FORTINET | COLOMBIA & ECUADOR

XPERTS26

FortiAI Assist

Qué se puede hacer en cada producto Fortinet y qué prompts ejecutar

PUNTO DE PARTIDA

¿Qué es el FortiAI-Assist?

1 Asistente de IA generativa

Se apoya en los datos de FortiGuard Labs y en modelos entrenados con el conocimiento de producto de Fortinet. El administrador pregunta y pide tareas en lenguaje natural sin salir de la GUI.

2 Responde con datos del equipo

Además de documentación con RAG, consulta en vivo logs, políticas, dispositivos y estado del sistema. Las respuestas incluyen texto, widgets accionables y enlaces a la documentación.

3 Se abre desde el banner

Ícono FortiAI en la barra superior de cualquier página, módulo propio en el árbol de menús y botones dedicados en paneles concretos: Analyze with AI, Explain with AI, Triage Agent.

4 Licencia y tokens

Requiere licencia o suscripción FortiAI válida. El consumo se mide en tokens de entrada y salida; al agotarse la cuota mensual el acceso se suspende hasta el siguiente ciclo.

Tres modelos distintos: La mayoría del portafolio usa el servicio FortiAI de Fortinet con tokens incluidos, y FortiSOC lo consume por un conector ya preconfigurado. FortiSIEM y FortiSOAR se apoyan en OpenAI o Azure OpenAI, y FortiOS deja elegir. En FortiSandbox, "FortiAI" no es un chat sino el appliance usado como método de veredicto.

El acceso al servicio necesita salida directa a internet sin proxy web: fai.fortinet.net en FortiManager y FortiAnalyzer, fortiai.forticloud.com en FortiClient EMS. Al cerrar o recargar la sesión se pierde el hilo salvo en FortiOS y FortiSIEM, que guardan historial y preguntas.

MAPA DEL PORTAFOLIO

Qué forma toma FortiAI en cada producto

FortiOS

8.0.0 · Asistente + CLI Code Lab

Documentación con RAG, análisis de diagnósticos y ejecución de comandos CLI. Elige FortiAI u OpenAI.

FortiManager

8.0.0 · Seis agentes MCP

Agentes que leen el entorno y, con confirmación, ejecutan tareas: políticas, scripts, VPN, provisioning.

FortiAnalyzer

8.0 / 7.6 · Asistente SOC

Incidentes, threat hunting, handlers, FortiView y reportes. Suma Triage Agent y Threat Posture Timeline.

FortiSIEM

7.6.0 · Chat + análisis agéntico

Consultas a CMDB y eventos vía MCP, análisis agéntico de incidentes y ayudante de SQL.

FortiSOAR

8.0.0 · Agentes de IA

AI Agents sobre servidores MCP, contexto organizacional con SOPs, insights y ML clásico.

FortiSOC

26.2.2 · IA embebida en el SOC

Playbooks de IA, enriquecimiento de casos, panel Insight y agente de investigación contextual.

FortiClient EMS

8.0.0 · Asistente (add-on)

Endpoints, perfiles, políticas, tags de postura y vulnerabilidades. Solo super admins.

FortiWeb

8.0.6 · Asistente consultivo

Q&A documental, logs de ataque, reputación de IP, salud del sitio y Lua. No aplica cambios.

FortiADC

8.0.3 · Asistente en Beta

Guía documental, estado de virtual servers, análisis de logs y generación de scripts Lua.

FortiSandbox

4.0.6 · FortiAI como veredicto

No hay chat: el appliance FortiAI actúa de prefiltro antes del escaneo en máquina virtual.

Nueve de los diez comparten el mismo patrón: asistente dentro del producto, consumo medido por tokens, enmascarado de datos y control por perfil de administrador. FortiSandbox es el caso aparte.

Asistente embebido y CLI Code Lab

FortiAI-Assist viene embebido en FortiOS y aporta soporte documental con RAG, análisis automático de diagnósticos y ejecución de scripts CLI. Es el único producto del portafolio donde el administrador elige el proveedor de IA.

F Proveedor FortiAI

- Optimizado y probado por Fortinet, con tokens incluidos.
- RAG sobre el FortiOS Administration Guide y el CLI Reference.
- Responde leyendo logs directamente del FortiGate y analizando el debug que pega el administrador.
- Contrasta sus respuestas contra el equipo para que apliquen al modelo concreto.

O Proveedor OpenAI

- Tokens y facturación directamente con OpenAI; FortiAI no reporta ese consumo.
- Se configura con clave, modelo, project ID y organization ID.
- En CLI: set gui-llm-provider openai dentro de config system admin.
- La GUI sigue llamándose FortiAI aunque el LLM sea de OpenAI.

CLI Code Lab	Genera, edita y ejecuta comandos. Se abre desde el banner (CLI Console > CLI Code Lab) o con el botón Edit sobre los comandos que devuelve el chat; luego Execute y Commit changes.
Modelos y suscripción	Hardware con más de 2 GB de RAM y FortiCare Premium: 2.000.000 de tokens iniciales al mes por equipo. FortiGate-VM serie S: Premium o bundle Enterprise, UTP o ATP. Los modelos con 2 GB o menos no lo soportan.
Permisos	Se controla por perfil de administrador (Allow using AI Assistant / set gui-ai-assistant enable). FortiAI llama a las REST API de FortiOS con los mismos permisos del admin conectado.
Historial y ajustes	Lista de chats anteriores, control del largo de Message history que se reenvía como contexto, exportación de chat o thread a JSON y conmutador de enmascarado de datos.

