



Олександр Іллюша

Керівник служби технічної
підтримки ESET в Україні

alex@eset.ua



**Хмарний сервер управління:
як швидко забезпечити централізований контроль
захисту ПК в умовах віддаленого режиму роботи**

План

1. Необхідність централізованого моніторингу та управління усіма ПК
2. ESET Cloud Administrator – спрощений варіант сервера управління
3. Основні інструменти хмарного серверу управління:
 - розгортання рішень комплексного захисту на різних ОС
 - моніторинг загального стану безпеки усіх контрольованих ПК
 - миттєві сповіщення про критичні події
4. Автоматична реакція на критичні події:
 - запуск оновлень ОС за фактом відповідного стану
 - послідовність дій при виявленні невидалених загроз
 - ізоляція ПК у разі виявлення мережесих атак

Віддалена робота раніше



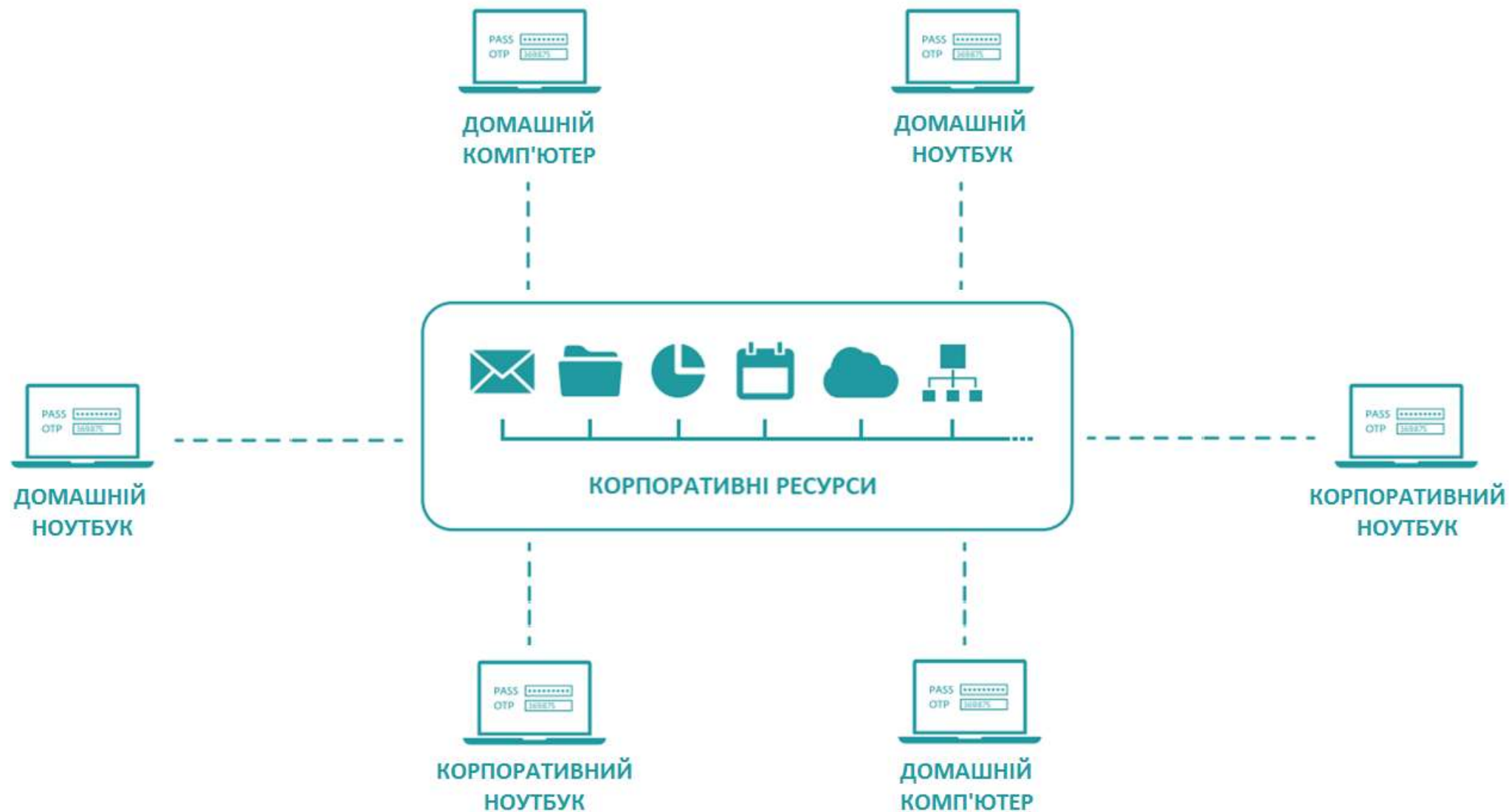


Реалії сьогодення



**Вимушений доступ
незахищених ПК
до корпоративних ресурсів**

Вимушений доступ незахищених ПК до корпоративних ресурсів



Необхідність централізованого моніторингу та управління усіма ПК

- **Основні ризики для корпоративної інфраструктури:**
 - велика кількість слабозахищених домашніх ПК
 - кожний віддалений ПК – потенційна точка проникнення
- **Можливості, що надає централізоване адміністрування:**
 - контроль параметрів безпеки на віддалених ПК
 - своєчасне реагування на складні та приховані загрози
 - автоматичне попередження критичних подій



CLOUD ADMINISTRATOR

ESET Cloud Administrator – спрощений варіант сервера управління

- **Основні переваги хмарного сервера управління:**
 - економія апаратних ресурсів
 - наявність безпечних каналів зв'язку
 - багатофакторна аутентифікація під час входу на портал eca.eset.com
 - швидке розгортання на віддалених та домашніх ПК
 - простий та інтуїтивно зрозумілий інтерфейс

The background is a dark, teal-colored abstract digital pattern. It consists of numerous thin, glowing blue lines and dots that create a sense of depth and movement, resembling a complex network or data flow. The lines are arranged in a way that suggests perspective, with some appearing to recede into the distance. The overall effect is a high-tech, futuristic aesthetic.

Основні інструменти хмарного серверу управління

**Розгортання рішень
комплексного захисту
на різних ОС**

Розгортання рішень комплексного захисту на різних ОС

The screenshot shows the ESET Cloud Administrator interface. A 'Startup Wizard' dialog box is open in the center, displaying a cloud icon with a checkmark and the text: 'Welcome to ESET Cloud Administrator. To add devices you need to create Live Installer which downloads, activates a chosen ESET product and connects devices to ECA automatically. CONTINUE'. The background interface includes a top navigation bar with 'eset CLOUD ADMINISTRATOR', a notification bell, 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. A left sidebar lists menu items: DASHBOARD, COMPUTERS, DETECTIONS, Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and Submit Feedback. The main content area shows a 'Dashboard' with tabs for 'Status Overview', 'Security Overview', 'Computers', 'Antivirus detections', 'Firewall detections', 'ESET applications', and 'Software'. A 'Device status' section shows a table for 'Desktops' with columns for status and count. A 'Product version status' section shows a bar chart for 'Agent', 'Endpoint', and 'Server' with categories 'Up to date', 'Outdated', and 'Unknown'.

Status	Count
Ok	6
Attention required	0
Security risk	0
Total	6

Category	Up to date	Outdated	Unknown
Agent	50%	0%	0%
Endpoint	~75%	~25%	0%
Server	0%	0%	0%

Розгортання рішень комплексного захисту на різних ОС

The screenshot displays the ESET Cloud Administrator interface. In the foreground, a 'Startup Wizard' dialog is open, showing the 'Create Live Installer' step. Below this, the 'Package contents' section lists several components, with 'ESET Endpoint Security' selected. A 'Select product' dialog is also open, displaying a list of ESET products. The 'ESET Endpoint Security' product is highlighted, and a context menu is visible over it, offering options to 'View changelog' and 'Select previous version'. The 'Select previous version' option is active, showing a list of version numbers: 7.2.2055, 7.1.2064, 7.1.2053, 7.0.2100, 6.6.2089, and 6.5.2132. The background shows the main dashboard with various navigation options and a 'Device status' section.

Startup Wizard

1 Create Live Installer
Installer **downloads, activates** a chosen ESET product and **connects devices to ECA automatically.**

Package contents

- Management Agent
- Security Agent
- Full Disk Encryption

To deploy

Select product

If no product version is specified, the latest available version will be used.

- ESET Endpoint Antivirus
- ESET Endpoint Security
- ESET File Security for Microsoft Windows Server
- ESET Full Disk Encryption
- ESET Mail Security for IBM Domino
- ESET Mail Security for Microsoft Exchange Server
- ESET Security for Microsoft SharePoint Server
- ESET Endpoint Antivirus for OS X
- ESET Endpoint Security for OS X

View changelog

Select previous version

7.2.2055
7.1.2064
7.1.2053
7.0.2100
6.6.2089
6.5.2132

CONFIRM CANCEL

BACK CONTINUE

ESET CLOUD ADMINISTRATOR

DASHBOARD

COMPUTERS

DETECTIONS

Reports

Tasks

Policies

Computer Users

Installers

Quarantine

Exclusions

Notifications

Status Overview

Submit Feedback

Dashboard

Status Overview

Total number of devices

Attention required

Software

Device status

Desktops

Ok	6
Attention required	0
Security risk	0
Total	6

Endpoint Server

Outdated Unknown

Розгортання рішень комплексного захисту на різних ОС

The screenshot displays the ESET Cloud Administrator interface. The main window is titled "Startup Wizard" and is currently on step 2, "Choose a deployment option". The wizard provides instructions on how to distribute a created Live Installer, either locally or via remote deployment. Under the "Local deployment" section, there are two radio button options: "Show Live Installer download link" (which is selected) and "Send Live Installer link via email". Below these options, the "Name" is set to "ESET Endpoint Security (uk_UA)". A "Download link" is displayed in a text box: "https://proxy.eset.com/li-handler/?uuid". To the right of the link are two buttons: "COPY" and "DOWNLOAD". At the bottom of the wizard, there are "BACK" and "FINISH" buttons. The background interface shows the "Installers" section with a "webinar" tag and various navigation options like "DASHBOARD", "COMPUTERS", "DETECTIONS", "Reports", "Tasks", "Policies", "Computer Users", "Quarantine", "Exclusions", "Notifications", and "Status Overview".

ESET CLOUD ADMINISTRATOR

Computer Name | QUICK LINKS | HELP | ТЕХПІДТРИМКА УКРАЇНИ | LOGOUT

Installers

Tags: webinar

Startup Wizard

2 Choose a deployment option
Distribute a created Live Installer locally or in a bulk by remote deployment.

Local deployment
You can share a download link or distribute the package using USB drive.

- Show Live Installer download link
- Send Live Installer link via email

Name
ESET Endpoint Security (uk_UA)

Download link
https://proxy.eset.com/li-handler/?uuid

Remote deployment via your network
Download Remote Deployment Tool which enables you to distribute a created Live Installer into your network in a bulk. [Learn more...](#)

BACK FINISH

Розгортання рішень комплексного захисту на різних ОС

The screenshot displays the ESET Cloud Administrator interface. The main window is titled "Startup Wizard" and is currently on step 2, "Choose a deployment option". The wizard provides instructions to "Distribute a created Live Installer locally or in a bulk by remote deployment." There are two main deployment options: "Local deployment" and "Send Live Installer to email addresses".

Local deployment
You can share a download link or distribute the package using USB drive.

