CES ESAおよびCMDのGUIからのログのダウンロード

内容

概要

このドキュメントでは、コマンドライン(CMD)を使用してSecure Email Cloud Gateway(CES)のグラフィカルユーザインターフェイス(GUI)からログをダウンロードする方法について説明します。

前提条件

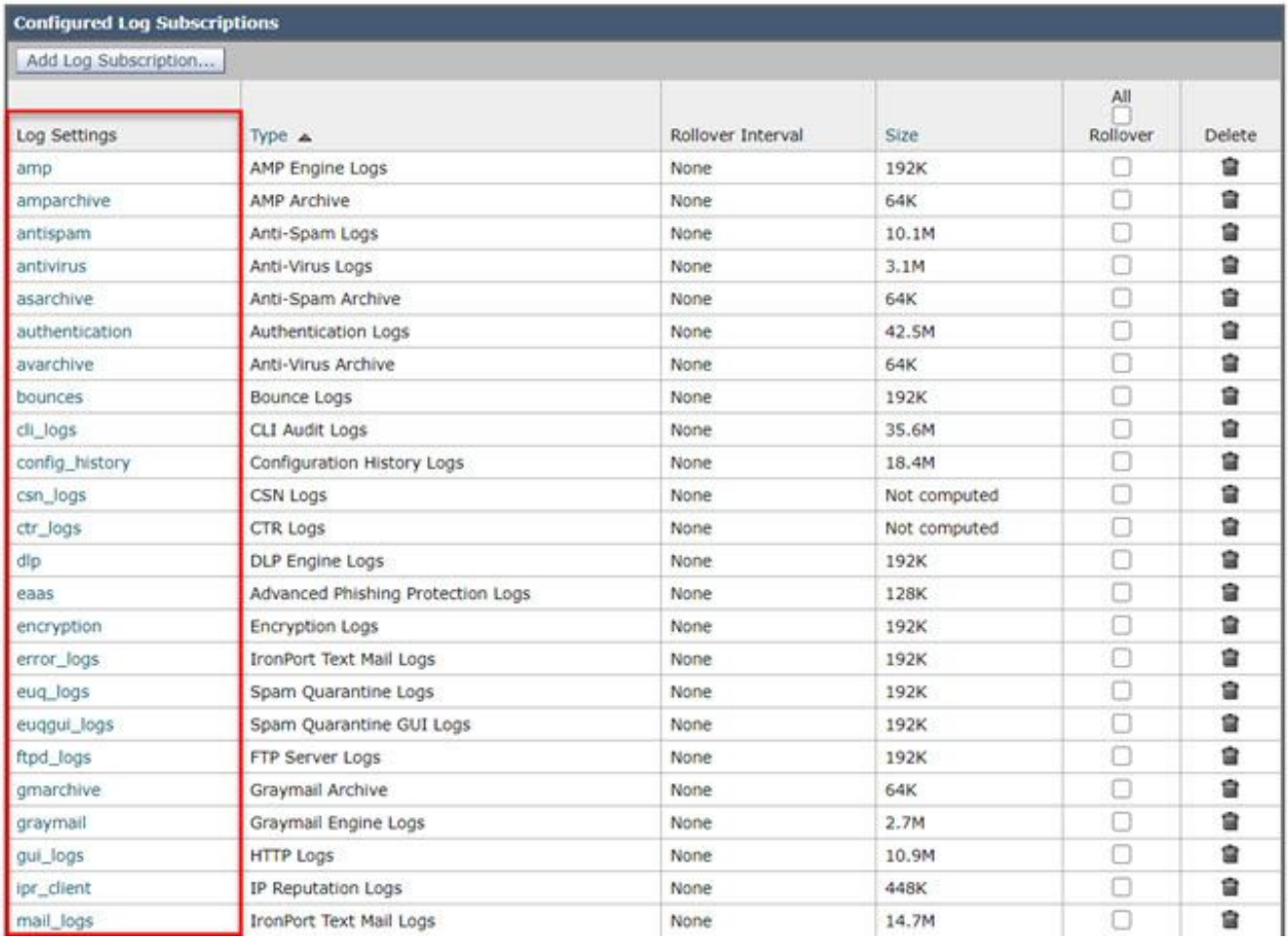
管理者権限またはクラウド管理者権限を持つユーザアカウント。

GUIからのログのダウンロード

1. CES Eメールセキュリティアプライアンス(ESA)インスタンスのGUIにログインし、[System Administration] > [Log Subscriptions] に移動します。

2.ブラウザに表示されるURLに注意してください(例：System Administration Log Subscriptions)

