



# **HPE Aruba Networking EdgeConnect SD-WAN**

Security and System Hardening Guide

Version 3 – November 2023

## Important Notice

© Copyright 2023 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Aruba Networks and the Aruba logo are registered trademarks of Aruba Networks, Inc. Third-party trademarks mentioned are the property of their respective owners. To view the end-user software agreement, go to [Aruba EULA](#).

Revision A, November 2023

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



**Table of Contents**

HPE Aruba Networking SD-WAN Platform Architecture..... 5

    Orchestrator Configuration ..... 6

        Orchestrator Configuration and Security Settings..... 7

        IP Allow List – Orchestrator UI ..... 8

        Licensing & Cloud Portal ..... 9

        Orchestrator User Management..... 11

        API Keys..... 12

        Role-Based Access Control (RBAC)..... 13

        Orchestration Settings ..... 14

        Security Settings ..... 15

        IPsec Key Rotation..... 15

        Advanced Security Settings ..... 16

        Custom CA Certificate Trust Store ..... 19

        Advanced Properties – sslIncludeCiphers ..... 20

        Orchestrator – Self-Managed – Setup Script ..... 21

        Loopback Orchestration ..... 22

        Restricting Gateway Management Plane Access ..... 24

        Orchestrator Templates to Manage EdgeConnect Gateways ..... 26

        Orchestrator Configuration & Templates Best Practices Summary ..... 36

SD-WAN Fabric Data Plane..... 37

    Orchestrator Tunnel Settings..... 37

        EdgeConnect to EdgeConnect IPsec UDP Tunnels ..... 38

        EdgeConnect-to-EdgeConnect IKE-Based IPsec Tunnels ..... 40

        EdgeConnect-to-Third-Party IKE-Based IPsec Tunnels ..... 40

    SD-WAN Fabric Dataplane Configuration - Best Practice Summary ..... 41

EdgeConnect Gateway Configuration..... 42

    Configuration Wizard – Admin Password ..... 43

    WAN Interface Firewall ..... 44

    Management Interfaces (MGMT0 / MGMT1) ..... 45

    EdgeConnect Gateway Configuration - Best Practice Summary ..... 46

Appendix: Password Considerations ..... 47



## **Purpose of this document**

This document provides overviews and recommendations of best practices for EdgeConnect SD-WAN system security and hardening configurations.



## Version Control

Document Version	Software Version Coverage	Release Date
Version 1 – Initial Release	Orchestrator 9.1 & ECOS 9.1	January 2022
Version 2	Orchestrator 9.3 & ECOS 9.3	October 2023
Version 3	Orchestrator 9.3 & ECOS 9.3	November 2023



## HPE Aruba Networking SD-WAN Platform Architecture

The EdgeConnect SD-WAN Platform systems interconnection can be categorized into management plane and data plane, as illustrated in Figure 1.

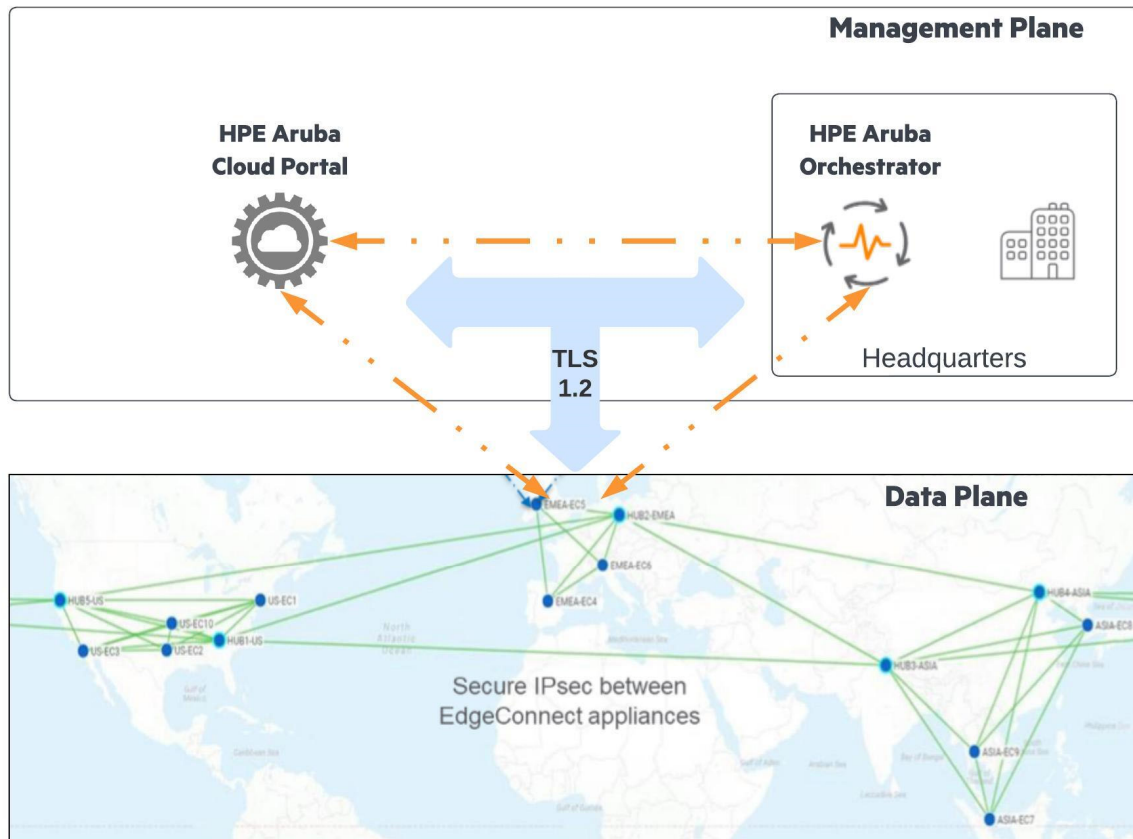


Figure 1: EdgeConnect Platform Architecture

EdgeConnect's management plane uses secure TLS 1.2. The management plane generally utilizes permanent WebSocket connections between EdgeConnect gateways, Orchestrator, and Cloud Portal. This assumes that all components have internet access.

In cases where specific customer requirements do not permit or cannot provide direct internet from branch sites or via backhaul (e.g., MPLS Only with Explicit proxy for Internet traffic), EdgeConnect gateways can reach Cloud Portal through their connection to Orchestrator.

For data plane traffic, EdgeConnect SD-WAN, by default, uses patented "IKE-less" IPsec technology (aka IPsec UDP), allowing tunnel cryptographic material to be distributed via the Orchestrator. Subsequent tunnel encryption keys are generated using the distributed material, ensuring a secure and robust tunnel architecture with minimal overhead.

EdgeConnect SD-WAN also supports standard IKE-based IPsec, Generic UDP, or GRE tunnel encapsulations for transport. Determining which tunnel encapsulation type to use is based on customer requirements (e.g., FIPS Compliance) and is outside this document's scope. For conciseness, the remaining sections of this document will refer to the default and recommended IKE-less IPsec (IPsec UDP) configuration.



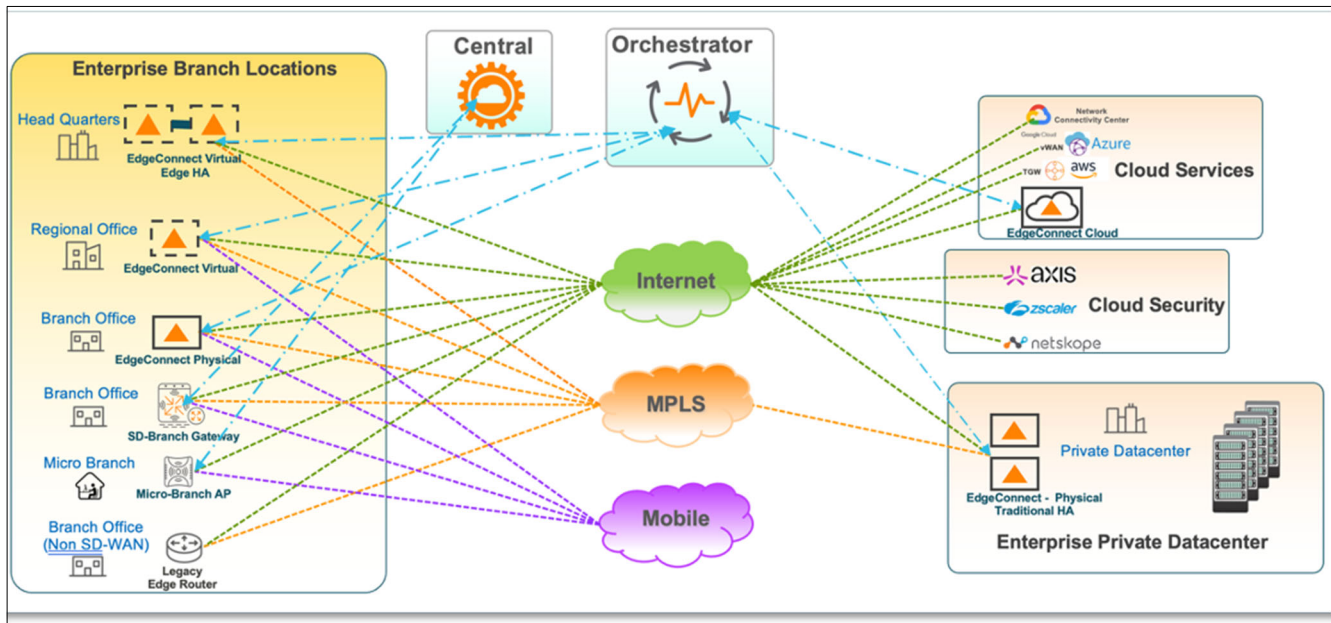


Figure 2: EdgeConnect SD-WAN Platform Architecture

Figure 2 depicts the EdgeConnect architecture from several perspectives:

- An enterprise with a mix of EdgeConnect physical and virtual gateways that interconnect via multiple underlay networks, with internet through traditional wired or wireless/mobile access, as well as private MPLS networks.
- Networking between EdgeConnect gateways (aka the SD-WAN “fabric”) and between EdgeConnect gateways and third-party services such as security services and public clouds.
  - Management Plane: interconnects HPE Aruba’s Cloud Portal, the HPE Aruba Networking SD-WAN Orchestrator, and HPE Aruba Networking EdgeConnect SD-WAN gateways and runs over TLS 1.2 secure connections.
  - Data Plane: Orchestrator automatically creates (orchestrates) data plane tunnels between EdgeConnect gateways. EdgeConnect-to-EdgeConnect data plane tunnels are by default, constructed using HPE Aruba Networking’s IPsec UDP (aka IKE-less) technology. Tunnels between EdgeConnect gateways and third-party services use standard IKE-based (IKEv1 or IKEv2) IPsec tunnels.
  - Data Plane – 3<sup>rd</sup> Party – Automated: Orchestrator automatically creates tunnel configurations end-to-end for third-party automated services such as AWS TGNM, Azure Virtual WAN, CheckPoint Harmony, Netskope or Zscaler ZIA.
  - Data Plane – 3<sup>rd</sup> Party – Orchestrated: Orchestrator automatically creates tunnel configurations for third-party orchestrated services configured via “Service Orchestration.”<sup>1</sup>

## Orchestrator Configuration

<sup>1</sup> [SD-WAN Docs - Service Orchestration](#)



Before deployment, discovery, acceptance, and configuration of EdgeConnect gateways into an SD-WAN fabric, it is essential to prepare Orchestrator settings and configuration templates per HPE Aruba Networking's best practices to ensure the full effectiveness of all enterprise security policies.

## Orchestrator Configuration and Security Settings

This section details security settings for Orchestrator itself. Important configuration menus about orchestration settings, management plane security, and data plane security are listed here, along with an explanation of critical parameters.

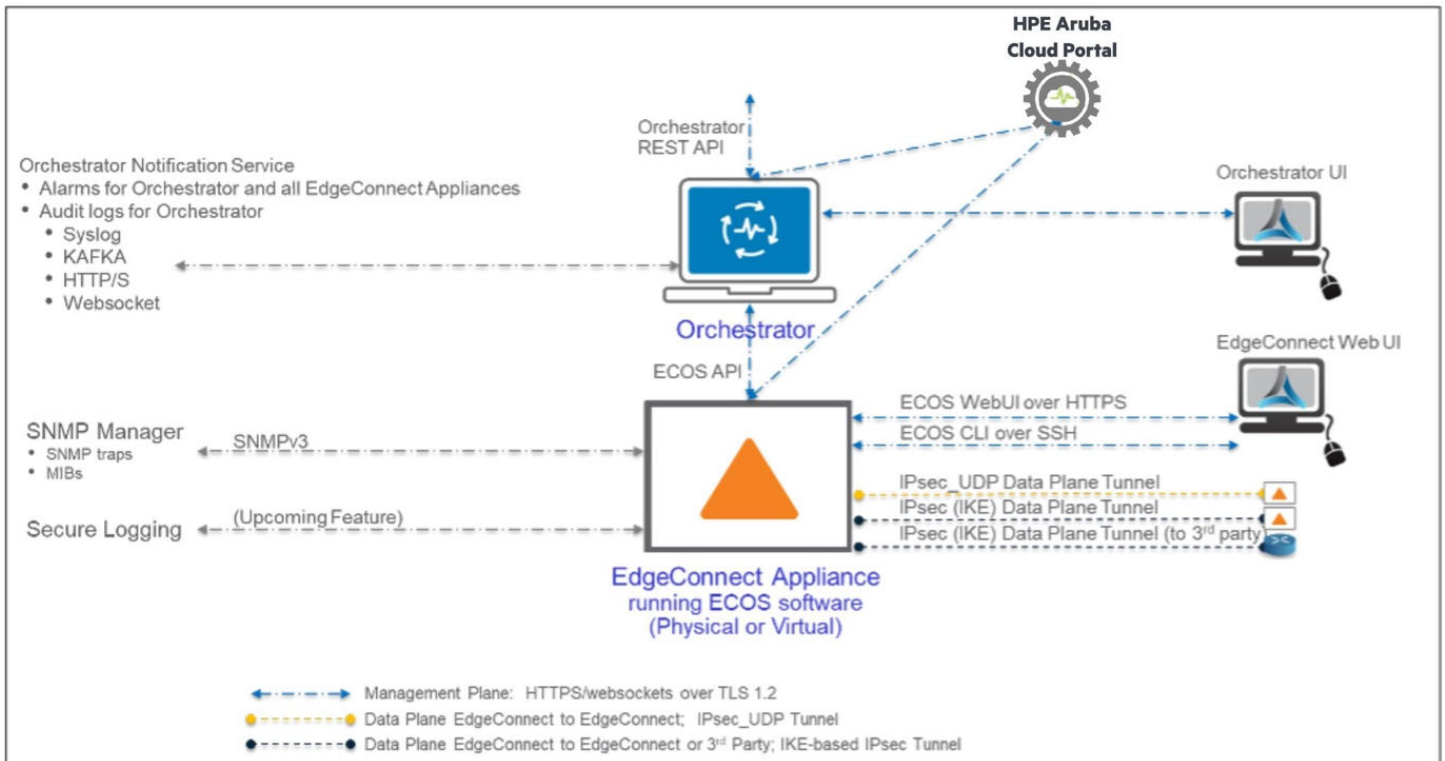


Figure 3: EdgeConnect Cryptographic Connections

Figure 3 shows EdgeConnect's management plane and data plane cryptographic connections. Most of the Orchestrator, template, and EdgeConnect-specific settings affect the security of these connections.



