aruba
a Hewlett Packard Enterprise company

Aruba Orchestrator for Service Providers

USER GUIDE

V1.0

DECEMBER 2, 2022

TABLE OF CONTENTS

ARUBA ORCHESTRATOR^{SP} FUNDAMENTALS

The Aruba Orchestrator for Service Providers (SP) enables providers to offer carrier-grade managed SD-WAN network infrastructure services to their customers. This secure, managed cloud-native infrastructure significantly benefits service providers and enterprise customers. Aruba Orchestrator^{SP} is a secure, cloud-hosted, multi-tenant management Software-as-a-Service platform that enables service providers to manage their enterprise end-customer tenants centrally. Each tenant has its Orchestrator that manages its SD-WAN fabric, ensuring complete isolation and independence between tenants. The Orchestrator^{SP} cloud-native architecture provides a secure, scalable, multi-tenant infrastructure as a service that scales on demand with reliable, secure infrastructure.

This document explains how Aruba Orchestrator^{SP} enables service providers to deliver these benefits to their customers.

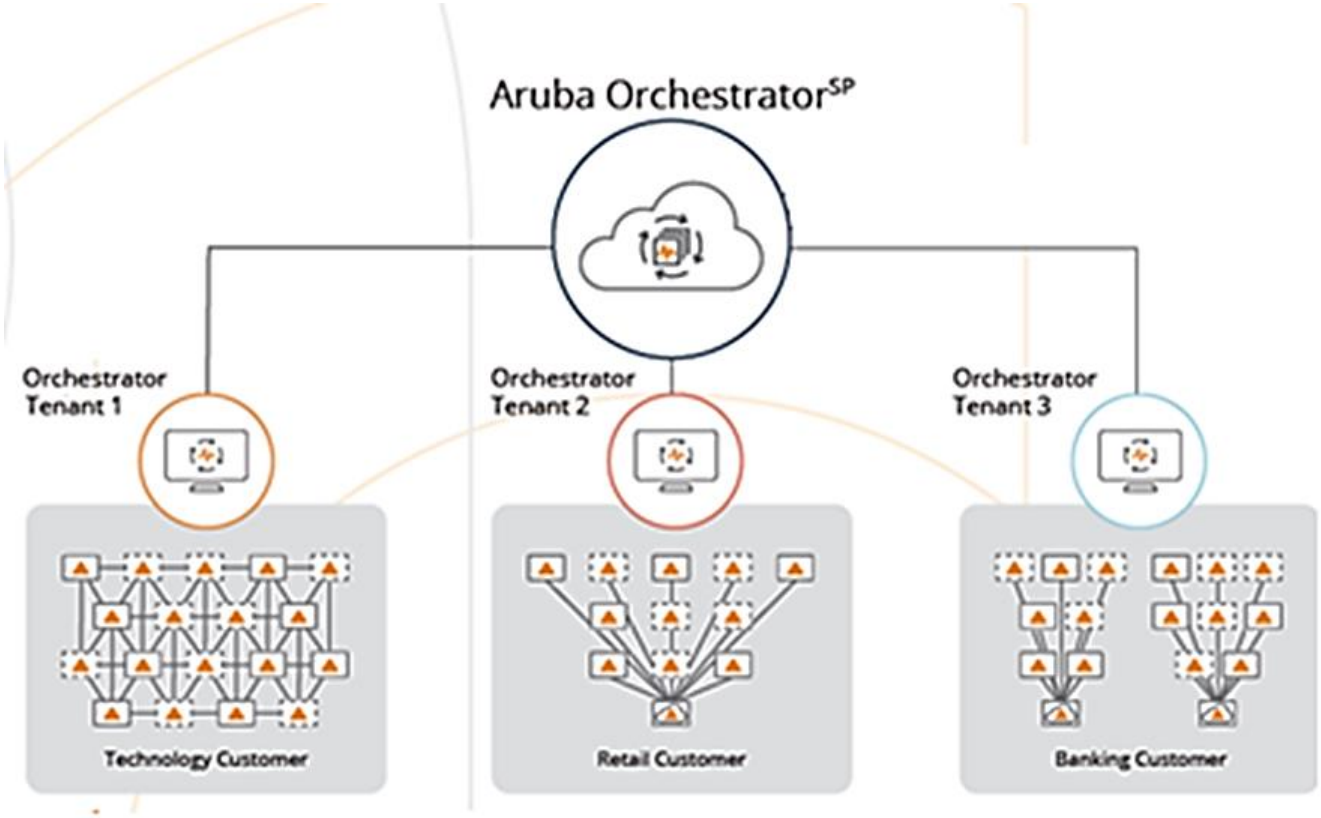


Figure 1: Orchestrator^{SP} Overview

Orchestrator^{SP} provides operational efficiency by minimizing order-to-deployment touch points with an intuitive GUI and centralized SD-WAN configuration. It provides granular visibility into customer networks enabling rapid response for troubleshooting and support issue resolution.

Key Features

- Single Screen Administration: Automates the implementation of network-wide business intent overlay policies for each enterprise customer's applications, eliminating manual device configuration at each branch location and enabling secure global administration of deployment assets (appliances and licenses).

- Multi-tenant Management and Administration: Scales to support SD-WAN deployments for hundreds to thousands of individual enterprise customers.
- Live View: Monitors real-time throughput, loss, latency, and jitter across SD-WAN overlays and the underlying transport services to proactively identify potential performance impacts.
- Centralized Alarm View Across Multiple Tenants: Enables alarm monitoring with an aggregated view of alarms for all managed SD-WAN tenants; a single click provides alarm details for a specific tenant SD-WAN.
- Real-time Enterprise Customer Monitoring and Historical Reporting: In combination with tenant Orchestrators, provides granular visibility into application, location, and network statistics, including continuous performance monitoring of loss, latency, and packet ordering for each enterprise customer's network paths.
- Integration with Business Support Systems (BSS) for service fulfillment and assurance and Operations Support Systems (OSS) for billing, revenue management, and customer management.
- Tenant-level Orchestrator Blueprint templates allow service providers to align Orchestrator settings to service provider service definitions.
- Asset management of Aruba hardware allows service providers to manage one pool of assets and distribute them to their tenants.
- Single Sign-On (SSO) with:
    - Role-Based Access Control (RBAC) at the Orchestrator^{SP} level and the tenant Orchestrator level.
    - Tenant Access Control–allows access to all or a specific list of tenants.
    - Tenant-level Gateway Access Groups (AAG).
- Identity provider integration with OAuth.

Key Benefits

- Easy and rapid onboarding of any number of new customers.
- Secure, unlimited scalability and multi-tenancy enable lowering the cost of new deployments.
- Global orchestration across each customer's SD-WAN enables faster service creation.
- Centralized visibility and management of SD-WAN assets yield higher customer satisfaction.
- Flexible licensing and billing for pay-per-usage and bandwidth tiers.

Orchestrator^{SP} allows service providers to have a single console to access all underlying Aruba Orchestrator tenant instances.

Consumption Model

The Aruba SD-WAN consumption models are designed for the needs of different types of customers.

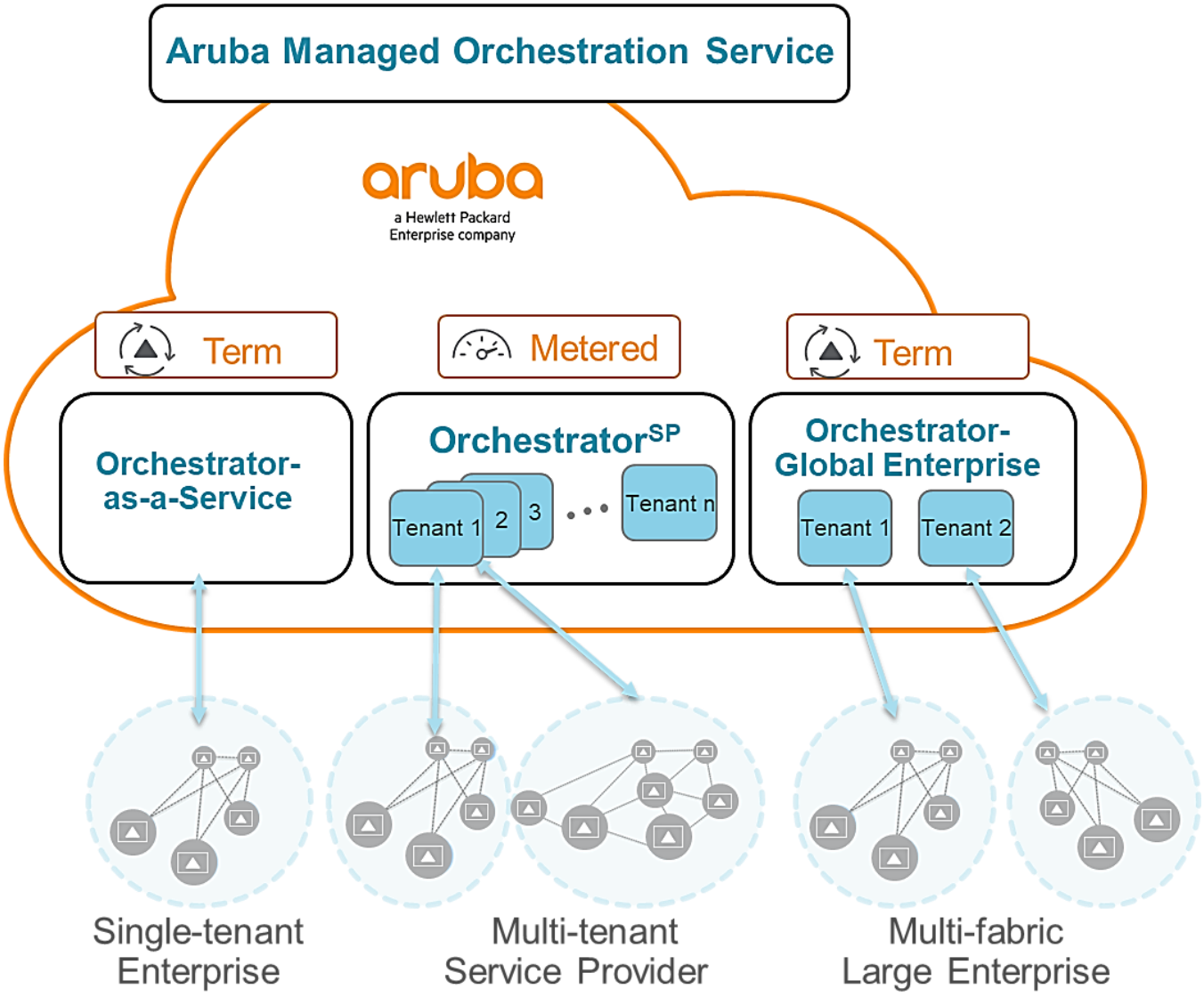


Figure 2: Consumption Models

The following consumption models are available:

- Orchestrator-as-a-Service single-tenant SaaS.
- Orchestrator^{SP} multi-tenant.
- Global Enterprise multi-tenant.

Orchestrator^{SP} supports cloud-hosted, Orchestrator-as-a-Service (default), and self-hosted Orchestrator tenants. Orchestrator^{SP} supports scalable operations of multi-tenant SD-WANs in service provider networks. This ranges from onboarding new tenants and turning up new sites to ongoing lifecycle management of the SD-WAN service.

Where Orchestrator^{SP} Fits in the Aruba SD-WAN Platform

Aruba Orchestrator^{SP} provides automated orchestration of tenant SD-WAN infrastructure. The managed orchestration service solution comprises a mix of the following:

- SD-WAN Edge Connect appliance (hardware or virtualized).
- Scalable multi-tenant OrchestratorSP that provides intelligent, logically centralized management capabilities and control policies for each tenant's SD-WAN deployments.
- Open REST APIs accessible for flow-through automation of all fault, configuration, performance, and security management functionality.
- An eco-system of partners that help bring pre-validated multi-vendor Network Function Virtualization (NFV) orchestration solutions that help ease service provider migration to multi-vendor service and network orchestration.

The Aruba SD-WAN platform includes the following major components: the Cloud Portal for licensing administration and activation, tenant Orchestrators for authentication of, access to, and management of SD-WAN assets, and EdgeConnect appliances (virtual and physical).

