



POLICIA FEDERAL ARGENTINA

Procedimiento Estado Fortinet

**Superintendencia FEDERAL DE TECNOLOGÍAS DE
LA INFORMACIÓN Y COMUNICACIONES**



Estado de Fortinet

EDICIÓN 1
Tipo de Documento:
Monitorio
Versión: 2.0 / 2023
Página 2 de 6

Tabla de contenido

REVISIÓN ESTADO DEL FORTISIEM.....	3
REVISIÓN DE ESTADO DEL SANDBOX	4
VERIFICACIÓN ESTADO EMS:	5
VERIFICAR ESTADO DEL FORTIANALYZER	6



Estado de Fortinet

EDICIÓN 1

Tipo de Documento:

Monitorio

Versión: 2.0 / 2023

Página 3 de 6

Revisión estado del FortiSIEM

Existen tres (03) estados del SIEM:

- **Normal** (verde)
- **Warning** (amarillo, significa que algún servicio / proceso se inició hace menos de 1 hr.)
- **Critical** (rojo, los servicios / procesos están caídos)

Si hace clic sobre el estado (el color) se desplegará los servicios / procesos que están en funcionamiento o no.

- **Admin**
 - **Health** (observará el estado del SIEM)

The screenshot shows the FortiSIEM interface with the 'Health' tab selected under 'Device Support'. At the top, there are summary statistics: 1 Total, 0 No Connection, 1 Critical, 0 Warning, and 0 Normal. Below this, a table lists a single device: 'fortsiem.teleprocesos.cc...'. The 'Health' column for this device is highlighted with a red box and labeled 'Critical'. A red arrow points from this label to a larger, detailed table below titled 'Process health for fortsiem.teleprocesos.ccam.pfa (10.1.78.10)'. This detailed table has columns for Process Name, Owner, Status, Uptime, CPU, Memory, Resident Memory, Disk Read Rate, Disk Write Rate, SharedStore Type, SharedStore Position, and SharedStore Percent. All processes listed are in a 'Down' state, indicated by a red icon in the 'Status' column. A red box highlights the entire 'Status' and 'Uptime' row of the table.

Process Name	Owner	Status	Uptime	CPU	Memory	Resident Memory	Disk Read Rate	Disk Write Rate	SharedStore Type	SharedStore Position	SharedStore Percent
AppServer	admin	Down	1d 48m	7%	20.10%	6.22 GB	0KBps	0KBps	writer	0	0%
phParser		Down	N/A	0%	0%	0 MB	0KBps	0KBps			
phQueryMaster		Down	N/A	0%	0%	0 MB	0KBps	0KBps			
phRuleMaster		Down	N/A	0%	0%	0 MB	0KBps	0KBps			
phRuleWorker		Down	N/A	0%	0%	0 MB	0KBps	0KBps			
phQueryWorker		Down	N/A	0%	0%	0 MB	0KBps	0KBps			
phDataManager		Down	N/A	0%	0%	0 MB	0KBps	0KBps			
phDiscover		Down	N/A	0%	0%	0 MB	0KBps	0KBps			
phReportWorker		Down	N/A	0%	0%	0 MB	0KBps	0KBps			
phReportMaster		Down	N/A	0%	0%	0 MB	0KBps	0KBps			



Estado de Fortinet

EDICIÓN 1

Tipo de Documento:

Monitorio

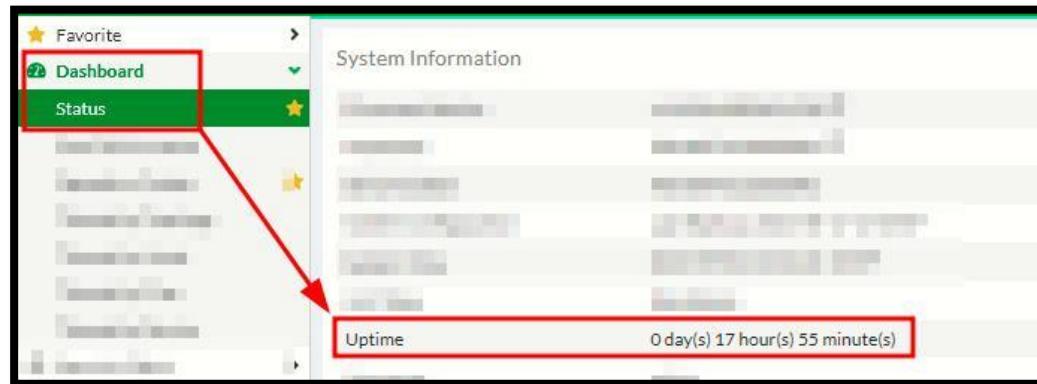
Versión: 2.0 / 2023

Página 4 de 6

Revisión de estado del Sandbox

- 1ro. En el **Dashboard / Status**

- Corroborar el **Uptime** (tiempo encendido) en *System Information*.



- Confirmar **File Scan – Last 24 hours.**



- 2do. En caso de que se haya caído realizar la siguiente comprobación y acción.

