# Alter the Methods and Ciphers Used with SSL/TLS on the ESA

TAC **Document ID: 117855**

Contributed by James Noad and Robert Sherwin, Cisco TAC Engineers.

Jan 07, 2016

## Contents



## Introduction

This document describes how to alter the methods and ciphers that are used with Secure Socket Layer (SSL) or Transport Layer Security (TLS) configurations on the Cisco Email Security Appliance (ESA).

## Alter the Methods and Ciphers Used with SSL/TLS

**Note**: The SSL/TLS methods and ciphers should be 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.

With Cisco AsyncOS for Email Security, an administrator can use the **sslconfig** command in order to configure the SSL or TLS protocols for the methods and ciphers that are used for GUI communication, advertised for inbound connections, and requested for outbound connections:

```
esa.local> sslconfig

sslconfig settings:
 GUI HTTPS method: tlsv1/tlsv1.2
 GUI HTTPS ciphers:
 MEDIUM
 HIGH
 -SSLv2
 -aNULL
 !RC4
 @STRENGTH
 -EXPORT
 Inbound SMTP method: tlsv1/tlsv1.2
 Inbound SMTP ciphers:
 MEDIUM
 HIGH
 -SSLv2
 -aNULL
 !RC4
 @STRENGTH
 -EXPORT
```

```
 Outbound SMTP method: tlsv1/tlsv1.2
 Outbound SMTP ciphers:
 MEDIUM
 HIGH
 -SSLv2
 -aNULL
 !RC4
 @STRENGTH
 -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.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2
2. SSL v3
3. TLS v1/TLS v1.2
4. SSL v2 and v3
5. SSL v3 and TLS v1/TLS v1.2
6. SSL v2, v3 and TLS v1/TLS v1.2
[3]>

Enter the inbound SMTP ssl cipher you want to use.
[MEDIUM:HIGH:-SSLv2:-aNULL:!RC4:@STRENGTH:-EXPORT]>

sslconfig settings:
 GUI HTTPS method: tlsv1/tlsv1.2
 GUI HTTPS ciphers:
 MEDIUM
 HIGH
 -SSLv2
 -aNULL
 !RC4
 @STRENGTH
 -EXPORT
 Inbound SMTP method: tlsv1/tlsv1.2
 Inbound SMTP ciphers:
 MEDIUM
 HIGH
 -SSLv2
 -aNULL
 !RC4
 @STRENGTH
 -EXPORT
 Outbound SMTP method: tlsv1/tlsv1.2
 Outbound SMTP ciphers:
 MEDIUM
 HIGH
 -SSLv2
 -aNULL
 !RC4
 @STRENGTH
 -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.
[]>
```

If changes are made to the SSL configuration, ensure that you **commit** any and all changes.

# SSL Methods

In AsyncOS for Email Security Versions 9.6 and later, the ESA is set to use the *TLS v1/TLS v1.2* method by default. In this case, TLSv1.2 takes precedent for communication, if in use by both the sending and receiving parties. In order to establish a TLS connection, both sides must have at least one enabled method that matches, and at least one enabled cipher that matches.

**Note**: In AsyncOS for Email Security versions prior to Version 9.6, the default has two methods: *SSL v3* and *TLS v1*. Some administrators might want to disable SSL v3 due to recent vulnerabilities (if SSL v3 is enabled).

# SSL Ciphers

When you view the default cipher that is listed in the previous example, it is important to understand the reason that it shows two ciphers followed by the word *ALL*. Although *ALL* includes the two ciphers that precede it, the order of the ciphers in the cipher list determines the preference. Thus, when a TLS connection is made, the client picks the first cipher that both sides support based on the order of appearance in the list.

**Note**: The RC4 ciphers are enabled by default on the ESA. In the previous example, the **MEDIUM:HIGH** is based on the Prevent Negotiations for Null or Anonymous Ciphers on the ESA and SMA Cisco document. For further information in regards to RC4 specifically, refer to the Security/Server Side TLS Mozilla document, and also the On the Security of RC4 in TLS and WPA document that is presented from the *USENIX Security Symposium 2013*. In order to remove the RC4 ciphers from use, refer to the examples that follow.

Through manipulation of the cipher list, you can influence the cipher that is chosen. You can list specific ciphers or cipher ranges, and also reorder them by strength with the inclusion of the **@STRENGTH** option in the cipher string, as shown here:

```
Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

Ensure that you review all of the ciphers and ranges that are available on the ESA. In order to view these, enter the **sslconfig** command, followed by the **verify** sub-command. The options for the SSL cipher categories are **LOW**, **MEDIUM**, **HIGH**, and **ALL**:

```
[]> verify

Enter the ssl cipher you want to verify.
[]> MEDIUM

ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
IDEA-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=IDEA(128) Mac=MD5
RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
```

You can also combine these in order to include ranges:

```
[]> verify

Enter the ssl cipher you want to verify.
```

```
[]> MEDIUM:HIGH

ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
IDEA-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=IDEA(128) Mac=MD5
RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
ADH-CAMELLIA256-SHA SSLv3 Kx=DH Au=None Enc=Camellia(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-DSS-CAMELLIA256-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
ADH-CAMELLIA128-SHA SSLv3 Kx=DH Au=None Enc=Camellia(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
DHE-DSS-CAMELLIA128-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
ADH-AES256-SHA SSLv3 Kx=DH Au=None Enc=AES(256) Mac=SHA1
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-DSS-AES256-SHA SSLv3 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
ADH-AES128-SHA SSLv3 Kx=DH Au=None Enc=AES(128) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
ADH-DES-CBC3-SHA SSLv3 Kx=DH Au=None Enc=3DES(168) Mac=SHA1
EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH Au=DSS Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
DES-CBC3-MD5 SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5
```

Any of the SSL ciphers that you do not want configured and available should be removed with the "**-**" option that precedes the specific ciphers. Here is an example:

```
[]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:
    -EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA
```

The information in this example would negate the *NULL*, *EDH-RSA-DES-CBC3-SHA*, *EDH-DSS-DES-CBC3-SHA*, and *DES-CBC3-SHA* ciphers from advertisement and prevent their use in the SSL communication.

You can also accomplish similar with the inclusion of the "**!**" character in front of the cipher group or string that you desire to become unavailable:

```
[]> MEDIUM:HIGH:-SSLv2:-aNULL:!RC4:@STRENGTH
```

The information in this example would remove all of the RC4 ciphers from use. Thus, the *RC4-SHA* and *RC4-MD5* ciphers would be negated and not advertised in the SSL communication.

If changes are made to the SSL configuration, ensure that you **commit** any and all changes.

---

Updated: Jan 07, 2016 Document ID: 117855