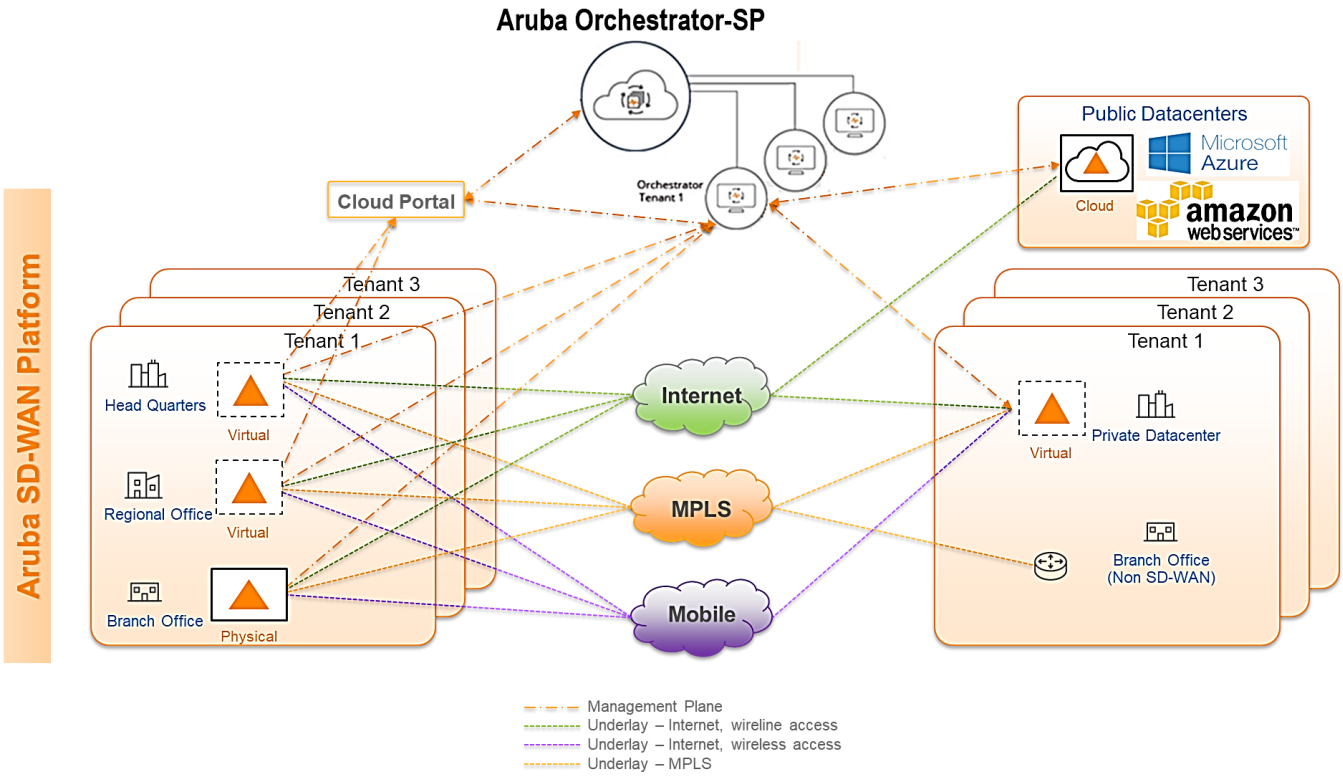


Figure 3: Where Orchestrator^{SP} fits in the Aruba SD-WAN Platform

Orchestrator^{SP} employs a scalable architecture that provides an administrative layer above multiple independent Orchestrator instances, enabling rapid instantiation of new tenant-specific domain Orchestrators and their corresponding SD-WAN appliances.

- **Orchestrator^{SP}**: the Aruba multi-tenant SD-WAN orchestration system enables service providers to create, manage, and monitor tenant SD-WAN deployments. Orchestrator-SP employs a scale-out architecture and dynamically instantiates new private and secured Orchestrator instances per tenant while providing administrative functionality across multiple tenants and license management in conjunction with the cloud portal.
- **Aruba SD-WAN Platform:** The Aruba EdgeConnect Enterprise SD-WAN platform includes various constructs that enable enterprises to create multiple application-specific virtual WAN overlays. Each Business Intent Overlay (BIO) specifies priority and quality of service requirements for application groups based on business requirements or intent. These policy definitions automate secure EdgeConnect Enterprise traffic steering on an end-to-end basis across all underlying WAN transport services, including MPLS, broadband internet, and 4G/LTE. Each BIO has its link bonding policy specify which underlay transports the BIO uses, the service level, path conditioning, and virtual topology.
    - **Orchestrator**: the Aruba SD-WAN Orchestrator is an integrated management system and controller that provides comprehensive visibility and control over SD-WAN overlays and policies that securely and intelligently manage endpoint traffic across the LAN and WAN as well as the supporting underlay resources.
    - **EdgeConnect**: Aruba EdgeConnect is the family of SD-WAN physical, virtual, and cloud appliances that can be deployed at customer sites and data centers. EdgeConnect implements SD-WAN, LAN, and WAN data plane functions and control policies, as dictated by Orchestrator.

Aruba Cloud Portal Automates Product Activation

The Cloud Portal registers EdgeConnect appliances, licenses, and subscriptions. When you purchase one of these products, an account name and instructions to obtain your account key are sent to you. You use these to register your products.

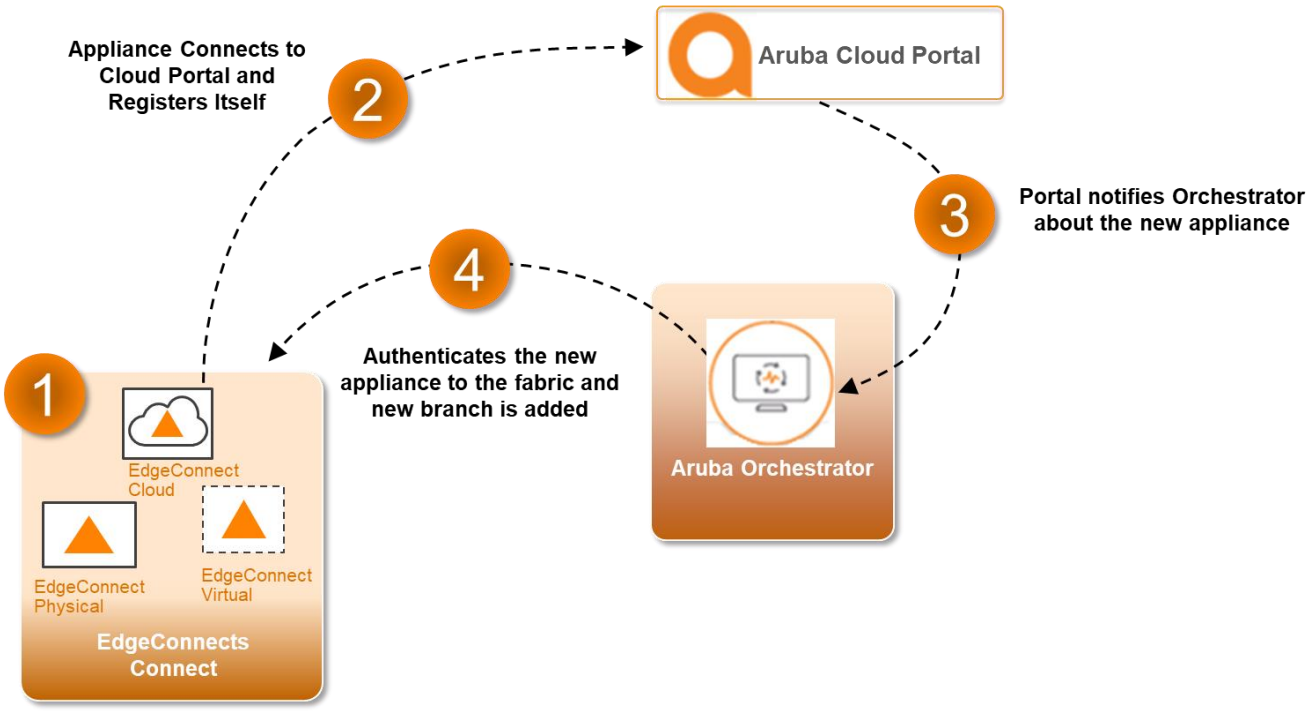


Figure 4: Zero Touch Deployment

The Cloud Portal populates the Contact field from information included in your purchase order. Using these services requires that your appliances access the Cloud Portal via the internet.

Multi-Tenant Management Model

Aruba Orchestrator^{SP} enables centralized management of multiple tenant Aruba Orchestrator instances. Multi-tenant SD-WAN service offerings need to support web-scale elasticity and support a consistent, repeatable operational model, whether there are two or 1000+ tenants, with as little manual intervention as possible.

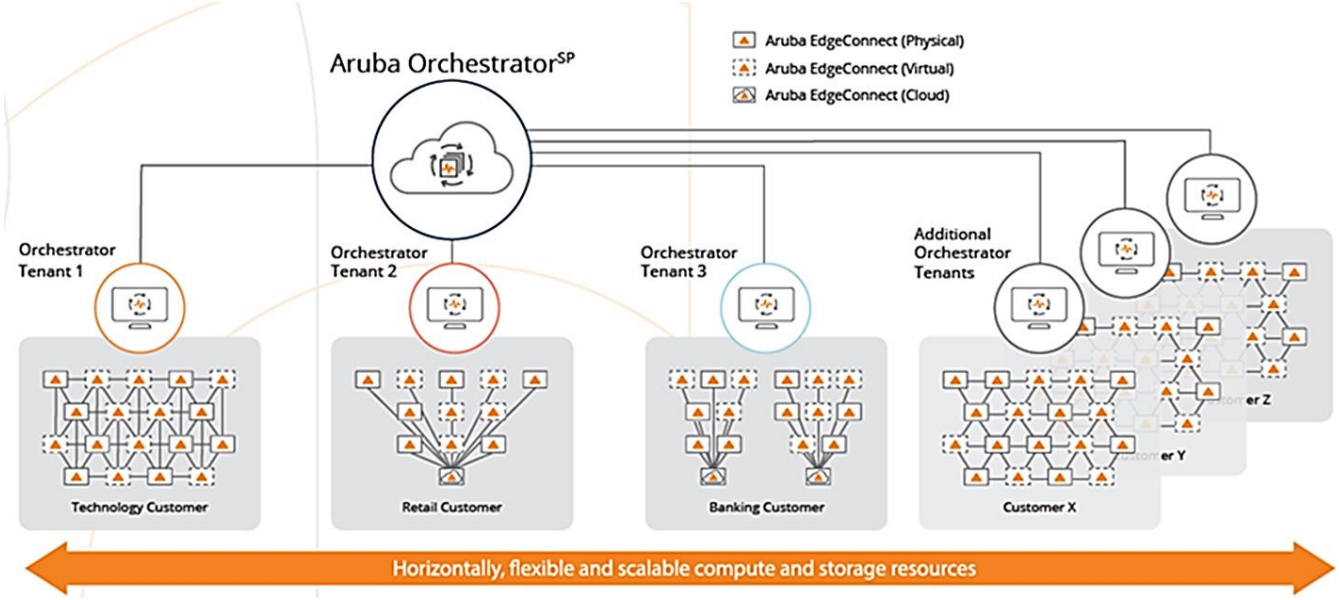


Figure 5: Orchestrator^{SP} Manages Multiple Tenant Orchestration

Each tenant SD-WAN fabric can be specified in the following sizes:

- **Small:** up to 50 node instances
- **Medium:** up to 200 node instances
- **Large:** up to 1,000 approximately node instances
- **Extra-large:** up to about 2,000 node instances
- **Extra-extra-large:** up to about 3,000 node instances.

Carrier-grade multi-tenant infrastructure that uses a cloud-centric, horizontal scale-out approach enables service providers to scale their deployments dynamically. Web-scale virtualization and cloud computing allow a scale-out approach to multi-tenancy. Orchestrator^{SP} automation enables service providers to scale out elastically. Tenant instances can be dynamically instantiated (or decommissioned) in real time on an as-needed basis.