- Show Live Installer download link
- Send Live Installer link via email

Send Live Installer to email addresses

EMAIL ADDRESS	NAME	Remove All
<input type="text"/>	<input type="text"/>	

Buttons: +, MORE, See email preview...

Remote deployment
Paste from clipboard... your network

[Download Remote Deployment Tool](#) which enables you to distribute a created Live Installer into your network in a bulk. [Learn more...](#)

Buttons: BACK, SEND

The background interface shows the "Installers" section with a "webinar" tag. The top navigation bar includes "eset CLOUD ADMINISTRATOR", a notification bell, "Computer Name", "QUICK LINKS", "HELP", "ТЕХПІДТРИМКА УКРАЇНИ", and "LOGOUT". The left sidebar contains various navigation items like Dashboard, Computers, Detections, Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, and Status Overview. At the bottom, there are buttons for "CREATE INSTALLER...", "ACTIONS", and a "COLLAPSE" button.

Розгортання на Windows




Recycle Bin



Google Chrome



epi_win_liv...


PACKAGE
INSTALLER

Вітаємо
Інсталяція
Завершення

Програму інстальовано


Програму ESET Endpoint Security інстальовано. Тепер вона постійно перевірятиме ваш комп'ютер на віруси та шкідливе програмне забезпечення.

Натисніть кнопку *Готово*, щоб завершити налаштування продукту й розпочати активацію.

Докладніше про безпеку: [база знань ESET](#)

ESET у соціальних мережах: [Facebook](#) [Twitter](#) [YouTube](#)

Готово

 **Firewall & network protection**

View firewall options
Windows Firewall and ESET Брандмауер are both turned off. Tap or click to see available options.



Розгортання на Windows

eset CLOUD ADMINISTRATOR

Computer Name QUICK LINKS HELP ТЕХПІДТРИМКА УКРАЇНИ LOGOUT

Computers

SHOW SUBGROUPS All (4) Tags... ADD FILTER PRESETS

Groups	COMPUTER NAME	STAT	MODULES	LAST CONNECTED	ALER	DETEC
CUSTOM GROUPS						
All (4)						
Lost & found (4)						
DYNAMIC GROUPS						
Windows computers						
Windows (desktops)						
Windows (servers)						
Linux computers						
Mac computers						
Computers with outdated modules						
Computers with outdated operating system						
Problematic computers						
Not activated security product						
No manageable security product						

Tags

webinar

ADD COMPUTER ACTIONS MUTE

COLLAPSE

Розгортання на Windows

eset CLOUD ADMINISTRATOR

Computer Name: client1.study.local

QUICK LINKS | HELP | ТЕХПІДТРИМКА УКРАЇНИ | LOGOUT

COMPUTERS > client1.study.local

- OVERVIEW
- CONFIGURATION
- LOGS
- TASK EXECUTIONS
- INSTALLED APPLICATIONS**
- ALERTS
- QUESTIONS
- DETECTIONS AND QUARANTINE
- DETAILS

client1.study.local
Add description
Select tags

FQDN	Client1.study.local
Parent Group	/All/Lost & found
IP	192.168.200.17
Applied Policies Count	3
Member of Dynamic Groups	Loading...

Microsoft Windows 10 Enterprise LTSC Evaluation 64-bit
VMware, Inc., VMware7,1
S/N VMware-42 3a e3 10 1c ad 09 eb-ed 50 d3 af 16 9c 94 87

AMD EPYC 7401P 24-Core Processor	RAM 4 GiB	Storage 32 GiB
----------------------------------	-----------	----------------

Everything is OK

Alerts	No alerts
Unresolved Detections Count	0
Last Connected Time	2020 Apr 7 13:21:11
Last Scan Time	n/a
Detection Engine	n/a
Updated	Unknown

Products & Licenses

CLOSE | COMPUTER | SAVE | HARDWARE

Розгортання на Windows

eset CLOUD ADMINISTRATOR Computer Name QUICK LINKS ▾ HELP ▾ ТЕХПІДТРИМКА УКРАЇНИ LOGOUT

DASHBOARD
COMPUTERS
DETECTIONS
Reports
Tasks
Policies
Computer Users
Installers
Quarantine
Exclusions
Notifications
Status Overview
[Submit Feedback](#)

< BACK Computers > client1.study.local

- OVERVIEW
- CONFIGURATION
- LOGS
- TASK EXECUTIONS
- INSTALLED APPLICATIONS**
- ALERTS
- QUESTIONS
- DETECTIONS AND QUARANTINE
- DETAILS

NAME	VENDOR	VERSION	SIZE (MB)	AGENT SUPPORT	LATEST APPLICATION	VERSION CHECK
ESET Management Agent	ESET, spol. s r.o.	7.1.717.0	172	yes	7.1.717.0	Up-to-date versio...
Microsoft Visual C++ 2008 Redistributab...	Microsoft Corpora...	9.0.30729.6161	13	yes		
VMware Tools	VMware, Inc.	10.2.0.7253323	83	yes		
ESET Endpoint Security	ESET, spol. s r.o.	7.2.2055.0	200	yes		
Google Chrome	Google LLC	80.0.3987.149		no		
Microsoft Visual C++ 2008 Redistributab...	Microsoft Corpora...	9.0.30729.6161	10	yes		

CLOSE COMPUTER ▾ UNINSTALL UPDATE ESET PRODUCTS


Розгортання на MacOS

Имя	Размер	Тип	Дата добавления
epi_mac_live_installer.pkg	3,9 МБ	Устано...й пакет	Сегодня, 6:57

- Избранное
 - Недавние
 - iCloud Drive
 - Программы
 - Рабочий ст...
 - Документы
 - Загрузки
- Устройства
 - Удаленный...
 - BOOT
- Теги
 - Красный
 - Оранжевый
 - Желтый
 - Зеленый

Установка: Бизнес-решения ESET

Установка успешно завершена.



Установка прошла успешно.

ПО успешно установлено.

- Введение
- Загрузчик
- Размещение
- Тип установки
- Установка
- Обзор**

eset

Назад Закреть

Розгортання на MacOS

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a 'Computer Name' dropdown, 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS', 'Reports', 'Tasks', 'Policies', 'Computer Users', 'Installers', 'Quarantine', 'Exclusions', 'Notifications', 'Status Overview', and a 'Submit Feedback' button. The main content area is titled 'Computers' and features a toolbar with status icons, 'SHOW SUBGROUPS', a filter for 'Mac computers (1)', a 'Tags...' dropdown, 'ADD FILTER', and 'PRESETS'. Below the toolbar is a table with columns: 'COMPUTER NAME', 'STATUS', 'MODULES', 'LAST CONNECT', 'ALER', and a settings icon. The table lists one computer: 'imac-5.local' with IP '10.0.2.15', status 'Updated', and a last connect time of '2020 Apr 8 19:06:21'. The left sidebar also shows a tree view of groups: 'CUSTOM GROUPS' (All (8), Lost & found (8)), 'DYNAMIC GROUPS' (Windows computers, Windows (desktops), Windows (servers), Linux computers, Mac computers), and 'Computers with outdated modules', 'Computers with outdated operating system', 'Problematic computers', 'Not activated security product', and 'No manageable security product'. At the bottom, there are buttons for 'ADD COMPUTER', 'ACTIONS', 'MUTE', and a set of navigation icons.

eset CLOUD ADMINISTRATOR

Computer Name

QUICK LINKS

HELP

ТЕХПІДТРИМКА УКРАЇНИ

LOGOUT

DASHBOARD

COMPUTERS

DETECTIONS

Reports

Tasks

Policies

Computer Users

Installers

Quarantine

Exclusions

Notifications

Status Overview

Submit Feedback

COLLAPSE

Computers

Groups

CUSTOM GROUPS

All (8)

Lost & found (8)

DYNAMIC GROUPS

Windows computers

Windows (desktops)

Windows (servers)

Linux computers

Mac computers

Computers with outdated modules

Computers with outdated operating system

Problematic computers

Not activated security product

No manageable security product

Tags

webinar

ADD COMPUTER

ACTIONS

MUTE

COMPUTER NAME	STATUS	MODULES	LAST CONNECT	ALER
imac-5.local 10.0.2.15	Updated	Updated	2020 Apr 8 19:06:21	0

Розгортання на MacOS

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a 'Computer Name' dropdown, 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS', 'Reports', 'Tasks', 'Policies', 'Computer Users', 'Installers', 'Quarantine', 'Exclusions', 'Notifications', 'Status Overview', and a 'Submit Feedback' button. The main content area is titled 'Computers > imac-5.local' and features a sub-menu with 'OVERVIEW', 'CONFIGURATION', 'LOGS', 'TASK EXECUTIONS', 'INSTALLED APPLICATIONS', 'ALERTS', 'QUESTIONS', 'DETECTIONS AND QUARANTINE', and 'DETAILS'. The 'OVERVIEW' section shows the computer name 'imac-5.local' with options to 'Add description' and 'Select tags'. Below this is a table of system information:

FQDN	iMac-5.local
Parent Group	/All/Lost & found
IP	10.0.2.15
Applied Policies Count	2
Member of Dynamic Groups	/All/Mac computers

A green status box indicates 'Everything is OK' with a checkmark and a speaker icon. Below it is another table of status information:

Alerts	No alerts
Unresolved Detections Count	0
Last Connected Time	2020 Apr 8 19:16:21
Last Scan Time	n/a
Detection Engine	21133 (20200408)
Updated	Updated

Hardware information is shown in a separate box:

- macOS 10.13 (High Sierra) 64-bit
- innotek GmbH, iMac11,3
- S/N 0
- Intel(R) Core(TM) i5-2320 CPU @ 3.00GHz
- RAM 2 GiB
- Storage 60 GiB

The 'Products & Licenses' section lists installed software:

- ESET Endpoint Security 6.8.400.0 (Up-to-date version)
- ESET Management Agent 7.1.840.0 (Up-to-date version)
- 3AH-2C8-5NF ESET Endpoint Security for Mac OS X (2020 Jun 6 15:00:00)

At the bottom, there are buttons for 'CLOSE', 'COMPUTER', 'SAVE', and 'HARDWARE'.

Розгортання на MacOS

eset® CLOUD ADMINISTRATOR

Computer Name QUICK LINKS HELP ТЕХПІДТРИМКА УКРАЇНИ LOGOUT

< BACK Computers > imac-5.local

- DASHBOARD
- COMPUTERS
- DETECTIONS
- Reports
- Tasks
- Policies
- Computer Users
- Installers
- Quarantine
- Exclusions
- Notifications
- Status Overview
- Submit Feedback

- OVERVIEW
- CONFIGURATION
- LOGS
- TASK EXECUTIONS
- INSTALLED APPLICATIONS
- ALERTS
- QUESTIONS
- DETECTIONS AND QUARANTINE
- DETAILS

NAME	VENDOR	VERSION	SIZE [MB]	AGENT SUPPORT	LATEST APPLIC	VERSION CHECK
iBooks		1.15		no		
iTunes		12.8.2		no		
Calculator		10.13		no		
Calendar		10.0		no		
Chess		3.15		no		
Contacts		11.0		no		
DVD Player		5.8		no		
Dictionary		2.2.2		no		
ESET Endpoint Security	ESET, spol. s r.o.	6.8.400.0	134	yes	6.8.400.0	Up-to-date versio...
ESET Management Agent	ESET, spol. s r.o.	7.1.840.0	107	yes	7.1.840.0	Up-to-date versio...
Font Book		8.0		no		
Image Capture		7.0		no		
Mail		11.5		no		
Maps		2.0		no		
Messages		11.0		no		

CLOSE COMPUTER UNINSTALL UPDATE ESET PRODUCTS

Розгортання на Linux



НАСОЛОДЖУЙСЯ БЕЗПЕКОЮ

Розгортання на Linux



DASHBOARD



COMPUTERS



DETECTIONS



Reports



Tasks



Policies



Computer Users



Installers



Quarantine



Exclusions



Notifications



Status Overview



Submit Feedback



COLLAPSE

Agent Installer Script

Installers > Agent Installer Script

Name

Agent installer (Linux)

Description

Tags

Select tags

Parent group (optional)

Select existing group or Create new group

Initial installer configuration [?]

