti-spam signature. This option lets you first download Anti-spam updates on clients.

#### No password for pause protection

Selecting this option lets you pause eScan protection without entering password.





# **ODS/Schedule Scan**

**ODS (On Demand Scanning)/Schedule Scan** provides you with various options like – checking for viruses, and making settings for creating logs and receiving alerts. You can also create task in the scheduler for automatic virus scanning.

**NOTE** Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

It consists following tabs:

- Options
- Scheduler

| OD\$/Schedule Scan  |  | ? Hel                |
|---|--|----------------------|
| Options Scheduler<br>Virus Check Alert  |  |                      |
| In the case of an infection:<br>Priority of scanner:<br>File types:<br>Use separate exclude list for ODS: | Automatic<br>Normal (normal runtime)<br>Automatic type recognition<br>Add / Delete | <b>T</b><br><b>T</b> |
| Default Advanced Setting Save   | Cancel   |                      |





# Options

Options tab lets you make the settings for checking viruses and receiving alerts. There are two tabs – Virus Check and Alerts. You can do the following activities.

- Virus check
- Alerts

#### **Virus Check**

It lets you configure the settings for checking viruses.

To set virus check,

- 1. Specify the following field details.
  - In the case of an infection: Select an appropriate option from the dropdown list. For example, Log only, Delete infected file, and [Default] Automatic.
  - Priority of scanner: Select an appropriate option from the drop-down list.
     o For example,
    - High (short runtime)
    - Normal (normal runtime) [Default]
    - Low (long runtime)
  - **File types:** Select an appropriate option from the drop-down list. For example, \[Default\] Automatic type recognition and only program files.
  - Use separate exclude list for ODS: Select this option to add a list of file/folders that should be excluded from scan.
- 2. Click **Save**.

#### Alerts tab

It lets you configure the settings for virus alert. You can also create a log of the infected viruses.

To set alerts,

- 1. Under **Alert** section, Select the [Default] **Warn**, if virus signature is more than x days old checkbox, and then enter the number of days in the x days old field, if you want to receive alerts when virus signature exceeds the specified days. By default, value 3 appears in the field.
- 2. Select the **Warn**, if the last computer analysis was more than x days ago checkbox, and then enter the number of days in the x days ago field, if you want to receive alerts when last computer analysis exceeds the specified days. By default, 3 appears in the field.
- 3. Under **Log Settings** section, select the [Default] **Prepare Log** checkbox, if you want to prepare log of the infected files, and then select an appropriate option.
- 4. Click **Save**.

**NOTE** Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.





# Scheduler

Scheduler tab lets you create/delete various tasks in the scheduler for automatic virus scanning.

| Options | Options Scheduler |                      |            |
|---------|-------------------|----------------------|------------|
| N       | ame               | Schedule             | Next start |
|         |                   |                      |            |
|         |                   |                      |            |
|         |                   |                      |            |
|         |                   |                      |            |
|         | lear All          | Add task Delete task | Edit       |
|         |                   |                      |            |
|         |                   |                      |            |

**NOTE** Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

**Clear All -** This button will clear all the listed tasks.





#### Add Task

|  | ×                 |
|--|-------------------|
| Automatic virus scan   | <sub>?</sub> Help |
| Job Analysis extent Schedule Virus scan  |                   |
| Name 🕑 Active  |                   |
| Start Type<br>Start in foreground Allow user to cancel scan<br>Start in background<br>Quit:<br>Do not quit if virus detected T<br>Scan only when idle Automatically shutdown machine after scan<br>Allow user to delete and to change properties of this job |                   |
| Save Cancel  |                   |

Automatic Virus Scan lets you do following activities:

- a. Creating job
- b. Setting analysis extent
- c. Scheduling virus execution
- d. Scheduling virus scan

#### a) Job

It lets you create the job details for virus scanning.

- 1. Click the **Job** tab.
- 2. Specify the following field details.
  - Name: Enter a name for the task.
  - Active [Default]: Select this checkbox, if you want to allow the client to schedule the task.
  - Start in foreground [Default]: Click this option if you want to view scanning process running in front of you.
     When this option is selected, the Scan only when idle option becomes unavailable.
  - **Start in background**: Click this option if you want scanning process to run in the background. By default, Do not quit if virus is detected option is selected. When you select this option, the Quit drop-down list becomes unavailable.
- 3. Click Save.

#### b) Analysis Extent

It lets you configure analysis extent settings for virus scanning.





| Automatic virus scan   |  |
|--|--|
| Job Analysis extent Schedule Virus scan  |  |
| <ul> <li>Scan Startup</li> <li>Scan memory, registry and services</li> <li>Scan local hard drives</li> <li>Scan System Drive</li> <li>Scan Data Drives</li> <li>Scan network drives</li> </ul> |  |
| Save Cancel  |  |

- 1. Click the **Analysis Extent** tab.
- 2. Select the **Scan Startup** option, if you want to scan all startup entries.
- 3. Select the **Scan memory, registry** and **services** option, if you want to scan memory, registry and services.
- 4. Select the [Default] **Scan local hard drives** option, if you want to scan local hard drives.
- 5. Select Scan network drives option, if you want to scan network drives. Users should note that scanning a network drive may affect system performance.
- 6. Click Save.

#### c) Scheduling

It lets you schedule the date and time of execution for virus scanning.

| Automa | atic virus scan     |   | Help |
|--------|---------------------|---|------|
|        | Job Analysis extent | Schedule Virus scan                     |      |
|        | Execute             |   |      |
|        | Once                | Weekly                                  |      |
|        | Hourly              | Monthly                                 |      |
|        | Daily               | <ul> <li>With system startup</li> </ul> |      |
|        | Date and time       |   |      |
|        | 09/26/2019          | 12:00 pm                                |      |
|        |                     |   |      |
|        |                     |   |      |
|        | Canada and          |   |      |
| Sav    | Cancel              |   |      |

- 1. Click **Schedule** tab.
- 2. Under Execute section, select an appropriate option. For example, [Default] Once, weekly, hourly, and so on.
- 3. Under Date and time section, click the calendar icon. The calendar appears.





4. Select an appropriate date from the calendar.

**NOTE** Click the left < and right > sign to navigate to the previous or next month and year from the calendar respectively.

- 5. Click the Time icon. The Timer appears.
- 6. Click the **AM** tab to view the before noon time and **PM** tab to view the afternoon time, and then select an appropriate time from the list.
- 7. Click **Save**.

#### d) Virus Scan

It lets you schedule virus scanning.

| tomatic virus scan   | <b>1</b>                   |
|--|----------------------------|
| Job Analysis extent Schedule                                 | Virus scan                 |
| In the case of an infection:                                 | Automatic 🔻                |
| Priority of scanner:   | Normal (normal runtime)    |
| File types:  | Automatic type recognition |
| Log Settings     Prepare Log     Only infection to be logged |                            |
| Full log   |                            |
| Save Cancel  |                            |

- 1. Click the **Virus Scan** tab.
- 2. Specify the following field details.
  - In the case of an infection: Select an appropriate option from the dropdown list. For example, Log only, Delete infected file, and [Default] Automatic.
  - Priority of scanner: Select an appropriate priority from the drop-down list.
  - **File types**: Select an appropriate option from the drop-down list. For example, [Default] Automatic type recognition and Only program files.
- 3. Under Log Settings section, select the [Default] Prepare Log checkbox, if you want to prepare log of the infected files, and then click an appropriate option.
- 4. Click Save.

Delete Task – Clicking Delete Task lets you delete the particular task from the list.

Edit – Clicking Edit lets you edit the properties of the particular task from the list.





# MWL (MicroWorld WinSock Layer)

eScan's "MicroWorld-WinSock Layer" (MWL) is a revolutionary concept in scanning Internet traffic on a real-time basis. It has changed the way the world deals with Content Security threats. Unlike the other products and technologies, MWL tackles a threat before it reaches your applications. MWL is technically placed above the WinSock layer and acts as a "Transparent Gatekeeper" on the WinSock layer of the operating system. All content passing through WinSock has to mandatorily pass through MWL, where it is checked for any security violating data. If such data occurs, it is removed and the clean data is passed on to the application.

# **MWL Inclusion List**

Inclusion List contains the name of all executable files which will bind itself to MWTSP.DLL. All other files are excluded.

**NOTE** Click **Default** to apply default settings, done during eScan installation. It loads and resets the values to the default settings.

You can do the following activities.

- Adding files to Inclusion List
- Deleting files from Inclusion List
- Removing all files from Inclusion List

| MWL Inclusion List | 👔 Help    |
|--------------------|-----------|
|                    |           |
| telnet.exe         | Add       |
| msimn.exe          | Delete    |
| outlook.exe        | RemoveAll |
| eudora.exe         |           |
| winpm-32.exe       |           |
| phoenix.exe        |           |
| thebat.exe         |           |
| 🗌 jrew.exe         |           |
| Jre.exe            |           |
| inetinfo.exe       |           |
| Default Ok Cancel  |           |





# **Adding files to Inclusion List**

To add executable files to the Inclusion List, follow the steps given below:

- 1. Enter the executable file name and then click **Add**.
  - The executable file will be added to the Inclusion List.
- 2. Click **OK**.

### **Deleting files from Inclusion List**

To delete executable files from the Inclusion List, follow the steps given below:

- 1. Select executable files, and then click **Delete**. A confirmation prompt appears.
- 2. Click **OK**. The executable file will be deleted from the Inclusion List.

### **Removing all files from Inclusion List**

To remove all executable files from the Inclusion List, follow the steps given below:

1. Click **Remove All**.

A confirmation prompt appears.

2. Click **OK**. All executable files will be removed from the Inclusion List.





# **MWL Exclusion List**

**MWL (MicroWorld WinSock Layer) Exclusion List** contains the name of all executable files which will not bind itself to **MWTSP.DLL**.

**NOTE** Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.

You can do the following activities.

- Adding files to Exclusion List
- **Deleting files** from Exclusion List
- Removing all files from Exclusion List

|          | 🝸 He      |
|----------|-----------|
|          |           |
| <b>A</b> | Add       |
|          | Delete    |
|          | RemoveAll |
|          |           |
|          |           |
|          |           |
|          |           |
|          |           |
|          |           |
| -        |           |
|          |           |

### Adding files to Exclusion List

To add executable files to the Exclusion List, follow the steps given below:

- 1. Enter the executable file name and then click **Add**. The executable file gets added to the Exclusion List.
- 2. Click **OK**.

### **Deleting files from Exclusion List**

To delete executable files from the Exclusion List, follow the steps given below:

- 1. Select the appropriate file checkbox, and then click **Delete**. A confirmation prompt appears.
- 2. Click **OK**. The executable file gets deleted from the Exclusion List.





# **Removing all files from Exclusion List**

To remove all executable files from the Exclusion List, follow the steps given below:

- 1. Click **Remove All**. A confirmation prompt appears.
- 2. Click **OK**. All executable files get removed from the Exclusion List.





# **Notifications & Events**

| Notifications & Events   |                         | 🝸 Help |
|--|-------------------------|--------|
| Notifications Events   |                         |        |
| r Warning Notification Settings  |                         |        |
| Virus Alerts   | Warning Mails           |        |
|  | Delete Meile Forty Loss |        |
| Mail Server Settings SMTP Mail Server SMTP Port User Authentication(Opt.) Authentication Password(Opt.)  | Add Delete RemoveAll    |        |
| <ul> <li>Attachment Removed Warning To Sender</li> <li>Attachment Removed Warning To Recipient</li> <li>Virus Warning To Sender</li> <li>Virus Warning To Recipient</li> <li>Content Warning To Sender</li> <li>Content Warning To Recipient</li> </ul>                          |                         |        |
| attrem.snd   |                         |        |
| <pre>#Lines starting with # are comment lines.<br/>#This file specifies warning sent to Mail-Sender by<br/>#eScan when it deletes attachments.<br/>#<br/>The attachment(s) that you sent with the following mail<br/>was deleted by eScan (not delivered to the recipient)</pre> |                         |        |
| The Mail came from : %<br>The Mail recipient : %<br>Subject of the Mail : %<br>Message-ID : %<br>Received : %r   |                         |        |
|  |                         |        |
| Default Advanced Setting OK Cancel   |                         |        |

# Notifications

Notifications tab lets you configure the notification settings. It lets you send emails to specific recipients when malicious code is detected in an email or email attachment. It also lets you send alerts and warning messages to the sender or recipient of an infected message. You can configure the following settings:

#### Virus Alerts [Default]

This section contains **Show Alert Dialog box** option. Select this option if you want Mail Anti-Virus to alert you when it detects a malicious object in an email.

#### **Warning Mails**

Configure this setting if you want Mail Anti-Virus to send warning emails and alerts to a given sender or recipient. The default sender is **postmaster** and the default recipient is **postmaster**.




#### Attachment Removed Warning To Sender [Default]

Select this checkbox if you want Mail Anti-Virus to send a warning message to the sender of an infected attachment. Mail Anti-Virus sends this email when it encounters a virus infected attachment in an email. The email content is displayed in the preview box.

#### Attachment Removed Warning To Recipient [Default]

Select this checkbox if you want Mail Anti-Virus to send a warning message to the recipient when it removes an infected attachment. The email content is displayed in the preview box.

#### Virus Warning To Sender [Default]

Select this checkbox if you want Mail Anti-Virus to send a virus warning message to the sender. The email content is displayed in the preview box.

#### Virus Warning To Recipient [Default]

Select this checkbox if you want Mail Anti-Virus to send a virus warning message to the recipient. The email content is displayed in the preview box.

#### **Content Warning To Sender**

Select this checkbox if you want Mail scanner to send a content warning message to the sender. The email content is displayed in the preview box.

#### Content Warning To Recipient [Default]

Select this checkbox if you want Mail scanner to send a content warning message to the recipient. The email content is displayed in the preview box.

#### **Delete Mails From User**

You can configure eScan to automatically delete emails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete Mails From User** field. The **Add**, **Delete**, and **Remove All** buttons appear as dimmed. After you enter text in the **Delete Mails From User** field, the buttons get enabled.





### **Events**

Events tab lets you define the settings to allow/restrict clients from sending alert for following events:

- Executable Allowed
- Website Allowed
- Cleaned Mail

By default all events are selected.

| Notifications & Events   | 🝸 Help |
|--|--------|
| Notifications Events   |        |
| Do not allow client to send event for<br>Executable Allowed<br>WebSite Allowed<br>Cleaned Mail |        |
| Default Advanced Setting OK Cancel   |        |







### **Schedule Update**

The Schedule Update lets you schedule eScan database updates.

| Jule Update    |          |            |                 |       |
|----------------|----------|------------|-----------------|-------|
| Automatic Down | nload    | O Scł      | nedule Download |       |
| Daily          |          |            |                 |       |
| Weekly         | Mon      | Tue        | Wed             | 🔲 Thu |
|                | 🗌 Fri    | Sat        | Sun             |       |
| Monthly        | 1 .      |            |                 |       |
| At             | 12:00 am | © <b>▼</b> |                 |       |
|                |          |            |                 |       |

The updates can be downloaded automatically with **Automatic Download** option. -OR-

The updates can be downloaded on a schedule basis with **Schedule Download** option. Select intervals and time basis as per your preferences.





### Tools

| Too | İs                   |                   |   | <u>?</u> Help |
|-----|----------------------|-------------------|---|---------------|
|     | EBackup RMM Settings |                   |   |               |
|     | Add Backup Set       | ]                 |   |               |
|     | Backup Name          | Next Start        | Created On                                  | -             |
|     |                      | (*) eBackup polic | ry is not applicable for Policy Criteria Te | emplates.     |
|     | Ok Cancel            |                   |   |               |

The Tools lets you configure eBackup and RMM Settings.

### eBackup

Taking regular backup of your critical files stored on your computer is very important, as files may get misplaced or damaged due to issues such as virus outbreak, modification by a ransomware or another user. This feature of eScan allows you to take backup of your important files stored on your computer such as documents, Photos, media files, music files, and contacts. It allows you to schedule the backup process by creating tasks. The backed up data is stored in an encrypted format in a folder secured by eScan's real-time protection. You can create Backup jobs by adding files, folders to take a backup either manually or schedule the backup at a defined time or day.

With eBackup feature you can:

- Create, schedule, edit, and delete backup jobs as per requirement.
- Take a backup of specific folder(s)/file extension(s) on local endpoint, external drives or network drive.
- Exclude specific folder(s)/file extension(s) from being backed up.
- Add specific file extensions to be backed up along with regular backup as per requirement.
- Save the backup data in external hard drive or local drive.

#### Add Backup Set

To add a Backup Set, follow the steps given below:





- 1. Go to Managed Computers.
- 2. Click Policy Templates > New Template.

**NOTE** You can add the backup set for existing Policy Templates by selecting a Policy Template and clicking **Properties**. Then, follow the steps given below:

- 3. Select **Tools** check box and then click **Edit**.
- 4. Click Add Backup Set. Add Backup Set window appears.

| ckup Set  |                     |          |          |  |
|---|---------------------|----------|----------|--|
|   |                     |          |          |  |
| Job Backup Source and Exclusion                     |                     |          |          |  |
| ✓ Active  |                     |          |          |  |
| Name  |                     |          |          |  |
|   |                     |          |          |  |
| Scheduler   |                     |          |          |  |
| Execute   |                     |          |          |  |
| Once Usuala   | Weekly              |          |          |  |
|   | With system startun |          |          |  |
| - 560   |                     |          |          |  |
| Destination Path Settings                           |                     |          |          |  |
| Add Destination Path                                |                     |          |          |  |
| Destination Path for Backed up Files.               |                     | UserName | Password |  |
|   |                     |          |          |  |
| Note : Only Drive name or full UNC path is Allowed. |                     |          |          |  |
| 2. "\\192.168.0.96\external\backup"                 |                     |          |          |  |
|   |                     |          |          |  |
|   |                     |          |          |  |
| ave Cancel  |                     |          |          |  |

- 5. Enter a name for the backup.
- 6. In the Scheduler section, select a preferred interval for backup execution.
- 7. If you want to specify a custom location for backup file on network, select the checkbox **Add Destination Path**.
- 8. Enter the destination path and login credentials of destination network.
- 9. Click Backup Source and Exclusion tab.

| Add Backup Set  |   | 👔 Help 🔺            |
|---|---|---------------------|
| Job Backup Source and E<br>Folder Settings<br>Add File Types for Backup<br>Office Documents <u>Customize</u><br>All Files | File/Folder Exclusion         Add File/Folder         Image: State of the stat | Add                 |
|   | File/Folder Type  | Delete<br>RemoveAll |
| Save Cancel   |   |                     |

- 10. Select the type of files for backup. By default, Office Documents option is selected.
- 11. Under the File/Folder Exclusion section, you can exclude a specific folder or a file format from getting backed up.
- 12. Click Save.





The Backup Set will be created at network location.

**NOTE** By default, **Active** option is selected. If **Active** option is not selected, a Backup Set will be created but eScan won't backup data.

#### **Edit Backup Set**

To edit a Backup Set, follow the steps given below:

- 1. Select a Backup Set.
- 2. Click Edit Backup Set.
- 3. After making the necessary changes, click **Save**. The Backup Set will be edited and saved.

#### **Delete Backup Set**

To delete a Backup Set, follow the steps given below:

- 1. Select a Backup Set.
- 2. Click **Delete Backup Set**. A confirmation prompt appears.
- 3. Click **OK**. The Backup Set will be deleted.

### **RMM Settings**

The RMM settings let you configure default connection settings for connecting to client computers. You will get the following configuration options:

| Tools   |                                     | <br> | 🝸 Help |
|---|-------------------------------------|------|--------|
| EBackup   | RMM Settings                        |      |        |
| <ul> <li>Manual</li> <li>Auto S</li> <li>User Ad</li> </ul> | Start<br>tart<br>cceptance Required |      |        |
| Show F  | XMM Connection Alert                | <br> |        |

- **Manual Start**: If this option is selected, client endpoint users have to manually start the RMM service to establish a RMM connection.
- **Auto Start**: If this option is selected, RMM service will be started automatically and all client endpoints will be connected to your main eScan server.
- User Acceptance Required: If this check box is selected, a pop-up appears on client endpoint for RMM connection acceptance. If left unselected, pop-up doesn't appear and you get direct access to the client endpoint.





• Show RMM Connection Alert: If this check box is selected, a notification appears on client endpoint informing about active RMM connection. If left unselected, notification doesn't appear on client endpoint.

After making the necessary changes click **OK**. Click **Save**. The Policy Template gets saved.

#### **RMM - Manual Start**

To take a remote connection by using Manual Start option

1. Tell the client endpoint user to right-click the eScan Protection Center icon 💱 and click **Start eScanRMM**.



 After the client endpoint user has clicked Start eScanRMM, select the target endpoint and then click Client Action List > Connect to Client (RMM). Following disclaimer appears.









3. Read the disclaimer thoroughly and then click **Accept**.

Your default browser opens eScan Remote Access window (Google Chrome, Mozilla Firefox, MS Edge, etc.)



Following notification appears on client endpoint displaying IP address of RMM connecting endpoint and connection ID (If **Show RMM Connection Alert** option is selected).



#### **RMM - Auto Start**

If **Auto Start** option is selected, then client endpoints get automatically connected to your eScan server.

 Go to Managed Computers, select the target endpoint and then click Client Action List > Connect to Client (RMM).

RMM disclaimer appears.

Read the disclaimer thoroughly and then click Accept.
 Your default browser opens eScan Remote Access window (Google Chrome, Mozilla Firefox, MS Edge, etc.)

After you are done performing an activity, click the **Disconnect** icon to end remote connection.

**NOTE** To get detailed information about RMM feature, <u>click here</u>.





## Assigning Policy Template to Group (s)

To assign a Policy to a group, follow the steps given below:

- 1. In the Managed Computers screen, click **Policy Templates**. Policy Templates window appears.
- 2. In the **Policy Template** window, select a policy template.

| Policy Templates Sefresh 👔 Help |                         |                         |                      |                         |  |
|---------------------------------|-------------------------|-------------------------|----------------------|-------------------------|--|
| New Template Properties         | Parent Policy           | Assign to Group(s)      | gn to Computer(s)    | y Template              |  |
| Name of Template                | Created On              | Modified On             | Assigned to Group(s) | Assigned to Computer(s) |  |
| Sample Policy Template          | Sep 24 2019 12:33:42 PM | Sep 24 2019 12:33:42 PM |                      |                         |  |

3. Click **Assign to Group(s)**. Select Group window appears.

| Sel | ect Group            | lp |
|-----|----------------------|----|
|     | E. Managed Computers |    |
|     | Ok Cancel            |    |

 Select the group(s) and click **OK**. The policy will be assigned to the selected group(s).





## Assigning Policy Template to Computer(s)

To assign a policy template to computers, follow the steps given below:

1. In the **Policy Templates** window, select a policy.

| F   | Policy Templates Sefresh 👔 Help |                        |                         |                         |            |  |  |
|---|---------------------------------|------------------------|-------------------------|-------------------------|------------|--|--|
| Template Properties Properties Properties Parent Policy Template Assign to Group(s) Assign to Computer(s) Copy Template |                                 |                        |                         |                         | y Template |  |  |
| Name of Template         Created On         Modified On         Assign  |                                 | Assigned to Group(s)   | Assigned to Computer(s) |                         |            |  |  |
|   | 1                               | Sample Policy Template | Sep 24 2019 12:33:42 PM | Sep 24 2019 12:33:42 PM |            |  |  |
| ιľ  |                                 |                        |                         |                         |            |  |  |

#### 2. Click Assign to Computer(s).

Assign Template to computer window appears.

| Assig | gn template to computer | 👔 Help |
|-------|-------------------------|--------|
| s     | elect Computer          |        |
|       | 🗄 🗔 🚰 Managed Computers |        |
|       | Ok Cancel               |        |

- 3. Click Managed Computers.
- Select the computer(s) and click **OK**. The policy template will be assigned to the selected computers.





## **Deleting Policy Template**

To delete a Policy Template, follow the steps given below:

1. In the Policy Template window, select a policy.

| P   | Policy Templates |                        |                         |                         |                      |                         |  |
|---|------------------|------------------------|-------------------------|-------------------------|----------------------|-------------------------|--|
| Rew Template Properties Parent Policy 🔂 Delete Assign to Group(s) Assign to Computer(s) Copy Template |                  |                        |                         |                         | y Template           |                         |  |
|   | •                | Name of Template       | Created On              | Modified On             | Assigned to Group(s) | Assigned to Computer(s) |  |
|   | 1                | Sample Policy Template | Sep 24 2019 12:33:42 PM | Sep 24 2019 12:33:42 PM |                      |                         |  |

2. Click **Delete**.

|  | × |
|--|---|
| Policy Templates                                   |   |
| Do you want to delete selected policy template(s)? |   |
| Ok Cancel  |   |

3. Click **Ok**. The Policy Template will be deleted.

## Copying a Policy Template

To copy a Policy Template, follow the steps given below:

1. In the Policy Templates window, select a policy.

| Po | Policy Templates Sefresh 👔 Help                |                        |                         |                         |                      |                         |
|----|--|------------------------|-------------------------|-------------------------|----------------------|-------------------------|
| [  | Rew Template Properties Parent Policy 😭 Delete |                        |                         | Assign to Group(s)      | gn to Computer(s)    | y Template              |
|    | 2  | Name of Template       | Created On              | Modified On             | Assigned to Group(s) | Assigned to Computer(s) |
| V  |  | Sample Policy Template | Sep 24 2019 12:33:42 PM | Sep 24 2019 12:33:42 PM |                      |                         |

#### 2. Click Copy Template.

New Template window appears displaying settings from the original template.

- 3. Enter a name for the template.
- 4. Make the necessary changes and click **Save**. The template will be copied.





