

## **Promisec Spectator™ Quick Install guide.**

|       |   |   |
|-------|---|---|
| 1     | Introduction.....                                   | 2 |
| 2     | Requirements .....                                  | 2 |
| 2.1   | System Requirements for Promisec Spectator .....    | 3 |
| 2.2   | Inspected host system requirements.....             | 3 |
| 3     | Install and license.....                            | 3 |
| 3.1   | Installation.....                                   | 3 |
| 3.2   | Obtaining and Entering a Serial Number .....        | 3 |
| 4     | Running Promisec Spectator for the First Time ..... | 4 |
| 4.1   | Selecting which hosts to inspect.....               | 4 |
| 4.1.1 | Selecting a Single Host .....                       | 4 |
| 4.1.2 | Selecting a Domain .....                            | 4 |
| 4.1.3 | Selecting Hosts from a Text File .....              | 5 |
| 4.1.4 | Selecting Hosts based on IP address Range.....      | 5 |
| 4.2   | Configuring the inspection .....                    | 5 |
| 4.2.1 | Inspection set up .....                             | 5 |
| 4.2.2 | Setting up the inspection performance.....          | 8 |
| 4.3   | Running the inspection.....                         | 8 |
| 4.4   | Inspection results.....                             | 9 |
| 4.4.1 | Real time view .....                                | 9 |
| 4.4.2 | HTML Executive Report .....                         | 9 |

## **1 Introduction**

Promisec Spectator is a Clientless Endpoint Security Management (CESM) solution that protects your network without the need to install any invasive client software on any enterprise PC or Server – no client applications, no thin clients, not even an ActiveX. Promisec Spectator is a comprehensive non-intrusive solution, addressing a wide variety of threats from a single console. Only minutes after installation, you can define a baseline security policy, inspect every PC in the network, generate detailed exception reports, remotely repair problems, and take a giant step forward to securing your enterprise network and data, from both inside and out. Promisec Spectator enables you to:

- Continuously monitor the enterprise PCs (applications, devices, processes, start-up commands, services, toolbars, network shares, suspicious files, and baseline security policy compliance) without overloading the network, the PCs or your staff;
- Detect all deviations from the security policy;
- Detect and remotely repair potential security problems;
- Ensure the availability of third-party security clients;
- Alert administrators of urgent issues and generate exception reports.

## **2 Requirements**

Promisec Spectator inspects remote hosts, reports the findings and remediates the problems. In order to perform all these actions the user running Promisec Spectator needs to have local administrative rights for the inspected hosts. Domain administrator rights while not required will allow more actions with active directory.

## 2.1 System Requirements for Promisec Spectator

- Windows 2000 / Windows XP Professional / Windows 2003 / Windows Vista
- Internet Explorer Version 5.01 or higher
- 512 MB of memory
- 1 GB of free disk space (for reports)
- 1024 x 768 video adapter card
- Microsoft .NET 2.0

## 2.2 Inspected host system requirements

These services are required in order to inspect remote hosts.

- Server service.
- Remote Procedure Call (RPC).
- Remote Registry
- File and Print Sharing
- Windows Management Instrumentation (WMI) service (only required to stop processes).

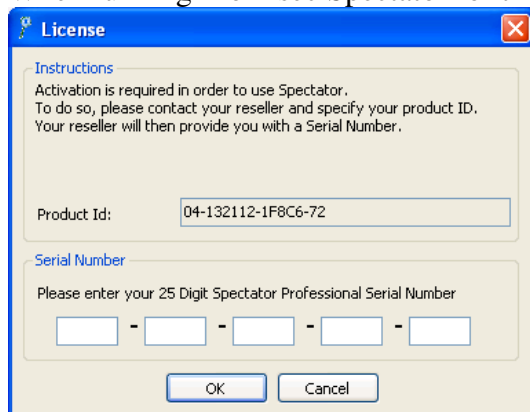
## 3 Install and license

### 3.1 Installation

Insert the Promisec Spectator disc into your CD/DVD drive and follow the on-screen instructions. If the Auto Play option is disabled for the drive, navigate to the drive in Windows Explorer or "My Computer" and double click on the "setup.exe" file. Promisec Spectator will install .NET Frameworks 2 if it does not exist on the inspecting machine. Once the installation is completed, double click on the Promisec Spectator icon to launch the application.

