



Управление филиальной сетью, контроль доступа пользователей, защита рабочих станций и мобильных устройств при помощи решений и продуктов компании Fortinet.



SENETSY

FortiManager



- ❑ Минимизирует как первоначальные затраты, так и текущие операционные расходы
- ❑ Централизованное распределение обновлений с помощью локального кеш-сервера FortiGuard
- ❑ Централизация управления устройствами для продуктов Fortinet
 - Конфигурирование устройств (Device provisioning)
 - Мониторинг
 - Логирование и отчетность

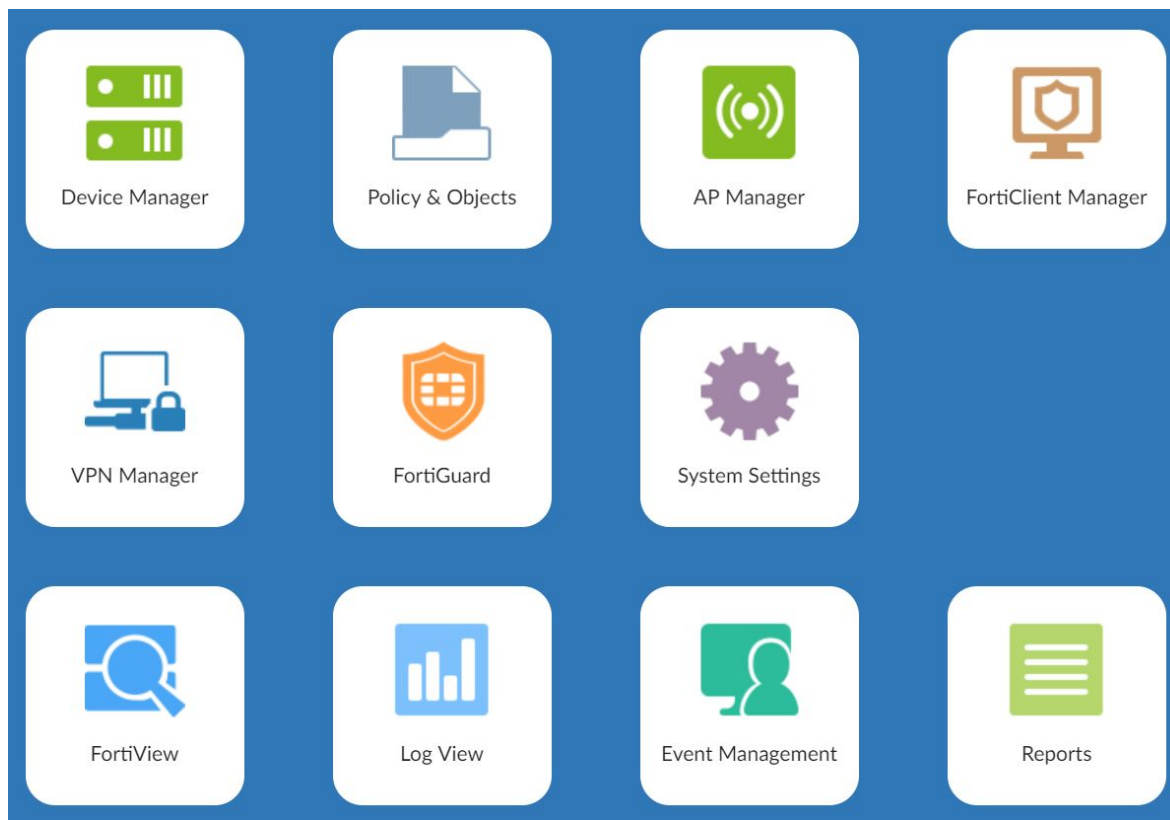


- ❑ Минимизирует как первоначальные затраты, так и текущие операционные расходы
- ❑ Централизованное распределение обновлений с помощью локального кеш-сервера FortiGuard
- ❑ Централизация управления устройствами для продуктов Fortinet
 - Конфигурирование устройств (Device provisioning)
 - Мониторинг
 - Логирование и отчетность