## **Parent Policy**

The **Parent Policy** lets you to implement a change in policy setting to multiple policies at the same time. For example, if you want to make a policy change in a single module like **File Anti-Virus** in multiple policies; you can do this all at a time using Parent Policy. To configure Parent Policy, follow the steps given below:

- 1. In the Managed Computers screen, click **Policy Templates**. Policy Templates window appears.
- 2. In the Policy Template window, click **Parent Policy**.

| Poli | Policy Templates Sefresh 👔 Help |                          |                         |                      |                         |  |
|------|---------------------------------|--------------------------|-------------------------|----------------------|-------------------------|--|
|      | New Template                    | s Parent Policy 📄 Delete | Assign to Group(s)      | gn to Computer(s)    | y Template              |  |
|      | Name of Template                | Created On               | Modified On             | Assigned to Group(s) | Assigned to Computer(s) |  |
|      | Sample Policy Template          | Sep 24 2019 12:33:42 PM  | Sep 24 2019 12:33:42 PM |                      |                         |  |
|      |                                 |                          |                         |                      |                         |  |

Properties (Parent Policy) window appears displaying all the policies.

| es (Parent Policy)      |      |                         |      | <u></u> |
|-------------------------|------|-------------------------|------|---------|
| -lieu Deteile           |      |                         |      |         |
|                         |      |                         |      |         |
| File Anti-Virus         | Edit | Mail Anti-Virus         | Edit |         |
| Assign To Select Policy |      | Assign To Select Policy |      |         |
| Anti-Spam               | Edit | Web Protection          | Edit |         |
| Assign To Select Policy |      | Assign To Select Policy |      |         |
| 🔲 FireWall              | Edit | EndPoint Security       | Edit |         |
| Assign To Select Policy |      | Assign To Select Policy |      |         |
| Privacy Control         | Edit |                         |      |         |
| Assign To Select Policy |      |                         |      |         |
| Administrator Password  | Edit | ODS/Schedule Scan       | Edit |         |
| Assign To Select Policy |      | Assign To Select Policy |      |         |
|                         |      |                         |      |         |

3. Select and edit the required module according to your preferences.





4. Click **Assign To** drop-down and select the policies for which the parent policy changes should be applied.

| Virus                    |   | Edit  |
|--------------------------|---|-------|
| Select Policy            |   |       |
| Filter<br>Enter Key Word |   | )     |
|                          | Uneneck M   |       |
| tech 🗌                   |   |       |
|                          |   |       |
|                          |   | )     |
|                          |   |       |
|                          |   |       |
| ator Password            |   | Edit  |
|                          | Virus<br>Select Policy<br>Filter<br>Enter Key Word<br>Check All<br>tech | Virus |

5. Click **OK**. The Parent policy will be updated and changes will be applied to all the policies selected.

| NOTE | Before disabling a module in Parent Policy, ensure that policies are unchecked from |
|------|---|
| NOTE | Assign To drop-down.  |





# Policy Criteria Templates

This button allows to add criteria template based on the endpoints conditions.

### Adding a Policy Criteria Template

To define Policy Criteria Template, follow the steps given below:

1. In the Managed Computers screen, click **Policy Criteria Templates**.

Policy Criteria screen appears.

| Policy Criteria Sefresh 👔 Help |                 |             |                             |                         |  |  |
|--------------------------------|-----------------|-------------|-----------------------------|-------------------------|--|--|
| New Criteria                   | Delete Criteria | Assign To 🔻 |                             |                         |  |  |
| Name of Criteria               | Created On      | Modified On | <u>Assigned to Group(s)</u> | Assigned to Computer(s) |  |  |
|                                |                 |             |                             |                         |  |  |

#### 2. Click New Criteria.

Policy Criteria screen displays parameter for creation.

| olicy Criteria           |  |  |
|--------------------------|--|--|
|                          |  |  |
| Criteria Name            |  |  |
| Description:             |  |  |
| Conditions for criteria: |  |  |
| Add V Edit Delete        |  |  |
|                          |  |  |
|                          |  |  |
| Save Close               |  |  |

- 3. Enter Name and Description.
- 4. Click Add drop-down.
- 5. Click Add AND Condition.





#### Specify Criteria screen appears.

| Specify criteria   | ? | Hel | p |
|--|---|-----|---|
| Type : Computer IP Address   |   |     | 1 |
| If the client computer has one of the IP addresses listed below        |   |     |   |
| If all of the IP addresses of the client computer are listed below     |   |     |   |
| If the client computer does not have any of the addresses listed below |   | _   |   |
| Image: Type         Content  | - |     |   |
|  |   |     |   |
|  |   |     |   |
|  |   |     |   |
|  |   |     |   |
|  |   |     |   |
|  |   |     |   |
| 4  | × |     |   |
|  | _ |     |   |
| Add Edit Delete  |   |     |   |
| Ok Cancel  |   |     | - |

- 6. Click the **Type** drop-down. It displays following options:
  - Computer IP Address
  - Management Server Connection
  - Users
  - Machine Name

Depending upon the option, the conditions and settings vary.

### **Computer IP Address**

- 1. Select the appropriate condition.
- 2. Click **Add**.

Address window appears.

| Address      |            |
|--------------|------------|
| Type :       | IP Address |
| IP Address : |            |
| Ok           | Cancel     |
|              |            |

- 3. Enter the IP address.
- 4. Click **OK**.

The Policy Criteria Template for an IP Address will be saved.





### **Management Server Connection**

| Specify criteria |   |  |  |
|------------------|---|--|--|
|                  | Type : Management Server Connection 🔻                           |  |  |
|                  | If the client computer can connect to the management server     |  |  |
|                  | If the client computer can not connect to the management server |  |  |
| [                | Ok Cancel   |  |  |

- 1. Select the appropriate condition.
- 2. Click **OK**.

The Policy Criteria Template for Management Server Connection will be saved.

### Users

| Specify criteria  | 🝸 Help   |
|---|----------|
| Type : Users  |          |
| If the client computer has one of the Username listed below     Condition |          |
|   | <b>^</b> |
|   | -        |
|   |          |
|   |          |
|   |          |
|   |          |
|   |          |
| 4   | <b>Y</b> |
|   |          |
| Add Add AD users Edit Delete  |          |
| Ok Cancel   |          |

### **Adding Local Users**

1. To add local users, click **Add**. Username window appears.

| Username |        |
|----------|--------|
| Username |        |
| Ok       | Cancel |

2. Enter a Username.





3. Click **OK**.

The local user will be added.

### **Adding Active Directory Users**

To add Active Directory users, follow the steps given below:

1. Click Add AD Users.

Add Active Directory Users window appears.

| Add Active Directory Users                    |   | 👔 Help |
|---|---|--------|
| <u>User Accounts</u> > Add Active Directory U | Jsers   |        |
| Search Criteria                               |   |        |
| User's name*:                                 |   |        |
|   | For Example: user or user*                    |        |
| Domain*:                                      |   |        |
| AD IP Address*:                               |   |        |
| AD Admin User name*:                          |   |        |
|   | For Active Directory account: domain\username |        |
| AD Admin Password*:                           |   |        |
| Use SSL Auth.:                                |   |        |
| AdsPort*:                                     | 389   |        |
| Search  |   |        |
| Search Results                                |   |        |
| Users   | Selected Users                                |        |

- 2. Enter data in mandatory fields.
- 3. Click Search.
- Search Results section displays a list of discovered users in Users list. Select a user and then click button to add the user to Selected Users list. Vice versa the added user can be moved from Selected Users to Users by clicking
- 5. Click **OK**.

The Policy Criteria Template for Users will be saved.





### **Machine Name**

| Specify criteria  |
|---|
|   |
| Type : Machine Name   |
| If the client computer has one of the machine name listed below |
|   |
|   |
|   |
|   |
|   |
|   |
|   |
|   |
|   |
|   |
| 4   |
|   |
| Add Delete  |
| Ok Cancel   |

1. Click **Add**. Select Computer screen appears displaying all managed computers.

|                                      |               | ×      |
|--------------------------------------|---------------|--------|
| Select Computer                      |               | 👔 Help |
| Select Computer<br>Managed Computers | Add<br>Remove |        |
|                                      | Ok Ca         | ncel   |

2. Select the computer(s) to be added under this criterion and click **Add** > **OK**. The Policy Criteria Template for selected machines will be saved.





## Viewing Properties of a Policy Criteria template

To view the properties of a Policy Criteria Template, follow the steps given below:

- 1. Select a policy criteria template.
- 2. Click Properties.

| Poli | y Criteria          |                                |                         |   | 💲 Refresh 🛛 👔 Help      |
|------|---------------------|--------------------------------|-------------------------|---|-------------------------|
|      | New Criteria 📑 Prop | perties 📄 Delete Criteria 📑 As | sign To 🗸               |   |                         |
|      | Name of Criteria    | Created On                     | Modified On             | Assigned to Group(s)                      | Assigned to Computer(s) |
|      | aaa                 | Sep 26 2019 03:44:12 PM        | Sep 26 2019 03:44:12 PM | Group Default Policy<br>Managed Computers |                         |

Policy Criteria window appears.

| Policy Criteria                 | lelp |
|---------------------------------|------|
| Criteria Name: aaa Description: | ]    |
| Conditions for criteria:        |      |
| - 192.168.0.01                  |      |
|                                 |      |
| Save Close                      | ]    |

3. Make the necessary changes and click **Save**. The Policy Criteria template will be saved and updated.





## Deleting a Policy Criteria template

To delete assigned policy criteria template, follow the steps given below:

The Policy Criteria window displays to which group or computer the template is assigned in Assigned to Group(s) or Assigned to Computer(s) column.

For explanation, we are following the procedure as per the screenshot below

- 1. Select a policy criteria template.
- 2. Click **Assign To** > **Groups**.

| Poli | cy Criteria         |                                |                         |   | 💲 Refresh 🛛 👔 Help      |
|------|---------------------|--------------------------------|-------------------------|---|-------------------------|
|      | New Criteria 📑 Prop | perties 👔 Delete Criteria 🛐 As | sign To 🗸               |   |                         |
|      | Name of Criteria    | Created On                     | Modified On             | Assigned to Group(s)                      | Assigned to Computer(s) |
|      | aaa                 | Sep 26 2019 03:44:12 PM        | Sep 26 2019 03:44:12 PM | Group Default Policy<br>Managed Computers |                         |

#### Assign Criteria to Group window appears.

| Assign Criteria to group                       | ? |
|--|---|
| Select Policy Template                         |   |
| Group Default Policy<br>Sample Policy Template |   |
|  |   |
|  |   |
|  |   |
|  |   |
|  |   |
|  |   |
| Ok Cancel                                      |   |

3. Click Group Policy Template > OK.





Assign Criteria to group window displays Managed Computers folder tree.

| Assign Criteria to group | 👔 Help |
|--------------------------|--------|
| Select Group             |        |
| È I Canaged Computers    |        |
| Ok Cancel                |        |

- 4. Uncheck the selected group.
- 5. Click **OK**.

The Policy Criteria Template will no longer be assigned to any group. This enables **Delete Criteria** button.

| Policy Criteria                           |        |                         |                         |
|---|--------|-------------------------|-------------------------|
| New Criteria Properties 👔 Delete Criteria |        |                         |                         |
| Name of Cr                                | iteria | Created On              | Modified On             |
| 🗹 aaa                                     |        | Sep 26 2019 03:44:12 PM | Sep 26 2019 03:44:12 PM |
|   |        |                         |                         |

- 6. Select the template.
- 7. Click Delete Criteria.

The Policy Criteria Template will be deleted.





# **Client Action List**

Client Action List lets you take action for specific computer(s) in a group. To enable this button, select computer(s) and then click **Client Action List**. The drop-down consists of following options:

- Set Host Configuration
- Deploy/Upgrade Client
- Uninstall eScan Client
- Move to Group
- Remove from Group
- Connect to Client RMM
- Add to RMM License
- Manage Two-FA License
- Export
- Show Installed Softwares
- Force Download
- Send Message
- Outbreak Prevention
- Delete All Quarantine Files
- Create OTP
- Pause Protection
- Resume Protection
- Properties

The Client Action List contains few options similar to Action List. These options perform same, except they perform the action only for selected computer(s).





## Set Host Configuration

If you are unable to view details of Windows OS installed computer with **Properties** option, set its **Host Configuration**. Doing so will build communication between the server and selected computer, displaying its details.

To set Host Configuration for a selected computer, follow the steps given below:

- 1. Select the computer.
- 2. Click **Client Action List** > **Set Host Configuration**. Set Host Configuration window appears.

| Set Host Configura                       | tion   |                |
|--|--|----------------|
| Login Information                        | 1  |                |
| Computer Name:<br>Remarks:<br>User name: | Administrator  |                |
| Password:                                |  |                |
| Note: If Host Nan                        | ne is in another Domain, Please mention Domain Name Ex. Do | main1\HostName |
| Save Cancel                              |  |                |

3. Enter Remarks and login credentials.

#### 4. Click **Save**.

The Host will be configured as per new settings.





## Deploy/Upgrade Client

To Deploy/Upgrade eScan client on selective computers in a group or an individual computer, follow the steps given below:

### **Installing eScan Client on a Client Computer**

- 1. Select a client computer within a group to install eScan client.
- Click Client Action List > Deploy/Upgrade Client. Client Installation window appears.

| ient Installation  |
|--|
| elect Application for Installation:  |
| Install eScan  |
| Select eScan Installation Options:   |
| Auto Reboot after Install  |
| Install Without Firewall   |
| Disable auto downloading of Windows patches by eScan                           |
| Installation Path  |
| <default>  Add</default>   |
| Install Other Software   |
| Linux/MAC Client Setup   |
| Required files for Installation  |
| C:\PROGRA~2\eScan\Setup\Launchit.Exe,C:\PROGRA~2\<br>eScan\Setup\Setup.exe Add |
| Executable file  |
| Launchit.exe T Edit Script   |
| Parameters   |
| /Setupfile=Setup.exe   |
| Install Agent  |
| Install local client setup   |
| Required files for Installation  |
|  |

3. Select Install eScan option.

By Default eScan is installed at the following Path on a Client computer. C:\Program Files\eScan (default path for 32-bit computer) OR

C:\Program Files (x86)\eScan (default path for 64-bit computers).

- 4. To define a different installation path, click **Add**. (Skip this step if default path chosen).
- 5. Click Install.





A window displays File transfer progress. After Installation, the eScan status will be updated in Managed Computers list.

### Uninstall eScan Client

To uninstall eScan Client on any computer, follow the steps given below:

- 1. Select the computer for uninstallation.
- 2. Click **Client Action List** > **Uninstall eScan Client**. Client Uninstallation window appears.

| Client Uninstallation  |
|--|
| Ready to Start Uninstallation<br>Click "Uninstall" to Start Uninstallation |
| Uninstall Cancel   |

#### 3. Click Uninstall.

The Client Uninstallation window displays the progress.

| Client Uninstallation  |   |
|--|---|
| 9/26/2019 4:47:37 PM : [<br>9/26/2019 4:47:37 PM : [                             | ]: Connecting to Computer<br>]: Reading Host Details  |
| 9/26/2019 4:47:37 PM : [<br>9/26/2019 4:47:37 PM : [<br>9/26/2019 4:47:37 PM : [ | ]: Version 14.0.1400.2220<br>]: Service Pack 2220<br>]: Service Version (Second Second |
| 9/26/2019 4:4/:3/ PM : [   | ]: Task Uninstall escan on Host(s) successfully scheduled on  |
| Close Cancel   |   |

4. After the uninstallation process is over, click **Close**.

NOTEYou can uninstall eScan Client from all the computers in the group by selecting the<br/>Group and then Click Action List > Uninstall eScan Client.





### Move to Group

To move computers from one group to other, follow the steps given below:

- 1. Go to Managed Computers.
- 2. Select the desired computers present in a group.
- 3. Click **Client Action List** > **Move to Group.**
- 4. Select the group in the tree to which you wish to move the selected computers and click **OK**. The computers will be moved to the selected group.

### Remove from Group

To remove computers from a group, follow the steps given below:

- 1. Go to Managed Computers.
- 2. Select the desired computers for removal.
- 3. Click **Client Action List** > **Remove from Group**. A confirmation prompt appears.
- 4. Click **OK**. The computers will be removed from the group.

## Connect to Client (RMM)

To connect to client via RMM service, follow the steps given below:

- 1. Go to Managed Computers.
- 2. Select the client computer for which you want to take remote connection.
- Click Client Action List > Connect to Client (RMM). RMM disclaimer appears.
- 4. Click Accept.

You will get connected to the client computer via RMM service. Read more about RMM configuration.

## Add to RMM License

To add a computer to RMM licensed category, follow the steps given below:

- 1. Go to Managed Computers.
- 2. Select the client computer which you want to add to RMM License.
- Click Client Action List > Add to RMM License. RMM disclaimer appears.
- Read the disclaimer thoroughly as this action is irreversible. To proceed, click **OK**. The endpoint gets added to RMM license. After adding the endpoint to RMM license
   icon appears next to the RMM enabled endpoints.

**NOTE** After adding a client endpoint to RMM license, it is mandatory that the client endpoint should be updated with latest eScan updates.





## Manage Two-FA License

To manage Two-FA license, follow the steps given below:

- 1. Go to Managed Computers.
- 2. Select the client computer which you want to manage Two-FA License.
- 3. Click **Client Action List** > Manage Two-FA License.
- 4. Manage 2FA License window appears.

|   |      | × |
|---|------|---|
| Two-Factor Authentication   |      |   |
| <ul> <li>Add</li> <li>Remove</li> <li>License Information</li> <li>License Size : 60</li> <li>License Remaining : 57</li> </ul> | <br> |   |
| Ok Cancel   |      | ] |

5. Select **Add** to add a client computer to 2FA license or **Remove** to remove the added client computer and then click **OK**.

The computer gets added or removed from 2FA license as per your preferred option. Read more about <u>Two-Factor Authentication</u>.





## Export

To export a client computer's data, follow the steps given below:

1. In the Managed Computers folder tree, select a group and then click **Client Computers**.

The right pane displays the list of computers in the group and their detailed information.



 Select a client computer and the click Client Action List > Export. Export Selected Columns window appears displaying export options and a variety of columns to be exported.

| Export Selected Columns                         |                   |                              | 👔 Help              |
|---|-------------------|------------------------------|---------------------|
| Export Option     Excel                         |                   | O PDF                        |                     |
| Select All Columns                              |                   |                              |                     |
| Computer Name                                   | IP Address        | IP Address of the connection | User name           |
| <ul> <li>Local Administrator User(s)</li> </ul> | eScan Status      | <ul> <li>Version</li> </ul>  | Last Connection     |
| Installed Directory                             | Monitor Status    | Anti-Spam                    | Mail Anti-Virus     |
| Web Protection                                  | Endpoint Security | <ul> <li>Firewall</li> </ul> | Last Update         |
| ✓ Update Server                                 | Client OS         | Status                       | Last Policy Applied |
| Last Policy Applied Time                        |                   |                              |                     |
| Export Cancel                                   |                   |                              |                     |

- 3. Select the preferred export option.
- 4. Select the preferred report columns.
- 5. Click **Export**.

The report will be exported as per your preferences.





## Show Installed Softwares

This feature displays a list of installed softwares on a computer.

To view the list of installed softwares, follow the steps given below:

1. In the Managed Computers folder tree, select a group and then click **Client Computers**.

The right pane displays the list of computers in the group and their detailed information.

| ₽ Search 🛜 Update Agent   |                         |                  |                              |                     |             |  |
|---|-------------------------|------------------|------------------------------|---------------------|-------------|--|
| Action List 🔻 👔 Client Action List 🔻 🔁 Refresh Client 🍈 Select Columns Computer Selected: 1 |                         |                  |                              |                     |             |  |
| 🖻 🚞 Managed Computers   | 💿 💻 eScan Installed 🛛 🛛 | eScan Not Instal | led                          |                     |             |  |
| 🔃 Policy  | Computer Name           | IP Address       | IP Address of the connection | User name           | Local Admi  |  |
| - 🐻 Group Tasks   |                         | 20-001-01-       |                              | REALIST ARRANGED IN | Administrat |  |
| 🚽 Client Computers (1)  |                         |                  |                              | 1                   |             |  |
| 🗄 🧫 Roaming Users   |                         |                  |                              |                     |             |  |
| 🗄 🧰 sample  |                         |                  |                              |                     |             |  |
|   |                         |                  |                              |                     |             |  |
|   |                         |                  |                              |                     |             |  |

# 2. Select a client computer and then click **Client Action List** > **Show Installed Softwares**.

Installed Softwares window appears displaying list of installed softwares and in the top right corner displays total number of installed softwares.

| Installed Softwares                                    | 🝸 Help                             |
|--|------------------------------------|
| Computer Name:   | Total No.Of Installed Programs: 65 |
| Currently Installed Programs                           |                                    |
| Active Directory Authentication Library for SQL Server |                                    |
| Adobe Reader XI (11.0.10)                              |                                    |
| Advanced IP Scanner 2.5                                |                                    |
| AnyDesk  |                                    |
| Apple Application Support (32-bit)                     |                                    |
| Apple Application Support (64-bit)                     |                                    |
| Apple Mobile Device Support                            |                                    |
| Apple Software Update                                  |                                    |
| Bonjour  |                                    |
| Canon CAPT Print Monitor 1.51                          |                                    |





## Force Download

The Force Download feature forces a client computer to download Policy Template modifications (if any) and updated virus signature database.

To activate this feature for computers, follow the steps given below:

1. In the Managed Computers folder tree, select a group and then click **Client Computers**.

The right pane displays the list of computers in the group and their detailed information.

| ₽ Search  |   |                       |                   |                              |                   |             |
|---|---|-----------------------|-------------------|------------------------------|-------------------|-------------|
| The Action List V Client Action List V Refresh Client Select Columns Computer Selected: 1 |   |                       |                   |                              |                   |             |
| 🗄 🧰 Managed Computers   | 0 | 💻 eScan Installed 🛛 🛛 | 📕 eScan Not Insta | lled                         |                   |             |
| 🔟 Policy  |   | Computer Name         | IP Address        | IP Address of the connection | <u>User name</u>  | Local Admi  |
| - Group Tasks   |   |                       | 28-281-28-        |                              | ALC: NO. AREASTIC | Administrat |
| 🚽 Client Computers (1)  |   |                       |                   |                              |                   |             |
| 🗄 🧫 Roaming Users   |   |                       |                   |                              |                   |             |
| 🗄 🧰 sample  |   |                       |                   |                              |                   |             |
|   |   |                       |                   |                              |                   |             |
|   |   |                       |                   |                              |                   |             |

 Select client computers and then click Client Action List > Force Download. Client Status window appears displaying the process.







## On Demand Scanning

This option lets you scan a eScan installed client computer. To scan a client computer on demand, follow the steps given below:

- 1. Go to Managed Computers.
- 2. Select the client computer which you want to scan.
- 3. Click **Client Action List** > **On Demand Scanning**. On Demand Scanning window appears.

|                                      | ×                   |
|--------------------------------------|---------------------|
| On Demand Scanning                   | 👔 Help              |
| Scan Option                          |                     |
| Spyware And Adware                   | Computer StartUp    |
| Memory Scan                          | 🗖 Registry          |
| 🗖 System Folder                      | Scan network drives |
| Scan Local Drives                    |                     |
| 🔲 Scan System Drive                  |                     |
| 🔲 Scan Data Drives                   |                     |
| Scan Option                          |                     |
| Scan Archives                        |                     |
| Auto Shut Down After Scan Completion |                     |
| Scan Only                            |                     |
| Scan Cancel                          |                     |

4. Select the preferred scan options and then click **Scan**. The On Demand Scan for selected client computer begins.





## Send Message

The Send Message feature lets you send a message to computers.

To send message to computers, follow the steps given below:

1. In the Managed Computers folder tree, select a group and then click **Client Computers**.

The right pane displays the list of computers in the group and their detailed information.

| ₽ Search               |                         |                   |                              |                           |             |
|------------------------|-------------------------|-------------------|------------------------------|---------------------------|-------------|
| Computer Selected: 1   |                         |                   |                              |                           |             |
| 🖻 🧰 Managed Computers  | 💿 💻 eScan Installed 🛛 🔿 | 📃 eScan Not Insta | alled                        |                           |             |
| 🔯 Policy               | Computer Name           | IP Address        | IP Address of the connection | <u>User name</u>          | Local Admi  |
| 🔯 Group Tasks          |                         | 1011001100        |                              | \$111111 (\$\$500000) (\$ | Administrat |
| 🚽 Client Computers (1) |                         |                   |                              |                           |             |
| 🗄 🧰 Roaming Users      |                         |                   |                              |                           |             |
| 🗄 🧰 sample             |                         |                   |                              |                           |             |
|                        |                         |                   |                              |                           |             |
|                        |                         |                   |                              |                           |             |

2. Select client computers and then click **Client Action List** > **Send Message**. Send Message window appears.

|                | ×           |
|----------------|-------------|
| Message Text : | 350/350     |
|                |             |
|                |             |
|                |             |
|                |             |
|                |             |
|                |             |
|                |             |
|                | Send Cancel |

3. Enter the message and click **Send**. The message will be sent to the selected computers.





### **Outbreak Prevention**

Upon virus detection, eScan quarantines the virus and restricts it from spreading across the network. The Outbreak Prevention feature lets you configure policies for the network.

### **Deploying Outbreak Prevention**

To deploy Outbreak Prevention feature for specific client computer(s), follow the steps given below:

- 1. Go to Managed Computers.
- 2. Select the computer(s) for which you want to deploy Outbreak Prevention.
- 3. Click Client Action List > Outbreak Prevention.

Outbreak Prevention window appears.

|   | n Deltaine   |  |  |
|---|--|--|--|
| Jutbreak Preventi   | on Policies  |  |  |
| Limit access to   | shared folders (Allow  | read access only)  |  |
| Deny write acc  | ess to local files and f   | older  |  |
| Block Specific  | orts   |  |  |
| Block All Ports   | (Other than trusted c  | lient-server ports)  |  |
| Automatically res   | tore outbreak preve  | ention after 1 V hours(s)  |  |
| configuration of the  | se policies settings ca  | in cause major problems with the c   | computers.   |
| Julbreak Preventi   |  |  |  |
|   |  |  |  |
| Notify client us  | ers when outbreak pr   | evention starts  |  |
| Notify client us  | ers when outbreak pr   | evention starts  | 207/2  |
| Notify client us<br>Message:<br>eScan has detected<br>administartor has | ers when outbreak pr<br>l a security risk outbr<br>nforced measures th | evention starts<br>eak on your network. To prevent th<br>at may prevent you from accessing | 207/2<br>he security risk from spreading, your eScan<br>I network resources. |

#### Limit access to shared folders

Select this checkbox to limit the infection's access to shared folders.

#### Deny write access to local files and folder

Select this checkbox to deny the infection write access for any file. Clicking the link displays another window that lets you specifically select folders and subfolders that should be denied and allowed access for modification.





#### **Block specific ports**

Select this checkbox to prevent infection from accessing specific ports. Clicking the link displays another window that lets you block incoming and outgoing data packets along with TCP and UDP ports.

#### Block All Ports (Other than trusted client-server ports)

Select this checkbox to block all ports other than trusted client server ports.

#### Automatically restore the outbreak prevention after hour(s)

This feature lets you restore outbreak prevention automatically after set duration (hours). Click the drop-down and select the preferred duration.

#### **Outbreak Prevention Notification**

To send a notification to client users after Outbreak Prevention is deployed, select the checkbox **Notify client users when outbreak prevention starts**. You can even write your own custom message for this feature in the Message field.

After making the necessary selections, click **Deploy**. The Outbreak Prevention feature will be deployed for the selected group.

