Acceder a registros de appliances web seguros

Contenido

Introducción

Este documento describe los métodos para ver los registros de Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- SWA físico o virtual instalado.
- Licencia activada o instalada.
- Cliente Secure Shell (SSH).
- El asistente de configuración ha finalizado.
- Acceso administrativo al SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Tipos de registro SWA

El Secure Web Appliance registra sus propias actividades de gestión del sistema y del tráfico escribiéndolas en archivos de registro. Los administradores pueden consultar estos archivos de registro para supervisar y solucionar problemas del dispositivo.

En esta tabla se describen los tipos de archivo de registro de Secure Web Appliance.

Tipo de archivo de registro	Descripción	¿Admite Syslog Push?	¿Habilitado de forma predeterminada?
Registros del motor de control de acceso	Registra mensajes relacionados con el motor de evaluación de ACL (lista de control de acceso) de proxy web.	No	No
Registros de Secure EndpointEngine	Registra información sobre el análisis de la reputación de archivos y el análisis de archivos (Secure Endpoint.)	Yes	Yes
Registros de auditoría	Registra eventos AAA (autenticación, autorización y contabilidad). Registra toda la interacción del usuario con la aplicación y las interfaces de línea de comandos, y captura los cambios registrados. Algunos de los detalles del registro de auditoría son los siguientes: • Usuario: inicio de sesión • Usuario: error al iniciar sesión con contraseña incorrecta • Usuario: error de inicio de sesión con nombre de usuario desconocido • Usuario: la cuenta de inicio de sesión ha caducado • Usuario: cierre de sesión • Usuario - Bloqueo • Usuario - Activado • Usuario: cambio de contraseña	Yes	Yes

Tipo de archivo de registro	Descripción	¿Admite Syslog Push?	¿Habilitado de forma predeterminada?
	• Usuario: restablecimiento de contraseña • Usuario: cambio de perfil/configuración de seguridad • Usuario - Creado • Usuario: eliminado/modificado • Grupo/rol - Eliminación / modificación • Grupo/rol: cambio de permisos		
Registros de acceso	Registra el historial del cliente de proxy web.	Yes	Yes
Registros del marco del motor ADC	Registra mensajes relacionados con la comunicación entre el proxy web y el motor ADC.	No	No
Registros del motor ADC	Registra los mensajes de depuración del motor ADC.	Yes	Yes
Registros del marco de autenticación	Registra el historial de autenticación y los mensajes.	No	Yes
Registros del marco del motor AVC	Registra mensajes relacionados con la comunicación entre el proxy web y el motor AVC.	No	No
Registros del motor AVC	Registra los mensajes de depuración del motor AVC.	Yes	Yes
Registros de auditoría de CLI	Registra una auditoría histórica de la actividad de la interfaz de línea de comandos.	Yes	Yes

Tipo de archivo de registro	Descripción	¿Admite Syslog Push?	¿Habilitado de forma predeterminada?
Registros de configuración	Registra mensajes relacionados con el sistema de administración de la configuración de proxy web.	No	No
Registros de administración de conexiones	Registra mensajes relacionados con el sistema de administración de conexiones de proxy web.	No	No
Registros de seguridad de datos	Registra el historial del cliente para las solicitudes de carga evaluadas por los filtros de seguridad de datos de Cisco.	Yes	Yes
Registros del módulo de seguridad de datos	Registra mensajes relacionados con los filtros de seguridad de datos de Cisco.	No	No
Registros del marco del motor DCA (Análisis de contenido dinámico)	Registra mensajes relacionados con la comunicación entre el proxy web y el motor de análisis de contenido dinámico de los controles de uso web de Cisco.	No	No
Registros del motor DCA (Análisis de contenido dinámico)	Registra mensajes relacionados con el motor de análisis de contenido dinámico de los controles de uso web de Cisco.	Yes	Yes
Registros de proxy predeterminados	Registra errores relacionados con el proxy web. Éste es el más básico de todos los registros relacionados con Web Proxy. Para solucionar problemas de aspectos más específicos relacionados con el proxy web, cree una suscripción de registro para el módulo de proxy	Yes	Yes

Tipo de archivo de registro	Descripción	¿Admite Syslog Push?	¿Habilitado de forma predeterminada?
	web aplicable.		
Registros del Administrador de discos	Registra los mensajes del proxy web relacionados con la escritura en la caché del disco.	No	No
Registros de autenticación externa	Registra los mensajes relacionados con el uso de la función de autenticación externa, como el éxito o el fracaso de la comunicación con el servidor de autenticación externo. Incluso si la autenticación externa está inhabilitada, este registro contiene mensajes acerca de los usuarios locales que han iniciado sesión correctamente o que no han podido iniciarla.	No	Yes
Registros de comentarios	Registra los usuarios web que informan de páginas clasificadas erróneamente.	Yes	Yes
Registros de proxy FTP	Registra mensajes de error y de advertencia relacionados con el proxy FTP.	No	No
Registros del servidor FTP	Registra todos los archivos cargados y descargados desde el dispositivo web seguromediante FTP.	Yes	Yes
Registros de GUI (Interfaz gráfica de usuario)	Registra el historial de las actualizaciones de página en la interfaz web. Los registros de GUI también incluyen información sobre transacciones SMTP; por ejemplo, información sobre informes programados enviados por correo electrónico desde el dispositivo.	Yes	Yes
Registros de pajar	Los registros de Haystack registran el procesamiento de datos de seguimiento de transacciones web.	Yes	Yes

