



**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 displays the FortiSIEM Admin interface. The top navigation bar includes 'ADMIN'. The 'Health' section is active, showing a summary of system health: 1 Total, 0 No Connection, 1 Critical, 0 Warning, and 0 Normal. Below this, a table lists system components and their health status. The 'Health' column for the 'fortisiem.teleprocesoos.ccm' component is highlighted in red and labeled 'Critical'. A red box highlights the 'Health' column header, and a red arrow points to the 'Critical' status. Below the main table, a 'Process health for fortisiem.teleprocesoos.ccm.pfe (10.1.78.10)' section is visible, showing a list of processes and their status. The 'Status' column for the 'Admin' process is highlighted in red and labeled 'Up'.

Name	IP Address	HA/DR Role	Health	Last Status Updated	Version	EPS	Load Average	CPU	Memory	Swap	Disk	Max Disk Read Wait	Max Disk Write Wait	Upload Buffer	Content Version	
fortisiem.teleprocesoos.ccm	10.1.78.10	Super	Primary Leader	Critical	Sep 30, 2023, 10:26:11 AM	6.7.7.1756	N/A	0.74,0.76,0.78	4.40%	29%	0%	54%	0	0.20ms	Total: 0 KB Queue: 1	400

Process Name	Owner	Status	Uptime	CPU	Memory	Resident Memory	Disk Read Rate	Disk Write Rate	SharedStore Type	SharedStore Position	SharedStore Percent
Admin	admin	Up	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

