Hewlett Packard Enterprise

Technical Brief

HPE Aruba Networking EdgeConnect SD-WAN

Cryptographic Algorithms, Cipher Profiles, & Commercial Solutions for Classified (CSfC)

Orchestrator and ECOS Releases 9.4.4, 9.5.4, and 9.6.0

Contents

Important Notice

Revision C, August 2025

Open Source Code:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America

Document Conventions

1. Orchestrator releases are identified with three digits, e.g. 9.5.4. EdgeConnect OS (ECOS) release are identified with four digits, e.g. 9.5.4.0. Since most features depend on Orchestrator and ECOS, all releases will be designated with three digits.
2. CLI commands are displayed in console font: `system fips enable`

Document Revision History

Document Version	Description of Revisions	EdgeConnect Release	Release Date
Rev A	Initial version of this document.	EdgeConnect 9.2.0	August 2022
Not published	Updated to reflect changes for release of 9.4.0.	EdgeConnect 9.4.0	June 2024
Rev B	Updated to reflect changes for release of 9.4.4, 9.5.4., and 9.6.0.	EdgeConnect 9.4.4, 9.5.4, 9.6	May 2025
Rev C	Minor corrections	EdgeConnect 9.4.4, 9.5.4, 9.6.0	August 2025

Introduction

This document covers all cryptographic suites used by HPE Aruba Networking EdgeConnect gateways including management plane connections to Orchestrator and Cloud Portal, and data plane connections between EdgeConnect appliances, as well as between EdgeConnect appliances and third-party devices. Figure 1 depicts all management plane and data plane connections to Orchestrator and EdgeConnect gateways.

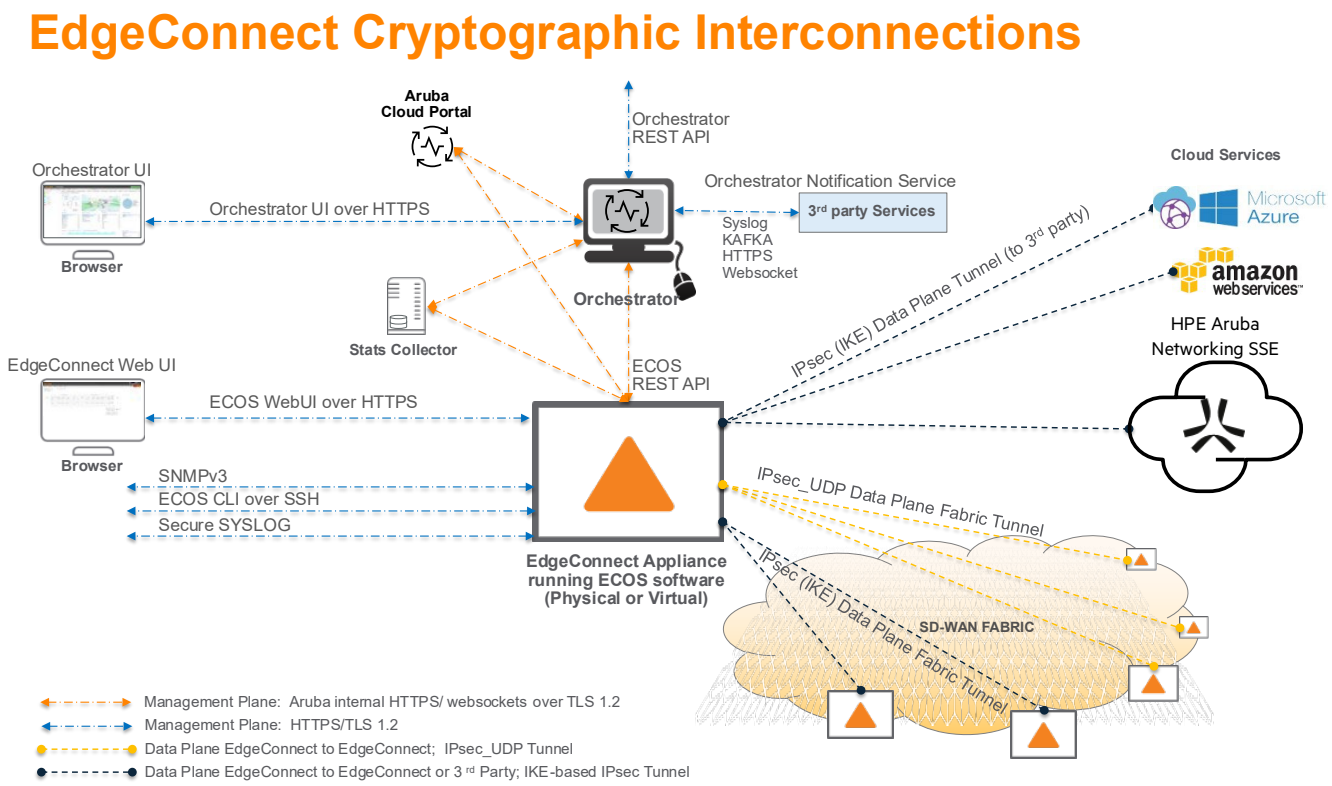

Figure 1: EdgeConnect Cryptographic Interconnections

Management Plane Interfaces

The following management interfaces can be used to configure or provision EdgeConnect gateways/appliances running ECOS software.

Orchestrator User Interface

Orchestrator acts as an aggregation layer for configuration, provisioning, monitoring, and reporting for all EdgeConnect gateways in an SD-WAN. Administrative users interact with the Orchestrator user interface (UI) to orchestrate policies in the SD-WAN, manage templates across all or subsets of appliances, configure site-specific parameters on EdgeConnect appliances.

Orchestrator API

For machine-to-machine systems integration, Orchestrator provides a RESTful Application Programming Interface (API). Using the API, configuration actions (POST, PUT, DELETE) and queries (GET) can be applied to all appliances or a single appliance using the NE Primary Key (NE.Pk) as an identifier. The REST API runs over a secure WebSocket connection using TLS 1.2 between the Orchestrator and the ECOS appliance.

Orchestrator Notification Service

Orchestrator Notification Service provides real-time streaming of EdgeConnect and Aruba Orchestrator alarms or Orchestrator logs. Depending on the protocol, Orchestrator will act as server or client.

ECOS Web User Interface

Administrative users can use the Web User Interface (Web UI), which provides a highly intuitive, graphical interface for the comprehensive set of ECOS capabilities. The Web UI can be accessed from a TLS-enabled web browser using HTTPS on logical port 443. It is always recommended to use Orchestrator for all provisioning and configuration.

ECOS SNMP

The EdgeConnect SNMP interface supports Management Information Base (MIB-II) as described in RFC 1213. This interface is used to receive notifications or traps from the appliance whenever an alarm is raised or cleared. SNMP is not used for configuration.

ECOS CLI Over SSH

Administrative users can use the CLI to perform security-sensitive and non-security-sensitive monitoring and configuration. The CLI can be accessed remotely by using the SSHv2 secured management session over the Ethernet ports. CLI is typically only used for diagnostic and/or troubleshooting. CLI should not be used for general provisioning, all provisioning/configuration should be performed on Orchestrator.

ECOS Appliance-Level API

EdgeConnect appliances running ECOS software provide an appliance-level API. This interface is used for all configuration, provisioning, monitoring, and reporting between the Orchestrator and the ECOS appliance. Administrative users typically do not access the ECOS API. However, to reduce Orchestrator workload when gathering minute-granularity network statistics, it is suggested to collect the stats directly from the appliance API for all appliances, and not Orchestrator.

ECOS Secure Logging

EdgeConnect appliances provide secure transport to remote log receivers, providing the flexibility of shipping logs using TCP_SSL (TLSv1.2). ECOS also provides the option to configure client-side end-entity certificates if required by the Syslog server.

Data Plane Interfaces

IPSec tunnels are used as data plane transport. EdgeConnect to EdgeConnect tunnels are referred to as “SD-WAN Fabric” tunnels and are automatically created and managed through Orchestration. SD-WAN fabric tunnels use IPSec UDP tunnels by default. For customers that require FIPS and Common Criteria compliance, standard, IKE-based IPSec tunnels can be used.

IPSec tunnels to Security Service Edge (SSE) and Infrastructure-as-a-Service (IaaS) partners always use standard, IKE-based IPSec tunnels

TLS Cipher Suite Notation Introduction

There are 4 parts in the cipher name.

1. Key exchange algorithm: for example, ECDHE
2. Authentication algorithm: for example, RSA
3. Symmetric encryption algorithm: AES-CBC mode 128 bits or AES-GCM mode 128 bits

4. Message authentication code (MAC) algorithm: SHA-256

Examples of common ciphers used in ECOS for TLS 1.2:

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Cipher input string syntax follows the format specified by openssl.org at:

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

FIPS Mode

Self-hosted/On-prem Orchestrator and ECOS 9.4 are FIPS compliant against FIPS 140-2, Level 1 security.

FIPS mode is disabled by default on Orchestrator and ECOS. In FIPS mode, certain ciphers are restricted, and entropy sources must pass self-tests to provide underlying services.

Enabling FIPS Mode on Orchestrator

On self-hosted/on-prem Orchestrator command line interface:

```
root@orchestrator:/root$ fips-mode-setup --check
FIPS mode is disabled.
root@orchestrator:/root$ fips-mode-setup --enable
Setting system policy to FIPS
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies to
fully take place.  FIPS mode will be enabled.
Please reboot the system for the setting to take effect.
root@orchestrator:/root$ reboot
```

Enabling FIPS Mode on EdgeConnect

On ECOS, FIPS mode is enabled via CLI Command.

In Release 9.4.0.0 – 9.4.2.0:

Execute **`fips enable`**

Execute **`fips enable noconfirm`** Use for machine-to-machine or API automation

Execute **`fips show`** show status

In Release 9.4.3 and later:

Execute **`system fips enable`**

Execute **`system fips enable noconfirm`** Use for machine-to-machine or API automation

Execute show **`system fips`** show status

Common Criteria Mode

Self-hosted/On-prem Orchestrator[1] and ECOS 9.4 introduce Common Criteria mode compliant with three protection profiles:

1. Common Criteria Network Device Collaborative Protection Profile v2.2e.
2. PP-Module for Virtual Private Networks version 1.3.
3. collaborative PP-Module for Stateful Traffic Filter Firewalls v1.4e.

Common Criteria is disabled by default on Orchestrator and ECOS. In Common Criteria mode, certain ciphers are restricted, and ALL TLS connections require X.509 certificate validation.

Enabling Common Criteria mode on Orchestrator

On self-hosted/on-prem Orchestrators, Common Criteria mode is enabled in Orchestrator Advanced Properties.

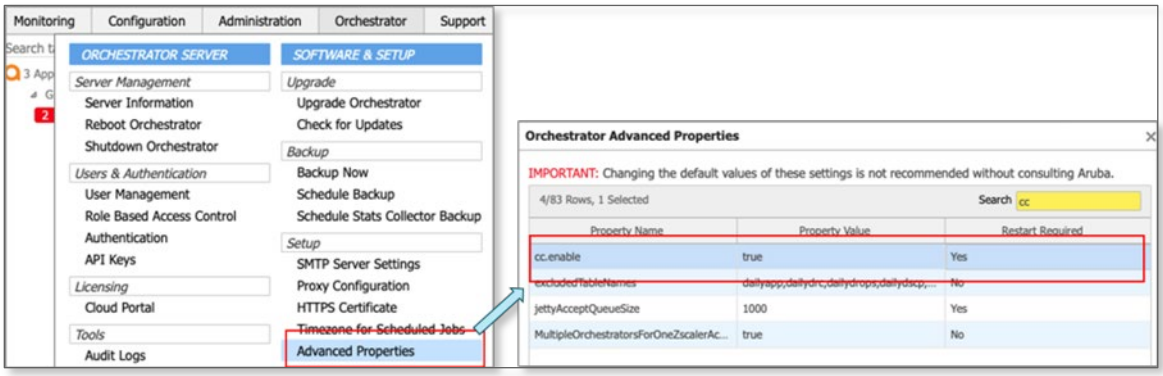

Figure 2: Common Criteria Mode on Orchestrator

Enabling Common Criteria mode on EdgeConnect

On ECOS, Common Criteria mode is enabled via CLI Command.

In Release 9.4.0.0 – 9.4.2.0:

Execute **`cc enable`**

Execute **`cc enable noconfirm`** Use for machine-to-machine or API automation

Execute **`cc show`** show status

In Release 9.4.3 and later:

Execute **`system cc enable`**

Execute **`system cc enable noconfirm`** Use for machine-to-machine or API automation

Execute show **`system cc`** show status

[1] Common Criteria mode is not applicable for Orchestrator-as-a-Service.

EdgeConnect Management Plane Cryptographic Algorithms, Releases Prior to 9.4.4 and 9.5.4

ECOS TLS as Server and Client (prior to ECOS 9.4.4, 9.5.4)

Starting with ECOS 9.0.3 and Orchestrator 9.0.4, the Session Management template provides a way to directly enter an OpenSSL Cipher List if required by the enterprise customer security team. This is intended to be used only by enterprise customers who have strict security requirements and want to set their own ciphers Web UI (TLS server). Orchestrator provides the Session Management template option that orchestrates the TLS cipher setting across all appliances. For more information on the Session Management template, see Session Management Template in the Orchestrator User Guide.

Figure 3 shows the Templates tab with the Session Management template expanded. A warning informs users to test the proposed cipher in their environment to ensure compatibility with connected systems.

NOTE: Starting with Releases 9.4.4 and 9.5.4, Cipher Profile settings should be used.

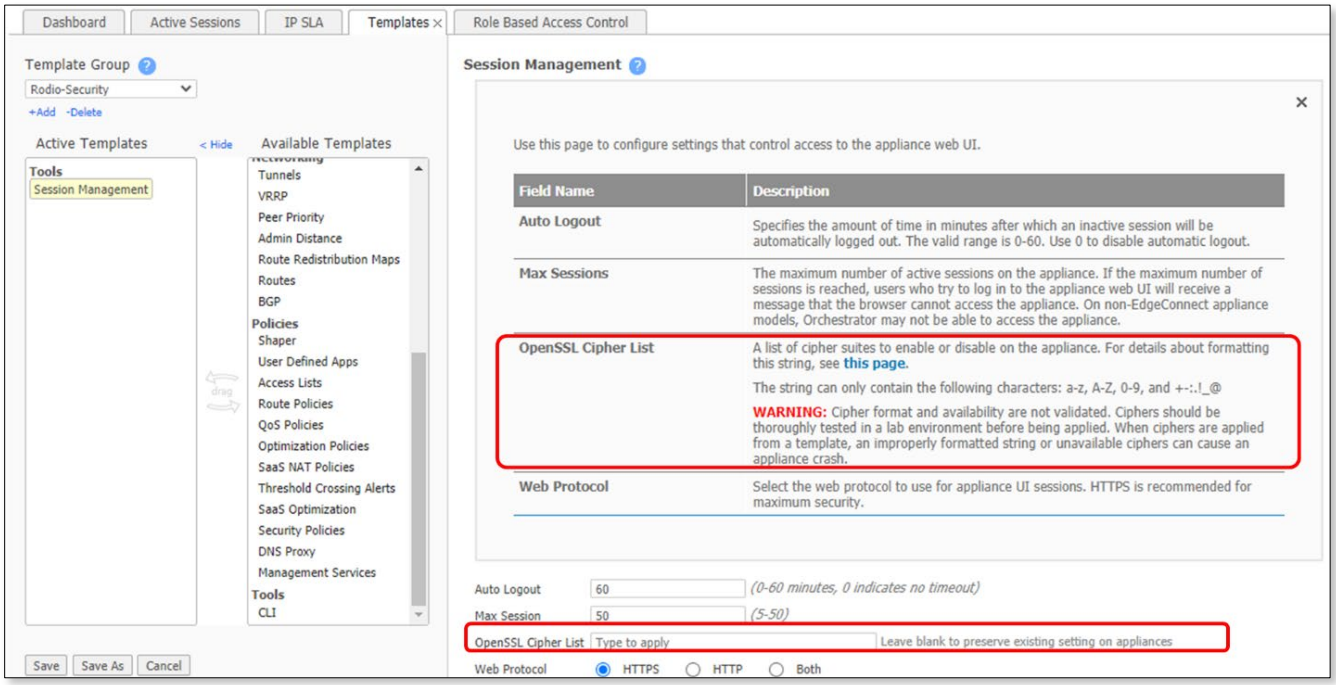

Figure 3: Session Management Template with Explicit Cipher control (use with releases < 9.4.4)

TLS Cipher Suites supported on ECOS Release 9.2 are dependent on whether Common Criteria mode is enabled.