Tipo de archivo de registro	Descripción	¿Admite Syslog Push?	¿Habilitado de forma predeterminada?
Registros HTTPS	Registra mensajes de proxy web específicos para el proxy HTTPS (cuando el proxy HTTPS está activado).	No	No
Registros del servidor ISE	Registra la conexión de los servidores ISE y la información operativa.	Yes	Yes
Registros del módulo de licencias	Registra mensajes relacionados con la licencia del proxy web y el sistema de gestión de claves de característica.	No	No
Registros del marco de registro	Registra los mensajes relacionados con el sistema de registro del proxy web.	No	No
Registros de registro	Registra errores relacionados con la administración de registros.	Yes	Yes
Registros de McAfee Integration Framework	Registra mensajes relacionados con la comunicación entre el proxy web y el motor de exploración de McAfee.	No	No
Registros de McAfee	Registra el estado de la actividad de exploración antimalware desde el motor de exploración de McAfee.	Yes	Yes
Registros del administrador de memoria	Registra los mensajes del proxy web relacionados con la administración de toda la memoria, incluida la caché en memoria para el proceso del proxy web.	No	No
Registros de módulos proxy variados	Registra mensajes de proxy web que utilizan principalmente desarrolladores o el servicio de atención al cliente.	No	No
Registros de	Registra la interacción entre el dispositivo web	Yes	Yes

Tipo de archivo de registro	Descripción	¿Admite Syslog Push?	¿Habilitado de forma predeterminada?
AnyConnect Secure Mobility Daemon	seguroy el cliente AnyConnect, incluida la comprobación de estado.		
Registros NTP (Network Time Protocol)	Registra los cambios en la hora del sistema realizados por el protocolo de tiempo de la red.	Yes	Yes
Registros de PAC File Hosting Daemon	Registra el uso del archivo de configuración automática de proxy (PAC) por parte de los clientes.	Yes	Yes
Registros de omisión de proxy	Registra las transacciones que omiten el proxy web.	No	Yes
Registros de informes	Registra un historial de generación de informes.	Yes	Yes
Registros de consultas de informes	Registra errores relacionados con la generación de informes.	Yes	Yes
Solicitar registros de depuración	Registra información de depuración muy detallada sobre una transacción HTTP específica de todos los tipos de registro del módulo Web Proxy. Es recomendable crear esta suscripción de registro para solucionar un problema de proxy con una transacción determinada sin crear todas las demás suscripciones de registro de proxy. Nota:Puede crear esta suscripción de registro sólo en la CLI.	No	No
Registros de autenticación	Registra mensajes relacionados con la función Control de acceso.	Yes	Yes

Tipo de archivo de registro	Descripción	¿Admite Syslog Push?	¿Habilitado de forma predeterminada?
Registros SHD (Demonio de estado del sistema)	Registra un historial del estado de los servicios del sistema y un historial de reinicios inesperados del demonio.	Yes	Yes
Registros SNMP	Registra los mensajes de depuración relacionados con el motor de administración de red SNMP.	Yes	Yes
Registros del módulo SNMP	Registra mensajes de proxy web relacionados con la interacción con el sistema de supervisión SNMP.	No	No
Registros de Sophos Integration Framework	Registra mensajes relacionados con la comunicación entre el proxy web y el motor de análisis de Sophos.	No	No
Registros de Sophos	Registra el estado de la actividad de análisis antimalware desde el motor de análisis de Sophos.	Yes	Yes
Registros de estado	Registra información relacionada con el sistema, como las descargas de claves de característica.	Yes	Yes
Registros del sistema	Registra DNS, error y actividad de confirmación.	Yes	Yes
Registros de errores del monitor de tráfico	Registra la interfaz L4TM y los errores de captura.	Yes	Yes
Registros del monitor de tráfico	Direcciones de registros agregadas al bloque L4TM y listas de permitidos.	No	Yes
Registros de UDS	Registra datos sobre cómo el proxy web detecta el nombre de usuario sin realizar una	Yes	Yes