Функции
управления

Функции
логирования и
отчетности





Policy & Objects ▾ Policy Packages Object Configurations admin ▾ 1

Policy Package ▾ Install ▾ ADOM Revisions Tools ▾ Collapse All

Search... Create New ▾ Edit ▾ Delete ▾ Section ▾ Column Settings ▾ Interface Pair View By Sequence

default
Офисы
 Большие офисы
 IPv4 Policy
 Installation Targets
 Маленькие офисы
 IPv4 Policy
 Installation Targets

Seq.#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles
▼ Доступ администраторов (Policy 1 / Total 1)										
1	ADMIN_ACCESS	LAN_Zone	any	all	all	always	ALL	ADMIN_USERS	Accept	all_default
▼ Доступ к серверам (Policy 2 / Total 1)										
2	Mail	LAN	DMZ_Zone	LAN	all	always	SMTP SMTPS	ALL_USERS	Accept	default block-high-risk high_security default
▼ Доступ к внешним ресурсам (Policy 3 / Total 1)										
3	Internet	LAN	WAN	LAN	all	always	ALL	ALL_USERS	Accept	default monitor-all block-botnet deep-inspection default
▼ Implicit (Policy 7 / Total 1)										
7	Implicit Deny	any	any	all	all	always	ALL		Deny	



Install ▾ | ADOM Revisions | Tools ▾ | Collapse All

Revision Diffs Between 2 and Current DB

Summary

Global Policy

Two revisions have no difference on policy package.

Policy Package - Added (2) Changed (1) Deleted (2)

Type	Policy Package	Update Time	User	
Added	Офисы/Большие офисы	2017-9-30 19:44:24	admin	[Details]
Added	Офисы/Маленькие офисы	2017-9-30 20:21:20	admin	[Details]
Changed	default	2017-9-30 20:18:01	admin	[Details]
Deleted	Офисы/Большой Офис	2017-9-30 19:44:24	admin	[Details]
Deleted	Офисы/Малый офис	2017-9-30 19:43:35	admin	[Details]

Download | Close



Policy & Objects ▾

Policy Packages

Object Configurations

ADOM Revisions Tools ▾

Zone/Interface ▾

+ Create New ▾

Edit

Delete

Column Settings ▾

More ▾

Interface



Interface

Default Mapping

Per-Device Mapping

Firewall Objects >



▼ Interface (14)

Security Profiles >



DMZ

> 0 out of 1

User & Device >



LAN

Port3

> 0 out of 1

Dynamic Object >



WAN

Port1

> 0 out of 1

Advanced >



port1

> 1 out of 1

CLI Only Objects >



port10

> 1 out of 1



port2

> 1 out of 1



port3

> 1 out of 1



port4

> 1 out of 1



port5

> 1 out of 1



port6

> 1 out of 1



port7

> 1 out of 1



port8

> 1 out of 1



port9

> 1 out of 1



ssl.root

> 1 out of 1



▼ Zone (3)



DMZ_Zone

DMZ

> 0 out of 1



LAN_Zone

port1, port10, LAN

> 0 out of 1



WAN_Zone

port2, WAN

> 0 out of 1



VPN Manager ▾ IPsec VPN SSL VPN

VPN Community ▾ Install Wizard

All VPN Communities

- ☒ Full-mesh
- ☐ Monitor

+ Create New Edit Delete Column Settings ▾

☒	Seq.#	Name	Gateways	Authentication
☒	1	☒ Full-mesh	1 Gateway Test[root]	Pre-shared Key