Configuration type

- Do not configure
- Select configuration from the list of policies

Product improvement program [?]

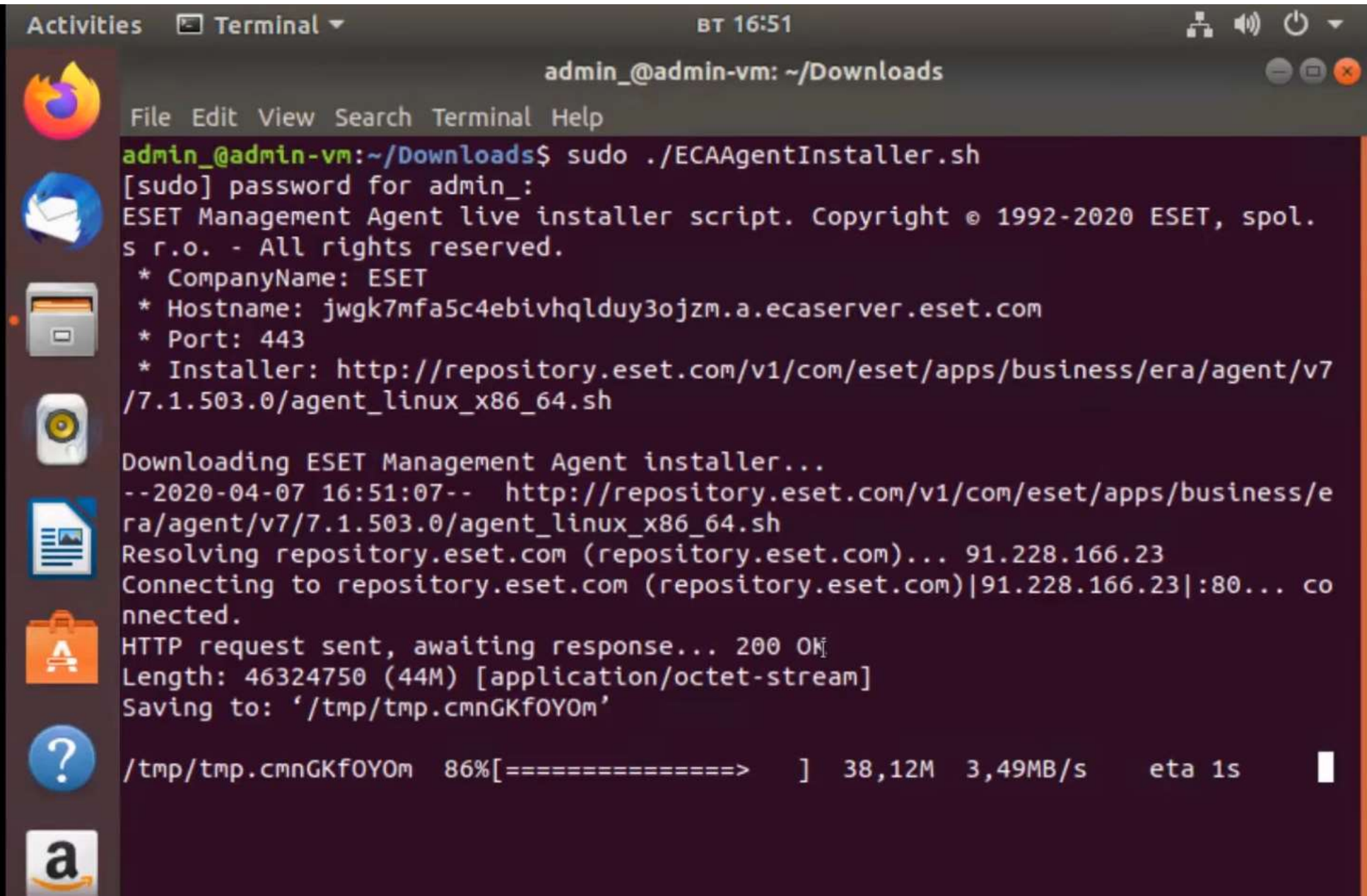
- Participate in product improvement program

SAVE & DOWNLOAD

SAVE AND CLOSE

CANCEL

Розгортання на Linux



```
admin_@admin-vm: ~/Downloads
File Edit View Search Terminal Help
admin_@admin-vm:~/Downloads$ sudo ./ECAAgentInstaller.sh
[sudo] password for admin_:
ESET Management Agent live installer script. Copyright © 1992-2020 ESET, spol.
s r.o. - All rights reserved.
* CompanyName: ESET
* Hostname: jwgk7mfa5c4ebivhqlduy3ojzm.a.ecaserver.eset.com
* Port: 443
* Installer: http://repository.eset.com/v1/com/eset/apps/business/era/agent/v7
/7.1.503.0/agent_linux_x86_64.sh

Downloading ESET Management Agent installer...
--2020-04-07 16:51:07-- http://repository.eset.com/v1/com/eset/apps/business/e
ra/agent/v7/7.1.503.0/agent_linux_x86_64.sh
Resolving repository.eset.com (repository.eset.com)... 91.228.166.23
Connecting to repository.eset.com (repository.eset.com)|91.228.166.23|:80... co
nected.
HTTP request sent, awaiting response... 200 OK
Length: 46324750 (44M) [application/octet-stream]
Saving to: '/tmp/tmp.cmngKfOY0m'

/tmp/tmp.cmngKfOY0m 86%[=====> ] 38,12M 3,49MB/s eta 1s
```


Розгортання на Linux

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a 'Computer Name' dropdown, 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS', 'Reports', 'Tasks', 'Policies', 'Computer Users', 'Installers', 'Quarantine', 'Exclusions', 'Notifications', 'Status Overview', and a 'Submit Feedback' button. The main content area is titled 'Tasks' and features a filter bar with 'Software Install (1)', a 'Tags...' dropdown, 'ADD FILTER', and 'PRESETS' buttons. Below the filter bar is a table with columns for 'NAME', 'TAGS', 'STATUS', and 'TYPE'. A single task is listed: 'EEA for Linux Install' with a status of '1' and a type of 'Software Install'. The left pane shows a tree view of task types, with 'Software Install' selected under 'Client Tasks'. The bottom of the interface includes a 'webinar' tag, 'NEW...' and 'ACTIONS' buttons, and a pagination control showing '1'.

eset CLOUD ADMINISTRATOR

Computer Name

QUICK LINKS

HELP

ТЕХПІДТРИМКА УКРАЇНИ

LOGOUT

Tasks

Task Types

Client Tasks

- ESET Security Product
 - Diagnostics
 - End computer isolation from network
 - Export Managed Products Configuration
 - Isolate computer from network
 - Modules Update
 - Modules Update Rollback
 - On-Demand Scan
 - Product Activation
 - Quarantine Management
 - Run SysInspector Script
 - Server Scan
 - Software Install
 - SysInspector Log Request (Windows only)
 - Upload Quarantined File
- ESET Cloud Administrator
- Operating System

Tags

webinar

Software Install (1)

ADD FILTER

PRESETS

NAME	TAGS	STATUS	TYPE
EEA for Linux Install		1	Software Install

NEW...

ACTIONS

1

Розгортання на Linux

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a search bar for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS, Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a 'Submit Feedback' button. The main content area is titled 'Computers' and features a filter bar with 'SHOW SUBGROUPS' (checked), 'Linux computers (1)', a 'Tags...' dropdown, 'ADD FILTER', and 'PRESETS'. Below this is a table with columns: 'COMPUTER NAME', 'STATUS', 'MODULES', 'LAST CONNECTED', 'ALERTS', and 'DETECTIONS'. A single entry is visible: 'admin-vm' with IP '192.168.120.19', status 'OK', and 'Updated' modules. The left sidebar also shows a 'Groups' section with 'CUSTOM GROUPS' (All (4), Lost & found (4)) and 'DYNAMIC GROUPS' (Windows computers, Windows (desktops), Windows (servers), Linux computers (selected), Mac computers, Computers with outdated modules, Computers with outdated operating system, Problematic computers, Not activated security product, No manageable security product). At the bottom, there are 'ADD COMPUTER', 'ACTIONS', and 'MUTE' buttons, along with a 'COLLAPSE' button and a 'webinar' tag.

eset CLOUD ADMINISTRATOR

Computer Name

QUICK LINKS

HELP

ТЕХПІДТРИМКА УКРАЇНИ

LOGOUT

Computers

Groups

COMPUTER NAME

STATUS

MODULES

LAST CONNECTED

ALERTS

DETECTIONS

CUSTOM GROUPS

All (4)

Lost & found (4)

DYNAMIC GROUPS

Windows computers

Windows (desktops)

Windows (servers)

Linux computers

Mac computers

Computers with outdated modules

Computers with outdated operating system

Problematic computers

Not activated security product

No manageable security product

Tags

webinar

ADD COMPUTER

ACTIONS

MUTE

COMPUTER NAME	STATUS	MODULES	LAST CONNECTED	ALERTS	DETECTIONS
admin-vm 192.168.120.19	OK	Updated	2020 Apr 7 16:57:18	0	0

Розгортання на Linux

eset CLOUD ADMINISTRATOR

Computer Name QUICK LINKS HELP ТЕХПІДТРИМКА УКРАЇНИ LOGOUT

DASHBOARD COMPUTERS DETECTIONS Reports Tasks Policies Computer Users Installers Quarantine Exclusions Notifications Status Overview

Submit Feedback

COLLAPSE

< BACK Computers > admin-vm

OVERVIEW CONFIGURATION LOGS TASK EXECUTIONS INSTALLED APPLICATIONS ALERTS QUESTIONS DETECTIONS AND QUARANTINE DETAILS

admin-vm Add description Select tags

FQDN	Loading...
Parent Group	/All/Lost & found
IP	192.168.120.19
Applied Policies Count	2
Member of Dynamic Groups	Loading...

Everything is OK

Alerts	No alerts
Unresolved Detections Count	0
Last Connected Time	2020 Apr 7 16:57:18
Last Scan Time	n/a
Detection Engine	21126 (20200407)
Updated	Updated

Ubuntu 64-bit VMware, Inc., VMware Virtual Platform Loading... Loading...