FortiOS 8.0.0 Administration Guide — "FortiAI assistant and CLI Code Lab", págs. 90-101 y "Access to FortiAI", pág. 3946.

Diagnosticar y configurar el FortiGate desde el chat

Ejemplo 1 · Troubleshooting con FortiAI

```
troubleshoot issue ipsec vpn tunnel
  to-headoffice is down
```

- FortiAI devuelve los comandos para recoger el debug de IKE y varias soluciones posibles.
- El administrador ejecuta el debug en SSH y pega la salida en el chat.
- FortiAI analiza el log y ordena las causas de más a menos probable: en el ejemplo, fallo de autenticación IKEv2 por PSK que no coincide.

Ejemplo 2 · Configuración con OpenAI

```
configure this fgt to block social media
  by webfilter
lan interface port2. wan interface port1.
  update existing policy 1 instead of
  creating a new one
```

- Devuelve el perfil de web filter y la política; con el segundo prompt afina el resultado a las interfaces y a la política existente.
- Con Edit se abre CLI Code Lab, se ajusta el código, se ejecuta y se confirman los cambios.

Otros prompts documentados y buenas prácticas de FortiOS

```
Create firewall addresses for 10.0.0.1 and awesome-domain.com
quarantine device
```

- Prompts cortos: "Create firewall addresses for 10.0.0.1 and awesome-domain.com" rinde más que la versión larga y educada.
- Usa verbos que existen en FortiOS, como "quarantine device", para que el asistente sepa qué acción ejecutar.
- Encadena dentro del hilo, pero recuerda que no conserva hilos anteriores.
- Acepta imágenes: se puede pedir una VPN site-to-site a partir de una topología cargada en el chat.

La ejecución de comandos siempre pasa por CLI Code Lab con confirmación y commit explícitos del administrador.

Seis agentes especializados sobre MCP

FortiAI en FortiManager usa Model Context Protocol para exponer el contexto y las acciones administrativas del equipo. El agente se elige en el desplegable antes del prompt: esa selección guía cómo interpreta la petición y qué funciones puede usar.

1 General

Preguntas de producto, comparación de funciones y especificaciones, navegación a páginas de la GUI y búsqueda de documentación.

2 Device Management

Salud, licencias, firmware, readiness de upgrade y riesgos. Explica en lenguaje llano qué cambió y con qué comandos CLI.

3 Firewall Policy

Buscar, inspeccionar, crear, editar, clonar, comparar versiones y hacer rollback de políticas y objetos.

4 CLI y Jinja Script

Convierte la intención en scripts CLI o Jinja para FortiGate y FortiManager, y explica scripts existentes.

5 VPN y SD-WAN Diagnostic

Diagnostica túneles, SD-WAN, rendimiento y equipos: analiza síntomas y guía la causa raíz paso a paso.

6 Provisioning Template

Overlays SD-WAN, plantillas de BGP, IPsec y sistema, onboarding de equipos y control de conflictos antes de aplicar.

Los agentes trabajan solos en su dominio o en equipo para problemas más complejos. Ninguna mutación de datos se aplica sin confirmación explícita del administrador.

FortiManager 8.0.0 Administration Guide, capítulo FortiAI, y AI Transparency Notes de FortiAI on FortiManager 1.1. La licencia permite hasta tres administradores locales en todas las plataformas.

Qué pedirle a los agentes General, Device y Policy

1 General Agent

```
Can you take me to the Device Manager page?
What is an ADOM?
How can I setup an HA Cluster in the GUI or CLI?
How can I create a read-only user with restricted permission?
```

2 Device Management Agent

```
Which devices need my attention?
Show me the last 5 configuration revisions of <device>.
Show me the last 10 tasks for <device>.
Find the device that has an interface IP equal to <IP>.
```

3 Firewall Policy Agent

```
Which policies match the traffic from <IP address>?
Can <IP A> access <IP B> using HTTPS?
Show me policies never hit in the last 30 days.
Show me the policy package changes since the last installation.
```

También documentado en el Firewall Policy Agent: "Turn on SSL deep inspection for policies."

Scripting, diagnóstico de red y provisioning

4 CLI Script Agent

```
Help me write a CLI script.
Help me write a Jinja CLI script.
```

```
What predefined variables can be used in FortiManager Jinja scripts?
Create a firewall address of <IP address> and <domain>.
```

5 VPN / SD-WAN Troubleshooting Agent

```
Help me diagnose why my VPN tunnel has issues.
Check why it is slow to access <online-service> from <asset-IP>.
```

```
Why is the network slow from <asset-IP> to <other-asset-IP>?
Diagnose the SD-WAN network from <asset-IP> to YouTube.
```

6 Provisioning Agent

```
Create a new SD-WAN overlay.
Onboard new devices to an SD-WAN overlay template.
```

```
Help me extract a template using a device configuration.
Create a new VPN tunnel between two devices.
```

FortiAI acepta imágenes de topología como entrada: "Help me configure an SD-WAN overlay based on a network diagram" y "Generate a network diagram based on an explained SD-WAN topology".

