从CES ESA和CMD的GUI下载日志

目录

简介

本文档介绍如何通过命令行(CMD)从安全邮件云网关(CES)的图形用户界面(GUI)下载日志。

先决条件

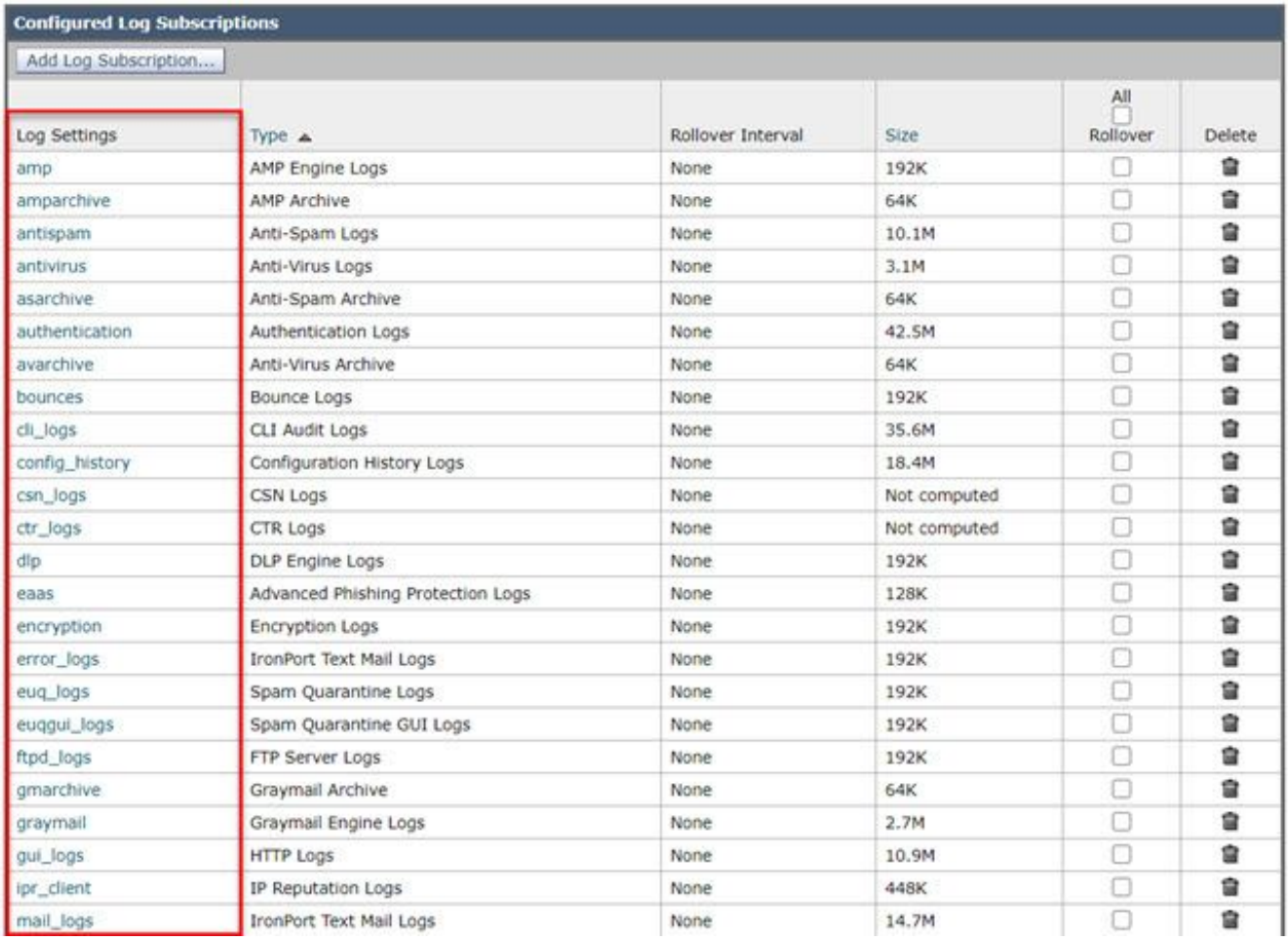
具有管理员或云管理员权限的用户帐户。

从GUI下载日志

1.登录到CES邮件安全设备(ESA)实例的GUI，然后导航到**系统管理>日志订用**。

2.注意浏览器中看到的URL(例如：System Administration Log Subscriptions)

