Logbestanden downloaden vanuit de GUI van uw CES ESA en CMD

Inhoud

Inleiding

Dit document beschrijft hoe u logbestanden kunt downloaden via de grafische gebruikersinterface (GUI) van uw Secure Email Cloud Gateway (CES) via Command Line (CMD).

Voorwaarden

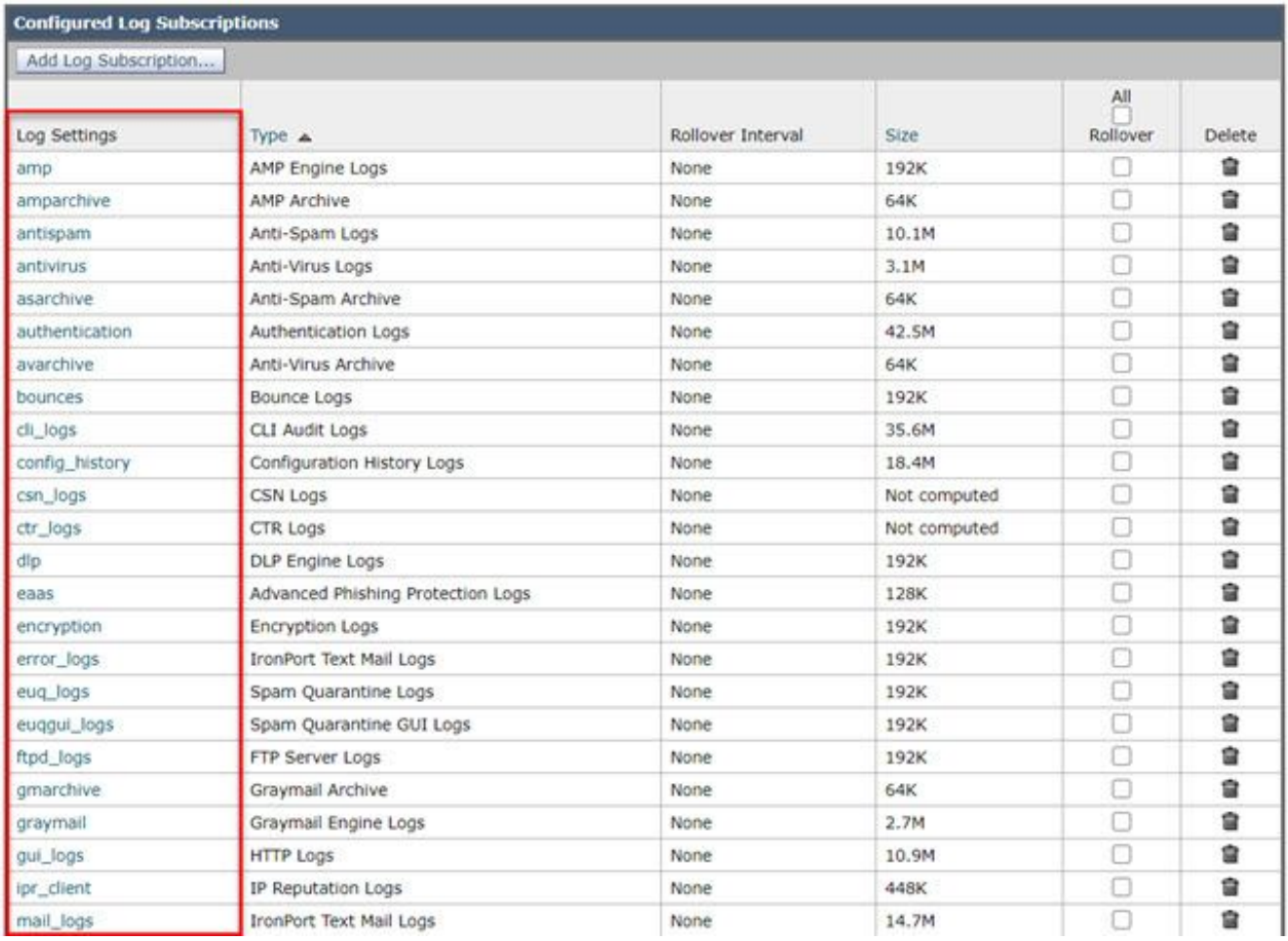
Een gebruikersaccount met toestemming van de beheerder of cloudbeheerder.