Table 1: TLS Cipher Suites – ECOS <9.4.4, FIPS Enabled or Disabled, Common Criteria Disabled

TLS Suite	ECOS <9.4.4, FIPS Enabled or Disabled, Common Criteria Mode Disabled
1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
3	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
4	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384

5	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
6	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
7	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
8	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
9	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
10	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
11	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
12	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
13	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
14	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
15	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
16	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
17	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
18	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
19	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
20	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
21	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
22	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
23	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256

NOTE: ECOS 8.3.2, 9.0, and 9.1 remove the support of RSA as key exchange mechanism (removal of Static Key Ciphers).

NOTE: Curve is secp256r1 for releases < 9.4.4.

Table 2: TLS Cipher Suites – ECOS <9.4.4, FIPS Enabled or Disabled, Common Criteria Enabled

TLS Suite	ECOS <9.4.4, FIPS Enabled or Disabled, Common Criteria Mode Enabled
1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

4	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
5	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
6	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
7	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
8	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
9	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
10	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
11	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
12	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

SNMP (prior to ECOS 9.5.4)

Prior to ECOS 9.5.4, SNMPv3 encryption and authentication algorithms are fixed. ECOS 9.5.4 includes SNMP in Cipher Profiles. For more information, see SNMPv3 (ECOS).

Table 3: SNMPv3 Encryption Algorithms (prior to ECOS 9.5.4)

Encryption	ECOS	Mode
AES_128 (Default)	All releases (prior to ECOS 9.4.4, 9.5.4)	CBC

Table 4: SNMPv3 Hash Algorithms (prior to ECOS 9.5.4)

Hash	ECOS
SHA-1 (Default)	All releases (prior to ECOS 9.4.4, 9.5.4)

SSH

Starting with ECOS 9.0.2, SSH configuration is performed on the ECOS CLI.

CLI configuration is no longer required starting with release 9.4.4+, 9.5.4+ when using Cipher Profile settings. For more information, see SSH (ECOS).

Table 5: SSHv2 MAC Algorithms

MAC	ECOS
SHA-1	All releases prior to 9.4.2; removed as a default in Release 9.4.2
hmac-sha1-96	(starting with ECOS 9.4.2)
hmac-sha2-256	Default (starting with ECOS 9.4.2)
hmac-sha2-512	(starting with ECOS 9.4.2)

Table 6: SSHv2 Encryption Algorithms

Encryption	ECOS	Mode
AES_128	Default (prior to ECOS 9.4.2)	CBC and CTR
AES_192	All releases	CBC and CTR
AES_256	All releases	CBC and CTR
aes128-gcm@openssh.com	All releases	GCM
aes256-gcm@openssh.com	All releases	GCM

Table 7: SSHv2 Key Exchange Algorithms

Key Exchange	ECOS
Diffie-Hellman Group 1-SHA1	All Releases
Diffie-Hellman Group 14-SHA1	Default prior to 9.3.4
Diffie-Hellman Group 14-SHA256	Default starting with 9.3.4
Diffie-Hellman Group 16-SHA512	All releases
Diffie-Hellman Group 18-SHA512	All releases
diffie-hellman-group-exchange-sha1	All releases
diffie-hellman-group-exchange-sha256	All releases
ecdh-sha2-nistp256	All releases
ecdh-sha2-nistp384	All releases
ecdh-sha2-nistp512	All releases
curve25519-sha256	All releases
curve25519-sha256@libssh.org	All releases

ECOS 9.3.4 added additional SSH settings: Host Key Algorithms, Public Key Algorithms Accepted, and CA-Signed Algorithms Accepted.

Table 8: SSHv2 Host Key Algorithms (ECOS 9.3.4+)

Host Key Algorithms	ECOS
ecdsa-sha2-nistp256-cert-v01@openssh.com	ECOS Release starting with 9.3.4
ecdsa-sha2-nistp384-cert-v01@openssh.com	ECOS Release starting with 9.3.4

ecdsa-sha2-nistp521-cert-v01@openssh.com	ECOS Release starting with 9.3.4
ssh-ed25519-cert-v01@openssh.com	ECOS Release starting with 9.3.4
rsa-sha2-512-cert-v01@openssh.com	ECOS Release starting with 9.3.4
rsa-sha2-256-cert-v01@openssh.com	ECOS Release starting with 9.3.4
ssh-rsa-cert-v01@openssh.com	ECOS Release starting with 9.3.4
ecdsa-sha2-nistp256	ECOS Release starting with 9.3.4
ecdsa-sha2-nistp384	ECOS Release starting with 9.3.4
ecdsa-sha2-nistp521	ECOS Release starting with 9.3.4
ssh-ed25519	ECOS Release starting with 9.3.4
rsa-sha2-512	ECOS Release starting with 9.3.4
rsa-sha2-256	ECOS Release starting with 9.3.4
ssh-rsa	ECOS Release starting with 9.3.4

Table 9: SSHv2 Public Key Algorithms Accepted (ECOS 9.3.4+)

Public Key Algorithms Accepted	**ECOS**
ecdsa-sha2-nistp256-cert-v01@openssh.com	ECOS Release starting with 9.3.4
ecdsa-sha2-nistp384-cert-v01@openssh.com	ECOS Release starting with 9.3.4
ecdsa-sha2-nistp521-cert-v01@openssh.com	ECOS Release starting with 9.3.4
ssh-ed25519-cert-v01@openssh.com	ECOS Release starting with 9.3.4
rsa-sha2-512-cert-v01@openssh.com	ECOS Release starting with 9.3.4
rsa-sha2-256-cert-v01@openssh.com	ECOS Release starting with 9.3.4
ssh-rsa-cert-v01@openssh.com	ECOS Release starting with 9.3.4
ecdsa-sha2-nistp256	ECOS Release starting with 9.3.4
ecdsa-sha2-nistp384	ECOS Release starting with 9.3.4
ecdsa-sha2-nistp521	ECOS Release starting with 9.3.4
ssh-ed25519	ECOS Release starting with 9.3.4
rsa-sha2-512	ECOS Release starting with 9.3.4

rsa-sha2-256	ECOS Release starting with 9.3.4
ssh-rsa	ECOS Release starting with 9.3.4

Table 10: SSHv2 CA Sign Algorithms Accepted (ECOS 9.3.4+)

CA Sign Algorithms Accepted	ECOS
ecdsa-sha2-nistp256	ECOS Release starting with 9.3.4
ecdsa-sha2-nistp384	ECOS Release starting with 9.3.4
ecdsa-sha2-nistp521	ECOS Release starting with 9.3.4
ssh-ed25519	ECOS Release starting with 9.3.4
rsa-sha2-512	ECOS Release starting with 9.3.4
rsa-sha2-256	ECOS Release starting with 9.3.4
ssh-rsa	ECOS Release starting with 9.3.4

ECOS Secure Logging

ECOS R9.2 introduced secure logging with configurable options:

1. Verify the server certificate (Required for Common Criteria Mode).
2. Upload client certificate for client to authenticate itself with the remote log receiver.
3. Flexibility of configuring any port.

For more information on logging, see Logging Template in the Orchestrator User Guide.

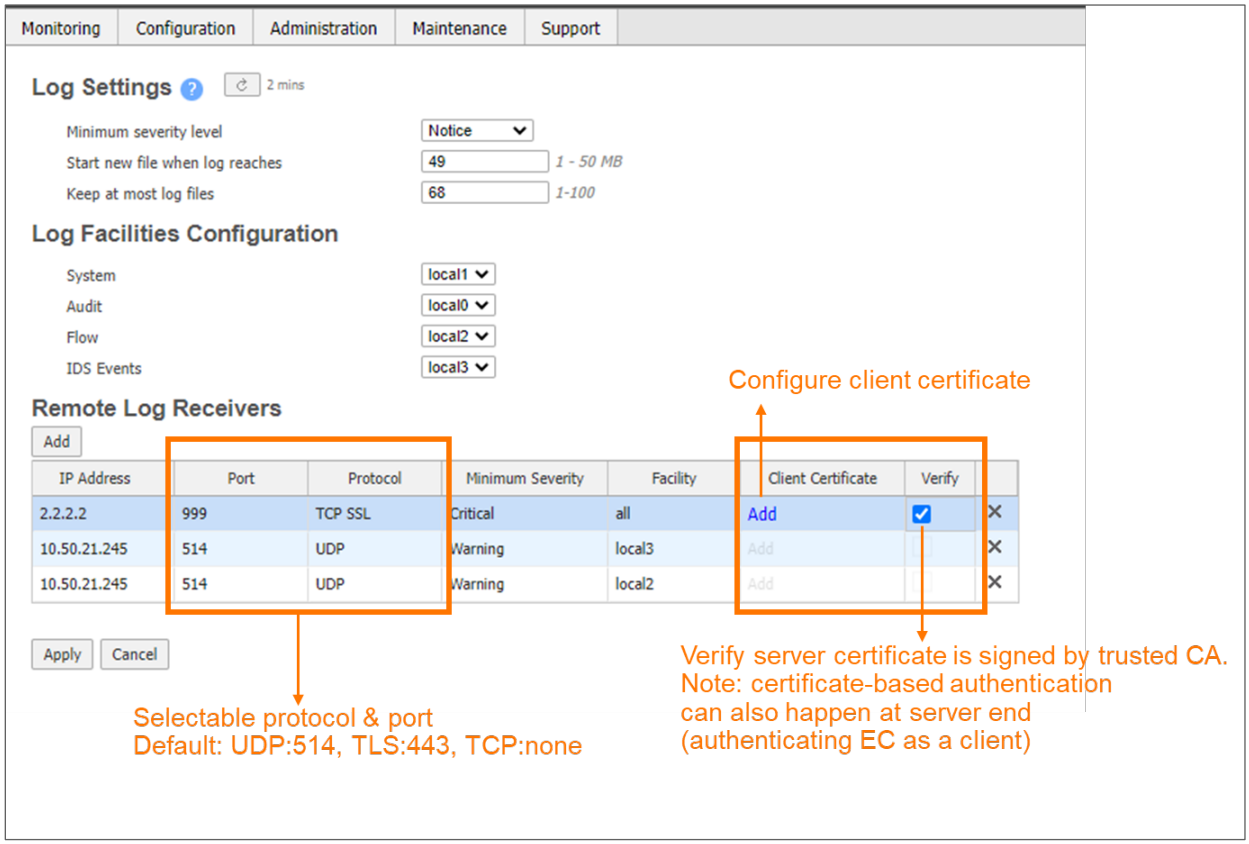

Figure 4 ECOS Secure Logging

The following table summarizes peer certificate authentication options for syslog server.

Table 11: Summary of ECOS Secure Logging Options

Client End-entity Certificate	Verify Option Selected	Behavior
No	No	This option should be used if the Syslog server is not configured to request a client certificate. EC does not verify the server certificate.
Yes	No	EC shares the client certificate with the server during TLS handshake. EC does not verify the server certificate.

Client End-entity Certificate	Verify Option Selected	Behavior
No	Yes	EC verifies the server certificate is from a trusted CA in the trust store. If a custom CA is used by the server, but the custom CA is not in the trust store, the connection fails. Additionally, if the server is configured to verify the client certificate, but no client certificate is configured, the connection fails.
Yes	Yes	EC shares client certificate with the server during TLS handshake. EC validates the server certificate.

EdgeConnect Data Plane Cryptographic Algorithms (IPSec)

Secure connections between EdgeConnect gateways are also referred to as Underlay Tunnels (UT). UTs have the option to use either proprietary IPSec UDP tunnels or standard, IKE-based IPSec tunnels. Orchestrated tunnel options are configured on a per-label basis. IPSec UDP tunnels are the default. IKE-based IPSec tunnels must be used for EdgeConnect-to-EdgeConnect secure connections if any of the following are required:

- FIPS compliance
- Common Criteria compliance
- Certificate-based peer authentication
- RFC 8784 Post Quantum Pre-Shared Key

Secure connections between EdgeConnect gateways and third-party services (including HPE SSE), also referred to as Passthrough Tunnels (PT), must use IKE-based IPSec tunnels.

EdgeConnect-to-EdgeConnect Underlay Tunnels, IPSec UDP

EdgeConnect uses a proprietary IPSec UDP technique to construct EdgeConnect to EdgeConnect IPsec Tunnels which provides advantages:

- Scalability / Faster tunnel establishment which accelerates the time required for EdgeConnect-to-EdgeConnect tunnels to be established. For example, after an ECOS software upgrade or reboot, an EdgeConnect Gateway may have to reestablish thousands of tunnels.
- IPSec UDP enables Edge-High Availability (Edge-HA) deployment configuration with multiple appliances at the same location, behind the same NAT.

IPSec UDP uses Orchestrator for Key Establishment, whereas IKE-based IPSec uses Diffie-Hellman. Starting with Release 9.4, Orchestrator uses FIPS-certified cryptographic modules.

EdgeConnect-to-Orchestrator Authentication

For EdgeConnect appliances to authenticate with their associated Orchestrator, newly installed EdgeConnect devices must first establish trust with Silver Peak’s Cloud Portal. Once trust is established with Cloud Portal, trust is established between the EdgeConnect appliance and its Orchestrator.

EdgeConnect hardware appliances authenticate to Cloud Portal with a built-in shared secret. Aruba virtual appliances require the account name and account key.

IPSec UDP Key Derivation and Establishment

Key Derivation and Establishment for IPSec UDP tunnels utilizes a proprietary process.

EdgeConnect appliances derive encryption keys for IPSec UDP tunnels by cryptographically combining two components:

- Orchestrator-derived ephemeral key material
- EdgeConnect nonce (Orchestrator provides the Nonce values as part of the tunnel configurations when the tunnel is created.)

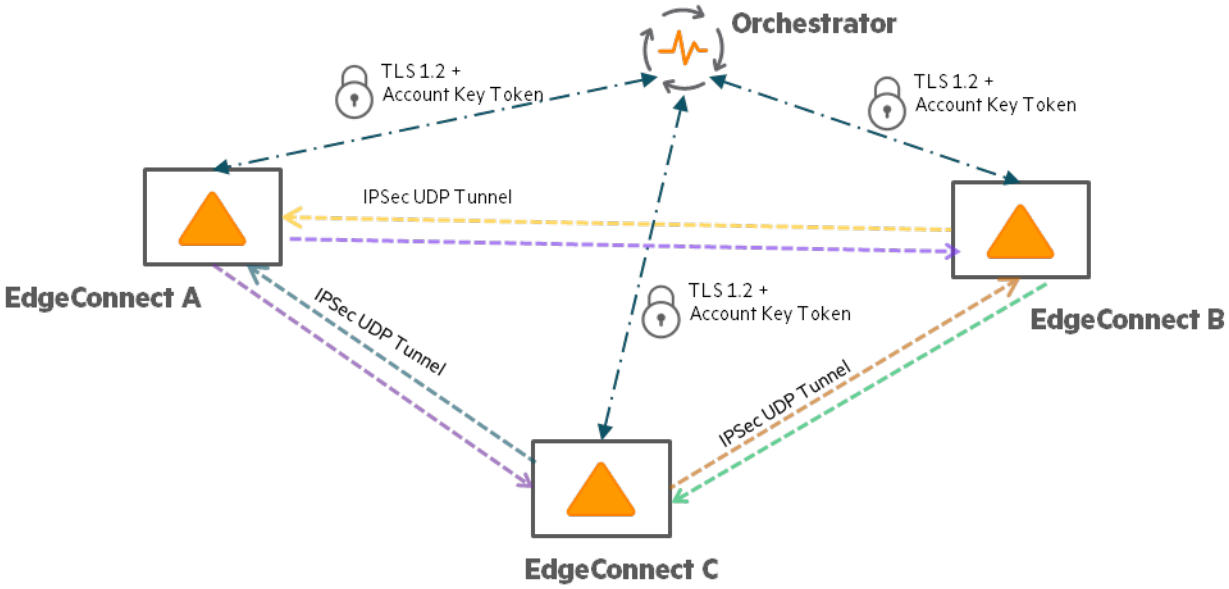

Figure 5: EdgeConnect Encryption Key Derivation

The derived encryption keys used in IPSec UDP tunnels are never sent on the wire (data plane or management plane). They are independently and uniquely derived per EdgeConnect appliance, Underlay Tunnel (UT), and direction. Orchestrator generates ephemeral key material, which is a time-varying “seed”, and distributes this key material to all appliances. Therefore, the key material is global to all appliances in the SD-WAN but varies by time.

NOTE: Orchestrator provides key material and not the encryption key itself. Key material lifetime, rotation period, and appliance storage/persistence are managed by Orchestrator.