VPN Manager ▾ IPsec VPN SSL VPN

+ Add SSL VPN Install Wizard

SSL VPN

+ Create New Edit Delete

☐	Device	Interface	Port	Certificate
☐	Test	any	443	Fortinet_SSL



SENETSY

SSL VPN



FortiGate VM64 FGVM010000108838

Dashboard

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Templates

SSL-VPN Portals

SSL-VPN Settings

User & Device

WiFi & Switch Controller

Log & Report

Monitor

Edit SSL-VPN Portal

Name

Limit Users to One SSL-VPN Connection at a Time ☒

☒ **Tunnel Mode**

Enable Split Tunneling ☐

Source IP Pools

Tunnel Mode Client Options

Allow client to save password ☐

Allow client to connect automatically ☐

Allow client to keep connections alive ☐

☒ **Enable Web Mode**

Portal Message

Theme

Show Session Information ☒

Show Connection Launcher ☒

Show Login History ☒

User Bookmarks ☒

Predefined Bookmarks

+ Create New

Edit

Delete

Name	Type	Location	Description
No matching entries found			



FortiGate VM64 FGVM010000108838

Dashboard

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Templates

SSL-VPN Portals

SSL-VPN Settings

User & Device

WiFi & Switch Controller

Log & Report

Monitor

SSL-VPN Settings

Connection Settings ⓘ

Listen on Interface(s)

port10

Listen on Port

4433

Web mode access will be listening at <https://172.19.0.7:4433>

Restrict Access

Allow access from any host

Limit access to specific hosts

Idle Logout



Server Certificate

Fortinet_Factory



You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.

[Click here to learn more](#)Require Client Certificate ☐

Tunnel Mode Client Settings ⓘ

Address Range

Automatically assign addresses

Specify custom IP ranges

IP Ranges

SSLVPN_TUNNEL_ADDR1

DNS Server

Same as client system DNS

Specify

Specify WINS Servers



Allow Endpoint Registration



Authentication/Portal Mapping ⓘ

+ Create New

Edit

Delete

Users/Groups

Portal

All Other Users/Groups

full-access



00:00:09 0 B ↓ 0 B ↑

SSL Портал

 Download FortiClient ▾

Your Bookmarks



FortiGate

 Quick Connection New Bookmark

History

Oct 1, 2017 12:29:17 AM	172.17.7.32	5 minute(s) and 5 second(s)	0 B in / 0 B out
Oct 1, 2017 12:01:56 AM	172.17.7.32	5 minute(s) and 1 second(s)	0 B in / 0 B out
Sep 30, 2017 11:16:10 PM	172.17.7.32	30 minute(s) and 32 second(s)	2.08 MB in / 56.67 MB out
Sep 30, 2017 11:05:36 PM	172.17.7.32	9 minute(s) and 8 second(s)	0 B in / 0 B out
Sep 30, 2017 10:56:18 PM	172.17.7.32	2 minute(s) and 32 second(s)	0 B in / 0 B out



00:03:09 0 B ↓ 0 B ↑

< New Bookmark



HTTP/HTTPS



FTP

SMB/CIFS



RDP

VNC

Citrix



SSH

Telnet

Port Forward

Name

Folder

SSO

Disabled

Automatic

SSO Credentials

SSL-VPN Login

Alternative

Description

Save

Cancel



SENETSY

FortiClient



Аудит и анализ

Телеметрия



Соответствие требованиям (Compliance)



Аудит и исправление уязвимостей



Безопасность и VPN

Антивирус



Web фильтр



МСЭ для приложений



IP Sec VPN



SSL VPN



Расширенная защита от угроз



Аутентификация и логирование

Централизованное логирование



Windows AD SSO Agent





	FORTICLIENT EMS LICENSE	FORTIGATE ENDPOINT LICENSE
Развертывание		
Централизованное развертывание	✓	
Интеграция с Microsoft AD	✓	
Обновление установленных клиентов	✓	
Соответствие требованиям		
Соответствие требованиям		✓
Исправление нарушений требований		✓
Авторизация доступа в сеть		✓
Удаленное управление		
Антивирусная проверка по запросу	✓	
Проверка уязвимостей по запросу	✓	
Карантин	✓	✓



FortiGate VM64 FGVM010000108838

Dashboard

FortiView

Network

System

Policy & Objects

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

Cloud Access Security Inspection

Intrusion Protection

FortiClient Profiles

Proxy Options

SSL/SSH Inspection

Web Rating Overrides

Web Profile Overrides

VPN

User & Device

WiFi & Switch Controller

Log & Report

Monitor

Edit FortiClient Profile

Profile Name

Comments 0/255

FortiClient endpoint compliance

Non-compliance action

Settings below control which features must be enabled for an endpoint to be considered compliant. Unselected options will be ignored when evaluating endpoint compliance. Non-compliant endpoints will have their configuration updated to comply with these settings.

