Logbestanden van beveiligde web-applicatie openen

Inhoud

Inleiding

Dit document beschrijft de methoden om de logs van Secure Web Appliance (SWA) te bekijken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Fysieke of virtuele SWA geïnstalleerd.
- Licentie geactiveerd of geïnstalleerd.
- Secure Shell-client (SSH).
- De setup-wizard is voltooid.
- Administratieve toegang tot de SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

SWA-logtypen

De Secure Web Applicatie registreert zijn eigen systeem- en verkeersbeheeractiviteiten door deze naar logbestanden te schrijven. Beheerders kunnen deze logbestanden raadplegen om het apparaat te bewaken en problemen op te lossen.

In deze tabel worden de logbestandstypen van Secure Web Appliance beschreven.

Type logbestand	Beschrijving	Ondersteunt Syslog Push?	Standaard ingeschakeld?
Logbestanden van Access Control Engine	Verslagen berichten met betrekking tot de de evaluatiemotor van de Proxy ACL van het Web (toegangscontrolelijst).	Nee	Nee
Secure Endpoint Engine-logbestanden	Registreer informatie over het scannen van de bestandsidentiteit en bestandsanalyse (Secure Endpoint).	Ja	Ja
Auditlogs	Records AAA-gebeurtenissen (verificatie, autorisatie en accounting). Registreert alle gebruikersinteractie met de toepassing en de opdrachtregelinterfaces, en legt toegezegde wijzigingen vast. Enkele details van het controlelogboek zijn als volgt: • Gebruiker - aanmelding • Gebruiker - Inloggen mislukt onjuist wachtwoord • Gebruiker - aanmelding mislukt onbekende gebruikersnaam • Gebruiker - aanmelding mislukt account verlopen • Gebruiker - Afmelden • Gebruiker - Lockout • Gebruiker - geactiveerd	Ja	Ja

Type logbestand	Beschrijving	Ondersteunt Syslog Push?	Standaard ingeschakeld?
	• Gebruiker - Wachtwoord wijzigen • Gebruiker - Wachtwoord opnieuw instellen • Gebruiker - Beveiligingsinstellingen/profielwijziging • Door gebruiker gemaakt • Gebruiker - Verwijderd/aangepast • Groep/Rol - Verwijdering / Aangepast • Groep/rol - wijzigingen in toegangsrechten		
Toegangslogboeken	Records Web Proxy client geschiedenis.	Ja	Ja
Logbestanden van ADC Engine Framework	Verslaat berichten met betrekking tot communicatie tussen de webproxy en de ADC-engine.	Nee	Nee
Logbestanden van ADC Engine	Records debuggen berichten van de ADC-engine.	Ja	Ja
Logbestanden van verificatiekader	Registreer authenticatiegeschiedenis en berichten.	Nee	Ja
AVC Engine Framework-logbestanden	Verslaat berichten met betrekking tot communicatie tussen de webproxy en de AVC-engine.	Nee	Nee
Logbestanden van AVC Engine	Records debuggen berichten van de AVC engine.	Ja	Ja
CLI-controlelogboeken	Registreert een historische controle van de interfaceactiviteit van de bevellijn.	Ja	Ja

Type logbestand	Beschrijving	Ondersteunt Syslog Push?	Standaard ingeschakeld?
Configuratielogboeken	Verslaat berichten met betrekking tot het Web Proxy configuratie management systeem.	Nee	Nee
Logboeken voor verbindingsbeheer	Verslaat berichten met betrekking tot het Web Proxy-verbindingsbeheersysteem.	Nee	Nee
Logbestanden voor gegevensbeveiliging	Registreert clientgeschiedenis voor uploadverzoeken die worden geëvalueerd door de Cisco Data Security Filters.	Ja	Ja
Logbestanden met gegevensbeveiligingsmodule	Registreert berichten die betrekking hebben op de Cisco-filters voor gegevensbeveiliging.	Nee	Nee
Logbestanden van DCA Engine Framework (Dynamische contentanalyse)	Registreert berichten met betrekking tot communicatie tussen de webproxy en de Cisco Web Usage Controls Dynamic Content Analysis engine.	Nee	Nee
Logbestanden van DCA Engine (Dynamische contentanalyse)	Registreert berichten met betrekking tot de Cisco Web Usage Controls Dynamic Content Analysis engine.	Ja	Ja
Standaard proxylogboeken	Verslaat fouten met betrekking tot de Web Proxy. Dit is de meest fundamentele van alle Web Proxy gerelateerde logs. Om meer specifieke aspecten met betrekking tot de Web Proxy problemen op te lossen, maak een logboekabonnement voor de toepasselijke Web Proxy module.	Ja	Ja

