# Configure Modern TLS and DTLS Ciphers for RAVPN

## Contents

Introduction
Prerequisites
Requirements
Components Used
Configure Platform Settings for Secure Firewall
Introduction to Platform Settings
Configure TLS / DTLS Ciphers
Verify
Verify from FTD CLI configuration
Verify from FTD CLI with Active Secure Client Connection
Verify from Client with Active Secure Client Connection
Troubleshoot
Debug from FTD CLI
Gather DART from Secure Client

## Introduction

This document describes the procedure to configure modern Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) ciphers.

## Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- Basic Remote Access VPN (RAVPN) and Secure Sockets Layer (SSL) knowledge
- RAVPN configuration on Secure Firewall tested and operational

## Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall Mangement Center 7.2
- Cisco Firewall Threat Defense 7.2
- Secure Client 5.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

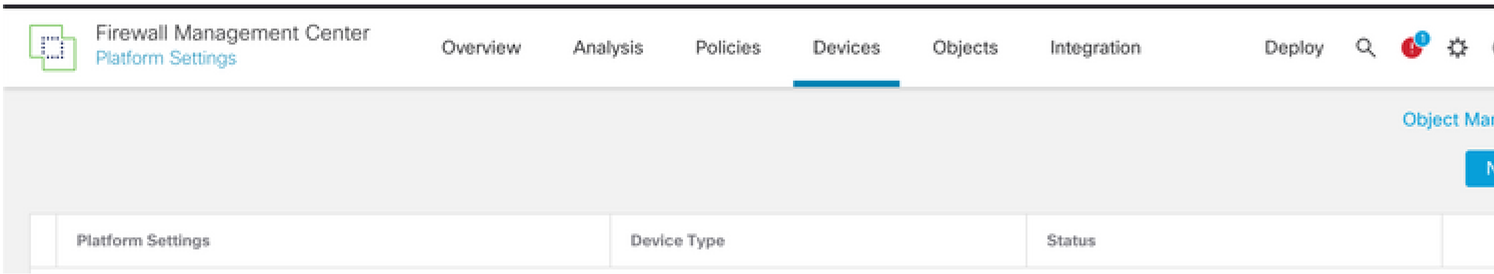
## Configure Platform Settings for Secure Firewall

## Introduction to Platform Settings

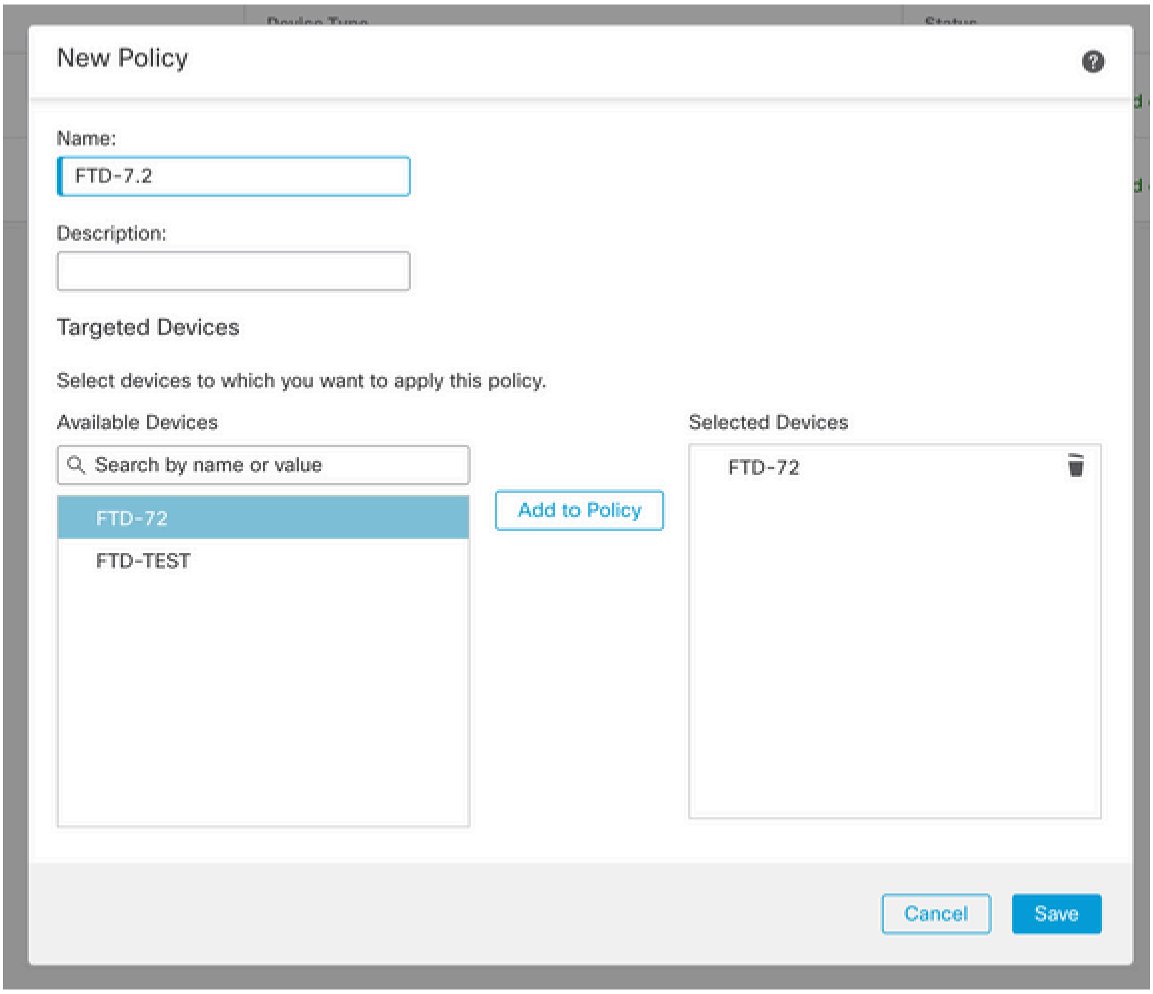
A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication. A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Read more about Platform Settings here.