## IP Allow List – Orchestrator UI

Access to Orchestrator UI can be limited and controlled by configuring the IP Allow list, thereby stipulating specific IP ranges that can access Orchestrator. This feature is available on self-hosted Orchestrators and HPE-hosted Orchestrator-as-a-Service (OaaS).

To access these settings in Orchestrator, navigate to **Orchestrator > Software & Setup > Setup > IP Allow List**. The dialog in *Figure 5* opens, where you can configure your enterprise IP ranges as needed. Once configured if a user attempts to access the Orchestrator UI from an IP address outside of what is contained in the IP Allow List the user will receive a message “You do not have sufficient privileges to access the resource. Contact your administrator.”

For troubleshooting purposes, you can view any attempts that were denied based on the IP Allow List by clicking on the “IP Allow List Drops” in the lower left corner of the IP Allow List dialog.

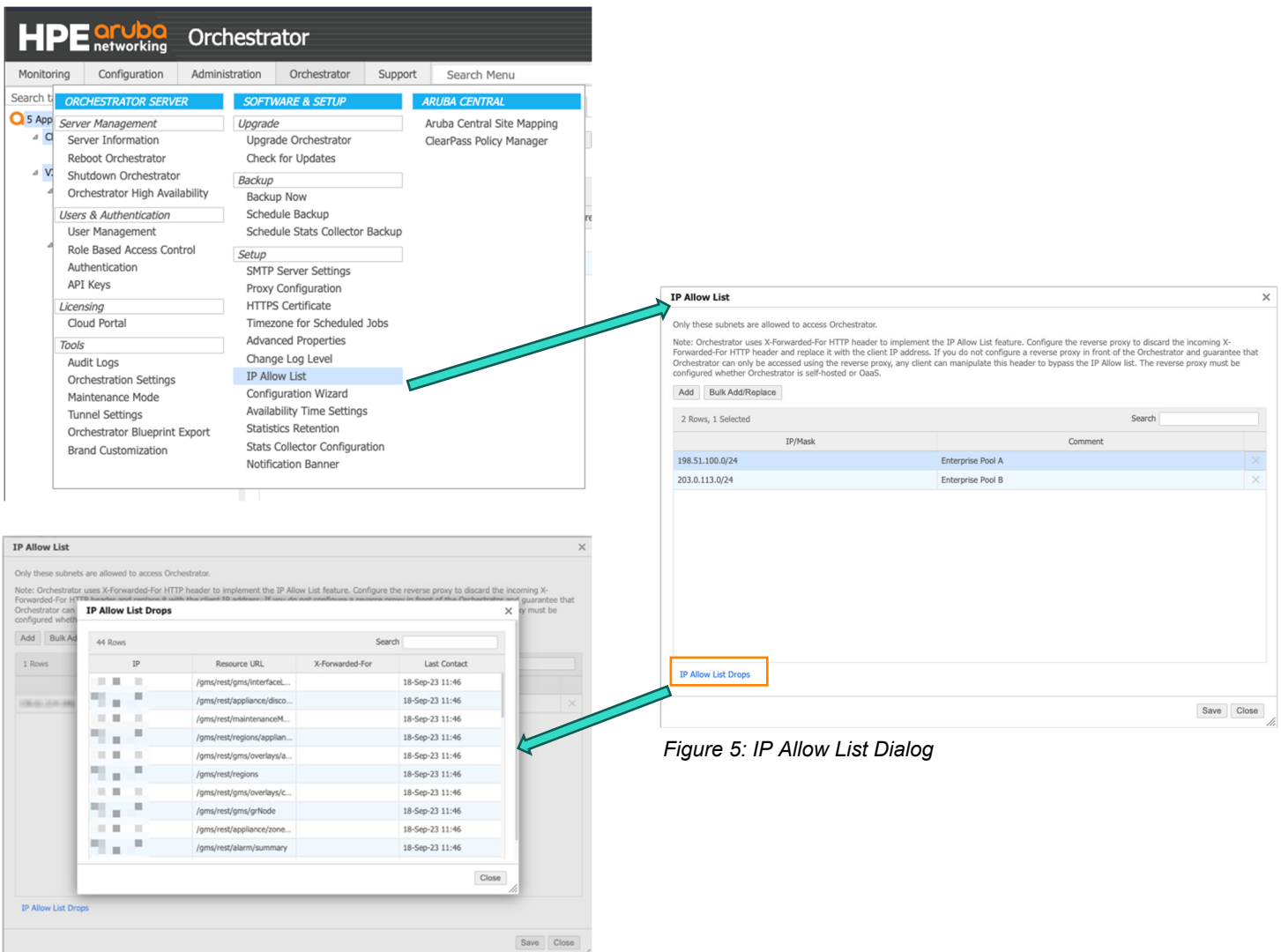


Figure 5: IP Allow List Dialog

Figure 5: IP Allow List Drops

**NOTE:** Orchestrator uses X-Forwarded-For (XFF) HTTP header to implement the IP Allow List feature, and it will check the LAST IP in the XFF list of IP addresses if multiple are present.

It is very important that you are careful to specify the correct set of Source IP ranges, to avoid lock-out of the WebUI. In the event of an inadvertent lock-out you must contact TAC support to revert the allow list configuration.



## Licensing & Cloud Portal

HPE Aruba Networking SD-WAN provides Zero Touch Provisioning (ZTP) for physical and virtual gateways. ZTP dramatically simplifies deployment and automatically reduces configuration errors by enabling remote gateways to download key configuration settings—such as site-specific network configuration data, Business Intent Overlay policies, and predefined configuration templates—when plugged into a network.

When an appliance is plugged into the network, it looks for a DHCP address (or a static IP address is provisioned through a mechanism such as CloudInit) and then connects via TLS 1.2 to the Cloud Portal at `portal.silverpeak.cloud`.

Physical gateways authenticate to Cloud Portal with a built-in shared secret. Virtual gateways require the account name and key, which can be pre-provisioned via CloudInit, USB Based ZTP, or a CLI command.

The account name, account key, and appliance tag can be provisioned with the following CLI command:

```
edgeconnect # conf t
edgeconnect(config) # system registration <My Account Key> <My Account Name> <Appliance Group Name> <Appliance Tag>
edgeconnect(config) # end
```

The configuration can be displayed with the `show system registration` command.

```
edgeconnect # show system registration
Account Key:          <My Account Key>
Account Name:        <My Account Name>
Appliance Group Name:
Appliance Site Name: <Appliance Tag>
edgeconnect #
```

---

NOTE: *Appliance Tag* is documented as “Site Name” and can be any site-specific information that assists with authentication when the appliance is discovered by Orchestrator.

---

While optional, Aruba strongly recommends provisioning the appliance tag, which serves two functions:

- The appliance tag can serve as “two-factor authentication” to verify the identity of a discovered appliance.
- The appliance tag links a discovered appliance to a pre-configuration YAML file on Orchestrator to automate an appliance’s initial configuration.

After the appliance has successfully connected and authenticated with the Aruba Cloud Portal, it shares its serial number.

The serial number is already associated with the enterprise customer account (or service provider account) in Aruba’s database for hardware gateways.

After registering the appliance, the Cloud Portal notifies the appropriate tenant Orchestrator that the new appliance is displayed in the “Discovered Appliances” list within the Orchestrator, where it can be approved, and configuration applied accordingly.



As an additional layer of security, the **Orchestrator > Licensing > Cloud Portal > Advanced** configuration menu provides an option requiring you to provision the account name and key on hardware gateways to authenticate with Cloud Portal.

This setting applies to all gateways on the account associated with this Orchestrator.

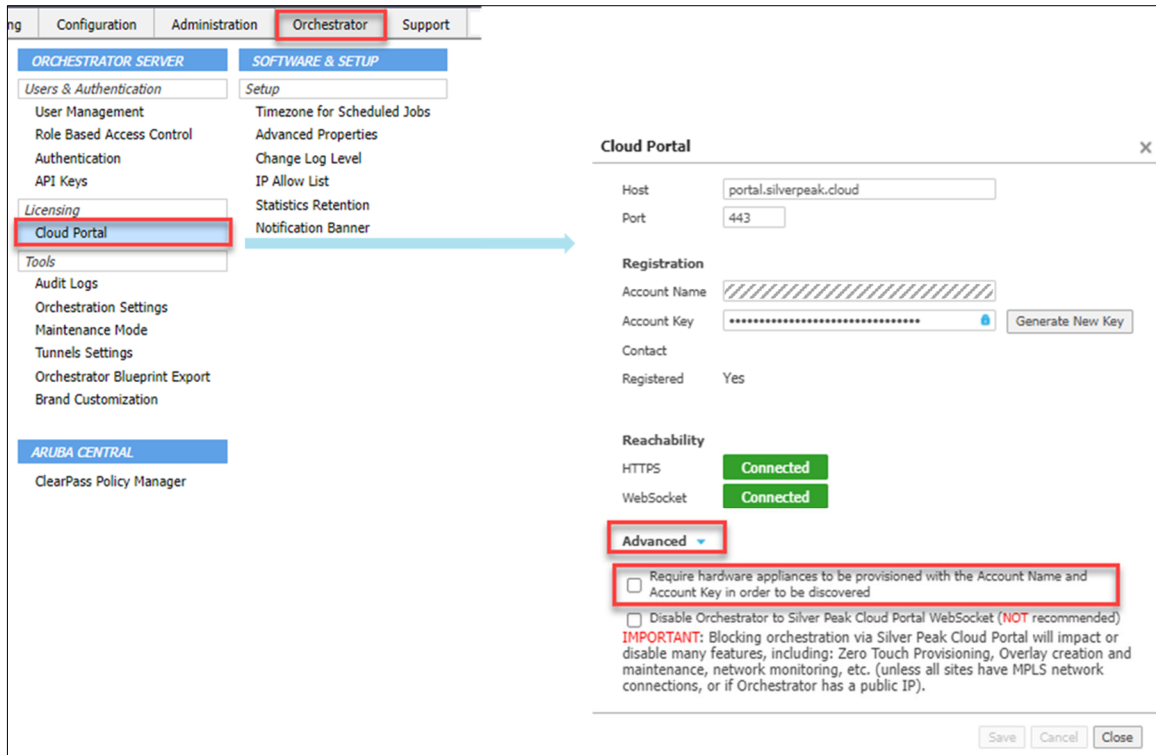


Figure 6: Cloud Portal Authentication in Orchestrator



## Orchestrator User Management

### Local User Account(s)

Use the User Management dialog to manage local user accounts with Read-Write or Read-Only access to Orchestrator. These accounts are local to the Orchestrator and should be limited in scope and used for initial stand-up configuration purposes only.

Local accounts should always use Multi-Factor Authentication (MFA), the Orchestrator supports MFA applications based on RFC 4226 and RFC 6238. Google Authenticator or Microsoft Authenticator are examples of applications that support these authentication methods.

Read-Only users will be restricted to “GET” API-Level access when using REST-API and Read-Write users are not restricted unless RBAC roles are applied to those users.

Please refer to the “Appendix: Password Considerations” for further best practice on defining passwords.

### Auto Logout – Orchestrator WebUI

Specifies the time in minutes after which an inactive WebUI session will be automatically logged out. The valid range is 0-60. Use 0 to disable automatic logout.

### Max Sessions – Orchestrator WebUI

Maximum number of active WebUI sessions on the Orchestrator. If the maximum number of sessions is reached, users who try to log in to the Orchestrator web UI will receive a message that the login has failed.

### Failed Login Handling

Invalid login attempts are automatically restricted for both the Orchestrator.

Login attempts directly to the Orchestrator WebUI are handled as follows,

- After four failed attempts, further login attempts using either the same user account or originating from the same IP address are locked out for 5 minutes, and an alarm is generated.



## Authentication – Remote Authentication (SAML, OAuth, JWT, TACACS+, RADIUS)

Use the Remote Authentication dialog box to manage different remote authentication methods for Orchestrator users.

Supported protocols for authentication are,

- SAML
- OAuth
- JWT
- TACACS+
- RADIUS

Please visit the SD-WAN Documentation pages [here](#) for information on configuring these different protocols.