AMD EPYC 7401P 24-Core Processor RAM 2 GiB Storage 16 GiB

Products & Licenses

ESET Management Agent 7.1.503.0
ESET Endpoint Antivirus 7.0.13.0

CLOSE COMPUTER SAVE HARDWARE

Розгортання рішень комплексного захисту на різних ОС

eset CLOUD ADMINISTRATOR

Computer Name QUICK LINKS HELP ТЕХПІДТРИМКА УКРАЇНИ LOGOUT

Installers

Tags

Tags... ADD FILTER PRESETS

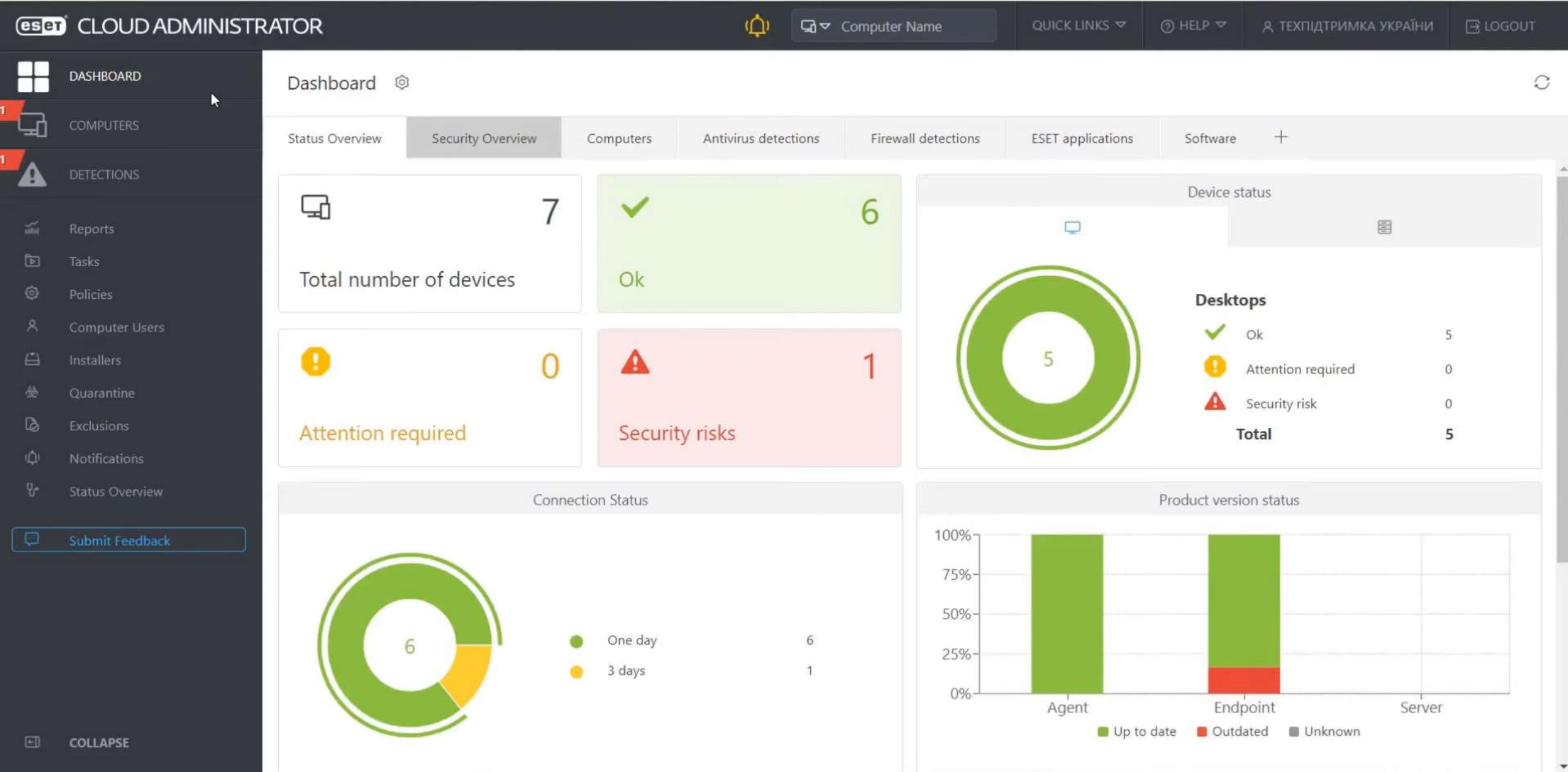
<input type="checkbox"/>	NAME	TAGS	TYPE	INST#	PROJ	POLI	LICE	LANG	<input type="checkbox"/>
<input type="checkbox"/>	ESET Endpoint Security (uk_UA)		All-in-one Installer	OK	ESET...		ЗАН...	uk_UA	
<input type="checkbox"/>	Agent installer (Linux)		Agent Live Installer	OK					
<input type="checkbox"/>	ESET Endpoint Security for OS X (en_US)		All-in-one Installer	OK	ESET...		ЗАН...	en_US	

webinar

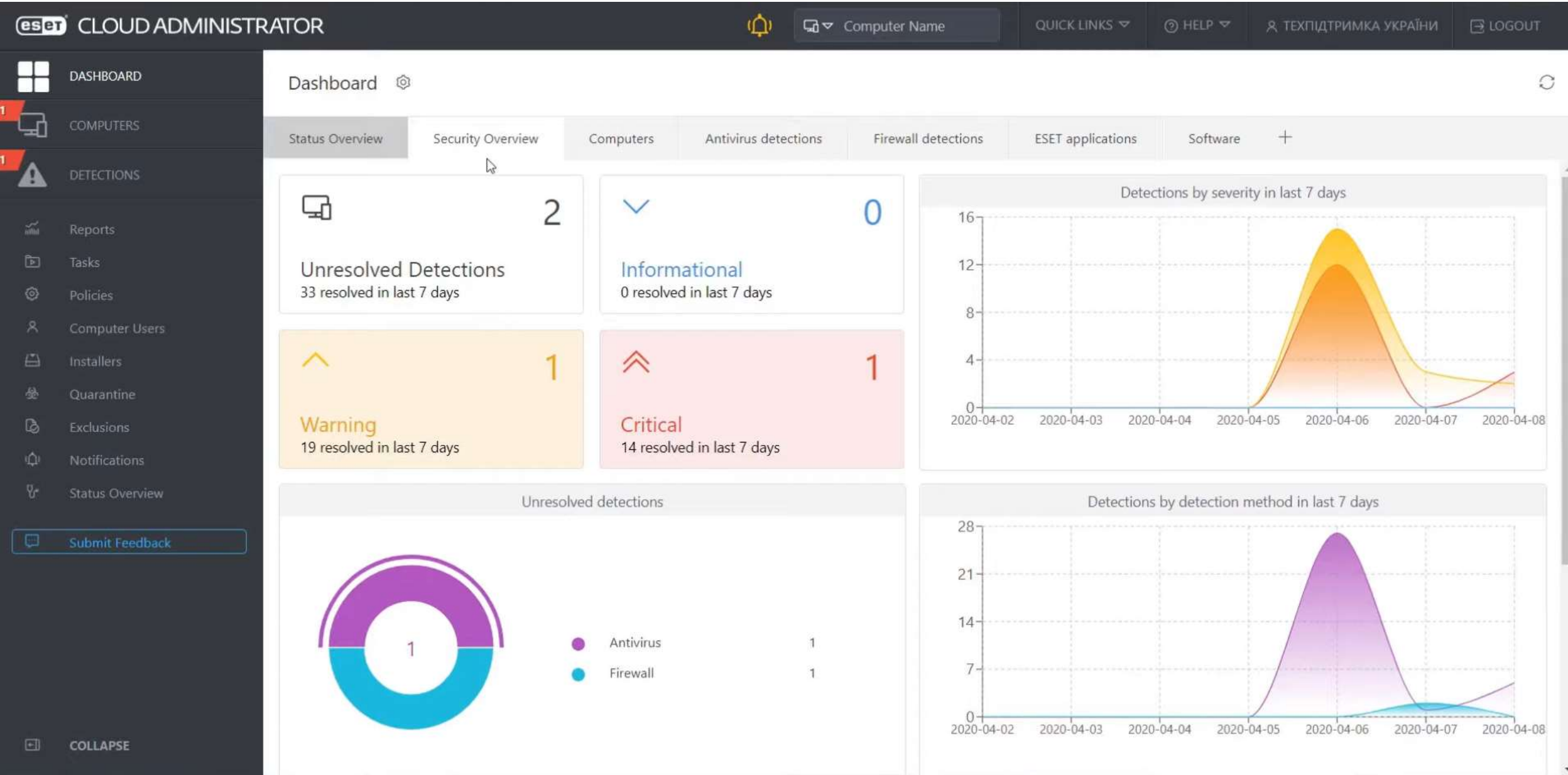
CREATE INSTALLER... ACTIONS

**Моніторинг загального
стану безпеки
усіх контрольованих ПК**

Моніторинг загального стану безпеки усіх контрольованих ПК



Моніторинг загального стану безпеки усіх контрольованих ПК



Моніторинг загального стану безпеки усіх контрольованих ПК

eset CLOUD ADMINISTRATOR

Computer Name | QUICK LINKS | HELP | ТЕХПІДТРИМКА УКРАЇНИ | LOGOUT

Dashboard

Status Overview | Security Overview | Computers | Antivirus detections | Firewall detections | ESET applications | Software

Daily summary of detection events in last 30 days

Count (Time of occurrence)

Fixed interval (Time of occurrence)

Generated 0 minutes ago

Top detections in last 7 days

- Win32/Pterodo.XG.gen
- Win32/Kryptik.GYOZ
- Win32/Agent.TXZ
- MSIL/Spy.Agent.CLD
- MSIL/Kryptik.UBJ
- Win32/Injector.EJWC
- MSIL/Kryptik.IRC
- Generik.BDLGDAC
- Win32/Kryptik.GYJC
- Win32/Filecoder.FS

Generated 0 minutes ago

Last scan

- Never
- One day
- 3 days

Generated 0 minutes ago

Top users with detection events in last 7 days

- WIN10_EES_6\admin
- WIN10_EES_7\Tester
- NT AUTHORITY\SYSTEM
- Administrator initiated scan

Generated 0 minutes ago

Unresolved high severity detection events in last 7 days

Computio	Time of	Severity	Detectio	Detectio	Detectio	Scanner	Detectio	Object	Object	Action	Action	Detectio	Restart	User	Process	Circumst
name	occurren		type	name	flags		engine	type	URI	perform	error	handled	required		name	
win10...	2020 ...	▲ Cr...	trojan	Win3...	Variant	On-d...	21129...	file	file:///...			no	no	Admi...	C:\Pr...	