Los siete flujos documentados de punta a punta

1	**Análisis de dispositivos IoT**	Prerequisite check, inventario, gráfico de torta, reporte y cuarentena por dirección MAC.
2	**Creación de scripts**	De la intención al script CLI o Jinja, guardado como script o plantilla si el rol lo permite.
3	**VPN site-to-site**	Configuración guiada del túnel entre dos equipos.
4	**Verificación y diagnóstico del túnel**	Chequeo de estado y diagnóstico paso a paso del IPsec.
5	**Overlay SD-WAN**	Diseño del overlay a partir de la topología descrita o de un diagrama cargado.
6	**Alta de equipos en VPN existentes**	Onboarding de nuevos FortiGate a redes VPN ya desplegadas.
7	**Lentitud de acceso a aplicaciones**	Diagnóstico, troubleshooting y remediación de acceso lento a nube u on-premise.

El RBAC va por capas: interruptor global con set ai-mode enable, acceso por administrador y alcance según el perfil. Fuente: FortiManager 8.0.0 Administration Guide, capítulo FortiAI.

El asistente para el SOC: detectar, investigar, responder

FortiAI se usa en FortiAnalyzer para investigación de incidentes, respuesta y threat hunting: interpreta eventos, genera resúmenes, identifica impacto y recomienda remediación. También crea consultas complejas a la base de datos, reportes y reglas de correlación desde lenguaje natural.

1 Detección

Crea alert handlers y event handlers desde cualquier panel de la GUI, con reglas ajustadas al entorno y apoyadas en la base SIEM. Aplica filtros al Event Monitor, por ejemplo por severidad crítica.

2 Investigación

Filtra Log View y FortiView con callbacks que aceptan filtros y ordenamiento, entrega datos de primer nivel y drill down, investiga por hash de archivo y lista incidentes y hosts comprometidos.

3 Respuesta

Chequeos de reputación de IPs, dominios y URLs con FortiGuard y VirusTotal, recopilación de procesos del endpoint, cuarentena por IP y recomendaciones de mitigación.

4 Conocimiento y reportes

Responde preguntas de producto con RAG y cita al final de cada respuesta la documentación de origen. Renderiza gráficos desde Log View y genera reportes de incidente descargables.

Fuera del chat: Triage Agent en el detalle de la alerta · FortiAI Threat Posture Timeline en Asset Identity Center, que consolida logs UTM, alertas e incidentes de FortiGate, FortiClient, FortiMail y FortiAuthenticator · El micrófono permite preguntar en otros idiomas y el asistente responde en el mismo.

Prompts para arrancar una investigación

Reconocimiento y análisis

```
Can you provide a summary of the latest
  security incidents detected?
Could you assist in identifying any anomalies
  in our network traffic?
Is there any unusual behavior observed from
  specific user accounts?
Is there any unusual outbound network traffic
  that could indicate data exfiltration?
Show the top threats in the last week.
```

Acciones sobre el entorno

```
Summarize alerts related to IP 1.1.1.1.
Create event handler for threat 'W32/Farfli.CM!tr'.
Keep me updated with same log happening again.
Generate a report for top 5 file hashes from
  the last 7 days.
Run a security reputation check for <IP>.
Quarantine endpoint <IP>.
Generate an incident report for incident <id>.
How much YouTube did <IP> watch today?
```

Prompts que NO funcionan bien

`"How many attacks will I receive tomorrow based on past trends?"` — obliga a FortiAI a suponer. Mejor pedir análisis de la tendencia actual y luego los pasos de mitigación.

`"Give me a report of PCI compliance for my infrastructure."` — demasiado vago: pedirá aclaraciones y consumirá tokens de más. Mejor acotar logs, equipos y ventana de tiempo.

La licencia habilita FortiAI para un máximo de tres administradores locales; no está disponible en el supervisor de un FortiAnalyzer Fabric.

Consultar el SIEM en lenguaje natural y analizar con agentes

El módulo phGenerativeAI conecta la base PostgreSQL y la base ClickHouse mediante MCP, una VectorDB interna y el LLM de OpenAI. El administrador pregunta en inglés y puede encadenar preguntas de seguimiento para profundizar en la respuesta.

1 FortiAI Chat

Siete familias de preguntas: documentación, CMDB, recolección de datos, incidentes, threat hunting, actividad de usuario y vulnerabilidades. Preguntas predefinidas y propias, que se pueden guardar en carpetas.

2 Incident Analysis agéntico

FortiAI arma un plan de pasos, genera el SQL de cada paso, encadena la salida de uno como entrada del siguiente y concluye si el incidente es falso positivo o real, con causa raíz.

3 Case y Log Analysis

Análisis básico no agéntico del caso, con la opción de añadir la respuesta a las notas. Un log crudo se analiza desde Analytics > Search con Action > FortiAI > Analyze Raw Message.

4 Advanced Search SQL Helper

Generate SQL convierte la pregunta en consulta, Fix Errors corrige la sintaxis y Summarize Results resume lo devuelto. La consulta generada reemplaza a la original o se copia al portapapeles.

5 Servicio MCP propio

Permite construir agentes externos contra el CMDB, incidentes y eventos en https://{Supervisor}/phoenix/mcp con token de API. Dieciséis herramientas expuestas, de get_incident_by_id a query_fsm_clickhouse.

6 Extras del chat

"visualize the data" genera un donut, "generate a PDF" produce el informe descargable y List by Category agrupa incidentes por similitud semántica con puntuación de riesgo.