### **Restore Outbreak Prevention**

In the Outbreak Prevention window, click **Restore Outbreak Prevention** tab.

| Dutbreak Prevention                         |   | 👔 Help             |
|---|---|--------------------|
| Deploy Outbreak Prevention                  | Restore Outbreak Prevention                     |                    |
| Restore Outbreak Prevention                 |   |                    |
| Notify client users after resto             | ring the original settings                      | 95/250             |
| Message:<br>eScan has stopped enforcing out | preak prevention policies and has restored pre- | outbreak settings. |
|   |   |                    |
|   |   | //                 |
|   |   | Restore            |

To restore Outbreak Prevention manually, click **Restore**.

To notify clients about Outbreak Prevention restoration, select the checkbox **Notify client users after the original settings**.





### **Delete All Quarantine Files**

The Delete All Quarantine Files feature lets you delete all quarantine files stored on a computer.

To delete all quarantine files on computers, follow the steps given below:

1. In the Managed Computers folder tree, select a group and under it click **Client Computers**.

The right pane displays the list of computers in the group and their detailed information.

| PSearch Rent  |                         |                   |                              |                  |             |  |
|---|-------------------------|-------------------|------------------------------|------------------|-------------|--|
| Action List V 👔 Client Action List V 🖓 Refresh Client 🛐 Select Columns Computer Selected: 1 |                         |                   |                              |                  |             |  |
| 🖻 🚞 Managed Computers   | 💿 💻 eScan Installed 🛛 🛛 | 📕 eScan Not Insta | lled                         |                  | ĭ           |  |
| 🔃 Policy  | Computer Name           | IP Address        | IP Address of the connection | User name        | Local Admi  |  |
| - Group Tasks   |                         | 201001-001        |                              | ALC: NO. ARCONC. | Administrat |  |
| Client Computers (1)  | · · ·                   |                   |                              |                  |             |  |
| ⊕   |                         |                   |                              |                  |             |  |
| 🕀 🧮 sample  |                         |                   |                              |                  |             |  |
|   |                         |                   |                              |                  |             |  |
|   |                         |                   |                              |                  |             |  |

 Select client computers and then click Client Action List > Delete All Quarantine Files. Client Status window appears displaying the progress.

| Client Status   | 🝸 Help |
|---|--------|
| 10/1/2019 12:53:20 PM : Processing with group : Sample Group<br>10/1/2019 12:53:20 PM : Connecting to Computer<br>10/1/2019 12:53:20 PM : Quarantine files successfully deleted |        |
|   |        |





## Create OTP

The password protection restricts user access from violating a security policy deployed in a network. For example, the administrator has deployed a security policy to block all USB devices, but a user needs USB access for a genuine reason. In such situation, One Time Password (OTP) can be generated for that disables USB block policy on specific computer. The administrator can define policy disable duration ranging from 10 minutes to an hour without violating existing policy.

### **Generating an OTP**

To generate an OTP, follow the steps given below:

- 1. In the **Managed Computers** screen, select the client computer for which you want to generate the OTP.
- 2. Click Client Action List > Create OTP. Password Generator window appears.

|                             |                    | (                    |
|-----------------------------|--------------------|----------------------|
| Password generator          |                    |                      |
|                             |                    |                      |
| Generate One Time Password  |                    |                      |
|                             |                    |                      |
|                             |                    |                      |
| Computer Name:*             | 101 101 101 101    |                      |
| Valid for:*                 | 10 mins 🔻          |                      |
|                             |                    |                      |
| Select Option               |                    |                      |
| File Anti-Virus             | Allow to Change Ip |                      |
| Web Protection              | Firewall           |                      |
| EPS App Control             | EPS USB            |                      |
| Mail Anti-Virus & Anti-Spam |                    |                      |
| New Password                |                    |                      |
|                             |                    |                      |
| Password                    |                    |                      |
|                             |                    |                      |
|                             |                    |                      |
|                             |                    |                      |
|                             |                    |                      |
| Generate Password Close     |                    | (*) Mandatory Fields |

- 6. In the **Valid for** drop-down, select the preferred duration to bypass the protection module.
- 7. In Select Option section, select the module you want to disable.
- 8. Click **Generate Password**. An OTP will be generated and displayed in **Password** field.




#### **Entering an OTP**

To enter an OTP, follow the steps given below:

1. In the Taskbar, right-click the eScan icon 👯. An option list appears.



2. Click Pause Protection. eScan Protection Center window appears.

| 50                        |          |                | ×         |
|---------------------------|----------|----------------|-----------|
|                           |          | eScan Protecti | on Center |
|                           |          |                |           |
| Enter eScan Administrator | Password |                |           |
|                           |          |                | _         |
| Duration                  |          |                |           |
| 15 minutes                |          |                |           |
|                           |          |                |           |
|                           |          | OK             | Cancel    |

- 3. Enter the OTP in the field.
- 4. Click **OK**.

The selected module will be disabled for set duration.





### **Pause Protection**

The Pause Protection feature lets you pause protection for computers.

To pause the protection for computers, follow the steps given below:

1. In the Managed Computers folder tree, select a group and then click **Client Computers**.

The right pane displays the list of computers in the group and their detailed information.

| P Search Supdate Agent                                    |                         |                   |                              |                  |             |  |  |
|---|-------------------------|-------------------|------------------------------|------------------|-------------|--|--|
| Action List  Computer Select Columns Computer Selected: 1 |                         |                   |                              |                  |             |  |  |
| 🖻 🔚 Managed Computers                                     | 💿 💻 eScan Installed 🛛 🔾 | 📕 eScan Not Insta | lled                         |                  |             |  |  |
| 🔃 Policy  | Computer Name           | IP Address        | IP Address of the connection | <u>User name</u> | Local Admi  |  |  |
| - Group Tasks   |                         | 2010011-001       |                              | ALC: NO. ARCONC. | Administrat |  |  |
|   |                         |                   |                              |                  |             |  |  |
| 🗄 🦲 Roaming Users   |                         |                   |                              |                  |             |  |  |
| 🗄 🧰 sample  |                         |                   |                              |                  |             |  |  |
|   |                         |                   |                              |                  |             |  |  |
|   |                         |                   |                              |                  |             |  |  |

2. Select client computers and then click **Client Action List** > **Pause Protection**. Client Status window appears displaying the progress.

| 10/1/2019 1:03:20 PM : Processing with group : Sample Group<br>10/1/2019 1:03:20 PM : Connecting to Computer<br>10/1/2019 1:03:20 PM : Successfully Paused Protection |  |
|---|--|





#### **Resume Protection**

The Resume Protection feature lets you resume protection for computers whose protection is paused.

To resume protection for computers, follow the steps given below:

1. In the Managed Computers folder tree, select a group and then click **Client Computers**.

The right pane displays the list of computers in the group and their detailed information.

| Search Supdate Agent                                      |                     |                     |                              |                     |             |  |  |
|---|---------------------|---------------------|------------------------------|---------------------|-------------|--|--|
| Action List  Computer Select Columns Computer Selected: 1 |                     |                     |                              |                     |             |  |  |
| 🖻 🚞 Managed Computers                                     | 💿 💻 eScan Installed | 🔿 🔳 eScan Not Insta | alled                        |                     |             |  |  |
| 🔯 Policy  | Computer Name       | IP Address          | IP Address of the connection | <u>User name</u>    | Local Admi  |  |  |
| - Group Tasks   |                     | 10.000.000          |                              | \$10110 (\$E\$1000) | Administrat |  |  |
|   |                     |                     |                              |                     |             |  |  |
| E - Caming Users  |                     |                     |                              |                     |             |  |  |
| 🗄 🧮 sample  |                     |                     |                              |                     |             |  |  |
|   |                     |                     |                              |                     |             |  |  |
|   |                     |                     |                              |                     |             |  |  |

2. Select client computers and then click **Client Action List** > **Resume Protection**. Client Status window appears displaying the progress.

| C | lient Status   | p |
|---|--|---|
|   | 10/1/2019 1:03:54 PM : Processing with group : Sample Group<br>10/1/2019 1:03:54 PM : Connecting to Computer ,<br>10/1/2019 1:03:54 PM : Successfully Resumed Protection |   |
|   |  |   |





### **Properties of Selected Computer**

To view the properties of a selected computer, follow the steps given below:

- 1. Select a computer.
- Click Client Action List > Properties. Properties window appears displaying details.



**NOTE** If multiple computers are selected, the Properties option will be disabled.





# **Unmanaged** Computers

To install eScan Client, define policies and tasks on the basis of group, it is necessary to move computers to the created groups. You can move the computers from **Unmanaged Computers** to desired groups created in the **Managed Computers** using the following submodules:

- Network Computers
- IP Range
- Active Directory
- New Computers Found





# **Network Computers**

This submodule displays a list of available networks. You can move the computers from the list of computers present in the Network Computers using the following steps –

- 1. In the navigation panel, click **Unmanaged Computers** > **Network Computers**.
- 2. Click Microsoft Windows Network.
- 3. Select the workgroup from where you want to move computers to the group created in Managed Computers section. A list of computers appears.

| Network Computers              |  |        |                  | 📚 Refresh        | 👔 Help     |
|--------------------------------|--|--------|------------------|------------------|------------|
| ₽ Search                       |  |        |                  |                  |            |
| Action List - 💦 Refresh Client |  |        |                  |                  |            |
| Network Computers              | Computer Name  | Groups | IP Address       | <u>User name</u> | <u>e</u> : |
| 🕂 🥻 Microsoft Windows Network  | and the second state of th |        | 1990-0000111-000 |                  | U          |
| ESBS                           |  |        | 8888011-1-881    |                  | U          |
| TESTD1                         |  |        | 991-88011-980    |                  | U          |
| WORKGROUP (67)                 |  |        | 10-10-10-11-00-1 |                  | U          |
| Web Client Network             |  |        | 49-1490-1-1490   |                  | e          |
|                                |  |        | 100              |                  | U          |
|                                | -Constant  |        | 49-14011-40      |                  | U          |
|                                |  |        |                  |                  | Ui         |

- 4. Select the computer(s) you want to move to the desired groups.
- 5. Click **Action List** > **Move to Group**. Select Group window appears.
- 6. Click **Managed Computers** tree to view the groups.

|                           | ×      |
|---------------------------|--------|
| Select Group              | 🝸 Help |
| Move Computer(s) to Group |        |
| 🗄 🚍 Managed Computers     |        |
| Roaming Users             |        |
| - Caroup                  |        |
|                           |        |
|                           |        |
|                           |        |
|                           |        |
|                           |        |
|                           |        |
|                           |        |
|                           |        |
| New Group Ok Cancel       |        |
|                           |        |

7. Select the group where you wish to move the selected computer(s) and click **OK**. The selected computer(s) will be moved to the group.





# Creating a New Group from the Select Group window

To create a new group from the Select Group window, follow the steps given below:

1. In the Select Group window, click **Managed Computers** > **New Group**.

|                           |   | ×    |
|---------------------------|---|------|
| Select Group              | ? | Help |
| Move Computer(s) to Group |   |      |
| ₩ 🚰 Managed Computers     |   |      |
| New Group Ok Cancel       |   |      |

Creating New Group window appears.

|                     |                  | ×      |
|---------------------|------------------|--------|
| Creating New G      | roup             | 🝸 Help |
| New Group<br>Name : | Create New Group |        |
| Ok                  | Cancel           |        |

- 2. Enter a name for the group.
- 3. Click **OK**. A new group will be created.





# **IP** Range

The **IP Range** submodule lets you scan the desired IP address or range of IP address and add the required computers to any of the managed groups. It also lets you add, search and delete an IP range.

### Adding New IP Range

To add an IP range, follow the steps given below:

1. In the IP range screen, click **New IP Range.** Specify IP Range window appears.

|                       |          | ×            |
|-----------------------|----------|--------------|
| Specify IP Range      |          | 🝸 Help       |
|                       |          |              |
|                       |          |              |
|                       |          |              |
|                       |          |              |
| Starting IP Address*: | ·        |              |
| Ending IP Address*:   |          |              |
|                       |          |              |
|                       |          |              |
|                       |          |              |
|                       |          |              |
| OK Cancel             | (*) Mand | atory Fields |

- 2. Enter the Starting and Ending IP address.
- 3. Click **OK**. The IP Range will be added.

Please enter the start and end IP address even if you want to search for single IP address, both the entries will have the same IP address in such a case. The selected
 IP Range will be added to the IP Range tree.
 When you select the IP Range all computers present in that IP Range will be displayed on the interface in the right.

Other details like IP Address of the computer, its group, Protection status (Unmanaged/Unknown/Protected/Not installed, Critical/Unknown); the table also displays Status of all modules of eScan.





#### Moving an IP Range to a Group

To move an entire IP range to a group, follow the steps given below:

- 1. Select an IP range.
- 2. Select the checkbox next to Computer Name column.
- 3. Click **Action List** > **Move to Group**. Select Group window appears.
- 4. Select the destination group.
- 5. Click **OK.** The IP range will be moved to the specified group.

#### Deleting an IP Range

To delete an IP range, follow the steps given below:

- 1. Select an IP Range.
- 2. Click **Delete IP Range**.

| IP Rang | e           |                  |                    |         |                 |
|---------|-------------|------------------|--------------------|---------|-----------------|
|         |             |                  |                    |         |                 |
| Act     | tion List 🔻 | 📑 New IP Range   | <u>व</u> Delete II | P Range | Search IP Range |
| M IP    | Range       |                  |                    |         | Computer Name   |
|         |             |                  | 1.8.8              |         | -               |
|         | 10.100      | 11.138.188.33.31 |                    |         |                 |
| - 🌧     | 10.100      |                  |                    |         |                 |
| - 🍂     | 10.100      | 120.00.000017    |                    |         |                 |
|         | 10.100      |                  |                    |         |                 |
|         | 33.38       |                  |                    |         |                 |

A confirmation prompt appears.



3. Click **OK**. The IP range will be deleted.





# **Active Directory**

The Active Directory submodule lets you add computers from an Active Directory.

### Adding an Active Directory

To add an Active Directory, follow the steps given below:

- 1. Click **Unmanaged Computers** > **Active Directory**.
- 2. Click Properties.

| Active Directory           |  |
|----------------------------|--|
| Action List 🗸 💕 Properties |  |
| 🦾 💑 Active Directory       |  |

Properties window appears.

| Properties                                 |
|--|
| 🔁 Add 🛃 Modify 💼 Delete                    |
| Active Directory Domain Controller Address |
| ОК   |

3. Click Add. Login Settings window appears.

| Login Settings      |     | 👔 Help               |
|---------------------|-----|----------------------|
|                     |     |                      |
| AD IP Address *:    |     |                      |
| User name *:        |     |                      |
| Password *:         |     |                      |
| Confirm Password *: |     |                      |
| Use SSL Auth.:      |     |                      |
| AdsPort*:           | 389 |                      |
|                     |     |                      |
| OK Cancel           |     | (*) Mandatory Fields |

 Fill in the required Login Credentials and click **OK**. The details including IP Addresses from active directory will be added instantly.





| Properties 7 H                             | elp |
|--|-----|
| Add 🛃 Modify 👔 Delete                      |     |
| Active Directory Domain Controller Address |     |
| 92.168.                                    |     |
| ОК   |     |

- 5. Select the Active Directory and click **OK**. The selected Active Directory will be added to the Active directory tree.
- 6. To view the details, click the **Active Directory**.

| Active Directory  |   |             |  | 💲 Refresh  ি He  |  |  |
|---|---|-------------|--|------------------|--|--|
| Action List  Properties   |   |             |  |                  |  |  |
| Active Directory      Active Directory  | G (A134     GA34     GA34 |             | Unknown status Unknow |                  |  |  |
| Constanting C | General     G |             | Unknown status<br>Unknown status<br>Unknown status<br>Unknown status   |                  |  |  |
|   | 📃 Unmanaged   | 📃 Protected | 💻 Not Installed / Critical   | 📃 Unknown status |  |  |

#### Moving Computers from an Active Directory

To move computers from an Active Directory, follow the steps given below:

- 1. Click an Active Directory.
- 2. Select the computers you want to move to other group.
- 3. Click **Action List** > **Move to Group**. Select Group window appears.
- 4. Select the Group and Click **OK**.

The selected computers will be moved to the selected group.





# **New Computers Found**

The New Computers Found submodule displays list of all new computers connected to the network. With the Action List drop-down you can set Host Configuration, Move Computers to a Group, view Properties and Refresh Client. You can also export the New Computers List to .xls file format.

After the computers are moved from Unmanaged Computers to groups under Managed Computers, you can assign it tasks, Set host configuration, Manage Policies, Deploy/Upgrade Client or deploy a Hotfix on all or any of the Managed Computer individually or in group.

| N | New Computers Found           |   |                  |           |                      |            |                     |  |
|---|-------------------------------|---|------------------|-----------|----------------------|------------|---------------------|--|
|   | Search                        |   |                  |           |                      |            |                     |  |
|   | Action List - Filter Criteria |   |                  |           |                      |            |                     |  |
|   |                               | Computer Name                                 | IP Address       | User name | Last Seen            | Belongs To | <u>eScan Status</u> |  |
|   |                               |   |                  |           | 23 Sep 2019 10:59:59 | Server     | Unknown status      |  |
|   |                               | an and an | 1891-1880-1991   |           | 23 Sep 2019 10:59:54 | Server     | Unknown status      |  |
|   |                               | ······································        | 1997-1898-11100  |           | 23 Sep 2019 11:00:12 | Server     | Unknown status      |  |
|   |                               | in the second state                           | 1891-1890-1-1201 |           | 23 Sep 2019 11:00:12 | Server     | Unknown status      |  |
|   |                               |   | 1997-1899-1-741  |           | 23 Sep 2019 10:59:54 | Server     | Unknown status      |  |
|   |                               |   | 1001100017-001   |           | 23 Sep 2019 10:59:54 | Server     | Unknown status      |  |
|   |                               | Jan 1999                                      | 100-100-1-00     |           | 23 Sep 2019 11:00:01 | Server     | Unknown status      |  |

#### Filter Criteria

The Filter Criteria lets you filter new computers found according to date range.

| New Computers Found             |                               |  |  |  |  |  |
|---------------------------------|-------------------------------|--|--|--|--|--|
| ₽ Search                        |                               |  |  |  |  |  |
| Action List 👻 🗣 Filter Criteria | Action List - Filter Criteria |  |  |  |  |  |
| Filter Criteria                 |                               |  |  |  |  |  |
| Date Range                      |                               |  |  |  |  |  |
| From (MM/DD/YYYY)               | 11/06/2019                    |  |  |  |  |  |
| To (MM/DD/YYYY)                 | 11/06/2019                    |  |  |  |  |  |
| Search Reset                    |                               |  |  |  |  |  |

- 1. Select appropriate date in **From** and **To** fields.
- 2. Click Search.

A list of computers discovered by eScan in the date range will be displayed.





### Action List

This drop-down provides following options:

- Set Host Configuration: To learn more, click here.
- Deploy/Upgrade Client: To learn more, click here.
- Move to Group: To learn more, <u>click here</u>.
- **Refresh Client**: To learn more, <u>click here</u>.
- **Export to Excel**: This option lets you to export the status of particular system into Excel reports.
- **Properties**: To learn more, <u>click here</u>.





# **Report Templates**

The Report Templates module lets you create template and schedule them according to your preferences. The module also consists of pre-loaded templates according to which the report can be created and scheduled.

| Repo | ort Templates  | 🖉 Properties 🤹 Refresh | 🝸 Help |
|------|--|------------------------|--------|
|      |  |                        |        |
|      | New Template 🛐 Create Schedule 🔐 Properties 🕤 Delete |                        |        |
| _    | Template Name  |                        |        |
|      | Virus Report   |                        |        |
|      | Update Report  |                        |        |
|      | Scan Report  |                        |        |
|      | Web Protection Report                                |                        |        |
|      | Application Control Report                           |                        |        |
|      | Attachment Control Report                            |                        |        |
|      | Anti-Spam Report                                     |                        |        |
|      | Mail Anti-Virus Report                               |                        |        |
|      | USB Control Report                                   |                        |        |
|      | Group Summary Report                                 |                        |        |
|      | Hardware Report                                      |                        |        |
|      | Software Report                                      |                        |        |
|      | File Activity Report                                 |                        |        |
|      | Computers with Critical Status Report                |                        |        |
|      | Asset Changes (Software) Report                      |                        |        |
|      | Asset Changes (Hardware) Report                      |                        |        |
|      | Top 10 Summary Report                                |                        |        |
|      | Anti-Ransomware Report                               |                        |        |





# Creating a Report Template

To create a Report Template, follow the steps given below:

- 1. In the navigation panel, click **Report Templates**.
- 2. Click **New Template**. New Template screen appears.



- 3. Enter a name for the template.
- 4. Select a report enter. Depending upon the report enter, the additional setting varies.
- 5. After making the necessary selections/filling data, click **Save**. The template will be created according to your preferences.





# Creating Schedule for a Report Template

The Report Template module lets you create a new schedule for the report templates. To learn more, <u>click here</u>.

# Viewing Properties of a Report Template

To view the properties of Report Template, follow the steps given below:

- 1. Select the Report Template whose properties you want to view.
- 2. Click **Properties**. Properties screen appears.

| Propertie         | 5                           |           |                      | 🝸 Help |
|-------------------|-----------------------------|-----------|----------------------|--------|
| <u>Report Ten</u> | nplates > sample Properties |           |                      |        |
| Co                | Popert Period               | % Cout Pu |                      |        |
| Ge                |                             | C SULL DY |                      |        |
|                   | Report Name                 |           |                      |        |
|                   | Report Name :               | sample    |                      |        |
|                   | Details                     |           |                      |        |
|                   | Selected Template Type      | :         | VIRUS REPORT         |        |
|                   | Created:                    |           | 5/29/2020 1:40:10 PM |        |
|                   | Modified:                   |           | 5/29/2020 1:40:10 PM |        |
|                   |                             |           |                      |        |
|                   |                             |           |                      |        |
|                   |                             |           |                      |        |

**NOTE** Depending upon the Report Template enter, the Properties varies.

3. After making the necessary changes, click **Save**. The Report Template's properties will be updated.

# Deleting a Report Template

To delete a Report Template, follow the steps given below:

- 1. Select the template you want to delete.
- 2. Click **Delete**.

A confirmation prompt appears.

3. Click **OK**. The Report Template will be deleted.

**NOTE** Default Report Templates cannot be deleted.





# **Report Scheduler**

The Report Scheduler module lets you create schedule, update and run the task according to your preferences.

Creating a Schedule

To create a Schedule, follow the steps given below:

1. In the Report Scheduler screen, click **New Schedule**. New Schedule screen appears.



- 2. In the **Settings** section, select preferred templates.
- 3. In the **Select Condition** section, select a condition for groups or specific computers.



4. In the **Send Report by Email** section, fill the required information to receive reports via email.





| Report Sender*:                     |    |          |        |
|-------------------------------------|----|----------|--------|
| Report Recipient*:                  |    |          | Add    |
|                                     |    | <b>A</b> | Delete |
|                                     |    | •        |        |
| Mail Server IP Address:             |    |          |        |
| Mail Server Port:                   | 25 |          |        |
| User Authentication:                |    |          |        |
| Password Authentication:            |    |          |        |
| * For Example: user@yourcompany.com |    |          |        |
|                                     |    |          |        |

- 5. Select the preferred report format.
- 6. In **Report Scheduling Settings** section, make the necessary changes.

| Enable Scheduler  | O Manual Start  |
|-------------------|-----------------|
| Daily             |                 |
| Weekly            | Mon Tue Wed Thu |
|                   | Fri Sat Sun     |
| Monthly           | 1 .             |
| Last Day of Month |                 |
|                   |                 |
| At 12:            | 00 pm           |
|                   |                 |

7. Click Save.

New schedule will be created.





# Viewing Reports on Demand

To view a report or a set of reports immediately, follow the steps given below:

1. Click **Report Scheduler** > **View & Create**. New Schedule screen appears.

| Report Scheduler > New Schedule  |  |
|--|--|
| Settings   |  |
| Select a Template for creating a Report  |  |
| Software Report     Software Report     Software Report     Scan Report     Scan Report     Scan Report     Select Condition |  |
| <ul> <li>Generate a Report for Groups</li> <li>Generate a Report for a List of Computers</li> </ul>                          |  |
| Select Target Groups   |  |
| Create Schedule Cancel View  |  |

- 2. Select the **Template** options, the **Condition** and the **Target Groups**.
- 3. Click **View**. A new window appears displaying the created report.

Clicking **Create Schedule** lets you create a new Schedule.





# Managing Existing Schedules

The Report Scheduler module lets you manage the existing schedules.

| Re  | Report Scheduler |               |                                   |                     |  |  |  |  |
|---|------------------|---------------|-----------------------------------|---------------------|--|--|--|--|
| Start Task 🕞 Results 🔐 Properties 👘 Delete 📑 New Schedule 👘 View & Create |                  |               |                                   |                     |  |  |  |  |
| 1   |                  | Schedule Name | Report Recipient                  | Scheduler Type      |  |  |  |  |
| 6   | /                | Hardware      | 1899 11 1111                      | Manually Start      |  |  |  |  |
| 0   |                  | New Report    | ALTERNATION CONTRACTOR CONTRACTOR | Manually Start      |  |  |  |  |
| (   |                  | New Report_1  |                                   | Automatic Scheduler |  |  |  |  |

#### Generating Task Report of a Schedule

To generate a task report, select the preferred report schedule name and click **Start Task**. A task window appears displaying the name of the report being generated.

### Viewing Results of a Schedule

To see the results of a schedule and its time stamp, select the report schedule and click **Results**. Results screen appears.

| Results(Hardware)         |                       |  |  |  |  |
|---------------------------|-----------------------|--|--|--|--|
| Report Scheduler >Results |                       |  |  |  |  |
| <u>Status</u>             | <u>Time</u>           |  |  |  |  |
| Completed                 | 9/21/2019 12:25:25 PM |  |  |  |  |
| Cancel                    |                       |  |  |  |  |





### Viewing Properties of a Schedule

To view the properties of a schedule, follow the steps given below:

- 1. Select a schedule.
- 2. Click **Properties**. Properties screen appears.

| Properti  | 25                   |                      |
|-----------|----------------------|----------------------|
| Report So | heduler >Properties  |                      |
|           | General Schedule Set | tings Groups         |
|           |                      |                      |
|           | Schedule Name :*     | Hardware             |
|           | Created:             | 09/20/19 04:42:20 PM |
|           | Status:              | Task Completed       |
|           |                      |                      |
|           |                      |                      |
| Ok        | Cancel               |                      |

The properties screen displays general properties and lets you configure Schedule, Settings and Groups settings.

### Deleting a Schedule

To delete a report schedule, follow the steps given below:

- 1. Select a schedule.
- 2. Click **Delete**. A confirmation prompt appears.



3. Click **OK**.

The schedule will be deleted.





# **Events and Computers**

eScan Management Console maintains the record of all the events sent by the client computer. Through the events & computers module, the administrator can monitor the Events and Computers, The module lets you sort the computer with specific properties.