3.次に、[Log Settings] 列を確認し、ダウンロードするログを見つける必要があります。この例では、**mail_logs**を使用します。



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.ステップ2のURLを取得し、変更を行います。

a./log_subscriptionsを削除します。

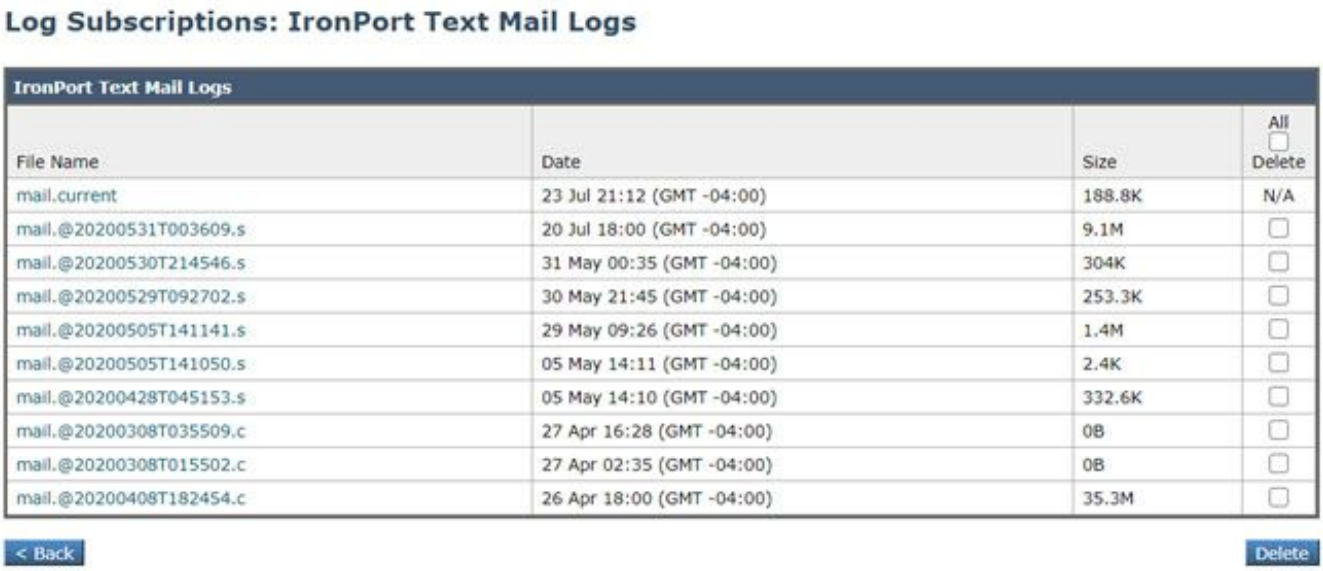
b.URLの末尾に/log_list?log_type=<logname>を追加します。ここで、<logname>は[Log Settings] に表示されるものに置き換えます

カラム.

c. dhXXXX-esa1.iphmx.comをESAの完全修飾ドメイン名(FQDN)に置き換えます。

注：この例でmail_logsを使用するには、System Administration Log SubscriptionsがSystem Administration Log Listになります。