## API Keys

API Keys can be configured to allow application access to the Orchestrator REST APIs without session authentication and management. You can specify your API keys' name, permission (read-only or read-write), expiration date, status, and IP allow list.

Additionally, starting in Orchestrator 9.3.1 for each API key you can specify the Role(s) and/or an Appliance Access Groups that will apply to the calls made using the API Key.

An API key can be passed either in the HTTP request header field *X-Auth-Token* or as a query parameter *apiKey*.

For more information on configuring API Keys please visit the SD-WAN Documentation pages [here](#).

Figure 7: API Key Dialog Orchestrator 9.3.0

Figure 9: API Key Dialog Orchestrator 9.3.1

---

**NOTE:** API Key IP allow lists are separate from the IP Allow List covered in a previous section of this document, both should be used based on best practices.

---



## **Role-Based Access Control (RBAC)**

Role-Based Access Control (RBAC) allows for a more personalized Orchestrator experience. You can assign specific roles to individual users, which determine their level of access, the menu options they see in the Orchestrator UI, and their ability to access appliance groups. In combination with remote authentication, RBAC ensures that users have the least access necessary to use Orchestrator effectively.

For more information on configuring Role-Based Access Control (RBAC) please visit the SD-WAN Documentation pages [here](#).



## Orchestration Settings

The recommended mode of operation for EdgeConnect SD-WAN is fully Orchestrated. By default, the Orchestrate Gateways by Applying and Updating Overlays check box is **not** selected in a new Orchestrator with no gateways. When gateways are added, this box is selected automatically.

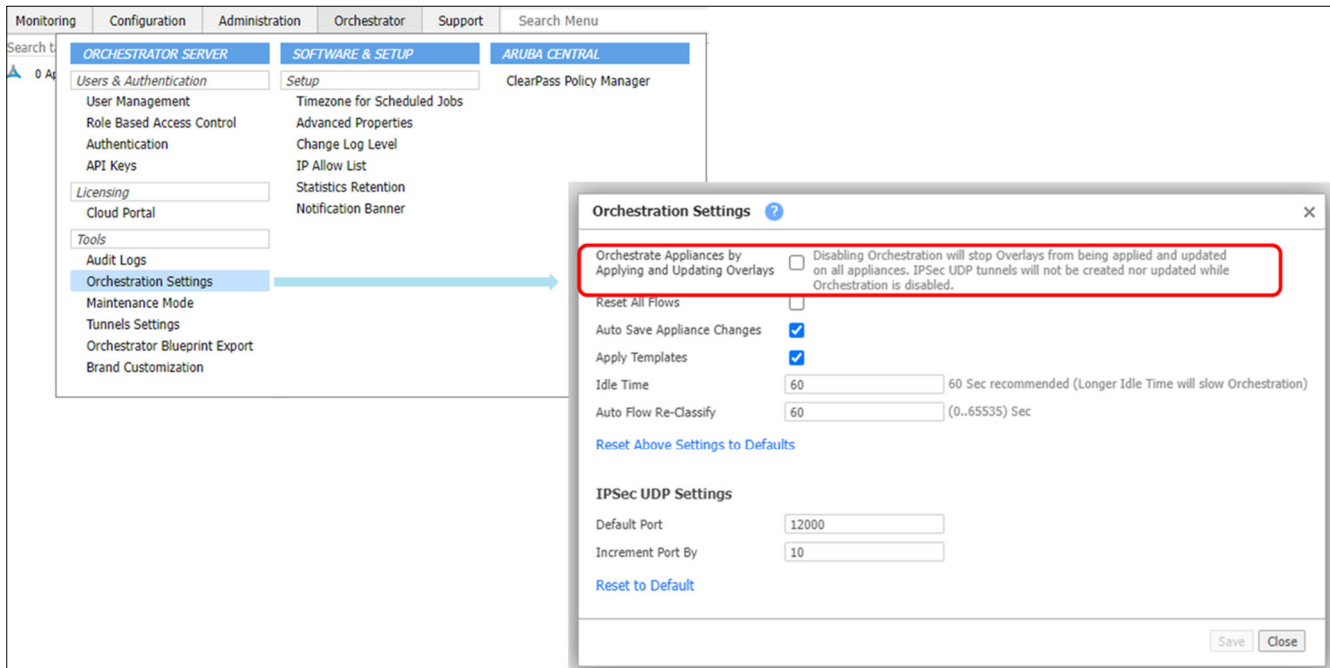


Figure 10: Orchestration Settings in Orchestrator



## Security Settings

The following security-relevant configuration menus in the Security group (Configuration > Overlays & Security > Security) should be set up prior to the discovery of EdgeConnect gateways:

- IPsec Key Rotation
- Advanced Security Settings
- Custom CA Certificate Trust Store

The sections that follow describe these menus.

### IPsec Key Rotation

IPsec Key Rotation is covered in the [SD-WAN Fabric Data Plane](#) section of this guide.



## Advanced Security Settings

The Advanced Security Settings menu provides controls for management plane security between Cloud Portal, Orchestrator, and EdgeConnect gateways.

From a security hardening perspective, Aruba strongly recommends enabling all these settings, including Secure Shell Access.

To enable these settings:

1. Navigate to **Configuration > Overlays & Security > Security > Advanced Security Settings**.
2. Select all checkboxes in the Advanced Security Settings window.
3. In the Appliance Shell Access Setting field, select Secure Shell Access.
4. Click Save.

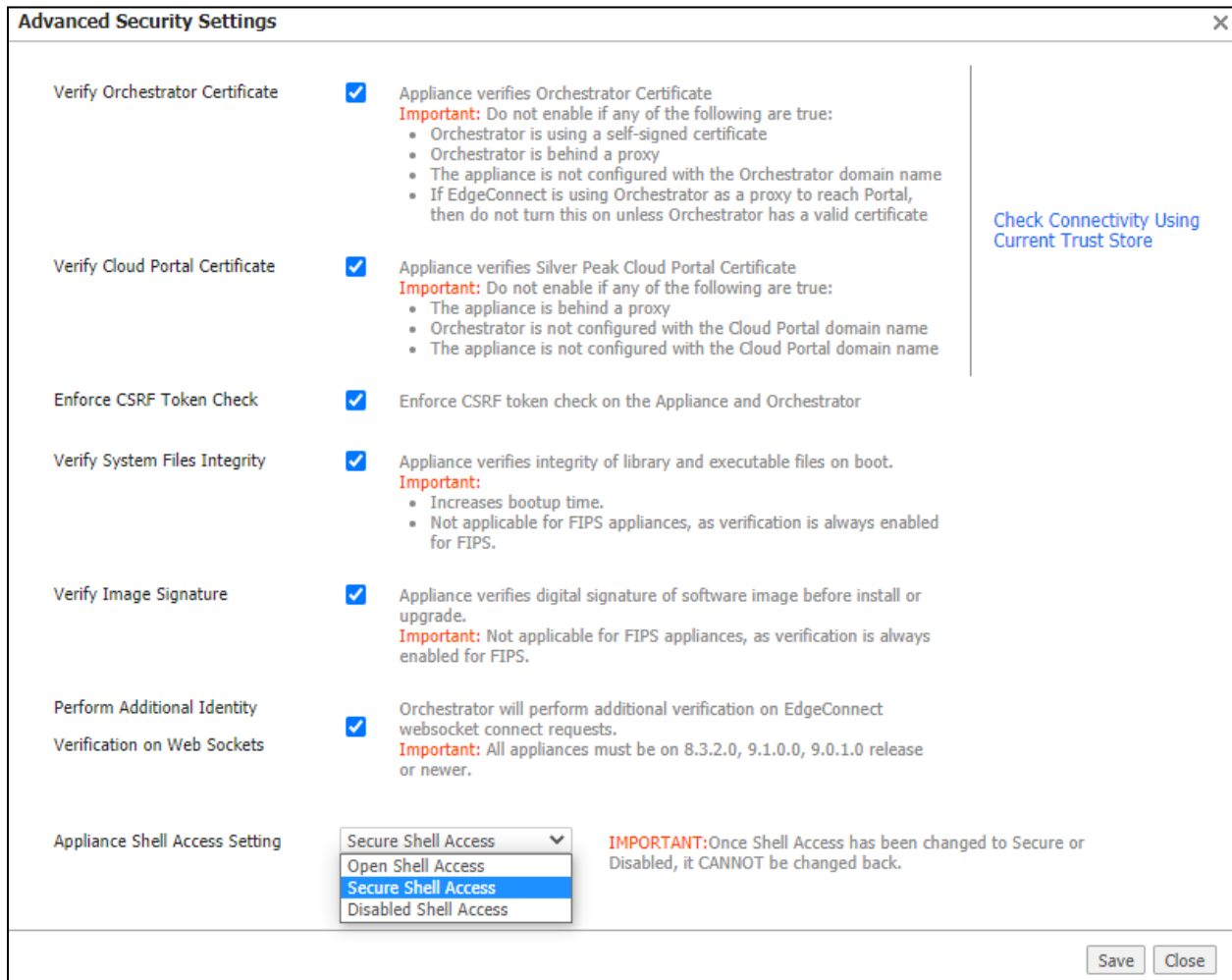


Figure 11: Orchestrator Advanced Security Settings

**NOTE:** Not all of these are set by default for new Orchestrators. The administrator must ensure that these settings are ALL enabled (Aruba recommendation).

For more details on each setting, see *Table 1*.



Table 1: Orchestrator 9.1 Advanced Security Settings

Setting	Description
<b>Verify Orchestrator Certificate</b>	<p>EdgeConnect gateways verify the Orchestrator Certificate. Aruba recommends this setting be enabled. <b>However, do not enable if any of the following are true:</b></p> <ul style="list-style-type: none"> <li>Orchestrator is behind a proxy.</li> <li>The appliance is not configured with the Orchestrator domain name.</li> <li>If EdgeConnect uses Orchestrator as a proxy to reach Cloud Portal, do not enable this setting unless Orchestrator has a valid certificate.</li> <li>Orchestrator does not have a certificate signed by a public certificate authority, or if Orchestrator does not have the appropriate private certificate authority root certificate.</li> </ul> <p>Aruba recommends this condition be remedied prior to deploying any EdgeConnect gateways.</p>
<b>Verify Cloud Portal Certificate</b>	<p>EdgeConnect gateways verify the Aruba Cloud Portal Certificate. Aruba recommends this setting be enabled. <b>However, do not enable if any of the following are true:</b></p> <ul style="list-style-type: none"> <li>The appliance is behind a proxy.</li> <li>Orchestrator is not configured with the Cloud Portal domain name.</li> <li>The appliance is not configured with the Cloud Portal domain name.</li> </ul>
<b>Enforce CSRF Token Check</b>	<p>Enforce CSRF token check on the appliance and Orchestrator. Aruba recommends this setting always be enabled.</p>
<b>Verify System Files Integrity</b>	<p>Appliance verifies the integrity of the library and executable files on boot. Aruba recommends this setting be enabled.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTES:</b></p> <ul style="list-style-type: none"> <li>When enabled, this setting increases bootup time.</li> <li>Gateways with FIPS mode enabled always perform system files integrity check.</li> </ul> </div>
<b>Verify Image Signature</b>	<p>Appliance verifies the digital signature of the software image before install or upgrade. Aruba recommends this setting be enabled.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> Gateways with FIPS mode enabled <b>always</b> verify image signature.</p> </div>
<b>Perform Additional Identity Verification on Web Sockets<sup>2</sup></b>	<p>Orchestrator performs additional verification on EdgeConnect WebSocket connection requests.</p> <ul style="list-style-type: none"> <li>ECOS uses the account name and account key to authenticate with Cloud Portal.</li> <li>ECOS creates a signed token using its account key and attaches it to the X-AUTH-TOKEN HTTP header of the WebSocket request.</li> </ul> <p>As a best practice, Aruba recommends that the Additional Identity Verification check always be enabled.</p>

<sup>2</sup> Starting with Orchestrator 9.3, the “Perform Additional Identity Verification on Web Sockets” setting is no longer modifiable and has been removed from the UI.



**Appliance  
Shell Access  
Setting**

**Open Shell Access:** ECOS admin users have full access to the underlying Linux shell. This is the case for Orchestrators prior to Release 9.0 and will remain the case after Orchestrator is upgraded to Release 9.0 or later.

**This setting is NOT recommended!**

**Secure Shell Access:** ECOS admin users need a token granted by Aruba Technical Support to access the underlying Linux shell for troubleshooting. This is the default value for Orchestrators instantiated with Release 9.0 or later.

At a minimum, Aruba recommends this setting.

**Disabled Shell Access:** Linux shell is **permanently** disabled.

**NOTES:**

- Gateways with FIPS mode enabled completely disable shell access independent of this setting.
- After shell access has been changed to Secure or Disabled, it **CANNOT** be changed back.



## Custom CA Certificate Trust Store

Starting with ECOS 9.0.3 and Orchestrator 9.0.4, EdgeConnect supports enterprise customers who use their own CA-certified certificates that may not be included in EdgeConnect’s Standard Trust Store.

This feature provides the capability to load an enterprise’s self-signed certificate or their own CA-issued certificate into their self-hosted Orchestrator and have ECOS validate the certificate as part of the management plane communications between ECOS and Orchestrator. This feature also includes utilities to test connectivity to both Cloud Portal and Orchestrator and ensure continuity of operations.

To add a custom certificate:

1. Navigate to **Configuration > Overlays & Security > Security > Custom CA Certificate Trust Store**.
2. Click **Add Certificate to Custom Trust Store**.
3. Add your certificate information, and then click **Save**.
4. Click **Test Connectivity to Portal** to validate that appliances can successfully connect to Orchestrator and Cloud Portal using the custom CA.
5. If the connectivity test is successful, you can select the **“Use Custom Certificate Trust Store”** check box, and then click **Apply Changes**.

