

Scaricare i log dalla GUI di CES ESA e CMD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Download dei log dalla GUI](#)

[Download dei log da CMD](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come scaricare i log dall'interfaccia grafica utente (GUI) del Secure Email Cloud Gateway (CES) tramite la riga di comando (CMD).

Prerequisiti

Account utente con autorizzazione Amministratore o Amministratore cloud.

Download dei log dalla GUI

1. Accedere alla GUI dell'istanza di CES Email Security Appliance (ESA) e selezionare **Amministrazione sistema > Registra sottoscrizioni**.
2. Si noti l'URL visualizzato nel browser (ad esempio: [Sottoscrizioni ai log di amministrazione del sistema](#))
3. Quindi, è necessario rivedere la colonna **Impostazioni log** e trovare un log che si desidera scaricare. Per questo esempio, utilizzare **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. Prendere l'URL dal secondo passaggio e apportare le modifiche:

r. Rimuovere /log_subscriptions.

b. Aggiungere /log_list?log_type=<logname> alla fine dell'URL, dove <logname> viene sostituito con quanto visualizzato in **Impostazioni registro**

colonna.

c. Sostituire dhXXXX-esa1.iphmx.com con il nome di dominio completo (FQDN) dell'ESA.

Nota: per utilizzare mail_logs come esempio, le [sottoscrizioni dei log di amministrazione del sistema](#) diventano [elenco dei log di amministrazione del sistema](#).

5. Infine, selezionare l'URL modificato e accedere. Viene visualizzata una pagina simile a quella mostrata nell'immagine in cui è possibile fare clic su un file, scaricarlo e salvarlo.

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

Download dei log da CMD

accertarsi di disporre dell'accesso CLI di CES ESA. Per la procedura di richiesta dell'accesso alla CLI, fare riferimento all'articolo [Accesso alla CLI del cliente](#).

Si consiglia di utilizzare Putty SCP (PSCP) deve avere accesso SSH per estrarre i log:

1. Scarica PSCP [Scarica PuTTY](#)
2. Aprire la configurazione proxy abilitata su ESA, quindi lasciare il proxy aperto.

```
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@esal.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 esal.hc905-75.ap.iphmx.com)>
```

3. Eseguire CMD e digitare: **pscp -P porta -r <utente>@localhost:/mail_logs/* /path/on/local/system**

1. La porta è quella precedentemente configurata per l'accesso dalla CLI.
2. /mail_logs/ indica che verranno scaricati tutti i file contenuti nella cartella specificata.
3. Se è necessario scaricare solo il file corrente, digitare /mail_logs/mail.current o il registro necessario.
4. Immettere la password quando richiesto dopo l'immissione del comando.

Comando di esempio: **pscp -P 2200 -r admin@127.0.0.1:/mail_logs/ C:/Users/band/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>_
```

Informazioni correlate

- [Cisco Email Security Appliance - Guide per l'utente](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).