5.最後に、変更したURLに移動してログインします。画像のようなページが表示され、ファイルをクリックしてダウンロードし、保存することができます。

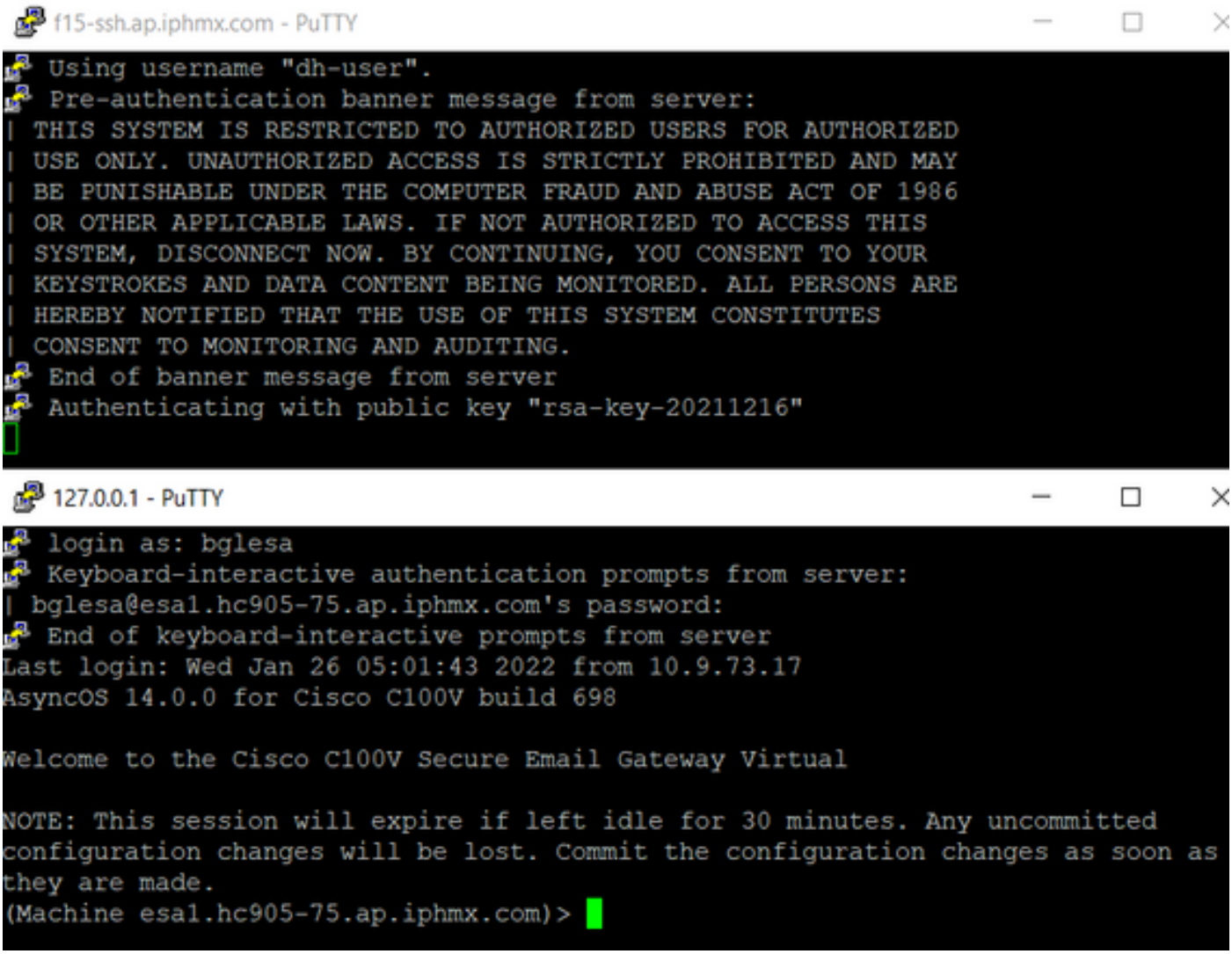


CMDからのログのダウンロード

CES ESAのCLIアクセス権があることを確認します。CLIアクセスを要求する手順については、「お客様のCLIアクセス」を参照してください。

使用することを推奨します。 ログを取得するためにSSHアクセスを持つPutty SCP(PSCP):

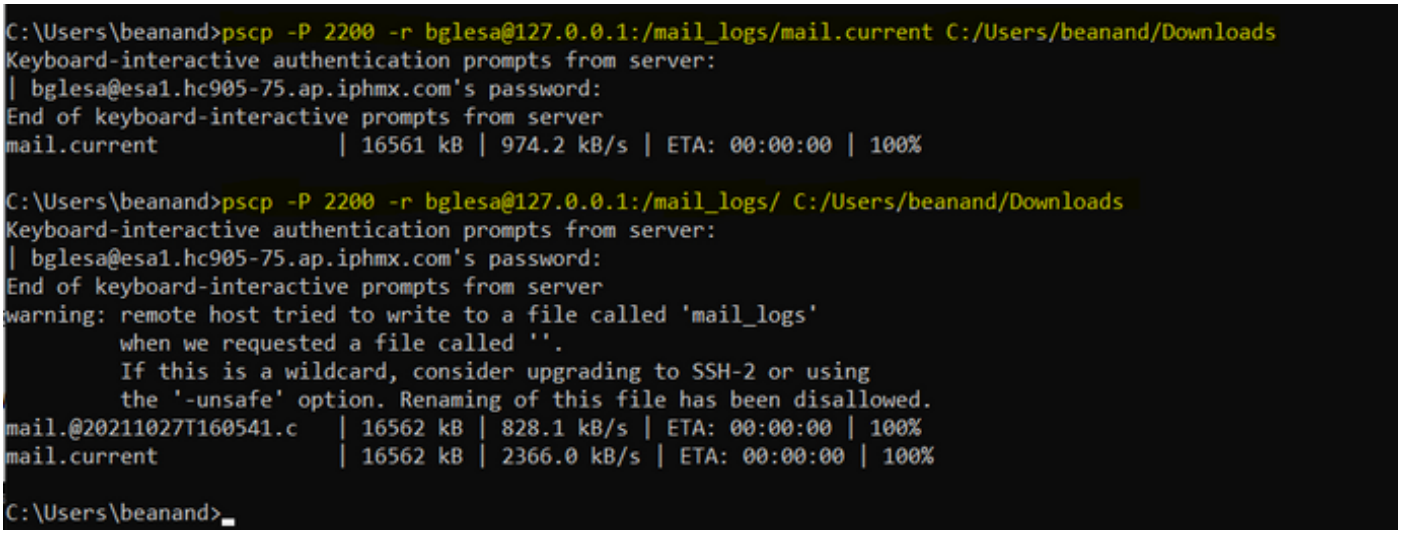
1. PSCPのダウンロードPuTTYのダウンロード
2. ESAで有効になっているプロキシ設定を開き、プロキシを開いたままにします。



3. CMDを実行し、次のように入力します。**pscp -P port -r <user>@localhost:/mail_logs/* /path/on/local/system**

1. ポートは、CLIアクセス用に事前に設定されているポートです。
2. /mail_logs/は、その特定のフォルダにあるすべてのファイルをダウンロードすることを意味します。
3. 現在のファイルだけをダウンロードする必要がある場合は、/mail_logs/mail.currentまたは必要なログを入力します。
4. コマンドを入力したら、要求に応じてパスワードを入力します。

コマンド例： **pscp -P 2200 -r admin@127.0.0.1:/mail_logs/ C:/Users/beanand/Downloads**



関連情報

- Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。