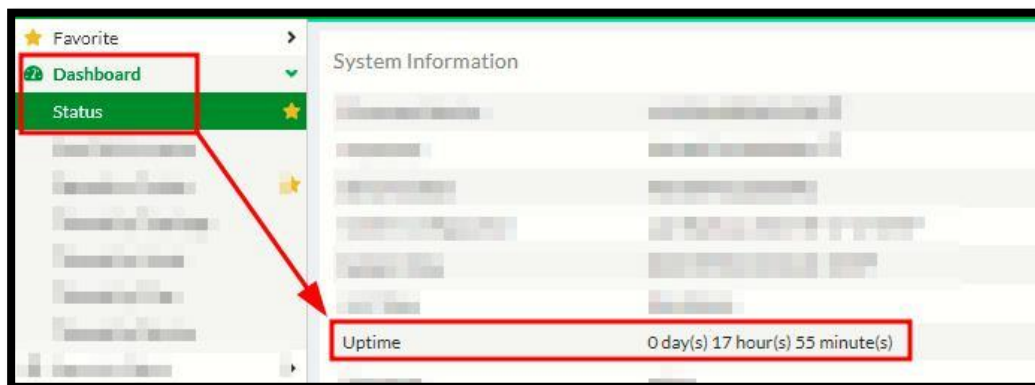
Tipo de Documento:  
Monitorio

Versión: 2.0 / 2023

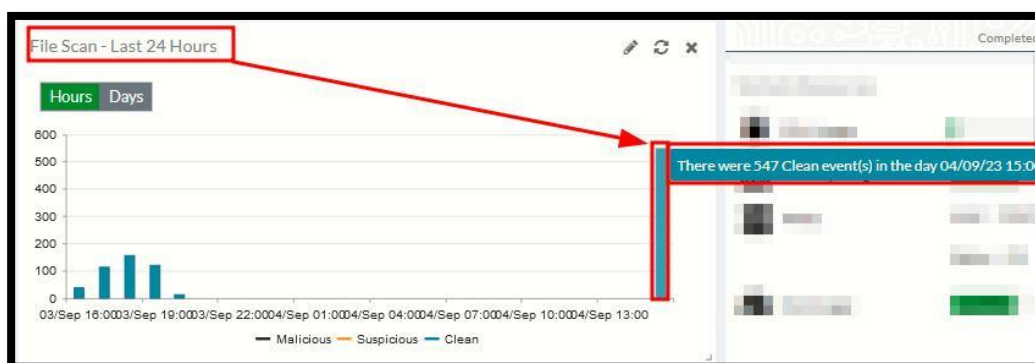
Página 4 de 6

## 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	<a href="#">Auth</a>
FWB-VM:root	FWBVMSTM23000365	0	0	0	0	0	0	N/A	N/A	<a href="#">Auth</a>
FWB-02	FV100ET222000021	0	0	0	0	0	0	N/A	N/A	<a href="#">Auth</a>
FWB-01	FV100ET222000008	0	0	0	0	0	0	N/A	N/A	<a href="#">Auth</a>
PFA1-FGT-1100E	FG10E0TB22903003	0	0	0	0	29	0	4.123	4.100	<a href="#">Auth</a>
PFA1-FGT-1100E:root	FG10E0TB22903003	0	0	0	0	29	0	4.123	4.100	<a href="#">Auth</a>
PFA2-FGT-1100E	FG10E0TB22903100	0	0	0	0	0	0	4.123	4.100	<a href="#">Auth</a>
PFA2-FGT-1100E:root	FG10E0TB22903100	0	0	0	0	0	0	4.123	4.100	<a href="#">Auth</a>
mail	FEVM04TM23000319	0	0	0	7	234...	0	N/A	N/A	<a href="#">Auth</a>
mail:policiafederal.g...	FEVM04TM23000319	0	0	0	7	234...	0	N/A	N/A	<a href="#">Auth</a>