Generated 0 minutes ago

Submit Feedback

COLLAPSE

Моніторинг загального стану безпеки усіх контрольованих ПК

eset CLOUD ADMINISTRATOR Computer Name QUICK LINKS HELP ТЕХПІДТРИМКА УКРАЇНИ LOGOUT

Dashboard Settings

Status Overview Security Overview Computers Antivirus detections Firewall detections ESET applications Software +

Installed applications

Group by (Application name)	Group by (Application vendor)	Group by (Application version)	Count (Application name)
7-Zip 19.00 (x64)	Igor Pavlov	19.00	2
ESET Endpoint Antivirus	ESET, spol. s r.o.	7.0.13.0	1
ESET Endpoint Security	ESET, spol. s r.o.	6.5.2132.6	1
ESET Endpoint Security	ESET, spol. s r.o.	7.2.2055.0	3
ESET Full Disk Encryption	ESET, spol. s r.o.	1.1.0.0	1
ESET Management Agent	ESET, spol. s r.o.	7.1.503.0	1
ESET Management Agent	ESET, spol. s r.o.	7.1.717.0	6
Google Chrome	Google LLC	80.0.3987.163	4
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30...	Microsoft Corporation	9.0.30729.6161	2
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30...	Microsoft Corporation	9.0.30729.6161	2
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0....	Microsoft Corporation	12.0.21005.1	1
Microsoft Visual C++ 2017 Redistributable (x64) - 14.12...	Microsoft Corporation	14.12.25810.0	4
Microsoft Visual C++ 2017 Redistributable (x86) - 14.12...	Microsoft Corporation	14.12.25810.0	4
Nmap 7.80	Nmap Project	7.80	1
Npcap 0.9982	Nmap Project	0.9982	1
VMware Tools	VMware, Inc.	10.2.0.7253323	2
VMware Tools	VMware, Inc.	10.3.10.12406962	4

Generated 0 minutes ago

COLLAPSE

Миттєві сповіщення про критичні події

Миттєві сповіщення про критичні події

eset CLOUD ADMINISTRATOR

Computer Name QUICK LINKS HELP ТЕХПІДТРИМКА УКРАЇНИ LOGOUT

Notifications

Tags... ADD FILTER PRESETS

Tags

webinar

<input type="checkbox"/>	NAME	TAGS	ENAE	STAT	NOTI	L
<input type="checkbox"/>	Malware outbreak alert (count per time criteria)	webinar	● ...	✓	Noti...	Texn...
<input type="checkbox"/>	Network attack alert	webinar	● ...	✓	Noti...	Texn...
<input type="checkbox"/>	Computers report problems alert		○ ...	✓	Noti...	Texn...
<input type="checkbox"/>	Outdated modules alert	webinar	● ...	✓	Noti...	Texn...
<input type="checkbox"/>	Managed clients not connecting alert		● ...	⚠ ...	Noti...	Adm...
<input type="checkbox"/>	Outdated ESET software alert	webinar	● ...	✓	Noti...	Texn...
<input type="checkbox"/>	Malicious file detected (trojan / worm / virus / application)		○ ...	✓	Noti...	Texn...
<input type="checkbox"/>	Notification has invalid configuration and will not be triggered		● ...	⚠ ...	At le...	Adm...
<input type="checkbox"/>	Outdated version of ESET Endpoint Antivirus detected		● ...	⚠ ...	Noti...	Adm...
<input type="checkbox"/>	At least one computer has not connected for more than 14 days	webinar	● ...	✓	Noti...	Texn...
<input type="checkbox"/>	Potentially unsafe application detected		● ...	⚠ ...	Noti...	Adm...
<input type="checkbox"/>	At least one infected file that was not cleaned automatically was detected during computer scan	webinar	● ...	✓	Exec...	Texn...
<input type="checkbox"/>	Detection occurred in memory	webinar	● ...	✓	Noti...	Texn...
<input type="checkbox"/>	Potentially unwanted application (PUA) detected		● ...	⚠ ...	Noti...	Adm...
<input type="checkbox"/>	High severity alert detected by HIPS occurred	webinar	● ...	✓	Noti...	Texn...

ACTIONS

Миттєві сповіщення про критичні події

oksana.ch@eset.ua - Becky!

Файл Правка Вид Почта Інструменти Справка Поиск в заголовках

Тема	От	Отправлено	Размер	Кому
Outdated ESET Software Alert!	ECA <ecareport@eca.eset.com>	08.04.2020 16:55:17	19,339	<support@eset.ua>
Problematic Computers Alert!	ECA <ecareport@eca.eset.com>	08.04.2020 7:34:29	19,332	<support@eset.ua>
Not cleaned detection occurred during computer scan	ECA <ecareport@eca.eset.com>	06.04.2020 23:04:59	20,709	<support@eset.ua>
Detection Win32/Adware.FileTour.FHO has occurred in memory on computer win10_ees_7.esetdemo.local	ECA <ecareport@eca.eset.com>	06.04.2020 22:06:05	20,111	<support@eset.ua>

От: ECA <ecareport@eca.eset.com> Кому: <support@eset.ua>
Тема: Not cleaned detection occurred during computer scan Дата: Mon, 6 Apr 2020 20:04:59 GMT

eset CLOUD ADMINISTRATOR

NEW NOTIFICATION

Not cleaned detection occurred during computer scan

Computer name: win10_ees_7.esetdemo.local
User account that was used to run the scan: Administrator initiated scan
Time of occurrence: 06.04.20, 22:54:30 UTC+3
Scanned targets: Оперативна пам'ять;C:\Завантажувальні сектори/UEFI;D:\Завантажувальні сектори/UEFI;C:\D:\
Number of scanned files: 183 722
Number of infected files: 90
Number of cleaned files: 0
Scanner: Сканер, доступний на вимогу

This message was sent by ESET cloud service

ESET Cloud Administrator
© 1992-2020 ESET, spol. s r.o. All Rights Reserved.

Автоматична реакція на критичні події

**Автоматичне оновлення ОС
за фактом відповідного стану ПК**

Автоматичне оновлення ОС за фактом відповідного стану ПК

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a search bar for 'Computer Name', and links for 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS', 'Reports', 'Tasks', 'Policies', 'Computer Users', 'Installers', 'Quarantine', 'Exclusions', 'Notifications', and 'Status Overview'. A 'Submit Feedback' button is located at the bottom of the sidebar.

The main content area is titled 'Computers' and features a toolbar with status icons (warning, info, success, error), 'SHOW SUBGROUPS' (checked), a filter 'Computers with out... (1)', a 'Tags...' dropdown, 'ADD FILTER', and 'PRESETS'. Below the toolbar is a table with columns: 'Groups', 'COMPUTER NAME', 'STATUS', 'MODULES', 'LAST CONNECT', and 'ALER'. The table lists several dynamic groups under 'All (7)', including 'Lost & found (7)', 'Windows computers', 'Windows (desktops)', 'Windows (servers)', 'Linux computers', 'Mac computers', 'Computers with outdated modules', 'Computers with outdated operating system' (highlighted), 'Problematic computers', 'Not activated security product', and 'No manageable security product'. A single computer entry is visible in the table:

Groups	COMPUTER NAME	STATUS	MODULES	LAST CONNECT	ALER
CUSTOM GROUPS	desktop-40B4c11 192.168.120.21	!	Unknown	2020 Apr 8 14:55:03	!

At the bottom of the interface, there are buttons for 'ADD COMPUTER', 'ACTIONS', and 'MUTE', along with a pagination control showing '1' and a refresh icon.

Автоматичне оновлення ОС за фактом відповідного стану ПК

eset® CLOUD ADMINISTRATOR

Computer Name QUICK LINKS HELP ТЕХПІДТРИМКА УКРАЇНИ LOGOUT

DASHBOARD COMPUTERS DETECTIONS Reports Tasks Policies Computer Users Installers Quarantine Exclusions Notifications Status Overview

Submit Feedback

< BACK Tasks > Task Details: Update OS - Triggers

Summary Executions Triggers

<input type="checkbox"/>	TRIGGER DESCRIPTION	TRIGGER TYPE	TARGETS	MODIFICATION TIME
<input type="checkbox"/>	Triggers when a client joins the dynamic group	Joined Dynamic Group Trigger	1 group(s)	2020 Apr 8 14:36:12

CLOSE DELETE

Автоматичне оновлення ОС за фактом відповідного стану ПК

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a 'Computer Name' dropdown, 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS', 'Reports', 'Tasks', 'Policies', 'Computer Users', 'Installers', 'Quarantine', 'Exclusions', 'Notifications', 'Status Overview', and a 'Submit Feedback' button. The main content area is titled 'Client Task Executions' for the computer 'desktop-4084c11'. It features a table with columns: TASK NAME, TASK DESCRIPTION, TYPE, PLANNED, and LAST STATUS. The table lists several tasks, with the first one, 'Update OS', having a status of 'Finished' with a green checkmark. A mouse cursor is hovering over the 'Finished' status. The table also includes a '2020' column on the far right. At the bottom of the interface, there are 'CLOSE' and 'COMPUTER' buttons.

eset CLOUD ADMINISTRATOR

Computer Name

QUICK LINKS

HELP

ТЕХПІДТРИМКА УКРАЇНИ

LOGOUT

< BACK Computers > desktop-4084c11

OVERVIEW

CONFIGURATION

LOGS

TASK EXECUTIONS

INSTALLED APPLICATIONS

ALERTS

QUESTIONS

DETECTIONS AND QUARANTINE

DETAILS

Client Task Executions

LAST ITEMS 1000

ADD FILTER

PRESETS

TASK NAME	TASK DESCRIPTION	TYPE	PLANNED	LAST STATUS	
Update OS		Operating System Update	yes	✓ Finished	2020
Sysinspector Log		SysInspector Log Request (Windows only)	yes		
Isolate (firewall detections)		Isolate computer from network	yes		
In-Depth Scan		On-Demand Scan	yes		
Display message about isolation		Display Message	yes		

CLOSE COMPUTER

**Автоматична реакція
при виявленні невидалених загроз**

Автоматична реакція при виявленні невидалених загроз

oksana.ch@eset.ua - Becky!

Файл Правка Вид Почта Инструменты Справка

Поиск в заголовках

Тема	От	Отправлено	Размер	Кому
Not cleaned detection occurred during computer scan	ECA <ecareport@eca.eset.com>	08.04.2020 4:09:59	20,409	<support@eset.ua>

От: ECA <ecareport@eca.eset.com> Кому: <support@eset.ua>
Тема: Not cleaned detection occurred during computer scan Дата: Wed, 8 Apr 2020 01:09:59 GMT

eset CLOUD ADMINISTRATOR

NEW NOTIFICATION

Not cleaned detection occurred during computer scan

Computer name: win10_ees_6_esetdemo.local
User account that was used to run the scan: WIN10_EES_6\admin
Time of occurrence: 08.04.20, 04:09:19 UTC+3
Scanned targets: C:\Users\admin\Documents\Core (1)\Core\8hwse1_808185588\8hwse1_808185588.exe
Number of scanned files: 1
Number of infected files: 1
Number of cleaned files: 0
Scanner: Сканер, доступний на вимогу

This message was sent by ESET cloud service

ESET Cloud Administrator
© 1992-2020 ESET, spol. s r.o. All Rights Reserved.

Автоматична реакція при виявленні невиданих загроз

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a 'Computer Name' dropdown, 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS' (highlighted with a red notification badge), 'Reports', 'Tasks', 'Policies', 'Computer Users', 'Installers', 'Quarantine', 'Exclusions', 'Notifications', and 'Status Overview'. A 'Submit Feedback' button is located at the bottom of the sidebar. The main content area is titled 'Detections' and features a filter bar with 'SHOW SUBGROUPS' (checked), 'All (1)', and a 'Tags...' dropdown. Below the filter bar, there are two filter boxes: 'DETECTION CATEGORY' set to 'Antivirus' and 'DETECTION RESOLVED' set to 'No'. An 'ADD FILTER' button is also present. The detection list table has columns for 'DETECTION TYPE', 'CAUSE', 'ACTION', 'OCCUR', 'RESOLVED', and 'COMPUTER NAME'. A single detection is listed: 'Antivirus trojan' with cause 'Win32/Kryptik.GYJC', 1 occurrence, and 0/1 resolved. The computer name is 'win10ees_6.esetde...'. At the bottom, there are buttons for 'SCAN COMPUTERS', 'RESOLVE', and 'ACTIONS', along with a pagination control showing '1'.

eset CLOUD ADMINISTRATOR

Computer Name

QUICK LINKS

HELP

ТЕХПІДТРИМКА УКРАЇНИ

LOGOUT

DASHBOARD

COMPUTERS

DETECTIONS

Reports

Tasks

Policies

Computer Users

Installers

Quarantine

Exclusions

Notifications

Status Overview

Submit Feedback

COLLAPSE

Detections

Groups

CUSTOM GROUPS

Dynamic Groups

Tags

webinar

SHOW SUBGROUPS

All (1)

Tags...