### 3.2 Obtaining and Entering a Serial Number

When running Promisec Spectator for the first time, you will be asked for a Serial Number.



During the installation process, a Product ID will be displayed. Contact your reseller and specify the product ID. Your reseller will provide you with a Serial Number. The Serial Number contains 25 digits and should be entered in the **License** after you click **OK**, Promisec Spectator will be activated and can be used. You can also enter the Serial Number by choosing **Enter Serial Number** from the **Help** menu.

## 4 Running Promisec Spectator for the First Time

### 4.1 Selecting which hosts to inspect

Before you can begin the inspection, you need to select which hosts to inspect.

#### 4.1.1 Selecting a Single Host

To select hosts individually:

1. In the **Single Host** tab, enter the host's name or its IP address.
2. Click **Add**.

The host you have selected is displayed under **Hosts to be Inspected**.

#### 4.1.2 Selecting a Domain

To select hosts by domain:

1. In the **Domain** tab, enter the domain name from which to select the hosts and click **Show OUs**.

A list of Organization Units (OUs) is displayed.

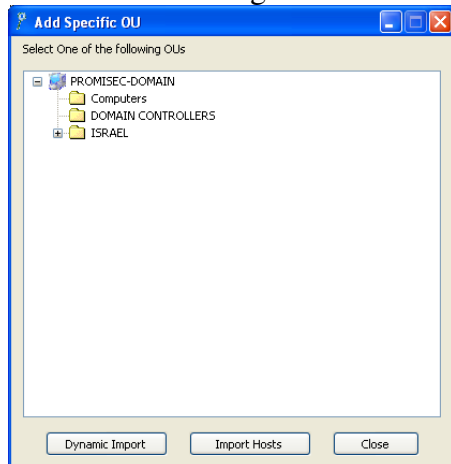


Figure 1- Selecting Domain

2. Select an OU to inspect and click on:
  - **Import Hosts** - will import the hosts currently in the OU to the list of hosts to be inspected, *or*
  - **Dynamic Import** - will import the hosts in the OU to the list of hosts to be inspected immediately before each inspection. This ensures that only hosts in the OU at the time of inspection are included in the inspection and not hosts that belong to the OU but are not currently connected.

The hosts in the specified OU are displayed in the selection box.

3. Select the hosts to be inspected in the **Adding Hosts for Inspection** box and click **Add**. The hosts you have selected are displayed under **Hosts to be Inspected** in the far left window.

#### 4.1.3 Selecting Hosts from a Text File

To select specific hosts listed in a text file, proceed as follows:

1. In the **File** tab, enter the name of a text file (or click **Browse** to find the file).

Each line in the file should specify one of the following:

- the name of one host only, *or*
- the IP address of one host only, *or*
- the entire class C segment (for example: 192.168.1.0/24)

The hosts listed in the file are displayed in the selection box.

2. Select the hosts to be inspected and click **Add**.

The hosts you have selected will be displayed under **Hosts to be Inspected** in the far left window.

#### 4.1.4 Selecting Hosts based on IP address Range

1. In the **IP Range** tab, enter a range of IP addresses and click **Show IP List**.

The hosts in the range of IP addresses are displayed in the selection box. Note that the list is simply a list of IP addresses in the specified range. There may or may not be actual hosts with these addresses in the network.

2. Select the hosts to be inspected and click **Add**.

The hosts you have selected are displayed under **Hosts to be inspected** in the far left window.

### 4.2 Configuring the inspection

The inspection is broken down into three major components Black list, White list (monitors) and hardware prevention. In this guide, we are going to focus on the tests that provide the quickest results with the least setup. If you want to read more about the other components please refer to Promisec Spectator user guide (located on the CD) or the built in help.

#### 4.2.1 Inspection set up

The black list checks for applications or objects that should not be installed, the exceptions are service packs and antivirus that needs to be installed. The radio buttons to the top right determine if you want to be notified if the application is installed or not.

The monitors work by creating a baseline of your organization and check inspected hosts against the baseline. Hardware prevention works by enforcing hardware prevention policy across the organization.

For best results, we suggest you enable the following:

1. Check if anyone is running messaging or P2P file sharing software. You should also enabled remote control to see if anyone has deployed rogue remote control applications in your organization.