- En **Security Fabric / Devices**, hacer clic sobre las cadenas en la columna de *Auth* (autenticación).

Device Name	Serial	Malicious	High	Medium	Low	Clean	Others	Mal Pkg	URL Pkg	Auth
FWB-VM	FWBVMSTM23000365	0	0	0	0	0	0	N/A	N/A	0%
FWB-VM:root	FWBVMSTM23000365	0	0	0	0	0	0	N/A	N/A	0%
FWB-02	FV100ET222000021	0	0	0	0	0	0	N/A	N/A	0%
FWB-01	FV100ET222000008	0	0	0	0	0	0	N/A	N/A	0%
PFA1-FGT-1100E	FG10E0TB22903003	0	0	0	0	29	0	4.123	4.100	0%
PFA1-FGT-1100E:root	FG10E0TB22903003	0	0	0	0	29	0	4.123	4.100	0%
PFA2-FGT-1100E	FG10E0TB22903100	0	0	0	0	0	0	4.123	4.100	0%
PFA2-FGT-1100E:root	FG10E0TB22903100	0	0	0	0	0	0	4.123	4.100	0%
mail	FEVM04TM23000319	0	0	0	7	234...	0	N/A	N/A	0%
mail:policiafederal.g...	FEVM04TM23000319	0	0	0	7	234...	0	N/A	N/A	0%



Estado de Fortinet

EDICIÓN 1

Tipo de Documento:

Monitorio

Versión: 2.0 / 2023

Página 5 de 6

Verificación estado EMS:

- Ingresar a la herramienta, en **Dashboard** ubicarse en **Status**, acto seguido buscar el Widget **System Information**.

The screenshot shows the FortiClient Endpoint Management Server interface. On the left, there's a sidebar with 'Dashboard' and 'Status' buttons, where 'Status' is highlighted with a red box. The main area displays various monitoring panels. A red arrow points from the 'Status' button to the 'System Information' panel on the right. This panel contains system details like Hostname, Version, Database, System Time, Uptime, and Mode. The 'Uptime' section is specifically highlighted with a red box.

- En caso de no tener el mencionado Widget, habilitarlo con el siguiente método.

This screenshot shows the 'Manage Widgets' dialog box overlaid on the dashboard. The 'Status' button in the sidebar is again highlighted with a red box. The dialog lists several widget categories with checkboxes. Under 'Endpoint Activity', 'Endpoint Alerts', 'Endpoint Connection', 'Managed Mac FortiClient Versions', 'Managed Windows FortiClient Versions', 'Managed Linux FortiClient Versions', 'Endpoint Management', 'Mac Operating Systems', 'Windows Operating Systems', 'Linux Operating Systems', 'iPhone Operating Systems', 'Android Operating Systems', and 'FortiGuard Outbreak Detection Service' are listed. Under 'Top 3 Lists', 'Antivirus Detection', 'Sandbox Detection', 'Vulnerability Detection', and 'Web Filter Detection' are checked. Under 'Others', 'System Information' and 'License Information' are checked. A red box highlights the 'System Information' checkbox. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons, with 'Save' also highlighted with a red box.



Estado de Fortinet

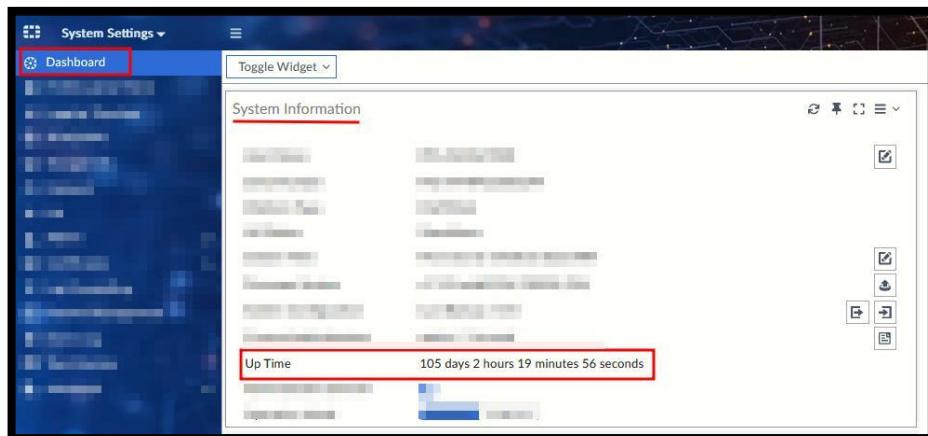
EDICIÓN 1
Tipo de Documento:
Monitorio
Versión: 2.0 / 2023
Página 6 de 6

Verificar estado del FortiAnalyzer

- Ingresando a la herramienta, ingresar a cualquier ADDOM, luego **System Settings**.



- En **System Settings**, diríjase al **Dashboard**, en el Widget System Information busque **Up Time**.



- Preventivamente, haga scroll dentro del **Dashboard** y verifique en el Widget System Resources que el **CPU – Memory Usage – Disk Usage** tengan actividad y se encuentren dentro los valores aceptables de funcionamiento.

