CES ESA 및 CMD의 GUI에서 로그 다운로드

목차

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

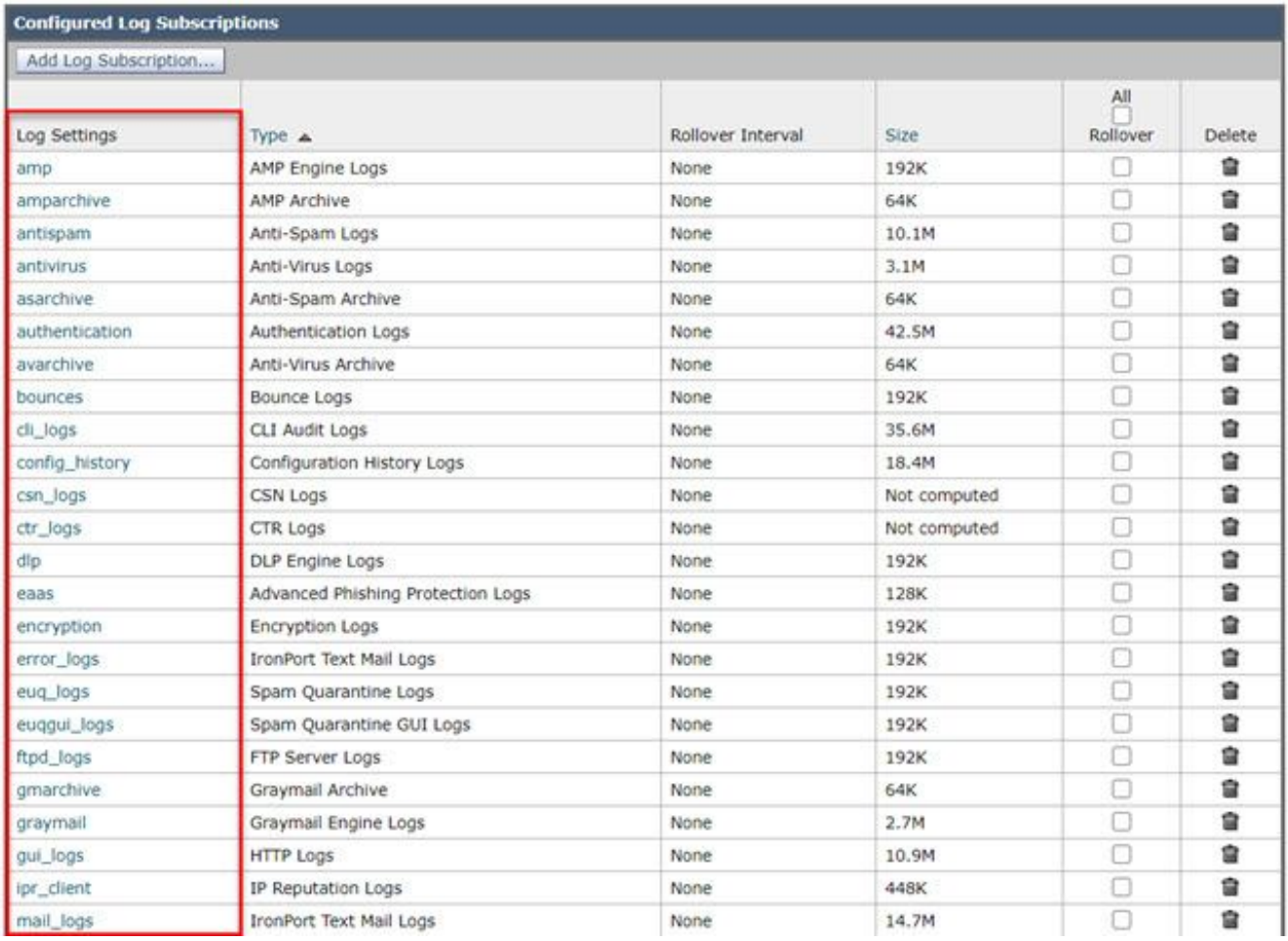
관리자 또는 클라우드 관리자 권한이 있는 사용자 계정입니다.

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_**logs**를 **사용합니다**.



Configured Log Subscriptions

Add Log Subscription...

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

4. 2단계에서 URL을 가져와 수정합니다.

a. /log_subscriptions를 제거합니다.