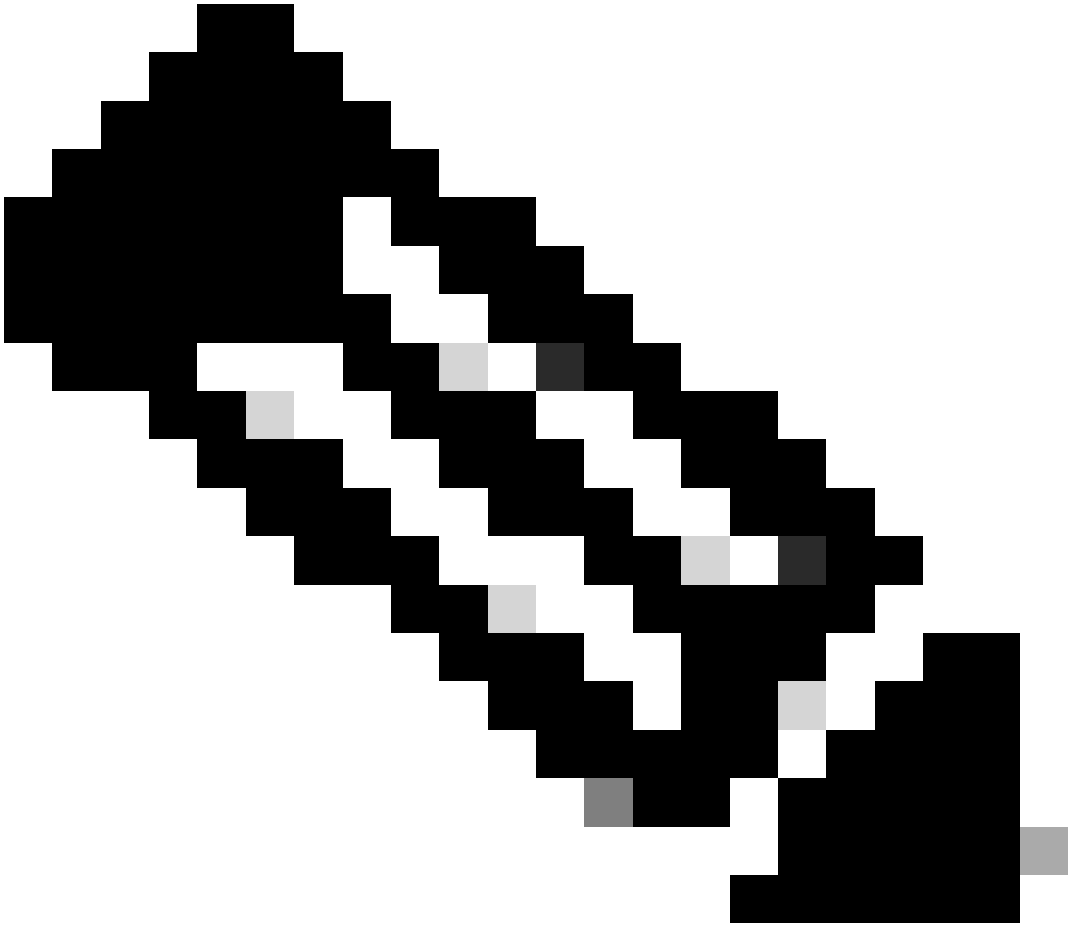
Tipo de archivo de registro	Descripción	¿Admite Syslog Push?	¿Habilitado de forma predeterminada?
(Servicio de detección de usuarios)	autenticación real. Incluye información sobre la interacción con el dispositivo de seguridad adaptable de Cisco para la movilidad segura, así como la integración con el servidor de Novell eDirectory para la identificación transparente de usuarios.		
Registros del actualizador	Registra un historial de WBRS y otras actualizaciones.	Yes	Yes
Registros W3C	Registra el historial del cliente de proxy web en un formato compatible con W3C. Para más información.	Yes	No
Registros WBNP (Participación de red SensorBase)	Registra un historial de las cargas de participación de Cisco SensorBase Network en la red SensorBase.	No	Yes
Registros de WBRS Framework (Puntuación de reputación en la Web)	Registra mensajes relacionados con la comunicación entre el proxy web y los filtros de reputación web.	No	No
Registros del módulo WCCP	Registra mensajes de proxy web relacionados con la implementación de WCCP.	No	No
Registros de Webcat Integration Framework	Registra mensajes relacionados con la comunicación entre el proxy web y el motor de filtrado de URL asociado a los controles de uso web de Cisco.	No	No
Registros de Webroot	Registra mensajes relacionados con la comunicación entre el proxy web y el motor de	No	No

Tipo de archivo de registro	Descripción	¿Admite Syslog Push?	¿Habilitado de forma predeterminada?
Integration Framework	análisis Webroot.		
Registros de Webroot	Registra el estado de la actividad de escaneo anti-malware desde el motor de escaneo de Webroot.	Yes	Yes
Registros de reconocimiento de página de bienvenida	Registra un historial de los clientes web que hacen clic en el botón Aceptar de la página de reconocimiento de usuario final.	Yes	Yes

Ver registros

De forma predeterminada, los registros se almacenan localmente en el SWA, puede descargar los archivos de registro almacenados localmente mediante la GUI o ver los registros desde CLI.

Descargar archivos de registro mediante GUI



Nota: El FTP debe estar activado en el dispositivo. Para activar FTP, consulte Activar FTP en dispositivo web seguro en este artículo.