Type logbestand	Beschrijving	Ondersteunt Syslog Push?	Standaard ingeschakeld?
Logbestanden voor Disk Manager	Records Web Proxy-berichten met betrekking tot schrijven naar de cache op schijf.	Nee	Nee
Externe verificatielogboeken	Registreert berichten met betrekking tot het gebruik van de externe verificatiefunctie, zoals communicatiestoringen of een storing met de externe verificatieserver. Zelfs als externe verificatie is uitgeschakeld, bevat dit logbestand berichten over lokale gebruikers die met succes zijn aangemeld of die niet kunnen worden aangemeld.	Nee	Ja
Feedbacklogbestanden	Registreert de webgebruikers die onjuiste geclassificeerde pagina's melden.	Ja	Ja
Logbestanden met FTP-proxy	Registreer fout- en waarschuwingsberichten met betrekking tot de FTP-proxy.	Nee	Nee
Logbestanden van FTP-server	Registreert alle bestanden die zijn geüpload naar en gedownload van de Secure Web Applicatie met FTP.	Ja	Ja
GUI-logbestanden (Graphical User Interface - grafische gebruikersinterface)	De geschiedenis van records van pagina-vernieuwingen in de webinterface. De GUI-logboeken bevatten ook informatie over SMTP-transacties, bijvoorbeeld informatie over geplande rapporten die vanaf het apparaat worden verzonden.	Ja	Ja
Haystack logs	Haystack logboeken registreren web transactie tracking gegevensverwerking.	Ja	Ja
HTTPS-logbestanden	Verslagen Web Proxy-berichten specifiek voor de HTTPS Proxy (wanneer de HTTPS Proxy is ingeschakeld).	Nee	Nee

Type logbestand	Beschrijving	Ondersteunt Syslog Push?	Standaard ingeschakeld?
ISE-serverlogbestanden	Registreer ISE server(s) verbinding en operationele informatie.	Ja	Ja
Logbestanden van licentiemodule	Verslaat berichten met betrekking tot het licentie- en functiesleutelverwerkingssysteem van de webproxy.	Nee	Nee
Logbestanden van vastlegging-framework	Verslagen berichten met betrekking tot het het registrerensysteem van de Proxy van het Web.	Nee	Nee
Logbestanden	Registreer fouten met betrekking tot logboekbeheer.	Ja	Ja
Logbestanden van McAfee Integration Framework	Registreert berichten met betrekking tot communicatie tussen de Web Proxy en de McAfee scanning engine.	Nee	Nee
McAfee Logs	Registreer de status van anti-malware scanactiviteit van de McAfee scanning engine.	Ja	Ja
Logbestanden van Geheugenbeheer	Records Web Proxy-berichten met betrekking tot het beheer van al het geheugen, inclusief het in-memory cache voor het Web Proxy-proces.	Nee	Nee
Diverse logboeken voor proxymodules	Verslagen Web Proxy-berichten die meestal worden gebruikt door ontwikkelaars of klantenondersteuning.	Nee	Nee
AnyConnect beveiligde mobiliteitsdatamodellen	Registreert de interactie tussen de Secure Web Applicatie en de AnyConnect-client, inclusief de statuscontrole.	Ja	Ja

Type logbestand	Beschrijving	Ondersteunt Syslog Push?	Standaard ingeschakeld?
NTP-logbestanden (Network Time Protocol)	Registreert veranderingen in de systeemtijd die door het Protocol van de Tijd van het Netwerk worden gemaakt.	Ja	Ja
Logbestanden van PAC-bestandshosting bij Daemon	Records proxy auto-config (PAC) bestandsgebruik door clients.	Ja	Ja
Logbestanden voor proxyomleiding	Verslaat transacties die de Web Proxy omzeilen.	Nee	Ja
Rapportagelogboeken	Registreer een geschiedenis van rapportgeneratie.	Ja	Ja
Rapportage van zoekopdrachten	Vermeld fouten met betrekking tot het genereren van rapporten.	Ja	Ja
Debug-logbestanden aanvragen	Registreer zeer gedetailleerde debug informatie over een specifieke HTTP-transactie van alle webmodulelogtypen. Het is aan te raden om dit logabonnement te maken om een proxyprobleem met een bepaalde transactie op te lossen zonder alle andere proxylogabonnementen te maken. Opmerking: u kunt dit logabonnement alleen in de CLI maken.	Nee	Nee
Autorisatielogboeken	Registreert berichten met betrekking tot de functie Toegangsbeheer.	Ja	Ja
SHD-logbestanden (System Health Daemon)	registreert een geschiedenis van de gezondheid van systeemdiensten en een geschiedenis van onverwachte daemon herstart.	Ja	Ja
SNMP-logbestanden	Records debuggen berichten met	Ja	Ja