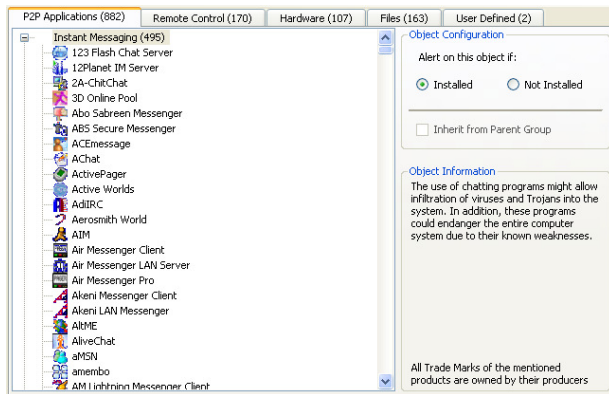


Figure 2 - Black list database

- Open required software under compliance group and check that Antivirus software is installed and running on all the endpoints. Unlike other tests in the black list, for Antivirus we want to be notified when it is not installed, so the "not installed" radio button is marked by default.

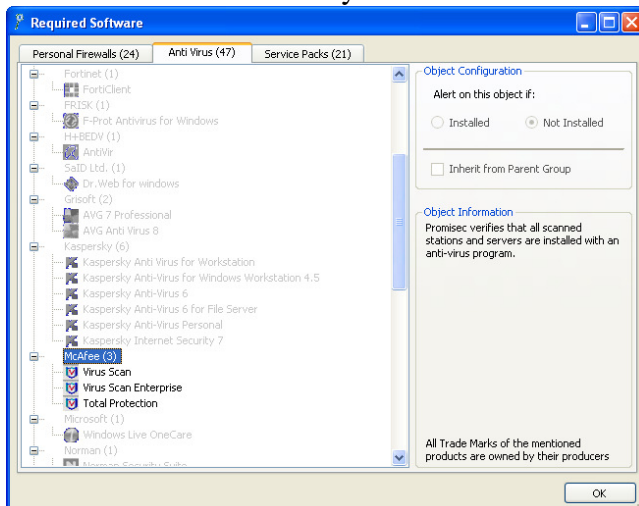


Figure 3 - Enabling anti-virus inspection

- In order to disable the tabs not needed for the current inspection, right click on the tab and select disable:

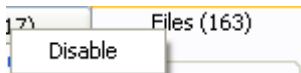


Figure 4 - Disabling tabs

#### 4. Check the update date for the Antivirus definitions

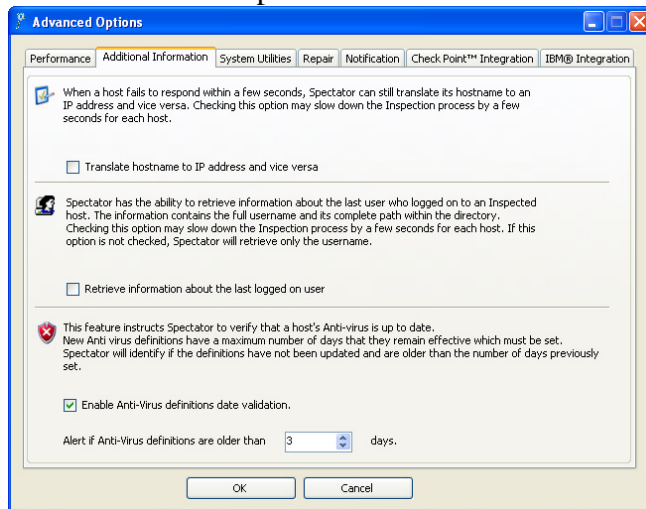


Figure 5 – Additional information advanced options

5. Under Files category, enable the video parent group. By default, this will only check for recently used files, you can changes this under advanced options to inspect the entire hard disk of each endpoint. Please note, however, inspecting the entire hard disk will take significantly longer to inspect than just the recent file history.