Puede descargar los archivos de registro desde la GUI:

Paso 1. Inicie sesión en la GUI

Paso 2. Vaya a Administración del sistema

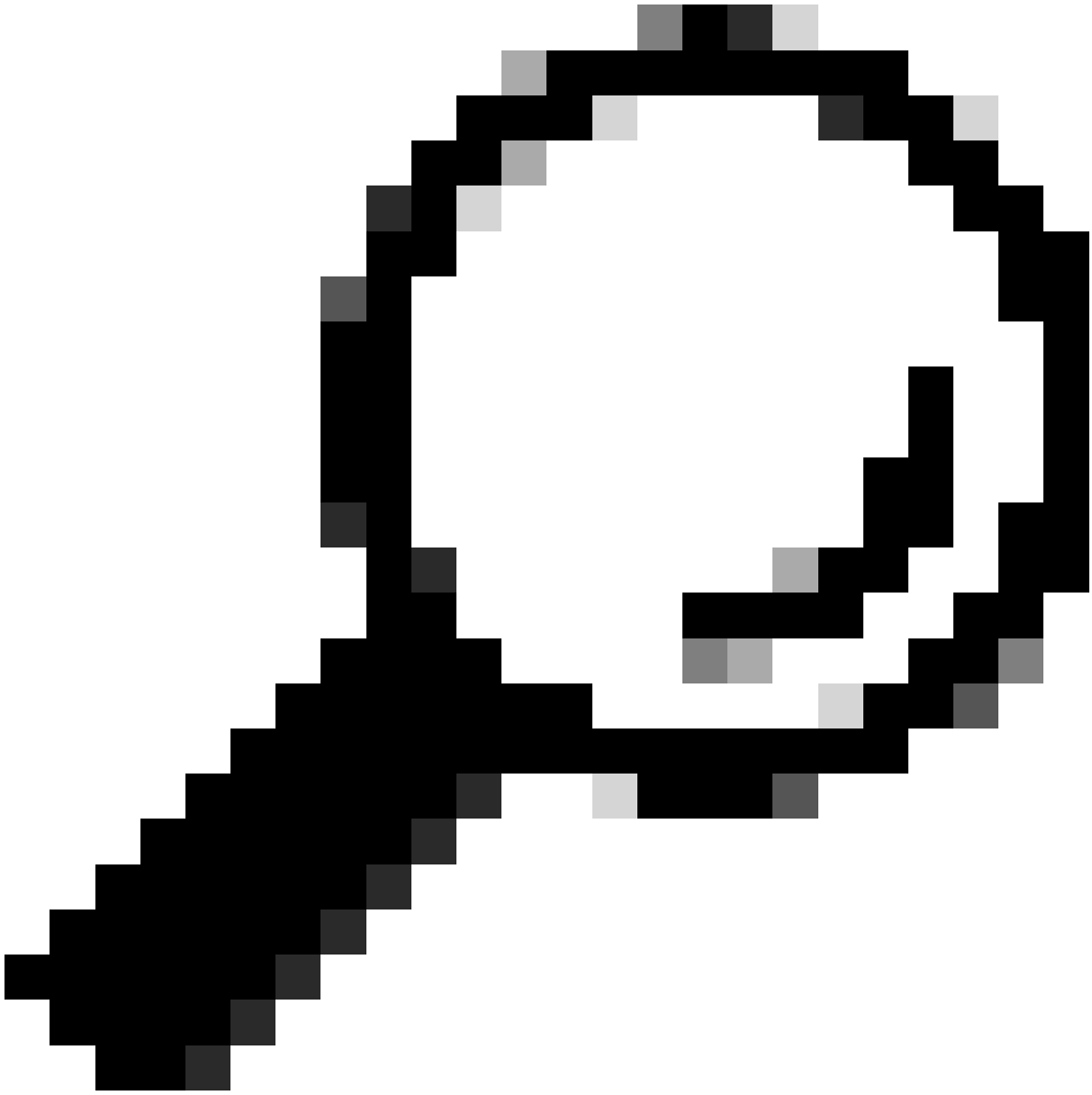
Paso 3. Seleccione Suscripciones de registro

Paso 4.Haga clic en el nombre de la suscripción de registro en la columna Archivos de registro de la lista de suscripciones de registro.

Paso 5.Cuando se le solicite, introduzca el nombre de usuario y la contraseña del administrador para acceder al dispositivo.

Paso 6.Cuando haya iniciado sesión, haga clic en uno de los archivos de registro para verlo en el

explorador o guardarlo en el disco.



Sugerencia: actualice el explorador para obtener resultados actualizados.