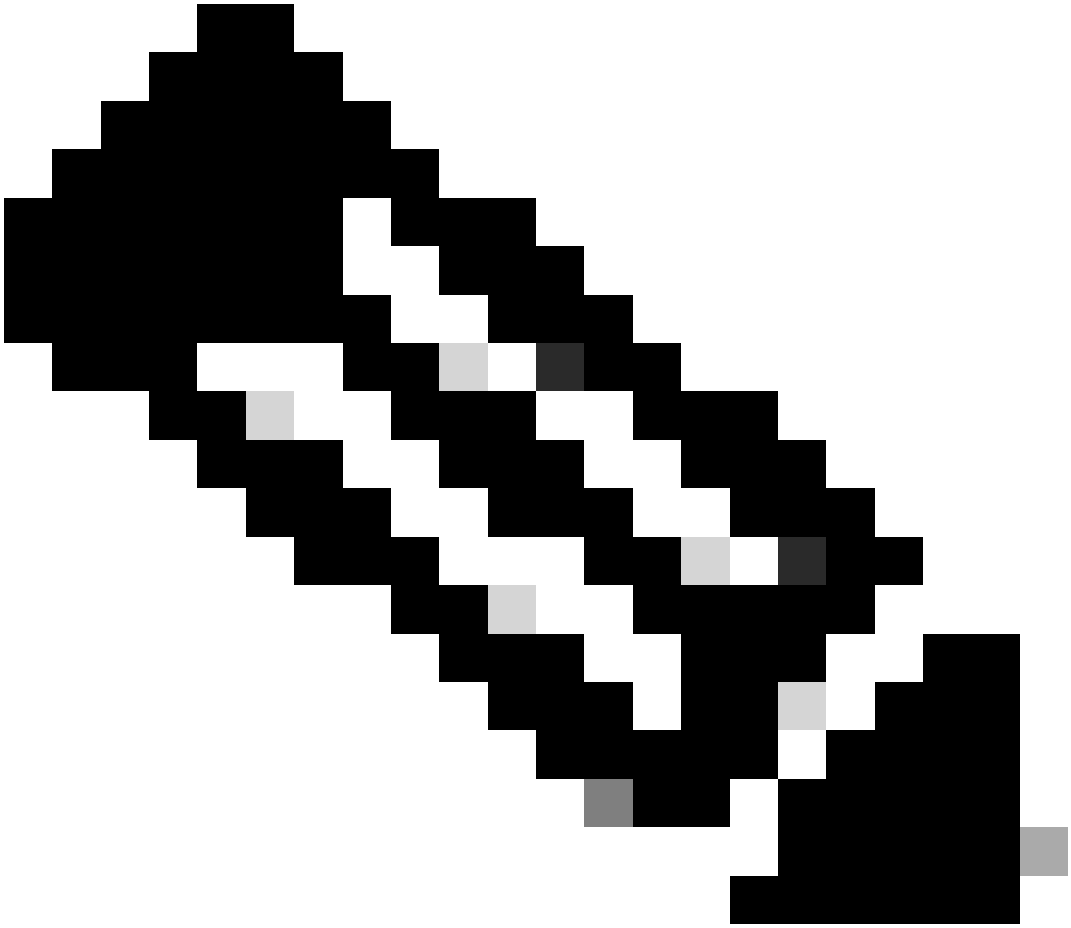
Type logbestand	Beschrijving	Ondersteunt Syslog Push?	Standaard ingeschakeld?
	betrekking tot de SNMP-netwerkbeheerengine.		
Logboeken voor SNMP-module	Registreert webproxyberichten met betrekking tot interactie met het SNMP-bewakingssysteem.	Nee	Nee
Logbestanden van Sophos-integratiekader	Verslaat berichten met betrekking tot communicatie tussen de Web Proxy en de Sophos scanning engine.	Nee	Nee
Sophos Logs	Registreer de status van anti-malware scanactiviteit van de Sophos scanning engine.	Ja	Ja
Statuslogboeken	Registreer informatie met betrekking tot het systeem, zoals downloaden van functiesleutels.	Ja	Ja
Systeemlogbestanden	Registreert DNS, fout, en begaat activiteit.	Ja	Ja
Foutlogboeken voor Traffic Monitor	Records L4TM interface en opname fouten.	Ja	Ja
Logboeken voor verkeersmonitor	Verslagen sites toegevoegd aan het L4TM blok en toestaan lijsten.	Nee	Ja
UDS-logbestanden (Gebruikersdetectieservice)	Verslaat gegevens over hoe de Web Proxy de gebruikersnaam ontdekt zonder daadwerkelijke verificatie te doen. Het bevat informatie over de interactie met het Cisco adaptieve security applicatie voor beveiligde mobiliteit en over de integratie met de Novell eDirectory-server voor transparante gebruikersidentificatie.	Ja	Ja

Type logbestand	Beschrijving	Ondersteunt Syslog Push?	Standaard ingeschakeld?
Updaterlogbestanden	Registreer een geschiedenis van WBRS en andere updates.	Ja	Ja
W3C-logs	Registreert de cliëntgeschiedenis van de Proxy van het Web in een W3C volgzaam formaat. Meer informatie.	Ja	Nee
WBNP-logbestanden (SensorBase-netwerkdeelname)	Registreert een geschiedenis van de deelname van Cisco SensorBase Network geüpload naar het SensorBase-netwerk.	Nee	Ja
WBRS-framelogboeken (Webreputatiescore)	Verslaat berichten met betrekking tot communicatie tussen de webproxy en de webreputatiefilters.	Nee	Nee
WCCP-modulelogboeken	Records Web Proxy-berichten met betrekking tot de implementatie van WCCP.	Nee	Nee
Logbestanden van webcat-integratiekader	Registreert berichten met betrekking tot communicatie tussen de webproxy en de URL-filtreerengine die aan Cisco Web Usage Controls is gekoppeld.	Nee	Nee
Logbestanden van Webroot-integratiekader	Registreert berichten met betrekking tot communicatie tussen de Web Proxy en de Webroot scanengine.	Nee	Nee
Webroot Logs	Registreer de status van anti-malware scanactiviteit van de Webroot scanning engine.	Ja	Ja
Logboeken voor welkomstpagina-bevestiging	Registreer een geschiedenis van webclients die op de knop Akkoord op de pagina van de eindgebruikersbevestiging klikken.	Ja	Ja