# Estado de Fortinet

EDICIÓN 1

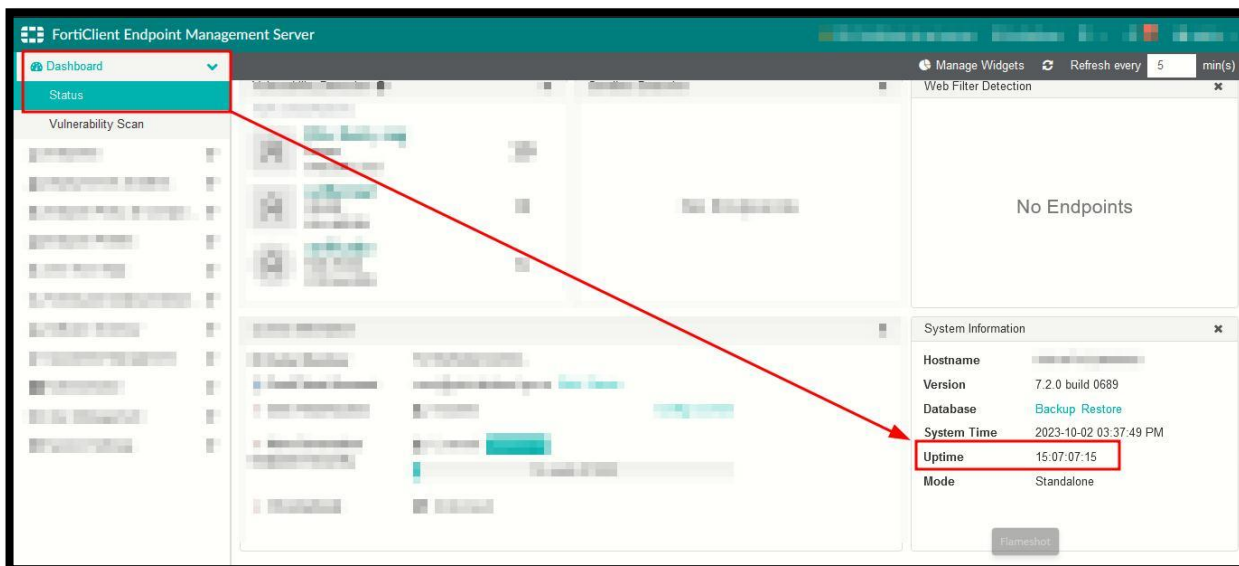
Tipo de Documento:  
Monitorio

Versión: 2.0 / 2023

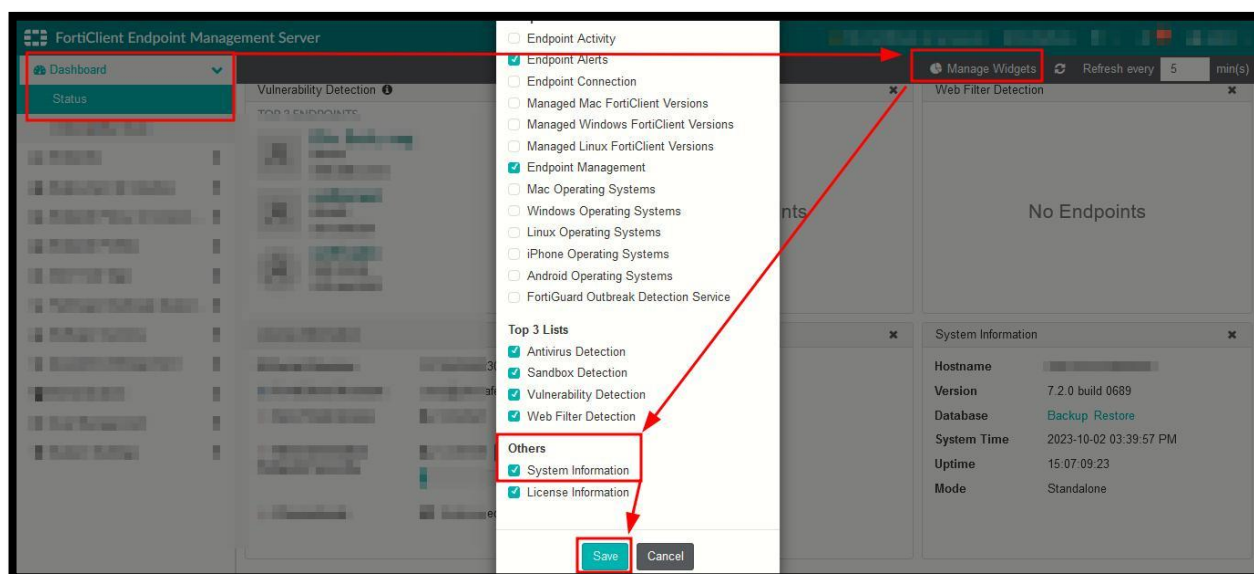
Página 5 de 6

## Verificación estado EMS:

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



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



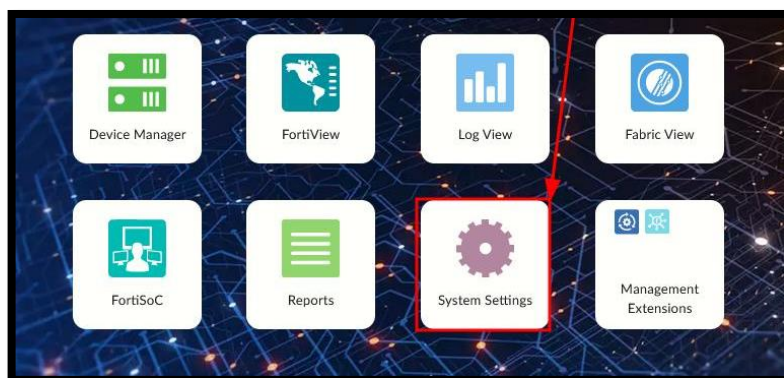


# Estado de Fortinet

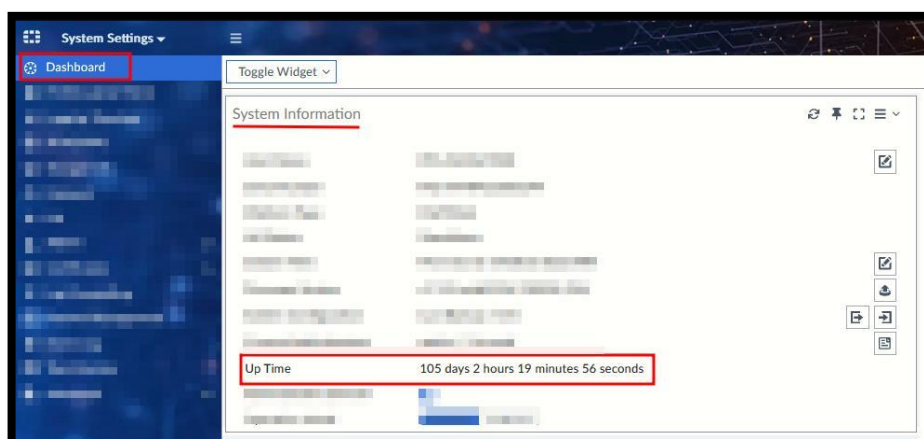
EDICIÓN 1
Tipo de Documento: Monitorio
Versión: 2.0 / 2023
Página 6 de 6

## 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.