Figure 12 below shows the test output for both the “Default CA Trust Store” and “Custom CA Trust Store”

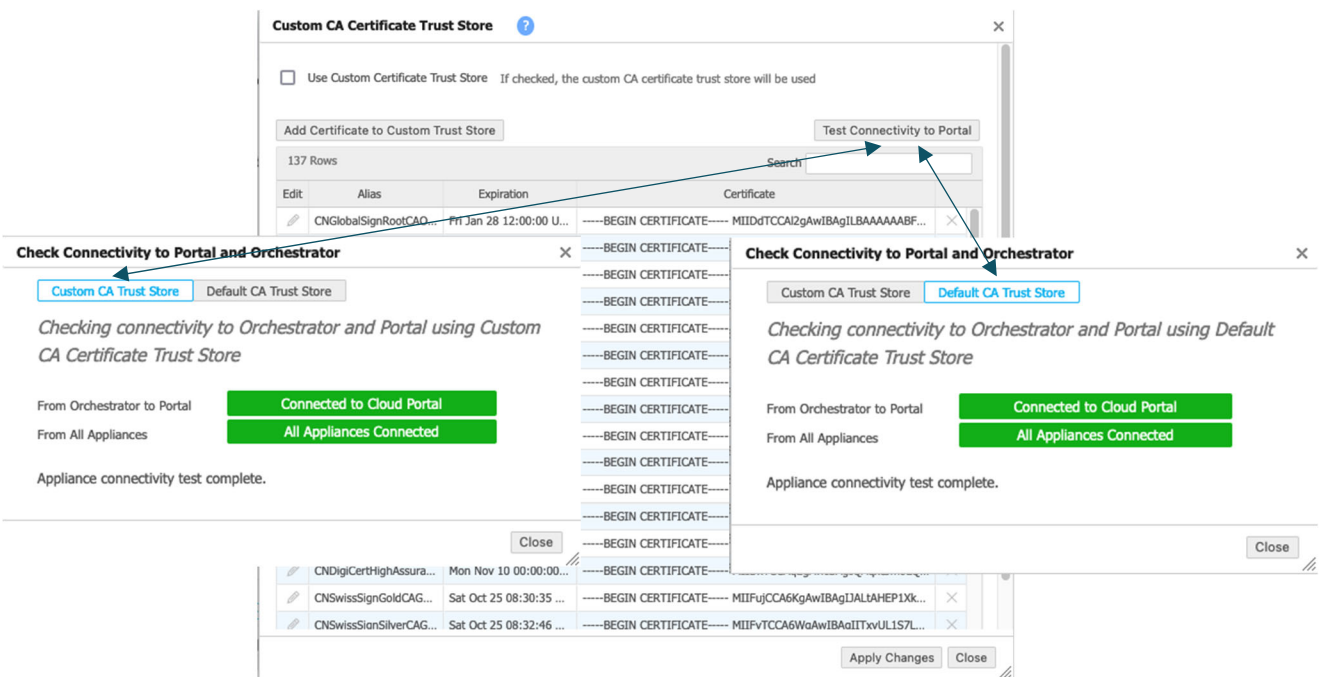


Figure 12: CA Certificate Trust Store and Test Results

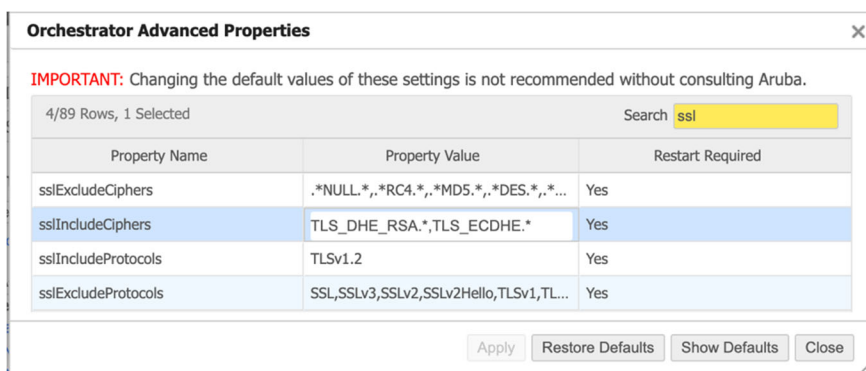


## Advanced Properties – sslIncludeCiphers

The Orchestrator administrator can use the “sslIncludeCiphers” property in its advanced configuration to control the supported ciphers for the Orchestrator UI.

To modify this configuration:

1. Navigate to **Orchestrator > Software & Setup > Setup > Advanced Properties**.
2. In the Search field enter “ssl”
3. Modify the configuration with the desired cipher (See example below)
4. After modification you will need to reboot your Orchestrator to apply the changes.



**Orchestrator Advanced Properties**

**IMPORTANT:** Changing the default values of these settings is not recommended without consulting Aruba.

4/89 Rows, 1 Selected Search

Property Name	Property Value	Restart Required
sslExcludeCiphers	.*NULL.*,*RC4.*,*MD5.*,*DES.*,*...	Yes
sslIncludeCiphers	TLS_DHE_RSA.*,TLS_ECDHE.*	Yes
sslIncludeProtocols	TLSv1.2	Yes
sslExcludeProtocols	SSL,SSLv3,SSLv2,SSLv2Hello,TLSv1,TL...	Yes

Apply Restore Defaults Show Defaults Close

Figure 13: Orchestrator Advanced Properties

The following string is recommended:

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
```

---

**NOTE:** This setting is only applicable for self-managed Orchestrators deployed either on-premises or in a customer owned cloud environment. OaaS customers cannot modify this configuration.

---



## Orchestrator – Self-Managed – Setup Script

For customers that opt for a self-managed Orchestrator deployment, either on-premises or via an IaaS provider such as AWS, Azure, or GCP, the orchestrator has a setup script that can be run to tune various configuration settings to improve the baseline security of the underlying OS.

To run the script after deploying your Orchestrator VM connect via Console or SSH, elevate to root privileges and run the following command,

```
root@orchestrator-rl:/$ cd /home/gms/gms/
root@orchestrator-rl:/home/gms/gms$ ./orch-setup -c

OS version: Rocky Linux release 9.1 (Blue Onyx)
=====
NOTE: Section of Orchestrator script has been removed for brevity.
=====

Choose from any of the following system configuration changes if you would like to perform
Would you like to set up symmetric NTP authentication? Enter 1.
Would you like to change fail2ban settings? Enter 2.
Would you like to change SSH config? Enter 3.
Would you like to setup password quality? Enter 4.
Would you like to set up Message Of The Day? Enter 5.
Would you like to set up Banner text? Enter 6.
Would you like to change SSH client timeout? [y/n] y
Would you like to change SSH Server timeout? [y/n] y