Logbestanden bekijken

Standaard worden de logbestanden lokaal opgeslagen in de SWA, kunt u de lokaal opgeslagen logbestanden via GUI downloaden of de logbestanden van CLI bekijken.

Logbestanden downloaden via GUI



> Opmerking: FTP moet op het apparaat zijn ingeschakeld. Als u FTP wilt inschakelen, raadpleegt u in dit artikel FTP inschakelen op Secure Web Applicatie.

U kunt de logbestanden downloaden via GUI:

Stap 1. Inloggen op GUI

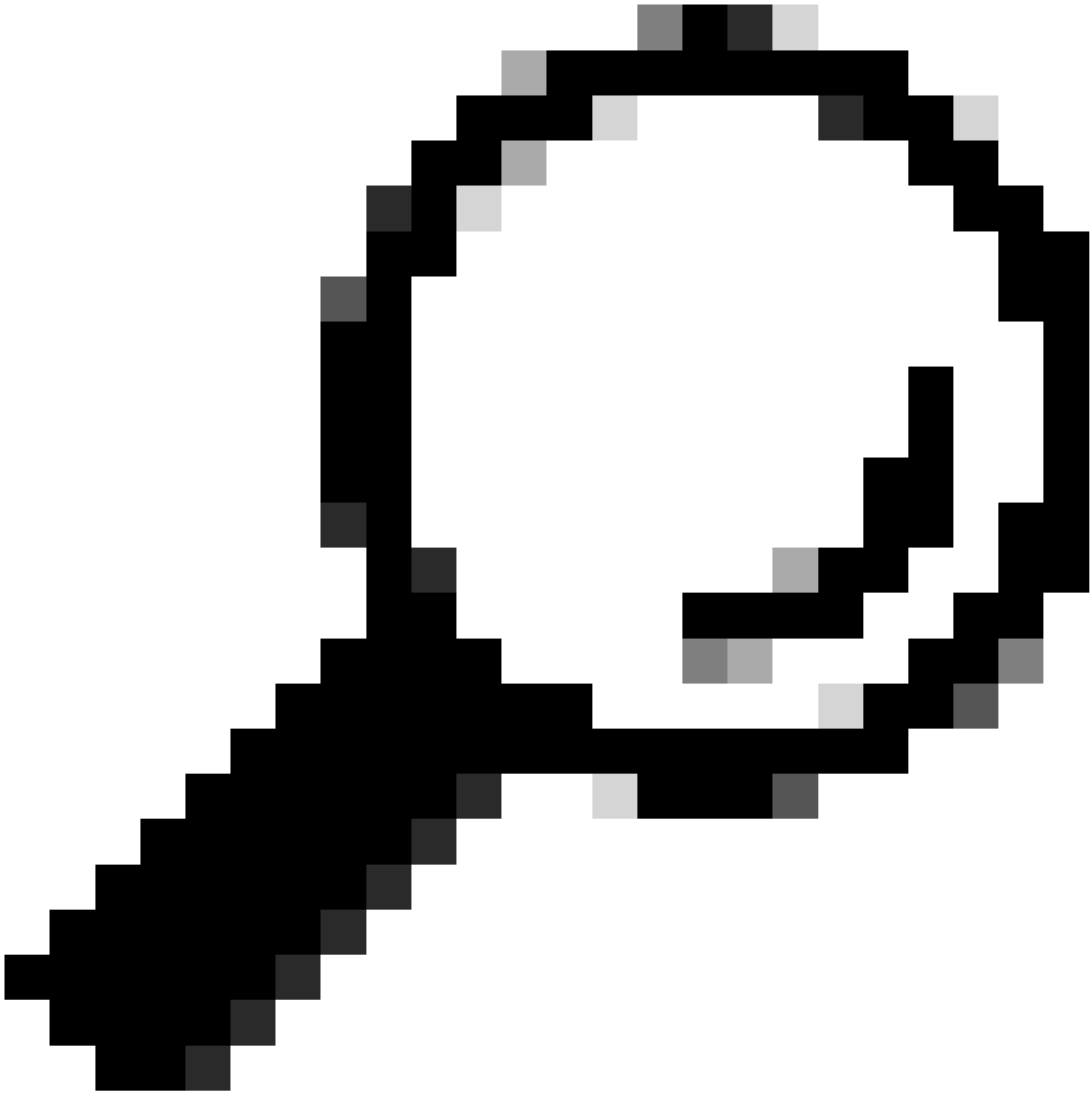
Stap 2. Navigeren naar systeembeheer

Stap 3. Logabonnementen kiezen

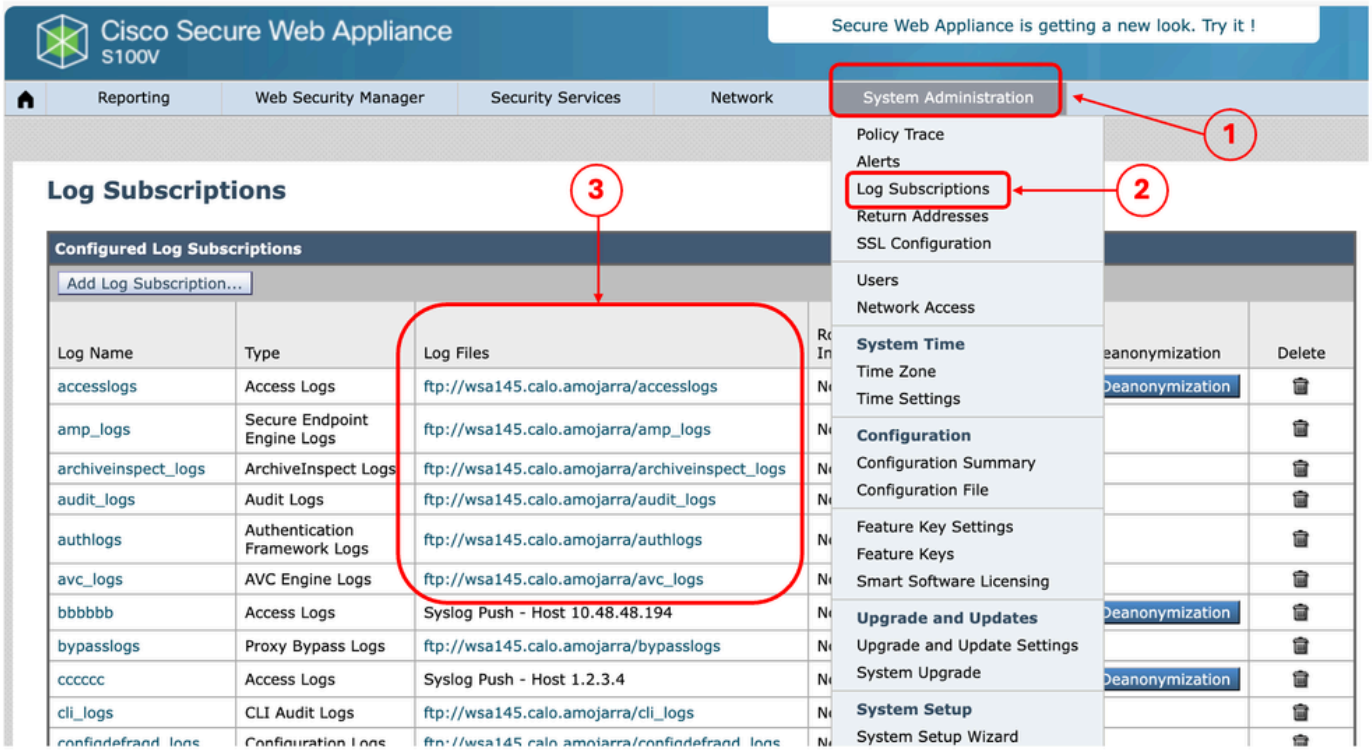
Stap 4.Klik op de naam van het logabonnement in de kolom Logbestanden van de lijst met logabonnementen.

Stap 5.Voer wanneer hierom wordt gevraagd de gebruikersnaam en het wachtwoord in voor toegang tot het apparaat.