To change Platform Settings, create a Policy if not already completed. If completed, skip to Configure TLS / DTLS Ciphers.

Navigate to Devices > Platform Settings and select New Policy to begin.



Assign the Firewall Threat Defense device to the policy.



New Policy

Name: FTD-7.2

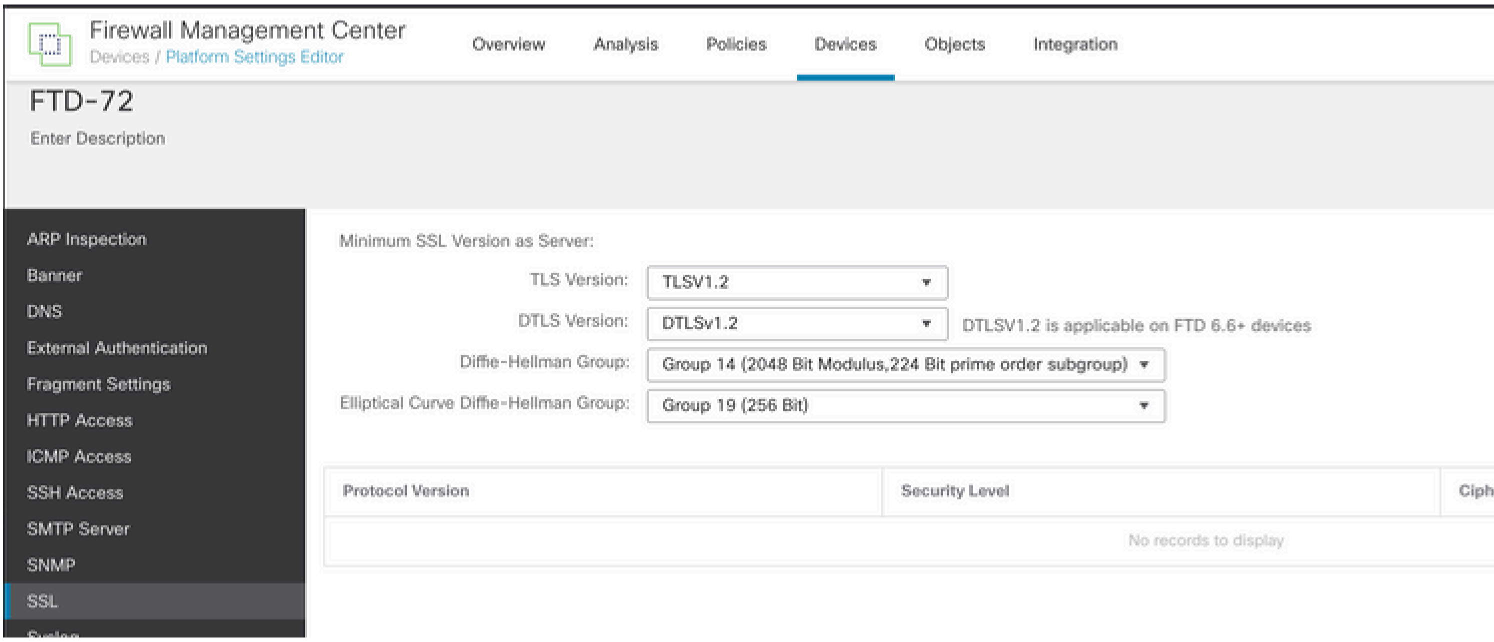
Description:

Targeted Devices

Select devices to which you want to apply this policy.

## Configure TLS / DTLS Ciphers

Navigate to SSL tab to access TLS / DTLS configuration. Create a custom cipher list by selecting the Add button.



Minimum SSL Version as Server:

TLS Version: TLSV1.2

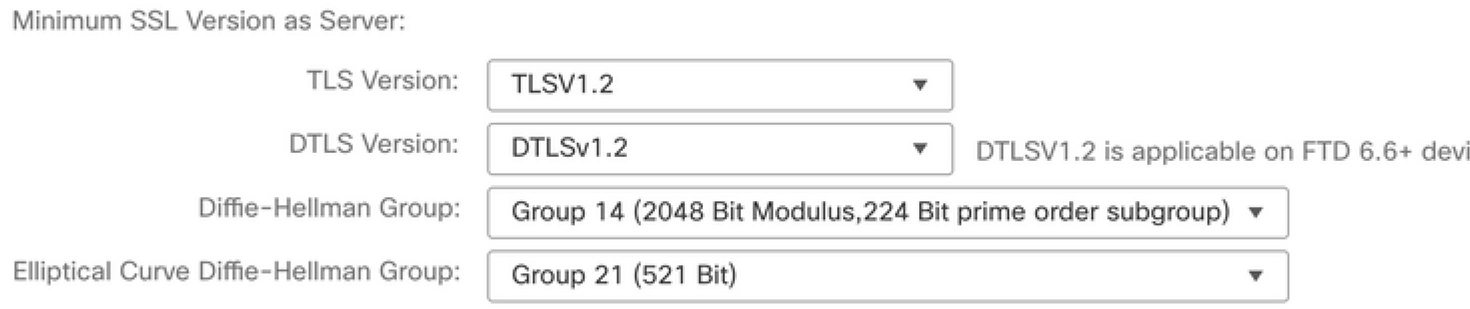
DTLS Version: DTLSv1.2 DTLSV1.2 is applicable on FTD 6.6+ devices

Diffie-Hellman Group: Group 14 (2048 Bit Modulus,224 Bit prime order subgroup)

Elliptical Curve Diffie-Hellman Group: Group 19 (256 Bit)

| Protocol Version | Security Level | Ciph |
|---|---|---|
| | No records to display | |

Change TLS / DTLS versions along with appropriate Elliptical Curve / Diffie-Hellman group values to fit your security needs.