DETECTION CATEGORY

Antivirus

DETECTION RESOLVED

ADD FILTER

PRESETS

	DETECTION TYPE	CAUSE	ACTION	OCCUR	RESOLVED	COMPUTER NAME
<input type="checkbox"/>	Antivirus trojan	Win32/Kryptik.GYJC		1	0/1	win10ees_6.esetde...

SCAN COMPUTERS

RESOLVE

ACTIONS

1

Автоматична реакція при виявленні невиданих загроз

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a home icon, a dropdown menu for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS (with a '2' badge), Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a 'Submit Feedback' button. The main content area shows the details for a computer named 'win10_ees_6.esetdemo.local'. The left sidebar menu is expanded to 'DETECTIONS AND QUARANTINE', which has a '1' badge. The computer details panel includes a 'Security risk' alert (indicated by a red warning icon and a speaker icon) and a table of status information. The table shows 'Alerts' as 'No alerts', 'Unresolved Detections Count' as '1', 'Last Connected Time' as '2020 Apr 8 04:26:56', 'Last Scan Time' as '2020 Apr 8 04:18:09', and 'Detection Engine' as '21129 (20200407)'. Other details include the FQDN 'Win10_EES_6.esetdemo.local', Parent Group '/All/Lost & found', IP '192.168.120.20', Applied Policies Count '3', and Member of Dynamic Groups. Hardware information shows 'AMD EPYC 7401P 24-Core Processor', 'RAM 4 GiB', and 'Storage 64 GiB'. The operating system is 'Microsoft Windows 10 Enterprise Evaluation 64-bit' with S/N 'VMware-42 3a 61 bf b0 b8 c3 9d-5a e8 07 0e 98 50 9f 38'. Products & Licenses section lists 'ESET Management Agent 7.1.717.0' (Up-to-date version) and 'ESET Endpoint Security 7.2.2055.0' (Up-to-date version). At the bottom, there are buttons for 'CLOSE', 'COMPUTER', 'SAVE', and 'HARDWARE'.

eset CLOUD ADMINISTRATOR

Computer Name

QUICK LINKS

HELP

ТЕХПІДТРИМКА УКРАЇНИ

LOGOUT

< BACK Computers > win10_ees_6.esetdemo.local

OVERVIEW

CONFIGURATION

LOGS

TASK EXECUTIONS

INSTALLED APPLICATIONS

ALERTS

QUESTIONS

DETECTIONS AND QUARANTINE

DETAILS

win10_ees_6.esetdemo.local

Add description

webinar

FQDN Win10_EES_6.esetdemo.local

Parent Group /All/Lost & found

IP 192.168.120.20

Applied Policies Count 3

Member of Dynamic Groups /All/Windows computers /All/Windows computers/Windows (desktops)

Microsoft Windows 10 Enterprise Evaluation 64-bit

VMware, Inc., VMware7,1

S/N VMware-42 3a 61 bf b0 b8 c3 9d-5a e8 07 0e 98 50 9f 38

AMD EPYC 7401P 24-Core Processor

RAM 4 GiB

Storage 64 GiB

Security risk

Alerts No alerts

Unresolved Detections Count 1

Last Connected Time 2020 Apr 8 04:26:56

Last Scan Time 2020 Apr 8 04:18:09

Detection Engine 21129 (20200407)

Products & Licenses

ESET Management Agent 7.1.717.0 Up-to-date version

ESET Endpoint Security 7.2.2055.0 Up-to-date version

3AH-2C8-5NF ESET Endpoint Security for Windows 2020 Jun 6 15:00:00

CLOSE COMPUTER SAVE HARDWARE

Автоматична реакція при виявленні невиданих загроз

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a dropdown for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS (with a '2' badge), Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a 'Submit Feedback' button. The main content area is titled 'Client Task Executions' for the computer 'win10_ees_6.esetdemo.local'. It features a table with columns: TASK NAME, TASK DESCRIPTION, TYPE, PLANNED, LAST STATUS, and a date column. The table lists several tasks, with 'In-Depth Scan' highlighted as 'Running'. A mouse cursor is pointing at the 'Running' status. The bottom of the interface has 'CLOSE' and 'COMPUTER' buttons.

eset CLOUD ADMINISTRATOR

Computer Name

QUICK LINKS

HELP

ТЕХПІДТРИМКА УКРАЇНИ

LOGOUT

< BACK Computers > win10_ees_6.esetdemo.local

OVERVIEW

CONFIGURATION

LOGS

TASK EXECUTIONS

INSTALLED APPLICATIONS

ALERTS

QUESTIONS

DETECTIONS AND QUARANTINE

DETAILS

Client Task Executions

LAST ITEMS 1000

ADD FILTER

PRESETS

TASK NAME	TASK DESCRIPTION	TYPE	PLANNED	LAST STATUS	
Sysinspector Log		SysInspector Log Request (Windows only)	yes	Finished	2020
Isolate (firewall detections)		Isolate computer from network	yes		
In-Depth Scan		On-Demand Scan	yes	Running	2020
Display message about isolation		Display Message	yes		

CLOSE COMPUTER

Автоматична реакція при виявленні невидалених загроз

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a dropdown for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS (with a red notification badge '2'), Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a 'Submit Feedback' button. The main content area is titled 'Client Task Executions' for the computer 'win10_ees_6.esetdemo.local'. It features a table with columns: TASK NAME, TASK DESCRIPTION, TYPE, PLANNED, LAST STATUS, and a date column. The table lists four tasks: 'Sysinspector Log' (Finished), 'Isolate (firewall detections)' (Planned), 'In-Depth Scan' (Running), and 'Display message about isolation' (Planned). A red notification badge '1' is visible next to the 'DETECTIONS AND QUARANTINE' menu item.

eset CLOUD ADMINISTRATOR

Computer Name

QUICK LINKS

HELP

ТЕХПІДТРИМКА УКРАЇНИ

LOGOUT

< BACK Computers > win10_ees_6.esetdemo.local

OVERVIEW

CONFIGURATION

LOGS

TASK EXECUTIONS

INSTALLED APPLICATIONS

ALERTS

QUESTIONS

DETECTIONS AND QUARANTINE

DETAILS

Client Task Executions

LAST ITEMS 1000

ADD FILTER

PRESETS

TASK NAME	TASK DESCRIPTION	TYPE	PLANNED	LAST STATUS	
Sysinspector Log		SysInspector Log Request (Windows only)	yes	Finished	2020
Isolate (firewall detections)		Isolate computer from network	yes		
In-Depth Scan		On-Demand Scan	yes	Running	2020
Display message about isolation		Display Message	yes		

CLOSE COMPUTER

Автоматична реакція при виявленні невиданих загроз

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a dropdown for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS' (with a red notification badge), 'Reports', 'Tasks', 'Policies', 'Computer Users', 'Installers', 'Quarantine', 'Exclusions', 'Notifications', 'Status Overview', and a 'Submit Feedback' button. The main content area shows the 'Computers' view for 'win10_ees_6.esetdemo.local'. The 'LOGS' section is active, displaying a table with columns for 'SysInspector', 'Log Collector', and 'Diagnostic logs'. A table entry for '2020 Apr 8 04:18:11' is highlighted, with a context menu open over it. The menu options are 'SysInspector Log', 'Download SysInspector Log', and 'Open SysInspector Log Viewer'. At the bottom, there are buttons for 'CLOSE', 'COMPUTER', and 'REQUEST LOG (WINDOWS ONLY)'. A 'javascript:' watermark is visible in the bottom-left corner.

Автоматична реакція при виявленні невидалених загроз

The screenshot displays the ESET Cloud Administrator interface. At the top, the header includes the ESET logo, 'CLOUD ADMINISTRATOR', a notification bell, a dropdown for 'Computer Name' (win10_ees_6.esetdemo.local), and links for 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS (with a red '2' badge), Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a 'Submit Feedback' button. The main content area is titled 'win10_ees_6.esetdemo.local' and has a '< BACK' button. It features a left-hand menu with 'OVERVIEW', 'CONFIGURATION', 'LOGS' (highlighted), 'TASK EXECUTIONS', 'INSTALLED APPLICATIONS', 'ALERTS', 'QUESTIONS', 'DETECTIONS AND QUARANTINE' (with a red '2' badge), and 'DETAILS'. The 'LOGS' section is further divided into 'SysInspector', 'Log Collector', and 'Diagnostic logs'. A 'Risk Level' indicator shows a scale from 1 to 9. A search bar is present in the top right of the logs area. The central pane lists system components: Running processes, Network Connections, Important Registry Entries, Services, Drivers, Critical Files, System Scheduler Tasks, System Information (highlighted with a mouse cursor), File Details, and About. At the bottom, there are buttons for 'CLOSE', 'COMPUTER' (with a dropdown arrow), and 'REQUEST LOG (WINDOWS ONLY)'.

Автоматична реакція при виявленні невиданих загроз

The screenshot displays the ESET Cloud Administrator interface for a computer named 'win10_ees_6.esetdemo.local'. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS (with a red notification badge), Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a Submit Feedback button. The main content area is divided into three tabs: SysInspector, Log Collector, and Diagnostic logs. The Log Collector tab is active, showing a Risk Level indicator with a slider set to 5-9. Below the indicator is a tree view of system components: Important Registry Entries, Critical Files (with a sub-item 'hosts'), System Scheduler Tasks, System Information, and About. A table with columns PROCESS, PATH, PID, USERNAME, STATUS, FILE DESCRIPTION, and COMPANY is visible but empty. The bottom of the interface includes buttons for CLOSE, COMPUTER (with a dropdown arrow), and REQUEST LOG (WINDOWS ONLY).

eset CLOUD ADMINISTRATOR

Computer Name

QUICK LINKS

HELP

ТЕХПІДТРИМКА УКРАЇНИ

LOGOUT

< BACK Computers > win10_ees_6.esetdemo.local

OVERVIEW

CONFIGURATION

LOGS

TASK EXECUTIONS

INSTALLED APPLICATIONS

ALERTS

QUESTIONS

DETECTIONS AND QUARANTINE

DETAILS

SysInspector Log Collector Diagnostic logs

Risk Level 5-9

Important Registry Entries

Critical Files

hosts

System Scheduler Tasks

System Information

About

PROCESS	PATH	PID	USERNAME	STATUS	FILE DESCRIPTION	COMPANY
---------	------	-----	----------	--------	------------------	---------

CLOSE COMPUTER REQUEST LOG (WINDOWS ONLY)

Автоматична реакція при виявленні невидалених загроз

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a dropdown for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS (highlighted), Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a 'Submit Feedback' button. The main content area shows the 'LOGS' section for a specific computer (win10_ees_6.esetdemo.local). The 'LOGS' section is divided into 'SysInspector', 'Log Collector', and 'Diagnostic logs'. A 'Risk Level' indicator shows a score of 5-9. A tree view on the left lists categories: Important Registry Entries, Critical Files (expanded to show 'hosts'), System Scheduler Tasks, System Information, and About. The 'hosts' file is highlighted, and a table below shows the detected threat details.

