

# Configurare Transport Layer Security versione 1.0 su ESA e CES

## Sommario

---

[Introduzione](#)

[Come abilitare TLSv1.0 su Cisco ESA e CES?](#)

[Interfaccia grafica dell'utente](#)

[Interfaccia della riga di comando](#)

[Cifrature](#)

[Informazioni correlate](#)

---

## Introduzione

Questo documento descrive come abilitare Transport Layer Security versione 1.0 (TLSv1.0) sulle allocazioni Cisco Email Security Appliance (ESA) e Cisco Cloud Email Security (CES).

## Come abilitare TLSv1.0 su Cisco ESA e CES?

---

 Nota: per impostazione predefinita, il protocollo TLSv1.0 è disabilitato per le allocazioni Cisco CES fornite in base ai requisiti di sicurezza a causa dell'impatto della vulnerabilità sul protocollo TLSv1.0. inclusa la stringa di crittografia per rimuovere tutti gli utilizzi della suite di crittografia condivisa SSLv3.

---

 Attenzione: i metodi e le cifrature SSL/TLS vengono impostati in base alle politiche e alle preferenze di sicurezza specifiche della società. Per informazioni di terze parti relative ai cifrari, consultare il documento [Security/Server Side TLS](#) Mozilla per le configurazioni server consigliate e informazioni dettagliate.

---

Per abilitare TLSv1.0 sull'ESA o sul CES Cisco, è possibile usare l'interfaccia grafica dell'utente (GUI) o l'interfaccia della riga di comando (CLI).

---

 Nota: per ottenere l'accesso al CES sulla CLI, rivedere: [Accesso all'interfaccia della riga di comando \(CLI\) della soluzione Cloud Email Security \(CES\)](#)

---

## Interfaccia grafica dell'utente

1. Accedere alla GUI.
2. Passare a Amministrazione sistema > Configurazione SSL.
3. Selezionare Modifica impostazioni.

4. Selezionare la casella TLSv1.0. È importante notare che TLSv1.2 e non possono essere abilitati insieme a TLSv1.0 a meno che non sia abilitato anche il protocollo di bridging TLSv1.1, come mostrato nell'immagine:

### Edit SSL Configuration

Mode -- Cluster: Hosted\_Cluster

Centralized Management Options

SSL Configuration			
GUI HTTPS:	Methods:	<input checked="" type="checkbox"/> TLS v1.2	<input checked="" type="checkbox"/> TLS v1.1
		<input checked="" type="checkbox"/> TLS v1.0	<input type="checkbox"/> SSL v3
	SSL Cipher(s) to use:	RC4-SHA:RC4-MD5:ALL:-aNULL:-EXPORT	
Inbound SMTP:	Methods:	<input checked="" type="checkbox"/> TLS v1.2	<input checked="" type="checkbox"/> TLS v1.1
		<input checked="" type="checkbox"/> TLS v1.0	<input type="checkbox"/> SSL v3
	SSL Cipher(s) to use:	RC4-SHA:RC4-MD5:ALL:-aNULL:-EXPORT	
Outbound SMTP:	Methods:	<input checked="" type="checkbox"/> TLS v1.2	<input checked="" type="checkbox"/> TLS v1.1
		<input checked="" type="checkbox"/> TLS v1.0	<input type="checkbox"/> SSL v3
	SSL Cipher(s) to use:	RC4-SHA:RC4-MD5:ALL:-aNULL:-EXPORT	

Note:  
TLSv1.0 and TLSv1.2 cannot be enabled simultaneously, but both can be enabled for use with TLSv1.1.

### Interfaccia della riga di comando

1. Eseguire il comando `sslconfig`.
2. Eseguire il comando `GUI` o `INBOUND` o `OUTBOUND` a seconda dell'elemento per cui si desidera abilitare TLSv1.0:

```
<#root>
```

```
(Cluster Hosted_Cluster)>
```

```
sslconfig
```

```
sslconfig settings:
```

```
GUI HTTPS method: tlsv1_2
```

```
GUI HTTPS ciphers:
```

```
RC4-SHA
```

```
RC4-MD5
```

```
ALL
```

```
-aNULL
```

```
-EXPORT
```

```
Inbound SMTP method: tlsv1_2
```

Inbound SMTP ciphers:

RC4-SHA  
RC4-MD5  
ALL  
-aNULL  
-EXPORT

Outbound SMTP method: `tlsv1_2`

Outbound SMTP ciphers:

RC4-SHA  
RC4-MD5  
ALL  
-aNULL  
-EXPORT

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.
- CLUSTERSET - Set how ssl settings are configured in a cluster.
- CLUSTERSHOW - Display how ssl settings are configured in a cluster.

[ ]> INBOUND

Enter the inbound SMTP ssl method you want to use.

1. TLS v1.0

2. TLS v1.1

3. TLS v1.2

4. SSL v2

5. SSL v3

[3]> 1-3

Enter the inbound SMTP ssl cipher you want to use.

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

## Cifrature

Le allocazioni ESA e CES possono essere configurate con suite di cifratura rigide. È importante assicurarsi che le cifrature SSLv3 non vengano bloccate quando si abilita il protocollo TLSv1.0. Se non si consentono le suite di cifratura SSLv3, si verificheranno errori di negoziazione TLS o interruzioni brusche delle connessioni TLS.

Stringa di esempio:

```
<#root>
```

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES  
:!SSLv3:!TLSv1  
:-aNULL:-EXPORT:-IDEA
```

Questa stringa di cifratura impedisce all'ESA/CES di consentire la negoziazione sui cifrari SSLv3 come indicato in !SSLv3:, ciò significa che quando il protocollo viene richiesto nell'handshake, l'handshake SSL ha esito negativo perché non sono disponibili cifrature condivise per la negoziazione.

Per garantire che la stringa di crittografia di esempio funzioni con TLSv1.0, è necessario modificarla per rimuovere !SSLv3:!TLSv1: visualizzato nella stringa di crittografia sostituita:

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES
```



Nota: è possibile verificare le suite di cifratura condivise sull'handshake SSL sulla CLI ESA/CES con il comando VERIFY.

---

Possibili errori registrati in mail\_logs/Message Tracking ma non limitati a:

```
Sun Feb 23 10:07:07 2020 Info: DCID 1407038 TLS failed: (336032784, 'error:14077410:SSL routines:SSL23_
Sun Feb 23 10:38:56 2020 Info: DCID 1407763 TLS failed: (336032002, 'error:14077102:SSL routines:SSL23_
```

## Informazioni correlate

- [Modifica dei metodi e dei cifrari utilizzati con SSL/TLS sull'ESA](#)
- [Dettagli livello di crittografia SSL](#)
- [Guida completa alla configurazione di TLS su ESA](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).