Minimum SSL Version as Server:

TLS Version: TLSV1.2

DTLS Version: DTLSv1.2 DTLSV1.2 is applicable on FTD 6.6+ devi

Diffie-Hellman Group: Group 14 (2048 Bit Modulus,224 Bit prime order subgroup)

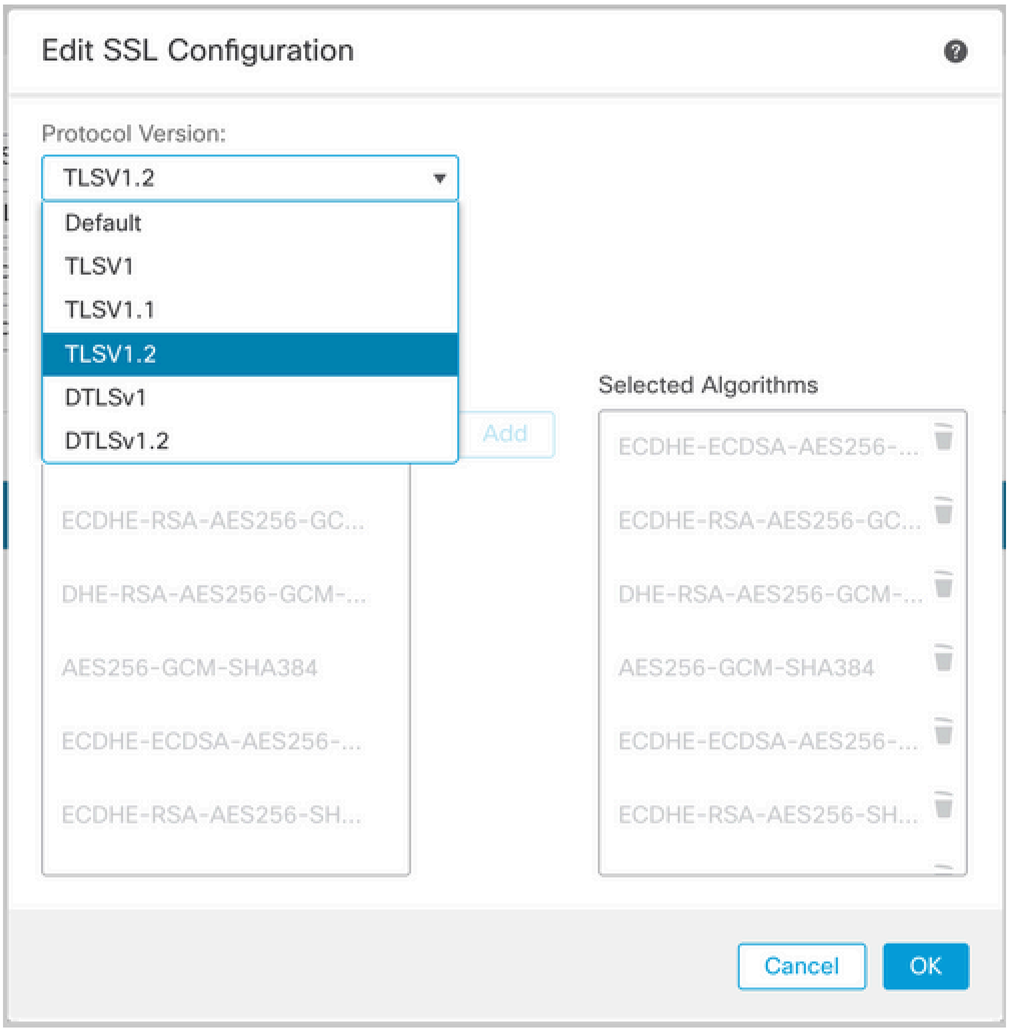
Elliptical Curve Diffie-Hellman Group: Group 21 (521 Bit)

---

**Note**: You can create your own custom list with custom supported attribute or select from the various levels of supported ciphers. Please select the list and cipher that best supports your security needs.

---

Select the protocol and cipher level.