Logboeken downloaden vanuit de GUI

1. Log in op de GUI van uw CES Email Security Applicatie (ESA) en navigeer naar **Systeembeheer > Abonnementen.**

2. Merk de URL op die in uw browser wordt gezien (Voorbeeld: Systeembeheerlogabonnementen)

3. Vervolgens moet u de kolom **Loginstellingen** bekijken en een logbestand zoeken dat u wilt downloaden. Gebruik bij dit voorbeeld **mail_logs**.



Configured Log Subscriptions

Add Log Subscription...

Log Settings	Type ▲	Rollover Interval	Size	All Rollover	Delete
amp	AMP Engine Logs	None	192K	☐	🗑
amparchive	AMP Archive	None	64K	☐	🗑
antispam	Anti-Spam Logs	None	10.1M	☐	🗑
antivirus	Anti-Virus Logs	None	3.1M	☐	🗑
asarchive	Anti-Spam Archive	None	64K	☐	🗑
authentication	Authentication Logs	None	42.5M	☐	🗑
avarchive	Anti-Virus Archive	None	64K	☐	🗑
bounces	Bounce Logs	None	192K	☐	🗑
cli_logs	CLI Audit Logs	None	35.6M	☐	🗑
config_history	Configuration History Logs	None	18.4M	☐	🗑
csn_logs	CSN Logs	None	Not computed	☐	🗑
ctr_logs	CTR Logs	None	Not computed	☐	🗑
dlp	DLP Engine Logs	None	192K	☐	🗑
eaas	Advanced Phishing Protection Logs	None	128K	☐	🗑
encryption	Encryption Logs	None	192K	☐	🗑
error_logs	IronPort Text Mail Logs	None	192K	☐	🗑
euq_logs	Spam Quarantine Logs	None	192K	☐	🗑
euqgui_logs	Spam Quarantine GUI Logs	None	192K	☐	🗑
ftpd_logs	FTP Server Logs	None	192K	☐	🗑
gmarchive	Graymail Archive	None	64K	☐	🗑
graymail	Graymail Engine Logs	None	2.7M	☐	🗑
gui_logs	HTTP Logs	None	10.9M	☐	🗑
ipr_client	IP Reputation Logs	None	448K	☐	🗑
mail_logs	IronPort Text Mail Logs	None	14.7M	☐	🗑

4. Neem de URL uit stap 2 en maak de wijzigingen:

a. Verwijder /log_abonnementen.

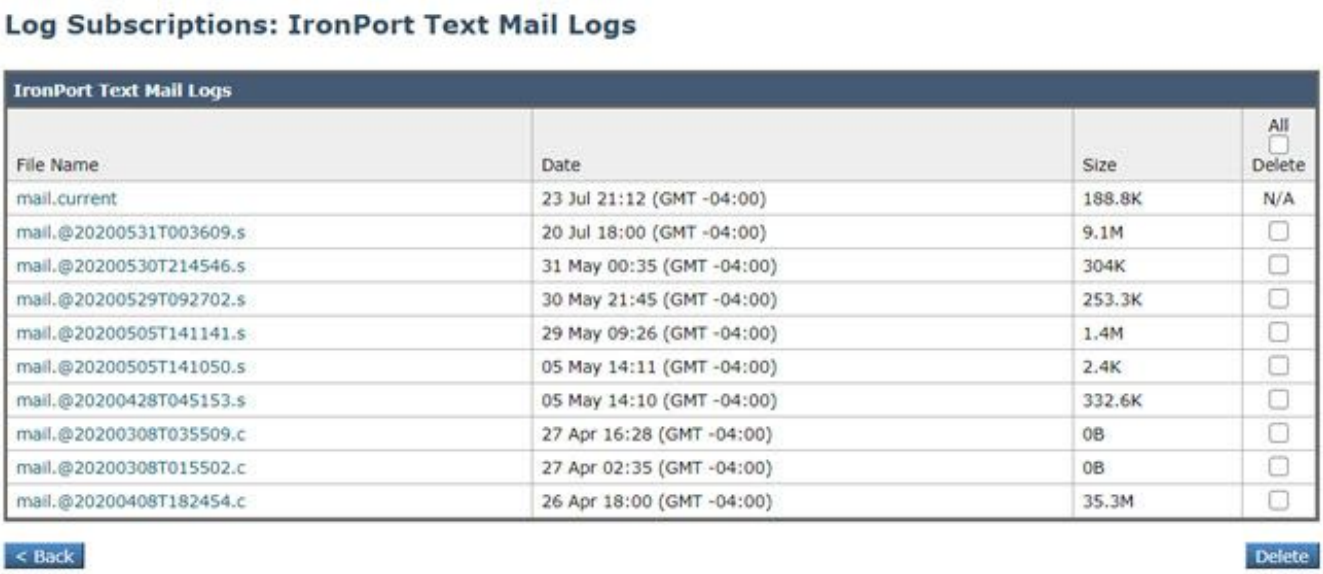
b. Voeg /log_list?log_type=<logname> toe aan het einde van de URL, waar <logname> wordt vervangen door wat wordt weergegeven onder de **loginstellingen**

kolom.