NAME	VALUE	STATUS
hosts		5
Line	192.168.120.20 microsoft-office-verification.azurewebsites.net	5

At the bottom of the interface, there are buttons for 'CLOSE', 'COMPUTER', and 'REQUEST LOG (WINDOWS ONLY)'.

Автоматична реакція при виявленні невидалених загроз

192.168.120.20 microsoft-office-verification.azurewebsites.net



Автоматична реакція при виявленні невидалених загроз

eset CLOUD ADMINISTRATOR

Computer Name

QUICK LINKS

HELP

ТЕХПІДТРИМКА УКРАЇНИ

LOGOUT

DASHBOARD

COMPUTERS

DETECTIONS

Reports

Tasks

Policies

Computer Users

Installers

Quarantine

Exclusions

Notifications

Status Overview

Submit Feedback

COLLAPSE

New Task

Tasks > New Task

Basic

Settings

Summary

Run command settings

Command line to run ⓘ

```
>office-verification.azurewebsites.net" > file.temp && echo.Y | move file.temp hosts
```

Working directory ⓘ

BACK CONTINUE FINISH CANCEL

Автоматична реакція при виявленні невидалених загроз

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a 'Computer Name' dropdown, 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS (with a red notification badge), Reports, Tasks (highlighted), Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a 'Submit Feedback' button. The main content area is titled 'Tasks' and features a filter bar with 'Run Command (1)', a 'Tags...' dropdown, and an 'ADD FILTER' button. Below the filter bar is a table with columns: NAME, TAGS, STATUS, and TYPE. A single task is listed: 'hosts' with a green status bar and the number '1', and a type of 'Run Command'. The left sidebar also shows a tree view of task categories: Client Tasks, ESET Security Product, ESET Cloud Administrator, Operating System (with sub-items: Display Message, Operating System Update, Run Command, Shutdown computer, Software Install, Software Uninstall, Stop Managing (Uninstall ESET Management Agent)), Full Disk Encryption, and Server Tasks. At the bottom, there is a 'Tags' section with a search icon and a 'webinar' tag. The bottom right corner contains a 'NEW...' button, an 'ACTIONS' dropdown, and a pagination control showing '1'.

eset CLOUD ADMINISTRATOR

Computer Name

QUICK LINKS

HELP

ТЕХПІДТРИМКА УКРАЇНИ

LOGOUT

Tasks

Task Types

Client Tasks

ESET Security Product

ESET Cloud Administrator

Operating System

Display Message

Operating System Update

Run Command

Shutdown computer

Software Install

Software Uninstall

Stop Managing (Uninstall ESET Management Agent)

Full Disk Encryption

Server Tasks

Tags

webinar

NAME	TAGS	STATUS	TYPE
hosts		✓ 1	Run Command

NEW...

ACTIONS

1

Автоматична реакція при виявленні невидалених загроз

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, the text 'eset CLOUD ADMINISTRATOR', a notification bell, a dropdown menu for 'Computer Name', 'QUICK LINKS', 'HELP', and 'ТЕХПІДТРИМКА УКРАЇНИ' (Ukrainian Technical Support), and a 'LOGOUT' button.

The left sidebar contains a navigation menu with the following items: DASHBOARD, COMPUTERS, DETECTIONS (with a red notification badge '2'), Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a 'Submit Feedback' button.

The main content area shows the configuration for a computer named 'win10_ees_6.esetdemo.local'. The 'LOGS' section is active, displaying a 'Risk Level' indicator (a horizontal bar with a green-to-red gradient) and a search box. Below this, a tree view shows the system scan results, with 'Critical Files' expanded to show 'hosts', 'system.ini', and 'win.ini'. The 'hosts' file is highlighted, and its details are shown in a table:

NAME	VALUE	STATUS
hosts		1

At the bottom of the interface, there are three buttons: 'CLOSE', 'COMPUTER' (with a dropdown arrow), and 'REQUEST LOG (WINDOWS ONLY)'.

Автоматична реакція при виявленні невиданих загроз

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a dropdown for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS' (highlighted with a red '1'), 'Reports', 'Tasks', 'Policies', 'Computer Users', 'Installers', 'Quarantine', 'Exclusions', 'Notifications', 'Status Overview', and a 'Submit Feedback' button. The main content area shows the 'Client Task Executions' page for the computer 'win10_ees_6.esetdemo.local'. The page has a breadcrumb trail: '< BACK Computers > win10_ees_6.esetdemo.local'. The 'TASK EXECUTIONS' menu item is selected. The table below shows the following data:

TASK NAME	TASK DESCRIPTION	TYPE	PLANNED	LAST STATUS	
Sysinspector Log		SysInspector Log Request (Windows only)	yes	✓ Finished	2020
Isolate (firewall detections)		Isolate computer from network	yes		
In-Depth Scan		On-Demand Scan	yes	✓ Finished	2020
Display message about isolation		Display Message	yes		

At the bottom of the interface, there are 'CLOSE' and 'COMPUTER' buttons.

Автоматична ізоляція ПК у разі виявлення мережеских атак



Recycle Bin



Google Chrome

ENDPOINT SECURITY

Мережеву загрозу заблоковано
Атака сканування портів TCP

З [комп'ютера](#) в мережі надходить зловмисний трафік. Це може свідчити про спробу атаки на ваш комп'ютер.

Загрозу заблоковано.

Докладніше про це повідомлення





Recycle Bin



Google Chrome

eset ENDPOINT SECURITY

⚠️ СТАТУС ЗАХИСТУ 1

🔍 СКАНУВАННЯ КОМП'ЮТЕРА 1

🔄 ОНОВЛЕННЯ

⚙️ ПАРАМЕТРИ

📁 ІНСТРУМЕНТИ •

❓ ДОВІДКА ТА ПІДТРИМКА

ENJOY SAFER TECHNOLOGIES™

⚠️ Попередження про небезпеку

⚠️ Доступ до мережі заблоковано

З міркувань безпеки адміністратор ізолював цей комп'ютер від мережі.

Доступ до мережі заблоковано на весь час ізоляції. Зв'яжіться з адміністратором, щоб

Message from 4/8/2020 12:52 AM

З міркувань безпеки адміністратор ізолював цей комп'ютер від мережі.
Доступ до мережі заблоковано на весь час ізоляції. Зв'яжіться з адміністратором за номером телефону +38 (044) 545 77 26, щоб вирішити проблему.

OK

eset ENDPOINT SECURITY

⚠️ Мережеву загрозу заблоковано

Атака сканування портів TCP

З [комп'ютера](#) в мережі надходить зловмисний трафік. Це може свідчити про спробу атаки на ваш комп'ютер.

Загрозу заблоковано.

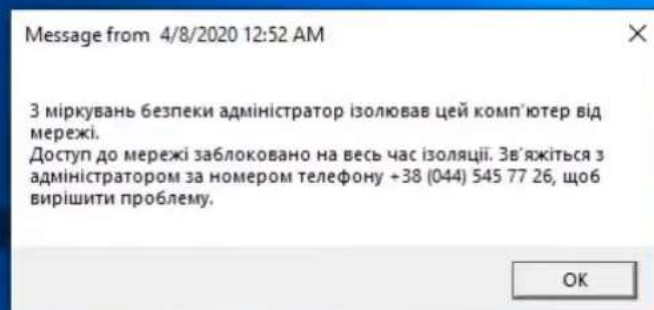
Докладніше про це повідомлення



Recycle Bin

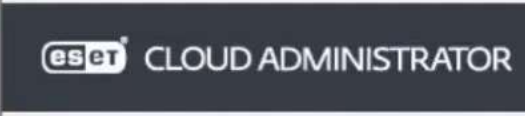


Google Chrome



Тема	От	Отправлено	Размер	Кому
Your reports from ESET Cloud Administrator, generated on 4/7/20, 11:36:56 PM UTC+3	ECA <ecareport@eca.eset.com>	07.04.2020 23:36:57	51,467	<support@eset.ua>
Your reports from ESET Cloud Administrator, generated on 4/6/20, 9:11:34 AM UTC+2	ECA <ecareport@eca.eset.com>	06.04.2020 10:11:36	51,268	<support@eset.ua>
Your reports from ESET Cloud Administrator, generated on 4/6/20, 11:40:44 PM UTC+3	ECA <ecareport@eca.eset.com>	06.04.2020 23:40:45	396,362	<support@eset.ua>

От: ECA <ecareport@eca.eset.com> Кому: <support@eset.ua>
Тема: Your reports from ESET Cloud Administrator, generated on 4/7/20, 11:36:56 PM UTC+3 Дата: Tue, 7 Apr 2020 20:36:57 GMT



GENERATE REPORT TASK
Your reports from ESET Cloud Administrator, generated on 4/7/20, 11:36:56 PM UTC+3
You have requested following reports from ESET Cloud Administrator, which are attached to this message:
• New Firewall event

To login to your ESET Cloud Administrator, go to <https://eca.eset.com>.

This message was sent by ESET cloud service
ESET Cloud Administrator
© 1992-2020 ESET, spol. s r.o. All Rights Reserved.

Автоматична ізоляція ПК у разі виявлення мережевих атак

New Firewall event

1 / 1




 CLOUD ADMINISTRATOR

New Firewall event

Generated at

2020 Apr 7 23:36:44 (UTC+03:00)

Computer name	Time of occurrence	Severity	Event	Source address	Source port	Target address	Target port	Protocol	Inbound communication	User	Process name	Rule name	Built-in rule name	Detection name	Occurrences per minute
client1.study.local	2020 Apr 7 23:34:40	 Warning	TCP Port Scanning attack	192.168.200.12	38549	192.168.200.17	110	TCP	yes						1



Автоматична ізоляція ПК у разі виявлення мережесих атак

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'CLOUD ADMINISTRATOR', a notification bell, a search bar for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains navigation options: DASHBOARD, COMPUTERS (with a red notification badge), DETECTIONS (with a red notification badge), Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, and Status Overview. A 'Submit Feedback' button is located at the bottom of the sidebar.

The main content area is titled 'Computers' and features a table of computer records. The table has columns for 'Groups', 'COMPUTER NAME', 'STATUS', 'MODULES', 'LAST CONNECT', and 'ALI'. The 'client1.study.local' computer is highlighted in red, indicating a network attack. The 'Status' column for this computer shows a red warning icon. The 'Last Connect' column for this computer shows '2020 Apr 9 20:36:10' and a red notification badge with the number '1'. Other computers in the list have a green checkmark in the 'Status' column and a yellow notification badge in the 'Last Connect' column.

Below the table, there is a 'Tags' section with a search bar and a 'webinar' tag. At the bottom of the interface, there are buttons for 'ADD COMPUTER', 'ACTIONS', and 'MUTE', along with a 'Stop' button in the bottom right corner.

Groups	COMPUTER NAME	STATUS	MODULES	LAST CONNECT	ALI
CUSTOM GROUPS					
All (6)					
Lost & found (6)					
DYNAMIC GROUPS					
Windows computers					
Windows (desktops)					
Windows (servers)					
Linux computers					
Mac computers					
Computers with outdated modules					
Computers with outdated operating system					
Problematic computers					
Not activated security product					
No manageable security product					
	admin-vm 192.168.120.19	✓	Updated	2020 Apr 7 21:16:36	0
	client1.study.local 192.168.200.17	⚠	Updated	2020 Apr 9 20:36:10	1
	desktop-vf3r1gg 192.168.200.20	✓	Updated	2020 Apr 6 15:56:...	0
	imac-5.local 10.0.2.15	✓	Updated	2020 Apr 9 20:36:21	0
	win10_ees_6.esetdemo.local 192.168.120.20	✓	Updated	2020 Apr 9 14:56:38	0
	win10_ees_7.esetdemo.local 192.168.120.28	✓	Updated	2020 Apr 7 10:26:...	0

Автоматична ізоляція ПК у разі виявлення мережевих атак

The screenshot displays the ESET Cloud Administrator web interface. At the top, the header includes the ESET logo, the text "eset CLOUD ADMINISTRATOR", a notification bell icon, a search bar for "Computer Name", and navigation links for "QUICK LINKS", "HELP", "ТЕХПІДТРИМКА УКРАЇНИ", and "LOGOUT".