At the time Orchestrator establishes tunnels between EdgeConnect gateways, Orchestrator sets the per-tunnel-direction nonces. Thereafter, EdgeConnect persists nonces per underlay tunnel (UT) and per direction which is static over the lifetime of the tunnel. When combined, every UT and direction has globally unique, time-varying encryption keys.

- Orchestrator generates and distributes key material (seed)
    - Global to Fabric
    - Time-varying
    - Rotation timing configured on Orchestrator
    - Distributed over secure management plane using TLS 1.2 + Account Key Token
    - Option to not persist on EdgeConnect. The reason for persisting the global seed is so that in case the EdgeConnect is shut down and restarted, it will have the global seed needed to form the encryption key without dependency on communications with Orchestrator.
    - 256-bit random number for both Nonce and Seed
- Nonce: local to EdgeConnect
    - Created when Orchestrator establishes the Underlay Tunnel
    - unique for every unidirectional SA (one-way IPSec tunnel)
- 32-byte Nonce and 32-byte Seed are concatenated and hashed using SHA-512 to form a 64-byte (512 bit) master secret

- Resulting keys are stored only in memory and are never sent on the wire

IPSec UDP Encryption Algorithms

Table 12: IPSec UDP – Encryption Algorithms

Encryption	ECOS	Mode
"Auto" is default on Orchestrator UI. **"Auto" for IPSec UDP = AES_128_CBC**	All releases	CBC
AES_128_CBC	All releases	CBC
AES_256_CBC	All releases	CBC
AES_128_GCM_16	ECOS 9.2+	GCM
AES_256_GCM_16	ECOS 9.2+	GCM

Table 13: IPSec UDP – Message Authentication Algorithms

Message Authentication	ECOS	Integrity Check Value (ICV) (Authentication Tag) Length
SHA-1 (Default)	All releases	12 octets
SHA-2 256	All releases	16 octets
SHA-2 384	All releases	24 octets
SHA-2 512	All releases	32 octets
AES_128_GCM	ECOS 9.2+	16 octets
AES_256_GCM	ECOS 9.2+	16 octets
AES_128_GMAC	ECOS 9.2+	16 octets
AES_256_GMAC	ECOS 9.2+	16 octets

NOTE: GCM mode includes authentication.

EdgeConnect to EdgeConnect Underlay and Passthrough Tunnels, IKE-based IPSec

Table 14: IKE-based IPSec – Key Exchange Algorithms

Key Exchange	ECOS	Peer Authentication
IKEv1 **(Default in all releases < ECOS 9.2.1)**	Available in All releases	Pre-shared Key
IKEv2	Available starting with ECOS 8.3+ Default starting with ECOS 9.2.1	Pre-shared Key

Table 15: IKE-based IPSec – IKE Encryption (IKEv1)

IKE Encryption (IKEv1)	AutoOrder selection	ECOS
"Auto" is default on Orchestrator UI and appliance web UI.	Encryption algorithm is negotiated by both ends in the order prescribed below (1 – first; 4 – last)	All releases
AES_128_CBC	2	All releases
AES_256_CBC	1	All releases
IKE Encryption (IKEv1)	AutoOrder selection	ECOS Release prior to 9.2.1

NOTE: For IKEv1-based IPSec, Auto means AES_128_CBC or AES_256_CBC are negotiated; the maximum common key lengths available on both peers is jointly selected in preference order listed above.

Table 16: IKE-based IPSec – IKE Encryption (IKEv2)

IKE Encryption (IKEv2)	AutoOrder selection	ECOS
"Auto" is default on Orchestrator UI and appliance web UI.	Encryption algorithm is negotiated by both ends in the order prescribed below (1 – first; 4 – last)	All releases
AES_128_CBC	4	All releases
AES_256_CBC	3	All releases
AES_128_GCM_16	2	ECOS 9.2.0+
AES_256_GCM_16	1	ECOS 9.2.0+

NOTE: For IKEv2-based IPSec, Auto means AES_128_CBC, AES_256_CBC, AES_128_GCM, AES_256_GCM are negotiated; the maximum common key lengths available on both peers is jointly selected in preference order listed above.

Table 17: IKE-based IPSec – IKE Authentication

IKE Authentication	IKE Version	ECOS	Integrity Check Value (ICV) (Authentication Tag) Length
SHA_1 (Default)	v1 or v2	All releases	12 octets
SHA_2_256	v1 or v2	All releases	16 octets
SHA_2_384	v1 or v2	All releases	24 octets
SHA_2_512	v1 or v2	All releases	32 octets

NOTE: When AES_128_GCM or AES_256_GCM are selected for encryption, these algorithms support Authentication.

Table 18: IKE-based IPSec – IKE (phase 1) Diffie-Hellman Groups, NIST Elliptic Curve Groups, and Modern Elliptical Curve Groups

IKE (phase 1) Diffie-Hellman Groups	Tunnel Type	ECOS	Length (bits)
Regular Modular Prime Groups			Modulus
Diffie-Hellman Group 1	PT only (Note below)	All releases	768
Diffie-Hellman Group 2 (default for PT)	PT only (Note)	All releases	1024
Diffie-Hellman Group 5	PT only (Note)	All releases	1536
Diffie-Hellman Group 14 (default for UT)	UT and PT	All releases	2048
Diffie-Hellman Group 15	UT and PT	All releases	3072
Diffie-Hellman Group 16	UT and PT	All releases	4096
Diffie-Hellman Group 17	UT and PT	All releases	6144
Diffie-Hellman Group 18	UT and PT	All releases	8192
NIST Elliptic Curve Groups			Prime Size
Diffie-Hellman Group 19	UT and PT	ECOS 9.2.0+	256
Diffie-Hellman Group 20	UT and PT	ECOS 9.2.0+	384
Diffie-Hellman Group 21	UT and PT	ECOS 9.2.0+	521
Diffie-Hellman Group 26	UT and PT	ECOS 9.2.0+	224
Modern Elliptical Curve Groups			Modulus
Diffie-Hellman Group 31	UT and PT	ECOS 9.2.0+	256

NOTE: Prior to the Cipher Profile feature introduced in 9.4.4 and 9.5.4, it was not possible to configure UTs with DH groups 1, 2, and 5. However, with Cipher Profiles, the Tunnel Profile works universally across all tunnel types.

Table 19: IKE-based IPSec – IKE Pseudo-Random Functions

IKE Pseudo-Random Functions	When Selectable	ECOS
SHA_2_256	AES_GCM_128 only	All releases
SHA_2_384		All releases
SHA_2_512		All releases

Starting with Release 9.2.0, when AES-GCM-128 or AES-GCM-256 is selected as the encryption algorithm:

- Authentication Algorithm shows as “NA”.
- Pseudo Random Function is displayed and configurable.

Prior to Release 9.2.0, the IKE Pseudo Random Function (PRF) used the same algorithm as the data integrity algorithm. GCM Data Integrity Authentication is not specified (it is included in GCM), the PRF must be explicitly configured. The use of Hashed Message Authentication Mode (HMAC) in conjunction with the SHA-256, SHA-384, and SHA-512 algorithms in IPSec is described in RFC 4868[2].

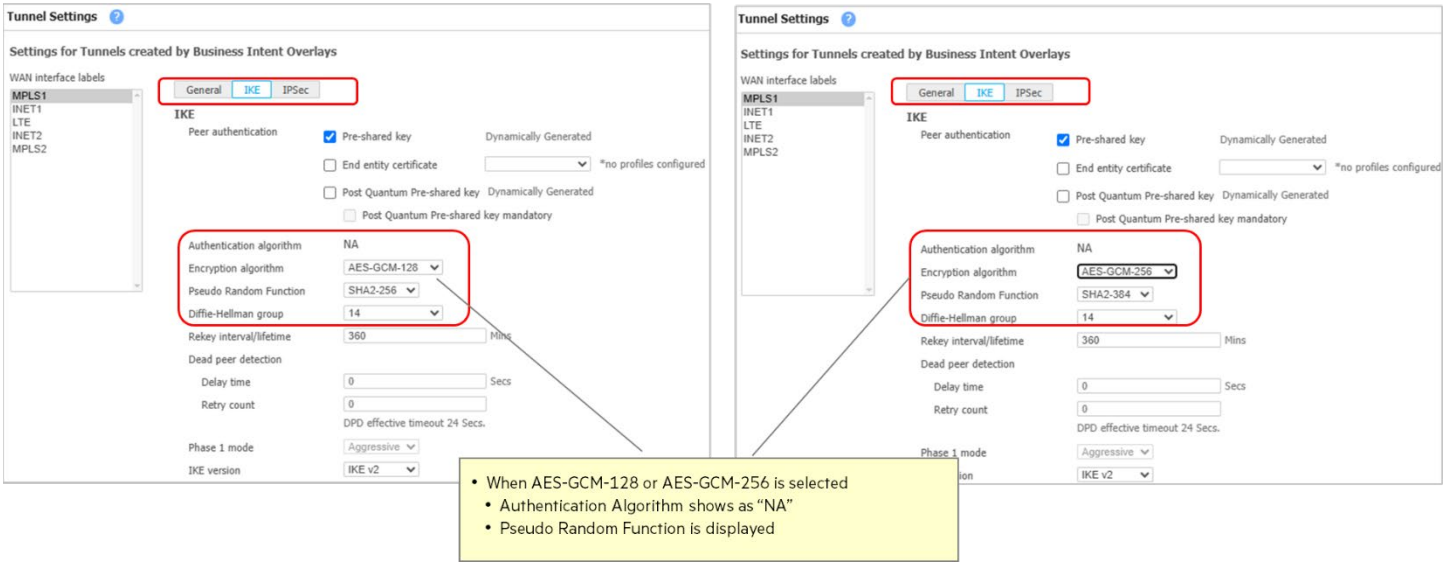

Figure 6 Pseudo Random Function

Table 20: IKE-based IPSec – IPSec Encryption

IPSec Encryption	ECOS	Mode	Authentication Tag
"Auto" is default on Orchestrator UI and appliance web UI. **See Note below**	All releases	CBC	16 octets
AES_128_CBC	All releases	CBC	16 octets
AES_256_CBC	All releases	CBC	16 octets
AES_128_GCM_16	ECOS 9.2.0	GCM	16 octets
AES_256_GCM_16	ECOS 9.2.0	GCM	16 octets

NOTE: Auto means AES_128_CBC or AES_256_CBC is negotiated; the maximum common key lengths available on both peers is jointly selected.

[2] RFC 4868, Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, May 2007

Table 21: IKE-based IPSec – IPSec Authentication

IPSec Authentication	ECOS
SHA_1 (Default)	All releases
SHA_2_256	All releases
SHA_2_384	All releases
SHA_2_512	All releases
AES_128_GMAC	ECOS 9.2.0
AES_256_GMAC	ECOS 9.2.0

Table 22: IKE-based IPSec – IKE (phase 2) Perfect Forwarding Secrecy Groups, NIST Elliptic Curve Groups, and Modern Elliptical Curve Groups

IPSec (phase 2) Perfect Forwarding Secrecy Groups	Tunnel Type	ECOS	Length (bits)
None (Default)*	UT and PT	All releases	
Regular Modular Prime Groups			Modulus
Diffie-Hellman Group 1	PT only**	All releases	768
Diffie-Hellman Group 2	PT only**	All releases	1024
Diffie-Hellman Group 5	PT only**	All releases	1536
Diffie-Hellman Group 14	UT and PT	All releases	2048
Diffie-Hellman Group 15	UT and PT	All releases	3072
Diffie-Hellman Group 16	UT and PT	All releases	4096
Diffie-Hellman Group 17	UT and PT	All releases	6144
Diffie-Hellman Group 18	UT and PT	All releases	8192
NIST Elliptic Curve Groups			Prime Size
Diffie-Hellman Group 19	UT and PT	ECOS 9.2.0+	256
Diffie-Hellman Group 20	UT and PT	ECOS 9.2.0+	384
Diffie-Hellman Group 21	UT and PT	ECOS 9.2.0+	521
Diffie-Hellman Group 26	UT and PT	ECOS 9.2.0+	224
Modern Elliptical Curve Groups			Modulus
Diffie-Hellman Group 31	UT and PT	ECOS 9.2.0+	256

***NOTE:** If set to None, no negotiation recurs during phase 2 and the same DH group is used from the IKE phase.

****NOTE:** Prior to the Cipher Profile feature introduced in 9.4.4 and 9.5.4, it was not possible to configure UTs with DH groups 1, 2, and 5. However, with Cipher Profiles, the Tunnel Profile works universally across all tunnel types.

EdgeConnect Other Cryptographic Services

Boost Network Memory Disk Encryption

ECOS All Releases	Mode
AES_128	CBC

ECOS Software Upgrade

ECOS upgrade packages require SHA 256 image verification.

SSL Proxy with WAN Optimization

By supporting the use of SSL certificates and keys, the EdgeConnect WAN Optimization feature provides deduplication for Secure Socket Layer (SSL) encrypted enterprise traffic.

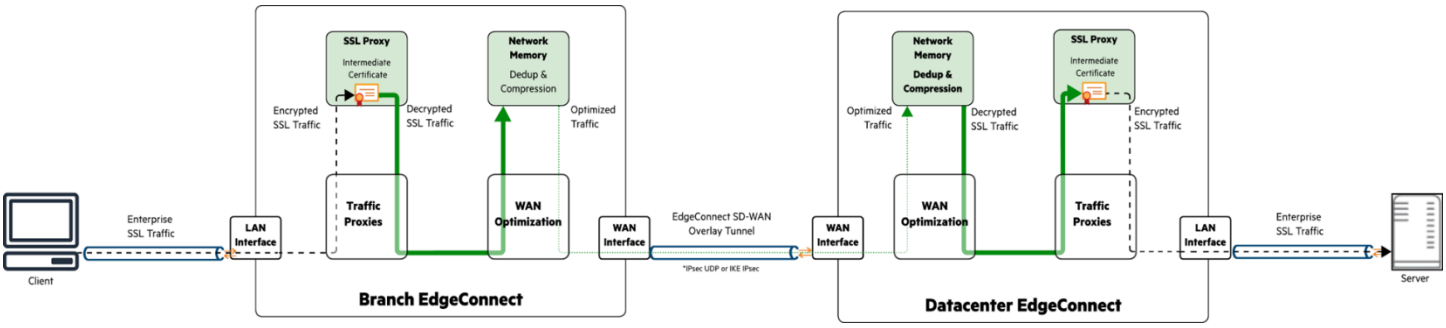

Figure 7 Data path showing SSL Proxy and WAN Optimization

- The client-side EdgeConnect decrypts enterprise SSL data using the SSL Proxy with configured certificates and keys, optimizes the data, and transmits data over an IPSec tunnel. The peer, server-side EdgeConnect appliance uses the configured SSL certificates to re-encrypt data before transmitting towards the LAN and on to the server.
- Peers that exchange and optimize SSL traffic must use the same certificate and key.
- If the enterprise certificate that is used for signing substitute certificates is subordinate to higher level Certificate Authorities (CA), then those CA certificates must be added. If the browser cannot validate up the chain to the root CA, it will issue a warning that it cannot trust the certificate.
- Orchestrator templates are used to provision a certificate and its associated key across multiple appliances.
    - Both PFX certificates (generally, for Microsoft servers) or PEM certificates are supported.
    - The default is PEM when PFX Certificate File is deselected.
    - If the key file has an encrypted key, then the passphrase needed to decrypt it must be provisioned.

Table 23: SSL Acceleration Protocol Support

SSL Acceleration Protocol Support	ECOS
SSL v3	All releases
TLS 1.0	All releases
TLS 1.1	All releases
TLS 1.2	All releases

Table 24: SSL Acceleration Key Exchange Algorithms

Key Exchange	ECOS
RSA	All releases
DHE_RSA	All releases
ECDHE_RSA	All releases

Table 25: SSL Acceleration Authentication Algorithms

Authentication	ECOS
RSA	All releases
ECDSA	All releases

Table 26: SSL Acceleration Encryption Algorithms

Encryption	ECOS	Mode
AES_128	All releases	CTR
AES_256	All releases	CTR
AES_128	All releases	GCM
AES_256	All releases	GCM
RC4	All releases	
3DES	All releases	

Table 27: SSL Acceleration Message Authentication Algorithms

Message Authentication	ECOS
MD5	All releases
SHA-1	All releases
SHA-2 384	All releases

Supported Extensions

EXTENDED_MASTER_SECRET

- SSL_EXT_TRUSTED_CA_KEYS
- SSL_EXT_SESSION_TICKET
- SSL_EXT_HEARTBEAT
- SSL_EXT_ALPN

- SSL_EXT_STATUS_REQUEST
- SSL_EXT_STATUS_REQUEST_V2
- SSL_EXT_NEXT_PROTOCOL_NEGOTIATION
- SSL_EXT_SERVER_NAME
- SSL_EXT_MAX_FRAGMENT_LENGTH
- SSL_EXT_RENEGOTIATION_INFO
- SSL_EXT_ELLIPTIC_CURVES
- SSL_EXT_EC_POINT_FORMATS
- SSL_EXT_SIGNATURE_ALGORITHMS

Supported Curves

- x25519
- sect163k1
- sect163r1
- sect163r2
- sect193r1
- sect193r2
- sect233k1
- sect233r1
- sect239k1
- sect283k1
- sect283r1
- sect409k1
- sect409r1
- sect571k1
- sect571r1
- secp160k1
- secp160r1
- secp160r2
- secp192k1
- prime192v1
- secp224k1
- secp224r1
- secp256k1
- prime256v1

- secp384r1
- secp521r1

Orchestrator Management Plane Cryptographic Algorithms

TLS Cipher Suite Supported on Orchestrator

Orchestrator acts as server for the following cases:

- User Interface (browser is client)
- EdgeConnect Appliance management plane (ECOS is client)
- Rest API
- Remote Log Receiver – WebSocket

Orchestrator as server chooses the strongest crypto cipher suite from the intersection between server and client.