Acceso y proveedor: por defecto solo los usuarios Admin pueden ejecutar FortiAI; para el resto hay que marcar FortiAI: Run en el rol. El proveedor se configura en Admin > Settings > Analytics > ML/AI y admite OpenAI o Azure OpenAI con clave propia.

Las siete familias de preguntas soportadas

Documentación	Can you give me guidance on tuning a rule in FortiSIEM to remove false positives?	VectorDB
CMDB	How many devices in my CMDB? Group by Vendor and Model.	PostgreSQL
CMDB	Show me all CMDB devices with Critical event collection status.	PostgreSQL
Recolección	What is the average incoming eps for last 1 hour? Show me a breakdown by 5 minutes?	ClickHouse
Incidentes	Tell me the Open incidents related to incident <id>. Provide ID, Title, Status.	PostgreSQL
Incidentes	List IOCs for incident <incident_id>.	PostgreSQL
Threat hunting	Show me top 10 countries that my hosts are communicating with, in last 1 hour.	ClickHouse
Threat hunting	Is there any traffic matching FortiGuard Malware IP in last 1 hour?	ClickHouse
Actividad	Are there any SSH root logons to linux servers in my environment in last 2 days?	ClickHouse
Vulnerabilidades	Check logs for last 2 days for hosts affected by well-known vulnerabilities with score greater than 8.	ClickHouse

La columna derecha indica a qué motor se enruta la pregunta. Las palabras "event" o "log" la mandan a ClickHouse; "incident", "device" o "CMDB", a PostgreSQL. Se puede forzar el destino escribiendo "Use ClickHouse" o "Use Postgres".

IA agéntica para investigar alertas de punta a punta

FortiSOAR no ofrece un chat de producto sino agentes de IA que automatizan la investigación, generan insights contextuales y recomiendan acciones sobre los datos analizados. La configuración vive en Settings > AI Configurations.

1 Servidores MCP

Cuatro por defecto: Module Management para consultar módulos y esquemas, Playbook Management para ejecutar y monitorear playbooks, SOC Framework para alertas, indicadores y caza de IOC, y Utility Tools.

2 Prompts como skills

Cada prompt define identidad, capacidades y límites del agente en la plantilla de sistema, más la tarea concreta en la de usuario con variables entre llaves y un formato de respuesta exigido.

3 Contexto organizacional

Registros con el conocimiento del negocio en tres categorías: INVESTIGATION_SOP con el procedimiento de cada tipo de alerta, NORMALIZATION_SCHEMA con los esquemas y ORGANIZATION_CONTEXT.

4 Insights

Analizan los datos del sistema para identificar riesgos, vigilar el rendimiento y destacar problemas operativos. Se activan, desactivan o eliminan, y alimentan la página AI > AI Insights.

5 Smart Recommendations

Machine learning clásico, no generativo: registros similares por Elasticsearch o clustering, sugerencia de campos y de playbooks a partir del histórico de la instancia.

6 Clasificación de phishing

Clasificador de ML que predice si un correo es phishing, con modelo preentrenado por el equipo de seguridad de Fortinet o entrenado con los registros del propio módulo.

Servicios nuevos: la función agéntica de la 8.0.0 añade tres servicios gestionados con csadm services: fsr-ai, mcp-server y fsr-ai-celery.

Consentimiento explícito en cada capa

1 Habilitar la IA	El administrador debe reconocer y aprobar el uso de funciones de IA antes de activarlas: al guardar aparece un cuadro de confirmación con Acknowledge. Al habilitarlas se consiente el procesamiento de los datos de investigación con modelos de IA, y todas las acciones quedan registradas para auditoría y cumplimiento.
2 Tokens	La página FortiAI muestra el consumo mensual. El derecho por defecto es de 5 millones de tokens por dispositivo al mes, ampliable con la licencia FortiAI Token Top-Up, que añade tokens a nivel de dispositivo. Se ven los restantes y los asignados, tanto mensuales como de top-up.
3 Agentes personalizados	Importar o subir agentes de IA propios exige consentimiento previo en Advanced Development Features, con permiso Security Update. Los agentes solo se editan importando un .zip por el asistente de importación o subiéndolo desde Manage > Upload AI Agent en el Content Hub.
4 Permisos de MCP	Crear un servidor MCP requiere al menos permiso de lectura en los módulos Security, Application y Connector, más Create y Read en MCP Configurations. Sin ellos la interfaz devuelve un error al intentar cargar los conectores.

Ejemplos de contexto que ya vienen cargados: SOP - Brute Force Attack · Organizational Context - Working Hours, con horario laboral y ventanas de mantenimiento aprobadas · Approved Vulnerability Scanners · Port Scanning Investigation.

IA embebida en el SOC como servicio

FortiSOC es una plataforma de operaciones de seguridad en la nube donde la IA no es un módulo aparte: reduce el ruido de alertas, acelera el triaje y automatiza respuestas de bajo riesgo. El servicio FortiAI viene incluido a través de un conector ya preconfigurado en la instancia.

1 Conector FortiAI

Actúa de proxy seguro: enruta las peticiones de chat completion por una capa controlada en lugar de mandarlas directas al proveedor del LLM. Expone Chat Completion, Create Response y Get Token Balance Details.

2 Playbooks de IA

La colección Fortinet FortiAI en Automation > Playbooks trae Case Impact Assessments, Case Extraction, Case Enrichment & Impact Analysis y su variante On Update, Asset Threat Posture Timeline y una demo de remediación autónoma.