The left sidebar contains a navigation menu with the following items: DASHBOARD, COMPUTERS, DETECTIONS (with a red notification badge), Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a "Submit Feedback" button at the bottom.

The main content area is titled "Alerts" and shows the path "Computers > client1.study.local". It features a sub-menu with "OVERVIEW", "CONFIGURATION", "LOGS", "TASK EXECUTIONS", "INSTALLED APPLICATIONS", "ALERTS" (highlighted with a red notification badge), "QUESTIONS", "DETECTIONS AND QUARANTINE" (with a yellow notification badge), and "DETAILS".

The "Alerts" section displays a "PROBLEM" card with the title "Network access blocked" and a description: "For security reasons this computer has been isolated from the network by the administrator". The card includes a red warning icon, a yellow information icon, and a dropdown arrow. There are also "ADD FILTER" and "PRESETS" buttons.

At the bottom of the interface, there are "CLOSE" and "COMPUTER" buttons.

Автоматична ізоляція ПК у разі виявлення мережевих атак

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'CLOUD ADMINISTRATOR', a notification bell, a dropdown for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS', 'Reports', 'Tasks', 'Policies', 'Computer Users', 'Installers', 'Quarantine', 'Exclusions', 'Notifications', 'Status Overview', and a 'Submit Feedback' button. The main content area shows the 'COMPUTERS' view for 'client1.study.local'. The 'LOGS' section is active, displaying a table with columns for 'SysInspector', 'Log Collector', and 'Diagnostic logs'. The table has a 'DATE' header and two entries: '2020 Apr 8 10:52:01' and '2020 Apr 7 23:35:01'. A mouse cursor is hovering over the first entry. At the bottom, there are buttons for 'CLOSE', 'COMPUTER', and 'REQUEST LOG (WINDOWS ONLY)'.

eset CLOUD ADMINISTRATOR

< BACK Computers > client1.study.local

OVERVIEW SysInspector Log Collector Diagnostic logs

CONFIGURATION

LOGS

TASK EXECUTIONS

INSTALLED APPLICATIONS

ALERTS

QUESTIONS

DETECTIONS AND QUARANTINE

DETAILS

2020 Apr 8 10:52:01

2020 Apr 7 23:35:01

CLOSE COMPUTER REQUEST LOG (WINDOWS ONLY)

Автоматична ізоляція ПК у разі виявлення мережевих атак

The screenshot displays the ESET Cloud Administrator interface. The main window is titled "Firewall rules" and contains a sub-dialog box titled "Add rule". The "Add rule" dialog has three tabs: "General", "Local", and "Remote". The "General" tab is active, showing the following configuration:

- Name: 192.168.200.12 block
- Enabled:
- Direction: Both
- Action: Deny
- Protocol: Any
- ICMP Type/Code: 0
- Profile: Any profile
- Logging severity: None
- Notify user:

The background interface shows a sidebar with navigation options: DASHBOARD, COMPUTERS, DETECTIONS, Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, and Status Overview. At the bottom, there are buttons for BACK, CONTINUE, FINISH, and CANCEL.

Автоматична ізоляція ПК у разі виявлення мережесих атак

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'CLOUD ADMINISTRATOR', a notification bell, a dropdown for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS', 'Reports', 'Tasks', 'Policies', 'Computer Users', 'Installers', 'Quarantine', 'Exclusions', 'Notifications', 'Status Overview', and a 'Submit Feedback' button. The main content area is titled 'Computers > client1.study.local' and shows a navigation pane with 'OVERVIEW', 'CONFIGURATION', 'LOGS', 'TASK EXECUTIONS', 'INSTALLED APPLICATIONS', 'ALERTS', 'QUESTIONS', 'DETECTIONS AND QUARANTINE', and 'DETAILS'. The 'CONFIGURATION' tab is active, displaying a table of applied policies. The table has columns for 'POLICY ORDER', 'POLICY PRODUCT', 'POLICY NAME', 'POLICY DESCRIPTION', 'STATUS', 'PARENT NAME', and 'PARENT'. Two policies are listed: 'ESET Management Agent' (order 2) and 'ESET Endpoint for Windows' (order 3). A mouse cursor is hovering over the 'ESET Endpoint for Windows' row. At the bottom, there are buttons for 'CLOSE', 'COMPUTER', and 'MANAGE POLICIES'.

POLICY ORDER	POLICY PRODUCT	POLICY NAME	POLICY DESCRIPTION	STATUS	PARENT NAME	PARENT
2	ESET Management Agent	Agent (soft)		Actual	All	Static Gro
3	ESET Endpoint for Windows	192.168.200.12 block		Actual	client1.study.local	Computer

Автоматична ізоляція ПК у разі виявлення мережесих атак

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'CLOUD ADMINISTRATOR', a notification bell, a search bar for 'Computer Name', and links for 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with options: DASHBOARD, COMPUTERS, DETECTIONS (highlighted with a red '1'), Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a 'Submit Feedback' button. The main content area shows the 'Computers' view for 'client1.study.local'. Under the 'DETECTIONS AND QUARANTINE' section, the 'DETECTIONS' tab is active. A table lists detected events:

DETECTION TYPE	RESOLVED	COMPUTER NAME	COMPUTER TA	CAUSE
<input checked="" type="checkbox"/> Firewall TCP Port Scanning attack	0/1	client1.study.local		

At the bottom of the interface, there are buttons for 'CLOSE', 'COMPUTER', 'MARK AS RESOLVED' (with a mouse cursor over it), and 'MARK AS NOT RESOLVED'. The 'MARK AS RESOLVED' button is highlighted in blue.

Автоматична ізоляція ПК у разі виявлення мережевих атак

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'CLOUD ADMINISTRATOR', a notification bell, a search bar for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains a menu with 'DASHBOARD', 'COMPUTERS', 'DETECTIONS', 'Reports', 'Tasks', 'Policies', 'Computer Users', 'Installers', 'Quarantine', 'Exclusions', 'Notifications', 'Status Overview', and a 'Submit Feedback' button. The main area is titled 'Tasks' and features a search bar with 'End computer isolat... (1)', a 'Tags...' dropdown, 'ADD FILTER', and 'PRESETS' buttons. Below this is a table with columns 'NAME', 'TAGS', 'STATUS', and 'TYPE'. A table row is visible with 'End PC isolation' and 'End computer isolation from network'. A context menu is open over this row, listing actions: 'Client Tasks', 'Show Details', 'Tags...', 'Edit...', 'Duplicate...', 'Run on...', 'Rerun on failed', 'Delete', and 'Executions'. The 'Run on...' option is highlighted. At the bottom, there is a 'Tags' section with a search bar containing 'webinar', and a footer with 'COLLAPSE', 'NEW...', 'ACTIONS', and navigation icons.

eset CLOUD ADMINISTRATOR

Computer Name QUICK LINKS HELP ТЕХПІДТРИМКА УКРАЇНИ LOGOUT

DASHBOARD COMPUTERS DETECTIONS Reports Tasks Policies Computer Users Installers Quarantine Exclusions Notifications Status Overview Submit Feedback

Tasks

Task Types

Client Tasks

ESET Security Product

- Diagnostics
- End computer isolation from network
- Export Managed Products Configuration
- Isolate computer from network
- Modules Update
- Modules Update Rollback
- On-Demand Scan
- Product Activation
- Quarantine Management
- Run SysInspector Script
- Server Scan
- Software Install
- SysInspector Log Request (Windows only)
- Upload Quarantined File

ESET Cloud Administrator

Operating System

Tags

webinar

NEW... ACTIONS

NAME	TAGS	STATUS	TYPE
End PC isolation			End computer isolation from network

- Client Tasks
 - Show Details
 - Tags...
 - Edit...
 - Duplicate...
 - Run on...
 - Rerun on failed
 - Delete
 - Executions

Автоматична ізоляція ПК у разі виявлення мережових атак

The screenshot displays the ESET Cloud Administrator interface. The top navigation bar includes the ESET logo, 'eset CLOUD ADMINISTRATOR', a notification bell, a dropdown for 'Computer Name', 'QUICK LINKS', 'HELP', 'ТЕХПІДТРИМКА УКРАЇНИ', and 'LOGOUT'. The left sidebar contains navigation options: DASHBOARD, COMPUTERS (highlighted), DETECTIONS, Reports, Tasks, Policies, Computer Users, Installers, Quarantine, Exclusions, Notifications, Status Overview, and a 'Submit Feedback' button. The main content area is titled 'Computers' and features a search bar, 'SHOW SUBGROUPS' (checked), 'All (6)', a 'Tags...' dropdown, 'ADD FILTER', and 'PRESETS'. Below this is a table of computers with columns: Groups, COMPUTER NAME, STATUS, MODULES, LAST CONNECTED, ALER, and a settings icon. The table lists six computers under the 'All (6)' group. At the bottom, there are buttons for 'ADD COMPUTER', 'ACTIONS', and 'MUTE', along with a pagination control showing '1'.

Groups	COMPUTER NAME	STATUS	MODULES	LAST CONNECTED	ALER	
CUSTOM GROUPS						
^ All (6)						
Lost & found (6)						
DYNAMIC GROUPS						
Windows computers						
Windows (desktops)						
Windows (servers)						
Linux computers						
Mac computers						
Computers with outdated modules						
Computers with outdated operating system						
Problematic computers						
Not activated security product						
No manageable security product						

Рішення ESET з управлінням на основі хмарних технологій



**Комплексний захист
робочих станцій та файлових серверів**



**Комплексний захист
робочих станцій, файлових та
поштових серверів**



Головна



Популярне



Підписки



Бібліотека



ESET in Ukraine

Підписалося 160 користувачів

ВИ ПІДПИСАЛИСЯ



ГОЛОВНА

ВІДЕО

СПИСКИ ВІДТВОРЕННЯ

КАНАЛИ

ОБГОВОРЕННЯ

ПРО КАНАЛ



Минулі прями трансляції ▶ ВІДТВОРИТИ ВСЕ



Шифрування конфіденційних даних: як...

204 перегляди • Трансляція відбулася 1 день

Віддалений режим роботи: як захистити конфіденцій...

318 переглядів • Трансляція відбулася 6 днів

Багатофакторна аутентифікація -...

517 переглядів • Трансляція відбулася 1

Відео про налаштування рішень ESET



Перехід на ESET Security Management Center 7

ESET in Ukraine • Оновлено сьогодні

Оновлення ERA 6.X Server до ESMC 7.0 Server • 8:03

Міграція клієнтів з ERA 6.5 Server на ESMC 7.0 Server (інша IP-адреса) • 19:24

[ПЕРЕГЛЯНУТИ ВЕСЬ СПИСОК ВІДТВОРЕННЯ \(2 ВІДЕО\)](#)

Завантаження ▶ ВІДТВОРИТИ ВСЕ





Дякуємо за увагу!