Orchestrator acts as client for the following cases:

- Connection to Cloud Portal
- 3rd party REST API services (e.g., HPE SSE, Zscaler, Netskope, AWS, Azure)
- Google Maps to convert address to Lat/Lon
- Remote Log Receiver – HTTPS, Syslog

Orchestrator Advanced Properties (use for releases prior to 9.4.4 and 9.5.4)

Whether Orchestrator is client or server, for releases prior to 9.4.4, 9.5.4, Orchestrator allows configuration of Allowed and Disabled Cipher Suites.

- Self-hosted Orchestrators: end-customers can modify these directly.
- Aruba-hosted, Orchestrator-as-a-Service: Technical Assistance Center (TAC) request is required.

For more information, see Orchestrator Advanced Properties in the Orchestrator User Guide.

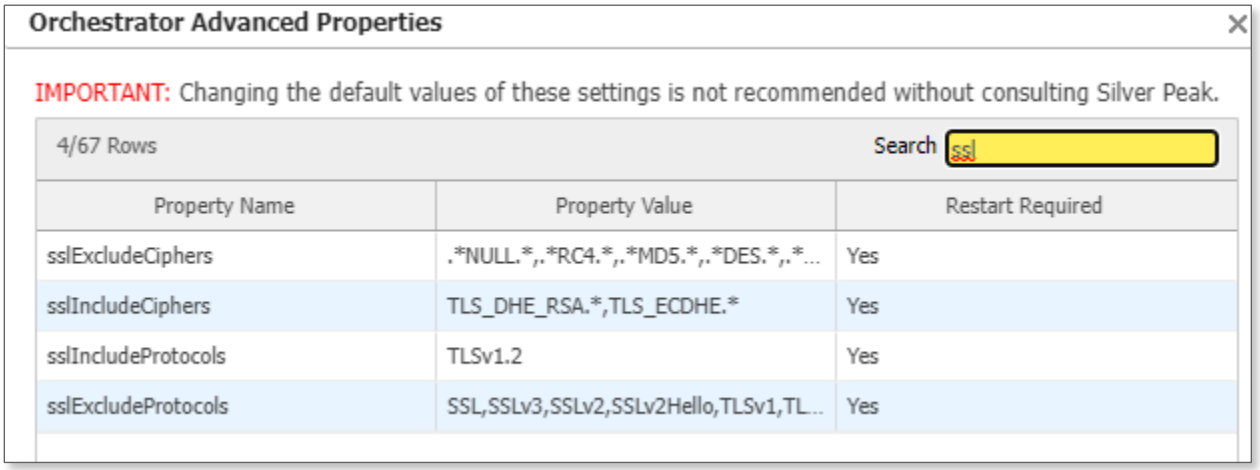

Figure 8: Orchestrator Advanced Properties Dialog Box

NOTE: Aruba recommends leaving these cipher suites as default. Any changes must be thoroughly tested for compatibility.

With the default SSL settings in Orchestrator Advanced Properties, the cipher suites listed in the table below are supported:

Table 28: Orchestrator TLS Cipher Suites Supported for all Releases Prior to 9.4.4

Key Exchange	Authentication	Symmetric Encryption	Key Length	AES Mode	Message Authentication	Combined Cipher String
DHE	DSS	AES	128	CBC	SHA	TLS_DHE_DSS_WITH_AES_128_CBC_SHA
DHE	DSS	AES	128	CBC	SHA256	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
DHE	DSS	AES	128	GCM	SHA256	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
DHE	DSS	AES	256	CBC	SHA	TLS_DHE_DSS_WITH_AES_256_CBC_SHA
DHE	DSS	AES	256	CBC	SHA256	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
DHE	DSS	AES	256	GCM	SHA384	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
DHE	RSA	AES	128	CBC	SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
DHE	RSA	AES	128	CBC	SHA256	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
DHE	RSA	AES	128	GCM	SHA256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
DHE	RSA	AES	256	CBC	SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
DHE	RSA	AES	256	CBC	SHA256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
DHE	RSA	AES	256	GCM	SHA384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
ECDH	ECDSA	AES	128	CBC	SHA	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
ECDH	ECDSA	AES	128	CBC	SHA256	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
ECDH	ECDSA	AES	128	GCM	SHA256	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
ECDH	ECDSA	AES	256	CBC	SHA	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
ECDH	ECDSA	AES	256	CBC	SHA384	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
ECDH	ECDSA	AES	256	GCM	SHA384	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
ECDH	RSA	AES	128	CBC	SHA	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
ECDH	RSA	AES	128	CBC	SHA256	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
ECDH	RSA	AES	128	GCM	SHA256	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
ECDH	RSA	AES	256	CBC	SHA	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
ECDH	RSA	AES	256	CBC	SHA384	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384

Key Exchange	Authentication	Symmetric Encryption	Key Length	AES Mode	Message Authentication	Combined Cipher String
ECDH	RSA	AES	256	GCM	SHA384	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
ECDHE	ECDSA	AES	128	CBC	SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ECDHE	ECDSA	AES	128	CBC	SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE	ECDSA	AES	128	GCM	SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE	ECDSA	AES	256	CBC	SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
ECDHE	ECDSA	AES	256	CBC	SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE	ECDSA	AES	256	GCM	SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE	RSA	AES	128	CBC	SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ECDHE	RSA	AES	128	CBC	SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE	RSA	AES	128	GCM	SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE	RSA	AES	256	CBC	SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
ECDHE	RSA	AES	256	CBC	SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDHE	RSA	AES	256	GCM	SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
See Note Below	RSA	AES	256	CBC	SHA	TLS_RSA_WITH_AES_256_CBC_SHA
	RSA	AES	128	CBC	SHA	TLS_RSA_WITH_AES_128_CBC_SHA
	RSA	AES	256	CBC	SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256
	RSA	AES	128	CBC	SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
	RSA	AES	128	GCM	SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
	RSA	AES	256	GCM	SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384

NOTE: RSA performs both Key Exchange and Authentication.

Orchestrator Remote Log Receiver Connections

Orchestrator Notification Service (ONS) provides the facility to stream Orchestrator and EdgeConnect alarms and Orchestrator log events to third-party systems. Protocol options include HTTP, HTTPS, KAFKA, SYSLOG, and WEBSOCKET. ONS connections using HTTPS, Syslog, or WebSocket follow the TLS suites above. For more information, see Remote Log Receivers in the Orchestrator User Guide.

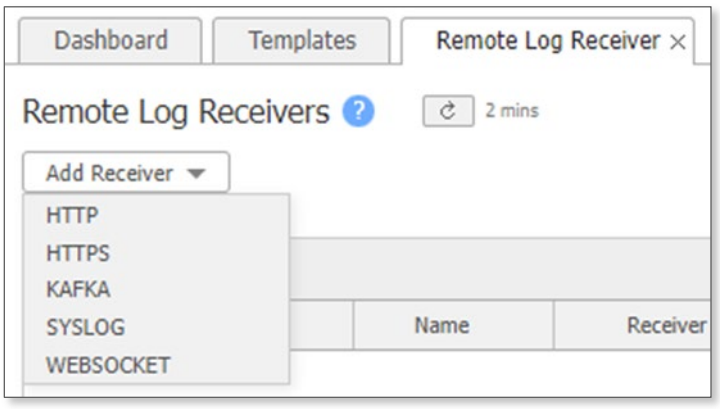

Figure 9: Orchestrator Remote Log Receiver Tab

Self-hosted / On-Prem Orchestrator SSH Cipher Suite

For self-hosted/on-prem Orchestrators, SSH configuration is performed at the Linux level via the SSH config file. The details of this configuration are not covered in this document. A reference can be found here: https://man.openbsd.org/OpenBSD-current/man5/ssh_config.5

Table 29: Self-hosted/On-Prem Orchestrator SSH Cipher Suites

Algorithm	Cipher Suite
kex_algorithms	
	curve25519-sha256
	ecdh-sha2-nistp256
	ecdh-sha2-nistp384
	ecdh-sha2-nistp521
	diffie-hellman-group-exchange-sha256
	diffie-hellman-group16-sha512
	diffie-hellman-group18-sha512
	diffie-hellman-group-exchange-sha1
	diffie-hellman-group14-sha256
	diffie-hellman-group14-sha1
	diffie-hellman-group1-sha1
server_host_key_algorithms	
	ssh-rsa

Algorithm	Cipher Suite
	rsa-sha2-256
	rsa-sha2-512
	ecdsa-sha2-nistp256
	ssh-ed25519
encryption_algorithms	
	aes256-ctr
	aes192-ctr
	aes128-ctr
	aes256-cbc
	aes192-cbc
	aes128-cbc
mac_algorithms	
	hmac-sha1
	hmac-sha2-256
	hmac-sha2-512

Cipher Profile Settings with Release 9.4.4, 9.5.4, 9.6.0

Releases 9.4.4, 9.5.4, and 9.6.0 include the ability to restrict the use of certain ciphers for the Orchestrator and ECOS services that use cryptography, as outlined in the following table.

Table 30: Orchestrator and ECOS Services that Use Cryptography

Service	System	Applicability
TLS	Orchestrator and ECOS	Orchestrator acts as a client or a server in various TLS connection use cases.
Tunnels	ECOS	EdgeConnect IPSec tunnels
SSH	ECOS	EdgeConnect CLI
Certificate	Orchestrator and ECOS	Orchestrator web server, EdgeConnect web server, Syslog client, IKE-based IPSec tunnels
SNMP	ECOS	Release 9.5.4+ The EdgeConnect SNMP interface supports Management Information Base (MIB-II) as described in RFC 1213. This interface is used to receive notifications or traps from the appliance whenever an alarm is raised or cleared. SNMP is not used for configuration.
NTP	ECOS	Secure NTP is available starting with ECOS 9.4.2.
Cluster	ECOS	The cluster feature is introduced in Release 9.5.2; security configuration is performed in the Cipher profile settings in Release 9.6.0.

Cipher restrictions are applied to services using a cipher profile. As listed above, some services apply to both Orchestrator and EdgeConnect OS (ECOS) and some apply only to ECOS.

The Cipher Profile settings determine which ciphers, algorithms, or parameters are allowed to be used by services requiring cryptographic functions. Changing the Cipher Profile settings may or may not change the ciphers used in existing connections and configurations.

IMPORTANT: For cryptographic services that require direct configuration, such as ECOS IPSec tunnels, the user must manually change the service configuration ***before activating any Cipher Profile changes***.

Service Impacts of Activating Cipher Profiles

The following table describes what happens for each cryptographic service when a Cipher Profile is changed, and any actions the user must take to change the service configuration.

Table 31 Service Impacts of Activating Cipher Profiles

	Orchestrator	ECOS
TLS	Changing the Cipher Profile changes the service configuration. Profile changes must be validated by the user before being applied; user does this by clicking the Validate button (user action is required). See NOTE below table. Upon changing the Cipher Profile, existing TLS sessions remain up. Self-Hosted/On Prem Orchestrators: User must perform "`service gms restart`" using the Orchestrator CLI, at which point existing TLS sessions are dropped. After the gms service is restarted, TLS sessions are automatically reestablished with the new Cipher Profile settings. Orchestrator-as-a-Service: Changing the Cipher Profile only affects services for which Orchestrator is client, such as API connections to third-party services. Users need to open a TAC case to restart their OaaS to have TLS Cipher Profile changes take effect.	Changing the Cipher Profile changes the service configuration. Profile changes must be validated by the user before being applied; user does this by clicking the Validate button (user action is required). See NOTE below table. TLS sessions are dropped and reestablished.
Tunnels	Not applicable	Changing the Cipher Profile DOES NOT change the service configuration for any use case. Tunnel configurations must be performed prior to changing the Cipher Profile. The user must explicitly validate the service configuration against the intended (to be activated) Cipher Profile. **NOTE: Existing tunnels, established with settings that will be disallowed in the intended Cipher Profile, will be DROPPED when the new Cipher Profile is activated.** See, Tunnels (ECOS).
SSH	For self-hosted/on-prem Orchestrators, SSH configuration is performed at the Linux level via the SSH config file; Cipher Profile settings do not apply. SSH does not apply to Orchestrator-as-a-Service	Changing the Cipher Profile changes the service configuration. ECOS SSH configuration is orchestrated via the Cipher Profile settings. There is no need to configure via CLI. See, SSH (ECOS).
Certificate	Existing end entity certificates configured with settings not allowed in the new/intended Cipher Profile will be invalid and not useable. Profile changes must be validated by the user before being applied; user does this by clicking the Validate button (user action is required). See NOTE below table.	Existing end entity certificates configured with settings not allowed in the new/intended Cipher Profile will be invalid and not useable. Profile changes must be validated by the user before being applied; user does this by clicking the Validate button (user action is required). See NOTE below table.

	Orchestrator	ECOS
SNMP	Not applicable	Starting with Release 9.5.4, ECOS SNMP configuration is performed via Orchestrator templates or via the Cipher Profile settings.
NTP	Not applicable	ECOS NTP server configuration is performed via Orchestrator templates. NTP secure algorithm parameters are configured via CLI and must be validated by the user prior to changing the service configuration.
Cluster	Not applicable	Changing the Cipher Profile changes the service configuration. The cluster feature was introduced in Release 9.5.2 with fixed cryptographic settings. Security configuration is performed in the Cipher Profile settings starting with Release 9.6.0.

NOTE: The Validate action provides feedback on the compatibility of HTTPS server certificates indicating if the new Cipher Profile will work with existing TLS connections. Whether the Validate function returns a pass or fail indication the user can still execute the profile change. The Validate action DOES NOT verify other services such as tunnels.

Cipher Settings Orchestrator UI Tab

Starting with Orchestrator Releases 9.4.4 and 9.5.4, cipher profiles are configured on the Cipher Settings tab (**Configuration > Overlays & Security > Security > Cipher Settings**).

The following table describes the information displayed on the Cipher Settings tab for each cipher profile.

Table 32: Cipher Settings Tab Columns

Column	Description
Edit	Contains an edit button for cloned cipher profiles. No edit button is available for the four preconfigured profiles (default, CSfC, FIPS, Common Criteria) because those cannot be edited.
Profile Name	Indicates the profile name. For cloned profiles, this name is entered by the user when they clone a profile.
Comment	For the four preconfigured profiles this is a description of the profile and indicates if it contains any cipher restrictions to meet any specific requirements. For cloned profiles, this shows the text the user enters in the Comments field for the profile.
Actions	Contains the user action buttons Validate, View, and Clone. When a profile is active, the Validate button turns green and the text toggles to “Active” to indicate that the profile has been activated.