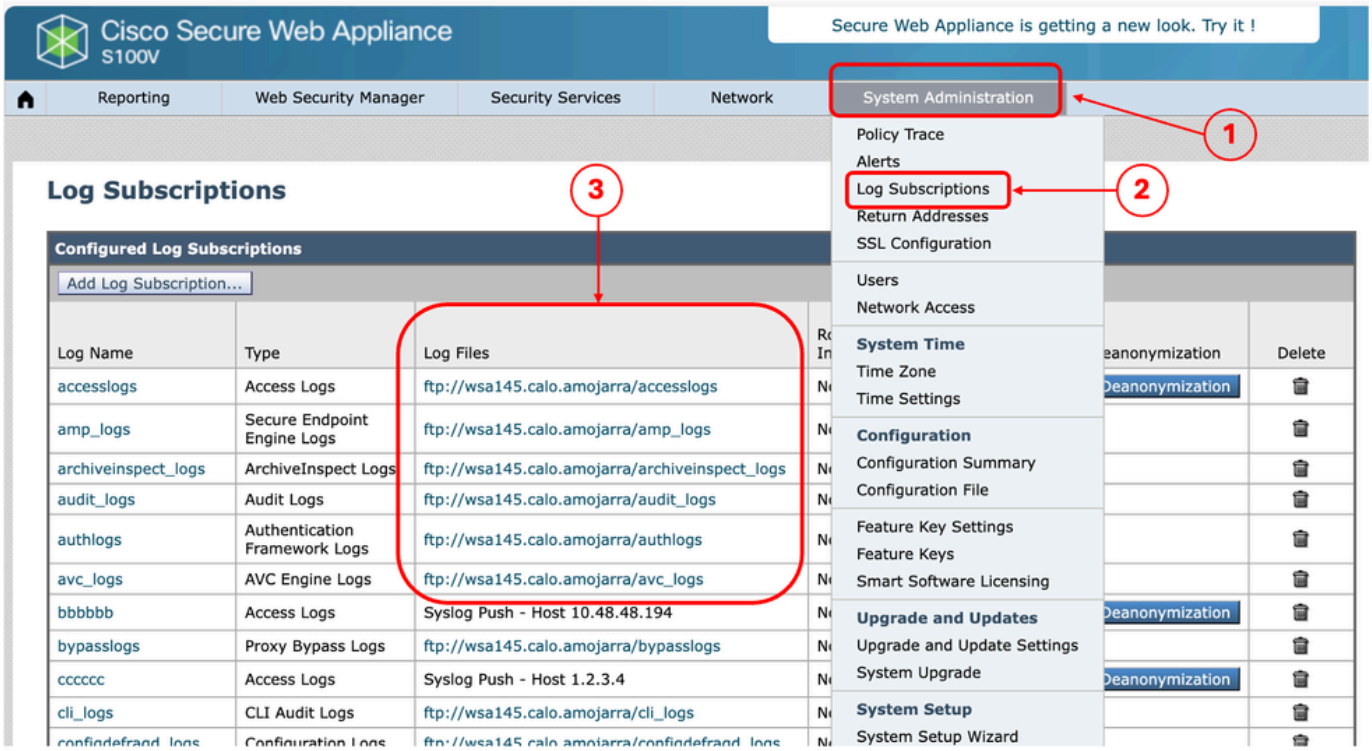
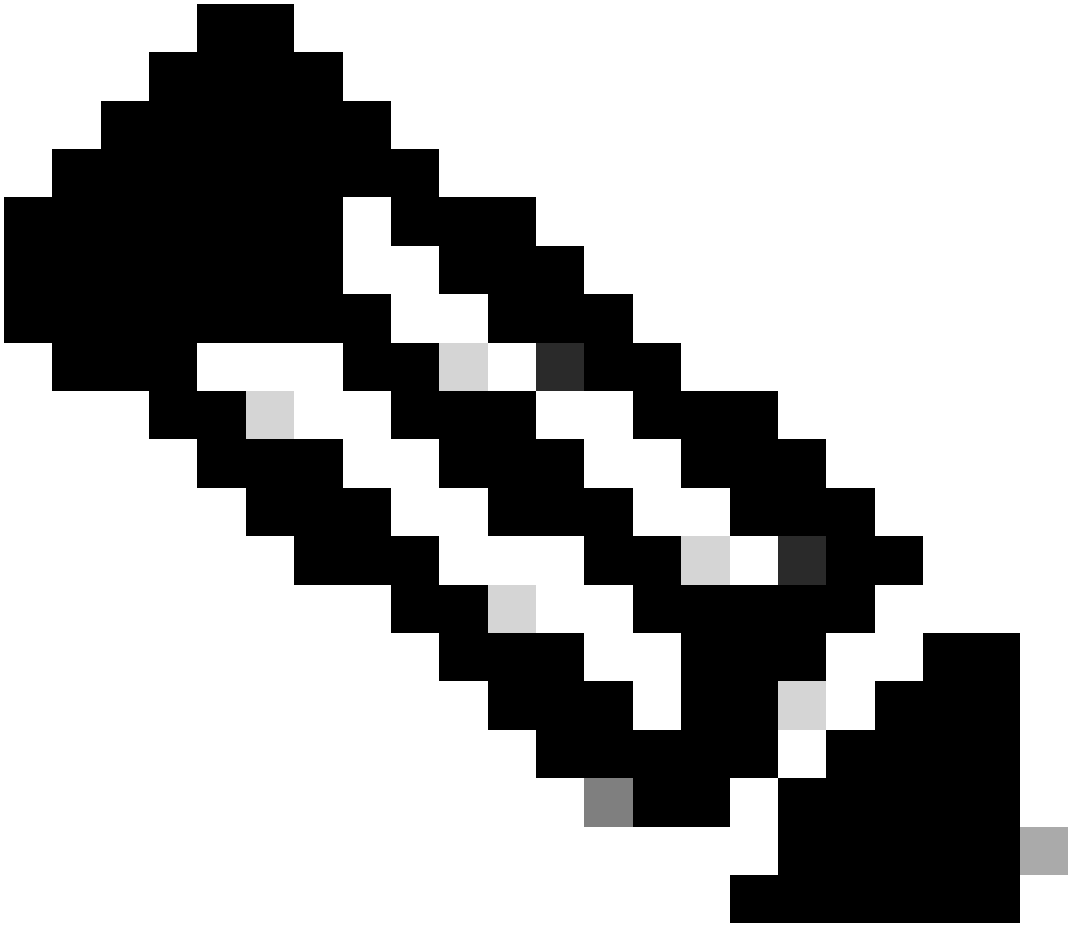