*****
SSH Server timeout is ClientAliveInterval multiplied by ClientAliveCountMax
*****
SSH server ClientAliveInterval(seconds): 60
SSH server ClientAliveCountMax: 10
Would you like to change the RekeyLimit? [y/n] n
=====
```

---

**NOTE:** For Orchestrator version 9.3 the underlying OS is CentOS 7, starting with Orchestrator 9.4 the underlying OS has been upgraded to Rocky Linux release 9.2.

---



## Loopback Orchestration

As a best practice, Aruba recommends setting up a loopback address for management services to serve as the host management address. This provides a stable, consistent source IP address for all management traffic and allows enterprise customers to create an allow list in external firewalls for the specific loopback address range for connectivity to Cloud Portal or for restricting management plane access directly to the gateway WebUI or CLI via SSH.

### Loopback Interface Label

To get started, an interface label for the loopback address must be created—by default, Orchestrator does not have a loopback label.

Navigate to **Configuration > Overlays & Security > Interface Labels**.

1. Click **New Label**.
2. Click **LAN**.
3. Name the label (e.g., LOOPBACK), click **Done**, and then click **Save**.

You should see your new loopback label on the Interface Labels table,

Interface Labels		
<a href="#">New Label</a>		
11 Rows		
Edit	Type	Label
	wan	LAB1
	wan	MPLS2
	wan	INET2
	wan	LTE (Hub & Spoke)
	wan	INET1
	wan	MPLS1
	lan	Loopback

Figure 14: Interface Labels Table



## Loopback Pool

Though Loopback Orchestration is not configured by default in Orchestrator, the best practice is to use orchestrated loopbacks.

### NOTE:

Before adding loopback interfaces, you must determine an appropriate loopback IP address pool to work with the enterprise's IP addressing scheme.

This document assumes that management traffic will be in the Default network segment (this assumes ECOS R9.0 or greater with network segmentation enabled). Starting with ECOS 9.1, network segmentation is enabled by default.

Navigate to **Configuration > Networking > Loopback Orchestration**.

1. On the Segment field → select the segment (in this example Default Segment is shown)
2. Click **+Add Loopback Interface**.
3. In the Label field, select **LOOPBACK** (or whatever you named your interface in the previous section).
4. In the Zone field, select **Default**.
5. In the Management field, select the **Show this IP in the Tree** check box.
6. Click **Add**.

*Figure 15: Loopback Orchestration Loopback Pool* the Loopback IP address pool of 172.23.1.0/27. As noted above, any appropriate IP address range should be reserved in your organization's IP Address manager for this global loopback pool.



Loopback Orchestration ? **NOTE:** Management IP is now configured on [Management Services](#) tab

[+Add Loopback Interface](#) Segment:

1 Rows Search

Segment	Label	Zone	Management IP	Loopback Pool	Allocated / Total	Deleted
Default	Loopback	Management	Yes	172.23.1.0/27	5 / 32	0

*Figure 15: Loopback Orchestration Loopback Pool*



## Restricting Gateway Management Plane Access

By configuring loopback interfaces on all gateways and setting up management services to source traffic from these interfaces, it provides a consistent and robust endpoint for management functions that is provided the same protections as regular data plane traffic. In addition to the robustness provided by the loopback we can also use the single address we can confidently restrict access to the appliance management plane services by configuring firewall policies to limit source subnets which are permitted to reach the loopback interfaces.

### Address Groups

Address groups provide a flexible and scalable way to configure IP address groups globally within the Orchestrator. These groups can be referenced in security policy as needed across the platform. In this example we will configure two address groups, one will contain the enterprise IP space permitted to access EdgeConnect gateways, and the second will contain the EdgeConnect gateway loopback IP range.

To configure the Address Group

1. Navigate to **Configuration > Templates & Policies > ACLs > Address Groups**
2. Click **“Add Group”**
3. In the **“Group Name”** enter a name for the Address Group (e.g. `Management_Networks`)
4. In the **“IPs to include”** field, enter the source IP ranges needing direct access to the gateway management plane.
5. Click **“Add”**
6. Repeat these steps and add an address group for the loopback IP pool (e.g. `Gateway_Loopbacks`).

The screenshot shows the 'Add Address Group' dialog box with the following fields:

- Group name:** Management\_Networks
- Rules:**
  - IPs to include:** 198.51.100.0/24, 203.0.113.0/24
  - IPs to exclude:** Example: 10.10.20.1, 10.10.20.2
  - Groups to include:** Example: Group1, Group2, Group3
  - Comment:** (empty)
- Buttons:** Add, Cancel

Figure 16: Address Group Dialog “Management\_Networks”

The screenshot shows the 'Add Address Group' dialog box with the following fields:

- Group name:** Gateway\_Loopbacks
- Rules:**
  - IPs to include:** 172.23.1.0/27
  - IPs to exclude:** Example: 10.10.20.1, 10.10.20.2
  - Groups to include:** Example: Group1, Group2, Group3
  - Comment:** (empty)
- Buttons:** Add, Cancel

Figure 17: Address Group Dialog “Gateway\_Loopbacks”



## Firewall Policies

To configure the necessary access control to restrict access to the WebUI, SNMP, and SSH:

1. Navigate to **Configuration > Networking > Routing > Routing Segmentation (VRF)**
2. Under the “Default” segment, click **+Add** under the “Firewall Zone Policies”
3. In the “Default” to “Default” Zone intersection, click **“Add Rule”**
4. Click **“Edit”** for the new rule under **“Match Criteria”**
5. Click **“More Options”**
6. In the **IP/Subnet** field change to **“Groups”** and for Source select **“Management\_Networks”** for Dest select **“Gateway\_Loopbacks”**
7. In the Port field enter the ports for your desired management services (e.g. 22 and/or 443), if you enter multiple ports separate them with a **“|”** symbol.
8. In the Protocol field select **“TCP”** (See **Error! Reference source not found.**)
9. Click **“Save”**
10. In the “Default” to “Default” Zone intersection, click **“Add Rule”**
11. Click **“Edit”** for the new rule under **“Match Criteria”**
12. Click **“More Options”**
13. In the **IP/Subnet** field change to **“Groups”** and for Source leave this set to **“any”** for Dest select **“Gateway\_Loopbacks”**
14. Click **“Save”**

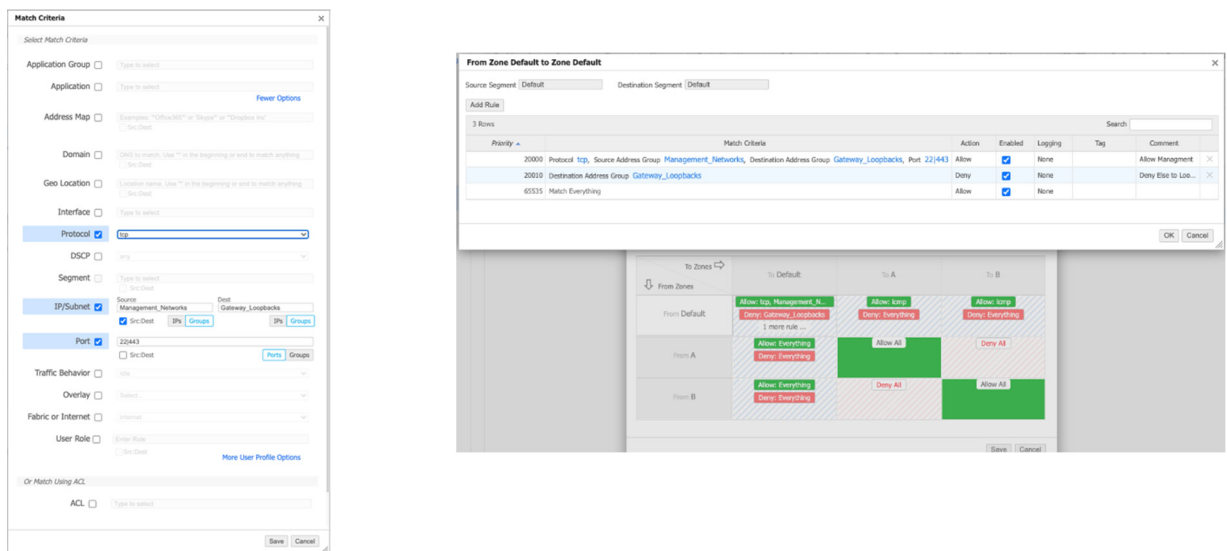


Figure 19: Management Networks Rule

### NOTES:

The above steps assume that the Orchestrator is an OaaS, if the Orchestrator is self-hosted you must add an explicit rule to allow communication between the loopbacks and your Orchestrator.

The above steps assume segmentation is enabled, and the loopbacks are part of the Default segment and Default Zone. If you are using a dedicated “Management” zone the zone intersection where you define the rules will need to be adjusted.



## Orchestrator Templates to Manage EdgeConnect Gateways

Services, functions, or features that are common to all (or a subset of) EdgeConnect gateways are managed by Orchestrator through templates (Configuration > Templates & Policies > Templates). Typically, templates are applied during the EdgeConnect appliance Zero Touch Provisioning (ZTP) process. Usually, the Default Template is applied.

The Default Template Group includes SNMP, DNS, Date/Time, Admin Distance, Shaper, Management Services, and Session Management. For system hardening, three Default Templates are covered in this section: SNMP, Management Services, and Session Management.

### Default Template Group

To view the Default Template Group:

1. Navigate to **Configuration > Templates & Policies > Templates**.
2. Under Template Group, select **Default Template Group**.
3. Select the template you want to edit under Active Templates

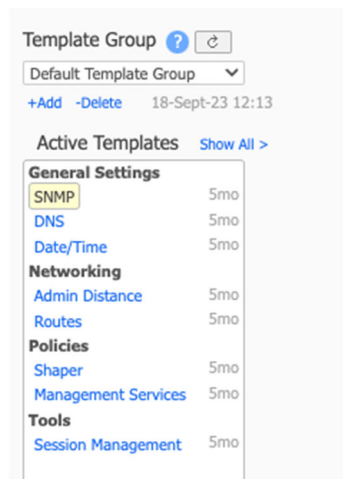


Figure 20: Default Template Group



## SNMP

SNMP is disabled by default. If SNMP management is required, Aruba recommends SNMPv3.

Template Group ? 🗑️  
Default Template Group ▼  
[+Add](#) [-Delete](#) 18-Sept-23 12:13

Active Templates [Show All >](#)

**General Settings**

- SNMP 5mo
- DNS 5mo
- Date/Time 5mo

**Networking**

- Admin Distance 5mo
- Routes 5mo

**Policies**

- Shaper 5mo
- Management Services 5mo

**Tools**

- Session Management 5mo

**SNMP** ? 22-Mar-23 21:05

**SNMP**

- Enable SNMP
- Enable SNMP Traps
- Default Trap Community

**SNMP V1/V2**

- Enable SNMP V1/V2
- Read-Only Community

**SNMP V3**

[Add](#)

Enabled	Username	Authenti...	Authentication Passw...	Privacy T...	Privacy Password	
<input checked="" type="checkbox"/>	snmp_user	SHA1	****	AES-128	****	<a href="#">X</a>

**Trap Receivers**

[Add](#)

Host	Version	Community/Username	Enabled	
<i>No Data Available</i>				

Figure 21 : SNMP Template