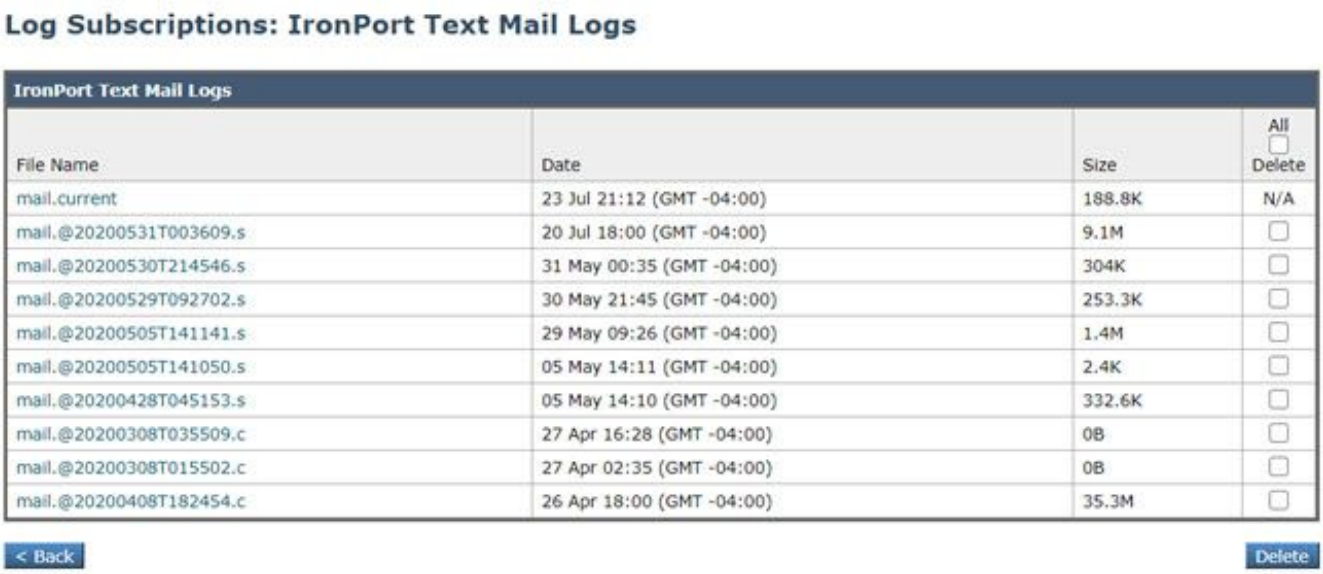
b. /log_list?log_type=<logname>을(를) URL의 끝에 추가합니다. 여기서 <logname>은 **로그 설정**에 표시된 내용으로 **교체됩니다**

열.

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.