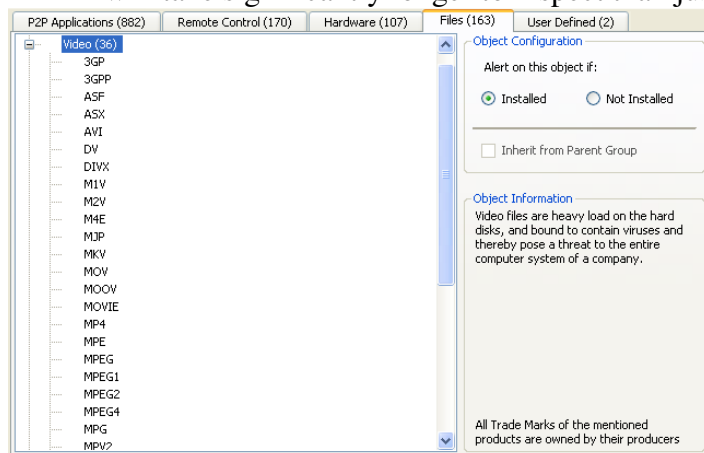


Figure 6 - Enabling video files inspection

### 4.2.2 Setting up the inspection performance

Under tools → advanced options → performance you can determine the inspection speed and overall performance.

1. Enable the ping option; this will check if the computers are operational and connected before beginning the inspection.
2. Next, configure the speed of inspection. If you are inspecting inside the LAN move the slider to “High Speed Level” otherwise set it somewhere in the middle.
3. Leave the inspection timeout on the default level, this will determine how much time to allocate for each host inspection.

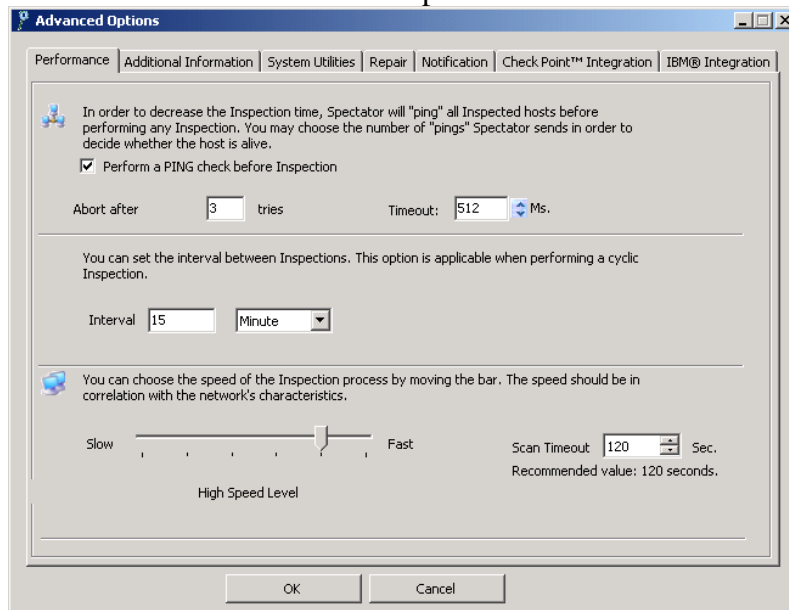
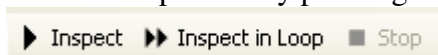


Figure 7 - Performance advanced options

### 4.3 Running the inspection

1. Start the inspection by pressing "Inspect"



2. After results will start to show, choose to filter out rows with no response, no findings and unknown reason. The rows with Access denied are important because they indicate places where the Administrator user does not have privileges and should be investigated.

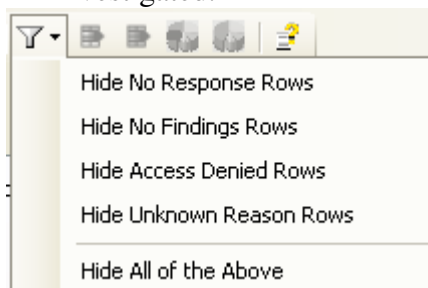


Figure 8 - Filtering results

3. After filtering the no response results generate a HTML report, see section 4.4.2.

#### 4.4 Inspection results

There are two ways to view the results of the inspection, either the built in report or in a HTML executive report.