---

**NOTE:** SNMPv3 Authentication only supports SHA1 and Privacy only supports AES-128

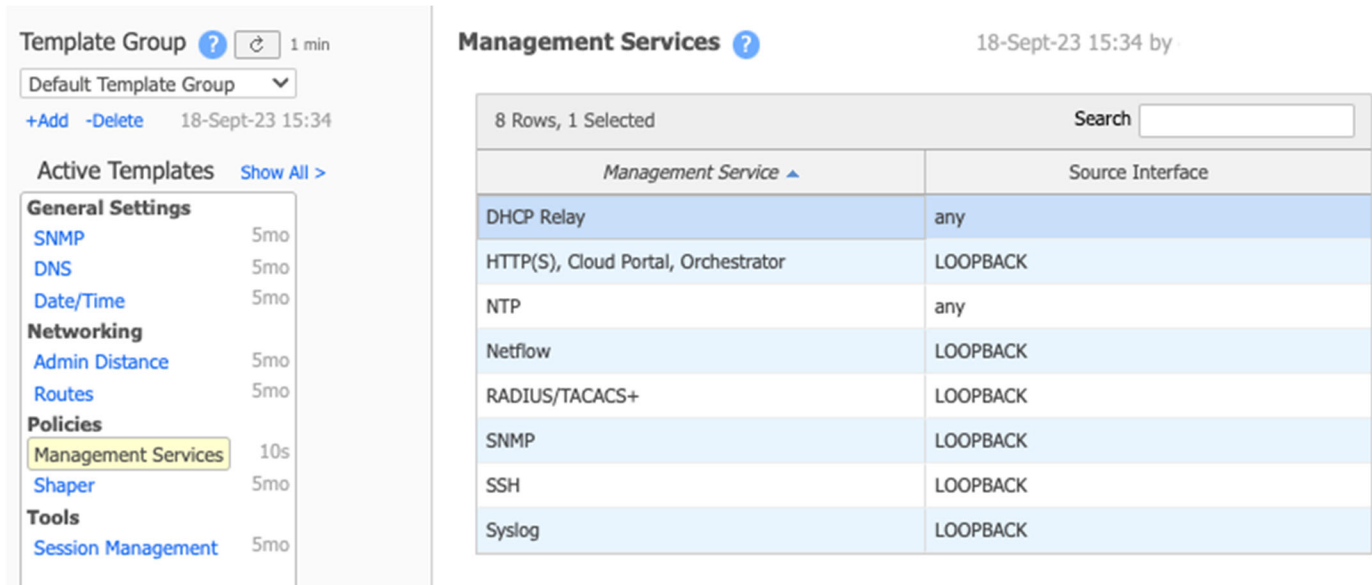
---



## Management Services

The EdgeConnect Management Services template specifies which interfaces an appliance should use for a particular management service. By default, the interface is set to any.

Aruba recommends setting the source interface to a loopback address, as detailed in the [Loopback Orchestration](#) section. This provides IP source address consistency across services.



Management Service	Source Interface
DHCP Relay	any
HTTP(S), Cloud Portal, Orchestrator	LOOPBACK
NTP	any
Netflow	LOOPBACK
RADIUS/TACACS+	LOOPBACK
SNMP	LOOPBACK
SSH	LOOPBACK
Syslog	LOOPBACK

Figure 22: Management Services Template

---

**NOTE:** It is recommended to keep DHCP relay set to any, this ensures that DHCP relay traffic can source from any LAN side interface. Option 82 is inserted to ensure that the DHCP lease is allocated from the correct DHCP scope and returned to the proper GIADDR address.

---



## Session Management

The Session Management template includes security settings that pertain to connecting to an EdgeConnect appliance Web User Interface (Web UI). By default, only HTTPS is allowed. HTTP should not be enabled.

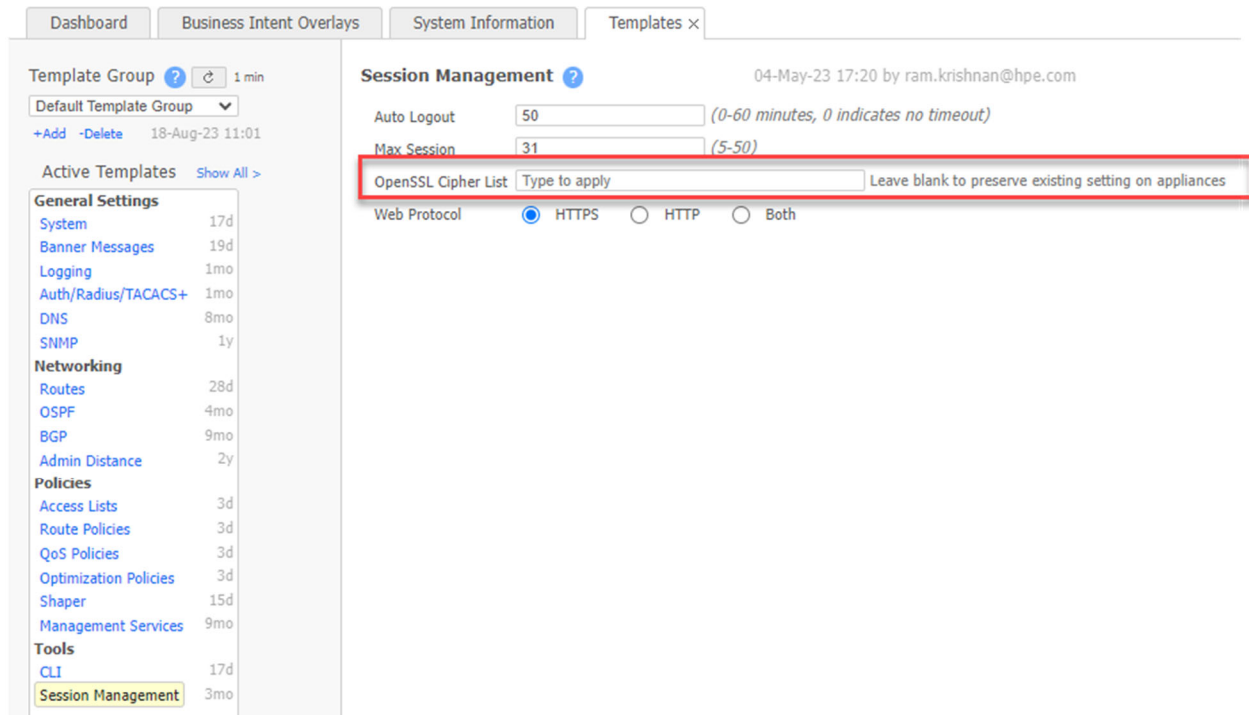


Figure 23: HTTPS Selected as the Web Protocol in Orchestrator

## Failed Login Handling

Invalid login attempts are automatically restricted for the EdgeConnect gateways.

Login attempts directly to the gateway WebUI or CLI via SSH are handled as follows,

- For the first 60 seconds, ECOS permits unlimited attempts,
- If there are more than four failed attempts in any 60 seconds after that, then login attempts are blocked for 60 seconds.



Orchestrator provides the Session Management template option, orchestrating the cipher setting across all gateways with one click. Figure 24 shows the template user interface with the help window expanded. A warning informs customers to test the proposed cipher in their environment to ensure compatibility with connected systems.

Starting with ECOS 9.0.3 and Orchestrator 9.0.4, the Session Management template also provides a way to directly enter an OpenSSL Cipher List, if the enterprise customer security team requires it. This is intended to be used only by enterprise customers with strict security requirements who want to set their own ciphers for the gateway Web UI (TLS server).

---

**NOTE:** Aruba recommends leaving the OpenSSL Cipher List field blank (default).

---

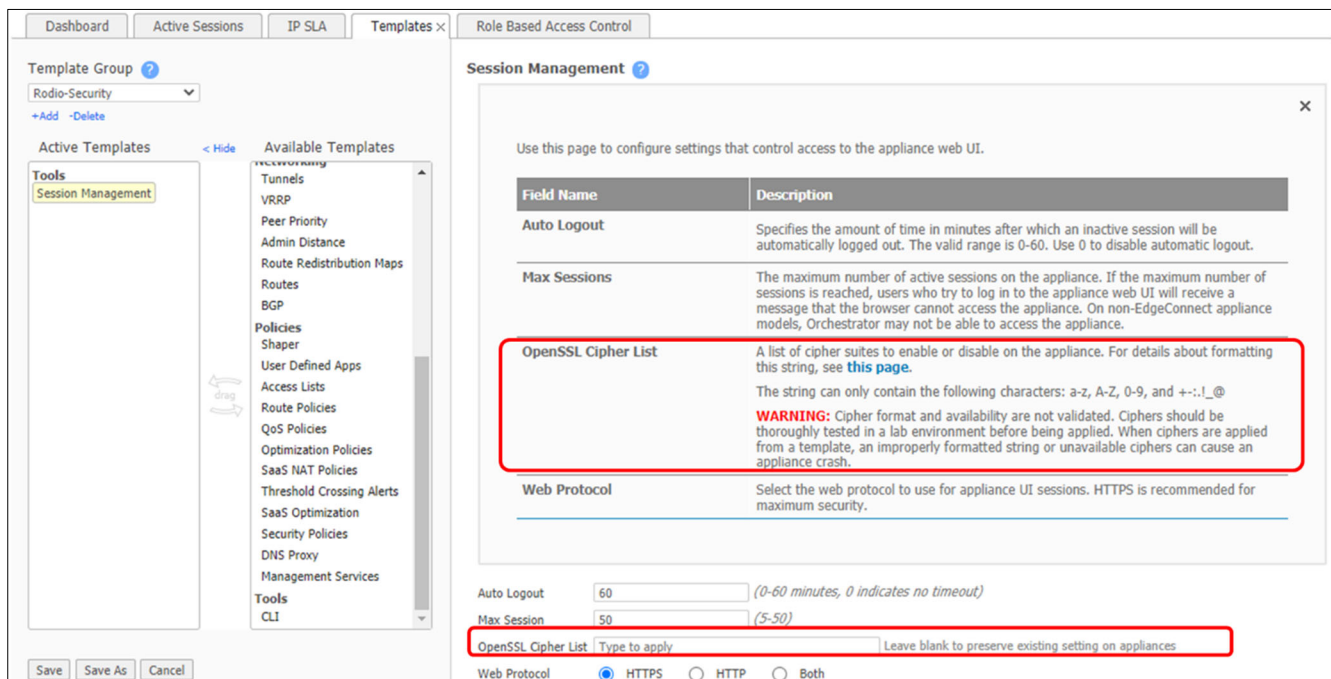


Figure 24: Session Management Template Help Window

Cipher input string syntax follows the format specified by openssl.org at <https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>.

There are four parts in the cipher name:

1. Key exchange algorithm (for example, ECDHE)
2. Authentication algorithm (for example, RSA)
3. Symmetric encryption algorithm (for example, AES-CBC mode 128 bits or AES-GCM mode 128 bits)
4. Message authentication code (MAC) algorithm (for example, SHA-256)

Examples of common ciphers ECOS uses for TLS 1.2 include:

- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256



### Adding Available Templates to the Default Template Group

For system hardening, there are a few additional non-default templates to consider. To access the complete list of available templates:

- Navigate to **Configuration > Templates & Policies > Templates**.
- Next to the Active Templates header, click **Show All**.
- The list of Available Templates opens.
- To add a template to the “Active Templates” list, simply select it in the “Available Templates list” and drag it to the “Active Templates” list on the right.

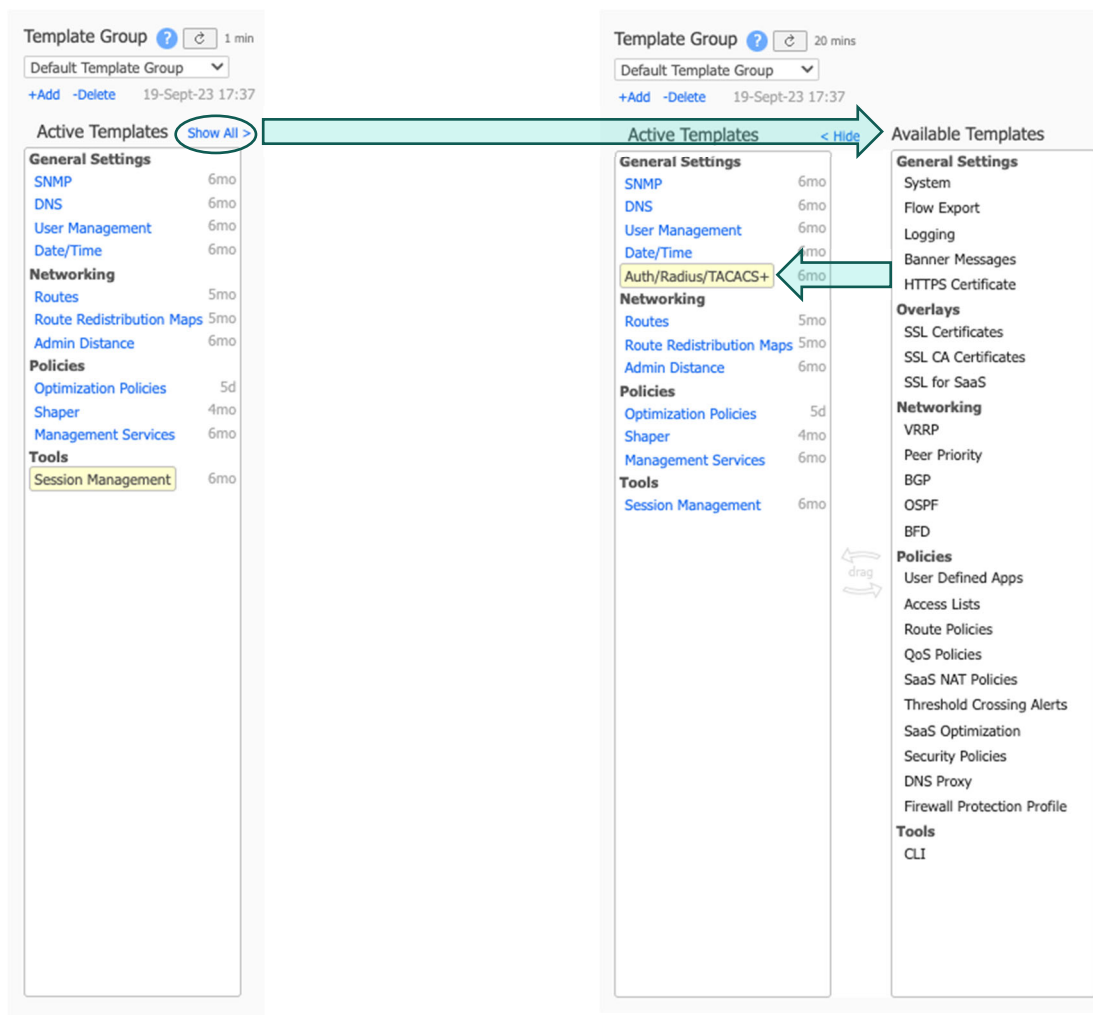


Figure 25: Active / Available Templates Dialog

The following sections focus on four of the available templates, these are not included by default and should be added for any new Orchestrator <<>>

- HTTPS Certificate
- Auth/RADIUS/TACACS+
- User Management
- CLI



## HTTPS Certificate

A certificate is needed for secure communications if the enterprise customer needs to access the appliance Web UI remotely. Generally, all provisioning should be completed through Orchestrator. Some enterprise customers want to enable Web UI access directly to the EdgeConnect gateways and therefore need to install a CA-issued certificate.

ECOS ships with a self-signed certificate issued by Aruba. The self-signed certificate should be replaced by a CA-issued certificate appropriate for the enterprise customer.

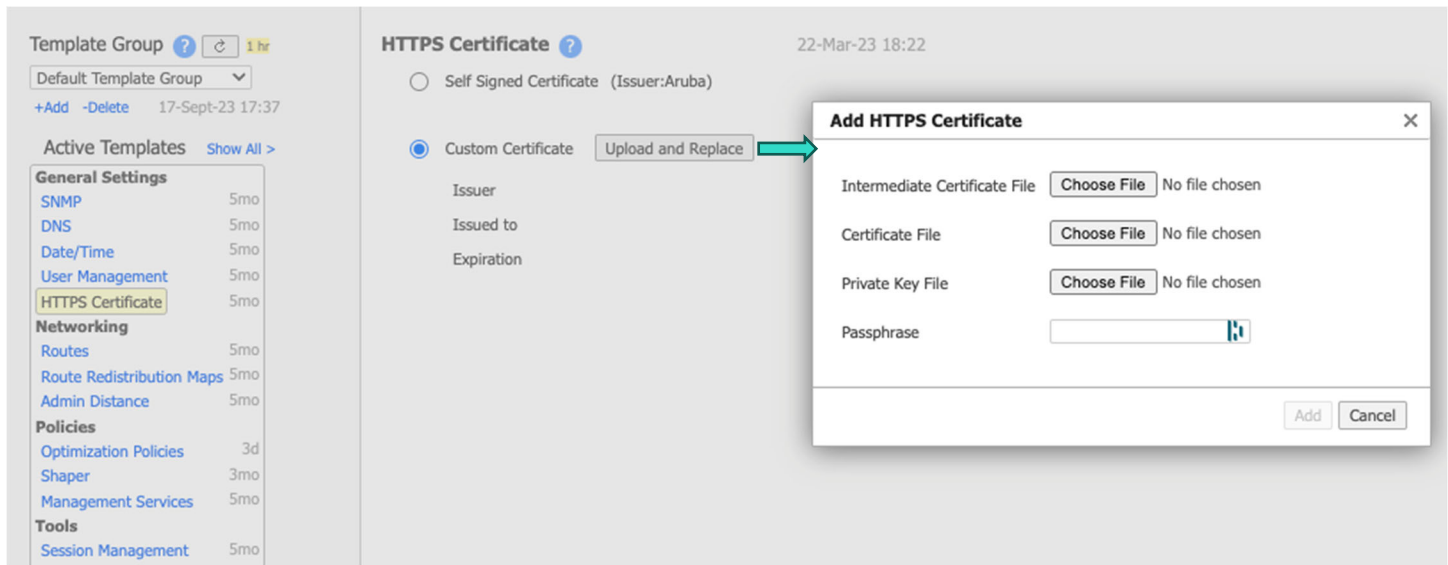


Figure 26 - HTTPS Certificate Template



## Auth/RADIUS/TACACS+

For organizations that require direct appliance access for statistics retrieval purposes, ECOS supports RADIUS and TACACS+ for authentication and basic authorization (read-only, read-write). Referring to the previous section, “[Management Services](#)” the appliance source address for RADIUS/TACACS+ traffic can be bound to the loopback interface.

**Template Group** 26 mins  
 Default Template Group  
 +Add -Delete 18-Sept-23 17:37

**Active Templates** Show All >

**General Settings**

- SNMP 6mo
- DNS 6mo
- User Management 6mo
- Date/Time 6mo
- Auth/Radius/TACACS+ 6mo

**Networking**

- Routes 5mo
- Route Redistribution Maps 5mo
- Admin Distance 6mo

**Policies**

- Optimization Policies 4d
- Shaper 3mo
- Management Services 6mo

**Tools**

- Session Management 6mo

Save Save As Cancel  
 Applies to all templates in group

**Auth/RADIUS/TACACS+** 22-Mar-23 18:22

**Authentication Order**

First: RADIUS Server  
 Second: TACACS+ Server  
 Third: Local

**Authorization Information**

Map Order: Remote First  
 Default Role: admin

**RADIUS Servers**

Order	Server IP	Auth Port	Key	Timeout	Retries	Enabled	
1	10.18.254.21	1812	****	3	1	<input checked="" type="checkbox"/>	✕
2	10.18.254.22	1812	****	3	1	<input checked="" type="checkbox"/>	✕
3	10.176.254.21	1812	****	3	1	<input checked="" type="checkbox"/>	✕

**TACACS+ Servers**

Order	Server IP	Auth Port	Auth Type	Key	Timeout	Retries	Enabled	
1	198.51.100.251	49	pap	****	3	1	<input checked="" type="checkbox"/>	✕
2	198.51.100.252	49	pap	****	3	1	<input checked="" type="checkbox"/>	✕
3	198.18.0.254	49	ascii	****	3	1	<input checked="" type="checkbox"/>	✕

Figure 27 - Auth/RADIUS/TACACS+ Template



## User Management

ECOS provides two default users: admin (enabled by default) with the capability “admin” which provides full read/write access and monitor (disabled by default) with the capability “monitor” which provides read-only access.

The password for the “admin” user must be changed from its default immediately upon ZTP if using the configuration wizard. Once ZTP is complete, the User Management template controls the local admin password.

The screenshot displays the 'User Management' configuration page. On the left, a sidebar lists various settings under 'Active Templates', with 'User Management' highlighted. The main content area is titled 'User Management' and shows a table of 'User Accounts'. The table has columns for 'User Name', 'Capability', 'Password', 'Confirm Password', and 'Enabled'. Two users are listed: 'admin' (enabled) and 'monitor' (disabled). Below the table, there are input fields for configuring the password for CLI 'Enable' privilege, including a checkbox for 'Require Password' and two password input fields.

User Name	Capability	Password	Confirm Password	Enabled
admin	admin	*****	*****	Yes
monitor	monitor	*****	*****	<input type="checkbox"/>

Figure 28: User Management Template

Local accounts on the EdgeConnect gateways should only be configured and managed via the User Management template.

When configuring user accounts for the EdgeConnect gateways, the following password requirements must be met,

1. The password length must be between 8 and 64 characters.
2. The password must contain at least one letter (uppercase or lowercase).
3. The password must contain at least one number.
4. The password must contain at least one of the 17 valid special characters (prohibited HTML characters are excluded)

Please see the section Appendix: Password Considerations for more information about password configuration and selecting a secure password.



## CLI

The CLI template offers a way to apply CLI commands through a template-based application. By default, SSH is disabled, and it is generally recommended to keep it that way. However, some organizations may need direct CLI access through SSH. In such cases, SSH can be enabled, and you can control the host key and cryptographic algorithms, as well as the auto-logout idle timer, by adding specific commands to the CLI template.

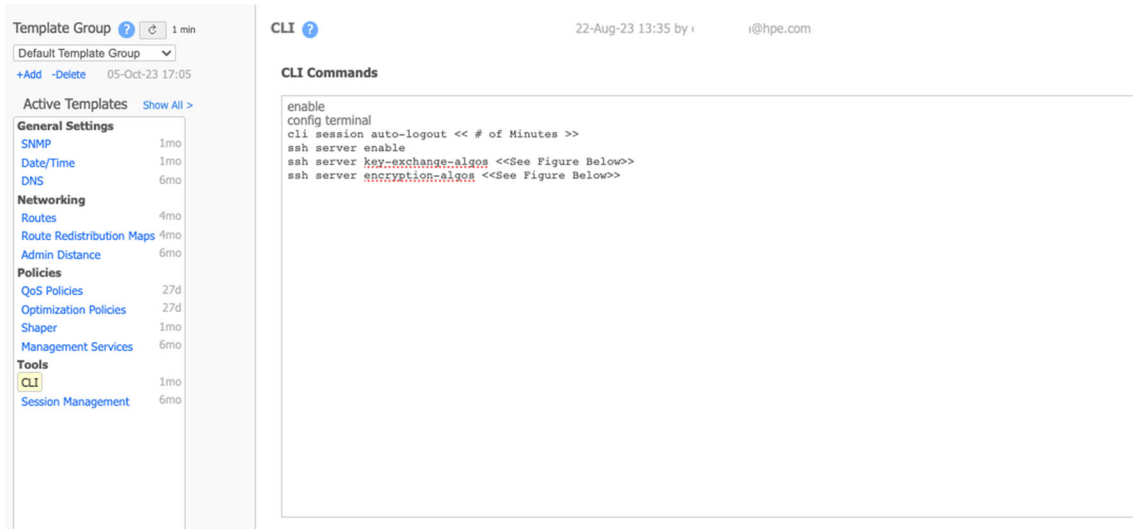


Figure 29: CLI Template

To determine the available settings for the CLI template configuration here is the output of each of the relevant commands with the configuration options,