3 Enriquecimiento de casos

Desde el detalle del caso, un botón lanza el enriquecimiento y el análisis de impacto. Si ya había una evaluación previa, pregunta si actualizarla o empezar de cero, y rellena la descripción y el campo Impact Assessments.

4 Estructura del análisis

El Impact Assessment sigue siempre la misma plantilla: Executive Highlights, Alert Correlation Analysis, Cybersecurity Concerns, Impact Analysis y, al final, un SOC Action Plan con los siguientes pasos sugeridos.

5 FortiAI Insight

Correlación profunda de casos y alertas que prioriza lo que hay que mirar primero, señala activos de alto riesgo, detecta patrones repetidos y marca alertas candidatas a falso positivo.

6 Investigation Agent

Chat contextual disponible en Alerts, Cases, Assets, Identities e Indicators. Devuelve texto, imágenes, widgets y datos de la propia instancia, y toda acción de respuesta exige aprobación del analista.

Licenciamiento: dos niveles por volumen de ingesta en GB/día. El acceso completo a los playbooks asistidos por IA del content hub es exclusivo del nivel Advanced, junto con la ingesta SIEM completa, UEBA e ITDR.

El panel Insight y el agente de investigación

Cases & Alerts > FortiAI Insight dispara una correlación profunda y devuelve cuatro bloques. Cada uno trae un botón AI Analysis con el razonamiento de FortiAI, y el conjunto se recalcula con Re-run Analysis.

1 Prioritized Cases

Casos ordenados por severidad crítica o alta, SLA incumplido, fase de investigación activa, IOC correlacionados y volumen de alertas.

2 High-Risk Assets

Activos marcados por vulnerabilidades críticas, casos abiertos en los que aparecen, indicadores asociados e identidades comprometidas.

3 Recurring Cases

Patrones entre casos: reutilización del mismo IOC, el mismo activo atacado varias veces o el mismo usuario como objetivo. Requiere dos casos o más.

4 Noise Reduction Alerts

Alertas candidatas a falso positivo por señal mínima, coincidencia con actividad benigna conocida o deriva de la regla de detección.

Qué pedirle al Investigation Agent

- Añadir contexto: información del activo, identidad del usuario e inteligencia de amenazas.
- Correlacionar eventos y construir una línea de tiempo de lo que pasó.
- Analizar los datos para identificar patrones o posibles escenarios de ataque.
- Sugerir el siguiente paso: escalar el caso, contener, seguir vigilando o cerrarlo.

Cómo se trabaja con él

- Los prompts sugeridos cambian según el panel y según si se abre en la lista o en el detalle del registro.
- Show reasoning despliega el razonamiento detrás de la respuesta.
- Export descarga la conversación completa en PDF para compartirla con el resto del equipo.
- Un prompt inválido es el ambiguo, el incompleto o el que pregunta por información ajena a FortiSOC.

FortiSOC 26.2.2 Administration Guide — "AI overview", págs. 103-110.

Seis áreas de asistencia sobre el parque de endpoints

1 Gestión de endpoints

Buscar por nombre, usuario, IP o tag; ver salud y riesgo; poner y quitar de cuarentena; enviar mensajes; revisar política y perfiles asignados.

2 Perfiles y políticas

Crear o actualizar perfiles de VPN, ZTNA, Web y Video Filter, Malware, Sandbox, Firewall, Data Protection, System y Vulnerability Scan; asignar políticas a grupos.

3 Tags de postura

Crear y actualizar security posture tags, ver cuáles aplican a un endpoint, explicar por qué un tag coincide o no, y listar endpoints por tag.

4 Vulnerabilidades

Top de vulnerabilidades, endpoints más vulnerables, detalle por endpoint, equipos afectados por una vulnerabilidad y recomendaciones de remediación.

5 Asistencia de UI

Navegar a las páginas de EMS, aplicar filtros y ordenamientos, y sacar a la vista eventos de seguridad, inventario de software y listas de endpoints.

6 Documentación

Buscar en la documentación de EMS y responder preguntas de producto con los manuales disponibles.

Despliegue: paquete add-on instalado junto con EMS o con emscli execute install-ai, activado en System Settings > EMS Settings, licencia FortiAI válida, salida directa a fortiai.forticloud.com y uso reservado a super admins.

El recorrido de ejemplo de la guía, prompt a prompt

1	**Descubrir**	`What can you do?`	La pestaña FortiAI abre con preguntas preconfiguradas; ésta devuelve el catálogo de tareas.
2	**Inventariar**	`List endpoints by name.`	Punto de partida para localizar equipos antes de actuar sobre ellos.
3	**Contener**	`Quarantine endpoint <device name>.`	FortiAI pide aprobación explícita antes de ejecutar la cuarentena.
4	**Comunicar**	`Send a one-way message to <endpoint>.`	Aviso al usuario final desde el mismo hilo.
5	**Configurar**	`Create a new firewall profile.`	Igual para perfiles de VPN, ZTNA, malware o data protection.
6	**Asignar**	`Assign policy <name> to workgroup <group>.`	Enlaza políticas con grupos del directorio.
7	**Etiquetar**	`Create a security posture tag.`	Pide OS, tipo de regla, nombre del tag y mensaje al usuario.
8	**Priorizar**	`Show the top 2 most vulnerable endpoints.`	Y luego: "Show the top 2 vulnerabilities on <endpoint>".