Endpoint Vulnerability Scan on Client

Vulnerability quarantine level

System compliance

Minimum FortiClient version ☐

Upload Logs to FortiAnalyzer ☒ Traffic ☒ Vulnerability ☒ Event

AntiVirus

Realtime Protection ☒

Up-to-date signatures ☒

Scan with FortiSandbox ☒

Third party AntiVirus on Windows ☒

Web Filter

Application Firewall

Application Control sensor

Apply

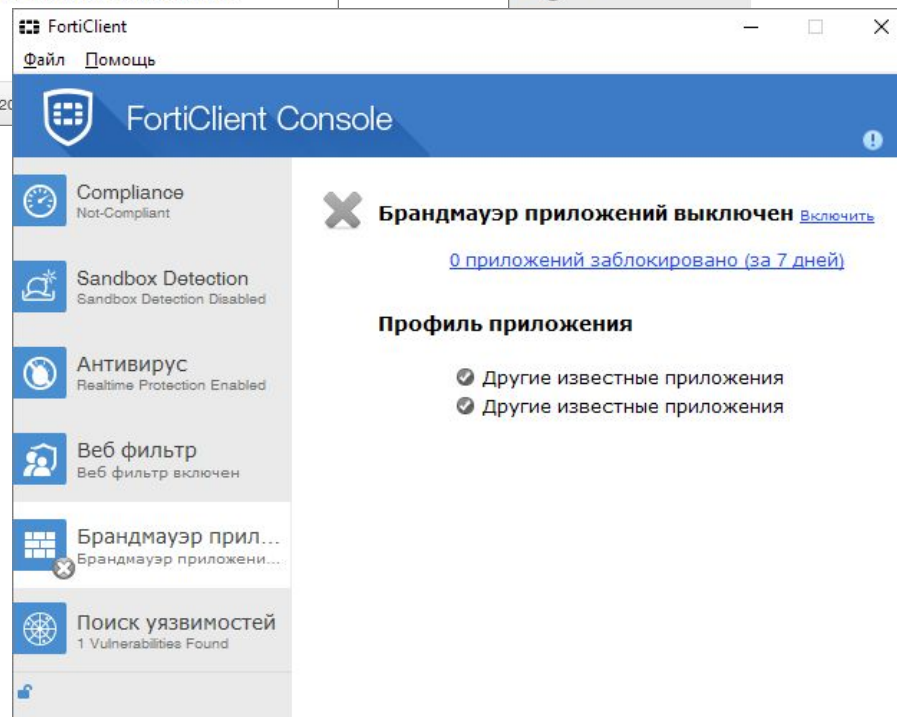
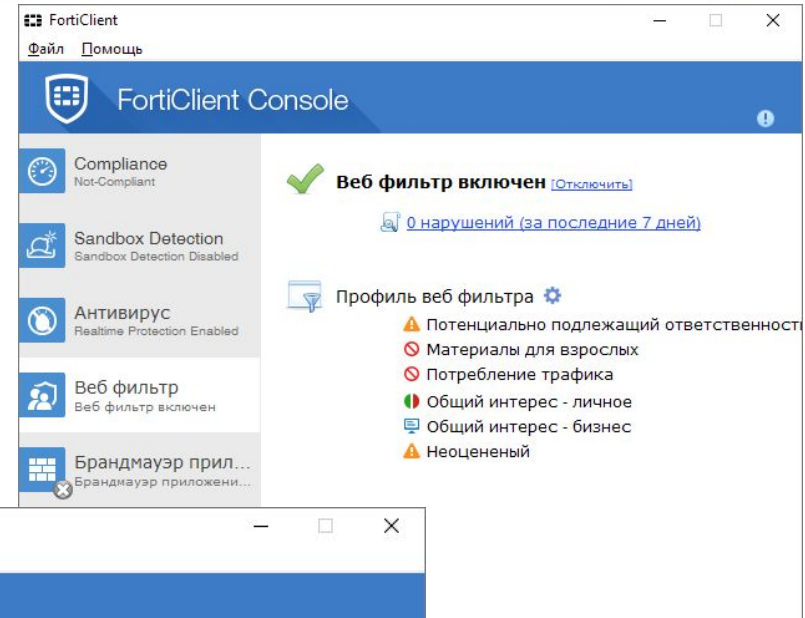
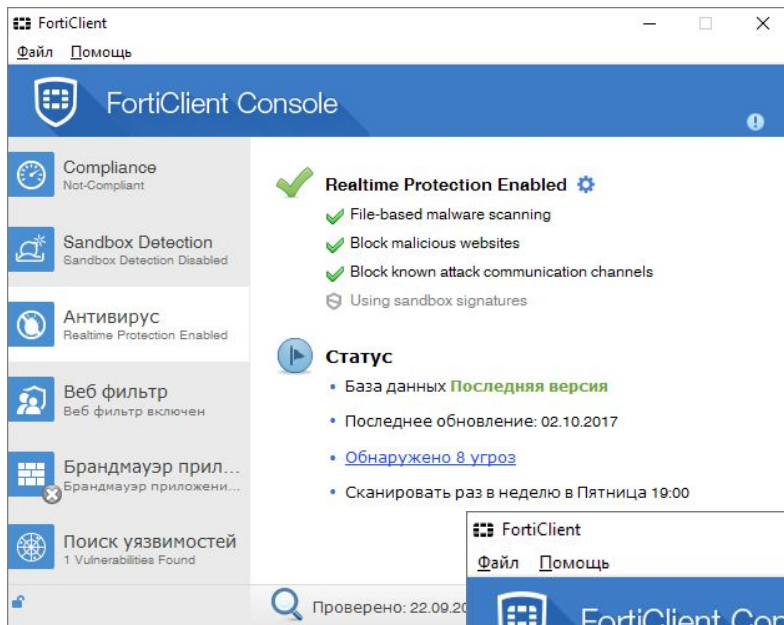
03.10.2017