From a service and device configuration perspective, centralized domain-wide configuration management is one of the critical features of the cloud-hosted Orchestrator^{SP} solution. Orchestrator^{SP} automatically monitors and allocates cloud resources as needed. Cloud-hosted SD-WAN deployments can grow without any human intervention. The architecture also allows each tenant Orchestrator to be customized and upgraded based on the customer's needs, independent of other tenants' deployments.

Each tenant Orchestrator provides domain-wide configuration and provisioning capabilities across all remote customer premise equipment within that tenant's domain. A secure private communication session is auto-initiated once an EdgeConnect appliance is deployed and brought into service. The ability of the tenant Orchestrator to effect changes across multiple devices includes changes to appliance configuration parameters, policies, software upgrades, and general lifecycle management functions. All operations, administration, maintenance, and provisioning functions associated with the tenant domain are accessible via a set of northbound RESTful APIs. These APIs enable automating processes via operations support systems, business support systems, software-defined networking, network function virtualization, network infrastructure, or by scripts. The registration and onboarding process of new customers and new appliances for hardware and virtualized solutions enables touchless onboarding of new customers and devices.

For networks where a head-end hub is desired to connect a customer to other Virtual Network Functions (VNF) or services within the service provider's point of presence or data center (e.g., firewalls, unified threat management, voice gateways, etc.) or to provide a centralized point for aggregating internet access, Aruba leverages a light-weight VM-hosted virtualized appliance that can be instantiated at the aggregation site on any available compute resource, using any of the significant hypervisors – ESXi, KVM, HyperV, XenServer. This provides isolated, tenant-specific gateway functionality that can be individually maintained, scaled and upgraded independently from other instances. From a management perspective, these virtualized instances are treated like other sites in the customer domain, providing a site where traffic can be steered to service provider-hosted services or functions and accessed via the Orchestrator^{SP} solution and open REST APIs for performing FCPS management functions. The virtualized EdgeConnect VM image can also be customized to create a single 'golden' image, which can be used for automated, touchless instantiation of new sites. To facilitate automation of the compute environment hosting the virtualized appliance, scripting and OpenStack can be leveraged for service providers who have already deployed such technologies.

Scalable Deployment

When creating a tenant, a service provider deploys pre-configured settings in a blueprint. The blueprint pre-configuration sets up the tenant orchestrator, not the SD-WAN EdgeConnect settings.

The blueprint is an action that is assigned to the tenant when you create the tenant in Orchestrator^{SP}. With a scale-out approach, blueprints automate the deployment of tenant instances by providing basic configuration automation for deploying multiple tenant instances.

The granularity afforded by the multi-instance scale-out approach benefits maintenance, migration, and upgradeability. This approach also ensures that maintenance-related operations can be done without impacting other tenants.

Upgrades, Version Control, Backup, And Restore

The horizontal scale-out approach to multi-tenancy leverages elastic cloud infrastructure and can thus quickly adopt similar principles on a per-tenant basis. For example, the instantiation of new tenants is not bound to a particular host. The per-instance modularity of horizontal scale-out architecture means complete flexibility and mobility of the tenant's instance to reside on any available compute/storage resources in the data center or cloud based on the tenant's specific needs or service provider resource availability. While individual tenant instances may exist in a distributed fashion in the data center, the integral automation framework associated with the multi-tenant solution provides all the administration and management capabilities that service providers need to deliver carrier-grade per-tenant SD-WAN infrastructure.

With the velocity at which new capabilities are being introduced in SD-WAN, service providers must know how upgrades are rolled out into the network. By nature of the multi-tenant site's aggregation role, particular care needs to be taken when upgrading such sites. Each tenant's instance is an independent entity that is individually upgradeable. Each tenant instance can

be upgraded without impact on any other tenant. Upgrades can be scheduled based on the tenant's specific needs, with each tenant running on the optimal release for their applications and business needs. Any failure of a tenant's instance is isolated, resulting in an outage for that single tenant only, and can be dealt with individually without any impact on any other tenant.

Backup and restoration operations for the SD-WAN infrastructure generally involve database operations. Operations involving backups, rollbacks, or recoveries are performed per tenant without impacting other tenants, as each instance maintains a private database and its own set of backup images.

Licensing Considerations

A service provider tenant deploys an SD-WAN design, which is done after Orchestrator^{SP} creates a tenant instance. An SD-WAN design is implemented in the tenant that Orchestrator^{SP} creates. While Orchestrator^{SP} does not manage SD-WAN configurations, it is helpful to highlight some essential elements of an Aruba SD-WAN deployment. The topics below briefly highlight SD-WAN considerations. Refer to Aruba product documentation and training for full explanations of how to use the Aruba SD-WAN platform technologies.

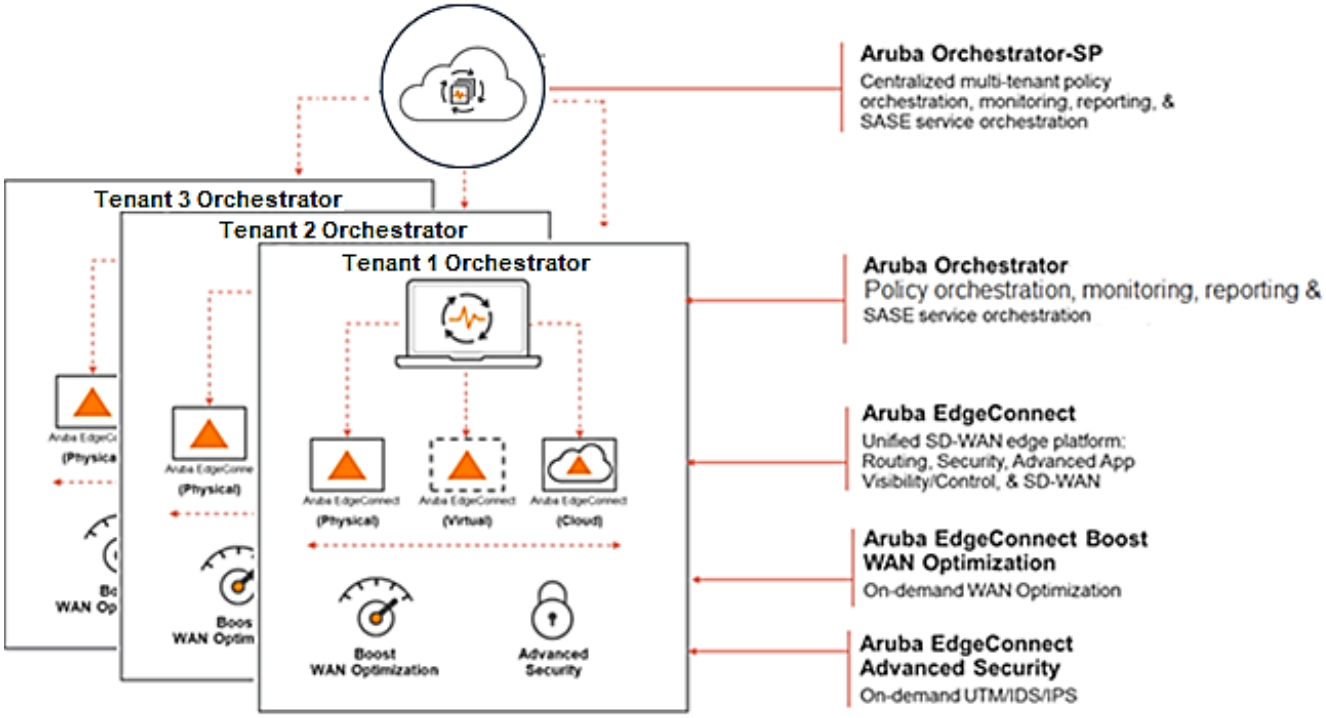


Figure 6: Aruba EdgeConnect Tenant Main Components

Aruba EdgeConnect Enterprise SD-WAN subscriptions include all SD-WAN features with two optional subscriptions:

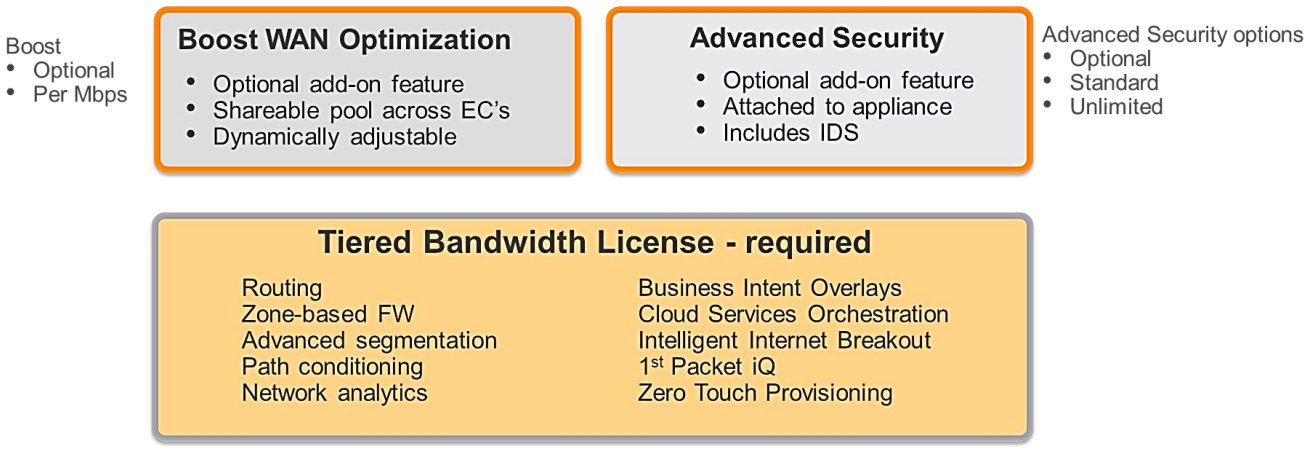


Figure 7 SD-WAN Licensing Overview

- **Optional Boost WAN Optimization Licenses** improve latency-sensitive applications' performance where large amounts of data must be transferred across the WAN. Boost can be provisioned after the initial SD-WAN roll-out. Boost includes Application Acceleration (Latency mitigation) and Data reduction (compression and deduplication).
- **Optional Advanced Security Licenses** include the widely deployed open-source Suricata IDS/IPS platform with signature feeds from Proofpoint. Aruba rule sets are regularly updated & validated to protect against an evolving threat landscape. Automated update service ensures SD-WAN has the latest signatures fully orchestrated via Orchestrator to all locations.

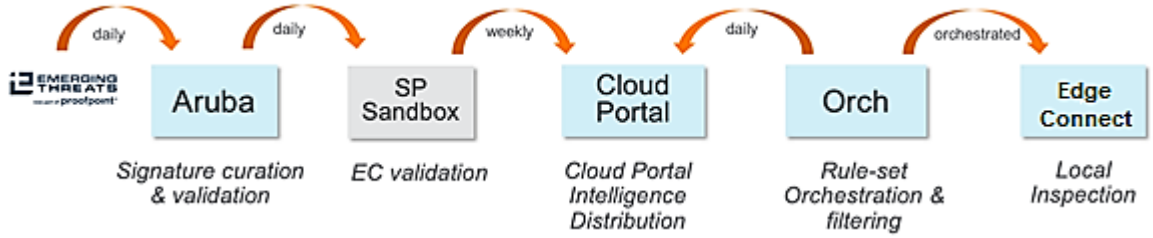


Figure 8: IDS/IPS Platform

Security Considerations

Both service providers and their clients have a keen interest in security considerations. Secure access service edge (SASE) is a cloud-based enterprise security framework designed to address the network and security challenges caused by ongoing digital business transformation. The move to the cloud, coupled with an increasingly mobile workforce that places users, devices, applications, and data outside the enterprise network, creates an "access pattern inversion."

Introduced by Gartner, the SASE model responds to this inversion, delivering networking and network security controls at the edge—as close to users as possible.