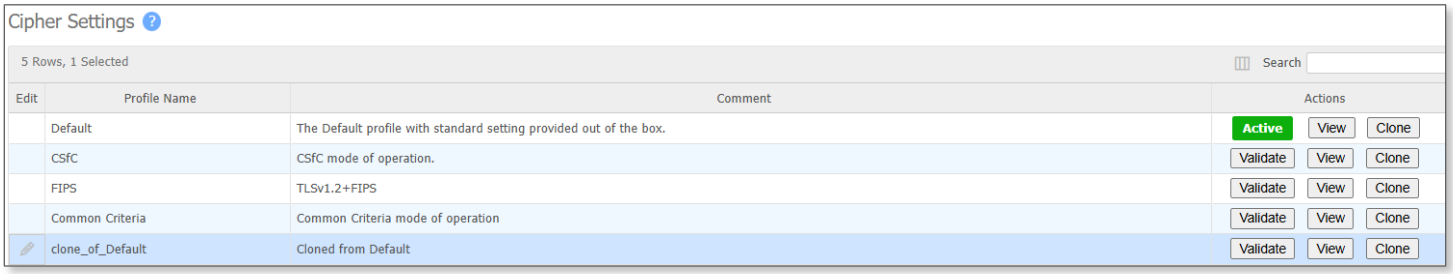

Figure 10: Orchestrator Cipher Settings Tab

Cipher Profiles Settings

Orchestrator has four preconfigured cipher profiles:

1. **Default** – This profile reflects the default values for new and upgraded Orchestrators with the least restrictive cipher algorithm options.
2. **FIPS** – This profile applies cipher restrictions that meet FIPS requirements, as outlined in FIPS 140-2 (Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules).
3. **Common Criteria** – This profile applies cipher restrictions that meet Common Criteria requirements outlined in the international standard The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408). More information on the standard is available at https://www.commoncriteriaportal.org/
4. **Commercial Systems for Classified** – This profile applies cipher restrictions that meet Commercial Solutions for Classified (CSfC) requirements, as outlined in the NSA Commercial Solutions for Classified (CSfC) Selections for Internet Protocol Security (IPsec) Virtual Private Network (VPN) Gateways document.

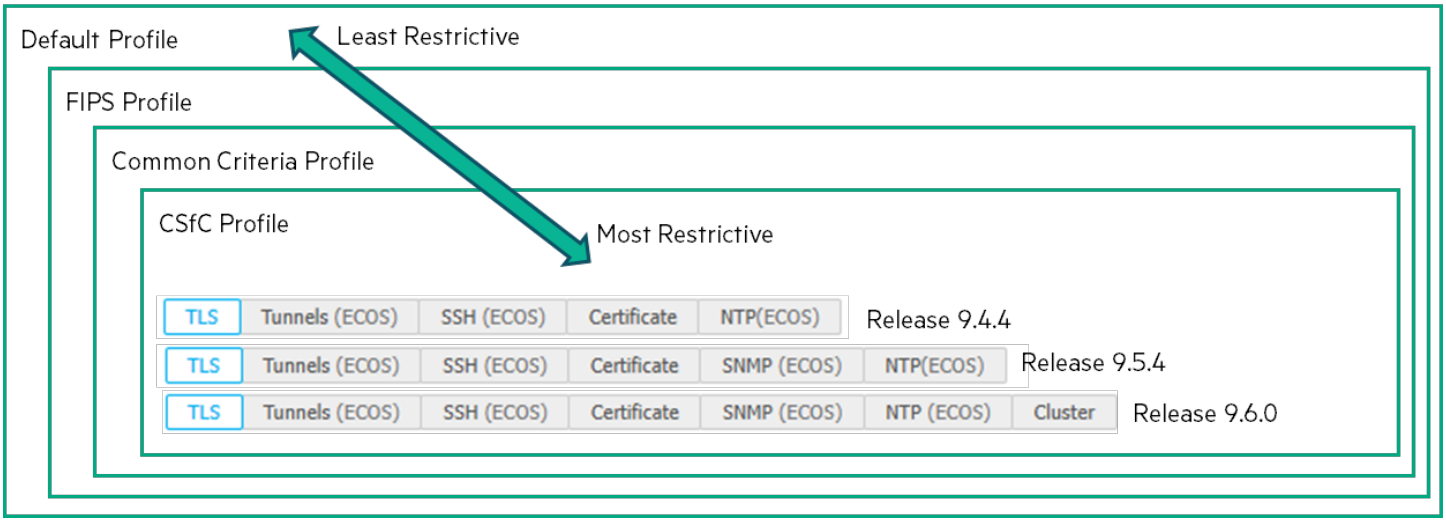

Figure 11: Comparison Restrictiveness of Preconfigured Cipher Profiles

These profiles cannot be edited. A custom profile can be created by cloning one of the preconfigured profiles and then editing it to match the needed requirements. Users should clone the preconfigured profile that is the closest to their required enterprise security policy.

NOTE: As of Releases 9.4.4 and 9.5.4, the FIPS and Common Criteria Profiles are identical.

Cipher Setting User Actions

User actions on the Cipher Settings tab include view, clone, edit, validate and then activate, and delete.

- To view the cipher restrictions associated with a cipher profile, click **View**. This only allows you to view the profile. It does not allow you to edit the profile.
- To clone a cipher profile, click **Clone**.
- To edit a cloned cipher profile, click the edit icon for the profile.
    - For more information on cloning and editing a cipher profile, see Editing a Cloned Cipher Profile.
- To validate a cipher profile, click **Validate**.
    - What is validated: Only Orchestrator and ECOS end-entity HTTPS Server Certificates are checked for compatibility against the profile.

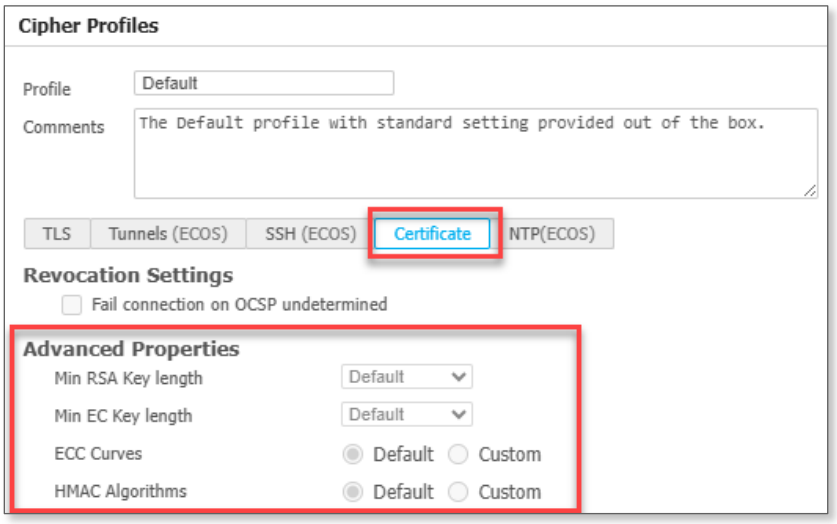

Figure 12: Cipher Settings for Certificate – Advanced Properties

    - What is not validated: All other services.
    - When validation is complete, apply the cipher profile by clicking **Activate**. Only one cipher profile can be active at a time.
- To delete a cloned/edited cipher profile, click the **X** for the profile. The four preconfigured cipher profiles cannot be deleted.

Modifying Cipher Profile Settings with Release 9.4.4, 9.5.4, 9.6.0

Editing a Cloned Cipher Profile

To change the cipher settings for a cloned cipher profile:

1. Navigate to **Configuration > Overlays & Security > Security > Cipher Settings**.
2. Click the edit icon for the cloned cipher profile you want to edit.

   The Cipher Profiles dialog box opens.
3. Click the button for the service for which you want to edit cipher settings (**TLS**, **Tunnels (ECOS)**, **SSH (ECOS)**, **Certificate, SNMP, NTP (ECOS), or Cluster)**.

4. Edit the cipher settings for the service. For information about the cipher settings for each service, see the section for that service:
   TLS
   Tunnels (ECOS)
   SSH (ECOS)
   Certificate
   SNMP (ECOS)
   NTP (ECOS)
   Cluster
5. Click **Save**.

TLS

TLS settings apply to both Orchestrator and EdgeConnect. There are two sections for the TLS profile settings, Cipher Suites and Advanced Properties. In the Cipher Suites section, you choose algorithms available for the following services: key exchange, encryption, and hash function. These building blocks form the composite cipher suites, which are shown in the Enabled and Disabled sections on the following figure. When editing the TLS settings, you can enable or disable the algorithms or the composite cipher suites.

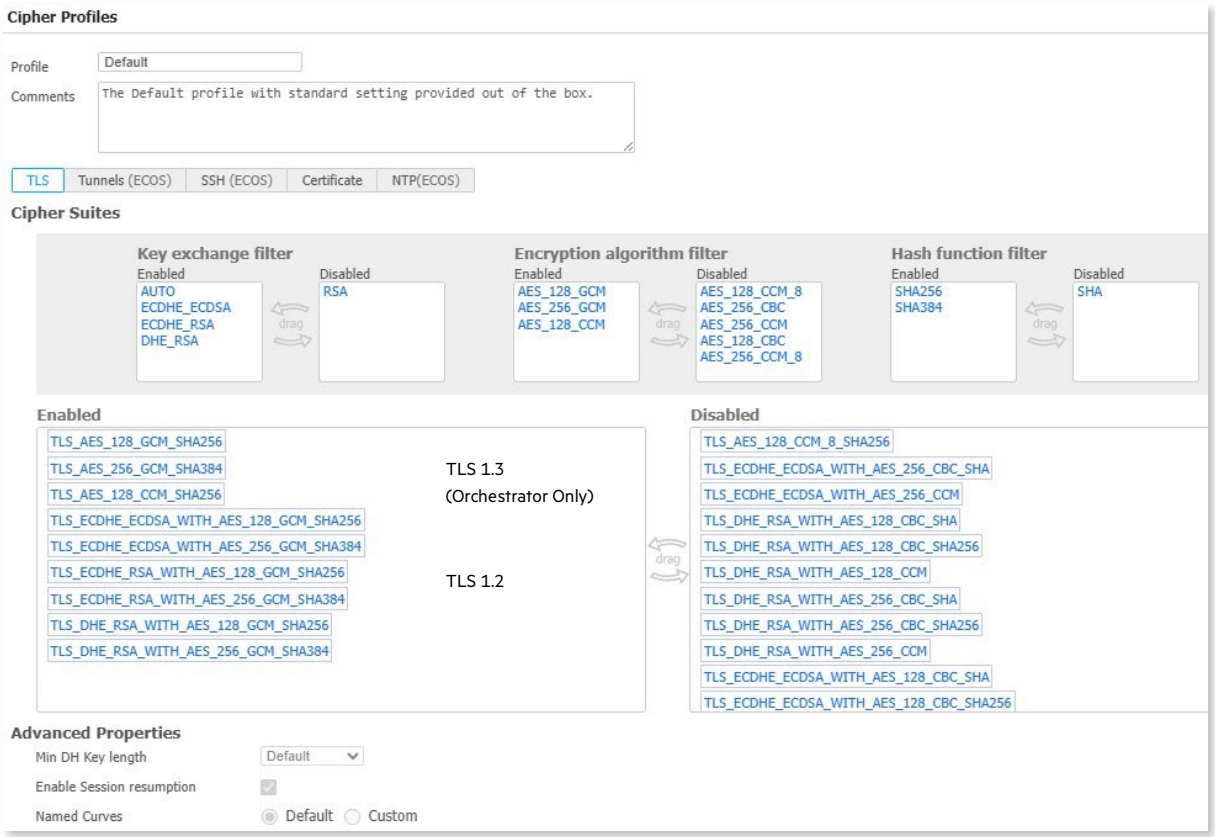

Figure 13: Orchestrator Cipher Profiles Dialog Box

To select an algorithm for a service, drag and drop it from the Disabled to Enabled column to make it available for use. When you enable an algorithm, any cipher suites that contain those algorithms move from Disabled to Enabled. The order that cipher suites appear in the Enabled column does not indicate the order in which the system (TLS server) offers them; the cipher suites that appear in the Enabled column are available for use for TLS.

Table 33: TLS Cipher Suites Settings

Setting	Description	Options
Key exchange algorithm	The algorithms available for Orchestrator to use to establish secure TLS connections.	NONE ECDHE_ECDSA ECDHE_RSA DHE_RSA RSA (Disabled by default)
Encryption algorithm	The algorithms available for Orchestrator to use to encrypt data being sent during a TLS session.	AES_128_GCM AES_256_GCM AES_128_CCM AES_128_CCM_8 (Disabled by default) AES_256_CBC (Disabled by default) AES_256_CCM (Disabled by default) AES_128_CBC (Disabled by default) AES_256_CCM_8 (Disabled by default)
Hash function	The secure hash algorithms available for Orchestrator to use for data integrity	SHA256 SHA384 SHA (Disabled by default)

Table 34: TLS Advanced Properties Settings

Settings	Description	Options
Min DH Key length	The minimum length of the Diffie-Hellman key for Orchestrator when establishing secure TLS connections.	2048 (Default) 3072 4096
Enable Session resumption	Enable/Disable Session Resumption for TLS If enabled, an existing TLS secure session can be “reused”. This allows for faster session establishment. TLS session resumption is not allowed in CSfC. Select or clear the check box.	Enabled or disabled

Settings	Description	Options
Named Curves	To customize, click **Custom** and select the check boxes for named curves to have available.	Custom options: secp224r1 secp256r1 (default) secp384r1 secp521r1 ffdhe2048 ffdhe3072 ffdhe4096 ffdhe6144 ffdhe8192

How to Configure TLS on Self-Hosted/On-Prem Orchestrators

For self-hosted/on-premises Orchestrators, changing the TLS Cipher Profile settings changes the service for all Orchestrator TLS connections. The user must validate proposed changes before activation. When connecting to a third-party service, it is important to understand the cipher options that the third-party service offers and ensure the TLS Cipher Profile is in alignment.

When the TLS Cipher Profile settings are changed, existing TLS sessions remain up. The user must perform "`service gms restart`" using the Orchestrator CLI, at which point existing TLS sessions are dropped.

After the gms service is restarted, TLS sessions are automatically reestablished with the new Cipher Profile settings.

How to Configure TLS on Orchestrator-as-a-Service

For OaaS, changing the TLS Cipher Profile settings only affects services for which Orchestrator is the client, such as API connections to third-party services and HTTPS or Syslog remote receiver connections.

The user must validate proposed changes before activation. When connecting to a third-party service, it is important to understand the cipher options that the third-party service offers and ensure the TLS Cipher Profile is in alignment.

Users need to open a TAC case to restart their OaaS to have TLS Cipher Profile changes take effect. After the OaaS service is restarted, TLS sessions are automatically reestablished with the new Cipher Profile settings.

How to Configure TLS on ECOS

Changing the TLS Cipher Profile settings changes the service for all ECOS TLS connections. The user must validate proposed changes before activation. After Cipher Profile changes are activated, ECOS resets all TLS connections automatically.

Tunnels (ECOS)

The Cipher Profile Settings for Tunnels apply to all tunnel types:

- Orchestrated Underlay Tunnels (UT)
  - IPSec UDP (IPSec phase only)
  - IKE-based, IPSec Underlay Tunnels
- Orchestrated IKE-based, IPsec Passthrough Tunnels (PT) to Select SSE Services (HPE SSE, Zscaler, Netskope, etc.)
- Unified Fabric, HPE ANW Central Tunnels (requires release 9.5.4 or later)
- Service Orchestration Constructed, EdgeConnect-to-Third Party Passthrough Tunnels
- Manually Constructed, EdgeConnect-to-EdgeConnect Tunnels
- Manually Constructed, EdgeConnect-to-Third Party Passthrough Tunnels

For Cipher Profile settings for tunnels, there are two sections, IKE and IPSec. The IKE section only applies to IKE-based IPSec tunnels and does not apply to IPSec UDP tunnels. To enable an algorithm, click its associated check box. All tunnel algorithms are enabled in the default profile.

