Security Infusion

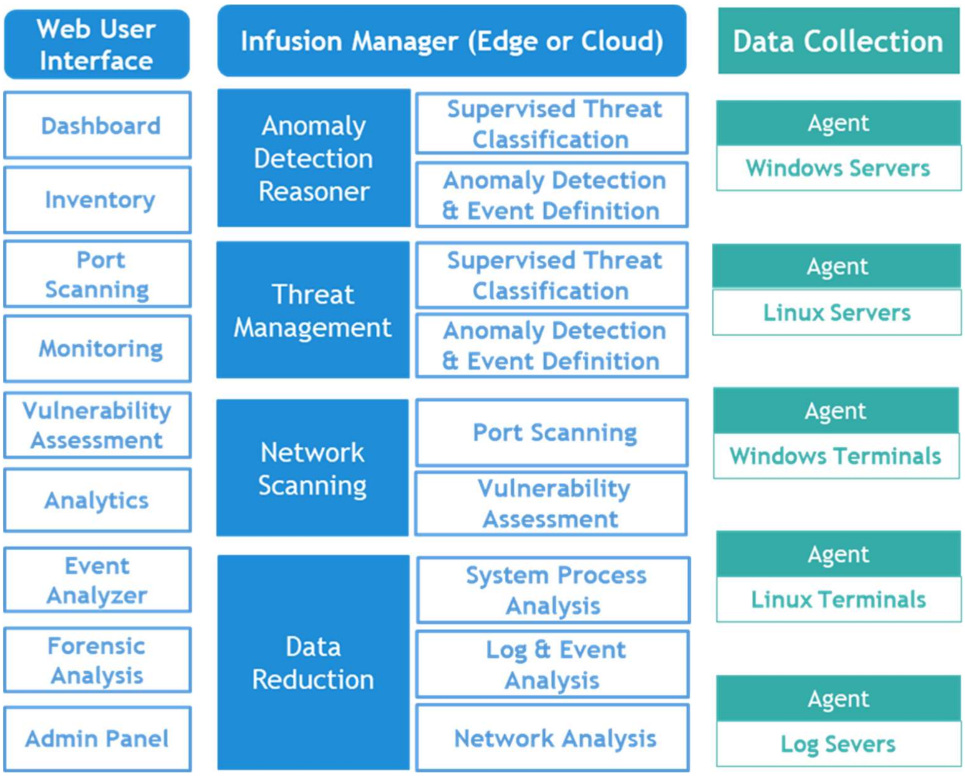
User Manual – Cloud Version

Contents

1. At a glance – Features

Functions designed to optimize the administrative overview while remain simple and straightforward

- Inventory: ICT Assets
- Port Scanning: Services running on devices.
- Monitoring: Host Status, Service Status, Alerts (email & Slack).
- Vulnerability Assessment: According to public vulnerability issues (i.e. CVE® lists). Report Generation.
- Analytics: System Profiling, Processes analysis, Performance Visualization.
- Event Analyzer
- Forensic Analysis



2. Admin user - Quick Start

Go to Settings -> Options to set the “Notification email”. This is the email address set to receive all alerts from Security Infusion.
To enable a new agent configuration, go to Settings -> Inventory. Select “Create new agent’, provide a name for the agent and type (windows or linux). After enabling a new agent, you can download the installation package and install it in the node you want to monitor. More information about agent installation can be found in Agent Installation and Configuration.

3. Agent Installation and Configuration

3.1. Windows version

Unzip the packaged installer, downloaded from https://www.secinfusion.itml.gr/admin. After installing the windows agent, you can configure a set of parameters, located in %Program data path%/Security Infusion/WindowsAuditDService.exe.config. A typical installation path in a 64bit node would be: C:\Program Files (x86)\Security Infusion.

The Security Infusion installer installs two windows services:

- Security Infusion Auditing
- OSSEC HIDS

The main configuration options of Security Infusion Agent are listed below. For changes to take effect, you need to restart the Security Infusion Auditing service.

Main Parameters	Default value	Description
SleepTime	120000	Time in milliseconds between active scans of system (collection and analysis of process list, open handles, DLLs, and open connections). The higher the value, the less frequent the active scans of the system are.
ReportAggregationNumber	3	Agent compares information from "**ReportAggregationNumber"** number of active scans of the system and sends to the cloud only one of them. This function conserves network bandwidth.
ProcMonEnabled	1	If **ProcMonEnabled** is set to "0", the collected data (process list, open handles, DLLs, and open connections) will not be sent to the cloud. Only local analysis of these data is performed.

