

Logbestanden downloaden vanuit de GUI van uw CES ESA en CMD

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Logboeken downloaden vanuit de GUI](#)

[Logbestanden downloaden vanaf CMD](#)

[Gerelateerde informatie](#)

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

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.

Log Subscriptions: IronPort Text Mail Logs

IronPort Text Mail Logs			
File Name	Date	Size	All <input type="checkbox"/> Delete
mail.current	23 Jul 21:12 (GMT -04:00)	188.8K	N/A
mail.@20200531T003609.s	20 Jul 18:00 (GMT -04:00)	9.1M	<input type="checkbox"/>
mail.@20200530T214546.s	31 May 00:35 (GMT -04:00)	304K	<input type="checkbox"/>
mail.@20200529T092702.s	30 May 21:45 (GMT -04:00)	253.3K	<input type="checkbox"/>
mail.@20200505T141141.s	29 May 09:26 (GMT -04:00)	1.4M	<input type="checkbox"/>
mail.@20200505T141050.s	05 May 14:11 (GMT -04:00)	2.4K	<input type="checkbox"/>
mail.@20200428T045153.s	05 May 14:10 (GMT -04:00)	332.6K	<input type="checkbox"/>
mail.@20200308T035509.c	27 Apr 16:28 (GMT -04:00)	0B	<input type="checkbox"/>
mail.@20200308T015502.c	27 Apr 02:35 (GMT -04:00)	0B	<input type="checkbox"/>
mail.@20200408T182454.c	26 Apr 18:00 (GMT -04:00)	35.3M	<input type="checkbox"/>

< Back Delete

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.

```
f15-ssh.ap.iphmx.com - PuTTY
Using username "dh-user".
Pre-authentication banner message from server:
| THIS SYSTEM IS RESTRICTED TO AUTHORIZED USERS FOR AUTHORIZED
| USE ONLY. UNAUTHORIZED ACCESS IS STRICTLY PROHIBITED AND MAY
| BE PUNISHABLE UNDER THE COMPUTER FRAUD AND ABUSE ACT OF 1986
| OR OTHER APPLICABLE LAWS. IF NOT AUTHORIZED TO ACCESS THIS
| SYSTEM, DISCONNECT NOW. BY CONTINUING, YOU CONSENT TO YOUR
| KEYSTROKES AND DATA CONTENT BEING MONITORED. ALL PERSONS ARE
| HEREBY NOTIFIED THAT THE USE OF THIS SYSTEM CONSTITUTES
| CONSENT TO MONITORING AND AUDITING.
End of banner message from server
Authenticating with public key "rsa-key-20211216"
```

```
127.0.0.1 - PuTTY
login as: bglesa
Keyboard-interactive authentication prompts from server:
| bglesa@esa1.hc905-75.ap.iphmx.com's password:
End of keyboard-interactive prompts from server
Last login: Wed Jan 26 05:01:43 2022 from 10.9.73.17
AsyncOS 14.0.0 for Cisco C100V build 698

Welcome to the Cisco C100V Secure Email Gateway Virtual

NOTE: This session will expire if left idle for 30 minutes. Any uncommitted
configuration changes will be lost. Commit the configuration changes as soon as
they are made.
(Machine esa1.hc905-75.ap.iphmx.com)>
```

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`

```
C:\Users\beanand>pscp -P 2200 -r bglesa@127.0.0.1:/mail_logs/mail.current C:/Users/beanand/Downloads
Keyboard-interactive authentication prompts from server:
| bglesa@esa1.hc905-75.ap.iphmx.com's password:
End of keyboard-interactive prompts from server
mail.current | 16561 kB | 974.2 kB/s | ETA: 00:00:00 | 100%

C:\Users\beanand>pscp -P 2200 -r bglesa@127.0.0.1:/mail_logs/ C:/Users/beanand/Downloads
Keyboard-interactive authentication prompts from server:
| bglesa@esa1.hc905-75.ap.iphmx.com's password:
End of keyboard-interactive prompts from server
warning: remote host tried to write to a file called 'mail_logs'
when we requested a file called ''.
If this is a wildcard, consider upgrading to SSH-2 or using
the '-unsafe' option. Renaming of this file has been disallowed.
mail.@20211027T160541.c | 16562 kB | 828.1 kB/s | ETA: 00:00:00 | 100%
mail.current | 16562 kB | 2366.0 kB/s | ETA: 00:00:00 | 100%

C:\Users\beanand>
```

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.