Imagen - Descargar archivos de registro



Nota: Si se comprime una suscripción a un registro, descárguela, descomprímala y ábrala.

Ver registros desde CLI

Puede ver los registros desde CLI. en este caso, puede tener acceso a los registros activos o filtrar una palabra clave en los registros.

Paso 1. Conexión a CLI

Paso 2. Escriba grep y pulse intro.

Paso 3. Introduzca el número del registro que desea ver

Paso 4. (Opcional) Puede filtrar la salida definiendo una expresión regular o una palabra; de lo contrario, pulse Intro

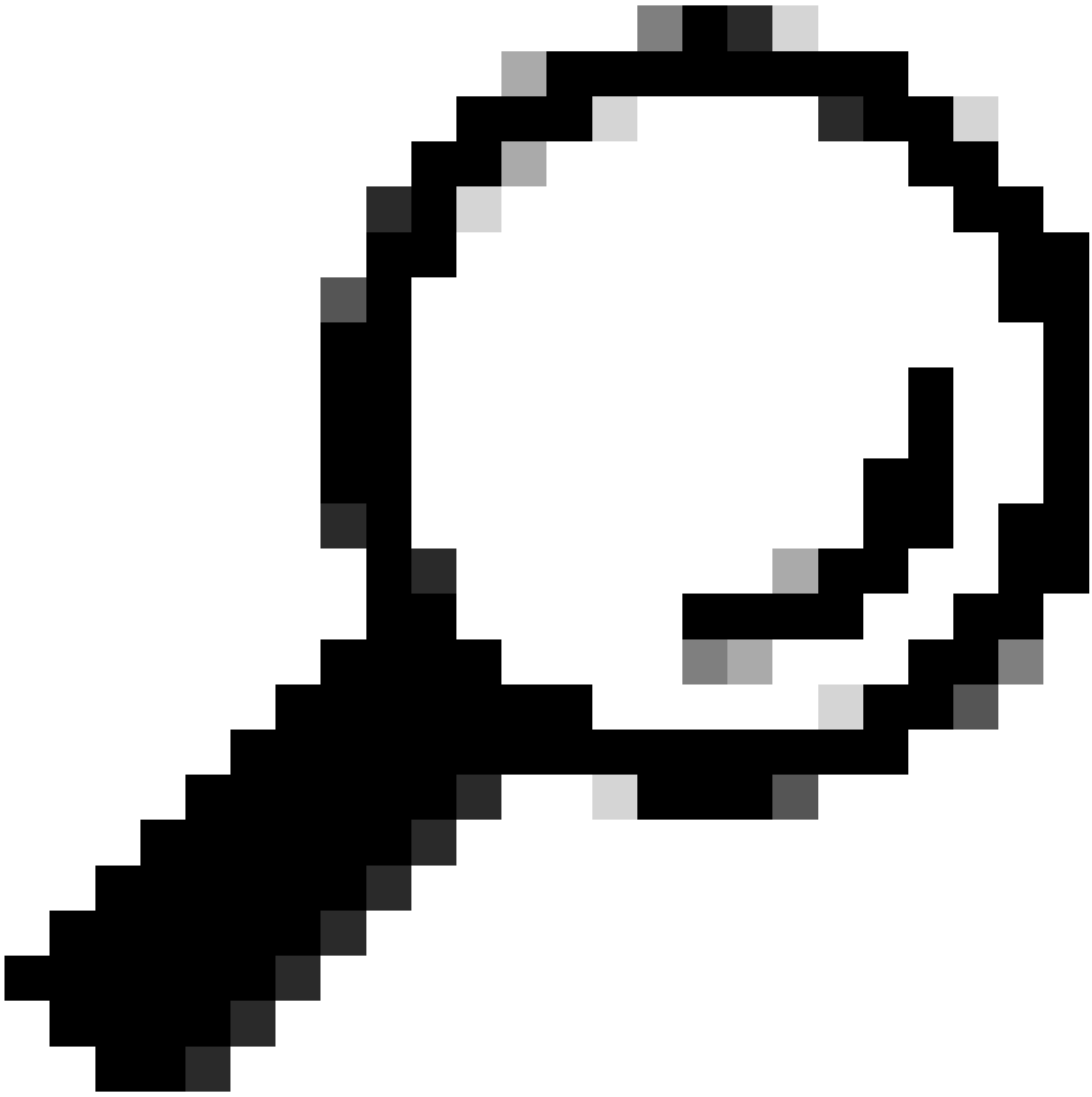
Paso 5. Si necesita que la búsqueda de la palabra clave introducida en el paso 4 no distinga