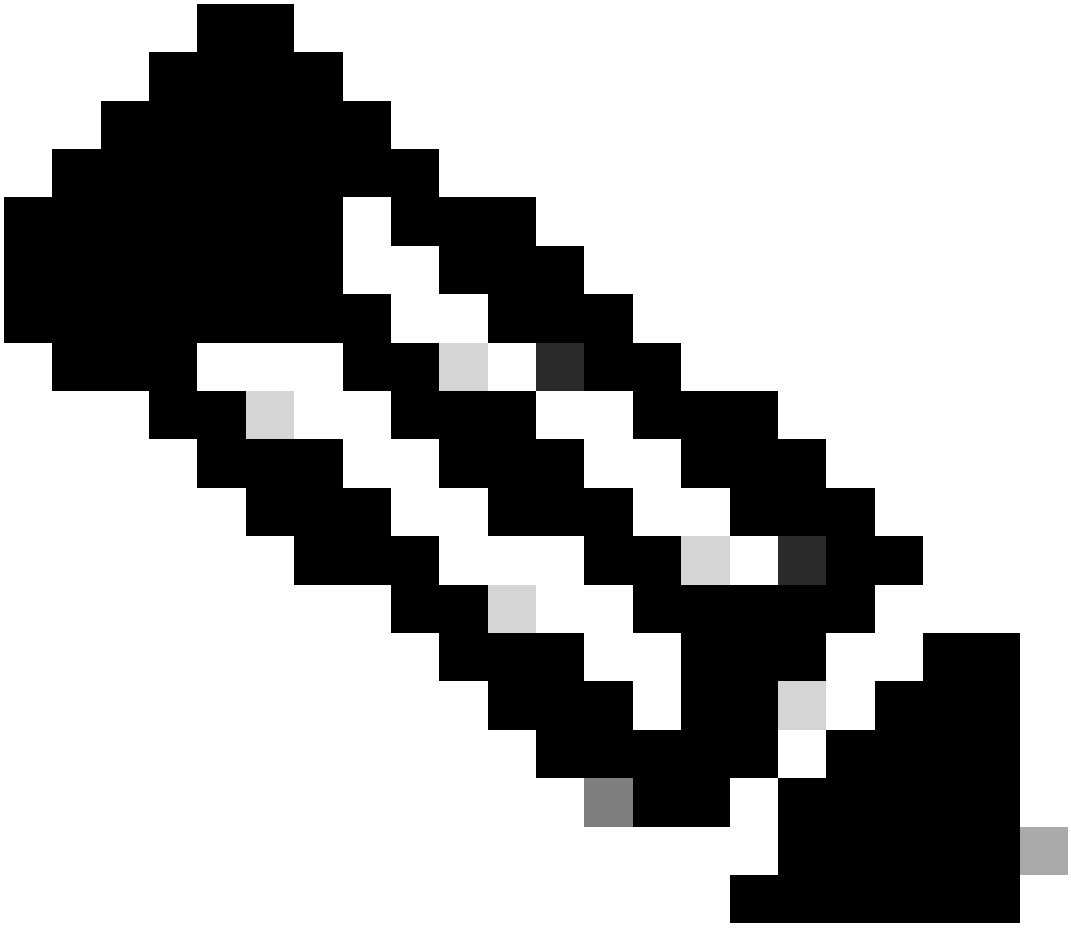
Stap 6.Na het inloggen klik op een van de logbestanden om deze in uw browser te bekijken of op schijf op te slaan.



Tip: Verfris de browser voor bijgewerkte resultaten.



Afbeelding - Logbestanden downloaden



Opmerking: als een logabonnement wordt gecomprimeerd, downloaden, decompresseren en vervolgens openen.

Logboeken van CLI bekijken

U kunt de logbestanden van CLI bekijken. In dit geval kunt u toegang hebben tot bewegende logbestanden of filteren op een trefwoord in de logbestanden.