Monitored Service Parameters	Default value	Description
CPULoadWarning	60	CPULoad monitors CPU usage. IF CPU Usage (%) passes the CPULoadWarning threshold , a warning alert is set off.
CPULoadCritical	95	IF CPU Usage (%) passes the CPULoadCritical threshold , a critical alert is set off.
AvailableMemoryWarning	500	If available RAM is less than AvailableMemoryWarning MBs, a warning alert is set off.
AvailableMemoryCritical	100	If available RAM is less than AvailableMemoryCritical MBs, a critical alert is set off.
FreeSpaceWarning	10	If Free space In any of the available disks of the system is below FreeSpaceWarning %, a warning alert is set off.
FreeSpaceCritical	5	If Free space In any of the available disks of the system is below FreeSpaceCritical %, a critical alert is set off.

Windows Agent Requirements

	Minimum	Recommended
OS	Window s 7	Windows 10 or higher
Requirements	32bit/64bit	32bit/64bit
CPU	Intel i3	Intel i5
Memory	2G	4G

3.2. Linux version

Untar the packaged installer (by running in a linux shell: tar zxvf linux_agent.tar.gz), downloaded from https://www.secinfusion.itml.gr/admin. Run (as root) the centos-installer or ubuntu-installer, based on your linux distribution. To run the installation script, you need to have Java 1.8 or later installed. The installer puts all new files in /var/secinfusion path. After installing the Linux agent, you can configure a set of parameters, located in /var/secinfusion/config.properties.
The Security Infusion installer installs two services:

- Secinfusion. To start, stop, or check the secinfusion service, you can type "service secinfusion {start|stop|status}
- OSSEC HIDS. To control the Ossec service, you can use the "/var/ossec/bin/ossec_control" script

The main configuration options of Security Infusion Agent are listed below. For changes to take effect, you need to restart the secinfusion service.

Main Parameters	Default value	Description
SleepTime	60	Time in seconds between active scans of system (collection and analysis of process list, open handles, DLLs, and open connections). The higher the value, the less frequent the active scans of the system are.
ReportAggregationNumber	3	Agent compares information from "**ReportAggregationNumber"** number of active scans of the system and sends to the cloud only one of them. This function conserves network bandwidth.
ProcMonEnabled	1	If **ProcMonEnabled** is set to "0", the collected data (process list, open handles, DLLs, and open connections) will not be sent to the cloud. Only local analysis of these data is performed.

Monitored Service Parameters	Default value	Description
CPULoadWarning	60	CPULoad monitors CPU usage. IF CPU Usage (%) passes the CPULoadWarning threshold , a warning alert is set off.
CPULoadCritical	95	IF CPU Usage (%) passes the CPULoadCritical threshold , a critical alert is set off.
AvailableMemoryWarning	500	If available RAM is less than AvailableMemoryWarning MBs, a warning alert is set off.
AvailableMemoryCritical	100	If available RAM is less than AvailableMemoryCritical MBs, a critical alert is set off.
LoadWarning	1	If load is above this threshold, a warning alert is set off.
LoadCritical	3	If load is above this threshold, a critical alert is set off.