mayúsculas de minúsculas, pulse Intro en "¿Desea que esta búsqueda no distinga mayúsculas de minúsculas? [Y]>"; de lo contrario, escriba "N" y pulse Intro.

Paso 6. Si necesita eximir la palabra clave de la búsqueda, escriba "Y" en "¿Desea buscar líneas no coincidentes? [N]>" en caso contrario, pulse Intro.

Paso 7. Si necesita ver los registros activos, escriba "Y" en "¿Desea seguir los registros? [N]>"; de lo contrario, pulse Intro.

Paso 8. Si desea paginar los registros para verlos página por tipo de página "Y" en "¿Desea paginar la salida? [N]>"; de lo contrario, pulse Intro.



Sugerencia: Si elige paginar, puede salir de los registros pulsando "q"

Aquí hay un ejemplo de salida que muestra todas las líneas que tienen "Advertencia":

```
SWA_CLI> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "Secure Endpoint Engine Logs" Retrieval: FTP Poll
3. "archiveinspect_logs" Type: "ArchiveInspect Logs" Retrieval: FTP Poll
4. "audit_logs" Type: "Audit Logs" Retrieval: FTP Poll
5. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
6. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
7. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
8. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
...
45. "upgrade_logs" Type: "Upgrade Logs" Retrieval: FTP Poll
46. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
47. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
48. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
49. "webtapd_logs" Type: "Webtapd Logs" Retrieval: FTP Poll
50. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 40

Enter the regular expression to grep.
[]> Warning

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]>

Do you want to paginate the output? [N]>
```

Activar FTP en dispositivo web seguro

De forma predeterminada, FTP no está habilitado en el SWA. Para activar FTP:

Paso 1. Inicie sesión en la GUI

Paso 2. Vaya a Red

Paso 3. Elegir interfaces

Paso 4. Haga clic en Edit Settings.

