

# Protokolle aus der Benutzeroberfläche Ihrer CES ESA und CMD herunterladen

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Protokolle über die Benutzeroberfläche herunterladen](#)

[Protokolle von CMD herunterladen](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Sie Protokolle über die grafische Benutzeroberfläche (GUI) des Secure Email Cloud Gateway (CES) über die Befehlszeile (CMD) herunterladen können.

## Voraussetzungen

Ein Benutzerkonto mit Administrator- oder Cloud-Administratorberechtigung.

## Protokolle über die Benutzeroberfläche herunterladen

1. Melden Sie sich bei der GUI Ihrer Instanz der CES Email Security Appliance (ESA) an, und navigieren Sie zu **Systemverwaltung > Protokollabonnements**.
2. Beachten Sie die in Ihrem Browser angezeigte URL (Beispiel: [Systemverwaltungsprotokollabonnements](#))
3. Als Nächstes müssen Sie die Spalte **Protokolleinstellungen** überprüfen und ein Protokoll finden, das Sie herunterladen möchten. Verwenden Sie für dieses Beispiel **mail\_logs**.

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"/>	
dip	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. Nehmen Sie die URL aus Schritt zwei und nehmen Sie die Änderungen vor:

antwort: /log\_subscriptions entfernen.

b. Hängen Sie /log\_list?log\_type=<logname> an das Ende der URL an, wobei <logname> durch das ersetzt wird, was unter den **Protokolleinstellungen** angezeigt wird.

Spalte.

c. Ersetzen Sie dhXXXX-esa1.iphmx.com durch den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) Ihrer ESA.

**Hinweis:** Um mail\_logs als Beispiel zu verwenden, werden [Systemverwaltungsprotokollabonnements](#) zur [Systemverwaltungsprotokolliste](#).

5. Navigieren Sie abschließend zur geänderten URL, und melden Sie sich an. Sie würden zu einer Seite kommen, die dem ähnelt, was im Bild angezeigt wird, wo Sie dann auf eine Datei klicken, sie herunterladen und speichern können.

## Log Subscriptions: IronPort Text Mail Logs

IronPort Text Mail Logs			
File Name	Date	Size	All 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

## Protokolle von CMD herunterladen

Stellen Sie sicher, dass Sie über den CLI-Zugang der CES ESA verfügen. Informationen zur Anforderung des CLI-Zugriffs finden Sie im Artikel [Customer CLI Access](#).

Die Anwendung von Putty SCP (PSCP) erhält SSH-Zugriff, um die Protokolle abzurufen:

1. PSCP herunterladen [PuTTY herunterladen](#)
2. Öffnen Sie die auf der ESA aktivierte Proxy-Konfiguration, und lassen Sie den Proxy geöffnet.

```
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. Führen Sie CMD aus, und geben Sie `pscp -P port -r <user>@localhost:/mail_logs/* /path/on/local/system` ein.

1. Port ist der Port, der zuvor für den CLI-Zugriff konfiguriert wurde.
2. `/mail_logs/` bedeutet, dass es alle Dateien in diesem bestimmten Ordner herunterlädt.
3. Wenn nur die aktuelle Datei heruntergeladen werden muss, geben Sie `/mail_logs/mail.current` oder das erforderliche Protokoll ein.
4. Geben Sie auf Anforderung nach Eingabe des Befehls das Kennwort ein.

Beispielbefehl: `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>_
```

## Zugehörige Informationen

- [Cisco Email Security Appliance - Benutzerhandbücher](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.