c. Vervang dhXXXX-esa1.iphmx.com door de volledig gekwalificeerde domeinnaam (FQDN) van uw ESA.

Opmerking: Om mail_logs als voorbeeld te gebruiken, worden systeembeheerlogabonnementen omgevormd tot systeembeheerloglijst.

5. Ga tot slot naar de aangepaste URL en log in. U zou naar een pagina komen gelijkend op wat in beeld wordt getoond waar u dan een dossier kunt klikken, downloaden en het opslaan.

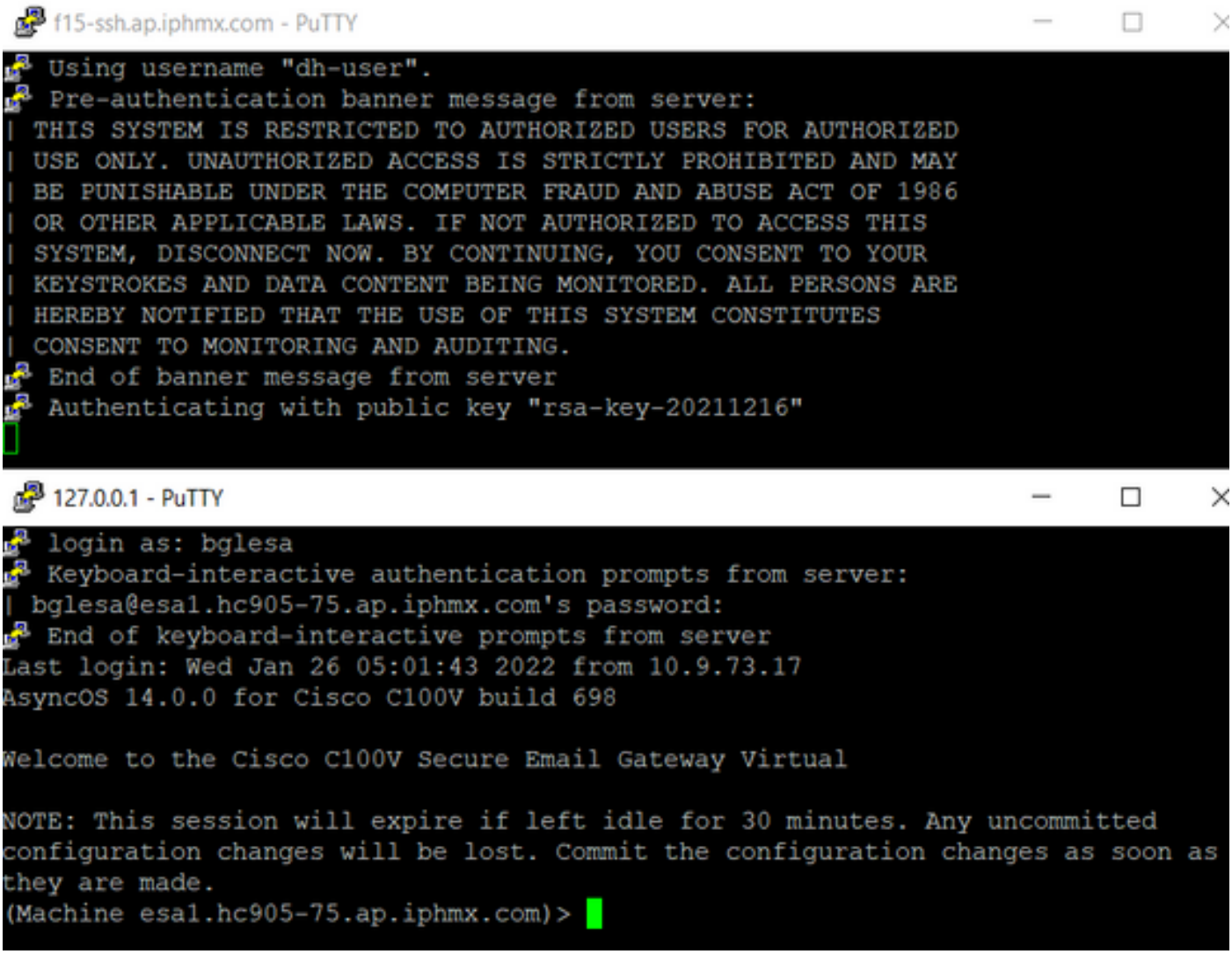


Logbestanden downloaden vanaf CMD

Zorg ervoor dat u de CLI Access van de CES ESA hebt. Raadpleeg het artikel Customer CLI Access voor stappen om CLI-toegang aan te vragen.

Het gebruik van Putty SCP (PSCP) heeft SSH-toegang om de logbestanden te kunnen ophalen:

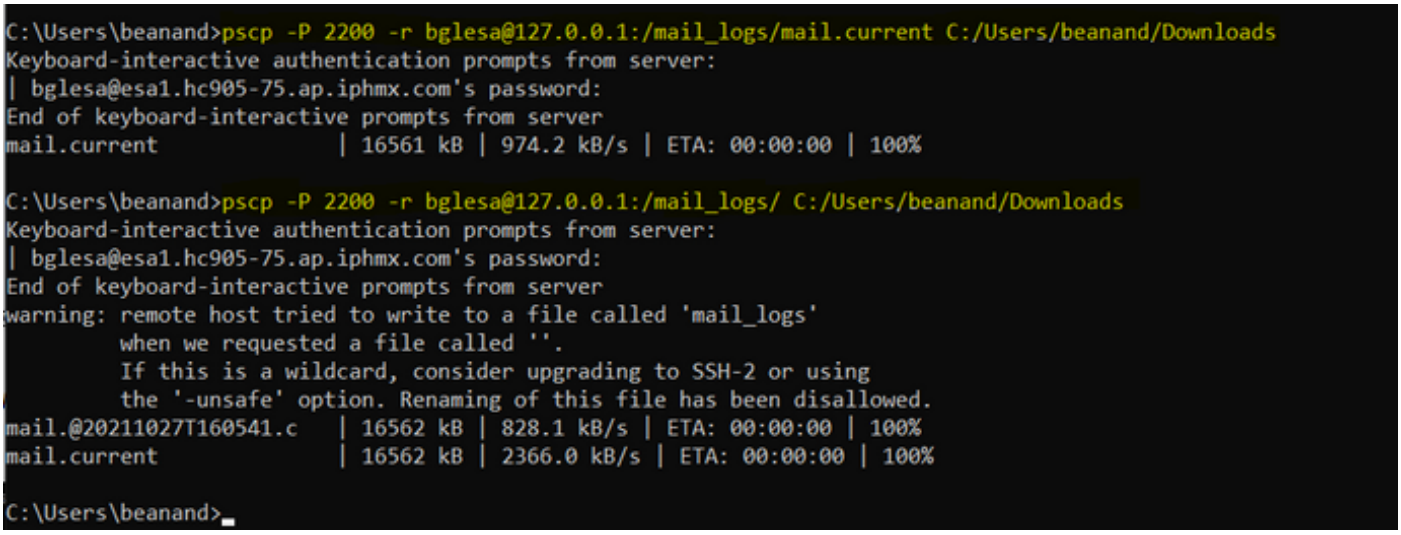
1. PSCP downloaden PuTTY
2. Open de proxyconfiguratie die op ESA is ingeschakeld en laat de proxy open.



3. Start CMD en type: **pscp -P-poort -r <gebruiker>@localhost:/mail_logs/* /path/on/local/system**

1. Port is de poort die eerder is geconfigureerd voor CLI-toegang.
2. /mail_logs/ betekent dat het alle bestanden onder die specifieke map downloadt.
3. Als alleen het huidige bestand gedownload moet worden, typt u /mail_logs/mail.current of het logbestand dat vereist is.
4. Voer het wachtwoord in als hierom wordt gevraagd zodra de opdracht is ingevoerd.

Opdracht Voorbeeld: **pscp -P 2200 -r admin@127.0.0.1:/mail_logs/ C:/users/beanand/downloads**



Gerelateerde informatie

- Cisco e-mail security applicatie – eindgebruikershandleiding

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.