FortiClient 8.0.0 EMS Administration Guide — "FortiAI example tasks".

Un analista de aplicación web dentro del banner

FortiAI en FortiWeb abre un panel lateral que permanece visible mientras se navega por la GUI. Está entrenado con el conocimiento de producto de Fortinet y con conceptos de seguridad web, y ha crecido en tres fases: integración inicial en 8.0.0, análisis de log individual en 8.0.1 y salud del sitio y Lua en 8.0.5.

1 Q&A documental

Responde sobre configuración y funciones consultando el Administration Guide, el CLI Reference, las Release Notes, el material de troubleshooting y los datasheets.

2 Análisis de logs

Analiza, resume y filtra los logs de Attack, Traffic y Event. Con Analyze with AI en el detalle de un ataque resume el evento, evalúa el riesgo y propone remediación.

3 Navegación y reputación

Redirige a la vista de log adecuada aplicando filtros, y consulta a FortiGuard la reputación de una o varias IP externas.

4 Salud del sitio (8.0.5)

Correlaciona configuración, red y negocio: estado de policies, VIP, server pools y content routing, uso de CPU, memoria y disco, y análisis de causa raíz.

5 Scripting Lua (8.0.5)

Genera scripts a partir de una descripción, explica código heredado con Explain with AI y diagnostica errores de ejecución devolviendo la versión corregida.

6 Límites del asistente

Es stateless: no conserva contexto entre consultas. No aplica cambios de configuración ni ejecuta comandos: toda la salida es informativa y consultiva.

Requisitos: licencia FortiAI válida, habilitado por defecto en los modelos soportados, máximo tres administradores locales con la opción FortiAI User y, en 8.0.0, solo despliegues VM sobre VMware.

Qué preguntarle y qué devuelve

Uso general	`How do I configure ML-Based Bot Detection?`	Busca en la documentación interna y devuelve el procedimiento resumido.
Uso general	`What does the HTTP Protocol Constraints feature do?`	Explica el propósito de la función y su aporte a la seguridad de capa 7.
Análisis de log	`show me attack log from 10.200.52.183 in last week`	Redirige al Attack Log y aplica el filtro de IP y de rango temporal.
Análisis de log	`List the top 10 attack types detected this month`	Devuelve el ranking de categorías con el número de detecciones.
Análisis de log	`Please analyze log data from current page`	Resume tendencias, orígenes frecuentes y patrones de la vista abierta.
Monitoreo	`Please check reputation of the IP 104.204.178.1`	Consulta FortiGuard y devuelve score y categorías de amenaza.
Postura	`How is the policy status for <policy> now?`	Detecta el estado offline, identifica el health check que falla y da remediación.
Postura	`My CPU usage is high. Can you help me diagnose the root cause?`	Informe de utilización, carga de tráfico y amenazas, con causa raíz.
Lua	`Generate a Lua script to redirect all HTTP traffic to HTTPS...`	Genera el código validado y explica la lógica de implementación.
Lua	`Explain what this script segment does: ...`	Identifica la lógica y las llamadas a la API de FortiWeb utilizadas.

Para ver el catálogo completo de tareas soportadas basta preguntar: "What can you help me with?".

Un experto de balanceo dentro de la consola

FortiAI Assistant abre un panel acoplable que se mantiene mientras se navega por la GUI. Entiende tanto la documentación oficial como el estado real del equipo, así que sirve lo mismo para configurar una función nueva que para diagnosticar un virtual server con problemas.

1 Guía técnica

Devuelve instrucciones resumidas y buenas prácticas desde la biblioteca oficial de FortiADC, con hipervínculos verificados a las páginas concretas de la documentación.

2 Estado en vivo

Consulta la configuración y la salud de virtual servers y real server pools, y revisa el historial de health checks para localizar cuándo se cayó un servicio.

3 Tres modos de log

Consulta en lenguaje natural, resumen masivo de todo lo visible en pantalla —Traffic, Security, Event y Script— y análisis individual con Analyze with AI, disponible solo en Traffic y Security.

4 Navegación y filtros

Los verbos "Go to" y "Show" llevan la consola a FortiView o al módulo de Log con un deep link, y los filtros de severidad, tiempo o IP se rellenan solos a partir de la pregunta.

5 Text-to-Script en Lua

Genera el script desde la descripción y admite refinamiento iterativo sobre el mismo hilo. El código se pega en Server Load Balance > Scripting, en HTTP o Stream, y se activa en el virtual server.

6 Sesión persistente

El hilo sobrevive a la navegación y al cierre del panel: solo Reset Session lo limpia. Hay micrófono para dictar, medidor de tokens y descarga en PNG, HTML o PDF.

Requisitos: función Beta sobre hardware y VM privada BYOL, con FortiCare Premium o Elite; no funciona en trial, Flex-VM ni nube pública PAYG. Solo en VDOM no-Global, solo cuentas locales y un máximo de tres administradores con la opción FortiAI User, que habilita el admin Global.