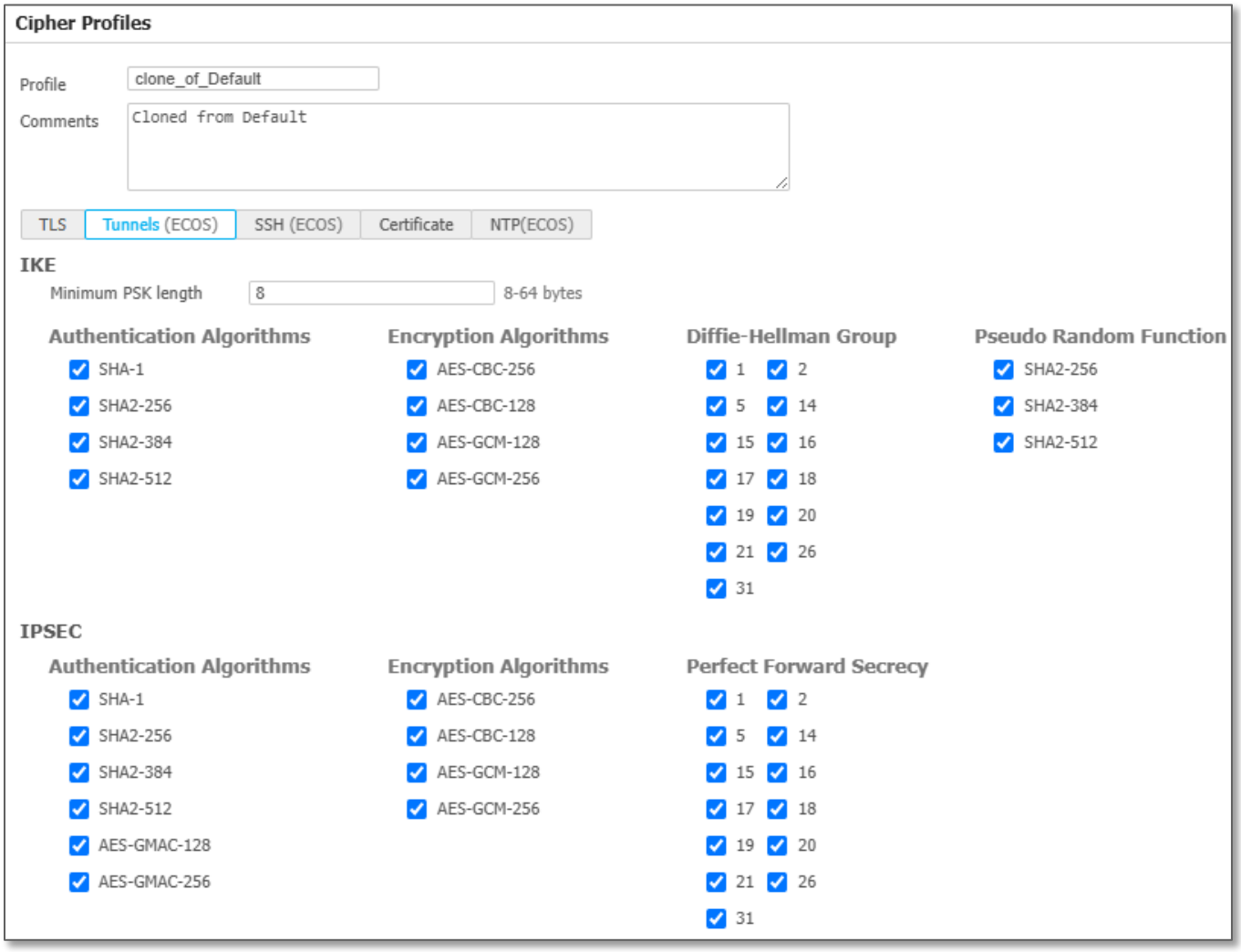

Figure 14 Editing the Tunnels Settings on a Cloned Cipher Profile (cloned from the Default profile)

Table 35: Tunnel Profile Settings

Setting	Description	Options
IKE Minimum Pre-Shared Key (PSK) length	The required minimum length of the IKE PSK (bytes). Enter a numeral in the range of 8-64.	8-64 bytes (8 bytes is the default)
IKE Authentication Algorithms	The authentication algorithms available for the IKE security association (SA).	SHA-1 (Default) SHA2-256 SHA2-384 SHA2-512

Setting	Description	Options
IKE Encryption Algorithms	The encryption algorithms available for the IKE security association (SA).	AES-CBC-256 AES-CBC-128 AES-GCM-128 AES-GCM-256 (Auto is Default) See EdgeConnect to EdgeConnect Underlay and Passthrough Tunnels, IKE-based IPSec.
IKE Diffie-Hellman Group	The Diffie-Helman groups available for IKE security association (SA).	1 2 5 14 (Default) 15 16 17 18 19 20 21 26 31
IKE Pseudo Random Function	The secure hash algorithms available for EdgeConnect IKE-based IPSec tunnels to use for pseudo random function.	SHA2-256 (default when AES-GCM-128 is selected for Encryption/Authentication) SHA2-384 (default when AES-GCM-256 is selected for Encryption/Authentication) SHA2-512
IPSEC Authentication Algorithms	The authentication algorithms available for EdgeConnect IPSec tunnels to use for IPSec security association (SA).	SHA-1 (default) SHA2-256 SHA2-384 SHA2-512 AES-GMAC-128 AES-GMAC-256
IPSEC Encryption Algorithms	The encryption algorithms available for EdgeConnect IPSec tunnels to use for IPSec security association (SA).	AES-CBC-256 (default) AES-CBC-128 AES-GCM-128 AES-GCM-256

Setting	Description	Options
IPSEC Perfect Forward Secrecy	The Diffie-Hellman groups available for EdgeConnect IPSec tunnels to use for IPSec security association (SA) negotiation.	1 2 5 14 (Default for IKE-based IPSec, n/a for IPSec UDP) 15 16 17 18 19 20 21 26 31

NOTE: Changing the Tunnel Cipher Profile settings DOES NOT change the service for any ECOS Tunnels.

Tunnel configurations must be performed prior to changing the Cipher Profile. The user must explicitly validate the service configuration against the intended (to be activated) Cipher Profile. ALL pre-existing tunnels, established with settings that will be disallowed in the intended (to be activated) Cipher Profile, will be DROPPED when the new Cipher Profile is activated.

Avoiding Dropped Tunnels When Changing Cipher Profile Tunnel Settings

The following instructions outline the recommended order of operations to follow when you change Cipher Profile Tunnel settings to avoid any dropped tunnels. These instructions reflect an Orchestrator that is starting with all default values, and the Default Cipher Profile is active.

1. Review the settings for the pre-configured Cipher Profiles (Default, FIPS, Common Criteria, and CSfC) to determine which profile has settings that are closest to your enterprise target security policy. For Tunnel Profile Settings, Default, FIPS, and Common Criteria have all algorithm options enabled. This is subject to change in future releases.
2. If none of the pre-configured profiles match the target security policy, clone the profile that is closest to the target.
3. Note any algorithms you plan to enable or disable for the Tunnels service.
4. Edit the cloned profile and make the necessary changes, but do not activate it yet.

After editing the cloned profile, you must implement the desired tunnel setting changes for all tunnel types including:

- Orchestrated Underlay Tunnels (UT), for ALL Labels
- Orchestrated IKE-based, IPSec Passthrough Tunnels to Select SSE Services (HPE SSE, Zscaler, Netskope, etc.)
- Unified Fabric, HPE ANW Central tunnels (requires release 9.5.4 or later)

- Manually Constructed, EdgeConnect-to-EdgeConnect Tunnels
- Manually Constructed, EdgeConnect-to-Third Party Passthrough Tunnels

---

NOTE: To avoid dropped tunnels, you must implement tunnel setting changes before you activate the Cipher Profile.

Orchestrated Underlay Tunnels (UT), for ALL Labels

In Orchestrator, navigate to **Orchestrator > Orchestrator Server > Tools > Tunnel Settings**.

- Orchestrated IPSec UDP Underlay Tunnels
  - IPSec UDP is the default for Orchestrated Underlay Tunnels
  - Only IPSec phase applies

General tab: No changes needed if continuing with IPSec UDP tunnels.

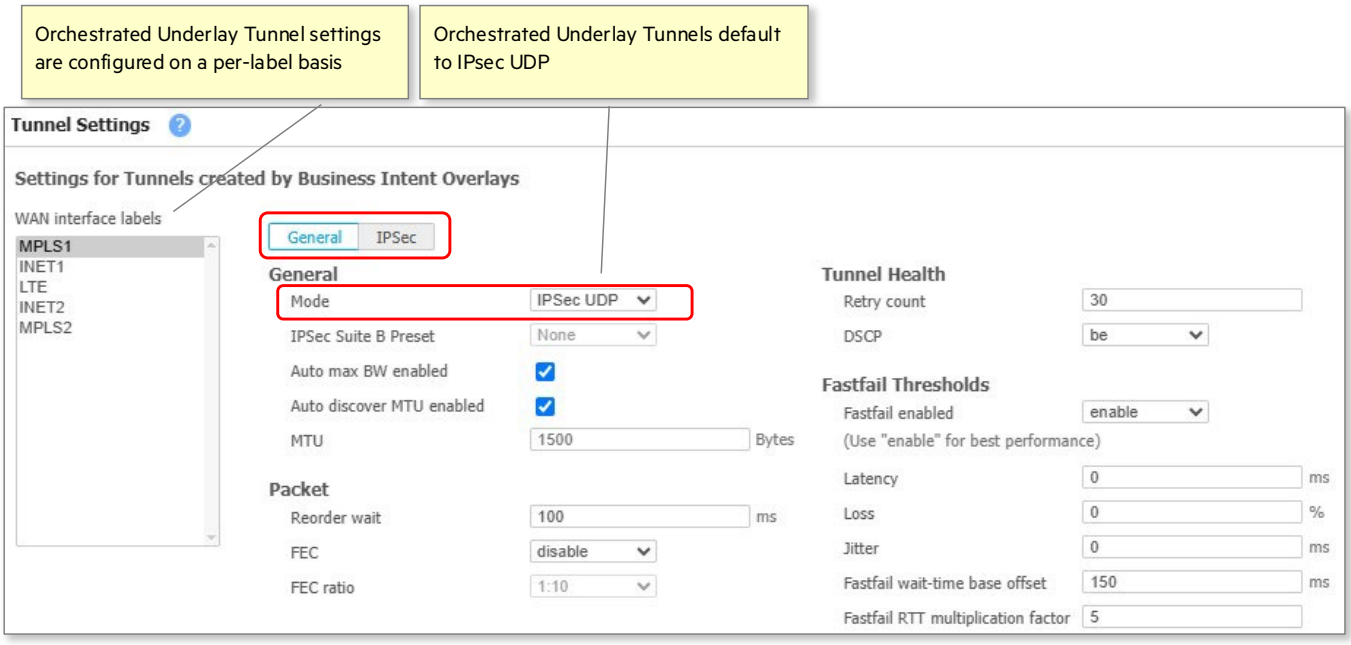

Figure 15: Orchestrated IPSec UDP Underlay Tunnel - General Tab

IPSec tab: There are two algorithms that correspond to Cipher Profile tunnel settings: Authentication algorithm and Encryption algorithm. Ensure that both settings use algorithms allowed in the Cipher Profile you plan to activate. The following figure shows the out-of-the-box default values.

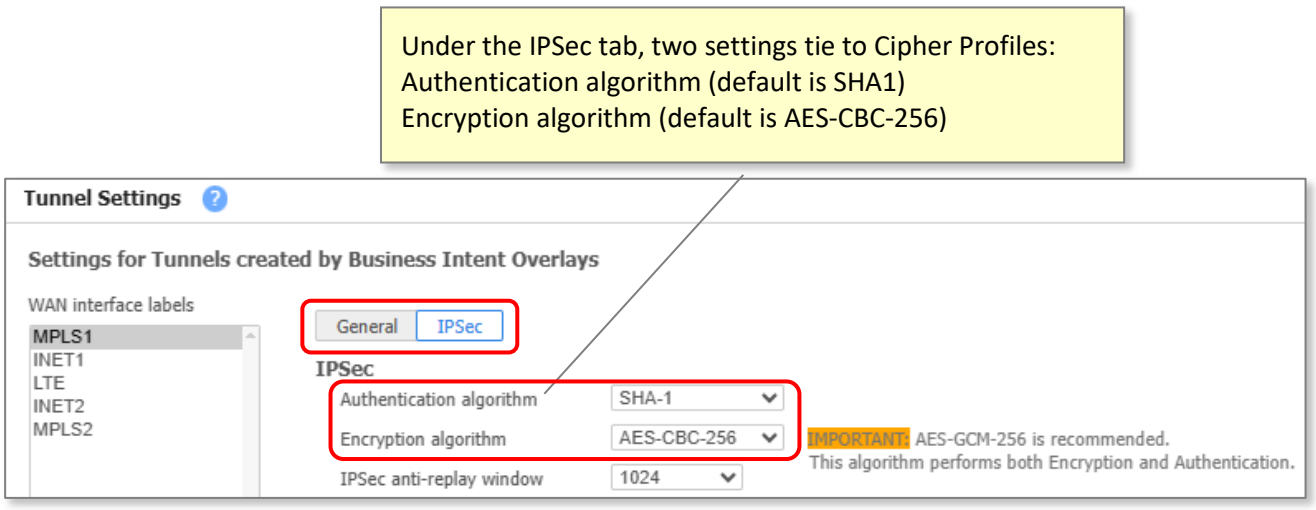

Figure 16: Orchestrated IPSec UDP Underlay Tunnel – IPSec Tab, Default Algorithm settings

If for example, the new Cipher profile will disallow SH1 and CBC-128, you can change to the recommended setting of AES-GCM-256.

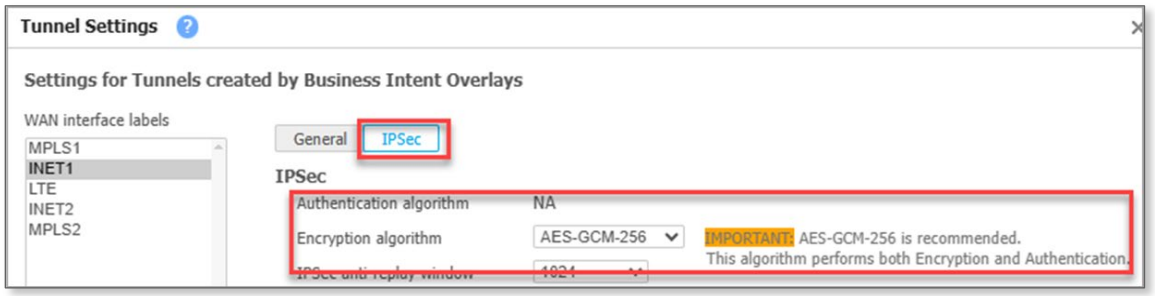

Figure 17: Orchestrated IPSec UDP Underlay Tunnel - IPSec Tab, Changing Encryption the Algorithm

- Orchestrated IKE-based, IPSec Underlay Tunnels

  For customers that require FIPS, Common Criteria, and/or CSfC compliance, standard, IKE-based IPsec tunnels can be used.

NOTE: When configuring the IKE and IPSec encryption algorithms for FIPS and Common Criteria Compliance, the IKE algorithms must be greater than or equal to in strength than the IPSec algorithms.

Table 36 shows an example of a supported and valid configuration.

Table 36: Supported Configuration

Setting	IKE-phase value	IPsec-phase value
Authentication Algorithm	n/a	n/a
Encryption Algorithm	AES_256_GCM_16	AES_256_GCM_16
Diffie-Hellman Group	DH 19	DH 19

Table 37 shows an example of a configuration that is unsupported and invalid because the IKE phase setting is cryptographically weaker than the IPSec phase setting.

Table 37: Unsupported Configuration

Setting	IKE-phase value	IPsec-phase value
Authentication Algorithm	n/a	n/a
Encryption Algorithm	AES_128_GCM_16	AES_256_GCM_16
Diffie-Hellman Group	DH 18	DH 14

General tab: To select IKE-based IPSec tunnels for a particular label, from the Mode menu select **IPSec**.

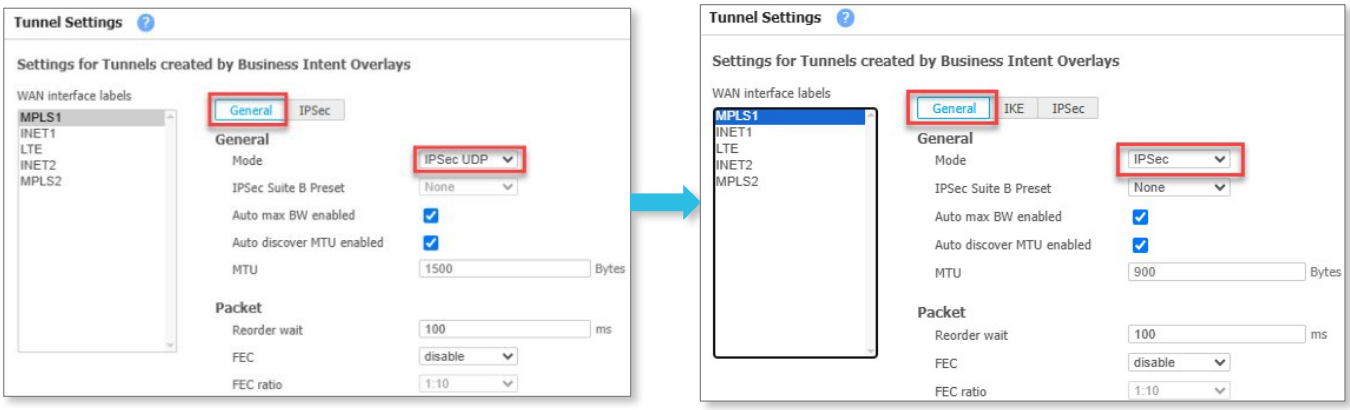

Figure 18: Orchestrated IKE-based IPSec Underlay Tunnel - General Tab

No other changes are needed on the General tab, unless the IPSec Suite B option is selected (only available for IKE-based IPSec Tunnels).[3]

NOTE: GCM-256 is recommended. GMAC options cover authentication only and do not provide encryption.