3.接下来，您需要查看**日志设置**列，并查找要下载的日志。在本示例中，请使用**mail_logs**。



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.使用步骤2中的URL进行修改：

a.删除/log_subscriptions。

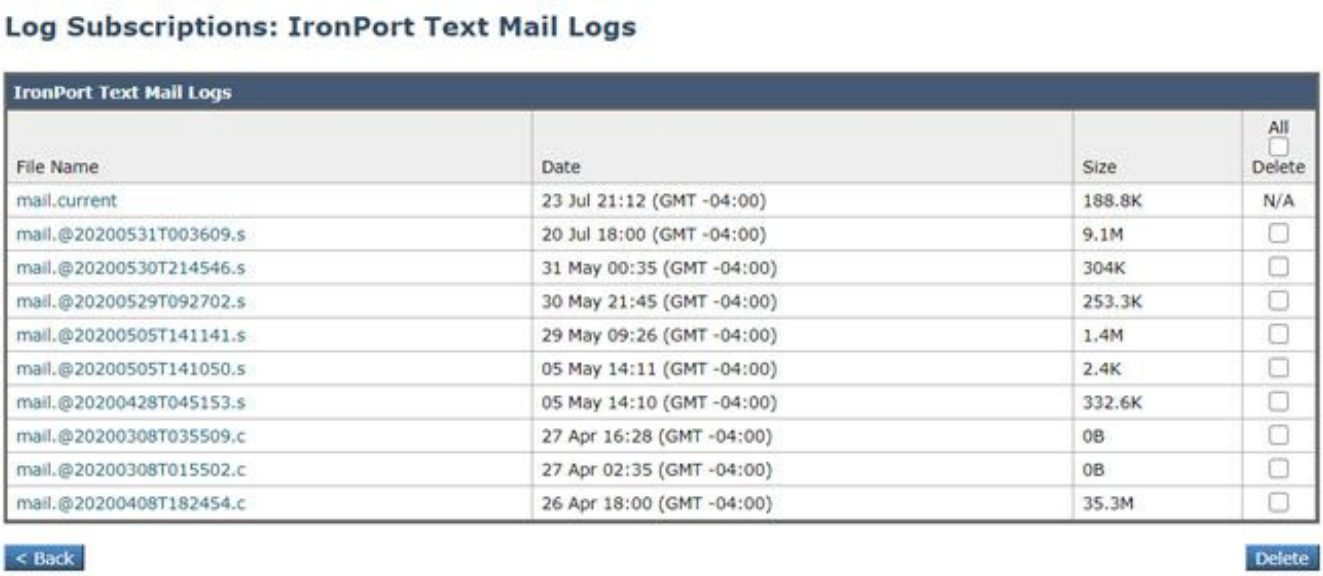
b.在URL的末尾附加/log_list?log_type=<logname>，其中<logname>替换为**Log Settings**下显示的内容

列.

c.将dhXXXX-esa1.iphmx.com替换为ESA的完全限定域名(FQDN)。

注意：如果使用mail_logs作为示例，System Administration Log Subscriptions将变为System Administration Log List。