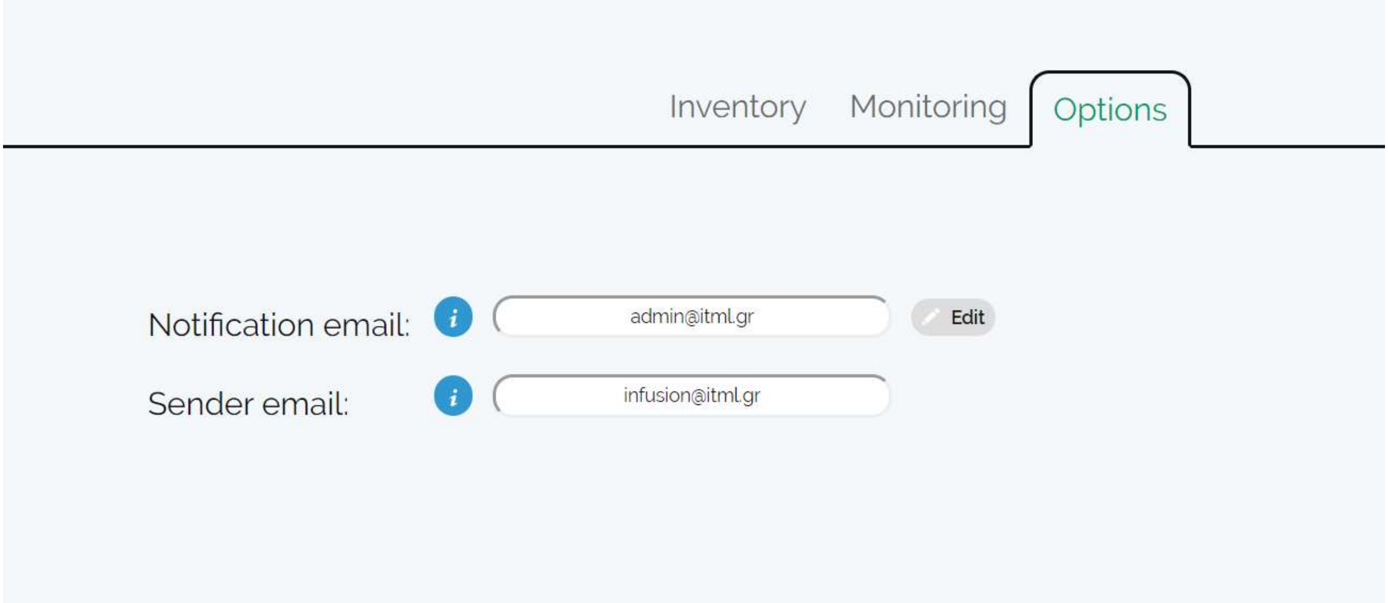
Linux Agent Requirements

	Minimum	Recommended
OS	Centos 7 or Ubuntu 18.04	Centos 7 or Ubuntu 18.04
Platform	32bit/64bit	32bit/64bit
Software requirements	JRE 1.8	JRE 1.8
CPU	Intel i3	Intel i5
Memory	2G	4G

4. Manager Configuration

4.1. Main configuration options

In https://www.secinfusion.itml.gr/admin , in the “Options” tab, you can setup a mail address for receiving alerts.

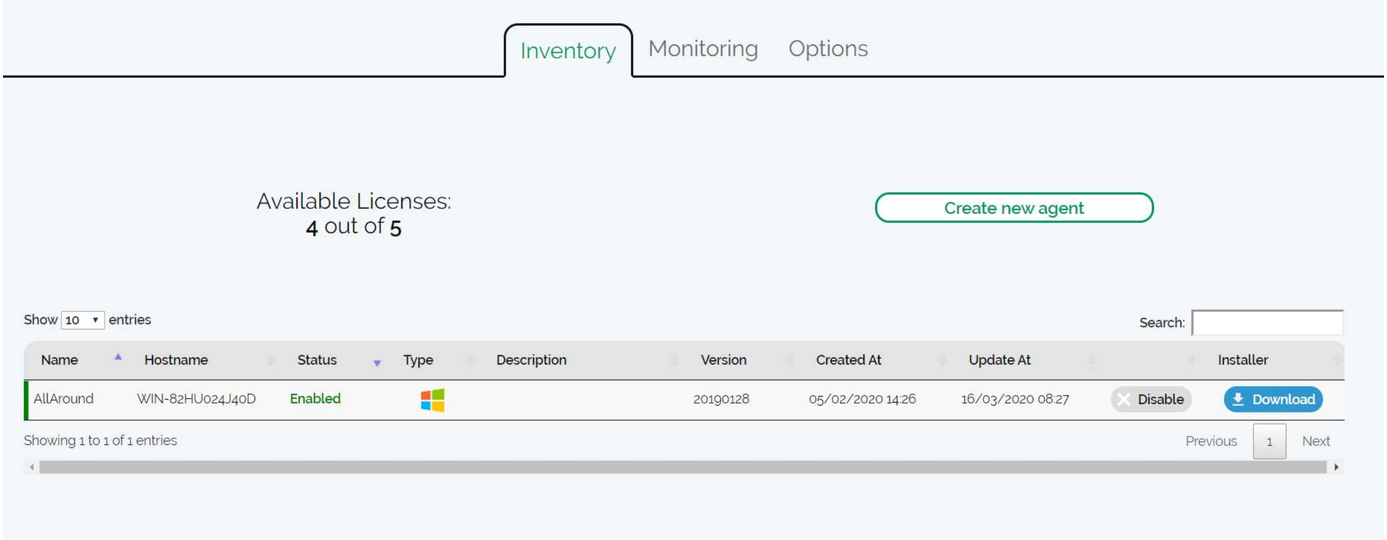


Notification email: admin@itml.gr

Sender email: infusion@itml.gr

4.2. Managing Agents

In https://www.secinfusion.itml.gr/admin , in the “Inventory” tab, you can check the remaining licenses, and enable/disable agents. You can also download the installation packages from this screen.



