

Configure Transport Layer Security Version 1.0 on the ESA and CES

Contents

[Introduction](#)

[How can you enable TLSv1.0 on the Cisco ESA and CES?](#)

[Graphical User Interface](#)

[Command Line Interface](#)


[Ciphers](#)


[Related Information](#)

Introduction

This document describes how to enable Transport Layer Security version 1.0 (TLSv1.0) on the Cisco Email Security Appliance (ESA) and Cisco Cloud Email Security (CES) allocations.

How can you enable TLSv1.0 on the Cisco ESA and CES?

 **Note:** Cisco CES allocations provisioned have TLSv1.0 disabled by default as per security requirements due to vulnerability impacts on the TLSv1.0 protocol. This includes the cipher string to remove all usage of the SSLv3 shared cipher suite.

 **Caution:** The SSL/TLS methods and ciphers are set based on the specific security policies and preferences of your company. For third-party information in regards to ciphers, refer to the [Security/Server Side TLS](#) Mozilla document for recommended server configurations and detailed information.

In order to enable TLSv1.0 on your Cisco ESA or CES, you can do so from the Graphical User Interface (GUI) or Command Line Interface (CLI).

 **Note:** In order to get access to your CES on the CLI please review: [Accessing the Command Line Interface \(CLI\) of Your Cloud Email Security \(CES\) Solution](#)

Graphical User Interface

1. Log into the GUI.
2. Navigate to **System Administration > SSL Configuration**.
3. Select **Edit Settings**.
4. Check the **TLSv1.0** box. It is important to note that TLSv1.2 and cannot be enabled in conjunction with TLSv1.0 unless the bridging protocol TLSv1.1 is also enabled as shown in the image:

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.

Command Line Interface

1. Run the command `sslconfig`.
2. Run the command `GUI` or `INBOUND` or `OUTBOUND` depending on which item you want to enable TLSv1.0 for:

```
<#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]>

Ciphers

ESAs and CES allocations can be configured with strict cipher suites, it is important to ensure SSLv3 ciphers are not blocked when you enable the TLSv1.0 protocol. Failure to allow the SSLv3 cipher suites result in TLS negotiation failures or abrupt TLS connection closures.

Sample cipher string:

<#root>

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


!SSLv3:!TLSv1

:-aNULL:-EXPORT:-IDEA

This cipher string stops the ESA/CES from allowing negotiation on SSLv3 ciphers as indicated on **!SSLv3:**, this means when the protocol is requested in the handshake, the SSL handshake fails as there are no shared ciphers available for negotiation.

In order to ensure the sample cipher string functions with TLSv1.0, it needs to be modified to remove **!SSLv3:!TLSv1:** seen in the replaced cipher string:

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

 **Note:** You can verify the cipher suites shared on SSL handshake on the ESA/CES CLI with the **VERIFY** command.

Possible errors logged in the mail_logs/Message Tracking but not limited to:

```
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_
```

Related Information

- [Alter the Methods and Ciphers Used with SSL/TLS on the ESA](#)
- [SSL Cipher Strength Details](#)
- [Comprehensive Setup Guide for TLS on ESA](#)
- [Technical Support & Documentation - Cisco Systems](#)