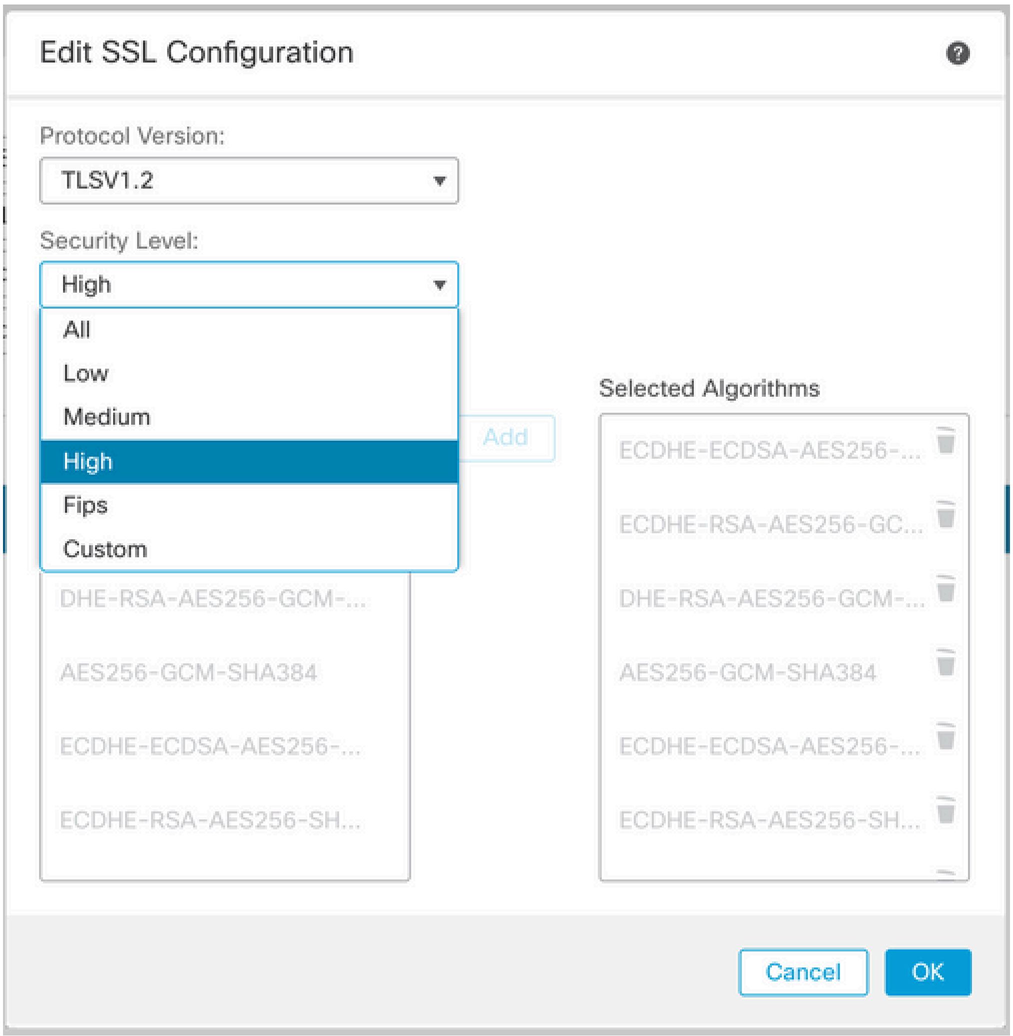
Edit SSL Configuration

Protocol Version: TLSV1.2

ECDHE-RSA-AES256-GC...
DHE-RSA-AES256-GCM-...
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-...
ECDHE-RSA-AES256-SH...

Selected Algorithms

ECDHE-ECDSA-AES256-...
ECDHE-RSA-AES256-GC...
DHE-RSA-AES256-GCM-...
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-...
ECDHE-RSA-AES256-SH...



Edit SSL Configuration

Protocol Version: TLSV1.2

Security Level: High

DHE-RSA-AES256-GCM-...

AES256-GCM-SHA384

ECDHE-ECDSA-AES256-...

ECDHE-RSA-AES256-SH...

Selected Algorithms

ECDHE-ECDSA-AES256-...

ECDHE-RSA-AES256-GC...

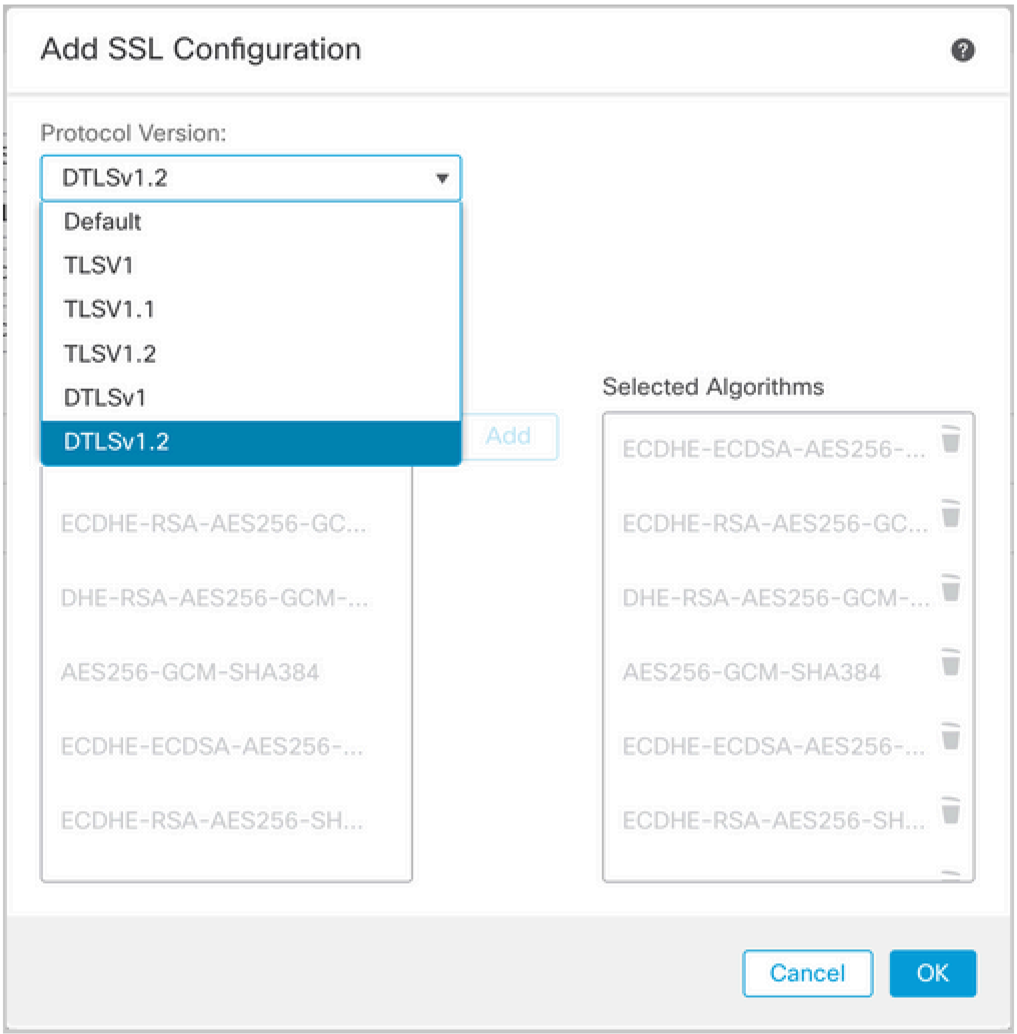
DHE-RSA-AES256-GCM-...

AES256-GCM-SHA384

ECDHE-ECDSA-AES256-...

