

Téléchargez les journaux depuis l'interface graphique de votre ESA CES et de votre CMD

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Télécharger les journaux depuis l'interface graphique](#)

[Télécharger les journaux depuis CMD](#)

[Informations connexes](#)

Introduction

Ce document décrit comment télécharger des journaux à partir de l'interface graphique utilisateur (GUI) de votre passerelle de cloud de messagerie sécurisée (CES) via la ligne de commande (CMD).

Conditions préalables

Un compte d'utilisateur avec l'autorisation Administrateur ou Administrateur cloud.

Télécharger les journaux depuis l'interface graphique

1. Connectez-vous à l'interface utilisateur graphique de votre instance ESA (Email Security Appliance) CES et accédez à **Administration système > Inscriptions au journal**.
2. Notez l'URL affichée dans votre navigateur (Exemple : [Abonnements au journal d'administration du système](#))
3. Ensuite, vous devez passer en revue la colonne **Log Settings** et trouver un journal que vous souhaitez télécharger. Pour cet exemple, utilisez **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. Prenez l'URL de l'étape deux et effectuez les modifications suivantes :

a. Supprimez /log_subscriptions.

b. Ajoutez /log_list?log_type=<nom_journal> à la fin de l'URL, où <nom_journal> est remplacé par ce qui est affiché sous les **paramètres de journal** colonne.

c. Remplacez dhXXXX-esa1.iphmx.com par le nom de domaine complet (FQDN) de votre ESA.

Remarque : pour utiliser mail_logs comme exemple, [System Administration Log Subscriptions](#) devient [System Administration Log List](#).

5. Enfin, accédez à l'URL modifiée et connectez-vous. Vous accédez à une page similaire à celle de l'image, où vous pouvez cliquer sur un fichier, le télécharger et l'enregistrer.

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

Télécharger les journaux depuis CMD

Assurez-vous que vous disposez de l'accès CLI de l'ESA CES. Pour connaître les étapes à suivre pour demander un accès à l'interface de ligne de commande, consultez l'article [Accès à l'interface de ligne de commande client](#).

Il est recommandé d'utiliser Putty SCP (PSCP) pour avoir un accès SSH afin d'extraire les journaux :

1. Télécharger PSCP [Télécharger PuTTY](#)
2. Ouvrez la configuration de proxy activée sur ESA et laissez le proxy ouvert.

```
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. Exécutez CMD et tapez : `pscp -P port -r <user>@localhost:/mail_logs/* /path/on/local/system`

1. Le port est celui qui est précédemment configuré pour l'accès CLI.
2. `/mail_logs/` signifie qu'il télécharge tous les fichiers sous ce dossier particulier.
3. Si seul le fichier actuel doit être téléchargé, tapez `/mail_logs/mail.current` ou le journal requis.
4. Entrez le mot de passe lorsque vous y êtes invité une fois la commande entrée.

Exemple de commande : `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>_
```

Informations connexes

- [Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.