# **Events Status**

The Event Status subfolder is divided into following sections:

- Recent
- Critical
- Information

#### Recent

The Recent section displays both Information and Critical events.

#### Critical 🝪

The Critical section displays Critical events and immediate attention.

For example, Virus detection, Monitor disabled.

The Critical events can be filtered on the basis of date range and the report can be exported in .xls or .html format.

#### Information 🕕

The Information section displays basic information events. For example, Virus database update, Status.





# **Computer Selection**

The Computer Selection subfolder displays computers that fall under different categories. It lets you select the computer and take the preferred action. You can also set the criteria for each section and sort the computer accordingly.

| Events & Computers           |   |  |  |  |  |  |  |
|------------------------------|---|--|--|--|--|--|--|
| Settings D Edit Selection -  |   |  |  |  |  |  |  |
| 🗄 🔝 Events & Computers       | Computer Selection                      |  |  |  |  |  |  |
| 🗄 🔝 Events Status            | Computers with the "Critical Status"    |  |  |  |  |  |  |
| ① Computers Selection        | 💭 Secondary Server Status (Not Updated) |  |  |  |  |  |  |
| 🗄 🔝 Software/Hardware Change | Computers with the "Warning Status"     |  |  |  |  |  |  |
| 🗄 🔝 Date / Time Violations   | 💭 Database are Outdated                 |  |  |  |  |  |  |
|                              | Many Viruses Detected                   |  |  |  |  |  |  |
|                              | 💭 No eScan Antivirus Installed          |  |  |  |  |  |  |
|                              | Not Connected for a long time           |  |  |  |  |  |  |
|                              | 💭 Not Scanned for a long time           |  |  |  |  |  |  |
|                              | Deprotection is off                     |  |  |  |  |  |  |
|                              | 📜 Update Agent Status                   |  |  |  |  |  |  |

The Computer Selection subfolder consists following sections:

- Computers with the "Critical Status"
- Secondary Server Status (Not Updated)
- Computers with the "Warning Status"
- Database are Outdated
- Many Viruses Detected
- No eScan Antivirus Installed
- Not Connected for a long time
- Not Scanned for a long time
- Protection is off
- Update Agent Status

#### Computers with the "Critical Status"

This section displays computers marked with Critical status.

#### Secondary Server Status (Not Updated)

A secondary server receives downlaods from the primary server and further distributes to the client computers. If the secondary server is not updated, it will be mentioned in the log.

#### **Computers with warning status**

This section displays computer with a warning status.

#### **Database is outdated**

This section displays computers whose virus database is outdated.

#### **Many Viruses Detected**

This section displays the computers whose virus count has exceeded.





#### No eScan installed

This section displays computers on which eScan is not installed.

#### Not connected for a long time

This section displays the computers which didn't connect to the eScan server for the set duration.

#### Not scanned for a long time

This section displays the computers which weren't scanned for the set duration.

#### **Protection is off**

This section displays the computers on which File Protection is disabled.

#### **Update Agent Staus**

This section displays the status of computers assigned as Update Agent.

The additional settings vary depending upon the Computer Status.

### Software/Hardware Changes

This subfolder displays all software/ hardware changes that occurred on computers. It consists following sections:

- Software Changes
- Hardware changes
- Existing System Info

| Events & Computers           |  |  |  |  |  |  |  |
|------------------------------|--|--|--|--|--|--|--|
|                              |  |  |  |  |  |  |  |
| Settings Edit Selection V    |  |  |  |  |  |  |  |
| 🖻 🔝 Events & Computers       | Software/Hardware Changes                                      |  |  |  |  |  |  |
| 🔃 证 Events Status            | L Software Changes<br>Hardware Changes<br>Existing System Info |  |  |  |  |  |  |
|                              |  |  |  |  |  |  |  |
| 🗄 🔝 Software/Hardware Change |  |  |  |  |  |  |  |
| 🗄 🔝 Date / Time Violations   |  |  |  |  |  |  |  |
|                              |  |  |  |  |  |  |  |
|                              |  |  |  |  |  |  |  |

#### **Software Changes**

This section displays software changes i.e. installation, uninstallation or software upgrades.





#### Hardware changes

This section displays hardware changes that occurred on computers. For example, IP address. Hard Disk, RAM etc.

#### **Existing System Info**

This section displays a computer's existing hardware information.

# Violations

#### **Date/Time Violations**

This subfolder consists Date/Time Violations that displays client computers whose users attempted to modify date and time.

| Events & Computers            |              |             |              |               |                  |                         |               | \$                 | Refresh     | 👔 Helj |
|-------------------------------|--------------|-------------|--------------|---------------|------------------|-------------------------|---------------|--------------------|-------------|--------|
| Edit Selection -              |              |             |              |               |                  |                         |               |                    |             |        |
| 🗄 🚺 Events & Computers        | ▲ Filter /   | Criteria    |              |               |                  | Export Option           |               |                    |             |        |
| 🗄 🚺 Events Status             |              |             |              |               |                  |                         | _             |                    |             |        |
| Computers Selection           | :e / Time Vi | olations Ev | ents         |               |                  | 1 - 9 of 9              | ) H page 1    | of 1 ⊨ Rows per pa | age: 10     | - Î    |
| 🗄 🚺 Software/Hardware Changes | <u>de</u>    | Time        | Machine Name | IP Address    | <u>User name</u> | Event Id                | Module Name   | Description        |             |        |
| - 12 Software Changes         | ) 3/6/2018   | 15:58:18    | COMPLEX      | 192.148.0.108 | COMPLEXIN        | File Anti-Mase (1801)   | eScan Monitor | Date/Time Modific  | ation Dis/  | abled  |
|                               | ) 3/6/2018   | 15:58:04    | COMPLES      | 192.348/0.108 | COMPLEXIN        | File Arth-Street (1804) | eScan Monitor | Date/Time Modific  | ation Dis:  | abled  |
| 🗄 🔃 Violations                | 3/6/2018     | 15:58:02    | COMPLES      | 192.148.0.108 | COMPLEXIN        | File Anti-Stree (1804)  | eScan Monitor | Date/Time Modific  | ation Dis:  | abled  |
| 🛄 🗍 Date / Time Violations    | ) 3/6/2018   | 14:50:16    | WE8307       | 192.148.7.84  | MEADER(UM        | File Anti-Mean (1801)   | eScan Monitor | Date/Time Modific  | ation Dis:  | abled  |
|                               | ) 3/6/2018   | 12:30:35    | WEADOW       | 192.148.0.217 | WEADOH/Dar       | File Anti-Stree (1805)  | eScan Monitor | Date/Time Modific  | cation Dis: | abled  |
|                               | ) 3/6/2018   | 12:30:15    | WEA208       | 192.148.7.79  | MEADDB/UM        | File Anti-Street (1895) | eScan Monitor | Date/Time Modific  | ation Dis/  | abled  |
|                               | 3/6/2018     | 12:30:15    | WEADOR       | 192.148.7.79  | MEADER COM       | File Anti-Stree (1805)  | eScan Monitor | Date/Time Modific  | ation Dis:  | abled  |
|                               | ) 3/6/2018   | 12:30:14    | WEA208       | 192.148.7.79  | WEADER/UN        | File Anti-Virus (1805)  | eScan Monitor | Date/Time Modific  | cation Dis: | abled  |
|                               | ) 3/6/2018   | 12:30:14    | WEATOR       | 192.148.7.79  | WEADER (UNV      | File Anti-Stree (1825)  | eScan Monitor | Date/Time Modific  | cation Dis: | abled  |
|                               |              |             |              |               |                  |                         |               |                    |             |        |
|                               |              |             |              |               |                  |                         |               |                    |             |        |

### Settings

You can define the Settings for Events, Computer Selection and Software/Hardware changes by clicking on the **Settings** option and defining the desired settings using the Tabs and options present on the Events and Computer settings window.





### **Event Status Setting**

Basically, events are activities performed on client's computer.

| Events & Computers | Settings           |                           | 👔 Help |
|--------------------|--------------------|---------------------------|--------|
| Events Status      | Computer Selection | Software/Hardware Changes |        |
| Events Events Na   | me Recent 💌        | 1000                      |        |
| Number             | r Of Records       | 1000                      |        |
|                    |                    |                           |        |
| Save               | Close              |                           |        |

On the basis of severity, the events are categorized in to the following types:

- **Recent:** It displays both critical and information events that occurred recently on managed client computers.
- **Critical:** It displays all critical events occurred on managed client computers, such as virus detection, monitor disabled status, and so on.
- **Information:** It displays all informative types of events, such as virus database update, status, and so on.

Steps to define event status settings:

Perform the following steps to save the event status settings:

- 1. Select the appropriate **Events Name**.
- 2. Enter the number of events that you want to view in a list, in the **Number of Records** field.
- 3. Click **Save**. The settings get saved.



### **Computer Selection**

| Ev | ents & Computers Settings  | 🝸 Help |
|----|--|--------|
|    | Events Status         Computer Selection         Software/Hardware Changes |        |
|    | Computers  |        |
|    | Computers Status Computers with the "Critical Status"                      | _      |
|    | Check for eScan Not Installed  |        |
|    | Check for Monitor Status   |        |
|    | Check for Not Scanned  |        |
|    | Check for Database Not Updated   |        |
|    | Check for Not Connected  |        |
|    | Database Not Updated from more than 7 days                                 |        |
|    | System Not Scanned from more than 7 days                                   |        |
|    | System Not Connected from more than 7 days                                 |        |
|    | Number Of Records  |        |
|    |  |        |
|    |  |        |
|    | Save Close   |        |
|    |  |        |
|    |  |        |

The **Computer Selection** lets you select and save the computer status settings. This module lets you do the following activities:

**Computers with the "Critical Status":** It displays a list of computers that are critical in status, as per the criteria\'s selected in computer settings. Specify the following field details.

- **Check for eScan Not Installed**: Select this checkbox to view the list of client systems under managed computers on which eScan has not been installed.
- **Check for Monitor Status**: Select this checkbox to view the client systems on which eScan monitor is not enabled.
- **Check for Not Scanned**: Select this checkbox to view the list of client systems which has not been scanned.
- **Check for Database Not Updated**: Select this checkbox to view the list of client systems on which database has not been updated.
- **Check for Not Connected**: Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **Database Not Updated from more than**: Enter the number of days from when the database has not been updated.
- **System Not Scanned for more than**: Enter the number of days from when the system has not been scanned.
- **System Not Connected for more than**: Enter the number of days from when the client system has not been connected to eScan server.
- **Number Of Records**: Enter the number of client systems that you want to view in the list.





**Secondary Server Status (Not Updated)**: A secondary server receives downlaods from the primary server and further distributes to the client computers. If the secondary server is not updated, it will be mentioned in the log.

• **Number Of Records**: Enter the number of client systems that you want to view in the list.

**Computers with Live status**: This section displays whether computers are Online or Offline.

• **Number Of Records**: Enter the number of client systems that you want to view in the list.

**Computers with the "Warning Status":** It displays the list of systems which are warning in status, as per the criteria\'s selected in computer settings. Specify the following field details:

- **Check for Not Scanned**: Select this checkbox to view the list of client systems which has not been scanned.
- **Check for Database Not Updated**: Select this checkbox to view the list of client systems on which database has not been updated.
- **Check for Not Connected**: Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **Check for Protection off**: Select this checkbox to view the list of client systems on which protection for any module is inactive.
- **Check for Many Viruses**: Select this checkbox to view the list of client systems on which maximum viruses are detected.
- **Database Not Updated from more than**: Enter the number of days from when the database has not been updated.
- **System Not Scanned for more than**: Enter the number of days from when the system has not been scanned.
- **System Not Connected for more than**: Enter the number of days from when the client system has not been connected to eScan server.
- Number Of Virus: Enter the number of viruses detected on client system.
- **Number Of Records**: Enter the number of client system that you want to view in the list.

**Database are Outdated:** It displays a list of systems on which virus database is outdated. Specify the following field details:

- **Database Not Updated from more than**: Enter the number of days from when the database has not been updated.
- **Number of Records**: Enter the number of client system that you want to view in the list.

**Many viruses Detected:** It displays a list of systems on which number of viruses exceeds the specified count in computer settings. Specify the following field details:

- **Number of Virus**: Enter the number of viruses detected on client system.
- **Number of Records**: Enter the number of client system that you want to view in the list.





**No eScan Antivirus Installed:** It displays the list of systems on which eScan has not been installed. Specify the following field detail:

• **Number of Records**: Enter the number of client system that you want to view in the list.

**Not connected to the eScan server for a long time:** It displays the list of systems which have not been connected to the server from a long time. Specify the following field detail:

• **Number of Records**: Enter the number of client system that you want to view in the list.

**Not scanned for a long time:** It displays the list of systems which have not been scanned from a long time, as specified in computer settings. Specify the following field details:

- **System Not Scanned for more than**: Enter the number of days from when the system has not been scanned.
- **Number of Records**: Enter the number of client system that you want to view in the list.

**Protection is off:** It displays the list of systems on which protection is inactive for any module, as per the protection criteria's selected in computer settings. It shows the status as "Disabled" in the list. Specify the following field details.

- **Check for Monitor Status**: Select this checkbox if you want to view the client systems on which eScan monitor is not enabled.
- **Check for Mail Anti-Phishing**: Select this checkbox if you want to view the list of client systems on which **Mail Anti-Phishing** protection is inactive.
- **Check for Mail Anti-Virus**: Select this checkbox if you want to view the list of client systems on which **Mail Anti-Virus** protection is inactive.
- **Check for Mail Anti-Spam**: Select this checkbox if you want to view the list of client systems on which **Mail Anti- Spam** protection is inactive.
- **Check for Endpoint Security**: Select this checkbox if you want to view the list of client systems on which **Endpoint Security** protection is inactive.
- **Check for Firewall**: Select this checkbox if you want to view the list of client systems on which **Firewall** protection is inactive.
- **Check for Proactive**: Select this checkbox if you want to view the list of client systems on which **Proactive** protection is inactive.
- **Check for Web Protection**: Select this checkbox if you want to view the list of client systems on which protection of
- **Web Protection** module is inactive.
- **Number of Records**: Enter the number of client system that you want to view in the list.

#### Steps to define computer settings

To save the computer settings, follow the steps given below:

1. Click Computers Selection tab.





- 2. Select a type of status for which you want to set criteria, from the **Computer status** drop-down.
- 3. Select the appropriate checkboxes, and then enter field details in the available fields. For more information, refer [Types and criteria of computer status] section.
- 4. Click **Save**. The settings will be saved.

### Software/ Hardware Changes Setting

You can set these settings, if you want to get updates on any changes made in the software, hardware, and to existing system.

| Country Charles | Computer Coloritor      | Software /Hardware Changes |   |
|-----------------|-------------------------|----------------------------|---|
| events status   | computer selection      | Surtware/Haruware Changes  | L |
|                 |                         |                            |   |
| [ Updates -     |                         |                            |   |
|                 | va/Handwaya Changes Ref | turne Changes 💌            |   |
| Softwa          | re/Hardware Changes Sor | tware changes 🔹            |   |
| Nun             | nber Of Days            | 1 days                     |   |
| Nun             | nber Of Records         | 1000                       |   |
|                 |                         |                            |   |
|                 |                         |                            |   |
|                 |                         |                            |   |
|                 |                         |                            |   |
| Save            | Close                   |                            |   |
|                 |                         |                            |   |
|                 |                         |                            |   |
|                 |                         |                            |   |

The **Software/ Hardware Changes** enable you to do the following activities: Type of Software/Hardware Changes

- Software changes
- Hardware changes
- Existing system info

To Change software/hardware settings, follow the steps given below:

- 1. Click the Software/Hardware Changes tab.
- 2. Specify the following field details.
  - **Software/Hardware Changes**: Click the drop-down and select the changes made.
  - **Number of Days**: Enter the number of days, to view changes made within the specified days.
  - **Number of Records**: Enter the number of client systems that you want to view in the list.
- 3. Click **Save**. The settings get saved.





### Performing an action for computer

To perform an action for a computer, follow the steps given below:

- 1. Select a computer.
- 2. Click **Edit Selection** drop-down.

| Edit Selection 🗸        |  |  |  |  |
|-------------------------|--|--|--|--|
| Protection              |  |  |  |  |
| Events                  |  |  |  |  |
| Deploy / Upgrade Client |  |  |  |  |
| Check Connection        |  |  |  |  |
| Remove from Group       |  |  |  |  |
| Connect to Client (RMM) |  |  |  |  |
| Force Download          |  |  |  |  |
| On Demand Scanning      |  |  |  |  |
| Send Message            |  |  |  |  |
| Properties              |  |  |  |  |

- 3. Click the preferred action.
  - **Protection**: This option is used to check the protection status of the computer.

|                             | ×    |
|-----------------------------|------|
| Protection                  | Help |
| Computers Status Warning    |      |
| Not Scanned for a long time |      |
|                             |      |
|                             |      |
|                             |      |
|                             |      |
| 4                           | •    |
| Close                       |      |
|                             |      |

- **Events**: This option provides the list of events performed on the computer.
- **Deloy/Upgrade Client**: To learn more, <u>click here</u>.
- **Check Connection**: This option used to check the connection between the endpoints. Once connection is successful, you will get the popup message for the same.





|                                    | × |
|------------------------------------|---|
|                                    | ? |
| Connecting to Computer SUPPORT-714 | ٦ |
| Connection : Successful            |   |
|                                    |   |
|                                    |   |
|                                    |   |
|                                    |   |
|                                    |   |
|                                    |   |
|                                    |   |
|                                    |   |
|                                    |   |
|                                    |   |
|                                    |   |
|                                    |   |
|                                    |   |
|                                    |   |
| Close                              | _ |
|                                    |   |

- **Remove from Group**: To learn more, <u>click here</u>.
- Connect to Client (RMM): To learn more, click here.
- Force Download: To learn more, click here.
- **On Demand Scanning**: To learn more, <u>click here</u>.
- Send Message: To learn more, <u>click here</u>.
- **Properties**: To learn more, <u>click here</u>.





# Tasks for Specific Computers

The Tasks for Specific Computers module lets you create a new task for computer(s) according to your preferences.

| Tasks For Specific Computers |                    |           |               |  |  |  |  |
|------------------------------|--------------------|-----------|---------------|--|--|--|--|
|                              |                    |           |               |  |  |  |  |
| New Task Start Task          | Properties Results |           |               |  |  |  |  |
| Task Name                    | Pending            | Completed | Schedule Type |  |  |  |  |

### Creating a task for specific computers

To create a task for specific computer(s), follow the steps given below:

- 1. In the navigation panel, click **Tasks for Specific Computers**.
- 2. Click **New Task**.

New Task Template form appears.

| New Task Template                               |                  |  |  |  |
|---|------------------|--|--|--|
| Tasks For Specific Computers >New Task Template |                  |  |  |  |
| Task Name                                       |                  |  |  |  |
| Tack Name:* Sample                              |                  |  |  |  |
| Task Name.                                      | P                |  |  |  |
| Assigned Tasks                                  |                  |  |  |  |
|   |                  |  |  |  |
| File Anti-Virus Status                          |                  |  |  |  |
| Enabled   |                  |  |  |  |
| Oisabled  |                  |  |  |  |
| Mail Anti-Virus Status                          |                  |  |  |  |
| Enabled   |                  |  |  |  |
| Disabled  |                  |  |  |  |
| Anti-Spam Status                                |                  |  |  |  |
| Enabled   |                  |  |  |  |
| Oisabled  |                  |  |  |  |
| Web Protection Status                           |                  |  |  |  |
| Enabled   |                  |  |  |  |
| Disabled  |                  |  |  |  |
| Endpoint Security Status                        |                  |  |  |  |
| Enabled   |                  |  |  |  |
| Disabled  |                  |  |  |  |
| Firewall Status                                 |                  |  |  |  |
| Disable Firewall                                |                  |  |  |  |
| Enable Limited Filter Mod                       | de of Firewall   |  |  |  |
| Enable Interactive Filter                       | Mode of Firewall |  |  |  |

- 3. Enter a name for task.
- 4. In the **Assigned Tasks** section, select the modules and scans to be run.





5. In the **Select Computers/Groups** section, select the computers/groups on which the tasks should be run and then click **Add**.

| - Select Computers/Groups       |               | <u>ــــــــــــــــــــــــــــــــــــ</u> |
|---------------------------------|---------------|---|
| 🖸 🧰 Roaming Users<br>🗹 💼 sample |               |   |
|                                 | Add<br>Remove |   |
|                                 |               |   |

6. In the **Tasks Scheduling Settings** section, configure the schedule settings.

| Enable Scheduler |          |     | Manual Start |     |
|------------------|----------|-----|--------------|-----|
| Daily            |          |     |              |     |
| Weekly           | Mon      | Tue | Wed          | Thu |
|                  | 🗖 Fri    | Sat | Sun          |     |
| Monthly          | 1 🔻      |     |              |     |
| At               | 12:00 pm |     |              |     |

7. Click **Save**. The task will be saved and run for specific computers according to your preferences.





# Viewing Properties of a task

To view Properties of a task, select the task and click **Properties**.

| mple                                    |                        | <b>7</b> |
|---|------------------------|----------|
| sks for specific computers > properties |                        |          |
| General Schedule Machines S             | ettings                |          |
| Task Name                               | sample                 |          |
| Task Creation Time:                     | 05/29/20 03:15:34 PM   |          |
| Status:                                 | Task not performed yet |          |
| Last Run:                               |                        |          |
|   |                        |          |
|   |                        |          |
| Chara D                                 |                        |          |

This section will have following tabs to configure:

- **General**: This tab allows to change the task name and provides details about the task creation, status, and last run.
- Sechedule: This tab allows to change the secheduler setting for the particular task.
- **Machines**: This tab allows to add or remove the endpoints added to the particular task.
- Settings: This tab allows to modify or select the modules and scans to be run.

**NOTE** To run a scheduled task manually, select the task and then click **Start Task**.

### Viewing Results of a task

To view Results of a task, select the task and click **Results**.

| Task Results (sample)                       |                             |                   |           |  |
|---|-----------------------------|-------------------|-----------|--|
| Tasks For Specific Computers > Task Results |                             |                   |           |  |
| Client Computers                            | Group                       | <u>Status</u>     | Date/Time |  |
|   | Managed Computers\TestGroup | Not Performed Yet |           |  |

This option will provide the summary details about the task like clients computers, group to which computers belong, status of the task, and more.





# Deleting a task for specific computers

To delete a task, follow the steps given below:

1. In the Tasks for Specific Computers screen, select the task you want to delete.

| Т | Tasks For Specific Computers                |            |         |           | 🤤 Refresh           | 🝸 Help             |  |
|---|---|------------|---------|-----------|---------------------|--------------------|--|
|   |   |            |         |           |                     |                    |  |
|   | Tex New Task Task Properties Results Telete |            |         |           |                     |                    |  |
|   |   | Task Name  | Pending | Completed | Schedule Type       |                    |  |
|   | 1   | New Task   | 1       | 0         | Manually Start      | <u>Task Status</u> |  |
|   |   | New Task_1 | 1       | 0         | Automatic Scheduler | Task Status        |  |

#### 2. Click **Delete**.

A confirmation prompt appears.

| ×  |
|--|
| Tasks For Specific Computers                 |
| Do you want to Delete the Selected Task(s) ? |
| Ok Cancel                                    |

3. Click **OK**. The task will be deleted.




## Asset Management

This module displays list of hardware configuration, software installed, software version number and a Software report for Microsoft software installed on **Managed Computers**. The Asset Management module consists following tabs:

- Hardware Report
- Software Report
- Software License
- Software Report (Microsoft)

## Hardware Report

The Hardware Report tab displays hardware configuration of all Managed Computers.

| sset Management     |                   |                |                             |  | 💲 Refresh 🛛 👔 Help          |
|---------------------|-------------------|----------------|-----------------------------|--|-----------------------------|
| Hardware Repor      | Software Repor    | t Software     | License Software Report (Mi | crosoft)                                   |                             |
| 🔺 Filter Criteria   |                   |                | 🔺 Ехрог                     | t Option                                   |                             |
| Computer Details    |                   |                |                             | 1 - 2 of 2 🗔 ( page 1 of 1 )               | N Rows per page: 10 🔻       |
| Computer Name       | Group             | IP Address     | <u>User's name</u>          | Operating System                           | Service Pack                |
| 100.007101.07047300 | Managed Computers | 196-186101127  | 100 00 101 - PAU 1100 VB    | Windows 10 Professional 32-bit             | Build 18362.836             |
|                     | TestGroup         | 1001100111101  |                             | Windows XP Professional x64 Edition 64-bit | Service Pack 2 (Build 3790) |
|                     | TestGroup         | 199-18910-1891 |                             | Windows XP Professional x64 Edition 64-bit | Service Pack 2 (Build 3790) |

The tab displays following details of managed computers:

- Computer Name
- Group
- IP Address
- Username
- Operating System
- Service Pack
- OS Version
- OS Installed Date
- Internet Explorer
- Processor
- Motherboard
- RAM
- HDD
- Local MAC Adapter(s)
- Wi-Fi MAC [Adapter]
- USB MAC [Adapter]
- PC Identifying Number
- Motherboard Serial No
- Network Speed
- Disk Free Space
- PC Manufacturer





- PC Model
- MB Manufacturer
- Graphic Card Details
- Software

To view the list of Software along with the installation dates, click **View** in **Software** column.

### Filtering Hardware Report

To filter the Hardware Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

| <ul> <li>Filter Criteria</li> </ul> |     |             | Export Option         |                        |
|-------------------------------------|-----|-------------|-----------------------|------------------------|
| Filter Criteria                     |     |             |                       |                        |
| Select All                          | In  | clude All 🔻 |                       | #Add Asset Information |
| Computer Name                       | * • | Include 🔻   | Internet Explorer     | * Include V            |
| User's name                         | *   | Include 🔻   | OS Version            | * Include V            |
| Operating System                    | *   | Include 🔻   | Processor             | * Include V            |
| Motherboard                         | *   | Include 🔻   | Local Adapter         | * Include V            |
| RAM                                 | *   | Include 🔻   | Wifi Adapter          | * Include V            |
| Group                               | *   | Include 🔻   | USB Adapter           | * Include V            |
| PC IdentifyingNumber                | *   | Include 🔻   | Motherboard Serial No | * Include V            |
| OS Type                             | *   | Include 🔻   | HDD                   |                        |
| IP Address                          | *   | Include 🔻   | OS Installed Date     |                        |
| Service Pack                        | *   | Include 🔻   | Disk Free Space       |                        |
| PC Manufacturer                     | *   | Include 🔻   | PC Model              | * Include V            |
| MB Manufacturer                     | *   | Include 🔻   | Graphic Card Details  | * Include V            |
| Search Reset                        |     |             |                       | (*) View All Items     |

Select the parameters you want to be included in the filtered report.

### Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search.** The Hardware Report will be filtered according to your preferences.





### **Exporting Hardware Report**

To export the Hardware Report, click **Export Option**. Export Option field expands.

| Filter Criteria | <ul> <li>Export Option</li> </ul> |        |
|-----------------|-----------------------------------|--------|
| Excel           | • HTML                            | Export |

Select the preferred option and then click **Export**. A success message appears.



Click the link to open/download the file.

## Software Report

The Software Report tab displays list of Software along with the number of computers on which they are installed.

| Asset Management  | 🗢 Refresh 🛛 👔 Help  |
|---|---|
| Hardware Report Software Report Software License Software | Report (Microsoft)  |
| ▲ Filter Criteria   | Export Option   |
| Software Details  | 1 - 100 of 1000 H ( page 1 of 10 ) H Rows per page: 100 ▼ |
| Software Name   | Computer Count  |
| 1ClickDownloader  | 1   |
| 2007 Microsoft Office system                              | <u>16</u>   |
| 2in1 Coundition Zero 1.1&Counter-Strike 1.6(build 2738)   | 1   |
| 3.5G Connect V3.1   | 1   |
| 3.75G Digiconnect v2.0.8.1884                             | 1   |
| 3DP Chip Lite v17.05                                      | 1   |
| 3DP Chip Lite v18.05                                      | 4   |

To view the computers on which the specific software is installed, click the numerical in **Computer Count** column.

Computer list window appears displaying following details:

- Computer Name
- Group
- IP Address
- Operating System
- Software Version
- Installed Date





### Filtering Software Report

To filter Software Report, click Filter Criteria field. Filter Criteria field expands.

| ✓ Filter Criteria                  |   | <ul> <li>Export Option</li> </ul> |  |                    |
|------------------------------------|---|-----------------------------------|--|--------------------|
| – Filter Criteria<br>Software Name | * | Include 👻                         | Group By<br>Software Name                        |                    |
| Computer Name                      | * | Include 🗸                         | <ul> <li>Computer Name</li> <li>Group</li> </ul> |                    |
| Search Reset                       |   |                                   |  | (*) View All Items |

The Software Report can be filtered on the basis of **Software Name** or **Computer Name**.

### Software Name

Entering the Software name displays suggestions. Select the appropriate software.

### **Computer Name**

Click the drop-down and select the preferred computer(s).

### **Group By**

The results can be grouped by Software name, Computer name or Group. If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click Search.

The Software Report will be filtered according to your preferences.

### **Exporting Software Report**

To export the Software Report, click **Export Option**. Export Option field expands.

| <ul> <li>Filter Criteria</li> </ul> | l.    |        | Export Option                 |
|-------------------------------------|-------|--------|-------------------------------|
| Export Option                       |       |        |                               |
| O Excel                             | O PDF | • HTML | Export Export Detailed Report |

Select the preferred option and then click **Export**. OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**. A success message appears.







## Software License

The Software License tab displays list of Software Licenses of managed computers.

| sh 🝸 He |
|---------|
|         |
|         |
| 10 🔻    |
|         |
|         |
|         |
|         |

The log displays License Key, Software Name and Computer Count. To see more details of the computer's license key installed, click the numerical value in License Key or Computer Count column.

### Filtering Software License Report

To filter Software Report, click Filter Criteria field. Filter Criteria field expands.

| ▼ Filter Criteria    |     | Export Option      |
|----------------------|-----|--------------------|
| Filter Criteria      |     |                    |
| Software License Key | *   | Include V          |
| Software Name        | *   | Include T Group By |
| Computer Name        | * , | Include  Group     |
| IP Address           | *   | Include V          |
| OS Type              | 8   | Include T          |
| Search Reset         |     | (*) View All Items |

### Software License Key

Entering the license key displays suggestions. Select the appropriate key.

### Software Name

Entering the Software name displays suggestions. Select the appropriate software.

### **Computer Name**

Click the drop-down and select the preferred computer(s).

### **IP Address**

Entering the IP address displays suggestions. Select the appropriate IP address.

### **OS Type**

Enter the OS type.

### Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After entering data in all fields, click **Search**. The Software License Report will be filtered according to your preferences.





### **Exporting Software License Report**

To export the Software License Report, click **Export Option**. Export Option field expands.

| Filter Criteria |            | <ul> <li>Export Option</li> </ul>                      |
|-----------------|------------|--|
| Export Option   |            |  |
| Excel O         | PDF   HTML | Export Detailed Report 🥙 Windows OS 🗹 Microsoft Office |

Select whether you want report for Windows OS and Microsoft Office.

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**. A success message appears.



Click the link to open/download the file.

## Software Report (Microsoft)

The Software Report (Microsoft) displays details of the Microsoft Software installed on the computers.

| Asset Management   | 🗢 Refresh 🛛 👔 Help                                    |
|--|---|
| Hardware Report         Software Report         Software License         Software           MS Office Software Report         Microsoft OS         Micro | Report (Microsoft)                                    |
| Filter Criteria  | Export Option   |
|  | 1 - 23 of 23 H ( page 1 of 1 ) H Rows per page: 100 ▼ |
| Software Name  | Computer Count  |
| Microsoft Office   | 38  |
| Microsoft Office 2003 Web Components   | 1   |
| Microsoft Office 2007 Primary Interop Assemblies   | 19  |
| Microsoft Office 2010 Primary Interop Assemblies   | 4   |
| Microsoft Office 365 - en-us   | 2   |
| Microsoft Office Access database engine 2007 (English)   | 2   |

The tab consists following subtabs:

- MS Office Software Report It displays Microsoft software name and computer count.
- Microsoft OS It displays Operating System, Service Pack, OS version and computer count.





### Filtering Software Report (Microsoft)

To filter Software Report (Microsoft), click Filter Criteria field. Filter Criteria field expands.

| ▼ Filter Criteria | <ul> <li>Export Option</li> </ul> |                    |
|-------------------|-----------------------------------|--------------------|
| Filter Criteria   |                                   |                    |
| Software Name     | Microsoft Office* Include T       | Group By           |
| Computer Name     | * 👻 Include 🔻                     | Group              |
| Search Reset      |                                   | (*) View All Items |

### **Computer Name**

Click the drop-down and select the preferred computer(s).

### **Group By**

If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click **Search**. The Software Report (Microsoft) will be filtered according to your preferences.

### Exporting Software Report (Microsoft)

To export the Software Report (Microsoft), click **Export Option**. Export Option field expands.

| Filter Criteria | a     |        | <ul> <li>Export Option</li> </ul> |
|-----------------|-------|--------|-----------------------------------|
| Export Option — |       |        |                                   |
| O Excel         | O PDF | • HTML | Export Detailed Report            |

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**. A success message appears.







### Filtering Microsoft OS Report

To filter the Microsoft OS report, click **Filter Criteria** field. Filter Criteria field expands.

| ▼ Filter Criteria |   | Export Option |                    |
|-------------------|---|---------------|--------------------|
| Filter Criteria   |   |               |                    |
| Operating System  | * | Include 🔻     |                    |
| Computer Name     | * | Include 🔻     | Group By           |
| Service Pack      | * | Include 🔻     | Group              |
| OS Version        | * | Include 🔻     |                    |
| Search Reset      |   |               | (*) View All Items |

### **Operating System**

Entering the operating system name displays list of suggestions. Select the appropriate OS.

#### **Computer Name**

Click the drop-down and select the preferred computer(s).

#### **Service Pack**

Entering the service pack name displays list of suggestions. Select the appropriate Service Pack.

### **OS Version**

Entering the OS version displays list of suggestions. Select the appropriate OS version.

### Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

#### After filling all the fields, click **Search**.

The Microsoft OS report will be filtered according to your preferences.

### **Exporting Microsoft OS Report**

To export the Microsoft OS Report, click **Export Option**. Export Option field expands.

| ▲ Filter Criteria |       |     | <ul> <li>Export Option</li> </ul> |        |
|-------------------|-------|-----|-----------------------------------|--------|
| Export Option     |       |     |                                   |        |
| O Excel           | O PDF | • н | TML                               | Export |

Select the preferred option and then click **Export**. A success message appears.







## User Activity

The User Activity module lets you monitor Print, Session and File activities occurring on the client computers. It consists following submodules:

- Print Activity
- Session Activity
- File Activity

## **Print Activity**

The Print Activity submodule monitors and logs print commands sent by all computers. It also lets you filter the logs on the basis of Computer name, Printer and Username. Furthermore, the module lets you export a detailed print activity report in .xls, .pdf and .html formats. The log report generated consists Print Date, Machine Name, IP Address, Username, Printer Name, Document Name along with number of Copies and Pages.

| Pr | int Activity                        |                            | Settings           | 📚 Refresh  👔 Help |
|----|-------------------------------------|----------------------------|--------------------|-------------------|
|    | <ul> <li>Filter Criteria</li> </ul> | Export Option              |                    |                   |
|    |                                     | <b>1 - 10</b> of 10 14 4 p | age 1 of 1 ) H Rov | vs per page: 10 🔻 |
|    | Printer Name                        |                            | <u>Copies</u>      | Pages             |
|    | Burrows (Test (Transp.              |                            | 3                  | 3                 |
|    | Report and Transport                |                            | <u>28</u>          | <u>34</u>         |
|    | BITTALINE   HERI - HERITER          |                            | 10                 | 192               |

### Viewing Print Activity Log

To view the Print log of a Printer, click its numerical value under **Copies** or **Pages** column. Print Activity window appears displaying details.

| Print Activity >>                                   | and the second second                            |               |                         |                           |  |        |       |  |  |  |  |  |
|---|--|---------------|-------------------------|---------------------------|--|--------|-------|--|--|--|--|--|
| fachine Name : *(Include) Export To:Select 🔻 Export |  |               |                         |                           |  |        |       |  |  |  |  |  |
|   | 1 - 3 of 3 H ( page 1 of 1 + H Rows per page: 10 |               |                         |                           |  |        |       |  |  |  |  |  |
| Client Date   | Machine Name                                     | IP Address    | User name               | Printer Name              | Document Name  | Copies | Pages |  |  |  |  |  |
| 18/09/19 1:33:43 PM                                 | a  | 1001100011110 | Second Company Station  | Bulley (BR) (Bridge       | NAMES // TABLE AND / CONTRACTORS OF AND A DESCRIPTION OF  | 1      | 1     |  |  |  |  |  |
| 18/09/19 12:40:41 PM                                | an   |               |                         | desident officer (Friday) | 144a / http://www.incomegno.com/http://wwww.incomegno.com/http://www.incomegno.com/http://www.in | 1      | 1     |  |  |  |  |  |
| 18/09/19 12:37:01 PM                                | and the second state Property of                 | 1001-000-0100 | Account Support Support | BUILDER CHERT STOLENE     | Http://internal/fainstructuragenatigeta-ag/fulfiligagamit-climing  | 1      | 1     |  |  |  |  |  |

To export this generated log, follow the steps given below:

- 1. Click the **Export to** drop-down.
- 2. Select a preferred format.
- 3. Click **Export**. A success message appears.







### Filtering Print Activity Log

To filter the print activity log, click **Filter Criteria**. Filter criteria field expands.

| <ul> <li>Filter Criteria</li> </ul> | •   | Export Option | n                  |
|-------------------------------------|-----|---------------|--------------------|
| Filter Criteria                     |     |               |                    |
| Computer Name                       | * • | Include 🔻     | Group By           |
| Printer                             | *   | Include 🔻     | Printer            |
| User name                           | *   | Include 🔻     | User name          |
| Date Range                          |     |               |                    |
| From (MM/DD/YYYY) 11/02/2019        |     |               |                    |
| To (MM/DD/YYYY) 11/02/2019          |     |               |                    |
| Search Reset                        |     |               | (*) View All Items |

### **Computer Name**

Click the drop-down and select the preferred computer.

### Printer

Enter the printer's name.

#### **User Name**

Enter the User's name.

#### Include/Exclude

Selecting Include/Exclude for a Machine or Printer lets you include or exclude it from the log.

### **Date Range**

To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**. The Print activity log will be filtered and generated according to your preferences.

### **Group By**

To view results by specific printer, select **Printer**, Date Range and click **Search**. To view results by specific user name, select **User name**, Date Range and click **Search**.





### **Exporting Print Activity Report**

To export the generated log, click **Export Option**. Export Option field expands.

| Filter Criteria |       | <ul> <li>Export Option</li> </ul> |        |
|-----------------|-------|-----------------------------------|--------|
| Excel           | O PDF | • HTML                            | Export |

Select the preferred option and then click **Export**. A success message appears.



Click the link to open/download the file.

### **Print Activity Settings**

Print Activity Settings lets you keep track of printers by adding them in a group and assigning it an alias name. The printers can be added or removed from this alias group.

To configure Print Activity Settings, follow the steps given below:

1. In the Print Activity screen, at the top right corner, click **Settings**. Printer Merge Setting window appears.

| lias Name |     | -          |        |              |        |
|-----------|-----|------------|--------|--------------|--------|
|           |     | Alias List |        | Printer List |        |
|           | Add |            | Remove | Add          | Remove |
|           |     | 4          | •      | 4            | •      |

- 2. Enter name in Alias Name field.
- 3. Select printer(s) for the alias.
- 4. Click **Add**. The printer(s) will be added to the alias.
- 5. Click **Save**. The Print Activity Settings will be saved.





## Session Activity Report

This submodule monitors and logs the session activity of the managed computers. It displays a report of the Operation type, Date, Computer name, Group, IP address and event description. With this report the administrator can trace the user Logon and Logoff activity along with remote sessions that took place on all managed computers.

### Viewing Session Activity Log

In the navigation panel, click **User Activity** > **Session Activity Report**. The log displays list of session activities and type of operation performed. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

| S | ession Activity Report |                     |   |               |                     |            |                            |          |  |  |
|---|------------------------|---------------------|---|---------------|---------------------|------------|----------------------------|----------|--|--|
| Γ | ▲ Filter Criteria      |                     |   | Export Option |                     |            |                            |          |  |  |
|   |                        |                     |   |               | 1 - 100 of 251 📧    | page 1 of  | 3 ) ▶ Rows per page: 100 ▼ |          |  |  |
|   | Operation Type         | <u>Client Date</u>  | Computer Name/Ip                        |               | Group               | IP Address | Description                | <b>^</b> |  |  |
|   | Start up               | 18/09/19 7:21:44 PM | (0.1014) (10-1000) (0.000)              |               | Marketing Team      | 10.00      |                            |          |  |  |
|   | Session LogOn          | 18/09/19 7:21:44 PM |   |               | Marketing Team      |            | User LogOn<br>User name:   |          |  |  |
|   | Shut Down              | 18/09/19 7:20:36 PM | 000000000000000000000000000000000000000 |               | Support Department  |            |                            |          |  |  |
|   | Session LogOff         | 18/09/19 7:20:32 PM | 10441041100-100100401                   |               | Support Department  |            | User LogOff<br>User name:  |          |  |  |
|   | Session LogOff         | 18/09/19 7:13:01 PM | 0.0000000000000000000000000000000000000 |               | Programming\Android |            | User LogOff<br>User name:  |          |  |  |
|   | Shut Down              | 18/09/19 7:01:51 PM | 000000000000000000000000000000000000000 |               | Production Dept     |            |                            |          |  |  |
|   | Session LogOff         | 18/09/19 7:01:49 PM | 10.0000 (C) (D. 10.0000)                |               | Production Dept     |            | User LogOff<br>User name:  |          |  |  |

### Filtering Session Activity Log

To filter session activities, click Filter Criteria field. Filter Criteria field expands.

| l | • Filter Criteria   |   |             | <ul> <li>Export Option</li> </ul> |   |                    |
|---|---------------------|---|-------------|-----------------------------------|---|--------------------|
|   | – Filter Criteria – |   |             |                                   |   |                    |
|   | Computer Name       | * | ✓ Include ▼ | IP Address                        | * | Include 🔻          |
|   | Operation Type      | * | ✓ Include ▼ | Group                             | * | Include 🔻          |
|   | Description         |   |             |                                   |   |                    |
|   | Date Range          |   |             |                                   |   |                    |
|   | From (MM/DD/YYYY)   |   | 09/19/2019  |                                   |   |                    |
|   | To (MM/DD/YYYY)     |   | 09/19/2019  |                                   |   |                    |
|   | Search Reset        |   |             |                                   |   | (*) View All Items |

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.





### **Computer Name**

Click the drop-down and select the preferred computers.

#### **Operation Type**

Click the drop-down and select the preferred activities.

#### Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the log.

#### **IP Address**

Enter the IP address in this field.

#### Group

Enter the group's name or click .... and select a group.

#### **Date Range**

To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**.

### **Exporting Session Activity Report**

To export the generated log, click **Export Option**. Export Option field expands.

| Filter Criteria |               |       |     | Export Option |        |
|-----------------|---------------|-------|-----|---------------|--------|
|                 | Export Option |       |     |               |        |
|                 | O Excel       | O PDF | • н | ITML          | Export |

Select the preferred option and then click **Export**. A success message appears.







## File Activity Report

The File Activity module displays a report of the files created, copied, modified, and deleted on managed computers. Additionally in case of a misuse of any official files can be tracked down to the user through the details captured in the report. Select and filter the report based on any of the details captured.

### Viewing File Activity Log

In the navigation panel, click **User Activity** > **File Activity Report**. The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

| 1 - 10 of 112848 ⊮∢ ∉ page 1 of 11285 |                     |                |            |                    |                  |               |             | Rows per page: 10 V |
|---------------------------------------|---------------------|----------------|------------|--------------------|------------------|---------------|-------------|---------------------|
| <u>Client Date</u>                    | Computer Name/Ip    | Group          | IP Address | <u>User's name</u> | File Action Type | Drive Type    | Source File | Destination File    |
| 4/20/2019 12:00:25 AM                 | 10.000.000          | 110,00         |            |                    | CREATE           | DRIVE_NETWORK | NewFile     | \\ \Images\GR000    |
| 4/20/2019 12:00:25 AM                 | 111082-05-10-       | (Instant)      | 01.01.10   |                    | CREATE           | DRIVE_NETWORK | NewFile     | \\ \Images\GR000    |
| 4/20/2019 12:01:52 AM                 | ILLUGRES (INC.      | <b>Phases</b>  |            |                    | CREATE           | DRIVE_NETWORK | NewFile     | \\ \images\GR000(   |
| 4/20/2019 12:01:52 AM                 | ALL AND A COLORADOR | (Instant)      |            |                    | CREATE           | DRIVE_NETWORK | NewFile     | \\ \images\GR000(   |
| 4/20/2019 12:04:15 AM                 | 111103-011-00-      | <b>Phyliot</b> |            |                    | CREATE           | DRIVE_NETWORK | NewFile     | \\ \Images\GR000    |
| 4/20/2019 12:04:15 AM                 | 11000 A 10-10-      | (Inside)       | -          |                    | CREATE           | DRIVE_NETWORK | NewFile     | \\ \Images\GR000    |

### Filtering File Activity Log

To filter file activities, click Filter Criteria field. Filter Criteria field expands.

| <ul> <li>Filter Criteria</li> </ul> |       |           | <ul> <li>Export Option</li> </ul> |     |                    |
|-------------------------------------|-------|-----------|-----------------------------------|-----|--------------------|
| Filter Criteria                     |       |           |                                   |     |                    |
| Computer Name                       | *     | Include 🔻 | IP Address                        | 26  | Include 🔻          |
| User's name                         | *     | Include 🔻 | Group                             | at: | Include 🔻          |
| File Action Type                    | *     | Include 🔻 | Drive Type                        | *   | ✓ Include ▼        |
| Source File                         | *     | Include 🔻 | Destination File                  | *   | Include 🔻          |
| Application                         | *     | Include 🔻 |                                   |     |                    |
| 🗹 Date Range                        |       |           |                                   |     |                    |
| From (MM/DD/YYYY)                   | 09/19 | /2019     |                                   |     |                    |
| To (MM/DD/YYYY)                     | 09/19 | /2019     |                                   |     |                    |
| Search Reset                        |       |           |                                   |     | (*) View All Items |

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

### **Computer Name**

Click the drop-down and select the preferred computers.

### Username

Enter the username of the computer.





### File Action type

Click the drop-down and select a preferred file action.

### Source File

Enter the source file's name.

### Application

Enter an application's name.

#### Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the log.

### **IP Address**

Enter an IP address.

### Group

Enter the group's name or click .... and select a group.

#### **Drive Type**

Click the drop-down and select the drive type.

#### **Destination File**

Enter the file path.

#### **Date Range**

To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**.

### **Exporting File activity Report**

To export the generated report, click **Export Option**. Export Option field expands.

| ▲ Filter Criteria |       |     | Export Option |        |
|-------------------|-------|-----|---------------|--------|
| Export Option     |       |     |               |        |
| O Excel           | O PDF | • н | TML           | Export |

Select the preferred option and then click **Export**. A success message appears.







## Patch Report

The Patch Report module displays the number of windows security patches installed and not installed on managed computers. This will help an administrator identify the number of vulnerable systems in the network and install the critical patches quickly.

| atch Management                     |                  |                   | 📚 Refresh 🛛 👔 H  |
|-------------------------------------|------------------|-------------------|--|
| Patch Report                        | All Patch Report |                   |  |
| <ul> <li>Filter Criteria</li> </ul> |                  | 📥 Ехро            | rt Option  |
|                                     |                  |                   | 1 - 10 of 255 K ( page 1 of 26 ) H Rows per page: 10 ▼ |
| Patch Name                          | Applied Count    | Not Applied Count | Not Applicable Count                                   |
| KB2207566                           | 0                | 0                 | Z  |
| KB2286198                           | 0                | 0                 | Z  |
| KB2305420                           | 0                | 0                 | Z  |
| KB2347290                           | 0                | 0                 | Z  |
| KB2393802                           | 0                | 0                 | Z  |
| KB2412687                           | 0                | 0                 | Z  |
| KB2419632                           | 0                | 0                 | Z  |
| KB2419635                           | 0                | 0                 | Z  |
| KB2419640                           | 0                | 0                 | Z  |
| KB2425227                           | 0                | 0                 | Z  |

## Patch report

The Patch report tab displays the Patch Name, Applied Count, Not Applied Count and Not Applicable Count. Clicking the numerical displays the patch name, details about the computer, the group it belongs to, IP address and User's name.

| Computer List >> KE     | 3958644                     |                |                     |  |
|-------------------------|-----------------------------|----------------|---------------------|--|
|                         |                             |                |                     | Export To:Select 👻 Export                  |
|                         |                             |                | 1 - 2 of 2 🔐 (page  | e 1 of 1 → ⊨ Rows per page: 10 →           |
| Computer Name           | <u>Group</u>                | IP Address     | <u>User's name</u>  | Operating System                           |
| HERE'S (Frank 1994)     | Managed Computers           | -368810-47     | AREASTAR (FAILTHAN) | Windows 10 Professional 32-bit             |
| THE PROPERTY PROFESSION | Managed Computers\TestGroup | 19911401111391 |                     | Windows XP Professional x64 Edition 64-bit |
|                         |                             |                |                     |  |

### Filtering Patch Report

To filter the Patch Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

| <ul> <li>Filter Criteria</li> </ul>   | <ul> <li>Export Option</li> </ul>       |              |
|---|---|--------------|
| Filter Criteria<br>Patch Name  Computer | Group By<br>Patch Name<br>Computer Name |              |
| Search Reset  | (*) Vi                                  | ew All Items |

Enter the Patch Name and Computer Name to be included in the filtered report.





### Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search.** The Patch Report will be filtered according to your preferences.

### **Exporting Patch Report**

To export the Patch Report, click **Export Option**. Export Option field expands. Select the preferred option and then click **Export**. A success message appears.



Click the link to open/download the file.

Other than security patch – for all patch Microsoft patch based on events **File AV** > **Advanced Settings** 

### All Patch Report

The All Patch Report tab displays all Microsoft patches based on following specific events.

- 1-KB patches
- 2-Security Update
- 4-Hotfix
- 8-Update
- 16-Service Pack
- 31-All

| P | atch Management                     |              |       |                                    | 🗢 Refresh 👔  | 🝸 Help |
|---|-------------------------------------|--------------|-------|------------------------------------|--|--------|
| _ | Patch Report All                    | Patch Report |       |                                    |  |        |
|   | <ul> <li>Filter Criteria</li> </ul> |              |       | <ul> <li>Export Option</li> </ul>  |  |        |
|   |                                     |              |       |                                    | 0 - 0 of 0   ( ( page 0 of 0 ) ) Rows per page: 10 | *      |
|   | Patch Name                          |              |       | Computer Count                     |  |        |
|   |                                     |              | There | are no items to show in this view. |  |        |
|   |                                     |              |       |                                    |  |        |
|   |                                     |              |       |                                    |  |        |





### Filtering All Patch Report

To filter the All Patch Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

| Patch Report All Patch Report                                  |   |  |
|--|---|--|
| ▼ Filter Criteria  | <ul> <li>Export Option</li> </ul>                             |  |
| Filter Criteria<br>Patch Name<br>Computer Name<br>Search Reset | <ul> <li>Include ▼</li> <li>* ▼</li> <li>Include ▼</li> </ul> | Group By  Patch Name Computer Name (*) View All Items  |
| Note : To enable   | All Patch Report Configure policy under File Antivirus-       | ->Advanced Setting>Send Windows Security Patch Events. |

Enter the Patch Name and Computer Name to be included in the filtered report.

 NOTE
 To enable All Patch Report Configure policy by going to File Antivirus-->

 Advanced Setting-->Send Windows Security Patch Events.

#### Include/Exclude

Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search**. The Patch Report will be filtered according to your preferences.

### **Exporting All Patch Report**

To export the All Patch Report, click **Export Option**. Export Option field expands.

Select the preferred option and then click **Export**. A success message appears.







## Notifications

This module lets you configure notifications for different actions/incidents that occur on the server. The Notifications module consists following submodules:

- Outbreak Alert
- Event Alert
- Unlicensed Move Alert
- New Computer Alert
- SMTP Settings

## **Outbreak Alert**

If the virus count exceeds the limits set by you, an outbreak email notification will be sent to the recipient.

To set an outbreak alert, follow the steps given below:

1. In the navigation panel, click **Notifications** > **Outbreak Alert**. Outbreak Notification screen appears.

| OutBreak Notification  |                         |
|--|-------------------------|
| OutBreak Alert Settings  |                         |
|  |                         |
| Send notification for viruses detected exceed the following number within the shown time |                         |
| Number 25 Time Limit 1 Day(s) T  | Configure SMTP Settings |
|  |                         |
| Save Cancel  |                         |

- 2. Select the checkbox **Send notification**.
- 3. Enter the preferred values in Number and Time Limit field.
- 4. Click **Save.** Outbreak Alert Settings will be saved.







