

在ESA和CES上配置傳輸層安全版本1.0

目錄

[簡介](#)

[如何在Cisco ESA和CES上啟用TLSv1.0?](#)

[圖形使用者介面](#)

[命令列介面](#)


[密碼](#)


[相關資訊](#)

簡介

本文檔介紹如何在思科郵件安全裝置(ESA)和思科雲郵件安全(CES)分配上啟用傳輸層安全1.0版(TLSv1.0)。

如何在Cisco ESA和CES上啟用TLSv1.0?

 註：由於漏洞對TLSv1.0協定的影響，根據安全要求，Cisco CES分配預設停用TLSv1.0。其中包括用於刪除SSLv3共用密碼套件所有用法的密碼字串。

 注意：SSL/TLS方法和密碼是根據您公司的特定安全策略和首選項設定的。有關口令的第三方資訊，請參閱[安全/伺服器端TLS](#) Mozilla文檔，以瞭解建議的伺服器配置和詳細資訊。

為了在Cisco ESA或CES上啟用TLSv1.0，您可以從圖形使用者介面(GUI)或命令列介面(CLI)中啟用。

 注意：要在CLI上訪問CES，請檢視：[訪問Cloud Email Security \(CES\)解決方案的命令列介面\(CLI\)](#)

圖形使用者介面

1. 登入到GUI。
2. 導航到系統管理> SSL配置。
3. 選擇Edit Settings。
4. 選中TLSv1.0框。必須注意的是，TLSv1.2不能與TLSv1.0一起啟用，除非還啟用了橋接協定TLSv1.1，如圖所示：

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.

命令列介面

1. 運行sslconfig命令。
2. 運行命令GUI、INBOUND或OUTBOUND (具體取決於要為以下哪個專案啟用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]>

密碼

ESA和CES分配可以使用嚴格的密碼套件進行配置，啟用TLSv1.0協定時，確保SSLv3密碼沒有被阻止，這一點非常重要。如果允許SSLv3密碼套件失敗，則會導致TLS協商失敗或突發TLS連線關閉。

密碼字串範例：

<#root>

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

!SSLv3:!TLSv1

:-aNULL:-EXPORT:-IDEA

此密碼字串會停止ESA/CES在SSLv3密碼上允許協商，如 !SSLv3 : 所示，這意味著在握手中請求協定時，SSL握手會失敗，因為不存在可用於協商的共用密碼。

為了確保TLSv1.0的示例密碼字串有效，需要修改它以刪除在替換的密碼字串中看到的
!SSLv3 : !TLSv1 : :

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



註：您可以使用VERIFY命令驗證ESA/CES CLI上SSL握手共用的密碼套件。

可能記錄在mail_logs/郵件跟蹤中的錯誤，但不限於：

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_

相關資訊

- [更改ESA上與SSL/TLS一起使用的方法和密碼](#)
- [SSL密碼強度詳細資訊](#)
- [ESA上的TLS綜合設定指南](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。