[3] IPSec Suite B is included in Commercial National Security Algorithm Suite (CNSA).

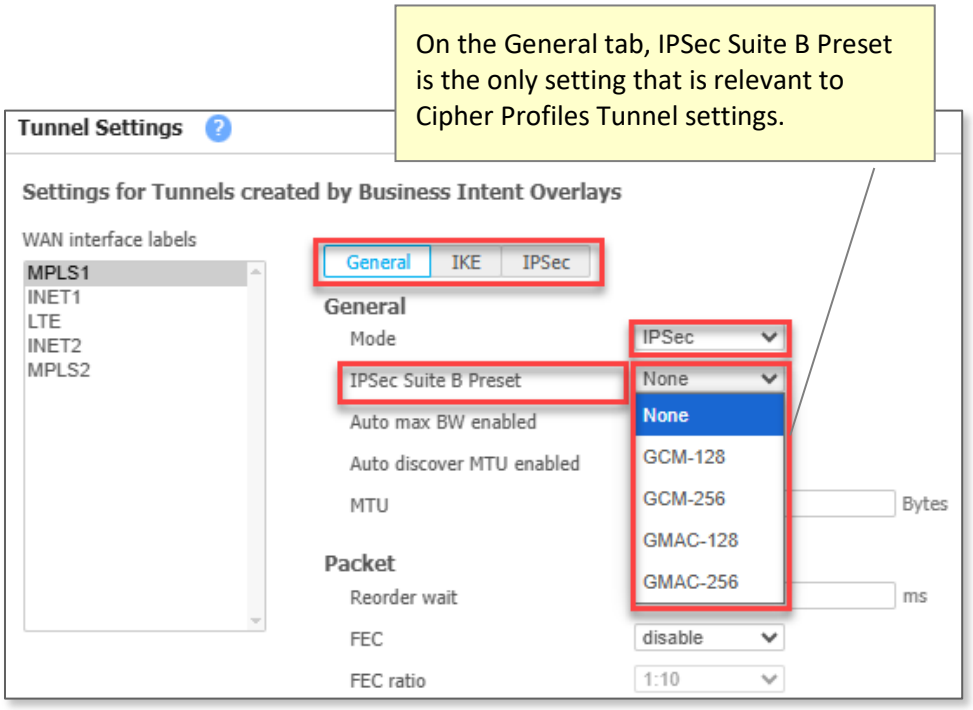

Figure 19: Orchestrated IKE-based IPSec Underlay Tunnel - General Tab, IPSec Suite B Options

IKE tab: For IKE-based IPSec tunnels there are three algorithms that correspond to Cipher Profile tunnel settings: Authentication algorithm, Encryption algorithm, and Diffie-Hellman group. Ensure these settings use algorithms allowed in the Cipher Profile you plan to activate.

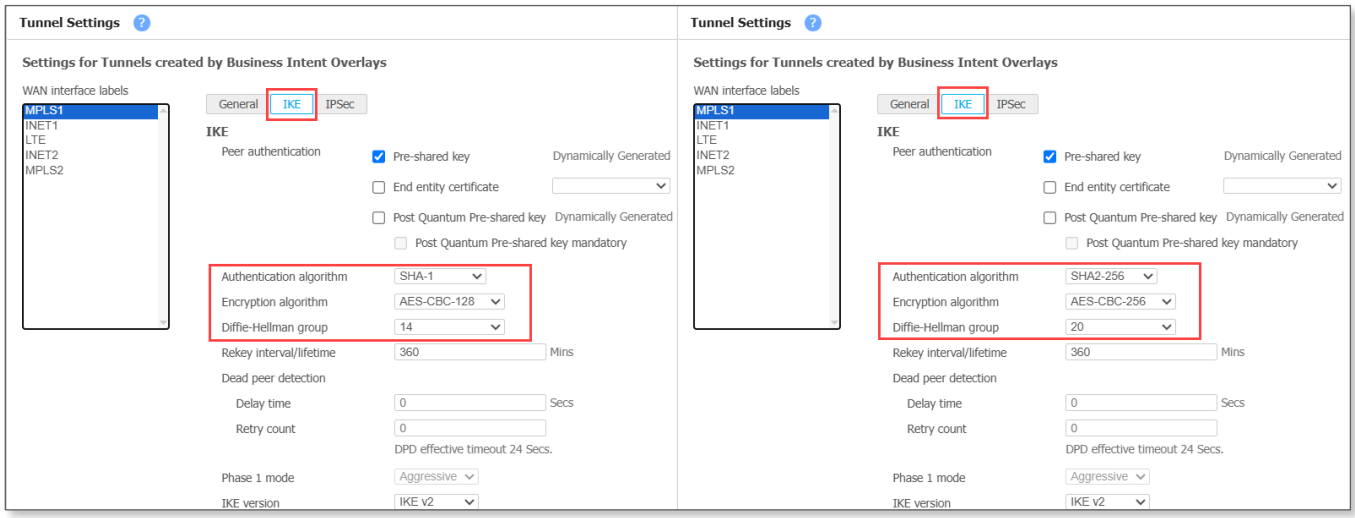

Figure 20: Orchestrated IKE-based IPSec Underlay Tunnel - IKE Tab

IPSec tab: For IKE-based IPSec tunnels there are three algorithms that correspond to Cipher Profile tunnel settings: Authentication algorithm, Encryption algorithm, and Perfect forward secrecy group. Ensure these settings use algorithms allowed in the Cipher Profile you plan to activate.

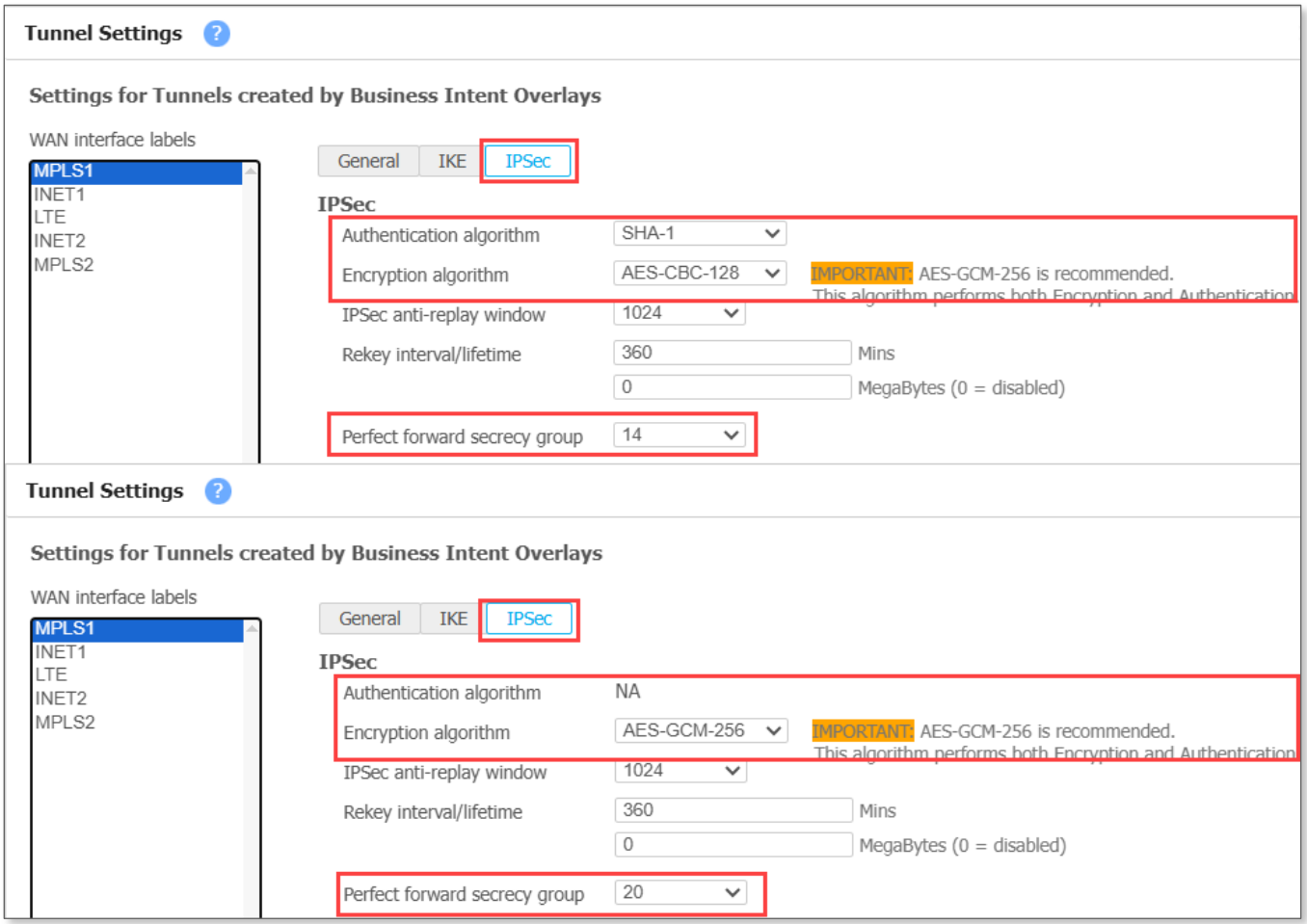

Figure 21: Orchestrated IKE-based IPSec Underlay Tunnel - IPSec Tab

Unified Fabric, HPE ANW Central Tunnels

Unified Fabric, which supports tunnels between EdgeConnect hub gateways and SD-Branch was introduced in Release 9.5.2.

Tunnel Cipher Profiles are introduced in 9.5.4, however the tunnel Cipher Profile is not communicated to HPE Aruba Networking Central Overlay Tunnel Orchestrator (OTO). With Orchestrator and ECOS Release 9.5.4, the following algorithms are used by HPE Aruba Networking Central and must be enabled in the Tunnel Cipher Profile:

- Authentication: SHA1
- Encryption: AES-256-CBC

Starting with Release 9.6.0, ECOS sends the authentication method and encryption method to HPE Aruba Networking Central OTO. When a subsequent change is made to the tunnel Cipher Profile, e.g. disallow SHA1, ECOS sends a resync message to OTO.

Orchestrated IKE-based, IPSec Passthrough Tunnels to Select SSE Services (HPE SSE, Zscaler, Netskope, etc.)

Tunnels are orchestrated for specific SSE services such as HPE SSE, Zscaler, and Netskope, and IaaS cloud services AWS and Azure.

Service Orchestration is used to automate the integration of third-party service providers without an API.

For each service, navigate to the tunnel settings for that service. Perform the actions on the algorithms listed in Table 38 for each subsection (General, IKE, IPSec) to ensure the settings use algorithms that are enabled in the Cipher Profile you plan to activate.

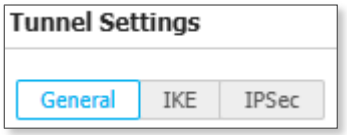

Figure 22: Tunnel Settings Subsections

You must also verify the allowable range of algorithm parameters for any partner service. Changing the Cipher Profile settings affects the “EdgeConnect end” of the tunnel and you must verify that any changes are compatible with the partner service.

- AWS Network Manager

  In Orchestrator, navigate to **Configuration > Cloud Services > AWS Network Manager**, and then click **Tunnel Settings**.

- HPE SSE

  In Orchestrator, navigate to **Configuration > Cloud Services > HPE SSE**, and then click **Tunnel Settings**.

- Microsoft Azure Virtual WAN

  In Orchestrator, navigate to **Configuration > Cloud Services > Azure Network Manager**. Click **On-prem Gateways**, and then click **Tunnel Settings**.

- Zscaler Internet Access

  In Orchestrator, navigate to **Configuration > Cloud Services > Zscaler Internet Access**, and then click **Tunnel Settings**.

- Netskope

In Orchestrator, navigate to **Configuration > Cloud Services > Netskope**, and then click **Tunnel Settings**.

- Service Orchestration Constructed, EdgeConnect-to-Third Party Passthrough Tunnels

  For services created within Service Orchestration, navigate to **Configuration > Cloud Services > Service Orchestration**, click on the tab for the service (if configured) and then click **Tunnel Settings**.

Manually Constructed, EdgeConnect-to-EdgeConnect Tunnels

1. In Orchestrator, navigate to **Configuration > Networking > Tunnels > Tunnels**.
2. Click the edit icon next to the appliance for which you want to add or modify a tunnel. The Tunnels dialog box opens.

   NOTE: To modify a tunnel, click the edit icon next to the tunnel. The Modify Tunnel dialog box opens.
3. Click **Underlay**.
4. Click **Add Tunnel**. The Add Tunnel dialog box opens.
5. Perform the actions on the algorithms listed in Table 38 for each subsection (General, IKE, IPSec) to ensure the settings use algorithms that are enabled in the Cipher Profile you plan to activate.

Manually Constructed, EdgeConnect-to-Third Party Passthrough Tunnels

1. In Orchestrator, navigate to **Configuration > Networking > Tunnels > Tunnels**.
2. Click the edit icon next to the appliance for which you want to add or modify a tunnel. The Tunnels dialog box opens.

   NOTE: To modify a tunnel, click the edit icon next to the tunnel. The Modify Tunnel dialog box opens.
3. Click **Passthrough**.
4. Click **Add Tunnel**. The Add Passthrough Tunnel dialog box opens.
5. Perform the actions on the algorithms listed in Table 38 for each subsection (General, IKE, IPSec) to ensure the settings use algorithms that are enabled in the Cipher Profile you plan to activate.

Table 38: IKE-based IPSec Settings for Validation

Tab	Action
General tab	No changes needed.
IKE Tab	For IKE-based IPSec tunnels there are three algorithms that correspond to Cipher Profile tunnel settings: • Authentication algorithm • Encryption algorithm • Diffie-Helman (DH) group Ensure these settings use algorithms that are enabled in the Cipher Profile you plan to activate.

IPSec tab	For IKE-based IPSec tunnels there are three algorithms that correspond to Cipher Profile tunnel settings: • Authentication algorithm • Encryption algorithm • Perfect forward secrecy group Ensure these settings use algorithms that are enabled in the Cipher Profile you plan to activate.

Troubleshooting Dropped Tunnels When Changing Cipher Profile Settings

If you do not follow the recommended order of operations when changing Cipher Profile settings, tunnels that are using algorithms that are disallowed by the active Cipher Profile will drop. If this happens, you can expect to see the following.

Alarms

If tunnels drop due to disallowed Cipher Profile settings, an alarm occurs for each tunnel that drops. To view the alarm description and recommended actions, navigate to **Monitoring > Summary > Alarms**. In the following example, the recommended action is to check the tunnel configuration and ensure that only allowed ciphers are used.

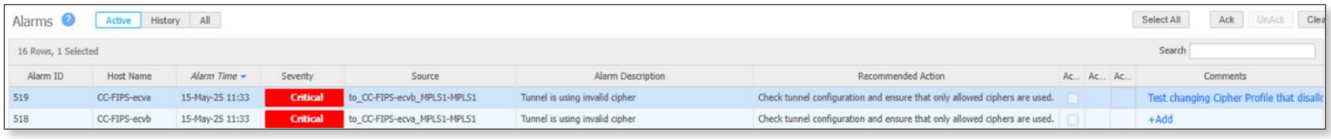

Figure 23: Orchestrator Alarms Tab

Tunnels Tab Status

On the Tunnels tab, tunnels that dropped due to use of disallowed ciphers show a status of “down - bad” in the Status column.

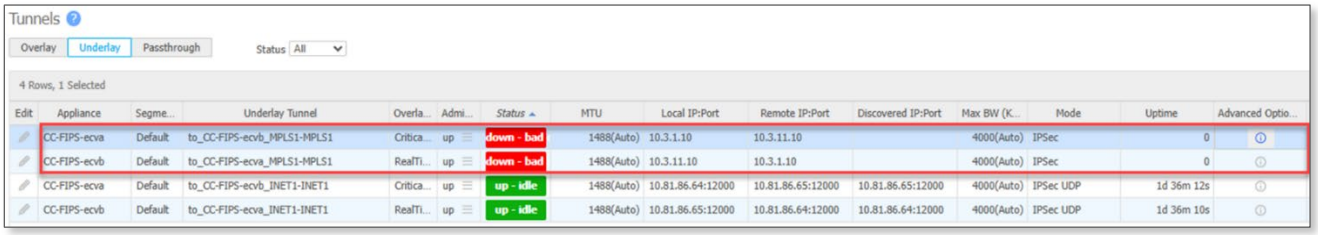

Figure 24: Orchestrator Tunnels Tab

Tunnel Settings Error Messages

If tunnels drop due to disallowed Cipher Profile settings, you need to manually correct the tunnel settings (**Orchestrator > Orchestrator Server > Tools > Tunnel Settings**). When attempting to save corrections for a single label, error messages appear on the dialog box for all nonconforming labels whether there are tunnels built for those labels or not, as shown in the following figure. You must correct the tunnel settings for each label to ensure they comply with the currently active Cipher Profile before you can click **Save**.