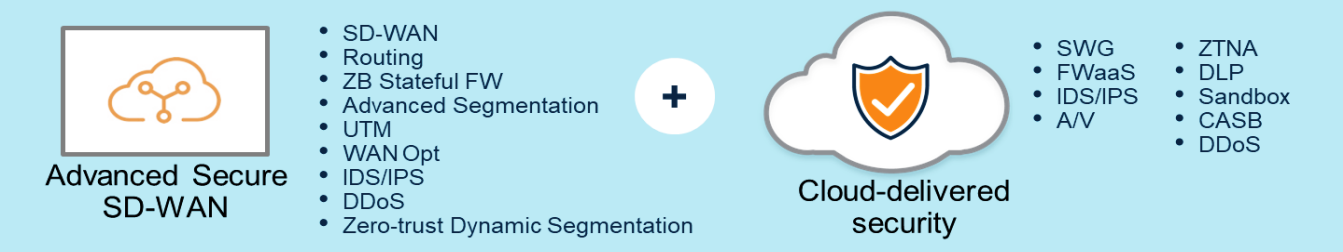


Figure 9: SASE

Orchestrator^{SP} Is a secure SaaS platform. Because the Orchestrator^{SP} service is hosted in AWS, it includes all the robust AWS security infrastructure. The following list highlights key AWS Cloud and Aruba SD-WAN security capabilities and standards compliance:

- AWS Cloud Compliance - OrchestratorSP is built on the AWS infrastructure and complies with several security and data protection cloud certifications.
- Hosted in Virtual Private Cloud (VPC) with secured internet access.
- Restricted access from specific NOC subnets.
- Multi-Factor authentication for user login.
- HTTPS-only user access and HTTPS-only connectivity from EdgeConnect appliances.
- Segregation of customer databases.
- Role-based user access with read-only, read/write permissions to all or a subset of customer accounts.
- Aruba ICSA Labs Secure SD-WAN Certification means SD-WAN Edge devices replace network security devices while providing the security protections like a firewall.

These cloud-delivered security services, complemented by the application and context-aware, business-driven Aruba EdgeConnect Enterprise SD-WAN Platform, provides a robust, secure access services edge (SASE) architecture.

USER MANAGEMENT

Orchestrator^{SP} is a virtual machine that provides network management functions for administering users and appliances in your tenant SD-WAN. Orchestrator^{SP} provides flexible user management via a modern, intuitive web-based management console.

Orchestrator[SP] Management Console

The Orchestrator[SP] management console lets you perform tenant, administration, and support tasks. A new instance of Orchestrator[SP] is provisioned for each service provider.

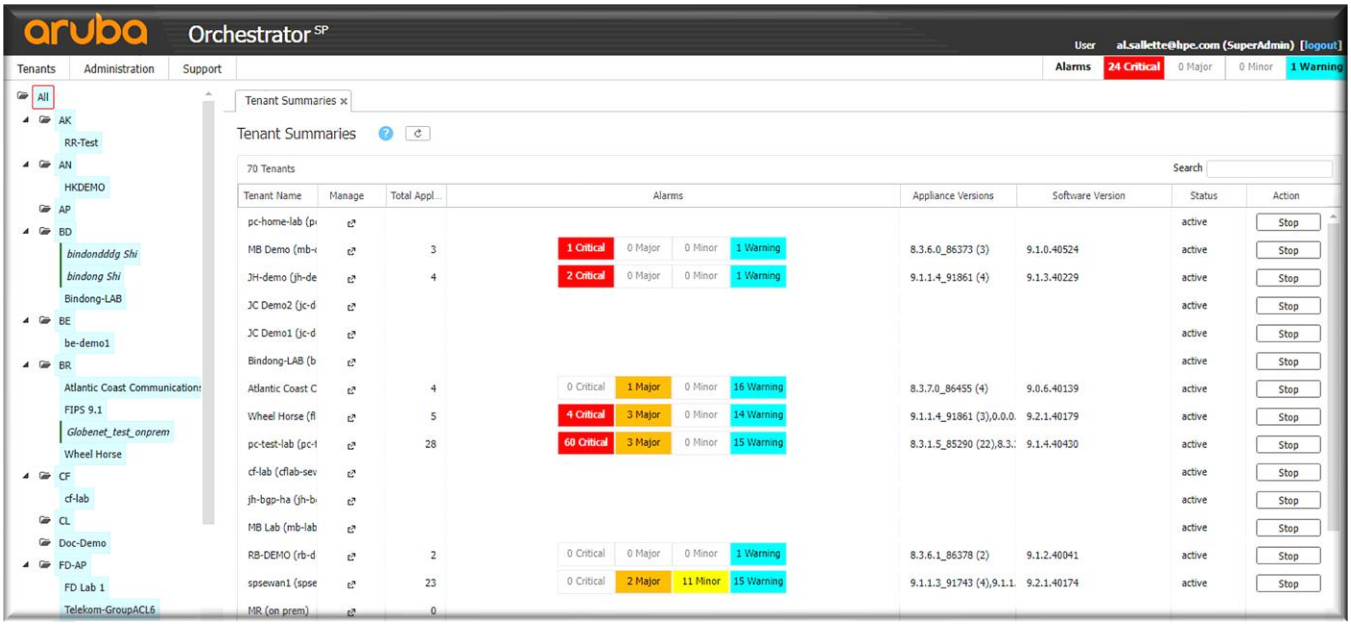


Figure 10: Orchestrator[SP] Management Console

NOTE: Google Chrome is the preferred browser to use with the Orchestrator[SP] management console.

Service Providers access Orchestrator[SP] via a web browser. Browser communication with Orchestrator[SP] is encrypted via HTTPS. Access to Orchestrator[SP] can be secured with 2-factor authentication.

- Unique username and password.
- One-time authentication code.
- At login, users can manage multiple customer accounts.
- User access can be restricted to specific customer accounts.
- User access privileges can also be restricted to read-write or read-only.

Service provider customers do not get access to Orchestrator[SP]. Service providers can allow their customers access to individual Orchestrator instances.

Customer user authentication is managed independently via the customer's Orchestrator with 2-factor authentication—username and password plus a one-time authentication code. Customer user access privileges can be restricted to read-write or read-only.

Role-Based Access Control

On a per-user basis, you can assign roles that specify access levels for a user, control the menu options available in the Orchestrator[SP] or Orchestrator UI, and grant or deny access to appliance groups.

The main steps for configuring user access are listed below:

1. Create user accounts that use local or remote authentication.
2. Create RBAC roles.
3. Create tenant access groups.
4. Create appliance access groups (optional).
5. Assign roles and tenant access groups to users.
6. Assign appliance access groups (optional) to users.

Procedure: Create Roles

Orchestrator^{SP} roles provide access to specific Orchestrator^{SP} features. Use the Add Role dialog to create custom roles. The capabilities you choose determine if the user can make changes to a capability or only view its settings. Orchestrator^{SP} custom roles enable permitting only necessary job task functions per user.

There are two components to roles: Role name and Capabilities. Orchestrator^{SP} includes these pre-defined roles:

- NetworkAdmin: Read-write access to multi-tenant admin capabilities except for user administration.
- SecurityAdmin: Read-write access to user administration.
- SuperAdmin: Read-write access to all capabilities.

You can create new roles or modify an existing part.

To create a role in Orchestrator^{SP}, complete these steps:

1. In Orchestrator^{SP,} go to Administration **> Role-Based Access Control (RBAC).**

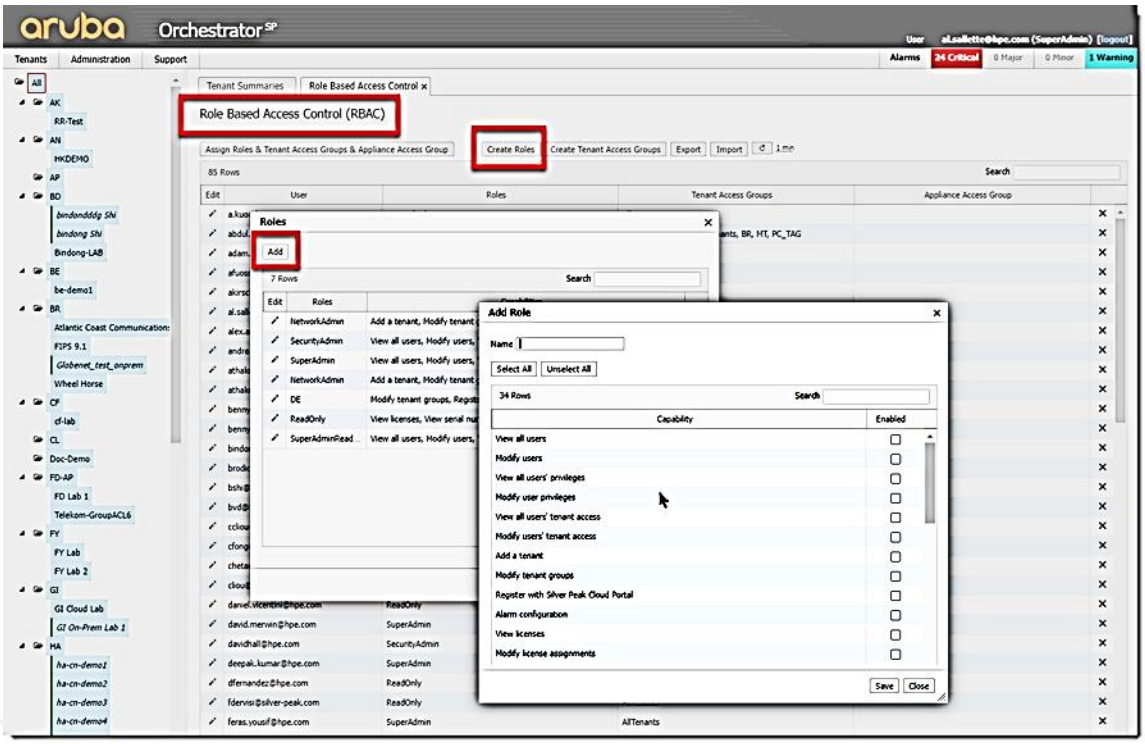


Figure 11 Create Roles

2. Click Create Roles. The Roles dialog box opens.
3. Click Add to create a new role or click the Edit icon to the left of any existing part.
4. Enter or modify the role name.
5. Select a category you want to assign to your user from the following tabs: Monitoring, Configuration, Administration, Orchestrator, Support, or Miscellaneous.
6. To assign the overall access level for the role, select Read Only or Read & Write.
7. Select the check box corresponding to the Orchestrator menu options you want to make available to the role.
8. Click Save.

Create Orchestrator^{SP} Tenant Access Groups

Tenant access groups divide tenant Orchestrators into domains of control. Large tenants can have multiple SD-WAN fabrics, each with its Orchestrator. A Tenant Access Group specifies which tenants or tenant groups are included, the access level (Read Only or Read/Write), and the Orchestrator RBAC role(s) that apply to this group.

1. To create Tenant Access Groups in the Orchestrator^{SP} management console, go to **Administration > Role Based Access Control (RBAC) > Create Tenant Access Groups > Add >** to open the Tenant Access Group dialog, click **Add** to Add Tenant Access Group.