```
ec(config) # cli session auto-logout ?
<number of minutes>
ec(config) #
```

Figure 30: CLI Session Auto Logout

<pre>ec(config) # ssh server encryption-algos ? cipher1 [cipher2 ...] aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com ec(config) #</pre>	<pre>ec(config) # ssh server key-exchange-algos ? KEX1 [KEX2 ...] 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 ec(config) #</pre>
--	---

Figure 31: EdgeConnect SSH Server CLI Settings



## Orchestrator Configuration & Templates Best Practices Summary

1. Orchestrator user authentication should be configured to use the corporate identity provider via SAML, OAuth, JWT, RADIUS, or TACACS+, local user accounts should only be used for initial provisioning and recovery purposes.
2. Add the following templates to the Default Template Group for any new Orchestrator, and configure them based on the enterprise requirements for your organization,
  - a. User Management
  - b. HTTPS Certificate
  - c. Auth/RADIUS/TACACS+
  - d. CLI
    - i. If enabling SSH access directly to the gateways, the recommended SSH settings are,  
**ssh server key-exchange-algos ecdh-sha2-nistp256**  
**ssh server encryption-algos [aes256-gcm@openssh.com](#)**
3. Configure the Auto Logout and Max Session settings under the “User Management” dialog in Orchestrator as per your organization's security policies, to enforce idle sessions to be logged out and to control the number of concurrent logins to the Orchestrator WebUI. Recommended values are 15 and 5 for auto logout and maximum session count.
4. Orchestrator users should be configured to use Role-Based Access to control the scope of accessible menus and appliances based on functional roles or other organizational delineations for access. Role assignments can be passed to the Orchestrator from your corporate identify provider. For more details on configuring remote authentication see the SD-WAN documentation page [here](#).
5. Accessing Orchestrator via API should be done via API Key, with the proper IP Allow List and API key lifecycle practices in place.
6. Orchestrator local accounts should be kept to an absolute minimum and used only for recovery actions. All local account passwords should be a minimum of 16 characters in length.
7. EdgeConnect gateway local accounts should be kept to an absolute minimum and used only for recovery actions.
8. Direct gateway access should be restricted to well-defined IP ranges and only used for statistics retrieval via the gateway API, and authentication should be configured to use RADIUS or TACACS+.
9. SD-WAN administrators should always use the Orchestrator for management access to gateways and not directly via SSH/WebUI.
10. Orchestrator WebUI access should be restricted using the IP Allow List feature to only permit well known administrative IP ranges.



# SD-WAN Fabric Data Plane

## Orchestrator Tunnel Settings

The Orchestrator Tunnel Settings menu (**Orchestrator > Orchestrator Server > Tools > Tunnels Settings**) configures the mode of EdgeConnect-to-EdgeConnect Underlay Tunnels (UTs) used in Business Intent Overlays (BIOs). Tunnel settings are configured on a per-WAN-Interface-Label basis.

HPE Aruba Networking recommends IPsec UDP tunnels, the default tunnel mode for the SD-WAN fabric. The only exception is the FIPS-Approved mode of operation, which requires IKE-based IPsec Tunnels.

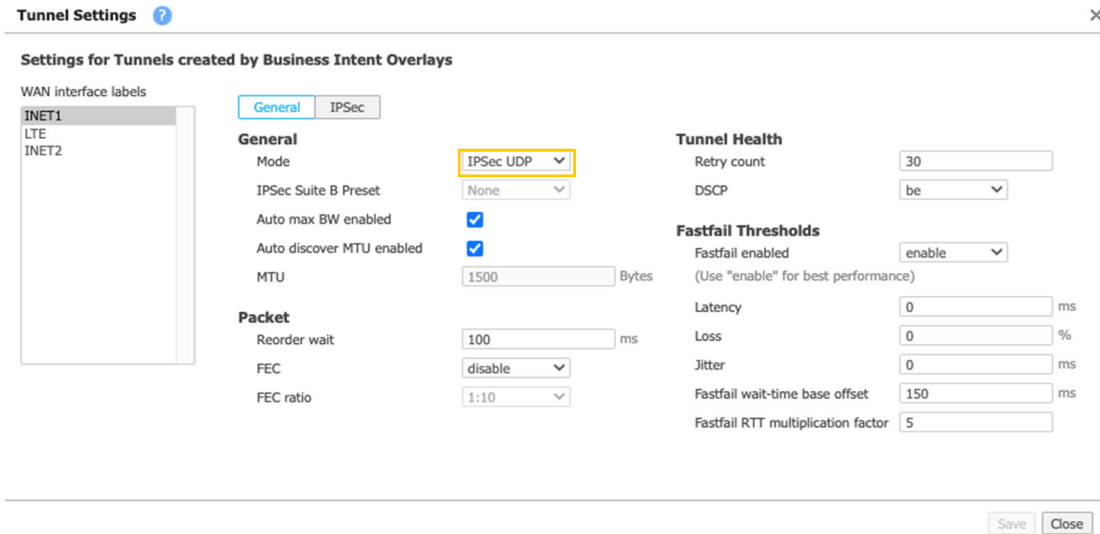


Figure 31: Label Mode Dialog

NOTE: UDP and GRE fabric tunnels are not recommended.

The recommended IPsec encryption algorithm for SD-WAN fabric tunnels (IPsec UDP or IKE Based) is **AES-GCM-256**, which natively supports encryption and authentication. This needs to be configured for each WAN label. *Figure 32* shows the IPsec configuration setting for one of the WAN labels (INET1); ensure the configuration is applied to all labels.

To modify an SD-WAN fabric in use, change one label and save it. Wait for the Orchestrator to recreate tunnels for that label with the new configuration, and repeat for each additional label in use.

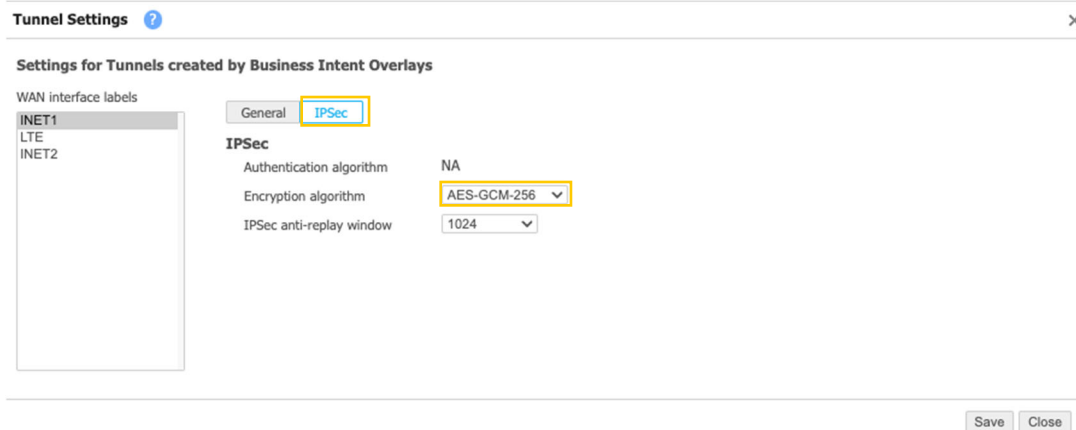


Figure 32: Recommended IPsec Encryption



## EdgeConnect to EdgeConnect IPsec UDP Tunnels

EdgeConnect gateways derive encryption keys for IPsec UDP tunnels by cryptographically combining two components:

- EdgeConnect nonce
- Orchestrator-derived ephemeral key material

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, and direction.

The orchestrator generates ephemeral key material, a time-varying “seed” that distributes the same key material to all gateways. Therefore, the key material is global to all gateways in the SD-WAN but varies by time.

---

**NOTE:** This is key material and not the encryption key itself. Orchestrator manages key material lifetime, rotation period, and appliance storage/persistence.

---

EdgeConnect gateways create and persist a nonce per underlay tunnel (UT) and per direction. Therefore, the nonce is static over the tunnel’s lifetime but varies by UT and direction. When combined, every UT and direction has globally unique, time-varying encryption keys.

Key parameters that relate to both IPsec UDP and IKE-based IPsec are shown in Figure 33.

**Schedule IPsec Key Rotation**

**SD-WAN IPsec UDP Key Material Rotation**

IPsec UDP tunnels are the default for the SD-WAN fabric, and are defined in *Orchestrator > Tunnel Settings, Mode "IPsec UDP"*. This is the key material and NOT the encryption key itself. Encryption keys used in IPsec UDP tunnels are NEVER sent on the wire. They are independently and uniquely derived per EC, tunnel, and direction. Lifetime and Rotation Period need to be configured correctly so that Key Material doesn't expire.

Enable Key Rotation  **IMPORTANT:** If enabled, Orchestrator cannot be down for more than Key Material Lifetime hours.

Persist Key Material  If enabled, key material is stored on each appliance, ensuring data plane tunnels are built quickly after an appliance reboot (no dependency on Orchestrator). If disabled, new key material from Orchestrator is required after any reboot (Orchestrator reachability is critical).

Max Activation Wait  hr New Key activation will wait until all appliances are reachable, but NOT LONGER than Max Activation Wait Time. After that time the new Key Material will be activated on all reachable appliances. In general, it is recommended to set value to half of Rotation Period.

Rotation Period   [View activation progress here](#)

Key Material Lifetime  hr Lifetime must be 3 times of the Rotation Period to ensure that the key material doesn't expire before next Rotation. Enter "0" to disable expiration.

**SD-WAN IPsec Pre-shared Key Rotation**

Regular IKE, IPsec tunnels in the SD-WAN fabric are defined in *Orchestrator > Tunnel Settings, Mode "IPsec"*. Key rotation is built-in as part of the IKE and IPsec protocols. The "Rekey/Lifetime" field under IKE and IPsec tabs indicate the configurable key rotation interval per tunnel.

Enable  **Service affecting, tunnels may go down briefly during key rotation. Should be scheduled during maintenance windows.**

Period

Figure 33: IPsec Key Rotation Parameters

For more details on each setting, see Table 2.



Table 2: Orchestrator 9.1 IPsec UDP Key Material Settings

Setting	Description
<b>Enable Key Rotation</b>	Orchestrator distributes ephemeral key material per the settings below. If enabled, Orchestrator cannot be down for more than Key Material Lifetime hours.
<b>Persist Key Material</b>	<p>If enabled, Orchestrator-distributed ephemeral key material is stored/persisted on each EdgeConnect appliance. This ensures that data plane tunnels are built quickly after an appliance reboot. In this scenario, there is no dependency on Orchestrator reachability to construct IPsec UDP tunnels after an appliance reboot.</p> <p>If disabled, after any appliance reboot, the appliance must establish a connection to the Orchestrator and obtain new key material. Therefore, Orchestrator reachability is critical for the data plane to become active.</p>
<b>Max Activation Wait</b>	New key activation waits until all gateways are reachable, but not longer than Max Activation Wait time. After that time, the new key material is activated on all reachable gateways.
<b>Rotation Period</b>	Specifies the schedule and periodicity for Orchestrator ephemeral material distribution—and therefore the derived-key rotation. Orchestrator provides a button to force a key rotation.
<b>Key Material Lifetime</b>	When specified, lifetime must be at least three times of the rotation period to ensure that the key material does not expire before the next rotation. Lifetime expiration can be disabled by entering <b>0</b> .



### EdgeConnect-to-EdgeConnect IKE-Based IPsec Tunnels

If required, EdgeConnect-to-EdgeConnect fabric tunnels can be configured to use IKE-based IPsec. This is required for customers that run in FIPS-approved mode of operation.

IKE-based IPsec tunnels in the SD-WAN fabric are defined in **Orchestrator > Orchestrator Server > Tools > Tunnels Settings**, on the IPsec tab.

---

**NOTE:** Tunnel protocol is set on a per-WAN-interface-label basis. Since IPsec UDP is the default, if a customer requires standard IPsec tunnels, this configuration must be performed on all Labels, whether pre-existing or newly created.

---

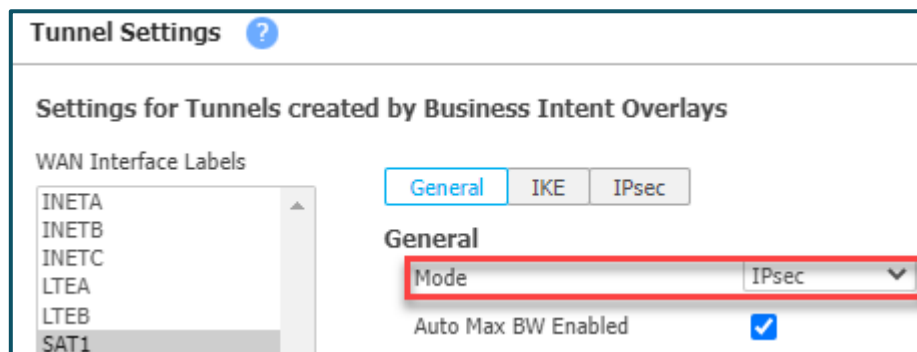


Figure 34: Label Mode - IPsec

Key rotation is built in as part of the IKE and IPsec protocols. The Rekey/Lifetime field under the IKE and IPsec tabs indicate the configurable key rotation interval per tunnel.

### EdgeConnect-to-Third-Party IKE-Based IPsec Tunnels

Tunnel configuration to third-party cloud-iaas and cloud-security services are performed per the requirements of the specific cloud-services partner. These settings are provisioned in the relevant Configuration > Cloud Services menu and are out of scope for this document.

---

**NOTE:** With some third-party integrations, Orchestrator may default to using IKEv1. The administrator must verify that the third-party service supports IKEv2, and if so ensure Orchestrator tunnels settings are IKEv2 for a given service.

---



## SD-WAN Fabric Dataplane Configuration - Best Practice Summary

1. For EdgeConnect-to-EdgeConnect Fabric tunnels (IPsec UDP or IKE Based) the recommended algorithm is **"AES-GCM-256"** as it is the most efficient and performs both authorization and encryption natively.
2. IPsec UDP (aka IKE-Less IPsec) is the recommended tunnel encryption mechanism unless FIPS compliance is required, then use IKE-based IPsec. For more information on IPsec UDP go [here](#)