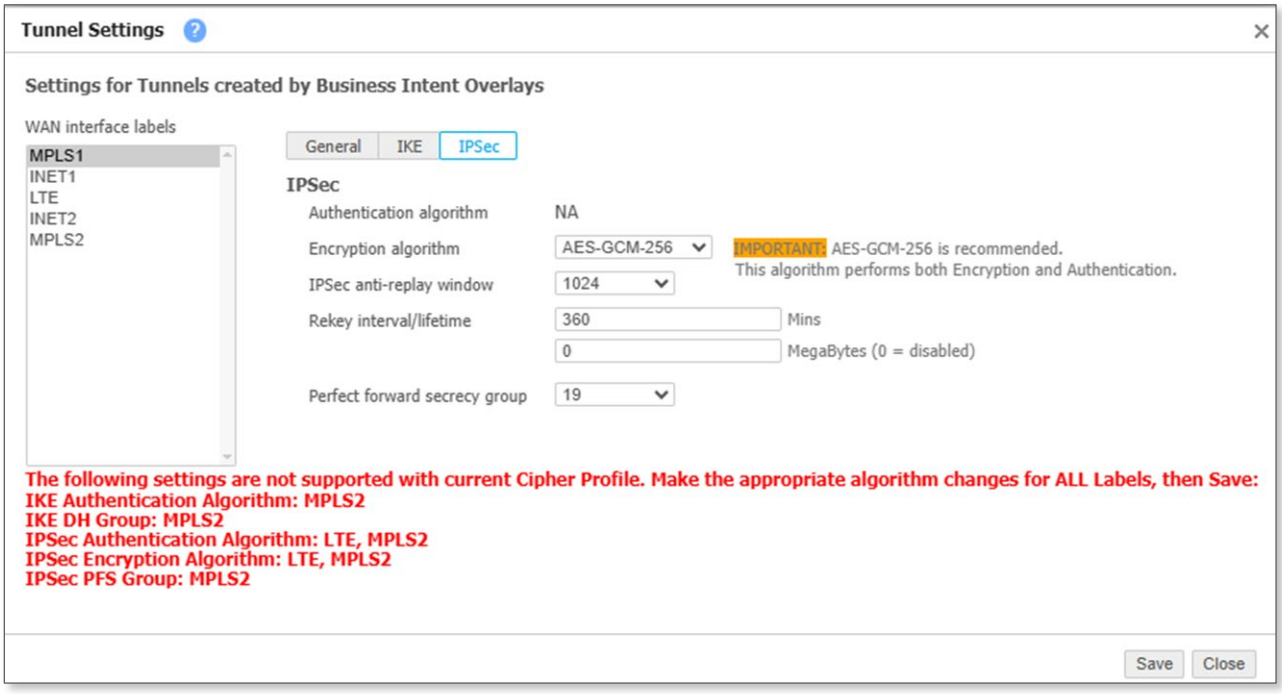

Figure 25: Cipher Profile Error Messages on Orchestrator Tunnel Settings Tab

SSH (ECOS)

To make an algorithm available for SSH service to use, click its associated check box.

Table 39: SSH Profile Settings

Setting	Description	Options
Key Exchange Algorithms	The algorithms available for EdgeConnect to use to establish a secure connection to the appliance CLI.	diffie-hellman-group1-sha1 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group-exchange-sha256 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 curve25519-sha256 curve25519-sha256@libssh.org

Setting	Description	Options
Encryption Algorithms	The algorithms available for EdgeConnect to use to encrypt data being sent to the appliance CLI.	aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com
HMAC Algorithms	The Hash-based Message Authentication Code (HMAC) algorithms available for EdgeConnect to use to when connecting to the appliance CLI.	hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-sha2-512
Host Key Algorithms		ecdsa-sha2-nistp256-cert-v01@openssh.com ecdsa-sha2-nistp384-cert-v01@openssh.com ecdsa-sha2-nistp521-cert-v01@openssh.com ssh-ed25519-cert-v01@openssh.com rsa-sha2-512-cert-v01@openssh.com rsa-sha2-256-cert-v01@openssh.com ssh-rsa-cert-v01@openssh.com ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-ed25519 rsa-sha2-512 rsa-sha2-256 ssh-rsa
CA Sign Algorithms		ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-ed25519 rsa-sha2-512 rsa-sha2-256 ssh-rsa

Setting	Description	Options
Public Key Algorithms		ecdsa-sha2-nistp256-cert-v01@openssh.com ecdsa-sha2-nistp384-cert-v01@openssh.com ecdsa-sha2-nistp521-cert-v01@openssh.com ssh-ed25519-cert-v01@openssh.com rsa-sha2-512-cert-v01@openssh.com rsa-sha2-256-cert-v01@openssh.com ssh-rsa-cert-v01@openssh.com ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-ed25519 rsa-sha2-512 rsa-sha2-256 ssh-rsa

NOTE: In ECOS Releases 9.4.4, 9.5.4, and 9.6.0, there is a bug that results in rsa-sha2-256 and rsa-sha2-512 algorithms being disabled (even if checked) unless the weaker cipher, ssh-rsa, is enabled. Instead of using RSA, ssh-ed25519 is recommended to be enabled for Host Key Algorithms, CA Sign Algorithms, and Public Key Algorithms.

How to Configure SSH on ECOS

ECOS SSH configuration is orchestrated via the Cipher Profile settings. While still an option, there is no need to configure via CLI.

Certificate

The certificate settings apply to end-entity certificates for both Orchestrator and EdgeConnect.

Table 40: Certificate Profile Settings

Setting	Description	Options
Fail connection on OCSP undetermined	When a certificate is uploaded in Orchestrator, the Online Certificate Status Protocol (OCSP) is run by Orchestrator and EdgeConnect to verify the status of the certificate. If communication cannot be established with the OCSP server, then the revocation check is ignored, but the connection does not necessarily fail. When this setting is enabled, if communication cannot be established with the OCSP server then the connection will fail.	Enabled or disabled
Min RSA Key length	Indicates minimum RSA key length for certificates.	2048 (default) 3072 4096

Setting	Description	Options
Min EC Key length		224 256 (default) 384 521
ECC Curves		Custom options: secp224r1 (included in default profile) secp256r1 (included in default profile) secp384r1 (included in default profile) secp521r1 (included in default profile)
HMAC Algorithms		Custom options: sha1 (included in default profile) sha256 (included in default profile) sha384 (included in default profile) sha512 (included in default profile)

NOTE: If ECOS is using a Certificate with key length 2048, it can talk to other TLS servers using a longer key length of 3072 (CSfC-compliant) certificates.

When applying a Cipher Profile, Orchestrator checks ECOS if it has a valid Certificate. If not, the Cipher Profile will NOT be applied, and alarm will be raised. During the time of Zero Touch Provisioning (initial deployment), ECOS TLS Client will accept a server certificate, for example key length of 3072, even if ECOS does not yet have CSfC Profile activated. This will enable initial communications ECOS to Cloud Portal and ECOS to Orchestrator.

How to Configure Certificates on Orchestrator and ECOS

For information on configuring certificates, see End Entity Certificates Tab and End Entity Certificate Validation at the Time of Upload in the Orchestrator User Guide.

SNMP (ECOS)

To make an algorithm available for SNMP service to use, click its associated check box.

Table 41: SNMP (ECOS) Profile Settings

Setting	Description	Options
Encryption Algorithms	The encryption algorithms available for EdgeConnect to use to for SNMP service.	AES-CBC-128 AES-CBC-256

Setting	Description	Options
Hash Algorithms	The secure hash algorithms available for EdgeConnect to use for SNMP service.	SHA-1 SHA2-256 SHA2-384 SHA2-512

How to Configure SNMP on ECOS

Starting with Release 9.5.4, SNMP configuration is performed via Orchestrator templates or via the Cipher Profile settings.

- If Cipher Profile settings change, and any SNMP configuration uses privacy algorithms that are no longer valid, the system overwrites the hash algorithms to use one of the values allowed in the Cipher Profile.
- Similarly, if the SNMP configuration is changed to set hash and privacy algorithms, the system performs a check at the ECOS end to ensure the values are WRT allowed values and if they are not, the values are overwritten.

NTP (ECOS)

For NTP, you can select the algorithms available for EdgeConnect to use for network time protocol (SHA2-265, SHA2-384, and SHA2-512). To make an algorithm available for NTP service to use, click its associated check box.

How to Configure NTP on ECOS

EdgeConnect OS supports NTP and manual time setting. NTP server can be setup for all appliances in the SD-WAN fabric using the Orchestrator template. However, Secure NTP requires configuration on the CLI.

Set up NTP Servers Using Orchestrator Template

Set up the NTP servers for all EdgeConnect appliances in the SD-WAN fabric using the Orchestrator Date/Time Template. For more information, see Date/Time Setting in the Orchestrator User Guide.

1. In Orchestrator, navigate to **Configuration > Templates & Policies > Templates**.

   The Date/Time template should be in the Default Template Group. If desired, new template groups can be created to set time zone by region.

2. Set time zone and NTP server, as shown in the following figure.

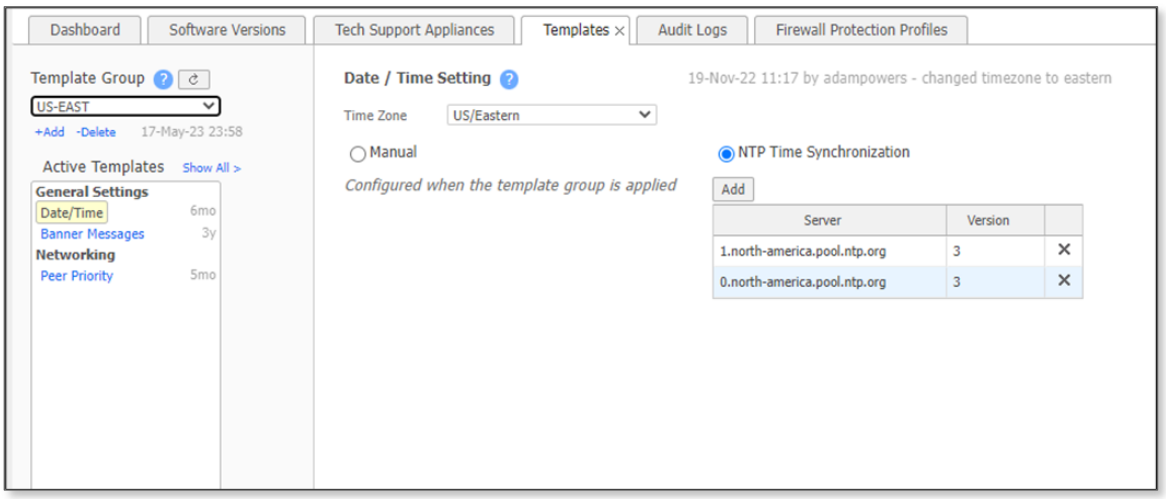

Figure 26: Orchestrator Date/Time Template

Configure Secure NTP on the CLI

Secure NTP Parameters

- Key id can be between 1-255.
- Algorithm is recommended to be **SHA384**.
- Pre-shared key can be any string. There is no restriction on string length or character composition.

Secure NTP Procedure

1. Authenticate to the EdgeConnect CLI/SSH.
2. Execute `enable`
3. Execute `configure terminal`
4. Add PSKs to the appliance:

   Execute `ntp key <Key id> <Algo> <pre shared key>`

   Example: `ntp key 10 sha384 uwefh8239hngli28`
5. Select one of the keys to securely connect:

   NOTE: You can only select keys from the list of available keys. To see the list of available keys:

   Execute `show ntp key`

   Execute `ntp select-key <Key id>`

   Example: `ntp select-key 10`
6. Restart the ntpd service:

   Execute: `pm process ntpd restart`

Optional CLI commands for secure NTP:

- Delete a Key: Execute `no ntp key <key id>`
- Displays all the ntp keys: Execute `show ntp key`
- Displays a specific key: Execute `show ntp key <key id>`

Manual NTP Server Setup

To manually set the NTP server for a single EdgeConnect appliance:

1. Execute `ntp server <IP address> version 4`
2. Execute `ntp enable`
3. Execute `write memory`

Manually Change Appliance Time or Date

1. Authenticate to the EdgeConnect CLI/SSH.
2. Execute `enable`
3. Execute `configure terminal`
4. Execute `clock set hh:mm:ss yyyy/mm/dd`
5. Execute `write memory`

Cluster

Starting with Release 9.5.2 the Cluster feature was introduced. Ciphers are not configurable and are fixed to AES-256-CBC for encryption and SHA-512 for hashing.

Starting with Release 9.6.0, Cluster is one of the services within the Cipher Profile settings.

Figure 27: Cipher Profiles Dialog Box - Cluster Settings (Release 9.6.0 only)

To make an algorithm available for Cluster service to use, click its associated check box.

Table 42: Cluster Profile Settings

Setting	Description	Options
Encryption Algorithm	The encryption algorithms available for Orchestrator and EdgeConnect to use for Clusters.	AES-CBC-256 AES-CBC-128 AES-GCM-128 AES-GCM-256

Setting	Description	Options
Authentication Algorithm	The authentication algorithms available for Orchestrator and EdgeConnect to use for Clusters.	SHA-1 SHA2-256 SHA2-384 SHA2-512 AES-GMAC-128 AES-GMAC-256

How to Configure Clusters on Orchestrator

For information on configuring Clusters, see Cluster Profiles and Clusters in the Orchestrator User Guide.

NOTE: Cluster security is only configured via Cipher Profile settings starting with Release 9.6.0.

Appendix A: Glossary of Terms

Table 43: Glossary

Abbreviation	Meaning
AES	Advanced Encryption Standard, as specified in [FIPS 197]
AES-GCM	AES with Galois/Counter Mode
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CNSA	Commercial National Security Algorithm Suite
CSfC	Commercial Solutions for Classified
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic Curve Diffie-Hellman (Algorithm)
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman (NIST SP 800-56A)
ECDSA	Elliptic Curve Digital Signature Algorithm
ECOS	EdgeConnect Operating System
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode (GCM) and GMAC Algorithm
HMAC	Keyed-Hash Message Authentication Code, as specified in [FIPS 198]
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IETF	Internet Engineering Task Force

Abbreviation	Meaning
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
KAS	Key Agreement Schemes and Key Confirmation (NIST SP 800-56A)
KDF	Key Derivation Function
MAC	Message Authentication Code
MD5	Message Digest 5
NIST	National Institute of Standards and Technology
NRBG	Non-deterministic Random Bit Generator
NSA	National Security Agency
NTP	Network Time Protocol
PKCS	Public Key Cryptography Standard
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest Shamir Adleman Cryptographic System (FIPS 186-4)
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SSE	Security Service Edge
SSH	Secure Shell
SSL	Secure Sockets layer
TLS	Transport Layer Security
UDP	User Datagram Protocol

Appendix B: References

https://csrc.nist.gov/publications/sp800

Table 44: NIST References

Reference	Specification
FIPS 140-2	Security Requirements for Cryptographic modules, May 25, 2001
FIPS 180-4	Secure Hash Standard (SHS)
FIPS 186-4	Digital Signature Standard
FIPS 197	Advanced Encryption Standard (AES)
FIPS 198-1	The Keyed-Hash Message Authentication Code (HMAC)
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
SP 800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
SP-800-52 Rev 2	Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
SP 800-56A Rev 3	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
SP 800-56B	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
SP 800-90A	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
SP 800-108	Recommendation for Key Derivation Using Pseudorandom Functions
SP 800-132	Recommendation for Password-Based Key Derivation
SP 800-133 Rev 2	Recommendation for Cryptographic Key Generation
SP 800-135	Recommendation for Existing Application –Specific Key Derivation Functions

Table 45: IETF References

Reference	Specification
RFC 8784	Mixing Pre-shared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

Table 46: Common Criteria References

Reference	Specification
CPP_ND_V2.2E	Collaborative Protection Profile for Network Devices (NDcPP) v2.2e, March 2020
MOD_VPNGW_v1.3	PP-Module for VPN Gateways Version 1.3, August 2023