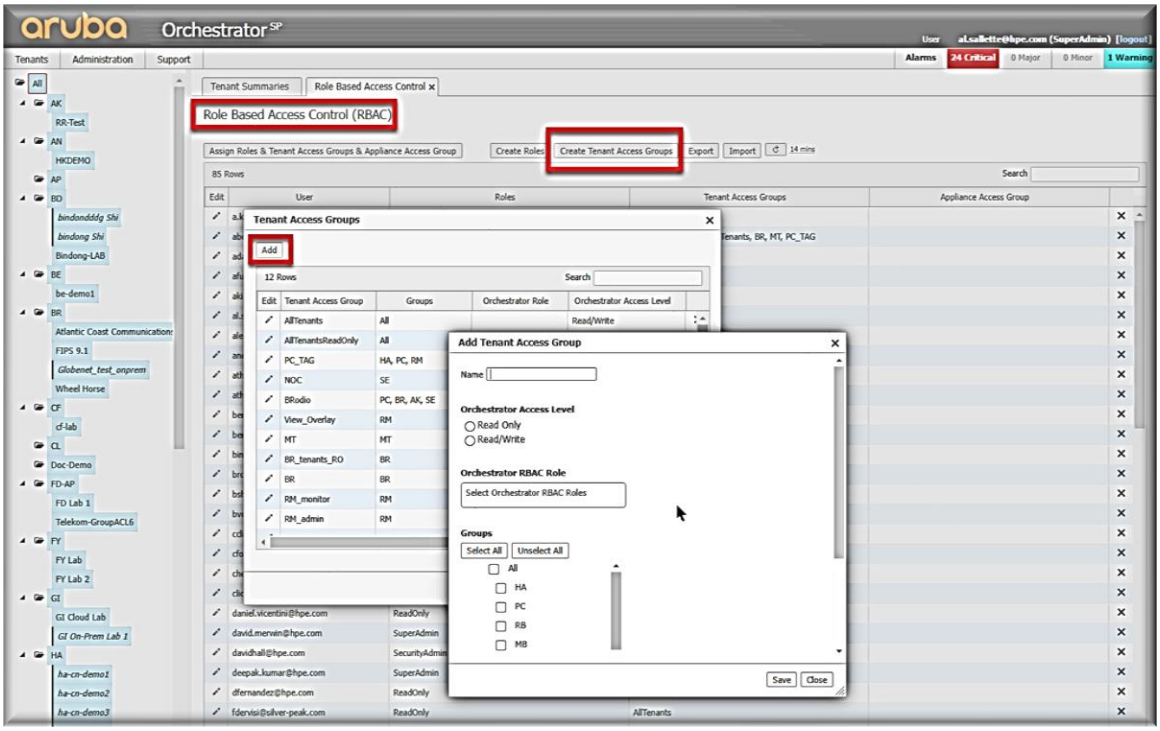


Figure 12: Tenant Access Groups

Orchestrator^{SP} includes two pre-defined tenant access groups: AllTenants and AllTenantsReadOnly.

- AllTenants has read/write access to all tenant Orchestrators.
- AllTenantsReadOnly has read-only access to all tenant Orchestrators.

2. Provide a name for the Add Tenant Access group, specify the access level you want to use, the RBAC roles you need for this group, and the tenant(s) you want to include. Click **Save** to save your changes.

Procedure: Create Tenant Orchestrator Appliance Access Groups

NOTE: This procedure is performed in the tenant Orchestrator, not in Orchestrator^{SP}.

Appliance access groups limit users to specific appliances managed by a tenant Orchestrator.

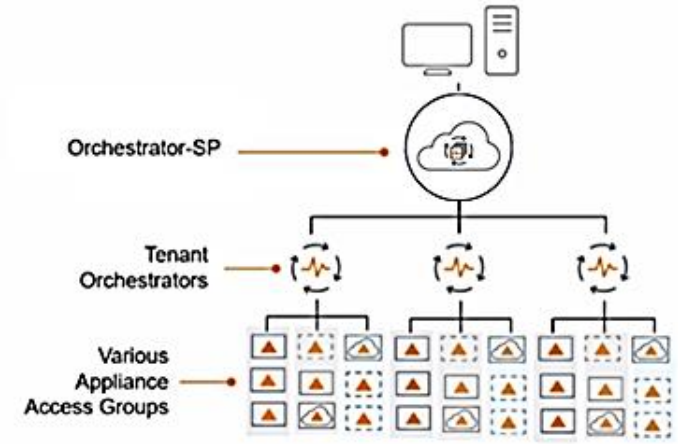


Figure 13: EdgeConnect Appliance Access Groups

You can restrict appliance access to one or more groups or regions with appliance access groups. Complete the following steps to customize appliance access.

1. In the tenant Orchestrator management console, go to **Administration > Role Based Access Control >** Create Appliance Access Groups. The Appliance Access Groups dialog box opens.

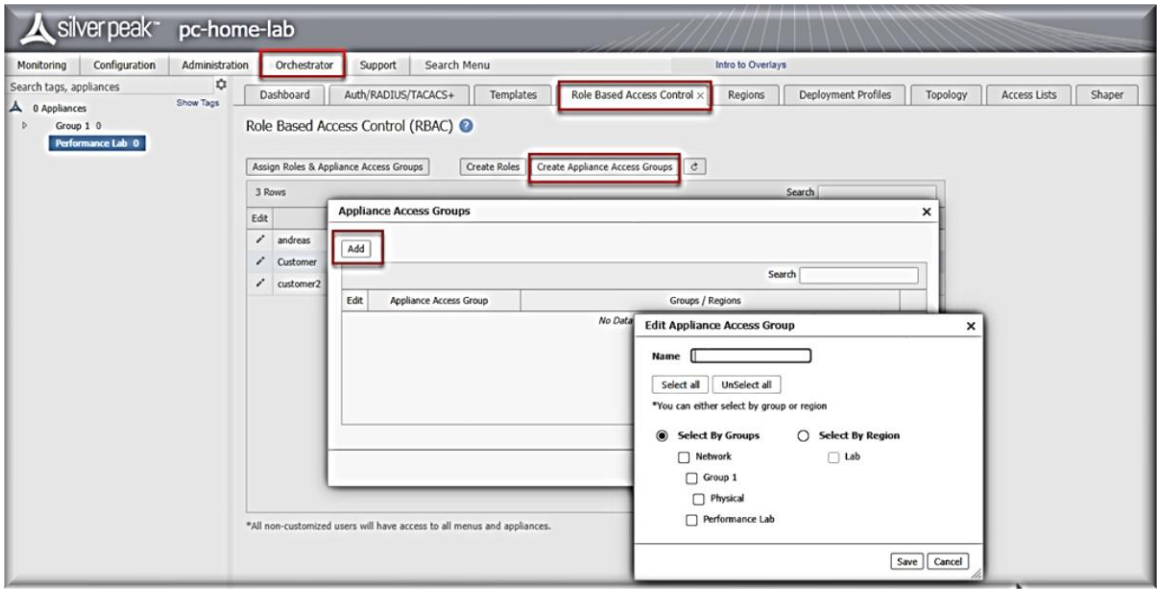


Figure 14: Create Appliance Access Groups

2. Click Add to create a new group or click the Edit icon to the left of any existing group.
3. Add or modify the name of the appliance access group.
4. Choose how you want to add appliances: Select By Group or Region. You can manually select groups or regions to include or use the buttons to select or clear all options.
5. Click Save.

NOTE: A non-RBAC user or an RBAC user with appliance access and no assigned role has access to the Appliance Manager, CLI Session, and Broadcast CLI. An RBAC user with any role assigned is denied access to the Appliance Manager, CLI Session, and Broadcast CLI.

User	Appliance Access	Roles	Menu Options
Non-RBAC	N/A	N/A	Appliance Manager, CLI Session, Broadcast CLI
RBAC	Yes	None Assigned	Appliance Manager, CLI Session, Broadcast CLI
RBAC	No	Any	Appliance Manager, CLI Session, and Broadcast CLI are denied

Procedure: Assign Roles, Tenant and Appliance Access Groups

You can assign various roles to Tenant and Appliance Access Groups.

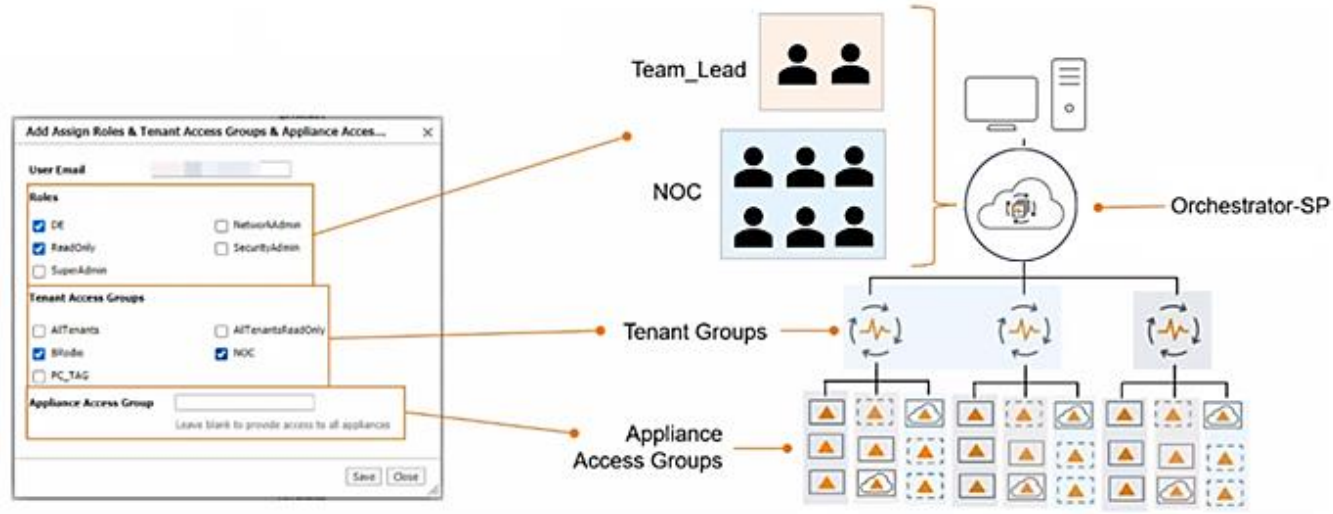


Figure 15: Assign Roles, Tenant Access Groups, and Appliance Access Groups

Complete the following steps to assign roles and appliance access.

1. In Orchestrator[SP], on the Role Based Access Control tab, click Add Assign Roles & Appliance Access Groups & Appliance Access Group.

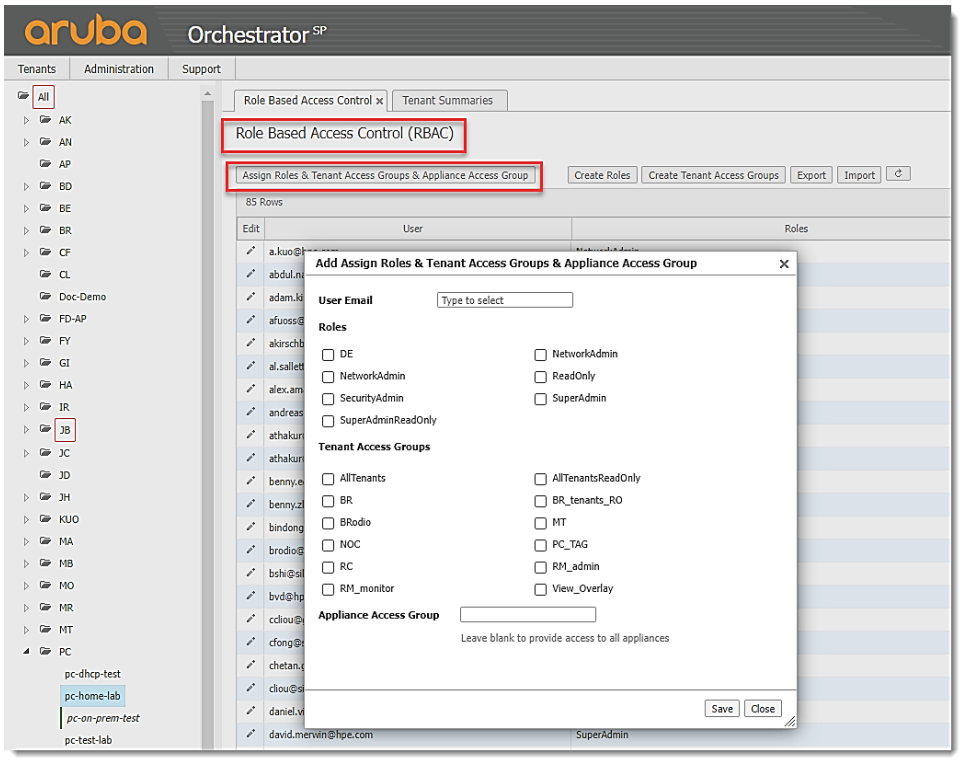


Figure 16: Assign Roles & Appliance Access Groups

2. In the **User Email** field, enter a user's email address.
3. In the **Roles** field, select role(s) for this user.
4. In the **Tenant Access Groups** field, select from the list of Appliance Access Groups.
5. In the **Appliance Access Group** field, specify the Appliance Access Group.
6. Click Save.