Stap 1. Connect met CLI

Stap 2. Typ grep en druk op ENTER.

Stap 3. Geef het nummer op van het logbestand dat u wilt bekijken

Stap 4. (optioneel) U kunt het uitvoersignaal filteren door een reguliere expressie of een woord te definiëren. Druk vervolgens op ENTER

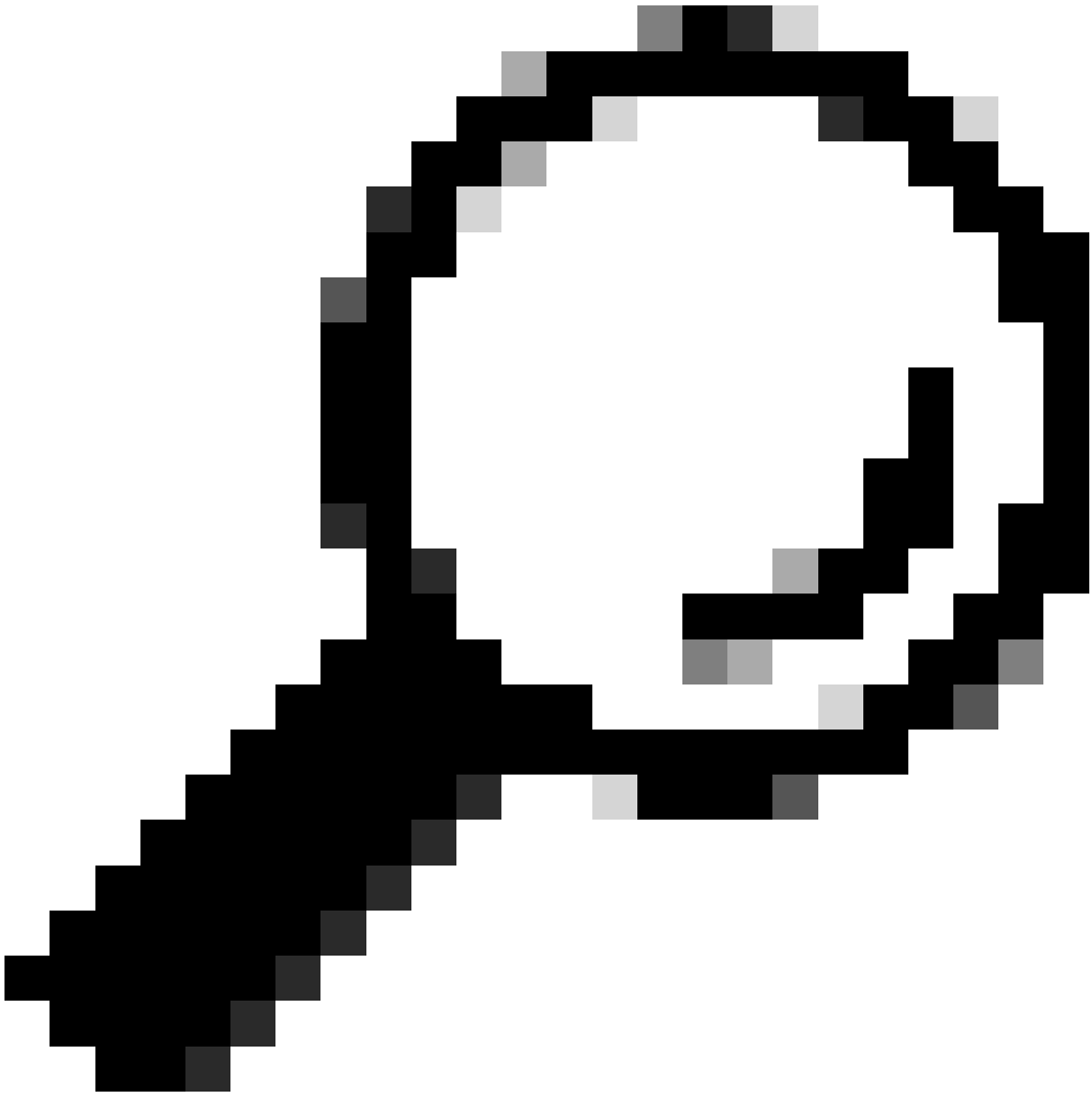
Stap 5. Als u de zoekfunctie nodig hebt voor het trefwoord dat in Stap 4 is ingevoerd, om case