Available Licenses:
4 out of 5

Show 10 entries

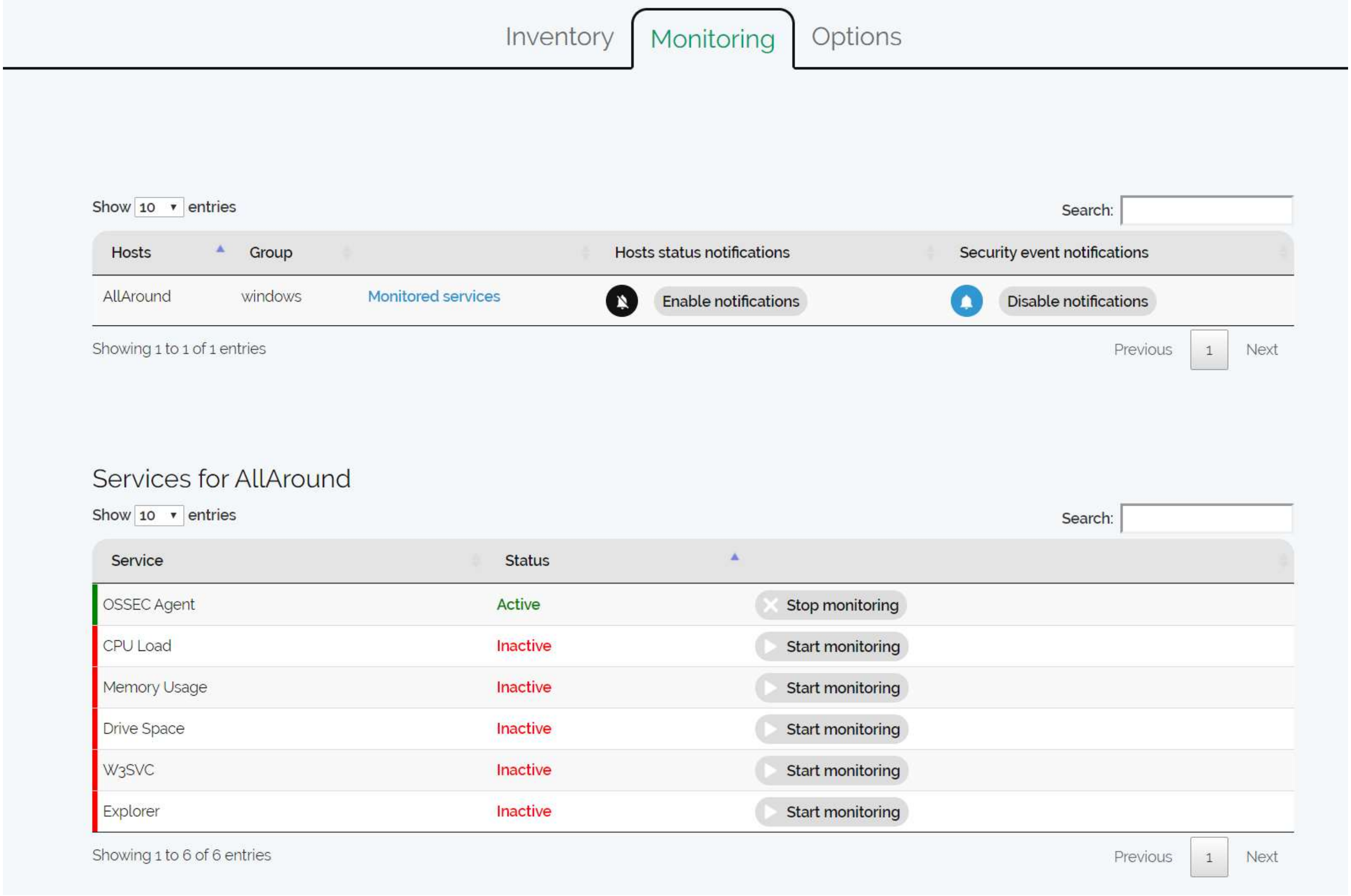
Name	Hostname	Status	Type	Description	Version	Created At	Update At		Installer
AllAround	WIN-82HU024J40D	Enabled	⊞		20190128	05/02/2020 14:26	16/03/2020 08:27	Disable	Download

Showing 1 to 1 of 1 entries

4.3. Monitoring and Alerting Functionality

In https://www.secinfusion.itml.gr/admin , in the “Monitoring” tab, you can enable or disable email notifications for you agents. There are three types of notifications:

- Host status notification: An email notification is sent when there is no communication with the agent for more that 10 minutes (Host down alert)
- Service status notification: An email notification is sent when a monitored service is in warning or critical state
- Security event notification: An email notification is sent when a suspicious event is detected. (The whole list of events per agent can be found in Event Analyser (https://www.secinfusion.itml.gr/event-analyser).



Hosts	Group		Hosts status notifications	Security event notifications
AllAround	windows	Monitored services	Enable notifications	Disable notifications

Services for AllAround

Service	Status	
OSSEC Agent	Active	Stop monitoring
CPU Load	Inactive	Start monitoring
Memory Usage	Inactive	Start monitoring
Drive Space	Inactive	Start monitoring
W3SVC	Inactive	Start monitoring
Explorer	Inactive	Start monitoring