##### 4.4.1 Real time view

Promisec Spectator displays the results of the inspection in real time in the report section of the user interface.

| Host Name     | IP Address   | Last Logged-On User    | Object                 | Status        | Details   |
|---------------|--------------|------------------------|------------------------|---------------|---|
| FOX-POR-TABLE | 192.168.1.16 |                        | Cannot Connect to Host | Access Denied |   |
| AMBR-NEW      | 192.168.1.36 |                        | Cannot Connect to Host | DNS Problem   | Real computer name: RAN-TESTING1                      |
| AVASTPRO      | 192.168.1.52 |                        | Cannot Connect to Host | DNS Problem   | Real computer name: DEV-WORKSTATION                   |
| BITDEF72      | 192.168.1.17 |                        | Cannot Connect to Host | DNS Problem   | Real computer name: ROI                               |
| BITDEFENDER72 | 192.168.1.19 |                        | Cannot Connect to Host | DNS Problem   | Real computer name: SARIT-YP2                         |
| FORROMI2      | 192.168.1.13 |                        | Cannot Connect to Host | DNS Problem   | Real computer name: ISRAEL                            |
| RAN-TESTING1  | 192.168.1.36 | PROMISEC-DOMAIN\tonerl | QQ                     | Installed     | Evidence for this item was found, but it is not li... |
| RAN-TESTING1  | 192.168.1.36 | PROMISEC-DOMAIN\tonerl | Skype                  | Installed     | Evidence for this item was found, but it is not li... |
| RAN-TESTING1  | 192.168.1.36 | PROMISEC-DOMAIN\tonerl | Windows Messenger      | Installed     | Evidence for this item was found. However, it ...     |
| RAN-TESTING1  | 192.168.1.36 | PROMISEC-DOMAIN\tonerl | Yahoo Messenger        | Installed     | Evidence for this item was found, but it is not li... |
| RAN-TESTING1  | 192.168.1.36 | PROMISEC-DOMAIN\tonerl | BitTorrent++           | Installed     |   |
| RAN-TESTING1  | 192.168.1.36 | PROMISEC-DOMAIN\tonerl | eMule                  | Installed     | "C:\Program Files\BearFlix\bearflix.exe" -noins...    |
| RAN-TESTING1  | 192.168.1.36 | PROMISEC-DOMAIN\tonerl | ReverseConnect         | Installed     | Evidence for this item was found, but it is not li... |
| RAN-TESTING1  | 192.168.1.36 | PROMISEC-DOMAIN\tonerl | GoToMyPC               | Installed     | Evidence for this item was found. However, it ...     |
| RAN-TESTING1  | 192.168.1.36 | PROMISEC-DOMAIN\tonerl | SNP                    | Installed     | Evidence for this item was found. However, it ...     |
| RAN-TESTING1  | 192.168.1.36 | PROMISEC-DOMAIN\tonerl | WebEx                  | Installed     | Evidence for this item was found. However, it ...     |

Figure 9 - Viewing results

By right clicking on any of the findings, you can drill down to get more information and perform remedial action. You can also expand the results.



Figure 10 - Expanding report

##### 4.4.2 HTML Executive Report

The HTML Executive Report shows the results in a more accessible way, summarizing the results. \*The HTML Executive Report will be opened in a new browser window.

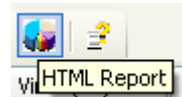


Figure 11 - HTML report

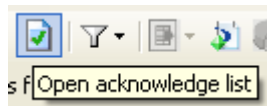
Once the HTML Executive Report is opened, (you might need to allow blocked content in order to show the entire report).

The HTML Executive Report is broken down into several parts:

1. Inspection summary giving you a brief view of the results.
2. Graphs showing the breakdown of problematic hosts Vs hosts with no findings, and the top 10 hosts with the most violations.
3. **“Problematic hosts”** lists the hosts and their violations; you can use this to drill down into specific hosts.
4. **“Problematic objects”** displays the security risks and allows you to focus on specific ones.

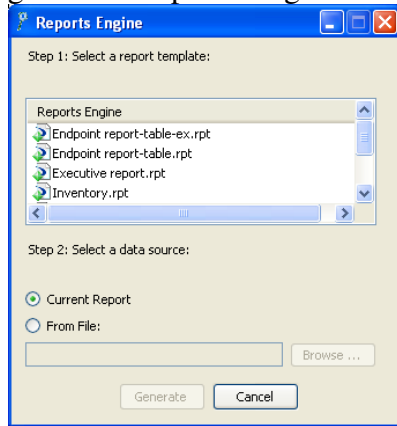
##### 4.4.3 Reporting engine

The reporting engine gives you the option to generate reports focused on different aspects of the inspection.



**Figure 12 – Opening report engine**

The report engine opens a list of reports you can pick from, by default select current report to generate a report using the results of the current inspection.



**Figure 13 - Reports engine**

You can later export the reports to a PDF file easily.



**Figure 14 - Exporting report**