ongevoelig te zijn, drukt u op ENTER in "Wilt u dat deze zoekactie hoofdletterongevoelig is? [Y]>" anders type "N" en druk op ENTER.

Stap 6. Als u uw trefwoord van zoekopdracht wilt uitsluiten, typt u "Y" in "Wilt u zoeken naar niet-overeenkomende regels? [N]>" Druk anders op ENTER.

Stap 7. Als u live logs wilt bekijken, typt u "Y" in "Wilt u de logs volgen? [N]>", drukt u anders op ENTER.

Stap 8. Als u de logbestanden wilt pagineren om ze pagina per paginatype "Y" in "Wilt u de uitvoer pagineren? [N]>" , drukt u op ENTER.



Tip: Als u ervoor kiest om te pagineren, kunt u de logs afsluiten door op "q" te drukken

---

Hier is een voorbeelduitvoer die alle regels toont met 'Waarschuwing' in:

```
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]>
```

FTP op beveiligde web-applicatie inschakelen

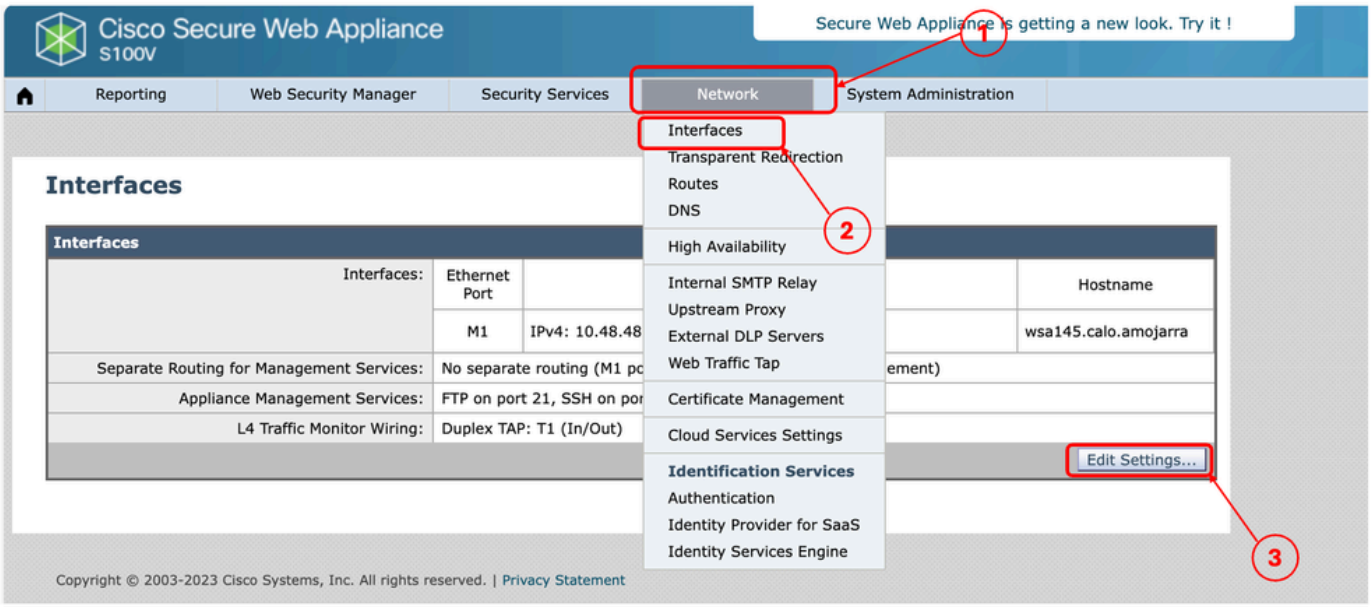
Standaard is FTP niet ingeschakeld op de SWA. Zo schakelt FTP in:

Stap 1. Inloggen op GUI

Stap 2. Naar netwerk navigeren

Stap 3. Interfaces kiezen

Stap 4. Klik op Instellingen bewerken.