The screenshot displays the FortiClient console interface. On the left, a sidebar lists various security features: Compliance (Not-Compliant), Sandbox Detection (Sandbox Detection Disabled), Антивирус (Realtime Protection Enabled), Веб фильтр (Веб фильтр включен), Брандмауэр прил... (Брандмауэр приложени...), and Поиск уязвимостей (1 Vulnerabilities Found). The main area shows a red 'X' icon indicating non-compliance with FGVM010000108838 (172.19.0.7). A red arrow points from the 'Show Compliance Rules From FGVM010000108838' link to a secondary window titled 'Compliance Rules From FortiGate'. This window lists the required configurations for network access:

- Антивирус**
 - Antivirus should be enabled
 - Realtime protection should be enabled
 - FortiClient Signatures are up-to-date
- Брандмауэр приложений**
 - Firewall Protection should be enabled
- Поиск уязвимостей**
 - Vulnerability Scan should be enabled
 - Endpoint should not have any High or Above Vulnerabilities
- Протоколирование**
 - Remote logging to FortiAnalyzer should be enabled

A final note states: 'Configuration that need to be corrected to gain compliance. Contact network administrator for details.' A 'Заккрыть' (Close) button is at the bottom right.





The screenshot displays the FortiClient console interface. On the left, a sidebar lists various security features: Compliance (Not-Compliant), Sandbox Detection (Disabled), Антивирус (Realtime Protection Enabled), Веб фильтр (Enabled), Брандмауэр прил... (Disabled), and Поиск уязвимостей (1 Vulnerability Found). The main panel shows the 'Поиск уязвимостей' (Vulnerability Scan) section, indicating that the scan is enabled and the database is up to date. A red arrow points from the 'Обнаружены уязвимости: 1' (1 vulnerability found) notification to a table of detected vulnerabilities.

The table lists the following vulnerability:

Название уязвимости	Суровость	Детали	Patch Status
Security vulnerabilities fixed in Firefox 55	5		Unpatched

A second red arrow points from the 'Детали' (Details) column to a detailed view window for the vulnerability.

