

CES ESAおよびCMDのGUIからのログのダウンロード

内容

[概要](#)

[前提条件](#)

[GUIからのログのダウンロード](#)

[CMDからのログのダウンロード](#)

[関連情報](#)

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 <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.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。

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

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。

```
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. 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`

```
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>_
```

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。