

# CES ESA 및 CMD의 GUI에서 로그 다운로드

## 목차

[소개](#)

[사전 요구 사항](#)

[GUI에서 로그 다운로드](#)

[CMD에서 로그 다운로드](#)

[관련 정보](#)

## 소개

이 문서에서는 CMD(Command Line)를 통해 CES(Secure Email Cloud Gateway)의 GUI(Graphical User Interface)에서 로그를 다운로드하는 방법에 대해 설명합니다.

## 사전 요구 사항

관리자 또는 클라우드 관리자 권한이 있는 사용자 계정입니다.

## GUI에서 로그 다운로드

1. CES ESA(Email Security Appliance) 인스턴스의 GUI에 로그인하여 **System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션)**로 이동합니다.
2. 브라우저에 표시된 URL을 확인합니다(예: [System Administration Log Subscriptions](#)).
3. 다음으로, **Log Settings(로그 설정)** 열을 검토하고 다운로드할 로그를 찾아야 합니다. 이 예에서는 mail\_logs를 사용합니다.

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. 2단계에서 URL을 가져와 수정합니다.

a. /log\_subscriptions를 제거합니다.

b. /log\_list?log\_type=<logname>을(를) URL의 끝에 추가합니다. 여기서 <logname>은 로그 설정에 표시된 내용으로 교체됩니다

예.

c. dhXXXX-esa1.iphmx.com을 ESA의 FQDN(Fully Qualified Domain Name)으로 바꿉니다.

**참고:** mail\_logs를 예로 사용하려면 [System Administration Log Subscriptions\(시스템 관리 로그 서브스크립션\)](#)가 [System Administration Log List\(시스템 관리 로그 목록\)](#)가 됩니다.

5. 마지막으로 수정된 URL로 이동하여 로그인합니다. 그림에 표시된 것과 유사한 페이지로 이동한 다음 파일을 클릭하여 다운로드하고 저장할 수 있습니다.

## 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

## CMD에서 로그 다운로드

CES ESA의 CLI 액세스 권한이 있는지 확인합니다. CLI 액세스를 요청하는 단계는 [고객 CLI 액세스 문서를 참조하십시오](#).

사용하는 것이 좋습니다. PSCP(Putty SCP)에서 로그를 풀링하기 위해 SSH 액세스 권한을 보유해야 합니다.

1. PSCP 다운로드 [PuTTY 다운로드](#)
2. ESA에서 활성화된 프록시 컨피그레이션을 열고 프록시를 열린 상태로 둡니다.

```
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. CMD를 실행하고 `pscp -P port -r <user>@localhost:/mail_logs/* /path/on/local/system`을 입력합니다

1. 포트는 이전에 CLI 액세스를 위해 구성된 포트입니다.
2. `/mail_logs/` 해당 특정 폴더 아래의 모든 파일을 다운로드한다는 의미입니다.
3. 현재 파일만 다운로드해야 하는 경우 `/mail_logs/mail.current` 또는 필요한 로그를 입력합니다.
4. 명령을 입력한 후 요청 시 비밀번호를 입력합니다.

명령 예: `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>
```

## 관련 정보

- [Cisco Email Security Appliance - 엔드 유저 가이드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.