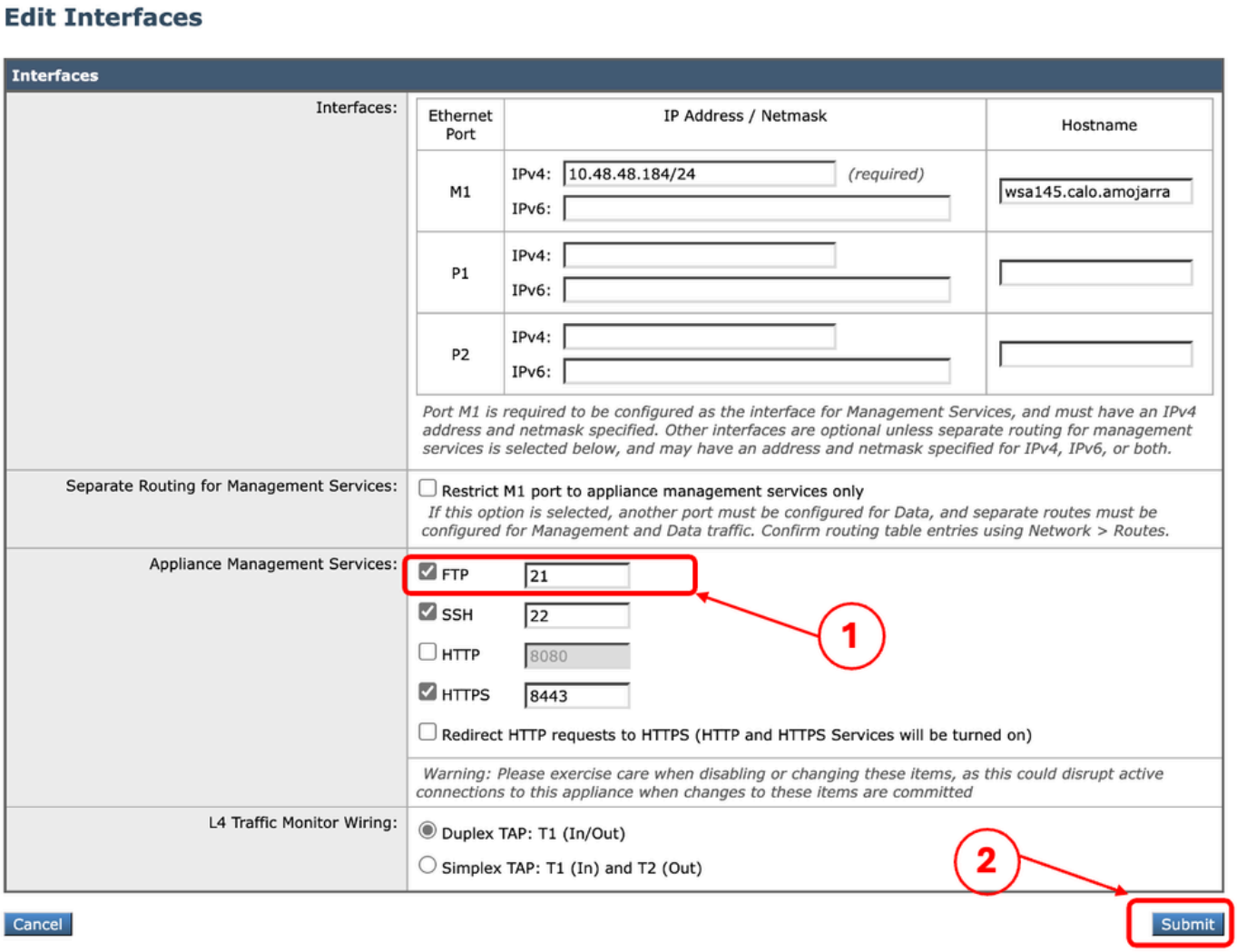


Afbeelding - FTP op SWA inschakelen

Stap 5. Selecteer het aankruisvakje voor FTP.

Stap 6. Geef het TCP poortnummer op voor FTP (de standaard FTP-poort is 21)

Stap 7. Wijzigingen verzenden en vastleggen



Afbeelding - FTP-parameter configureren in SWA

Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Applicatie - LD (Beperkte implementatie) - Probleemoplossing...]
- [SCP Push Logs in Secure Web Applicatie configureren met Microsoft Server - Cisco]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.