The detailed view window, titled 'Security vulnerabilities fixed in Firefox 55', provides the following information:

- Recommended Action:** Download and install patches as instructed
- Описание:** Security vulnerabilities fixed in Firefox 55 vulnerabilities exist in Firefox.
- Released:** August 8 2017
- Суровость:** 5 Критический
- Affected Products:** Firefox
- The fix for this vulnerability must be manually installed from:**
 - <https://www.mozilla.org/en-US/firefox/>
 - <https://www.mozilla.org/en-US/firefox/>
- CVE IDs:**

An 'OK' button is located at the bottom right of the detailed view window.



The image displays two overlapping screenshots of the FortiClient Console interface, illustrating a compliance check process. A red arrow points from the 'Not-Compliant' state in the background window to the 'Compliance' state in the foreground window.

Background Window (Not-Compliant State):

- FortiClient Console** (Title bar)
- Compliance** (Status: Not-Compliant)
- Sandbox Detection** (Status: Sandbox Detection Disabled)
- Антивирус** (Status: Realtime Protection Enabled)
- Веб фильтр** (Status: Веб фильтр включен)
- Брандмауэр прил...** (Status: Брандмауэр приложени...)
- Поиск уязвимостей** (Status: 1 Vulnerabilities Found)
- Message:** This computer is Not-Compliant with **FGVM010000108838 (172.19.0.7)**. [Click to Disconnect](#)
- Links:** [Show Compliance Rules From FGVM010000108838](#), [Show IP List That This FortiClient is Sending Telemetry Data To](#)
- Telemetry:** FortiClient Telemetry: Sent every 66 сек
- Buttons:** Fix Non-compliant Set...
- Footer:** Click on the button above to initiate compliance scan and help gain compliance for network devices

Foreground Window (Compliance State):

- FortiClient Console** (Title bar)
- Compliance** (Status: Compliance)
- Sandbox Detection** (Status: Sandbox Detection Disabled)
- Антивирус** (Status: Realtime Protection Enabled)
- Веб фильтр** (Status: 3 нарушений)
- Брандмауэр прил...** (Status: Брандмауэр приложени...)
- Поиск уязвимостей** (Status: Поиск уязвимостей вклю...)
- Message:** This computer is in Compliance with **FGVM010000108838 (172.19.0.7)**. [Click to Disconnect](#)
- User:** This computer is connected to FGVM010000108838 as **a.kalaev**. [View Details](#)
- Links:** [Show Compliance Rules From FGVM010000108838](#), [Show IP List That This FortiClient is Sending Telemetry Data To](#)
- Telemetry:** FortiClient Telemetry: Sent every 66 сек, next in 9 сек



FortiGate VM64 FGVM010000108838 admin

Block Quarantine Unregister Refresh Search

By Interface By Compliance Status FortiClient Endpoints Tracked 2/10

Device	Address	Status	FortiClient Version	FortiClient Profile	Compliance
port10 (10)					
00:16:c7:26:3b:19		Online			NO FORTICLIENT
00:19:99:9e:93:90		Online			NO FORTICLIENT
00:19:99:9e:93:a0		Online			NO FORTICLIENT
52:54:00:3d:bb:c4		Online			NO FORTICLIENT
80:71:1f:c3:7e:61	172.19.0.65	Online			NO FORTICLIENT
core-sw0.senetsy.lan		Online			NO FORTICLIENT
00:10:db:ff:10:01		Offline			NO FORTICLIENT
WIN-8B42BHMUTLE	172.19.0.12	Offline			NO FORTICLIENT
kalaev a.kalaev	172.17.5.7	Registered - Online	5.6.0	default	✓
DESKTOP-HLUSAK3 (2 interfaces) aleks	172.17.7.32	Registered - Offline	5.6.0	test_client	✓

Routing Monitor
DHCP Monitor
WAN Link Monitor
FortiGuard Quota
IPsec Monitor
SSL-VPN Monitor
Firewall User Monitor
User Quarantine Monitor
FortiClient Monitor
WiFi Client Monitor
Rogue AP Monitor
WiFi Health Monitor