5.最后，导航到修改后的URL并登录。您将进入与图像所示类似的页面，然后点击文件，下载并保存文件。

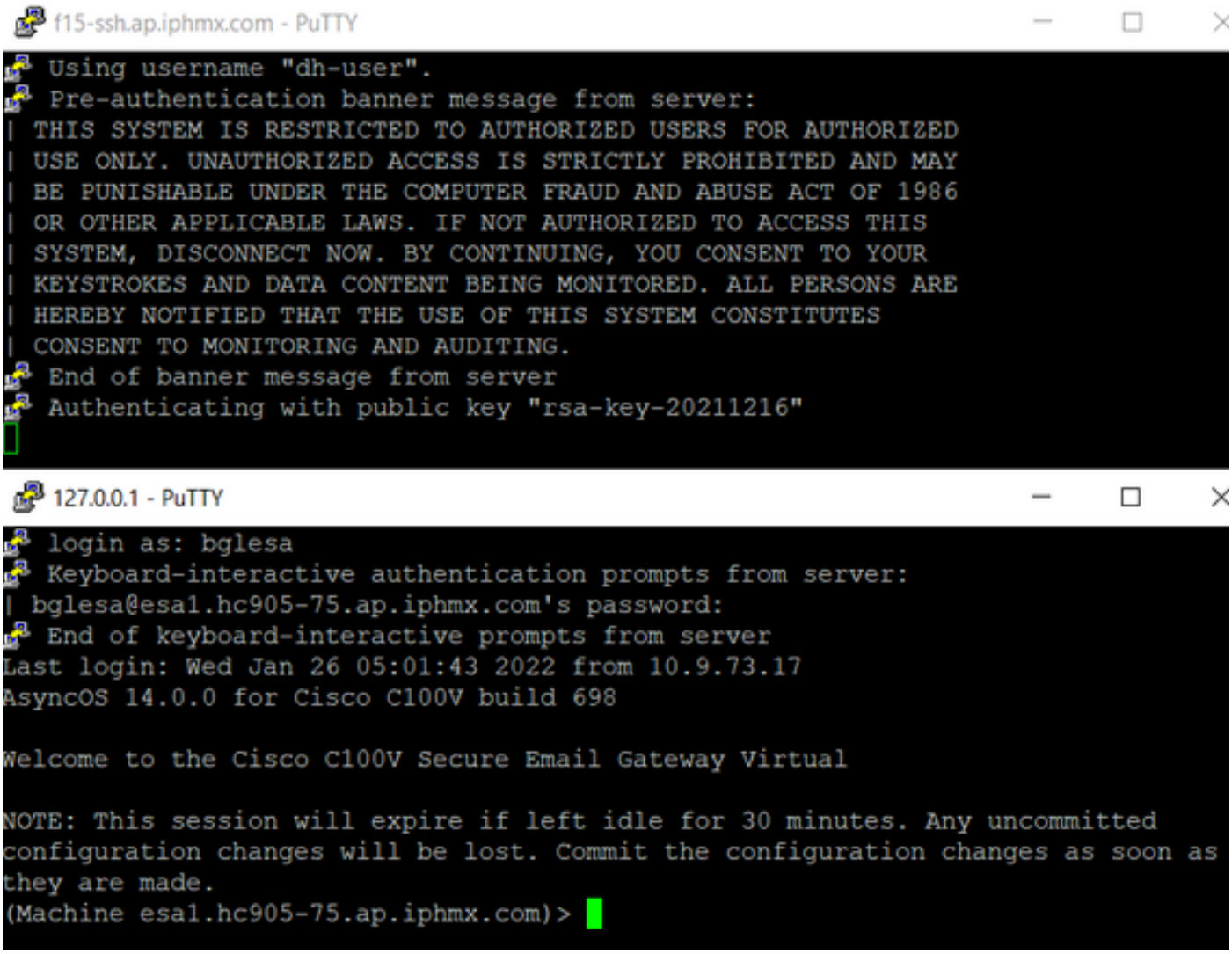


从CMD下载日志

确保您具有CES ESA的CLI访问权限。有关请求CLI访问的步骤，请参阅客户CLI访问一文。

建议使用 Putty SCP(PSCP)具有SSH访问权限以便提取日志：

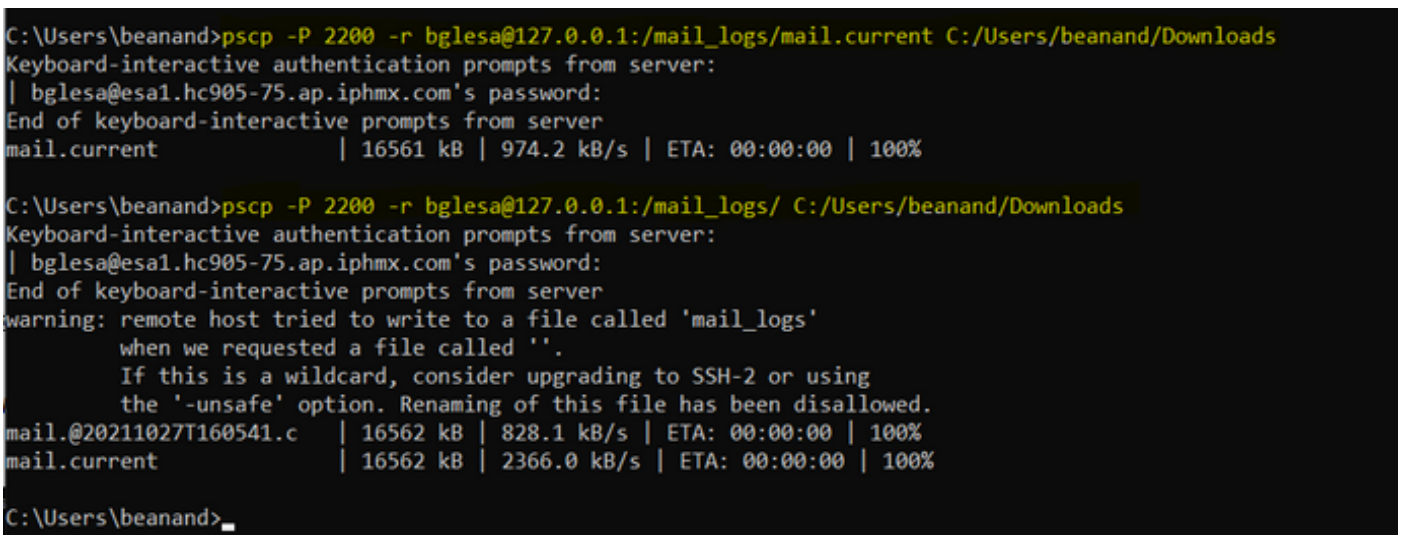
1. 下载PSCP下载PuTTY
2. 打开在ESA上启用的代理配置，保持代理打开。



3.运行CMD并键入：**pscp -P port -r <user>@localhost:/mail_logs/* /path/on/local/system**

1. 端口是之前为CLI访问配置的端口。
2. /mail_logs/表示它下载该特定文件夹下的所有文件。
3. 如果只需要下载当前文件，请键入/mail_logs/mail.current或所需的日志。
4. 输入命令后，在请求时输入密码。

命令示例： **pscp -P 2200 -r admin@127.0.0.1:/mail_logs/ C:/Users/beanand/Downloads**



相关信息

- 思科邮件安全设备 — 最终用户指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。