

Descargue los registros de la GUI de su ESA CES y CMD

Contenido

[Introducción](#)

[Prerequisites](#)

[Descargar registros desde la GUI](#)

[Descargar registros de CMD](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo descargar registros desde la interfaz gráfica de usuario (GUI) de Secure Email Cloud Gateway (CES) a través de la línea de comandos (CMD).

Prerequisites

Cuenta de usuario con permiso de administrador o administrador de la nube.

Descargar registros desde la GUI

1. Inicie sesión en la GUI de su instancia de CES Email Security Appliance (ESA) y navegue hasta **Administración del sistema > Registrar suscripciones**.
2. Observe la dirección URL que aparece en el explorador (por ejemplo, [Suscripciones a registros de administración del sistema](#))
3. A continuación, debe revisar la columna **Log Settings** y buscar un registro que desee descargar. Para este ejemplo, utilice **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. Tome la URL del paso dos y haga las modificaciones:

a. Quite /log_subscriptions.

b. Anexe /log_list?log_type=<nombre de inicio de sesión> al final de la URL, donde <nombre de inicio de sesión> se reemplaza por lo que se muestra en **Configuración de registro**

columna.

c. Sustituya dhXXXX-esa1.ipmx.com por el nombre de dominio completo (FQDN) de su ESA.

Nota: Para utilizar mail_logs como ejemplo, [System Administration Log Subscriptions](#) se convierte en [System Administration Log List](#).

5. Por último, navegue hasta la URL modificada e inicie sesión. Llegaría a una página similar a la que se muestra en la imagen, donde puede hacer clic en un archivo, descargarlo y guardarlo.

Log Subscriptions: IronPort Text Mail Logs

IronPort Text Mail Logs			
File Name	Date	Size	All 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

Descargar registros de CMD

Asegúrese de que dispone del acceso CLI del ESA CES. Para conocer los pasos para solicitar el acceso CLI, consulte el artículo [Acceso CLI del cliente](#).

Se recomienda utilizar Putty SCP (PSCP) para tener acceso SSH para extraer los registros:

1. Descargar PSCP [Descargar PuTTY](#)
2. Abra la configuración de proxy que está habilitada en ESA y deje el proxy abierto.

```
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. Ejecute CMD y escriba: `pscp -P port -r <user>@localhost:/mail_logs/* /path/on/local/system`

1. El puerto es el que se configuró previamente para el acceso CLI.
2. `/mail_logs/` significa que descarga todos los archivos bajo esa carpeta en particular.
3. Si sólo necesita descargar el archivo actual, escriba `/mail_logs/mail.current` o el registro necesario.
4. Introduzca la contraseña cuando se le solicite una vez introducido el comando.

Ejemplo de comando: `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>
```

Información Relacionada

- [Dispositivo de seguridad Cisco Email Security Appliance: guías del usuario final](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).