## **Event Alert**

This submodule lets you enable email notifications about any event that occurs on the client computers connected to the server.

| Event Notification              |                         |
|---------------------------------|-------------------------|
| Events Alert Settings           |                         |
| Enable email alert Notification | Configure SMTP Settings |
| Save Cancel                     |                         |

To enable the event alert, follow the steps given below:

- 1. In the navigation panel, click **Notifications** > **Event Alert**.
- 2. Select the checkbox Enable email alert Notification.
- 3. Select the events from the list for which you prefer an alert.

| nts Aleri | t Set  | tings          |   |   |
|-----------|--------|----------------|---|---|
|           | 1      | Enable ema     | il alert Notification Configure SMTP Settings |   |
|           |        | Send Inform    | nation only in subject line                   |   |
| - Select  | t Eve  | ant Ide        |   | _ |
| Select    | t acti | vities for whi | ich email alert is required                   |   |
|           |        | Event Id       | Description                                   |   |
| 6         | •      | 154            | AVPMAPP_UPDATES_DONE                          |   |
| 0         |        | 100            | ESCAN_DUMMY_EVENT                             |   |
| (         |        | 1              | MWAV_FOUND_MALWARE                            |   |
| 0         |        | 2              | MWAV_FOUND_VIRUS_AND_DELETED                  |   |
| 0         |        | 3              | MWAV_FOUND_VIRUS_AND_CLEANED                  |   |
| 0         |        | 4              | MWAV_FOUND_ADWARE                             |   |
| (         |        | 5              | MWAV_FOUND_ERROR                              |   |
| (         |        | 6              | MWAV_FOUND_VIRUS_AND_RENAMED                  |   |
| (         |        | 7              | MWAV_FOUND_ADWARE_AND_DELETED                 |   |
| 0         |        | 8              | MWAV_LAST_COMPUTER_SCAN                       |   |
| 0         |        | 9              | MWAV_START                                    |   |
| 0         |        | 10             | MWAV_SUMMARY                                  |   |
| (         |        | 501            | SCHED_MWAV_FOUND_MALWARE                      |   |
| 0         |        | 502            | SCHED_MWAV_FOUND_VIRUS_AND_DELETED            |   |
| (         |        | 503            | SCHED_MWAV_FOUND_VIRUS_AND_CLEANED            |   |
| E         |        | 504            |   |   |

- 4. Select the required hosts or group.
- 5. Click **Save.** The Event Alert Settings will be saved.





## Unlicensed Move Alert

This submodule lets you enable notification alert when a computer automatically moves to Unlicensed Computers category based on the setting done (under events and computers) for the computer which is not connected to the server for a long time.

| Unlicense Move Notification                 |                         |
|---|-------------------------|
| Unlicense Move Alert Settings               |                         |
| Send notification for unlicensed computers. | Configure SMTP Settings |
|   |                         |
| Save Cancel                                 |                         |

To enable the unlicensed move alert, follow the steps given below:

- 1. In the navigation panel, click **Notifications** > **Unlicensed Move Alert**.
- 2. Select the checkbox **Send notification for unlicensed computers**.
- 3. Click **Save**.

The Unlicensed Move Alert Settings will be saved.

## New Computer Alert

This submodule lets eScan send you a notification alert when a new computer is connected to the server within the IP range mentioned under the Managed Computers.

| New Computers Notification   |                         |
|--|-------------------------|
| New Computers Alert Settings   |                         |
| Send new Computers added notification within the shown time<br>Time Limit 1 Day(s) T | Configure SMTP Settings |
| Save Cancel  |                         |

To enable the new computer alert, follow the steps given below:

- 1. In the navigation panel, click **Notifications > New Computer Alert**.
- 2. Select the checkbox **Send new Computers added notification within the shown time**.
- 3. Enter the preferred values in Time limit field.
- 4. Click Save.

The New Computer Alert Settings will be saved.





## **SMTP Settings**

This submodule lets you configure the SMTP settings for all the email notifications.

| rP Set | tings                                 |  |
|--------|---------------------------------------|--|
| ITP Se | ettings                               |  |
|        |                                       |  |
|        | Sender:                               |  |
|        | Recipient:                            |  |
|        | SMTP Server:                          |  |
|        | SMTP Port:                            |  |
|        |                                       |  |
|        | Use SMTP Authentication               |  |
|        | Use SMTP Authentication<br>User name: |  |

To configure the SMTP settings, follow the steps given below:

- 1. In the navigation panel, click **Notifications** > **SMTP Settings**.
- 2. Enter all the details.
- 3. Click Save.

The SMTP Settings will be saved.

To test the newly saved settings, click **Test**.





## Settings

The Settings module lets you configure general settings. It contains following submodules:

- **EMC Settings**: This submodule lets you define settings for FTP sessions, Log Settings, Client Grouping and Client connection settings.
- **Web Console Settings**: This submodule lets you define settings for web console timeout, Dashboard Settings, Login Page settings, SQL Server Connection settings, SQL Database compression settings.
- **Update Settings**: This submodule lets you define settings for General Configuration, Update Notifications, and Scheduling.
- **Auto-Grouping**: This submodule lets you define settings for Grouping of computers after installation of eScan client is carried out.
- **Two-Factor Authentication**: This submodule lets you to add extra layer of protection to your endpoints.





## **EMC Settings**

The **EMC** (eScan Management Console) **Settings** lets you configure the eScan Management Console. You can configure the FTP settings, Bind to IP Settings, Log Settings, Client Grouping and Client Connection Settings.

You can bind announcement of FTP server to particular IP by selecting the IP address in the list. However, you can choose to leave it as 0.0.0.0, which mean it will announce on all available interface/IP.

| EMC Settings   |
|--|
| EMC Settings   |
| FTP Settings       Settings  |
| LOG Settings<br>Delete the user settings and user log files after uninstalling.<br>No of days Client logs should be kept 7                   |
| Client Grouping<br>Group Clients by<br><ul> <li>NetBIOS</li> <li>DNS Domain</li> </ul>   |
| Client Connection Settings<br>Increase Thread count 10 (1-100)<br>Increase Query Interval 10 (In seconds ) (1-100)<br>Restore default values |
| Save Cancel  |

### **FTP Settings**

This setting lets you approve the log upload from client computers. It also lets you set the maximum FTP download sessions allowed for client computers. (Note: 0 means unlimited)





### **Bind IP Settings**

This setting lets you bind an IP address. Click the drop-down and select the preferred IP address for binding. The default IP address is 0.0.0.0.

### Log Settings

This setting provides you with the option to delete the User settings and Log files after uninstallation of eScan from the computer. To enable the above setting, select the checkbox. After selecting the checkbox, you can store client logs for the preferred number of days.

### **Client Grouping**

This setting lets you manually manage domains and computers grouped under them after performing fresh installations.

Select **NetBIOS**, if you want to group clients only by hostname.

Select **DNS Domain**, if you want to group clients by hostname containing the domain name.

### **Client Connection Settings**

This setting lets you modify **Thread Count** and **Query Interval** (In Seconds). To reset the values, select **Restore default values** checkbox.

After performing the necessary changes, click **Save**. The EMC Settings will be updated.





## Web Console Settings

Web Console Settings submodule lets you configure web console Timeout, Dashboard, Login Page, SQL Server Connection Setting, SQL Database compression and RMM Settings.

| Web Console Settings  |                    | 🝸 Help          |
|---|--------------------|-----------------|
|   |                    |                 |
| Web Console Timeout Setting                                     |                    |                 |
| Enable Timeout Setting  |                    |                 |
| Automatically log out the Web Console after 60 🔻 minutes        |                    |                 |
| DashBoard Setting   |                    |                 |
| Show Status for Last 7 days (1 - 365)                           |                    |                 |
| Login Page Setting  |                    |                 |
| Show Client Setup Link  |                    |                 |
| Show Agent Setup Link   |                    |                 |
| Show eScan AV Report Link                                       |                    |                 |
|   |                    |                 |
| Sql Server Connection Setting                                   |                    |                 |
| Microsoft Windows Authentication Mode                           |                    |                 |
| SQL Server Authentication Mode                                  |                    |                 |
| Server instance:  |                    | Browse          |
| Host Name/IP Address:   |                    | ]               |
| Login name  |                    | ]               |
| Password  | an entry were star | Test Connection |
| SQL Database Purge Settings                                     |                    |                 |
| Enable Database Purge   |                    |                 |
| Database Size threshold in (MB)                                 | 1024 (500 - 3027)  |                 |
| Purge data older than specified days, if above threshold is met | 7 days (7 - 365)   |                 |
| RMM Settings  |                    |                 |
| Activate View Only  |                    |                 |
| De-Activate View Only   |                    |                 |
| Screen Quality  | Medium 🔻           |                 |
| Screen Ratio  | 70% ▼              |                 |
| Save Cancel   |                    |                 |

### Web Console Timeout Settings





To enable web console Timeout, select **Enable Timeout Setting** option. After selecting the checkbox, click the drop-down and select the preferred duration.

### **Dashboard Setting**

This setting lets you set number of days for which you wish to View the Status, Statistics and Protection Status Charts in the Dashboard. Enter the preferred number of days.

### Login Page Setting

This setting lets you show or hide the download links shared for eScan Client setup, Agent setup and AV Report. To show the download links on login page, select the checkboxes of respective links.

### **SQL Server Connection settings**

This setting lets you select an authentication mode between Microsoft Windows Authentication Mode to SQL Server Authentication Mode. Select the **SQL Server Authentication Mode** and define **Server instance** and **Host Name** along with the credentials for connecting to the database.

### Server Instance

It displays the current server instance in use. To select another server instance, click **Browse**. Select an instance from the list and click **OK**.

#### Hostname/IP Address

It displays the Hostname or IP Address of the server instance computer.

### Enter the credentials in Username and Password fields.

To check whether correct credentials are entered, click **Test Connection**.

### SQL Database Purge Settings

This setting lets you define the maximum SQL database size in MB and purge data older than the specified days. To enable SQL Database Purge Settings, select **Enable Database Purge** checkbox.

Enter the preferred value in Database Size threshold in (MB) field.

Enter the preferred number of days in **Purge data older than specified days, if above threshold** is met field.





### **RMM Settings**

This setting lets you configure default RMM setting for connecting to client via RMM service:

### **Activate View Only**

By default, after taking a remote connection, you can only view the endpoint screen and are unable to perform any activity.

### **De-Activate View Only**

To perform activity on an endpoint after taking remote connection, click **De-Activate View Only**.

#### **Screen Quality Settings**

This option lets you configure the screen as per your requirements. It consists following suboptions:

• Screen Quality can be set to Medium or High.

| Screen Quailty | Screen Ratio |
|----------------|--------------|
| Medium 🔻       | 80% •        |
| Medium         |              |
| High           |              |

• Screen Ratio can be set to anywhere from 20% to 100%.

| Screen Quailty | Screen Ratio  |
|----------------|---|
| Medium         | 80% ▼<br>100%<br>90%<br>80%<br>70%<br>60%<br>50%<br>40%<br>30%<br>20% |

| NOTE | To build a safe RMM connection between a Client to Server, Client to Update Agent, |
|------|--|
| NOTE | and Update Agent to Server, ensure that ports 2219, 2220 and 8098 are open.        |

After making the necessary changes, click **Save.** The web console Settings will be updated.

## **Update Settings**

The Update Settings submodule keeps your virus definitions up-to-date and protects your computer from emerging species of viruses and other malicious programs. This submodule lets you configure update settings, update notifications and schedule updates according to your need.





You can configure eScan to download updates automatically either from eScan update servers or from the local network by using FTP or HTTP. You can configure following settings.

### General Config

The **General Config** tab lets you configure update settings. The settings let you select the mode of update and configure proxy settings.

| Update Settings                                | <b>?</b>   | Help |
|--|--|------|
| General Config Update Notification S           | Scheduling   |      |
| Select Mode                                    | HTTP   |      |
| Proxy Settings     Download via Proxy     HTTP |  |      |
| HTTP Proxy Server IP :                         | Port: Password :   |      |
| FTP Proxy Server IP:                           | Logon Type<br>User@siteaddress<br>OPEN siteaddress<br>PASV Mode<br>Socks 4 v |      |
|  | Indata   |      |

### Select Mode

Select the mode for downloading updates. Following options are available:

- FTP
- HTTP

### **Proxy Settings**

Proxy Settings lets you configure proxy for downloading updates.

To enable Proxy Settings, select **Download via Proxy** checkbox. You will be able to configure proxy settings depending on the mode of selection.

If you are using HTTP proxy servers, enter the HTTP proxy server IP address, port number and HTTP proxy server's authentication credentials.

If you are using FTP proxy servers, along with HTTP settings mentioned above you will have to enter FTP proxy server IP address, Port number, FTP proxy server's authentication credentials and Logon enter.

After filling the necessary data, click **Save > Update**. The General Config tab will be saved and updated.





### **Update Notification**

The **Update Notification** tab lets you configure email address and SMTP settings for email notifications about database update.

| Update Settings                       |                     |            | <br>       | <br><u>?</u> Help |
|---------------------------------------|---------------------|------------|------------|-------------------|
| General Config                        | Update Notification | Scheduling |            |                   |
| Update Notific                        | ation               |            | <br>       | <br>1             |
| Sender:<br>Recipient:<br>SMTP Server: |                     |            | SMTP Port: |                   |
| Use SMTF<br>User name:<br>Password :  | Authentication      |            |            |                   |
| Test                                  |                     |            |            |                   |
|                                       |                     |            |            |                   |
| Save                                  | Cancel              | Update     |            |                   |

### **Update Notification**

To receive email notifications from eScan about virus signature database update, select this option.

### Sender

Enter an email ID for sender.

#### Recipient

Enter the notification recipient's email ID.

#### **SMTP Server and Port**

Enter the SMTP server's IP address and Port number in the respective fields.

#### **Use SMTP Authentication**

If the SMTP server requires authentication, select this checkbox and enter the login credentials in the **Username** and **Password** fields.

After filling the necessary data, click **Save > Update**. The Update Notification will be saved and updated.





### Scheduling

The Scheduling tab lets you schedule updates with Automatic or Schedule Download mode.

| date Settings<br>General Config Update                         | Notification Sche | duling  |         |     |   |
|--|-------------------|---------|---------|-----|---|
| <ul> <li>Automatic Download</li> <li>Query Interval</li> </ul> | 120 V minute      | 25      |         |     |   |
| Schedule Download  |                   |         |         |     |   |
| Daily  |                   |         |         |     |   |
| Weekly   | Mon               | Tue     | Wed     | Thu |   |
|  | 🔲 Fri             | Sat Sat | Sun Sun |     |   |
| Monthly  | 1 v of the        | e month |         |     |   |
| le At  | 12:00 pm          | © •     |         |     | _ |
|  |                   |         |         |     |   |
|  |                   |         |         |     |   |
|  |                   |         |         |     |   |
|  |                   |         |         |     |   |
|  |                   |         |         |     |   |
|  |                   |         |         |     |   |

### Automatic Download

The eScan Scheduler sends a query to the update server at set intervals and downloads the latest updates if available. To set an interval, click the **Query Interval** drop-down and select a preferred duration.

### Schedule Download

The eScan Scheduler lets you set a schedule the download for daily, weekly or monthly basis at a specified time. The scheduled query will be sent to the update server as per your preferences.

After filling the necessary data, click **Save** > **Update**. The Scheduling tab will be saved and updated.

## Auto-Grouping

The Auto grouping submodule consists following subsections:

- Auto Add Client setting
- Client(s) list excluded from Auto adding under Managed Group(s)
- Group and Client selection criteria for Auto adding under Managed Group(s)





| uto Grouping  |           |  |  |          | 💲 Refres      | h 🝸 He |
|---|-----------|--|--|----------|---------------|--------|
| Auto Add Client setting   |           |  |  |          |               |        |
| Auto adding client(s) under   | Manage    | d Group(s)   |  |          |               |        |
| lient(s) list excluded from   | Auto ad   | ding under   | Managed Group(s)   |          |               |        |
|   |           |  | ······································   |          |               |        |
| and the later of the second strength of the   |           | Add  |  |          |               |        |
| Contraction of the second second  |           | Remove   |  |          |               |        |
|   |           |  |  |          |               |        |
|   |           |  |  |          |               |        |
|   |           |  |  |          |               |        |
|   |           |  |  |          |               |        |
|   |           |  |  |          |               |        |
|   | -         |  |  |          |               |        |
| g.: Host Name   |           |  |  |          |               |        |
|   |           |  |  |          |               |        |
| Host Name with wildcard   |           |  |  |          |               |        |
| Host Name with wildcard<br>IP Address<br>IP Address Range   |           |  |  |          |               |        |
| Host Name with wildcard<br>IP Address<br>IP Address Range   |           |  |  |          |               |        |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr   | riteria f | or Auto add  | ling under Managed Group(s)  |          |               |        |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr   | riteria f | or Auto add  | ling under Managed Group(s)  |          |               |        |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr   | riteria f | <b>or Auto add</b><br>Add                            | ling under Managed Group(s)<br>Client Criteria   |          | Add           | Run N  |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr   | riteria f | or Auto add<br>Add<br>Remove                         | ling under Managed Group(s)<br>Client Criteria   | A        | Add           | Run No |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr   | riteria f | or Auto add<br>Add<br>Remove<br>Browse               | ling under Managed Group(s)<br>Client Criteria   |          | Add           | Run No |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr   | riteria f | or Auto add<br>Add<br>Remove<br>Browse               | ling under Managed Group(s)<br>Client Criteria   |          | Add<br>Remove | Run No |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr   | riteria f | Add<br>Add<br>Remove<br>Browse                       | Client Criteria  |          | Add<br>Remove | Run No |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr<br>roup Name                                  | riteria f | Add<br>Add<br>Remove<br>Browse                       | Client Criteria  |          | Add<br>Remove | Run No |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr<br>roup Name                                  | riteria f | or Auto add<br>Add<br>Remove<br>Browse               | Client Criteria  | <u></u>  | Add<br>Remove | Run No |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr<br>roup Name                                  | riteria f | or Auto add<br>Add<br>Remove<br>Browse               | Client Criteria  | •        | Add<br>Remove | Run No |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr<br>roup Name                                  | riteria f | or Auto add<br>Add<br>Remove<br>Browse<br>Up<br>Down | Client Criteria  | *        | Add<br>Remove | Run No |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection of<br>roup Name                                  | riteria f | or Auto add<br>Add<br>Remove<br>Browse<br>Up<br>Down | Client Criteria  |          | Add<br>Remove | Run No |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection of<br>roup Name                                  | riteria f | or Auto add<br>Add<br>Remove<br>Browse<br>Up<br>Down | Client Criteria  |          | Add<br>Remove | Run No |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection of<br>roup Name                                  | riteria f | Add<br>Add<br>Remove<br>Browse<br>Up<br>Down         | Client Criteria<br>Client Criteria<br>e.g.: Host Name<br>Host Name with wildcard<br>IP Address<br>IP Address Range | <b>A</b> | Add<br>Remove | Run Ne |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr<br>roup Name                                  | riteria f | or Auto add<br>Add<br>Remove<br>Browse               | Client Criteria  |          | Add<br>Remove | Run No |
| Host Name with wildcard<br>IP Address<br>IP Address Range<br>roup and Client selection cr<br>roup Name<br>g.: group1<br>group1\subgroup | riteria f | Add<br>Remove<br>Browse                              | Client Criteria  | ▲<br>▼   | Add<br>Remove | Run No |

### Auto Add Client setting

Selecting the checkbox **Auto adding client(s) under Managed Group(s)** enables automatic adding computers under Managed group(s) after manual installation of eScan client.

### Client(s) list excluded from Auto adding under Managed Group(s)

Adding a client in this list ensures that it does not auto add itself again after you remove it from the Managed computer(s).

### Group and Client selection criteria for Auto adding under Managed Group(s)

This section lets you define/create groups with client criteria for auto adding under managed group(s). You can add a list of clients under a particular group name here and then add it under the exclusion list if required.





# Excluding clients from auto adding under Managed Group(s)

To exclude clients from auto adding under managed group(s), follow the steps given below:

- 1. Enter either the host name, host name with wildcard, IP address or IP address range.
- 2. Click **Add**. The computer will be displayed in the list below.

### Removing clients from the excluded list

- 1. Select the computer you want to remove.
- 2. Click **Remove**. The computer will be removed from the list.

Group and Client selection criteria for Auto adding under Managed Group(s) This feature can be used to automate the process of adding computers/clients under a particular group. This process is manually done under unmanaged computers.





### Defining a group and client selection criteria for auto adding under managed computer(s)

To define group and client selection criteria for auto adding under managed groups(s), follow the steps given below:

| Group and Client selection criteria for Auto adding under Managed Group(s) |        |                  |   |        |         |
|--|--------|------------------|---|--------|---------|
| Group Name   |        | Client Criteria  |   |        |         |
|  | Add    |                  |   | Add    | Run Now |
|  | Remove |                  | * | Remove |         |
|  | Browse |                  |   |        |         |
|  |        |                  |   |        |         |
|  |        |                  |   |        |         |
|  |        |                  |   |        |         |
|  | Up     |                  |   |        |         |
|  | Down   |                  | - |        |         |
| e.g.: group1   |        | e.g.: Host Name  |   |        |         |
| group: (subgroup   |        | IP Address       |   |        |         |
|  |        | IP Address Range |   |        |         |

1. Under the Group Name, enter the group's name and click **Add.** OR

Click **Browse** and select the group from the existing list.

**NOTE** To browse through the list of groups, click **Up** or **Down**.

- 2. Select the group for which you want to define the criteria.
- 3. Under the Client Criteria, enter either Hostname, Hostname with wildcard, IP address or IP address range and click **Add**. The clients displayed in the list will be added under the selected group.
- 4. Click **Save**. The client will be saved under that group.
- 5. To apply the settings for the newly added client, click **Run Now**.





## Two-Factor Authentication (2FA)

The system login password is Single-Factor Authentication which is considered unsecure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your eScan web console login.

The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering eScan credentials. So, even if somebody knows your eScan credentials, the 2FA feature secures data against unauthorized logins. Only administrator can enable/disable the 2FA feature. It can also be enabled for added users as well.

To use 2FA login feature, you need to install the Authenticator app for Android devices from <u>Play Store</u> or for iOS devices from <u>App Store</u> on your smart device. The Authenticator app needs camera access for scanning a QR code, so ensure you get an appropriate approval to use device camera in your organization. If a COD or BYOD policy restricts you from using device camera in your organization, enter the Account Key in the Authenticator app.



| NOTE | Ensure that the smart device's date and time matches with the system's date |
|------|---|
| NOTE | and time or else TOTPs generated by app won't get validated.                |

| IMDODTANT | We recommend that you save/store the <b>Account Key</b> in offline storage or |
|-----------|---|
| IMPORTANT | a paperback copy, in case you lose the account access.                        |





### Enabling 2FA login

To enable 2FA login,

- 1. Go to **Settings** > **Two-Factor Authentication**.
- 2. Open the Authenticator app. After basic configuration following screen appears on smart device.



3. Select a preferred option. If you tapped **Scan a barcode**, scan the onscreen QR code via your smart device. If you tapped **Enter a provided key**, enter the Account Key and then tap **ADD**.

After scanning the Account QR code or entering Account Key the eScan server account gets added to the Authenticator app. The app then starts displaying a Timebased One-Time Password (TOTP) that is valid for 30 seconds.



4. Click **Enable Two-Factor Authentication**. Verify TOTP window appears.

|                           | × |
|---------------------------|---|
| Two-Factor Authentication |   |
| Verify T-OTP              |   |
| 05:00:32 PM               |   |
| Enter T-OTP               |   |
| Verify T-OTP              |   |
|                           |   |




- 5. Enter the TOTP displayed on smart device and then click **Verify TOTP**. The 2FA login feature gets enabled.
- 6. To apply the login feature for users, click **Manage Other User Settings** tab. The tab displays list of added users and whether 2FA status is enabled or disabled.

| ×÷     | - 2FA Disabled |
|--------|----------------|
| 1 4 -1 |                |

⊻ - 2FA Enabled

| 2FA Settings Manage Other User's Se   | ettings    |  |
|---|------------|--|
| Jser's name   | 2FA Status |  |
| and the second se |            |  |
| daria   |            |  |
| 801 FB  | <b>X</b> 🖯 |  |
| day in the second s  |            |  |
| 811/18-   | <b>X</b> 0 |  |

 To enable 2FA login for an added user, click the button to check icon. The 2FA login for added users gets enabled. After enabling the 2FA login for users, whenever they log in to eScan web console Verify TOTP window appears.

## **Disabling 2FA login**

To disable 2FA login,

- 1. Go to **Settings** > **Two Factor Authentication**.
- 2. Click Disable Two-Factor Authentication.







### Verify TOTP window appears.

|                           | × |
|---------------------------|---|
| Two-Factor Authentication |   |
| Verify T-OTP              |   |
| 05:00:32 PM               |   |
| Enter T-OTP               |   |
| Verify T-OTP              |   |
|                           |   |
|                           | 1 |

3. Enter the TOTP and then click **Verify TOTP**. The 2FA feature gets disabled.

**NOTE** After disabling the 2FA feature and enabling it again, the 2FA login status will be reinstated for added users.





# Administration

The Administration module lets you create User Accounts and allocate them Admin rights for using eScan Management Console. In a large organization, installing eScan client on all computers may consume lot of time and efforts. With this option, you can allocate rights to the other employees and allow them to install eScan Client, implement Policies and Tasks. The Administration module consists following submodules.