ECDHE-RSA-AES256-SH...

Repeat the same process for DTLS.



Add SSL Configuration

Protocol Version: DTLSv1.2

ECDHE-RSA-AES256-GC...

DHE-RSA-AES256-GCM-...

AES256-GCM-SHA384

ECDHE-ECDSA-AES256-...

ECDHE-RSA-AES256-SH...

Selected Algorithms

ECDHE-ECDSA-AES256-...

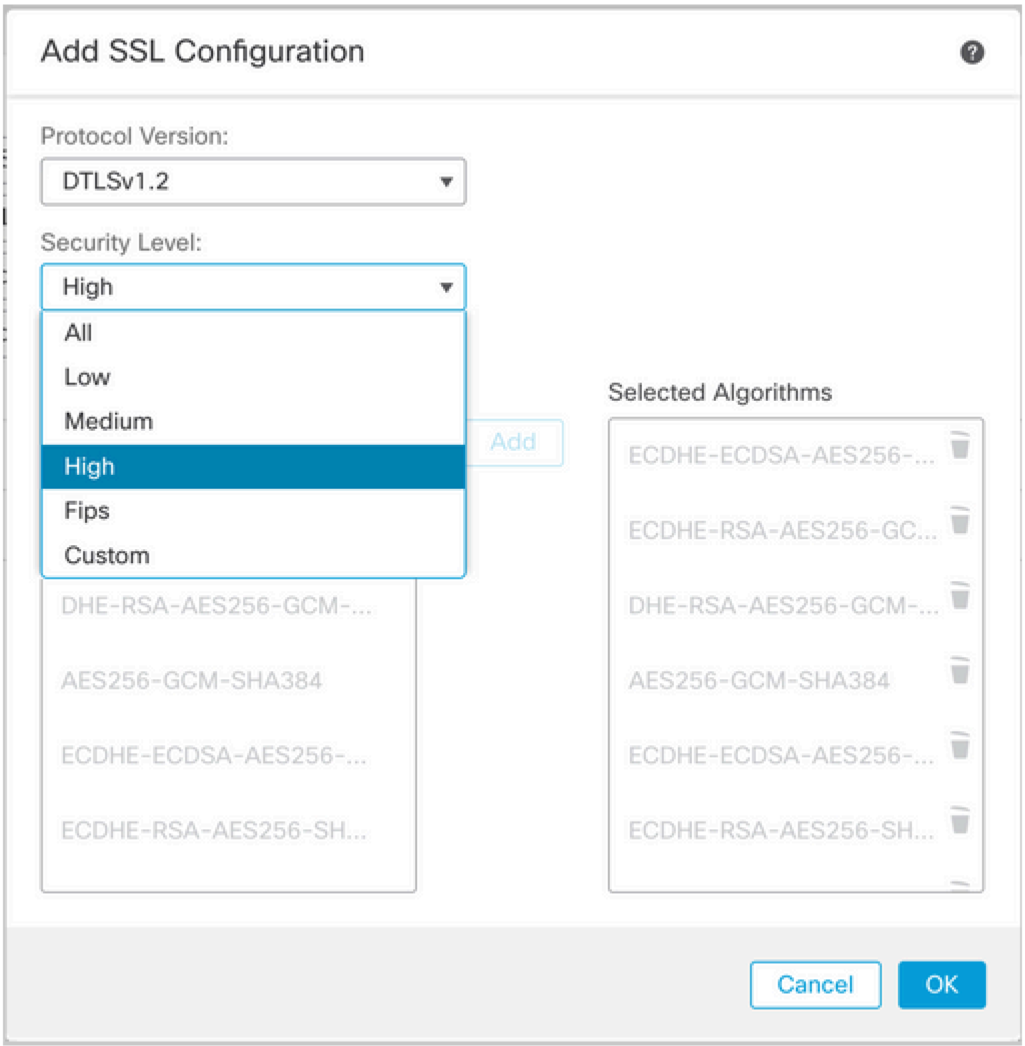
ECDHE-RSA-AES256-GC...

DHE-RSA-AES256-GCM-...

AES256-GCM-SHA384

ECDHE-ECDSA-AES256-...

ECDHE-RSA-AES256-SH...



Add SSL Configuration

Protocol Version: DTLSv1.2

Security Level: High

DHE-RSA-AES256-GCM-...

AES256-GCM-SHA384

ECDHE-ECDSA-AES256-...

ECDHE-RSA-AES256-SH...

Selected Algorithms

ECDHE-ECDSA-AES256-...

ECDHE-RSA-AES256-GC...

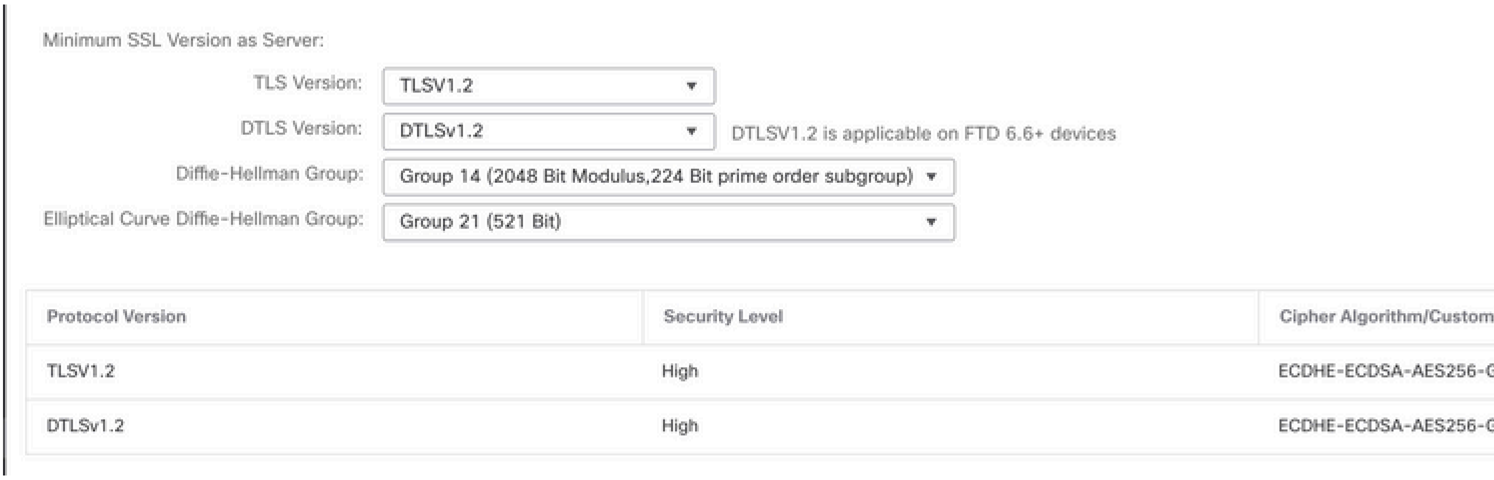
DHE-RSA-AES256-GCM-...