## EdgeConnect Gateway Configuration

Previous sections of this document covered orchestration configuration, which applies to all gateways in the SD-WAN fabric and orchestration templates, which apply to all or a specific subset of gateways. This section will cover security aspects of site-specific provisioning.

When Orchestrator discovers an appliance, users have two options for site-specific configuration:

1. Configuration Wizard
2. Preconfiguration

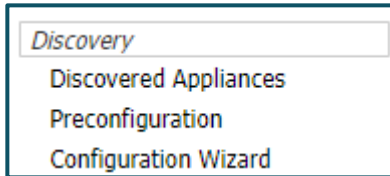


Figure 35: Configuration Wizard & Preconfiguration Menu

Configuration Wizard provides an intuitive and interactive experience to provision site-specific parameters ranging from basic appliance information to deployment configuration of interfaces and IP addresses, application of Business Intent Overlays, and template groups.

The configuration wizard is suitable for small deployments, but for larger deployments (>10 gateways) HPE recommends building Preconfiguration YAML files before appliance discovery to automate large deployments. For more information on using the Preconfiguration feature, please visit [Aruba VSG](#).



## Configuration Wizard – Admin Password

When the Configuration Wizard is first used to provision a gateway into the SD-WAN fabric, you must set the password for the “admin” account before proceeding with the additional provisioning steps. At this initial step, you can set your desired password for the account “admin”.

Appliance Wizard

Appliance Setup

1 2 3 4 5

Appliance\* edgeconnect Site Name Used to identify appliances at the same location. Tunnels will NOT be built between appliances with identical Site Names.

Group\* Group 1 Contact Name

Admin Password Contact Email customer@hpe.com

Confirm Password Serial Number\* 00-1B-8C-1F-8A-AF

Location

Address 1 2100 Moorpark Ave

Address 2

City San Jose State California

Zip Code 95128 Country US

Region No Region

IPsec UDP Port 12000

Hub Site

< Previous Next > Apply

Figure 36: Configuration Wizard – Step 1

At the completion of the Configuration Wizard, select the Default Template Group that includes the pre-configured "User Management" template for the organization's "admin" password and other local accounts needed for recovery or statistics retrieval.

Appliance Wizard

Appliance Setup

1 2 3 4 5

Add Business Intent Overlays to this Site

Overlays build and manage connections between sites, as well as define how traffic is routed and prioritized throughout the network. The Deploy Overlays tab allows you to view and manage overlays on each appliance.

RealTime

CriticalApps

BulkApps

DefaultOverlay

Select Template Groups to be applied to this Site

Templates are used to configure appliance settings including: Authentication, SSL Certificates, Threshold Crossing Alerts, DNS, SaaS Optimization and Date/Time.

Default Template Group

Admin Distance, Date/Time, DNS, Management Services, Optimization Policies, Routes, Route Redistribution Maps, Shaper, SNMP, [User Management](#), Session Management

< Previous Next > Apply

Figure 37: Configuration Wizard – Step 5

---

**NOTE:** This assumes that “Default Template Group” contains the User Management template.

---



## WAN Interface Firewall

WAN interfaces that are internet or LTE-facing must always have the FW Mode set to Harden, Stateful, or Stateful+SNAT. *Allow All* should only be enabled for trusted private networks such as MPLS, where inbound traffic from the underlay may be required for transitional purposes.

The administrator must determine if a transport network is trustworthy before applying the Allow All setting.

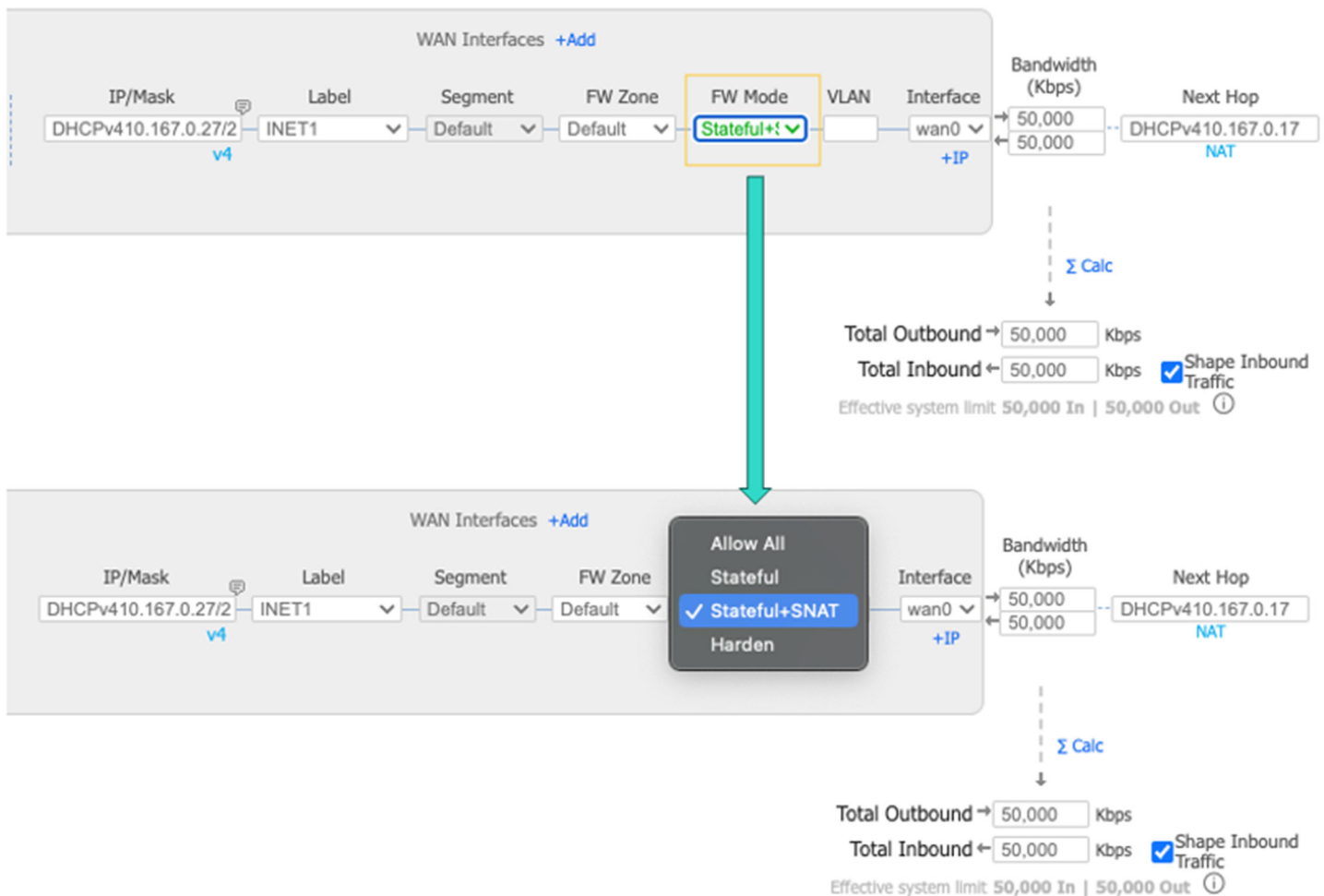


Figure 38: WAN Interface Firewall Settings

---

NOTE: Do not connect interfaces configured as LAN to the internet. They are on the trust-side of the network.

---

Note, there are non-cryptographic ports that ECOS will have open; the user should lock down if not using.

- NTP server
- BGP TCP 179 (if the protocol is enabled)



## Management Interfaces (MGMT0 / MGMT1)

Some EdgeConnect hardware and virtual gateways include dedicated interfaces called mgmt0 and mgmt1. These interfaces provide direct access to the EdgeConnect gateway management plane and are intended for use during initial ZTP operations and/or for fully out-of-band management network connectivity.

Use of these interfaces outside of initial provisioning operations, RMA, or other recovery scenarios is not recommended since these interfaces act as an additional point of entry where security policy and control must be handled outside the EdgeConnect SD-WAN platform. For environments where Segmentation is enabled, the mgmt0 and mgmt1 interfaces are part of the "Default" segment and cannot be moved to a different segment.

With the introduction of loopback interfaces the use of mgmt0/1 interfaces in a production network is no longer necessary since the in-band loopback interface can leverage the redundant SD-WAN data plane for providing reachability of the management plane functions of the gateway.

---

**NOTE:** Do not connect mgmt0/1 interfaces to the internet. They are on the trust side of the network.

---



## EdgeConnect Gateway Configuration - Best Practice Summary

1. It is recommended that WAN interfaces operate in Stateful, Stateful+SNAT, or Hardened mode, as opposed to the Allow All mode. The latter should only be used in specific cases, such as migration to SD-WAN from MPLS, and requires the administrator to be fully aware of its security implications.
2. It is advisable to avoid accessing gateways directly via WebUI or SSH, unless necessary for statistics retrieval purposes. In such sessions, authentication should be configured using RADIUS/TACACS+ as the primary method, with only local authentication as a fallback option.
3. Managing local "admin" account passwords through the "User Management" template is recommended. This allows for centralized control of credentials and ensures password consistency and compliance across the organization. All local account passwords should be a minimum of 16 characters in length.
4. It is recommended to avoid using mgmt0/1 after Day 1 provisioning unless there is a true out-of-band network with proper Layer 2 and above security controls to restrict access.
5. All configuration settings for EdgeConnect gateways should be managed via templates and pre-configuration, local configurations on the gateways is highly discouraged.



## Appendix: Password Considerations

Within the EdgeConnect SD-WAN platform, there are two distinct places where local user accounts are configured:

1. User Management – (Controls login credentials for Orchestrator)
  - a. **Orchestrator > Users & Authentication > User Management**
2. Template Groups – User Management (Controls login credentials for EdgeConnect gateways)
  - a. **Configuration > Templates & Policies > Templates > Default Template Group > Active Templates > User Management**

When configuring user accounts for the Orchestrator via the user management menu, the following password requirements must be met,

- The password length must be between 8 and 64 characters.
- The password must contain at least one letter (uppercase or lowercase).
- The password must contain at least one number.
- The password must contain at least one special character.

When configuring user accounts for the EdgeConnect gateways, via the user management template, the following password requirements must be met,

- The password length must be between 8 and 64 characters.
- The password must contain at least one letter (uppercase or lowercase).
- The password must contain at least one number.
- The password must contain at least one of the 17 valid special characters (prohibited HTML characters are excluded)<sup>1</sup>

### Password Combinations without Permutations:

When estimating the total number of password combinations without considering permutations, we look at the possible ways to create a password by selecting characters from a given character set, where the order of characters doesn't matter.

The total number of password permutations with eight characters without multiset permutation is,

$$26 * 26 * 10 * 17 * 79^4 = 4,476,143,308,520$$

### Password Combinations with Permutations:

Considering the permutation of multisets is as follows,

$$\frac{8!}{1! * 1! * 1! * 4!} = 1680$$

When assessing password strength with permutations considered, we are interested in the number of possible character combinations and the potential variations arising from different orders of these characters. In contrast to the previous summary, permutations assume that the order of characters matters, and that each arrangement is unique.



For instance, an 8-character password chosen from a character set of 79 unique symbols has approximately 7.52 quadrillion (7,519,920,000,000,000) possible permutations. This calculation accounts for all possible ways of arranging the characters within the password, assuming each arrangement is distinct. However, while permutations give a more significant number, they may overestimate password strength because not all permutations are practically relevant.

$$26 * 26 * 10 * 17 * 8! = 7,519,920,000,000,000$$

## Password Entropy

Entropy calculations for password strength typically use combinations rather than permutations because permutations imply that the order of characters matters. In password strength, the order of characters doesn't necessarily add security; it's the number of possible combinations that matter.

Combinations consider the number of ways you can choose a set of characters from the character set without regard to the order in which they appear. This is more relevant when estimating the strength of a password because it accounts for situations where the password might be "shuffled" or rearranged.

Permutations, on the other hand, consider the number of ways you can arrange the characters, which might overestimate the strength of a password since it assumes that all possible orders are unique and valid passwords.

In most cases, when assessing password strength, you want to calculate the entropy based on combinations, not permutations, as it provides a more accurate estimate of how difficult it is to guess or crack the password.

To measure password entropy, we use the following method,

- L = Password Length; Number of symbols in the password
- S = Size of the pool of unique possible symbols (character set)
- Number of Possible Combinations (if all character positions have the same number of possibilities) =  $S^L$
- Entropy =  $\log_2(\text{Number of Possible Combinations})$
- 

For EdgeConnect, the Entropy of a minimum 8-character password is:

$$\text{Entropy} = \log_2(4,476,143,308,520) = 40 \text{ bits of entropy.}$$

---

**NOTE:** HPE Aruba Networking recommends a *minimum* entropy of 96 bits, requiring passwords with at least 16 characters.

---

**END OF DOCUMENT**