## **User Accounts**

For a large organization, installing eScan Client and monitoring activities may become a difficult task. With User Accounts submodule, you can assign Administrator role to added users and reduce the workload. This submodule displays a list of users and their details like Domain, Role, Session Log and Status. You can create new user accounts and also add them from Active Directory.

| Use | r Accounts  |   |               |                   | 📚 Refrest     | n 🝸 Help      |
|-----|---|---|---------------|-------------------|---------------|---------------|
|     |   |   |               |                   |               |               |
|     | Create New Account                                  | Add from Active Directory                         | 1 - 1 of :    | 1 M page 1 of 1 M | Rows per page | : <u>10</u> ¥ |
|     | <u>User's name</u>                                  | Full Name   | <u>Domain</u> | Role              | Session Log   | <u>Status</u> |
|     | root  | Administrator account created during installation |               | Administrator     | <u>View</u>   | <b>V O</b>    |
|     | Create New Account Add from Active Directory Delete |   |               |                   |               |               |

## Creating a User Account

To create a User Account, follow the steps given below:

1. In the User Accounts screen, click **Create New Account**. Create User form appears.

| Create User                        |                                   |  |  |  |  |  |
|------------------------------------|-----------------------------------|--|--|--|--|--|
| <u>User Accounts</u> > Create User |                                   |  |  |  |  |  |
| Account Type and Information       |                                   |  |  |  |  |  |
| User's name*:                      |                                   |  |  |  |  |  |
| Full Name*:                        |                                   |  |  |  |  |  |
| Password*:                         |                                   |  |  |  |  |  |
| Confirm Password*:                 |                                   |  |  |  |  |  |
| Email Address:*                    |                                   |  |  |  |  |  |
|                                    | For Example: user@yourcompany.com |  |  |  |  |  |
| Account Role                       |                                   |  |  |  |  |  |
| Role*: Administrator               | Υ                                 |  |  |  |  |  |
| Save Cancel                        |                                   |  |  |  |  |  |

2. After filling all the details, click **Save**. The user will be added to the User Accounts list.





## Adding a User from Active Directory

1. In the User Accounts screen, click **Add from Active Directory**. Add Active Directory Users form appears.

| Add Active Directory Users                        |   |  |  |  |
|---|---|--|--|--|
| <u>User Accounts</u> > Add Active Directory Users |   |  |  |  |
| Search Criteria                                   |   |  |  |  |
| User's name*:                                     |   |  |  |  |
|   | For Example: user or user*                    |  |  |  |
| Domain*:  |   |  |  |  |
| AD IP Address*:                                   |   |  |  |  |
| AD Admin User name*:                              |   |  |  |  |
|   | For Active Directory account: domain\username |  |  |  |
| AD Admin Password*:                               |   |  |  |  |
| Use SSL Auth.:                                    |   |  |  |  |
| AdsPort*:   | 389   |  |  |  |
| Search  |   |  |  |  |
| Search Results                                    |   |  |  |  |
| Users   | Selected Users                                |  |  |  |
|   |   |  |  |  |
| >   |   |  |  |  |
| <   |   |  |  |  |
|   |   |  |  |  |
| · · · · · · · · · · · · · · · · · · ·             | <b>.</b>                                      |  |  |  |
| Account Role                                      |   |  |  |  |
| Role*: Administrator                              | T   |  |  |  |
| Save Cancel                                       |   |  |  |  |

- 2. After filling Search Criteria section details, click **Search.** A list of users will be displayed in the **Users** section.
- 3. Select a user and then click button to add the user to Selected Users section. Vice versa the added user can be moved from Selected Users to Users by clicking .
- 4. Click **Save**. The user will be added to the User Accounts list.





## **Deleting a User Account**

To delete a user account, follow the steps given below:

1. In the User Accounts screen, select the user you want to delete.

| User   | User Accounts   |   |  |  |  |  |
|--|---|---|--|--|--|--|
|  |   |   |  |  |  |  |
| Create New Account Add from Active Directory |   |   |  |  |  |  |
|  | <u>User's name</u>                                      | Full Name   |  |  |  |  |
|  | root  | Administrator account created during installation |  |  |  |  |
|  | test user   | Jon Doe   |  |  |  |  |
|  | Create New Account Add from Active Directory The Delete |   |  |  |  |  |

2. Click **Delete**. A confirmation prompt appears.

| ×  |
|--|
| User Accounts  |
| Do you want to delete the selected user account(s) ? |
| Ok Cancel  |

3. Click **OK**. The User Account will be deleted.





## User Roles

The User Roles submodule lets you create a role and assign it to the **User Accounts** with variable permissions and rights as defined in the role being assigned to them. It can be an Administrator role with set of permissions and rights Group Admin Role or a Read only Role.

You can re-define the Properties of the created role for configuring access to various section of eScan Management Console and the networked Computers. It also lets you delete any existing role after the task is completed by them. It allows the administrator to give permission to sub administrators to access defined modules of eScan and perform installation/uninstallation of eScan Client on network computers or define Policies and tasks for the computers allocated to them.

## Adding a User Role

To add a user role, follow the steps given below:

1. In the User Roles screen, click **New Role**. New Role form appears.

| New Role               |  |
|------------------------|--|
| Liner Deles - New Dele |  |
| USER KOIES > New Kole  |  |
| Role Details           |  |
| New Role Name :*       |  |
| Description :          |  |
| Select Group :         |  |
|                        |  |
| Ok                     |  |

- 2. Enter name and description for the role.
- 3. Click **Managed Computers** and select the specific group to assign the role. The added role will be able to manage and monitor only the selected group's activities.
- 4. Click **OK.** Permissions section appears displaying Main Tree Menu and Client Tree Menu tabs. The Main Tree Menu consists of Navigation Panel Access permissions while the Client Tree Menu consists of selected groups on which permissions the user is allowed to take further.





| issions                         |      |           |  |  |
|---------------------------------|------|-----------|--|--|
| Main Tree Menu Client Tree Menu |      |           |  |  |
| Menu                            | View | Configure |  |  |
| DashBoard                       | Ø    |           |  |  |
| Managed Computers               | ×.   | Ø         |  |  |
| Unmanaged Computers             |      |           |  |  |
| Network Computers               |      |           |  |  |
| IP Range                        |      |           |  |  |
| Active Directory                |      |           |  |  |
| Report Templates                |      |           |  |  |
| Report Scheduler                |      |           |  |  |
| Events & Computers              |      |           |  |  |
| System Action List              |      |           |  |  |
| Tasks For Specific Computers    |      |           |  |  |
| Asset Management                |      |           |  |  |
| User Activity                   |      |           |  |  |
| Print Activity                  |      |           |  |  |
| Session Activity Report         |      |           |  |  |
| File Activity Report            |      |           |  |  |

- 5. Select the checkboxes that will allow the role to view/configure the module.
- 6. After selecting the necessary checkboxes, click **Save**. The role will be added to the User Roles list.

### **Role Properties**

To view the properties of a role, follow the steps given below:

1. In the User Roles screen, select a role. This enables **Properties** and **Delete** buttons.

| U | User Roles        |               |                        |  |  |
|---|-------------------|---------------|------------------------|--|--|
|   |                   |               |                        |  |  |
|   | Properties Delete |               |                        |  |  |
|   |                   | Role Name     | Description            |  |  |
|   |                   | Administrator |                        |  |  |
| ( | •                 | Monitor       | For viewing activities |  |  |

2. Click Properties.





Properties screen appears. It lets you modify role description, permissions for accessing and configuring modules and assign the role to other groups by clicking **Select Group Tree**.

| roperties                            |       | 👔 Help  |
|--------------------------------------|-------|---|
|                                      |       |   |
| <u>ser noies</u> - Aroperoes         |       |   |
| Role Details                         |       |   |
| New Role Name :* Monitor             |       |   |
| Description : For viewing activities |       |   |
| Select Group :                       |       |   |
| Select Group Tree                    |       |   |
| Permissions                          |       |   |
| Main Tree Menu Client Tree Menu      |       |   |
|                                      | Mar . | Confirmer   |
| Menu                                 | View  | Configure   |
| DashBoard                            |       |   |
| Managed Computers                    | Ø     |   |
| Unmanaged Computers                  |       |   |
| Network Computers                    |       | <ul> <li>Image: A set of the /li></ul> |
| IP Range                             |       |   |
| Active Directory                     |       |   |
| Report Templates                     |       |   |
| Report Scheduler                     |       |   |
| Events & Computers                   |       |   |
| System Action List                   |       |   |
| Tasks For Specific Computers         |       |   |
| Asset Management                     | ۲     |   |
| User Activity                        |       |   |
| Print Activity                       | ۲     |   |
| Session Activity Report              |       |   |
| File Activity Report                 |       |   |
| Notifications                        |       | Image: A start and a start          |
| Outbreak Alert                       |       | ✓   |
| Event Alert                          |       |   |
| Unlicense Move Alert                 | ۲     |   |
| New Computer Alert                   |       |   |
| SMTP Settings                        |       |   |
| Settings                             | ✓     | ¥   |
| EMC Settings                         |       |   |
| Web Console Settings                 |       |   |
| Update Settings                      | ۲     |   |
| Auto Grouping                        |       |   |
| Administration                       | Ø     | Ø   |
| User Accounts                        |       |   |
| User Roles                           |       |   |
| Export & Import                      |       |   |
| Customize Setup                      | ✓     | 2   |
| License                              |       |   |
| Policy Templates                     |       |   |
| Policy Criteria Templates            |       | <   |
| Sure Count                           |       |   |
| Save Cancel                          |       |   |

3. To modify client configuration permissions, Click **Client Tree Menu**.





### **Client Tree Menu**

Define the Actions that the created role can configure for the allocated group. The menu has Action List, Client Action List, Select Policy Template, Policy Criteria, and Group Tasks.

| oles >Properties         |                                     |   |
|--------------------------|-------------------------------------|---|
| <u>ores</u> > Properties |                                     |   |
| Details                  |                                     |   |
| New Role Name :*         | a                                   |   |
| Description :            | Ь                                   |   |
| Select Group :           |                                     |   |
| Select Group Tree        |                                     |   |
| issions                  |                                     |   |
| Main Tree Menu Clie      | nt Tree Menu                        |   |
| Managed Computers        | [ Managed Computers/Roaming Users ] | Configure   |
|                          | Deploy / Upgrade Client             |   |
|                          | Uninstall eScan Client              |   |
|                          | Remove Group                        |   |
|                          | Properties                          |   |
|                          | Synchronize with Active Directory   |   |
|                          | Outbreak Prevention                 |   |
|                          | Create Client Setup                 |   |
|                          | Client Action List                  | Ø   |
|                          | Set Host Configuration              |   |
|                          | Deploy / Upgrade Client             |   |
|                          | Uninstall eScan Client              |   |
|                          | Move to Group                       |   |
|                          | Properties                          | Image: A start of the start          |
|                          | Remove from Group                   | st.   |
|                          | Refresh Client                      | <ul> <li>Image: A start of the start of</li></ul> |
|                          | Export                              | st.   |
|                          | Show Installed Softwares            |   |
|                          | Force Download                      | <b>A</b>  |
|                          | Send Message                        |   |
|                          | Outbreak Prevention                 | <b>A</b>  |
|                          | Delete All Quarantine Files         | Image: A start of the start          |
|                          | Create OTP                          | <ul> <li>Image: A set of the /li></ul> |
|                          | Select Policy Template              |   |
|                          | Policy Criteria                     | <b>v</b>  |
|                          | Group Tasks                         |   |

4. To let the role configure these actions, under the **Configure** column select the checkboxes of corresponding actions.

#### 5. Click **Save**.

The Role Properties will be updated accordingly.





## Deleting a User Role

To delete a user role, follow the steps given below:

1. In the User Roles screen, select the user role you want to delete.

| 1 | User | Roles               |                        |
|---|------|---------------------|------------------------|
|   |      | New Role Properties |                        |
|   |      | Role Name           | Description            |
|   |      | Administrator       |                        |
|   |      | Monitor             | For viewing activities |

#### 2. Click Delete.

A delete confirmation prompt appears.

| Delete Role                                 |
|---|
| Do you want to delete the selected Role(s)? |
| Ok Cancel                                   |

3. Click **OK**.

The User Role will be deleted.

## Export & Import

The Export & Import submodule lets you to take a backup of your eScan server settings, in case you want to replace the existing eScan server. You can export the Settings, Policies and the Database from existing server to a local drive and import it to the new server.





## **Export Settings**

This tab lets you export the eScan Server Settings, Policies and Database.

To export the eScan Server settings, follow the steps given below:

1. In the Export Import Settings screen, click **Export Settings** tab.

| Export Settings                               | Import Settings Scheduling                           |
|---|--|
| WMC Settings a Database Export                | nd Policies  |
| View Exported Files<br>Export files path: C   | \PROGRA~2\COMMON~1\microworld\apache2\EMCWebAdmin\   |
| 1. Select required se<br>2. Click on "Export" | ttings<br>o export eScan Management Console settings |

2. To backup Settings and Policies and Database, select both the checkboxes. The backup file will be exported to the path shown in Export File Path field. To change the file path, click **Change Path**. Enter the file path and click **Add**.

### 3. Click **Export**.

The backup file will be exported to the destination path. A success message appears at the top displaying date, time and a download link for the exported file.



## **Import Settings**

This tab lets you import the eScan Server Settings, Policies and Database.

To import the eScan Server settings, follow the steps given below:

1. In the Export Import Settings screen, click **Import Settings** tab.

| port Import Settings Export Settings Scheduling   |  |
|---|--|
| File Name       Choose File       No file chosen            WMC Settings and Policies        Database             Database        Import             View Exported Files               1. Select file to import (EservConf_[YYYYMMDDhhmm][_SCHD].zip)           2. Select required settings             3. Click on Timport*           Support to thom to import the saved settings |  |
|   |  |

#### 2. Click Choose File.

The Import Settings tab lets you import only Settings and Policies or Database.





- 3. To import Settings and Policies and Database, select both the checkboxes.
- 4. Click **Import**. The backup file will be imported. A success message is displayed after complete import.

**NOTE** After successfully taking a backup, eScan asks you to restart the server.

### Scheduling

This tab lets you schedule auto-backing up of Settings, Policies and Database.

| Import Setting                         | JS                        | Scheduling           |     |         |       |   |
|--|---------------------------|----------------------|-----|---------|-------|---|
|  |                           |                      |     |         |       |   |
| Enable Export                          | t Scheduler               |                      |     |         |       |   |
| ✓ WMC Sett                             | WMC Settings and Policies |                      |     | Dat     | abase |   |
| Daily                                  |                           |                      |     |         |       |   |
| Weekly                                 | - M                       | on 🗌                 | Tue | Wed     | 🔲 Thu |   |
|  | E Fr                      | i 🗌                  | Sat | Sun Sun |       |   |
| Monthly                                | 1 .                       | ]                    |     |         |       |   |
|  | 12:00 pr                  | 07                   |     |         |       |   |
| ~ AL                                   |                           |                      |     |         |       |   |
| SMTP Server:                           |                           |                      |     |         |       | _ |
| Use SM                                 | ITP Authentication        |                      |     |         |       |   |
| User name:<br>Password:                |                           |                      |     |         |       |   |
| Test                                   |                           |                      |     |         |       |   |
| 🗹 Enable Op                            | otional Settings          |                      |     |         |       |   |
| Select how m                           | any backup files to sto   | e                    | 2 🔻 |         |       |   |
| Create the ba<br>equal to :<br>Default | ckup only if drive space  | e is greater than or | 500 | MB ¥    |       |   |
| Delibert                               |                           |                      |     |         |       |   |
|  |                           |                      |     |         |       |   |
| Save                                   | J.                        |                      |     |         |       |   |

To create a Schedule for export, follow the steps given below:

- 1. Select Enable Export Scheduler checkbox.
- 2. Select the checkboxes whether to back up both Settings and Policies and Database.
- 3. Schedule the backup for a **Daily**, **Weekly** (Select a day) or **Monthly** (Select a date) basis.
- 4. For the **At** field, click the drop-down and select a time for backing up data.





If you want to receive email notifications about the procedure, select Enable Notifications Settings checkbox and fill in the necessary details. If the SMTP server requires authentication, select the Use SMTP Authentication checkbox and enter the credentials. To check if the SMTP settings are correct, click **Test**. A test email will be sent to recipient email ID.

To configure additional settings for backup file, select the Enable Optional Settings, and make the necessary changes. To restore the changes made, click **Default**.

5. After performing all the necessary steps, click **Save**. The export schedule will be saved.

## **Customize Setup**

This submodule lets you create a customized setup for a Client or an Agent with fewer modules and deploy it to various locations. This can be very useful, if there are locations to which a server is unable to push the setup or locations that are unable to connect to the server directly. The custom setup can be downloaded as a file and sent to different locations.

| Cre | ate Customized Setup      | 1                 |           |                |              |             |            | 💲 Refresh       | 👔 Help |
|-----|---------------------------|-------------------|-----------|----------------|--------------|-------------|------------|-----------------|--------|
| С   | lient \ Agent for Windows | Properties        | Delete    |                |              |             |            |                 |        |
|     | Setup Name                | <u>Group Path</u> | Server IP | <u>OS Type</u> | Distribution | Description | Created On | <u>Download</u> | ^      |
|     |                           |                   |           |                |              |             |            |                 |        |





## Creating a customized setup for Windows

To create a customized setup for Windows, follow the steps given below:

1. In Create Customized Setup screen, click **Client/Agent for Windows**. Customize New Setup screen appears.

| Customize New Setup  | 👔 Helt                  |
|--|-------------------------|
| Customize Setup > Client \ Agent for Windows   |                         |
| Setup File Settings  |                         |
| Setup for*:  | Olient O Agent          |
| Description*:  |                         |
| Group:   | Browse                  |
| Server IP*:  |                         |
|  | Enable Advance Settings |
| Advance Settings for Customized Setup<br>B B File AntiVirus<br>C Settings for Customized Setup<br>Remove Mail AntiVirus<br>C Set Remove AntiSpam<br>C Set Password<br>C Set Password<br>C Enable Schedule Scan<br>C Client Installation Settings<br>Additional Settings<br>C Schedule Download |                         |
| Save Cancel  | (*) Mandatory Fields    |

- 2. Select whether the setup file is being created for **Client** or **Agent**.
- 3. Enter description for the setup file.
- 4. Click **Browse** and select a group for which this setup is being created.
- 5. Enter eScan Server IP address.
- If you want to provide advanced settings with the setup, select the Enable Advance Settings checkbox. Doing so enables the bottom field. Select the setting checkboxes you want to provide.
- 7. Click **Save**.

The customized setup will be created.

### **Editing Setup Properties**

The properties can be edited for only customized Windows setup. To edit the customized Windows setup's properties, follow the steps given below:

1. In the Create Customized Setup screen, select the Windows setup you want to edit.

| Cr | eat  | te Customized Setup               |            |                               |                |              |             |                  | 📚 Refresh | 👔 Help |
|----|------|-----------------------------------|------------|-------------------------------|----------------|--------------|-------------|------------------|-----------|--------|
|    | Clie | nt \ Agent for Windows Properties | 前 Delete   |                               |                |              |             |                  |           |        |
| (  | V    | Setup Name                        | Group Path | Server IP                     | <u>OS Type</u> | Distribution | Description | Created On       | Download  | ^      |
| [  | V    | 158144;-;0000009;-;408000;0011222 |            | 19911001111111000010101001000 | Windows        |              | sample      | 05/29/2020 16:56 | Download  | 1      |
|    |      |                                   |            |                               |                |              |             |                  |           |        |

2. Click **Properties**. Edit Customized Setup screen appears.





| Edit Customized Setup                   |                         | 👔 Help               |
|---|-------------------------|----------------------|
| Setup File Settings                     |                         |                      |
| Setup for*:                             | Client O Agent          |                      |
| Description*:                           | sample                  |                      |
| Group:                                  | Browse                  |                      |
| Server IP*:                             |                         |                      |
|   | Enable Advance Settings |                      |
| Advance Settings for Customized Setting |                         |                      |
| Save Cancel                             |                         | (*) Mandatory Fields |

3. Make the necessary changes and then click **Save**. The setup will be updated.

## Deleting a Setup

To delete a setup, follow the steps given below:

1. In the Create Customized Setup screen, select the setup you want to delete.

| Crea | te Customized Setup               |            |           |                |              |             | ٩                | Refresh  | 👔 Help   |
|------|-----------------------------------|------------|-----------|----------------|--------------|-------------|------------------|----------|----------|
| Clie | nt \ Agent for Windows Properties | 💼 Delete   |           |                |              |             |                  |          |          |
| V    | Setup Name                        | Group Path | Server IP | <u>OS Type</u> | Distribution | Description | Created On       | Download | •        |
| V    | 1981au - Renomen, Landon-Amira au |            | -3938     | Windows        |              | sample      | 05/29/2020 16:56 | Download | <u>i</u> |
|      |                                   |            |           |                |              |             |                  |          | _        |

2. Click **Delete**. The setup will be deleted.





## License

The License module lets you manage user licenses. You can add, activate, and view the total number of licenses available for deployment, previously deployed, and licenses remaining with their corresponding values. The module also lets you move the licensed computers to non-licensed computers and vice versa.

| _icense  |                          |                                 |                                    | 💲 Re         | fresh 👔 Helj     |
|--|--------------------------|---------------------------------|------------------------------------|--------------|------------------|
| Register Information   |                          |                                 |                                    |              |                  |
| <u>License Key(30 char</u> )                                     | Activation Code(60 char) | Registration Status             | Contract Period Ends or            | No. of Users | Add On License   |
| Annan i sa can i milio i majani<br>Manan i milio i milio i milio | <u>Activate Now</u>      | Activate before 29-<br>Jun-2020 | -                                  | 10           | RMM+ DLP+<br>2FA |
| o Add License Click Here   |                          |                                 |                                    |              |                  |
| o nau Elecino <u>ener nore</u>                                   |                          |                                 |                                    |              |                  |
|  |                          | License                         |                                    |              |                  |
|  |                          | Licens                          | e in Use <u>1</u><br>e Remaining 9 |              |                  |
|  |                          | Total L                         | icense Size 10                     |              |                  |
|  |                          | 30 day                          | r(s) remain                        |              |                  |
|  |                          |                                 |                                    |              |                  |

## Adding and Activating a License

The License module lets you add only two licenses at a time. To add more licenses, it is mandatory that you activate at least one license. The **To Add License** <u>Click Here</u> link becomes unavailable after adding two licenses, and to make it available you have to at least activate one license.

To add and activate a license, follow the steps given below:

1. In the License screen, click the **Click Here** link.

To Add License <u>Click Here</u>

Add License Key dialog box appears.

|                               | ×         |
|-------------------------------|-----------|
| Add 30 Character License Key. |           |
|                               |           |
|                               |           |
|                               | OK Cancel |
|                               |           |

- 2. Enter the license key.
- 3. Click **OK**. The license key will be added and displayed in the **Register Information** table.
- 4. To activate the added license, click **Activate Now**.
- 5. Click **Activate now** link displayed in Activation Code column to activate the license key on eScan server system.





Online Registration Information form appears.

| Online Registration Information   | Privacy Policy | Refresh  | 👔 Help     |
|---|----------------|----------|------------|
| License > Online Registration Information   |                |          |            |
|   |                |          |            |
| License Key :   |                |          |            |
| I have Activation Code  |                |          |            |
| Enter Activation Code   |                |          |            |
|   |                |          |            |
| Activate Now  |                |          |            |
| Personal Information  |                |          |            |
| Name: Company Name:   |                |          |            |
| Country: India T Email Id:  |                |          |            |
| State: Maharashtra Customer Mobile No. *:   |                |          |            |
| Natur Fater and data and the second state and the second formation of the second state of the |                |          |            |
| Note: Enter Valid email id in order to receive backup copy or your license details.           |                |          |            |
| Email Subscription  |                |          |            |
| • Yes No  |                |          |            |
|   |                |          |            |
| Dealer Mobile No. *:  |                |          |            |
|   |                |          |            |
| Activate Cancel   |                | (*)Manda | tory Field |

- 6. Select a desired option for activation.
- 7. Enter details in Personal Information section.
- 8. Select a desired option for Email Subscription.
- 9. Enter the Dealer's mobile number.
- 10. Click Activate. (Ensure that the Internet connection is Active.)

## Moving Licensed Computers to Non-Licensed Computers

To move licensed computers to non-licensed computers, follow the steps given below:

1. In the License statistics box, click Manage License.



Manage License window appears.

The **Filter License** drop-down lets you filter computers according to RMM, 2FA or All license categories.





| Manage License             |                      |            |                     | <u>?</u> Hel        | lp |
|----------------------------|----------------------|------------|---------------------|---------------------|----|
| Licensed Computers (1)     | Filter License All   | •          | M 💼                 | love to Non-License |    |
| Machine Name               |                      | Group      |                     | 1                   |    |
|                            |                      | Managed Co | mputers             | 0                   |    |
|                            |                      |            |                     |                     |    |
|                            |                      |            |                     |                     |    |
|                            |                      |            |                     |                     |    |
|                            |                      |            |                     |                     |    |
|                            |                      |            |                     | · ·                 |    |
| Non-Licensed Computers (1) | Filter License       | All        | •                   | 音 Move to License   |    |
| Machine Name               | Group                |            | Unlicense Date Time | Description         |    |
| 🗈 🗿 Kar seneri kur ken san | Managed Computers\Te | stGroup    | 30/05/2020 11:44:06 |                     |    |
|                            |                      |            |                     |                     |    |
|                            |                      |            |                     |                     |    |
|                            |                      |            |                     |                     |    |
|                            |                      |            |                     |                     |    |
|                            |                      |            |                     | Ŧ                   |    |

- 2. Under the Licensed Computers section, select the computer(s) that you want to move to Non-Licensed Computers section.
- 3. Click **Move to Non-License**. The selected computer(s) will be moved to Non-Licensed computers section.

You can view the changes in the license count in the **License** window.







# Moving Non-Licensed Computers to Licensed Computers

To move non-licensed computers to licensed computers, follow the steps given below:

1. In the License statistics box, click **Manage License**.



Manage License window appears.

The **Filter License** drop-down lets you filter computers according to RMM, 2FA or All license categories.

| Manage License             |                             | 👔 Help              |
|----------------------------|-----------------------------|---------------------|
| Licensed Computers (2)     | Filter License All          | Move to Non-License |
| Machine Name               | Group                       | 1                   |
|                            | Managed Computers           | 0                   |
| 🔲 🚳 Har Samann (1995)      | Managed Computers\TestGroup | 1                   |
|                            |                             |                     |
|                            |                             |                     |
|                            |                             |                     |
|                            |                             | *                   |
| Non-Licensed Computers (0) | Filter License All          | move to License     |
|                            | No Record Found             | ^<br>^              |
|                            |                             |                     |
|                            |                             |                     |
|                            |                             |                     |
|                            |                             |                     |
|                            |                             |                     |
|                            |                             | ~                   |
| Close                      |                             |                     |

2. Under the Non-Licensed Computers section, select the computer(s) that you want to move to Licensed Computers section.





3. Click **Move to License**. The selected computer(s) will be moved to Licensed Computers section.

You can view the changes in the license count in the **License** window.