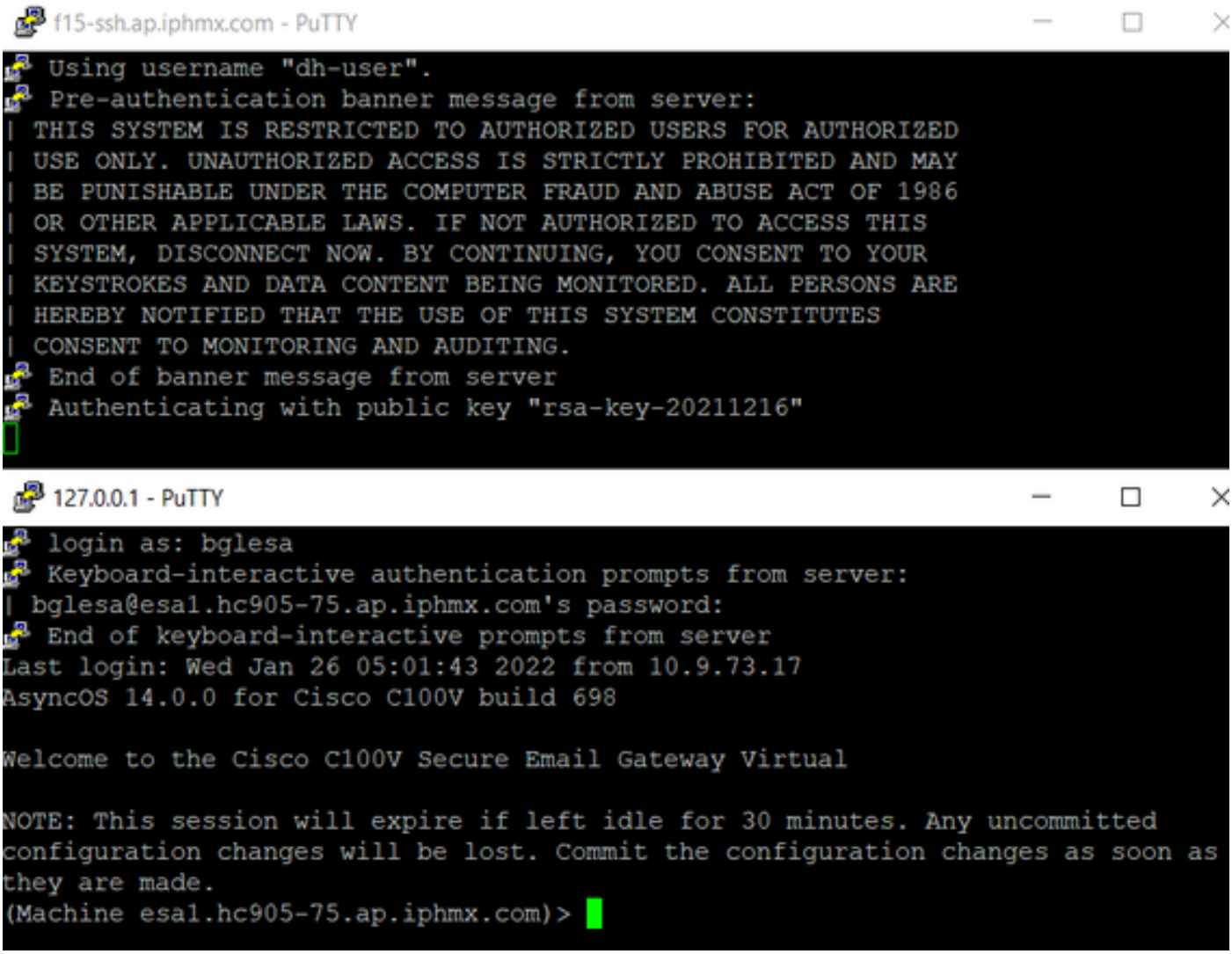


CMD에서 로그 다운로드

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.

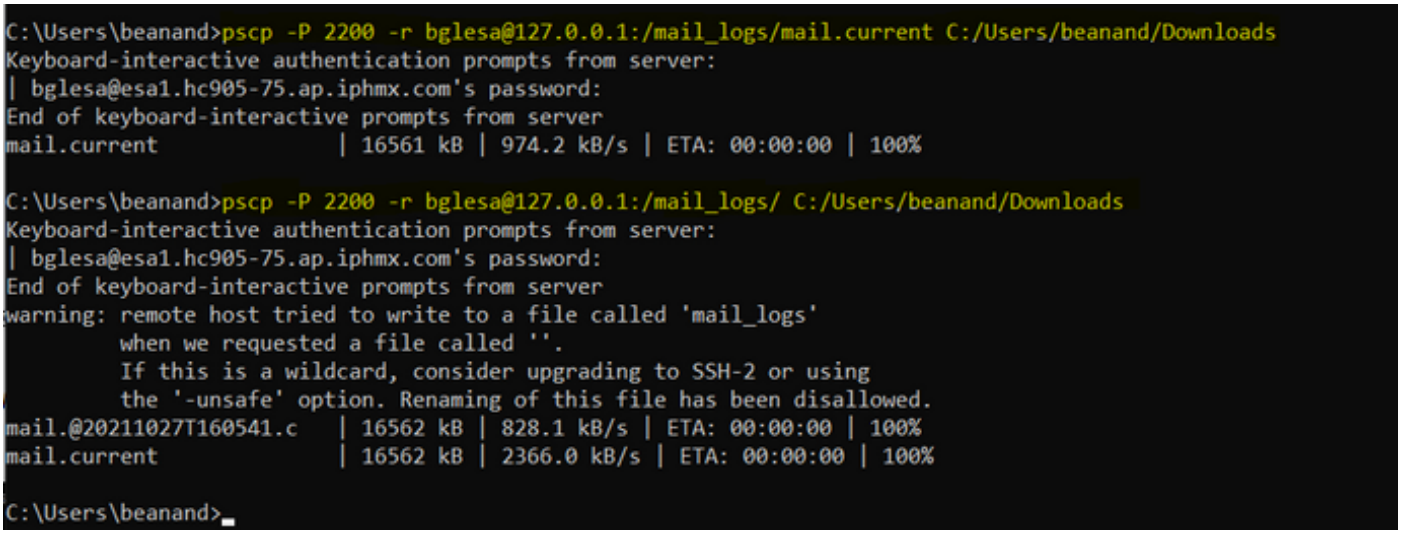
1. PSCP 다운로드 PuTTY 다운로드
2. ESA에서 활성화된 프록시 컨피그레이션을 열고 프록시를 열린 상태로 둡니다.



3. CMD를 실행하고 **pscp -P port -r <user>@localhost:/mail_logs/* /path/on/local/system을 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**



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.