

Come è possibile modificare i tipi di crittografia utilizzati nell'interfaccia grafica? È possibile disabilitare SSL v2 per la GUI?

Sommario

[Introduzione](#)

[Come è possibile modificare i tipi di crittografia utilizzati nell'interfaccia grafica? È possibile disabilitare SSL v2 per la GUI?](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come visualizzare e modificare i cifrari utilizzati insieme all'interfaccia grafica (GUI) su Cisco Email Security Appliance (ESA).

Come è possibile modificare i tipi di crittografia utilizzati nell'interfaccia grafica? È possibile disabilitare SSL v2 per la GUI?

I protocolli e le cifrature SSL annunciati per le connessioni GUI in ingresso possono essere configurati con il comando **sslconfig**. È possibile specificare il metodo ssl da utilizzare specificamente per la comunicazione SSL GUI.

Esempio:

```
myesa.local> sslconfig
```

```
sslconfig settings:  
GUI HTTPS method: sslv3tlsv1  
GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL  
Inbound SMTP method: sslv3tlsv1  
Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL  
Outbound SMTP method: sslv3tlsv1  
Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
```

```
Choose the operation you want to perform:  
- GUI - Edit GUI HTTPS ssl settings.  
- INBOUND - Edit Inbound SMTP ssl settings.  
- OUTBOUND - Edit Outbound SMTP ssl settings.  
- VERIFY - Verify and show ssl cipher list.  
[> GUI
```

Enter the GUI HTTPS ssl method you want to use.

1. SSL v2.
 2. SSL v3
 3. TLS v1
 4. SSL v2 and v3
 5. SSL v3 and TLS v1
 6. SSL v2, v3 and TLS v1
- [5]> 2

Enter the GUI HTTPS ssl cipher you want to use.

[RC4-SHA:RC4-MD5:ALL]>

Tornare alla CLI principale ed eseguire il **commit** di tutte le modifiche.

Informazioni correlate

- [Cisco Email Security Appliance - Guide per l'utente](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)