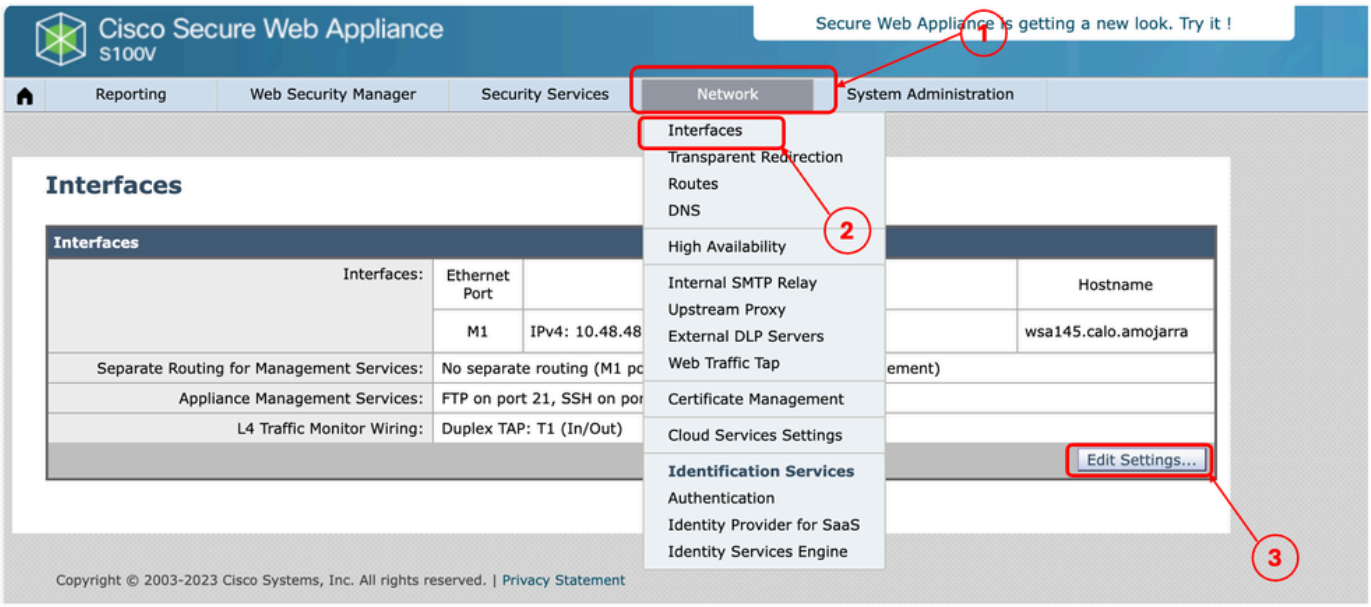


Imagen - Activar FTP en SWA

Paso 5. Active la casilla de verificación para FTP

Paso 6. Proporcione el número de puerto TCP para FTP (el puerto FTP predeterminado es 21)

Paso 7. Enviar y registrar cambios

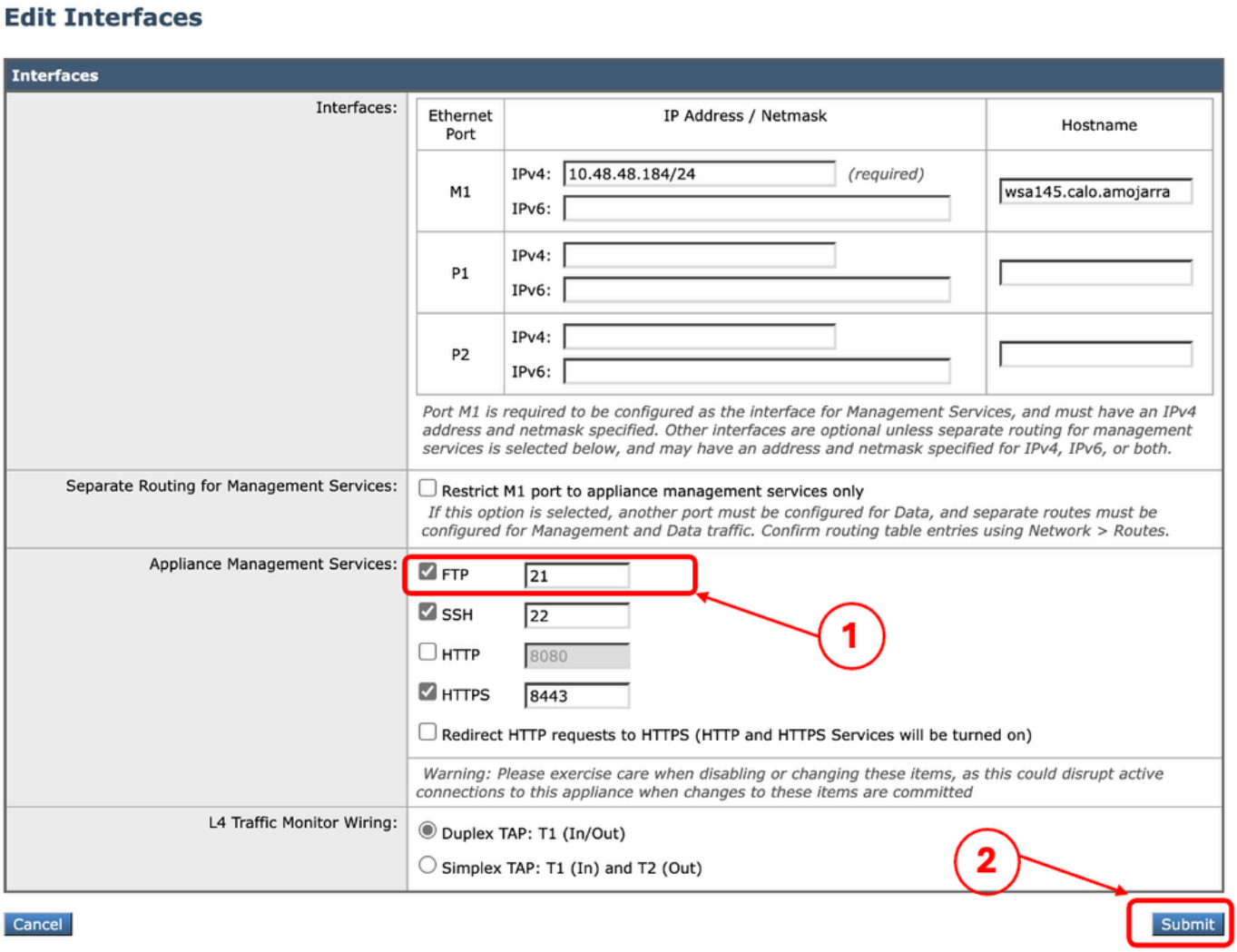


Imagen: Configuración del parámetro FTP en SWA

Información Relacionada

- Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance - LD (implementación limitada) - Solución de problemas...
- Configuración de registros push de SCP en un dispositivo web seguro con Microsoft Server - Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).