Qué preguntarle y qué hace con la petición

Documentación	`How do I configure advanced bot protection on FortiADC?`	Checklist de configuración resumido, con enlaces verificados.
Documentación	`What can Advanced Bot Protection do?`	Resume el módulo y sugiere funciones relacionadas.
Virtual server	`Show detailed information of virtual server vs-http-8888`	Tarjeta de estado en vivo: IP, puerto y salud de los real servers.
Virtual server	`Go to the fortiview page for virtual server vs-http`	Lleva la consola a la pestaña de FortiView del objeto.
Virtual server	`Check if virtual server vs-http experience any downtime in past one hour`	Rastrea fallos de health check y resume las transiciones Up/Down.
Logs	`List the top 3 attack types detected in this month`	Redirige al Attack Log y devuelve el ranking con sus conteos.
Logs	`Show me the url protection attack logs with severity low in past one month`	Navega a la página de log y construye el filtro por sí solo.
Logs	`Please analyze logs in current page`	Identifica IP de origen frecuentes y patrones de tráfico notables.
Lua	`Write a lua script to insert a message-id in request header`	Bloque de código con la sintaxis correcta de la API Lua.

Tokens de FortiADC: cuota fija por plataforma que se repone cada mes, sin opción de top-up. En VM va de 350.000 tokens con 1 vCPU a 4.500.000 con 32 o más; en hardware, de 200.000 en el 100F a 15.000.000 en el 5000F. Al agotarse, el asistente queda suspendido hasta el siguiente ciclo. El catálogo completo de tareas se obtiene preguntando "What can you help me with?".

Aquí FortiAI no es un chat: es un motor de veredicto

FortiSandbox puede usar FortiAI como uno de sus métodos para emitir veredictos. Se integra el appliance FortiAI dentro del prefiltro del escaneo, de modo que la IA decide si un archivo necesita o no pasar por el análisis en máquina virtual.

Limpio	Si FortiAI califica el archivo como limpio y el resto de métodos coincide, FortiSandbox no lo envía al escaneo en VM.
Malicioso o alto riesgo	FortiSandbox adopta esa misma calificación de forma directa.
Cualquier otra calificación	Se sigue el flujo de escaneo normal y el veredicto final se emite tras aplicar todos los métodos, incluida la VM.

Prerrequisitos

- Servidor FortiAI instalado y licenciado.
- FortiAI en versión superior a v1.5.0 build 0104.
- Token obtenido en FortiAI System > Administrator > Edit > API Key.

Configuración

- Security Fabric > FortiAI > Enable: IP del servidor, token, timeout de veredicto, timeout de carga y tamaño máximo de archivo.
- Scan Policy and Object > Scan Profile > Pre-Filter: activar FortiAI entrust y aplicar.
- Si se agota un timeout o el archivo excede el tamaño, sigue el flujo de escaneo normal.

El valor de FortiSandbox dentro del flujo conversacional está aguas abajo: sus veredictos llegan a FortiAnalyzer y a los perfiles Sandbox de FortiClient EMS, y allí sí se pueden consultar con el asistente.

Qué incluye la licencia en cada producto

1 FortiGate

Hardware con más de 2 GB de RAM y FortiCare Premium: 2.000.000 de tokens iniciales al mes por equipo; VM serie S con Premium o bundle Enterprise, UTP o ATP. Los adicionales se comparten entre los FortiGate de la cuenta.

2 FortiWeb y FortiADC

Cuota fija por plataforma que se repone cada mes y no admite top-up. FortiWeb va de 387.083 tokens en VM01 a 21.000.000 en el 4000F; FortiADC, de 200.000 en el 100F a 15.000.000 en el 5000F, y en VM de 350.000 a 4.500.000 según vCPU.

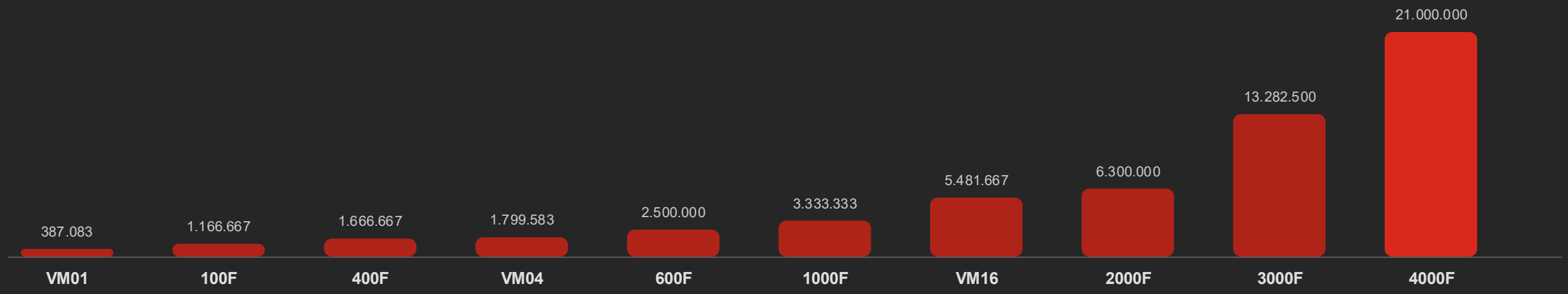
3 FortiManager, FortiAnalyzer y EMS

Asignación mensual de la licencia compartida por los usuarios del equipo, más SKU de top-up LIC-FAITOKEN-1M, 5M y 10M a nivel de cuenta FortiCare: apilables y compartidos entre productos.

4 FortiSOAR, FortiSIEM y FortiSOC

FortiSOAR entrega 5 millones de tokens por dispositivo al mes, ampliables con Token Top-Up. FortiSIEM se factura contra tu clave de OpenAI o Azure OpenAI. FortiSOC licencia por ingesta en GB/día y consulta el saldo con Get Token Balance Details.