AES256-GCM-SHA384

ECDHE-ECDSA-AES256-...

ECDHE-RSA-AES256-SH...

Completed configuration in Secure Firewall Management Center.



Minimum SSL Version as Server:

TLS Version: TLSV1.2

DTLS Version: DTLSv1.2 DTLSV1.2 is applicable on FTD 6.6+ devices

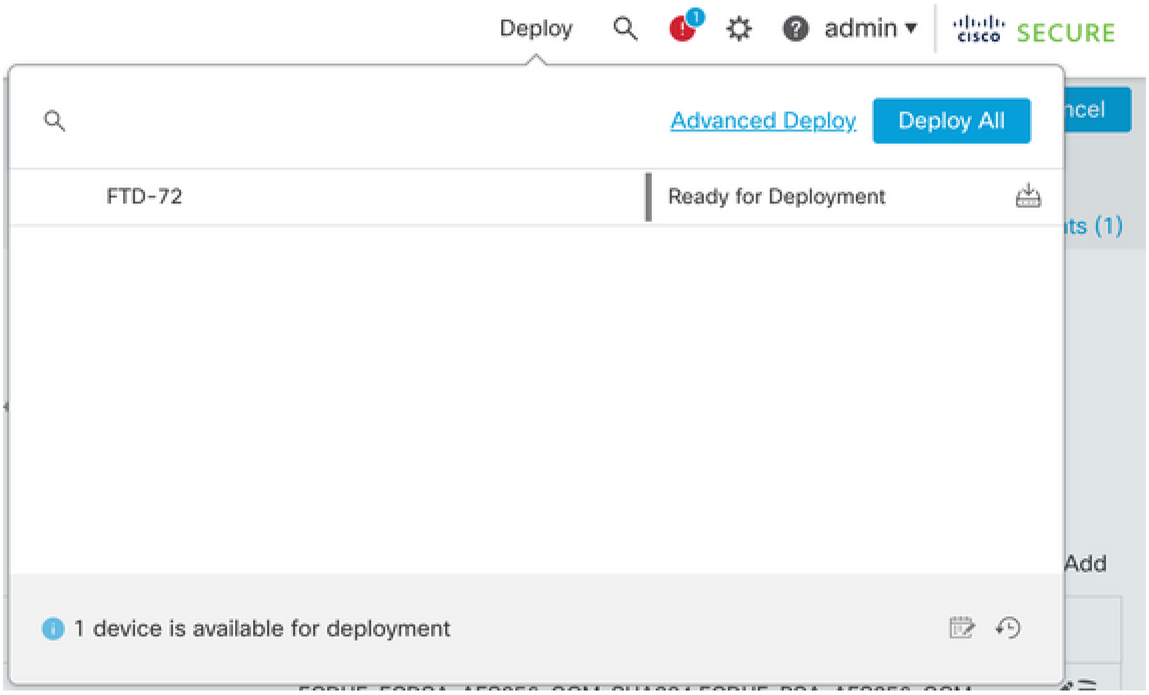
Diffie-Hellman Group: Group 14 (2048 Bit Modulus,224 Bit prime order subgroup)

Elliptical Curve Diffie-Hellman Group: Group 21 (521 Bit)

| Protocol Version | Security Level | Cipher Algorithm/Custom |
|---|---|---|
| TLSV1.2 | High | ECDHE-ECDSA-AES256-G |
| DTLSv1.2 | High | ECDHE-ECDSA-AES256-G |

Save configuration and deploy changes to the FTD.

> **Note**: These changes can be applied while users are connected. The TLS / DTLS ciphers negotiated for the Secure Client session only occur at the beginning of the session. If users are connected and you wish to make a change, existing connections are not to be disconnected. New connections to the Secure Firewall are to use the new secure ciphers.



FTD-72 Ready for Deployment

1 device is available for deployment

# Verify

After Secure Firewall Management Center has deployed the configuration to the Threat Defense device, you need to verify the ciphers are present in the FTD CLI. Open a terminal / console session to the device and issue the listed show commands and review their output.

## Verify from FTD CLI configuration

Ensure the selected TLS / DTLS list is shown with a **show run ssl**.