SINGLE SIGN-ON AUTHENTICATION

Each tenant can contain multiple Orchestrators, each Orchestrator managing a different SD-WAN fabric. Orchestrator authentication provides granular access controls for Orchestrator features or appliances. User accounts on Orchestrator and EdgeConnect appliances are two separate entities. Users with read-write permissions can make configuration changes, and users with read-only permissions can only view system information.

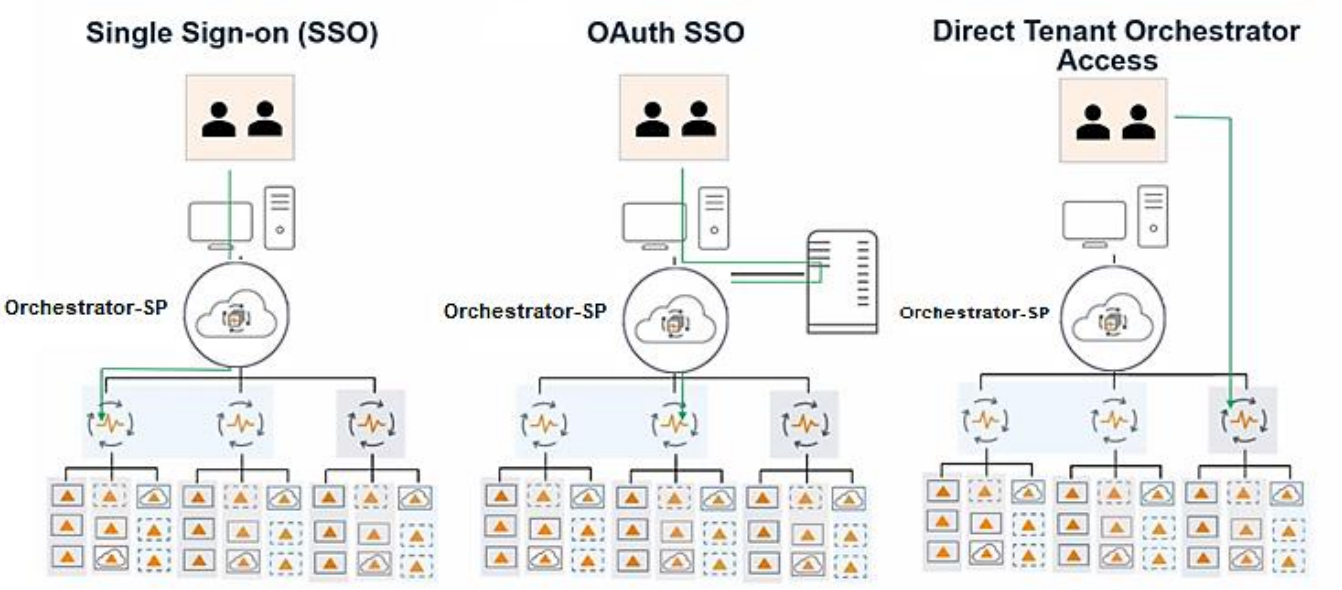


Figure 17: SSO Overview

Orchestrator^{SP} provides granular controls that permit users only the permissions and appliance access necessary to perform their job functions. Role Based Access Control (RBAC) works with Orchestrator users, not EdgeConnect appliances. RBAC improves control of user accounts, enables access to specific appliances, and lets you use pre-defined and custom roles. Orchestrator^{SP} controls which tenant Orchestrators users can access. Appliances are managed primarily via the Orchestrator GUI, but there is an additional Appliance Manager. When signed into Orchestrator, you can manage appliances via the Appliance Manager. The best practice is to sign in to Orchestrator to configure and manage appliances.

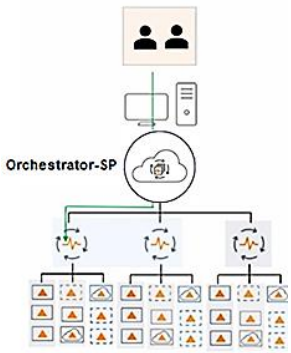
If RBAC is required for single sign-on (SSO), then the user must be defined in both the Orchestrator^{SP} and the tenant Orchestrator. The RBAC feature is defined at the tenant level.

ORCHESTRATOR^{SP}	TENANT	DESCRIPTION	BEHAVIOR
Yes	Yes	User IDin Orchestrator^{SP} and Tenant	SSO via Orchestrator^{SP}, RBAC enabled
Yes	No	User ID in Orchestrator^{SP} only	SSO via Orchestrator^{SP}, RO/RW, no RBAC
No	Yes	User ID in Tenant only	Must log in via Tenant URL, RBAC enabled

Procedure: SSO Via Orchestrator^{SP}

NOTE: This procedure applies to cloud Orchestrator instances, not on-prem instances.

A large service provider may have many users that need to log in to Orchestrator^{SP}. An overview of the process for Orchestrator^{SP} SSO authentication is listed below:



1. You assign role and tenant access groups to a user. Optionally, you can assign EdgeConnect appliance access groups to a user.
2. The user signs in to Orchestrator^{SP}.
3. Orchestrator^{SP} passes the role (and appliance access group) to the tenant Orchestrator.

Figure 18: Single Sign-On

Complete the following steps to add a user.

1. In the Orchestrator^{SP} management console, go to **Administration > User Management**. The User Management dialog box opens.

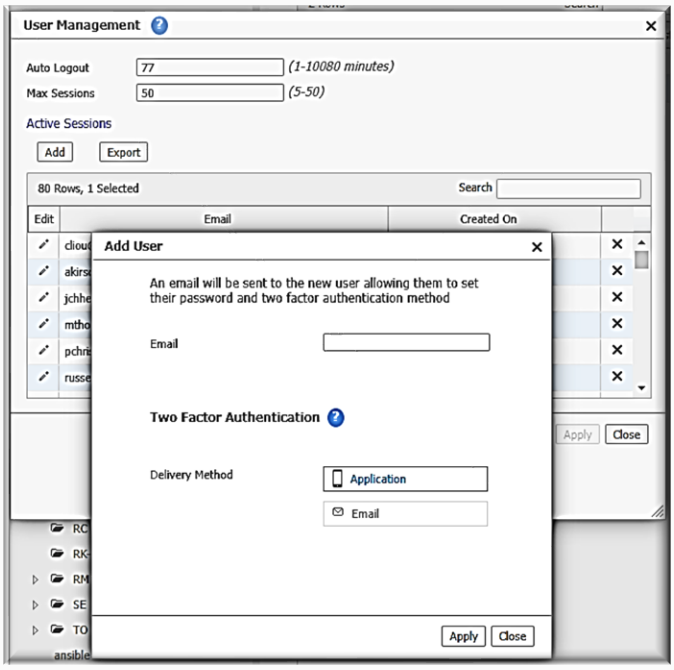


Figure 19: Add User

2. Click **Add** to add a new user. The Add User dialog box opens. The user email address is the user ID.
3. Click **Apply** to save the new user.

4. Click **Edit** for the user you just created to assign privileges. Your assigned privileges determine what you can see and access on the User Management pages and popups.

- Each privilege listed on the form is inherently either Read/Write or Read Only.
    - To select all privileges, click Enable Read/Write Privileges.
    - To select only the subset of privileges related to monitoring, click Enable Read Only Privileges.
    - Regardless of which button you click, you can select or clear individual capabilities.
- To designate user access to a tenant, click Tenants.
    - For each tenant listed, you can specify Read Only or Read/Write.
    - If you select neither, the user will not see that tenant.

Procedure: SSO To Orchestrator^{sp} Via OAuth

NOTE: This procedure applies to cloud Orchestrator instances, not on-prem instances.

The process for OAuth SSO authentication is listed below:

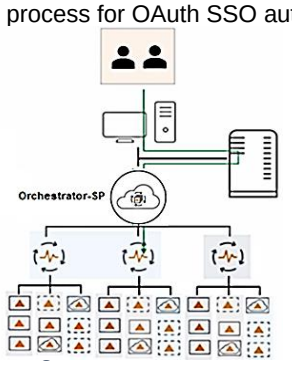


Figure 20 OAuth SSO

1. You configure the OAuth remote authentication server for Orchestrator^{SP}.
2. You assign role and tenant access groups to a user. Optionally, you can assign EdgeConnect appliance access groups to a user.
3. The user signs in on Orchestrator^{SP}.
4. The identity provider (idP), like Okta, passes through the role (and appliance access group) to the tenant Orchestrator.

You can configure remote authentication for RADIUS, TACACS+, OAuth, JSON Web Token (JWT), and SAML 2.0 (Security Assertion Markup Language) servers. After adding a new remote authentication server, you can log in to Orchestrator using that remote server on the Orchestrator login page.

Complete the following steps to add a remote authentication server:

1. Click **+Add New Server**. The Remote Authentication Server dialog box opens.

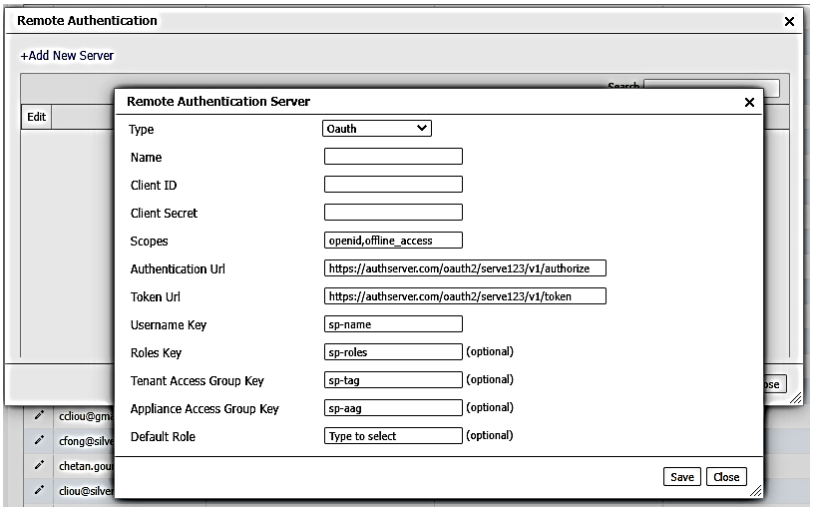


Figure 21: Remote Authentication Server Configuration

2. Select the **OAuth** authentication type from the drop-down list.
3. Provide a name for the remote authentication method displayed on a button on the Orchestrator login page.
4. Provide the following details for the remote **OAuth** server:

   Enter the **Client ID**, **Client Secret**, **Scopes**, **Authentication Url**, **Token Url**, and **Username Key** from the application you added to your OAuth provider. **Username Key**, **Roles Key**, and **Appliance Access Group Key** are retrieved automatically from your OAuth provider.

CAUTION: If Role-Based Access Control (RBAC) is enabled, you must supply a default role when configuring a remote authentication server in Orchestrator.

Roles and Appliance Access Groups

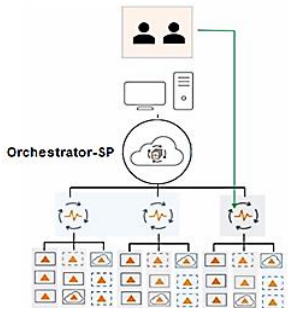
You can configure and apply roles and appliance access groups to users for your OAuth server on the RBAC tab in Orchestrator. After configuring the user roles in Orchestrator, you must ensure that the correct attributes are mapped and returned from your remote authentication server.

NOTE You can only permit access to a single appliance access group during configuration. If this is not provided, access is given to all appliances.

Procedure: Direct Tenant Orchestrator Authentication Access

NOTE: This procedure applies to *both* cloud and on-prem Orchestrator instances.

Direct tenant Orchestrator access *does not* go through Orchestrator^{SP}. Complete the following steps to configure direct authentication for either option.:



Option 1: Local user authentication according to users configured in Orchestrator.

Or

Option 2: Remote authentication servers configured for tenant Orchestrator access:

- RADIUS
- TACACS+
- OAuth
- JWT
- SAML

Figure 22: Direct Tenant Orchestrator Access

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

- To add a new remote authentication method, click **+Add New Server**.
- To view or modify the settings for an existing remote authentication method, click the Edit icon in the row of the existing method.

NOTE: Orchestrator supports remote authentication via the OAuth 2.0 framework. Before configuring an OAuth server in Orchestrator, you must register Orchestrator as an application with your OAuth provider.