# Graphical User Interface (GUI)

The GUI is pleasantly straightforward and is designed to suit the needs of both novice and expert users. This window is for the server-side of the eScan TSS for Business.

| escan tss for business                                    |   |                               | ? - ×  |
|---|---|-------------------------------|--|
| system is secured   |   |                               | Last computer scan - Not vet Scanned<br>Date of virus signatures - 02 Jun 2020 09:14 |
|   |   |                               |  |
| file anti-virus<br>Started                                | web protection<br>Started                                     | privacy control<br>Manual     | identity protection<br>Not Configured  |
| Dangerous Objects Detected 0<br>Total Files Scanned 20450 | Total Sites Scanned 0<br>Total Sites Blocked 0                |                               | Total Objects Blocked 0  |
| mail anti-virus<br>Stopped                                | firewall<br>Stopped   | data encryption               |  |
| Total Mails Scanned 0<br>Total Infected Objects 0         | Inbound Packets Blocked 0<br>Outbound Packets Blocked 0       | Total Number of Data Vault: 0 |  |
| anti-spam<br>Stopped                                      | endpoint security<br>Started                                  | two-factor authentication     |  |
| Totai Quarantined Mails 0<br>Totai Clear Mails 0          | Total Applications Allowed 11<br>Total Applications Blocked 0 |                               |  |
|   |   |                               |  |
| 🔎 Scan 🔄 Update   |   | eScan Remote Supp             | ort   Password   License Information   Tools   Reports                               |

While the GUI for client-side (endpoints) will be as follows:

| escan tss for business                                  | authrenitanaator  | ? – ×  |                                    |
|---|---|--|------------------------------------|
| system is secured                                       |   | Last computer scan - N<br>Date of virus signatures | lot yet Scanned<br>s - 02 Jun 2020 |
| and the second  |   |  |                                    |
| file anti-virus   | web protection  | pri∨acy cont                                       | trol                               |
| Started   | Started   | Mai  | nual                               |
| Dangerous Objects Detected 0<br>Total Files Scanned 360 | Total Sites Scanned 0<br>Total Sites Blocked 0                |  |                                    |
| mail anti-∨irus   | firewall  | data encrypti                                      | ion                                |
| Stopped   | Stopped   | Mai  | nual                               |
| Total Mails Scanned 0<br>Total Infected Objects 0       | Inbound Packets Blocked 0<br>Outbound Packets Blocked 0       | Total Number of Data ∀a                            | ault: O                            |
| anti-spam   | endpoint security   | identity protecti                                  | ion                                |
| Stopped   | Started   | Not Configu  | ured                               |
|   |   |  |                                    |
| Total Quarantined Mails 0<br>Total Clear Mails 0        | Total Applications Allowed 10<br>Total Applications Blocked 0 | Total Objects Bloc                                 | ked 0                              |
|   |   | 1  |                                    |
| 🔎 Scan 🤤 Update   | Rescue Mode   eScan remote su                                 | upport   Password   License Information            | Tools   Reports                    |





## Data Encryption

The Data Encryption module lets you protect sensitive and confidential data from unauthorized access and data leak. With this module, the user can create a Vault that stores data in encrypted format.

The Vault is encrypted using 256-bit Advanced Encryption Standard (AES) and HMAC-SHA 256-bit key. A password is required to access the vault. After you access the vault, the data stored will be automatically decrypted. Vice versa, after you close the vault, the data stored will be automatically encrypted.

## How to Create a Vault?

To create a vault, follow the steps given below:

- 1. Launch eScan.
- 2. Click data encryption.

| escan tss for business                                    |   |                               | ? - ×  |
|---|---|-------------------------------|--|
| system is secured   |   |                               | Last computer scan - Not yet Scanned<br>Date of virus signatures - 02 Jun 2020 09:14 |
|   |   |                               |  |
| file anti-virus<br>Started                                | web protection Started  | privacy control               | identity protection<br>Not Configured  |
| Dangerous Objects Detected 0<br>Total Files Scanned 20450 | Total Sites Scanned 0<br>Total Sites Blocked 0                |                               | Total Objects Blocked 0  |
| mail anti-virus<br>Stopped                                | firewall<br>Stopped   | data encryption               |  |
| Total Mails Scanned 0<br>Total Infected Objects 0         | Inbound Packets Blocked 0<br>Outbound Packets Blocked 0       | Total Number of Data Vault: 0 |  |
| anti-spam<br>Stopped                                      | endpoint security<br>Started                                  | two-factor authentication     |  |
| Total Quarantined Mails 0<br>Total Clear Mails 0          | Total Applications Allowed 11<br>Total Applications Blocked 0 |                               |  |
|   |   |                               |  |
| 🔎 Scan 🔄 Update   |   | eScan Remote Suppo            | ort   Password   License Information   Tools   Reports                               |

Data Vault window appears.





3. Click Create new Data Vault.



4. To add files or folders in Data Vault, click **Add folders to Data Vault** or **Add files to Data Vault**.







- 5. After adding required files and folder, click **Next**.
- 6. Configure the Data Vault:
  - Name of Data Vault: Enter a name for the vault.
  - Location of Data Vault: To select a custom location for Data Vault, click Browse. The default path for vault is c:\eScanVault.
  - Select a size for Data Vault, **Variable size** or **Fixed size**. If selected **Fixed size** enter the size in below field or use the arrow buttons to specify size.
  - Optionally, select the checkbox Create desktop shortcut for Data Vault.

| Data Va  | ılt                           |                                    |                                |                     |
|--|-------------------------------|------------------------------------|--------------------------------|---------------------|
| 👌 Vault sett   | ing                           |                                    |                                |                     |
| Name of Data   | Yault:                        |                                    |                                |                     |
| and the second sec |                               |                                    |                                |                     |
| Location of D  | ata Yault:                    |                                    |                                | Browse              |
| • Variable si  | ze 👔 Storage will increase a  | and decrease the size automatica   | lly to fit all containing dire | ectories and files. |
| ⊖ Fixed size   | Storage will be created       | d with specified size and can't be | increased or decreased i       | n the future.       |
| Size of Data V   | ault: 100 🚔 MB                |                                    |                                |                     |
| 🚹 You will no  | be able to change the size of | the data vault later.              |                                |                     |
| 🗹 Create de  | ktop shortcut for Data Va     | ault                               |                                |                     |
|  |                               |                                    | Back                           | Next C              |

7. After filling all the details, click **Next**.





8. Read the **Password Hint** and then enter the password.

| Noto | A forgotten password cannot be recovered.                 |
|------|---|
| note | If you forgot the password, you cannot access your files. |
|      |   |

| 🙋 Data | Yault ? = x  |
|--------|--|
| Passi  | word setting   |
|        | dataencryt         Password to access the Data Vault:         ●         ●         Confirm Password         ●         ●         ●         ▲ A forgotten password cannot be recovered. If you forgot the password, you will not be able to access your files.         Password Hint:         ●         ●         ●         ●         ■         ■         ■         ■         ■         ■         ■         ●         ■ |
|        | Password must match! Back Next Close   |

- 9. Click **Next**.
- 10. Data will be copied to the Data Vault. If you wish to delete the original files and folders outside the data vault by clicking **Delete** or else click **Skip**.

| 'e | Data Vault |   | ?=x     |
|----|------------|---|---------|
|    |            | Delete original files and folder outside the Data Vault?<br>Files outside the Data Vault are accessible without password. |         |
|    |            | Back Skip D   | ) elete |





11. Click **Finish**. You will be forwarded to the following screen. Click **Done**.

| 'C | Data Vault  | ?=x |
|----|---|-----|
|    | Data Vault created successfully, your files are protected   To add or alter the files , unlock Data Vault by entering the password Lock the Data Vault after you have access or changed the files. Image: |     |
|    |   |     |

12. The Data Vault will be created and get displayed on the data encryption list. To encrypt your data, click **Lock**.

| 🕑 Data Vault                              | ?=x                                     |
|---|---|
| Open the Data Vault to access your files. |   |
| Data Vault is unlocked<br>C:\eScanVault   | Open in Windows Explorer Lock           |
|   |   |
|   |   |
|   |   |
| I already have a Data Vault               | Create ne <del>w</del> Data Vault Close |

13. Click **Close**. The created Data Vault will be encrypted.

After the data vault is locked, you will get **More** button displayed the right-hand side of the screen. Through this option, you will get the following setting to configure the data vault:







#### Rename

You can rename the existing data vault. After clickin on this option, you will get the following screen, where you can rename the vault.

| 🙋 Data Vault             | ? = X |
|--------------------------|-------|
| Rename Data Vault        |       |
| New name for Data Vault: |       |

After renaming, click **Save**.

#### Show location of Data Vault

This option will open the location where data vault is created.

#### Create desktop shortcut

This option will create shortcut for the created vault for accessing it easily.





### Delete

You can delete the existing data vault. Click on this option, you will get the following screen prompting for password.

| <u> </u> | alt   |
|----------|---|
|          | dataencryt<br>Password to access the Data Vault:<br>•••••••••<br>All files in the Data Vault will be deleted permanently.<br>Delete Data Vault Back |

After entrying the password, click **Delete Data Vault**. This will delete the selected data vault.

### **Change Password**

This option allows you to change the password set for the data vault. Click this option, you will forwarded to the following screen.

| Data Vault   |                      |
|--------------|----------------------|
|              |                      |
|              |                      |
| Change Passw | rord                 |
|              |                      |
|              |                      |
|              | New Paccuord         |
|              | New Password         |
|              | Confirm New Password |
|              | Confirm New Password |
|              | Deat                 |
|              | DdCk                 |
|              |                      |
|              |                      |
|              |                      |
|              |                      |
|              |                      |

Enter the **Old Password**, **New Password**, and **Confirm New Password**. Click **Save**. This will change the password of the data vault.

|      | If you selected Create desktop shortcut for Data Vault checkbox, it will create a |
|------|---|
| Note | chortsut of data yoult (  |
|      |   |





## Identity protection

Identity protection is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences, especially if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.

| esc              | can tss for business (14.0.1400.2281)                    |                               | ٠   | ? – ×                                  |
|------------------|--|-------------------------------|---|--|
|                  |  |                               | <u>Last computer scan</u><br>Date of virus signatures - | - Not yet Scanned<br>01 Jun 2020 10:03 |
| $   \mathbf{E} $ | file anti-virus mail anti-virus anti-spam web protection | firewall endpoint security    | privacy control identity p                              | rotection                              |
|                  | identity protection                                      |                               |   |  |
|                  |  |                               |   |  |
|                  | Configuration  |                               |   |  |
|                  | Identity Protection Status                               | No                            | ot Configured   |  |
|                  |  |                               |   |  |
|                  |  |                               |   |  |
|                  | <u>Start</u> Settings                                    |                               |   |  |
|                  | Reports  |                               |   |  |
|                  | Total Objects Blocked                                    |                               | 0 Objects   |  |
|                  |  |                               |   |  |
|                  | Mary Damast  |                               |   |  |
|                  | <u>view Report</u>                                       |                               |   |  |
|                  |  |                               |   |  |
|                  |  |                               |   |  |
| <b>,</b> 0       | Scan 🤄 Update Rescue                                     | e Mode   eScan Remote Support | Password   License Informatior                          | Tools   Reports                        |

This module provides you with options required to configure the module. You can configure the settings from the following sections.





## Configuration

This section displays the following information:

Identity protection Status: It displays whether Identity protection is configured or not.

**Start/Stop**: Click on this option to enable or disable identity protection module.

**Settings**: This option gives you Identity Protection popup window. Under this we have two sections.

| dentity Protection  |   | ?:  |
|---|---|---|
|   |   |   |
| This feature lets you protect<br>numbers, Phone Numbers, s<br>web pages, email messages | sensitive data or information such as your acco<br>ocial security numbers etc. from being sent over<br>and instant messaging without your knowledge | unt numbers, credit card<br>r to the internet through |
| Privacy Information to prote  | ct  | /*****  |
| Category  | What to Protect   | Add   |
|   |   | Modify  |
|   |   | Pemove  |
|   |   | Kentove   |
|   |   |   |
| List of trusted websites  |   |   |
| Address   |   | Add   |
|   |   | Modify  |
|   |   | Remove  |
|   |   |   |
|   |   |   |
|   |   |   |
|   |   | <u>O</u> K <u>C</u> ancel                             |

This section lets you protect sensitive data or information such as your account numbers, credit card numbers, phone numbers, and more from being sent over the internet through web pages, email messages, and instant messaging without your knowledge.

**Privacy Information to protect:** From the **Privacy Information to protect** section click on **Add**. This Button helps you add domain category, and a textbox to add data that needs to be protected.

| Add New Category                  | ? X       |
|-----------------------------------|-----------|
| Category<br>Enter data to protect |           |
|                                   | OK Cancel |

Once domains are added in the list you can modify them by clicking on the **Modify** button.





**List of trusted websites**: Under **List of trusted websites** click the **Add** button to add the name of trusted website address.

| Add New Trusted WebS | ite ? X   |
|----------------------|-----------|
|                      |           |
| Trusted Website      |           |
|                      | OK Cancel |

Once websites are added in the list you can modify them by clicking on the **Modify** button.

### Reports

It displays following count along with the report:

### **Total Objects Blocked**

This option gives you the total number of objects blocked by the eScan Identity Protection module.

#### View Report

To view reports, click **View Report**.

| Note | The Two-Factor Authentication feature can be configured only through server-side |
|------|--|
|      | for the endoints.  |





# Help

On upper-right corner of the screen, you can view the name of the user, help button, minimize button and close button. When you click help button, the following window appears:



Click this button, to access live chat, eScan online help, MicroWorld forum, eScan remote support, and feedback.

- **Live Chat**: You need to have internet connection, to access this feature. You can contact eScan 24 x 7 online technical support team through chat either by clicking the Live Chat button or by visiting the following link: http://www.escanav.com/english/livechat.asp
- **eScan Online Help**: You need to have internet connection, to access this feature. eScan online help is located on the eScan wiki. It provides you with comprehensive information about products and features of eScan.

You can visit eScan online help pages either by clicking the eScan Online Help button or by visiting the following link:

http://www.escanav.com/wiki

eScan for TSS for Business also provides you context-sensitive help, where you can find information on any specific feature while accessing the eScan for TSS for Business application you can press *F1* button, then the relevant page is displayed.

• **eScan Forum**: You need to have internet connection, to access this feature. You can click this button to join the eScan forum and read the discussion threads on eScan.





- **eScan Remote Support**: Click this link, if you want to access the eScan remote support for troubleshooting queries or product assistance through remote connection.
- **Feedback**: Click this option to visit the eScan web site, where you can provide your feedback on various eScan products and send it to the eScan's quality assurance team.

On upper-right corner of the screen, you can view the date, month, year, and time of when the last computer is scanned in the dd/Month/yyyy min: sec format.

It also displays the date, month, year, and time when the latest virus signatures are updated in the dd/Month/yyyy format.





## Quick Access Links

On lower-right corner of the screen, you can view the following quick access links:

Rescue Mode | eScan Remote Support | Password | License Information | Tools | Reports

### **Rescue Mode**

Rescue Mode is a eScan feature that enables you to scan and disinfect all existing partitions on your hard drive inside and outside your operating system. Some sophisticated malware, like rootkits, need to be removed before Windows starts. Once eScan detects a threat that cannot be removed, it prompts you to reboot the computer in Rescue Mode for clean-up and restoration.



It allows you to boot into a secure environment during system startup without using any optical media. It uses Windows as well as Linux -based environment that not only helps you to scan and clean the system but also allows you to fix registry changes made by viruses and rootkits.





## eScan Remote Support

eScan Remote support is the option to get Remote Help from our Support Center; the technical Support Executive will take control of your system for resolving the reported issue. It requires an active internet connection.

Steps for availing remote support:

1. Click on eScan remote support link at the bottom of the interface. **Remote Support Disclaimer** window will be opened.

| 🔞 Remote Support Disclaimer   | × |
|---|---|
|   |   |
| Please read the following important information before continuing.  |   |
| Please read the following Remote Support Disclaimer. You must accept the terms of the<br>disclaimer before using this tool.   | 9 |
| eScan Remote Access Support Disclaimer  | ^ |
| Before you choose the "Accept" button at the botton of this window, carefully read<br>the Warranty Disclaimer below. By choosing the "Accept" button you are [1]<br>representing that you are over the age of 18 and have the capacity and authority to<br>bind yourself and your employer, as applicable, to the terms of the disclaimer below;<br>and [2] consenting on behalf of yourself and/or as an authorized representative of<br>your employer, as applicable, to be bound by this disclaimer. If you do not agree to all<br>of the terms and conditions of the disclaimer, or do not represent the foregoing, you<br>will not and may not receive Remote Access Support from eScan.<br>You have requested the assistance of an eScan Technical Support Representative | v |
| Laccent the disclaimer  |   |
| O I do not accept the disclaimer  |   |
| Copyright (c) MicroWorld  |   |
| Ok Cancel   | l |

- 2. Read and accept the disclaimer and click **Ok**. eScan Remote Support tool will open.
- 3. It will generate a user ID and password. Send this user id and password to the technical support executive. The executive will take remote support of your system.





### Tools

The tools link provides you with the options for easy and quick access to various tools for eScan and each tool will have its own functions.

| esc          | an tss f              | or business (14.0.1400.2281)  |                   |  | ٠   | ? – ×                                  |
|--------------|-----------------------|---|-------------------|--|---|--|
|              |                       |   |                   |  | <u>Last computer scan</u><br>Date of virus signatures - | - Not yet Scanned<br>01 Jun 2020 10:03 |
| E            | file anti-virus       | mail anti-virus anti-spam web prote   | ection firewall   | endpoint security  | privacy control identity p                              | protection                             |
|              | <b></b>               | tools   |                   |  |   |  |
|              | ©<br>//3<br>/11<br>** | eScan USB Stick Creation<br>Restore Windows Default Settings<br>Windows Essential Updates<br>Registry Cleaner | ¥<br>&<br>%       | Download eScan<br>Upload Samples<br>USB Vaccination<br>Vulnerability Sca | Service pack<br>nner                                    |  |
|              |                       |   |                   |  |   |  |
| <b>,</b> 0 S | ican 🔄                | Update  | Rescue Mode   eSo | can Remote Support   | Password   License Information                          | n   Tools   Reports                    |

It gives you access to the various eScan TSS for Business tools and it performs the following actions.

### eScan USB Stick Creation

You will have to burn the image on to a USB device before using it to repair/clean infected or damaged systems.



You can connect your USB to the device and select the device from the drop-down menu.




|   | Х |
|---|---|
| eScan USB Stick Creation  |   |
|   |   |
| Recording data to USB flash drive   |   |
| The wizard will record data to a USB flash drive  | - |
| Select the USB flash drive:   |   |
|   |   |
| Warning : Please use only USB tlash drives or USB hard drives to record eScan Rescue<br>ISO image. Do not use mp3-players, smart phones or similar devices. |   |
| Note: Booting from a USB drive depends upon additional BIOS configuration, hence it may fail in some scenario.  |   |
|   |   |
| < <u>Back</u> <u>N</u> ext > <u>C</u> ancel   |   |

After selecting the device, click **Next>**. It will prompt you to format the USB drive.







Click **Yes**. The process of recording the data in the USB will be initialized and you will get the following screen:

|   | Х |
|---|---|
| eScan USB Stick Creation  |   |
|   | _ |
| Recording data to USB flash drive                                       |   |
| The wizard is recording to a USB flash drive. It can take a few minutes | - |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |
| < <u>B</u> ack <u>N</u> ext > <u>C</u> ancel                            |   |

Once the recording process is completed, you will get the following screen. Click **Next>**.

|   | х |
|---|---|
| eScan USB Stick Creation                                |   |
|   | 7 |
| Recording data to USB flash drive                       |   |
| Process completed successfully, Press next to continue. | - |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |
| < <u>B</u> ack <u>N</u> ext > <u>C</u> ancel            |   |





Completing the Rescue USB stick Creation Wizard appears. Click Finish. The Rescue

USB stick will be created successfully.



#### **Download eScan service pack**

You can download the latest eScan service pack directly from here. This will include all the latest updates.

### **Restore Windows Default Settings**

You can restore the Windows® operating system settings, such as desktop and background settings, to eliminate all the modifications made by a virus attack by using this button. eScan automatically scans your computer for viruses when you click this button and sets the system variables to their default values.







## **Upload Samples**

This functionality will allow you upload the suspicious files that will be checked by eScan's R&D team. You can click on this link, it will be redirect to our website, where you can upload the sample and post your queries.

| File Edit View History Bookmarks Tools    | Help                                     |  |  |                   |              | - C   |
|---|--|--|--|-------------------|--------------|-------|
| '@ Select a department - Powere × +       |  |  |  |                   |              |       |
| (i) 🔏   support.mwti.net/support/index.ph | np?/Tickets/Submit                       |  | C <sup>e</sup> Q Search                      | ☆自                | <b>↓</b> 俞 ( |       |
|   |  |  |  |                   |              |       |
| eSean                                     |  |  |  |                   |              |       |
| <u>co</u> gan                             |  |  |  |                   |              |       |
| 🛆 Hama 🖉 Submit a Tia                     | kat 🕴 aSana Wildi 💻 aSana                | 54.0-                                  |  |                   | English (11  | (S) V |
|   | ket y escali wiki ili escali             | raus                                   |  |                   | English (o   |       |
| Login                                     | Rease type your search que               | ery here                               |  |                   | SEARCH       |       |
| Your email address                        |  |  |  |                   | _            |       |
|   | Select a department                      |  |  |                   |              |       |
| Remember me                               |  |  |  |                   |              |       |
| Lost password Login                       | If you can't find a solution to your pro | blem in our knowledgebase, you can sul | omit a ticket by selecting the appropriate o | lepartment below. |              |       |
|   | Departments                              |  |  |                   |              | - 1   |
| Live Support                              | O Support                                |  |  |                   |              |       |
| - ONLINE                                  | <ul> <li>Samples</li> </ul>              |  |  |                   |              |       |
| Live Chat Software by Kayako              | Registration                             |  |  |                   |              |       |
|   | <ul> <li>Europe Support</li> </ul>       |  |  |                   |              |       |
|   | O False Positive                         |  |  |                   |              |       |
|   |  |  |  |                   |              |       |
|   | Next »                                   |  |  |                   |              |       |
|   |  |  |  |                   |              |       |
|   |  |  |  |                   |              |       |





## **Windows Essential Updates**

It will update your system with the latest windows patch updates. eScan maintains a list of critical Windows Update patches on every computer that are available for free, whenever the user clicks on **Download Latest Hotfix (Microsoft Windows OS)** option, it checks the computer for missing patches on the OS by matching the installed patches with the released patch list in the database. The missing critical Windows update patches are then downloaded and installed on the computer where eScan is running. The database list is categorized on the basis of the operating system.

| 😡 MicroWorld Download Man | ager ( )   |                |  |  |
|---------------------------|--|----------------|--|--|
| CECTOR CONTRACTOR         | KB2618451 on XPSP3: Present         -2018-05-28 13:11:06- http://www.microsoft.com/en-us/download/details.aspx?id=35845&displaylang=         Proxy request sent, awaiting response 404 Not Found         2018-05-28 13:11:06 ERROR 404: Not Found         2018-05-28 13:11:06 ERROR 404: Not Found         XB2900986 on XPSP3: Present         KB4012538 on XPSP3: Present         KB4012538 on XPSP3: Present         KB4012538 on XPSP3: Present         KB4012539 on XPSP3: Present         KB4012547 on XPSP3: Present         KB4022747 on XPSP3: Present         KB4022420 on XPSP3: Present         KB4022402 on XPSP3: Present         KB4025218 on XPSP3: Present         KB4025418 on XPSP3: Present         KB4025410 on XPSP3: Present         KB4025410 on XPSP3: Present         KB4025218 on XPSP3: Present         KB4055218 on XPSP3: |                |  |  |
|                           |  |                |  |  |
|                           | Select tools to download   | Action         |  |  |
|                           | MWAV ESPATCH ESUPDATE  | Start Download |  |  |
| <b>'eScan</b> ™           | Options<br>✓ Execute after download  | Stop Download  |  |  |
| Copyright MicroWorld      | Use IE Proxy   | Exit           |  |  |

#### **USB Vaccination**

The USB devices are used for various purposes, but while using them you may not be aware that the system to which you are connecting is virus infected. When connected to such machines the USB devices also tend to get infected. So, to prevent such cases, eScan 14 has introduced a feature wherein you can vaccinate USB device, whenever needed. Once vaccinated it stays protected even if you connect the flash drive to an infected system, it doesn't become a carrier to infection.

By default, the **Choose a USB Drive** drop-down list and **Vaccinate** button appears dimmed. It is available only when you connect any USB device to your system.





To vaccinate, select an appropriate USB drive, which you want to vaccinate from the **Choose a USB Drive** drop-down list, and click the **Vaccinate** button.

| USB Vaccination   |   | ×                       |
|---|---|-------------------------|
|   |   |                         |
| USB Vaccination preve<br>undo the vaccination I<br>Choose a USB Drive | ents viruses from infecting ye<br>later if needed.<br><insert key="" usb=""></insert> | our USB Drives. You can |
|   |   | Close                   |

#### **Registry Cleaner**

eScan will scan for issues in the selected registry entries, all issues found will be displayed in the Panel on the right. You can select / unselect the issues found by eScan and fix selected issues button to fix the issues. eScan will fix the selected issues instantly.

#### **Vulnerability Scanner**

This option will check the vulnerability of the software installed on your computer for any kind of weakness that can be used by the attacker to gain access to the information stored on your computer without your permission. Using the options present in Vulnerability Scanner module of eScan, you can easily update the listed software's with the more secured version of the same.

| Vulnerability Scanner                       |                   |                |   |                 | Z X              |
|---|-------------------|----------------|---|-----------------|------------------|
|   |                   |                |   |                 |                  |
|   |                   | 1              |   |                 |                  |
| Program Name                                | Installed version | Secure Version |   | Status          | Company Name     |
|   |                   |                |   |                 | 1                |
| Notepad++ : a free (GNU) source code editor | 6.8.7.0           | 7.8.3.0        | 0 | Click to update | Don HO don.h@    |
|   |                   |                |   |                 | 2                |
| Firefox                                     | 75.0.0.7398       | 72.0.2.0       | 0 | Up-to-date      | Mozilla Corporat |
| VLC media player                            | 3.0.8.0           | 3.0.8.0        | 0 | Up-to-date      | VideoLAN         |
|   |                   |                |   |                 |                  |
|   |                   |                |   |                 |                  |
|   |                   |                |   |                 |                  |
|   |                   |                |   |                 |                  |
|   |                   |                |   |                 |                  |
|   |                   |                |   |                 |                  |
|   |                   |                |   | Scan Again      | Close            |





# Contact Us

We offer 24/7 free online technical support to our customers through email and live chat. We also provide free telephonic support to customers during our business hours.

Before you contact technical support team, ensure that your system meets all the requirements and you have Administrator access to it. Also, ensure that a qualified person is available at the system in case it becomes necessary to replicate the error/situation.

Ensure that you have the following information when you contact technical support:

- Endpoint hardware specifications
- Product version in use and patch level
- Network topology and NIC information
- Gateway, IP address and router details
- List of hardware, software and network changes if any carried out
- Step by step description of error/situation
- Screenshots, error messages and log/debug files
- Step by step description of troubleshooting if any attempted

# Chat Support

The eScan Technical Support team is available round the clock to assist you with your queries. You can contact our support team via Live Chat by clicking <u>here</u>.

# Forum Support

You can even join the MicroWorld Forum to discuss eScan related problems with eScan experts by clicking <u>here</u>.

# **Email Support**

If you have any queries, suggestions and comments regarding our products or this User Guide, please write to us at <a href="mailto:support@escanav.com">support@escanav.com</a>