Edit
Show in FortiView
FortiClient
Block
Quarantine
Unregister
Exempt for interface (port10)
Exempt this device (DESKTOP-HLUSAK3)
Exempt all devices of this type (Windows PC)
Edit interface exempt sources



FortiGate VM64 FGVM010000108838 admin

Block Quarantine Unregister Refresh Search

By Interface By Compliance Status FortiClient Endpoints Tracked 2/10

Device	Address	Status	FortiClient Version	FortiClient Profile	Compliance
port10 (10)					
00:16:c7:26:3b:19		Online			NO FORTICLIENT
00:19:99:9e:93:90		Online			NO FORTICLIENT
00:19:99:9e:93:a0		Online			NO FORTICLIENT
52:54:00:3d:bb:c4		Online			NO FORTICLIENT
80:71:1f:c3:7e:61	172.19.0.65	Online			NO FORTICLIENT
core-sw0.senetsy.lan		Online			NO FORTICLIENT
00:10:db:ff:10:01		Offline			NO FORTICLIENT
WIN-8B42BHMUTLE	172.19.0.12	Offline			NO FORTICLIENT
kalaev a.kalaev	172.17.5.7	Registered - Online	5.6.0	default	✓
DESKTOP-HLUSAK3 (2 interfaces) aleks	172.17.7.32	Registered - Offline	5.6.0	test_client	✓

Routing Monitor
DHCP Monitor
WAN Link Monitor
FortiGuard Quota
IPsec Monitor
SSL-VPN Monitor
Firewall User Monitor
User Quarantine Monitor
FortiClient Monitor
WiFi Client Monitor
Rogue AP Monitor
WiFi Health Monitor

Edit
Show in FortiView
FortiClient
Block
Quarantine
Unregister
Exempt for interface (port10)
Exempt this device (DESKTOP-HLUSAK3)
Exempt all devices of this type (Windows PC)
Edit interface exempt sources



FortiClient Enterprise Management Server

Trial | 10 | Enter License

8 View Help admin

Dashboard

Vulnerability Scan

Endpoints

Domains

Test

test.local

Domain Controllers

Workgroups

All Groups

Endpoint Profiles

EMS Profiles

Default

Gateway IP Lists

Fortigate

FortiClient Enterprise Management Server

Auto-refresh Refresh every 10 minutes

System Information

HostnameWIN-8B42BHMUTLE

Serial NumberFCTEMS0576884871

License StatusTrial

Used Licenses1 of 10 Enter License

System Time16:42:30, 10/2/2017

System DatabaseBackup Restore

Current Adminadmin

Uptime1 day, 5 hours, 22 minutes, 46 seconds

Event Summary

Endpoints with Out-of-date Protection0

Endpoints with Out-of-sync Profiles0

Endpoints with Pending Software Updates0

Errors or Warnings (last 7 days)1

Inactive Endpoints (last 30 days)0

Unprotected Clients0

Client Stats

Unmana... Managed Online On-Net

1 1 1 1

FortiGate Managed Endpoints

No Data Found

Installed FortiClient Version Summary - Windows

5.6.0.1075 100%

Installed FortiClient Version Summary - Mac



FortiClient Enterprise Management Server

Trial | 10 | Enter License

8 View Help admin

Dashboard Editing Profile: FGVM010000108838[root|default|Windows]

Vulnerability Scan

Profile Name default

Basic Advanced

Endpoints

Domains

Test

test.local

Domain Controllers

Workgroups

All Groups

Endpoint Profiles

EMS Profiles

Default

FGVM010000108838[ro...

default

default ios

default

Gateway IP Lists

Fortigate

AntiVirus Protection

Real-Time Protection

Scan Files as They Are Downloaded or Copied to My System

On Virus Discovery Deny Access to Infected Files

Alert When Viruses Are Detected

Block Known Communication Channels Used by Attackers

Block All Access to Malicious Websites

Scan Compressed Files

Max Size 10 Mb

0 means unlimited.