Assure that the following prerequisites are met:

- The OAuth server must support OAuth 2.0 authorization codes, ID tokens, and (optionally) refresh tokens.
- The ID token is used to get usernames, RBAC roles, and RBAC appliance access groups.
- The refresh token can be checked periodically to ensure that the user is still authorized.
- Depending on the OAuth server configuration, refresh tokens can be permanent or expire. If a token is revoked or expires, the user is forced to authenticate again.

Register Orchestrator as an App

Before adding an OAuth server in Orchestrator, register a new app on your OAuth server for Orchestrator. Provide the following details when registering the app:

Application Type	Register Orchestrator as a Web App
Allowed Grant Types	Authorization code (required) Refresh token (optional)
Redirect URL	Orchestrator endpoint to which the user is redirected after successful authentication, which should be https://**/gms/rest/authentication/OAuth/redirect

Procedure: Configure an OAuth Server

Follow these steps to configure a remote authentication server.

1. In Orchestrator, go to Administration > Remote Authentication >. Click Add New Server. The Remote Authentication Server dialog opens.

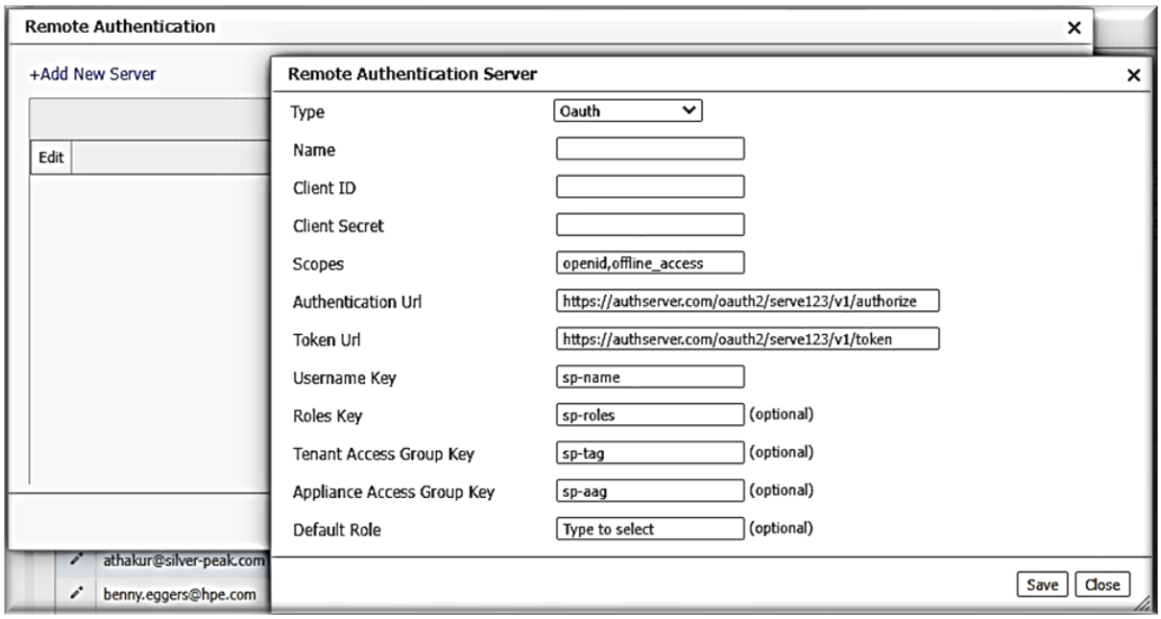


Figure 23: Configure Remote Authentication Server

2. Configure the OAuth Server Properties in Orchestrator.

   When adding a new OAuth server or modifying an existing server, configure the following fields in the Remote Authentication Server dialog box:

Field	Description
Allowed Grant Types	Authorization code (required) Refresh token (optional)
Redirect URL	Orchestrator endpoint to which the user is redirected after successful authentication, which should be https://**/gms/rest/authentication/OAuth/redirect
Name	Name to identify the server. This name is displayed on a button on the Orchestrator login page as an alternative authentication method.
Client ID	Client ID for the Orchestrator application that you created in your OAuth provider.
Client Secret	Client secret for the Orchestrator application that you created in your OAuth provider.
Scopes	OAuth 2.0 uses scope values defined in RFC 6749 to specify access privileges requested in Access Tokens. The default scopes for Orchestrator are opened offline access and email.
Authentication Url	The Issuer Identifier URL with the authentication request path is appended. For example, https://**/oauth2/v1/authorize.

Token Url	The Issuer Identifier URL with the token path is appended. For example, https://**/oauth2/v1/token.
Username Key	The OAuth attribute is to be sent as the username. If the username is an email address, use **email**. If any other key is used, ensure it is mapped to the correct scope on the OAuth server.
(Optional) Roles Key	This field can be left with the default value, sp-roles, or you can enter a new key name, but the key name must match what is configured in your OAuth provider. This is a user claim sent in the ID token that maps to Orchestrator roles defined in Role-Based Access Control (RBAC). For example, the OAuth server attribute userType maps to sp-roles, and the OAuth user in Orchestrator has userType set to OverlayAdmin.

Procedure: Configure A JWT Server

To begin JWT server configuration, the assigned admin must specify the following JWT configuration parameters:

- Issuer ‘iss.’
- Auditor ‘aud.’
- Expiration ‘exp’
- Signature
- User, role, and AAG
- Redirect URL based on successful authentication: https://?access_token=&id_token=&state=&token_type=Bearer&expires_in=3596

Review the following diagram for more details about the workflow of JWT authentication.

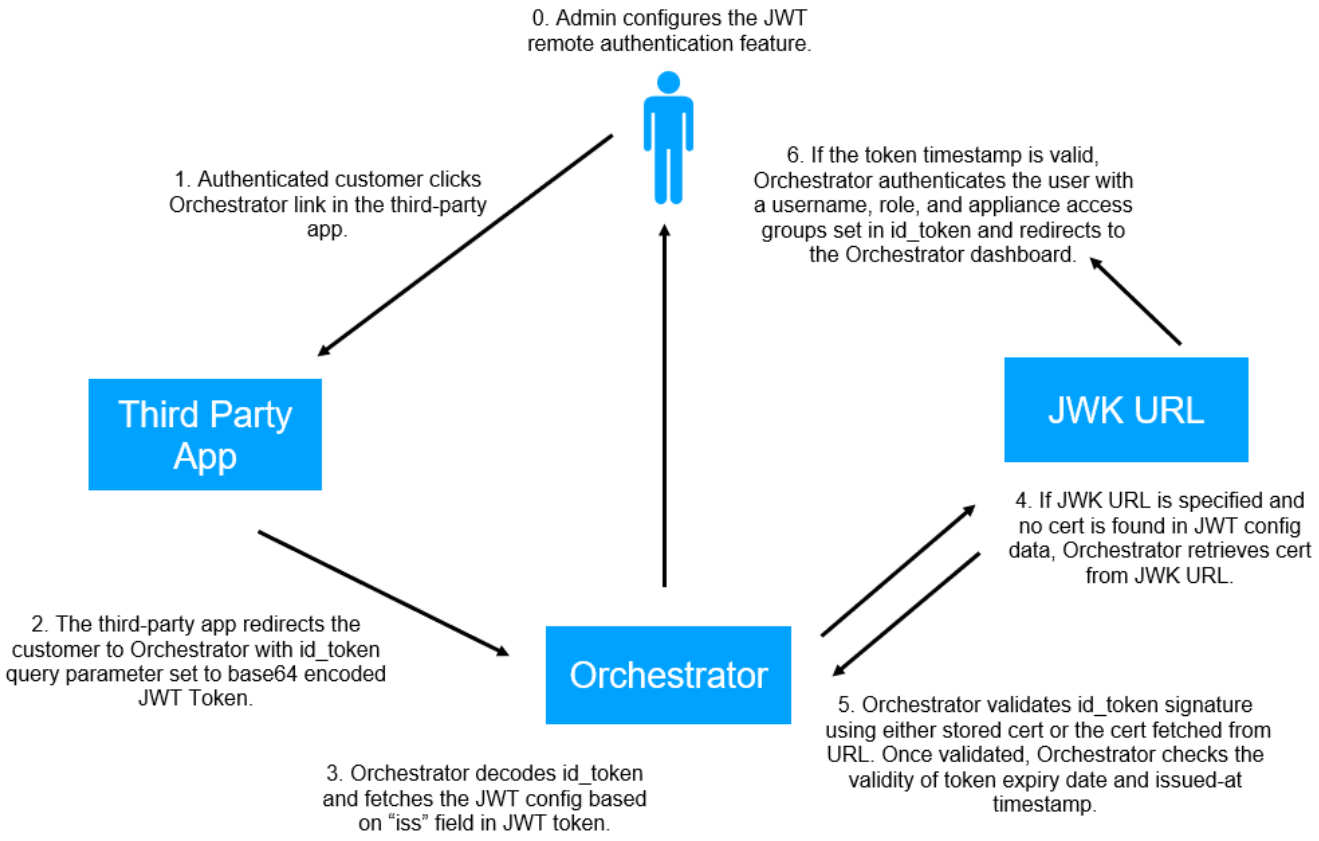


Figure 24: JWT Authentication Flow

Then, complete the following steps in the tenant Orchestrator:

1. Navigate to the Authentication tab in Orchestrator.
2. Click **+Add New Server**. The Remote Authentication Server window opens.
3. From the **Type** drop-down menu, select JWT and complete the following fields.

Field	Description
Name	Name of your JWT provider.
Cert/Signing Key	HMAC or RSA public key that is used to verify the id_token.
JWK URL	URL that hosts the public certification.
Validation Window	The maximum amount of time (in minutes) that the expiration is found for the id_token before a new id_token is created.
Issuer	Issuer claim found in the id_token.
Auditor	Auditor claim found in the id_token.

Username Key	This attribute is sent as the username. If the username is an email address, use email. If any other key is used, ensure it is mapped to the correct scope on the OAuth server.
Roles Key	This field can be left with the default value, sp-roles, or you can enter a new key name, but the key name must match what is configured in your JWT provider. This is a user claim sent in the ID token that maps to Orchestrator roles defined in Role-Based Access Control (RBAC). For example, the OAuth server attribute userType maps to 'sp-roles', and the OAuth user in Orchestrator has userType set to OverlayAdmin.
Appliance Access Group Key	This field can be left with the default value, sp-aag, or enter a new key name, but the key name must match what is configured in your JWT provider. This is a user claim sent in the ID token that maps to Orchestrator Appliance Access Groups defined in RBAC. For example, the JWT server attribute department maps to sp-aag, and the JWT user in Orchestrator has department set to Asia-Admin.
Default role	If RBAC is enabled, you must specify a default role.
JWT token-consuming URL	URL of Orchestrator remains the same.

Procedure: Configure A SAML Server

Orchestrator supports SAML 2.0 integration, providing authentication and authorization of your credentials through an IdP (Identity Provider), SP (Service Provider), and a Principal. Refer to the list below for the represented meanings:

- IdP: Okta
- SP: Orchestrator
- Principal: Principal end user

Use the following instructions to complete SAML and Orchestrator integration.

TIP: Keep Orchestrator open next to your Okta window while completing these instructions.