Tokens mensuales por modelo de FortiWeb



El consumo se mide sobre el prompt y la respuesta; los hilos largos cuestan más porque arrastran el historial. En FortiSIEM, la opción Optimize recorta cerca del 45% enviando solo las secciones relevantes.

Enmascarado de datos y control de acceso

FortiOS	IP, MAC, correo, teléfono y URL, con conmutador para activarlo o desactivarlo desde el propio chat. Aun así, el manual pide no enviar información confidencial ni regulada.	Perfil de administrador: Allow using AI Assistant.
FortiManager	Panel Masked Data con el texto original y el enmascarado. GPT-4.1 de Azure OpenAI a través del AI Proxy de Fortinet, con MCP Server autenticado.	RBAC por perfil e interruptor global set ai-mode enable.
FortiAnalyzer	Function callback más enmascarado de IP, MAC y usuarios, y paso por el FortiAI proxy. El valor sustituto depende de la cookie, así que cambia en cada sesión.	Máximo tres administradores locales.
FortiSIEM	Anonimiza los datos del cliente antes de enviarlos al LLM y revierte los valores al mostrar el resultado. En incidentes y casos protege IP, host, usuario y correo.	Rol con FortiAI: Run; por defecto solo Admin.
FortiSOAR	Todas las acciones de IA quedan registradas para auditoría y cumplimiento. Habilitarlas exige que el administrador reconozca de forma explícita el procesamiento.	Consentimiento por capa y permisos por módulo.
FortiSOC	El conector FortiAI hace de proxy: las peticiones al modelo pasan por una capa controlada en vez de ir directas al proveedor del LLM.	Toda acción de respuesta del agente exige aprobación del analista.
FortiWeb	IPv4, MAC, correo y usuarios. El LLM solo ve el prompt enmascarado y responde con un function callback; FortiWeb desenmascara en local y consulta el log.	Máximo tres administradores locales.
FortiADC	IPv4, IPv6, MAC, puerto TCP/UDP, usuarios y correo, con clave distinta por sesión. El proxy no deja que el motor use los datos del cliente para entrenar.	Tres cuentas locales con FortiAI User; solo en VDOM no-Global.
FortiClient EMS	Nombre, IP, correo y teléfono, con mapeo uno a uno que se revierte al responder. Las imágenes cargadas no se enmascaran y el producto avisa antes de enviarlas.	Solo super administradores de EMS.

Columna central: qué se protege antes de salir del equipo. Columna derecha: quién puede usar el asistente. Ningún producto aplica cambios sin confirmación explícita.

CÓMO ESCRIBIR LOS PROMPTS

Seis reglas que ahorran tokens y mejoran la respuesta

1 Concreto y corto

"Show recent logs for 10.10.10.10 (Past week)" rinde más que "Can you show me all the log entries for endpoint 10.10.10.10 from the past week?".

2 Filtra desde el prompt

Acota ventana de tiempo, IP, equipo o página afectada: el ahorro está sobre todo en la respuesta, no en la pregunta.

3 Usa el vocabulario del producto

"apply filter", "generate report", "quarantine device": nombrar la función existente le dice al asistente qué acción ejecutar.

4 Dirige la consulta al motor correcto

En FortiSIEM, "event" o "log" enrutan a ClickHouse y "incident", "device" o "CMDB" a PostgreSQL; se puede forzar con "Use ClickHouse" o "Use Postgres".

5 Encadena y reinicia a tiempo

Refiérete a lo ya obtenido para no repetir contexto, y empieza un chat nuevo tras unas diez interacciones si el histórico ya no aporta.

6 Aprovecha los optimizadores

La opción Optimize de FortiSIEM ahorra cerca del 45%, y en FortiSOAR unas skills bien definidas reducen tokens e iteraciones para cerrar la tarea.

Coste típico de cada tipo de consulta, según los ejemplos de FortiWeb:

80	192	365	720
Consulta de configuración	Explicación de función	Resumen de log con análisis	Correlación entre logs

PARA LLEVARSE

Por dónde empezar

1 Confirma licencia, modelo y tokens	El soporte depende del producto: FortiGate necesita más de 2 GB de RAM, FortiWeb y FortiADC tienen cuota fija por plataforma, EMS exige el paquete add-on y FortiSIEM una clave propia de OpenAI o Azure OpenAI.
2 Abre la salida y define permisos	Salida directa sin proxy a fai.fortinet.net y fortiai.forticloud.com, y perfiles o cuentas habilitadas en cada producto, con el límite de tres administradores donde aplica.
3 Prueba con consultas de solo lectura	"Which devices need my attention?", "How many devices in my CMDB? Group by Vendor and Model.", "List the top 10 attack types detected this month".
4 Escala a acciones con confirmación	Cuarentena, event handlers, scripts CLI, overlays SD-WAN, playbooks de enriquecimiento y análisis agéntico, revisando siempre el plan o el widget de confirmación antes de aplicar.
5 Documenta y codifica lo que funciona	Una biblioteca de prompts por producto, y en FortiSOAR los SOP y el contexto organizacional, es la forma más rápida de hacer las investigaciones repetibles y baratas.

Todo el contenido proviene de la documentación cargada en el proyecto. Las capacidades y los prompts cambian entre versiones: valida siempre contra la guía de la versión desplegada.


FORTINET
COLOMBIA
& ECUADOR
XPERTS26