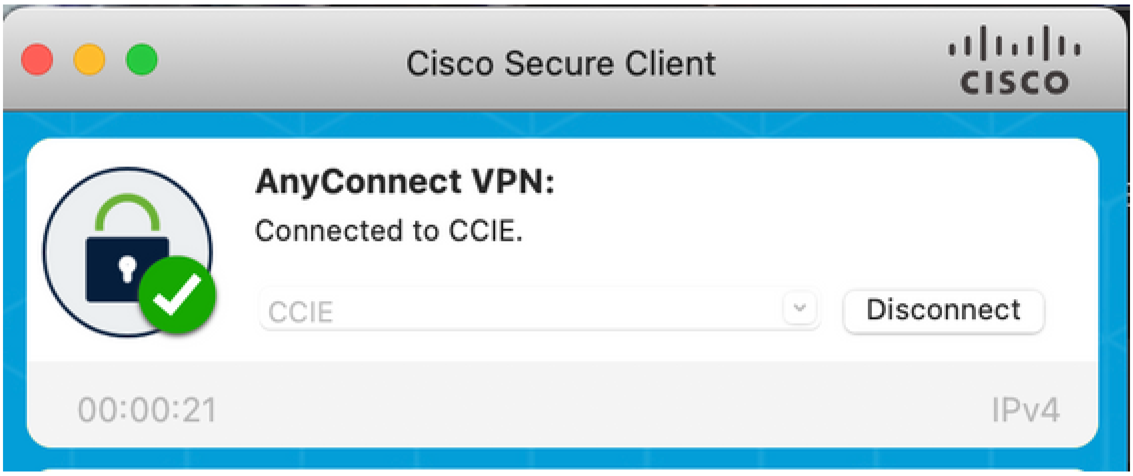
```
FTD72# show run ssl
ssl cipher tlsv1.2 high
ssl cipher dtlsv1.2 high
ssl ecdh-group group21
```

Ensure the selected TLS version to be negotiated along with Diffie-Hellman versions with a **show ssl.**

```
FTD72# show ssl
Accept connections using SSLv3 or greater and negotiate to TLSv1.2 or greater
Start connections using TLSv1.2 and negotiate to TLSv1.2 or greater
SSL DH Group: group14 (2048-bit modulus, FIPS)
SSL ECDH Group: group21 (521-bit EC)

SSL trust-points:
  Self-signed (RSA 2048 bits RSA-SHA256) certificate available
  Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
Certificate authentication is not enabled
```

## Verify from FTD CLI with Active Secure Client Connection

Connect Secure Client Session and review output from FTD CLI. To verify ciphers exchanged run this show command **show vpn-sessiondb detail anyconnect filter name *username*.**



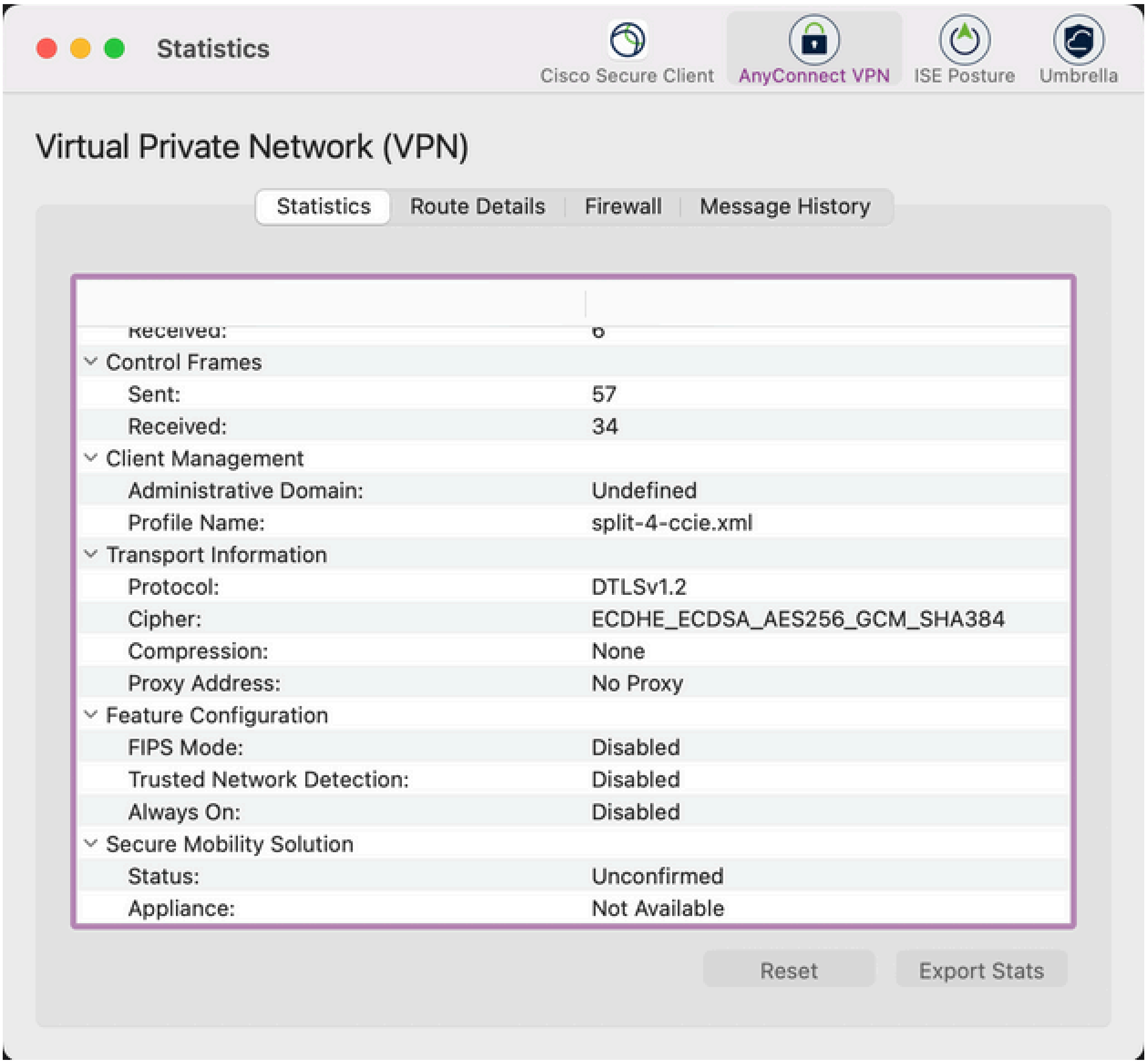
```
FTD72# show vpn-sessiondb detail anyconnect filter name trconner

Session Type: AnyConnect Detailed

Username     : trconner               Index        : 75
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 24350                  Bytes Rx     : 20451
Pkts Tx      : 53                     Pkts Rx      : 254
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : Split                  Tunnel Group : Split-4-CCIE
Login Time   : 08:59:34 UTC Fri Sep 9 2022
Duration     : 0h:01m:26s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a805810004b000631b0076
Security Grp : none

---Output Condensed-----

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 75.1
  TCP Src Port : 55581                  TCP Dst Port : 443

SSL-Tunnel:
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-RSA-AES256-GCM-SHA384
  Encapsulation: TLSv1.2                TCP Src Port : 55588

DTLS-Tunnel:
  Tunnel ID    : 75.3
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2              UDP Src Port : 64386
```