User Process Scanning Scan Files When Processes Read or Write T

Scan Network Files

System Process Scanning Scan Files When System Processes Write T

On Demand Scanning

On Virus Discovery Quarantine Infected Files

Integrate FortiClient into Windows Explorer's Context Menu

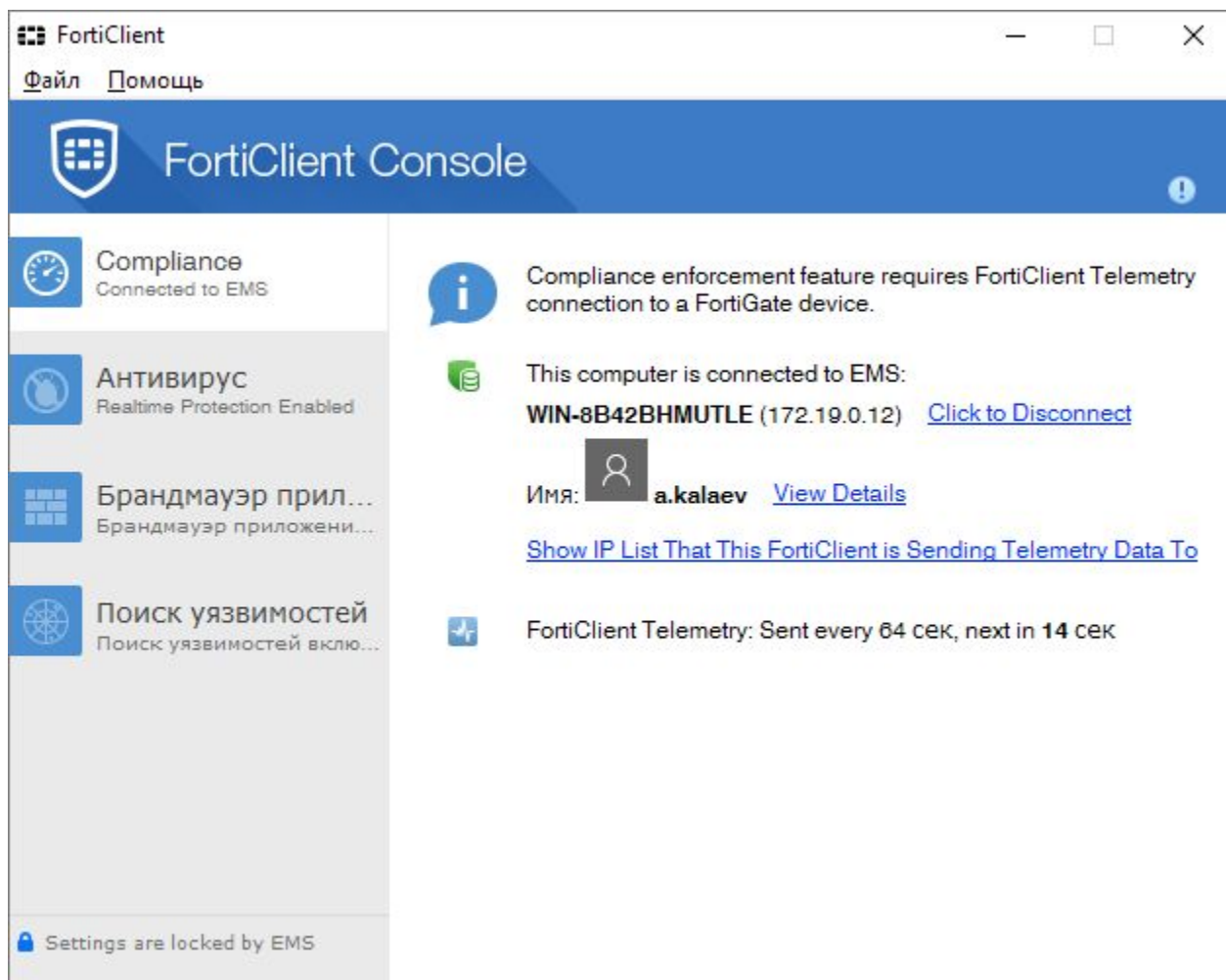
Pause Scanning When Running on Battery Power

Automatically Submit Suspicious Files to FortiGuard for Analysis

Scan Compressed Files

Max Size 0 Mb

Save Profile Discard Changes





SENETSY

Спасибо за внимание