### Verify from Client with Active Secure Client Connection

Verification of negotiated ciphers on the Secure Client application.

Open the Secure Client application.

Navigate to Statistics > AnyConnect VPN > Statistics to investigate. The cipher listed must be cross checked against the Firewall Threat Defense to confirm.



Virtual Private Network (VPN)

| | |
|---|---|
| Received: | 6 |
| Control Frames | |
| Sent: | 57 |
| Received: | 34 |
| Client Management | |
| Administrative Domain: | Undefined |
| Profile Name: | split-4-ccie.xml |
| Transport Information | |
| Protocol: | DTLSv1.2 |
| Cipher: | ECDHE_ECDSA_AES256_GCM_SHA384 |
| Compression: | None |
| Proxy Address: | No Proxy |
| Feature Configuration | |
| FIPS Mode: | Disabled |
| Trusted Network Detection: | Disabled |
| Always On: | Disabled |
| Secure Mobility Solution | |
| Status: | Unconfirmed |
| Appliance: | Not Available |

# Troubleshoot

### Debug from FTD CLI

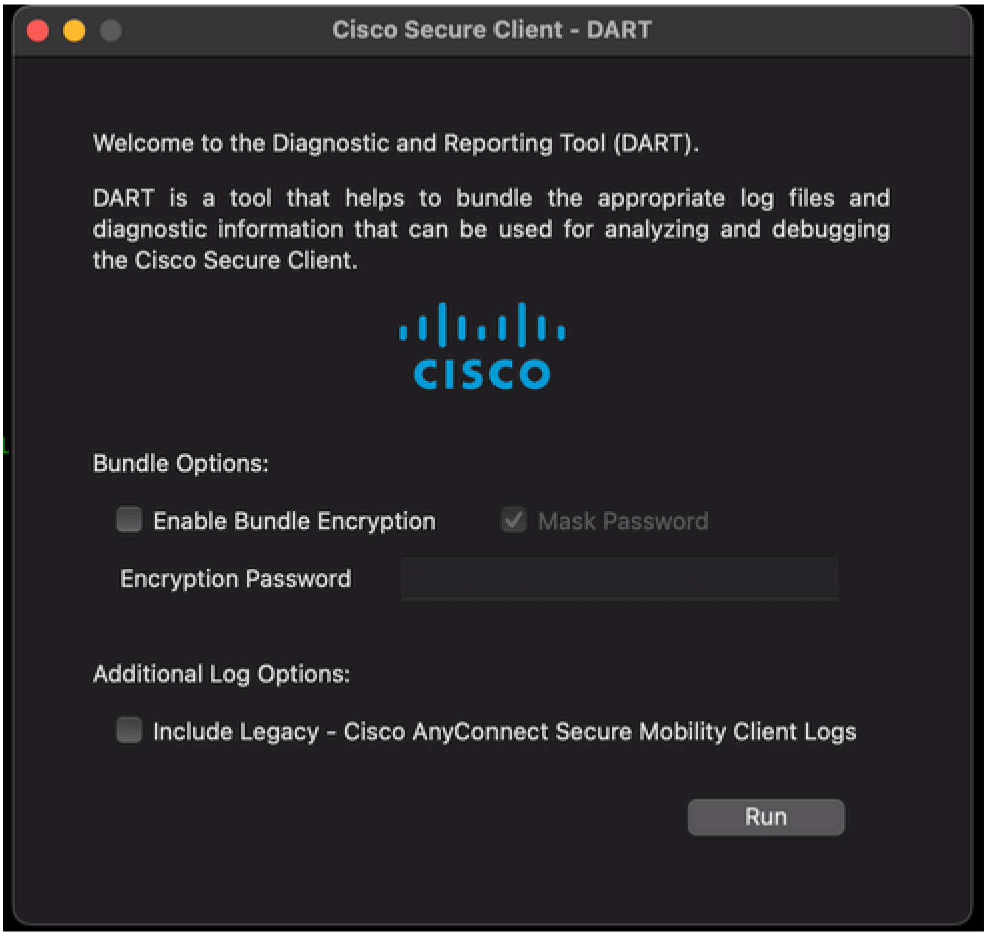
Connection errors on the Secure Client related to TLS / DTLS cipher exchanges can be investigated from the Firewall Threat Defense CLI with these debug commands.

```
debug ssl
debug ssl cipher
debug ssl state
debug ssl device
debug ssl packet
```

## Gather DART from Secure Client

Open Secure Client DART application and select Run.

> **Note**: If prompted for credentials please enter administrator level credentials to continue.



Welcome to the Diagnostic and Reporting Tool (DART).

DART is a tool that helps to bundle the appropriate log files and diagnostic information that can be used for analyzing and debugging the Cisco Secure Client.

Bundle Options:

☐ Enable Bundle Encryption ☑ Mask Password

Encryption Password

Additional Log Options:

☐ Include Legacy - Cisco AnyConnect Secure Mobility Client Logs

Gather a DART and debugs to engage Cisco TAC.

If deployed configuration as seen from Secure Firewall Management Center and Firewall Threat Defense CLI do not match. Please open a new case with Cisco TAC.