1. Sign in to your Okta account.
2. Select Add Application, and then select SAML 2.0.
3. Click Create New App.

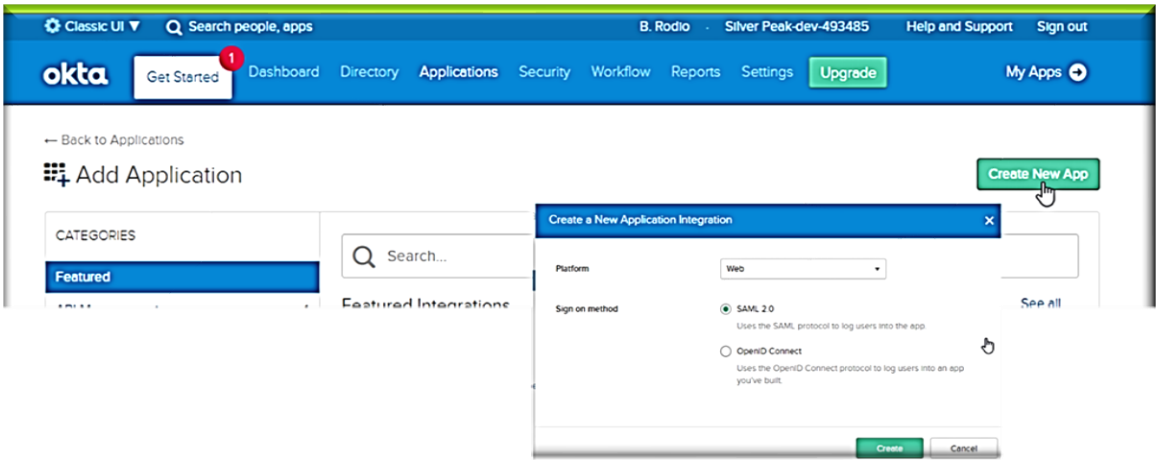


Figure 25: Okta Configuration

4. Sign in to Orchestrator and navigate to the Authentication tab **(**tenant Orchestrator > Users & Authentication > Authentication).
5. Click +Add New Server.
6. Select SAML from the Type field.
7. In Orchestrator, click the icon next to the ACS URL and SP SLO Endpoint fields to copy them.
8. Navigate back to your SAML application configuration window.
9. Paste the ACS URL in the Single Sign-On and Audience URL (SP Entity ID) fields.
10. Specify the attributes and their corresponding values on the SAML Settings page. These are configured and assigned on the RBAC tab in Orchestrator.
    - sp-name: user.email
    - sp-role: user.usertype
    - sp-aag: user.department
11. Click Next.
12. Click Finish.
13. Click the View Setup Instructions box on the completed SAML Application Settings page and enter the following URLs in the corresponding Orchestrator fields:

SAML Field	Orchestrator Field
Identity Provider Single Sign-On URL	SSO Endpoint
Identity Provider Issuer	Issuer URL
X.509 Certificate	IdP X.509 Cert

The following table provides more details about these fields.

Field	Description
Name	Any text value for your SAML account for identification purposes.
Username Attribute	Retrieves the username from the SAML XML response.
Issuer URL	Unique identifier of the issuer (for example, Okta, OneLogin).
SSO Endpoint	Unique endpoint for the SAML application created on the IdP server.
IdPX.509 cert	Certificate issued by IdP to verify and validate the response received from the IdP (Okta) server.
ACS URL	Orchestrator endpoint needed for configuration on the IdP server. This is provided as a redirect URL after you are authenticated on the IdP server.
(Optional) SP SLO Endpoint	Endpoint used by IdP to initiate the logout request from Orchestrator to the IdP server.
(Optional) IdP SLO Endpoint	Endpoint used by IdP to initiate the logout request from Orchestrator to the IdP server.
(Optional) SP X.509 Cert SLO	The certificate used by IdP to verify the Single Logout request initiated by Orchestrator to log out of the IdP.
(Optional) Roles Attribute	This field can be left with the default value, *sp-roles*, or you can enter a new key name, but the key name must match what is configured in your SAML provider. This is a claim sent to Orchestrator that maps to roles defined in Role-Based Access Control (RBAC).
(Optional) Appliance Access Group key	This field can be left with the default value, *sp-aag*, or enter a new key name, but the key name must match what is configured in your OAuth provider. This is a claim sent to Orchestrator that maps to Orchestrator Appliance Access Groups defined in RBAC.
Default role	If RBAC is enabled, you must specify a default role.

TENANT MANAGEMENT

You use Orchestrator^{SP} to manage user access, deploy a tenant, manage product licenses, or assign assets such as EdgeConnect appliances to the tenant. Deploying SD-WAN infrastructure (network infrastructure, business intent overlays, firewall or traffic steering, etc.) is done via the Orchestrator instance(s) within a tenant, which is not covered in this document. See the Aruba Orchestrator documentation for instructions on how to deploy SD-WAN infrastructure.

Provisioning

Deployment configuration areas of focus for tenant provisioning are illustrated below.

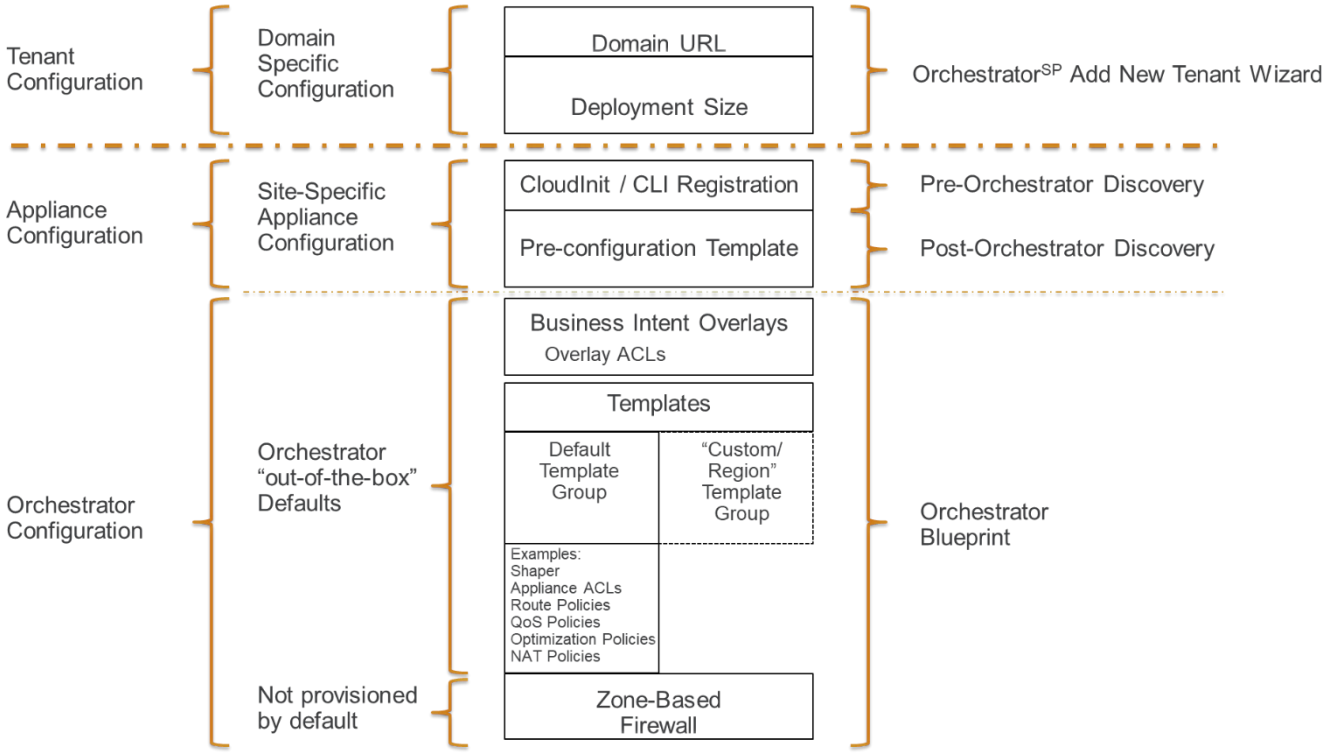


Figure 26: Tenant Provisioning

Again, you will notice that much of the SD-WAN infrastructure deployed in a tenant is handled via the tenant Orchestrator instances. However, the blueprint feature of Orchestrator^{SP} lets you set up a template that contains SD-WAN configurations that you can use to pre-populate a new tenant with common denominator SD-WAN options.

Procedure: Add a New Tenant with a Cloud-Hosted Orchestrator

Use the Add Tenant Wizard to provision a tenant Orchestrator initially.

1. In Orchestrator[SP], go to **Tenants > Add Tenant**.

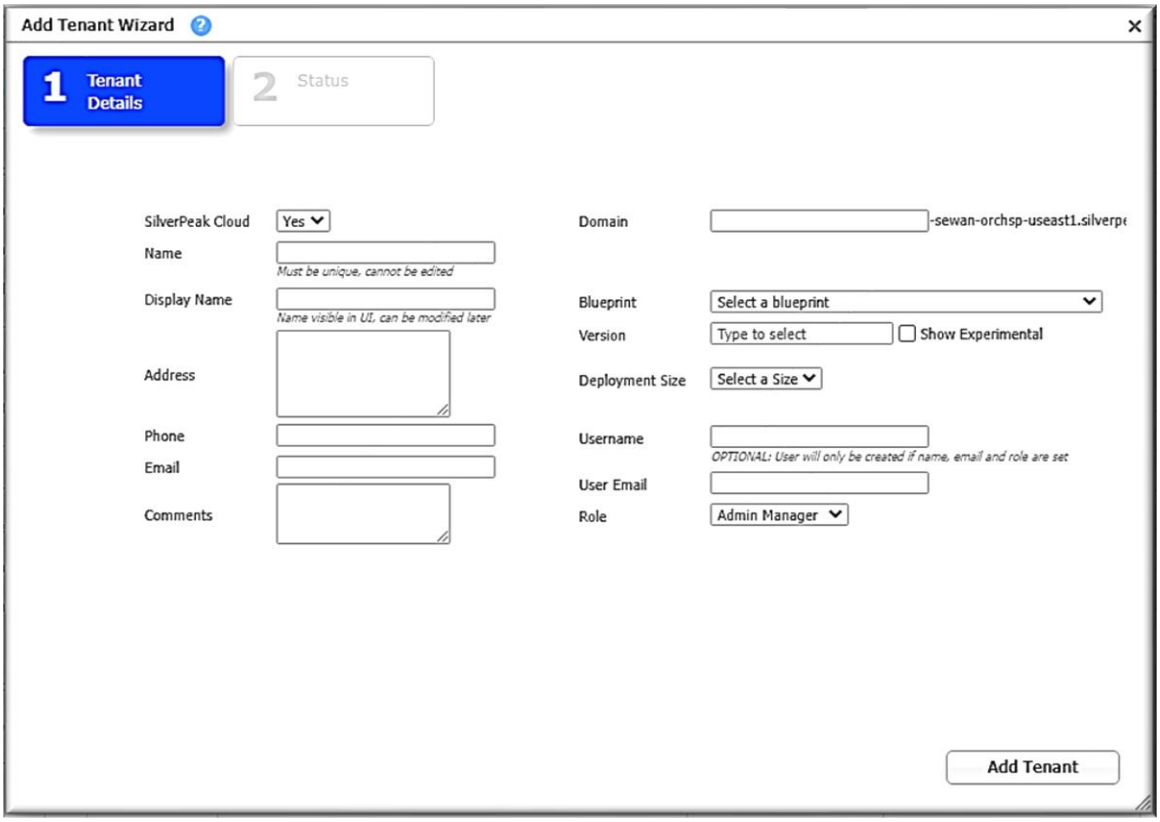


Figure 27: Add Tenant Wizard

- Select **Yes** from the **SilverPeak Cloud** menu.
- The **Tenant Name** is the name known to the portal. It will be used to create a sub-account for the tenant. Specify a unique Name. The name cannot be edited afterward.

  NOTE: The Tenant Name should be the same as the Account Name found in the tenant Orchestrator license.
- The **Display Name** is the name you assign to be visible in the user interface.
- This **Email** address receives the Orchestrator and appliance alarms.
- You specify a **Domain** for your network, which is prepended to the FQDN Aruba provides.
- The **Blueprint** is a configuration template you can use to 'pre-provision' a configuration previously saved as a Blueprint.
- Select what **Version** of the Orchestrator to provision. If using a Blueprint, the version is determined by the Blueprint.
- To provision sufficient resources (CPU, memory), specify the **Deployment Size**.
  If need be, you can change these later on the **Upgrade Tenants** page.
- The optional **Username, User Email,** and **Role** create a user in the new Tenant Orchestrator. This will result in an email sent to this user to set their password. If you leave these options blank, accounts in the Orchestrator[SP] that

have the appropriate RBAC role privileges are passed through to the tenant Orchestrator without needing a user account set up on that tenant Orchestrator.

2. Click the **Add Tenant** button. Step 2 of the Wizard displays the creation tenant process's status, which may take 20 minutes to complete depending on your choice. Alternatively, you can check the status in the **Tenants > Provisioning Tenant Status** screen.

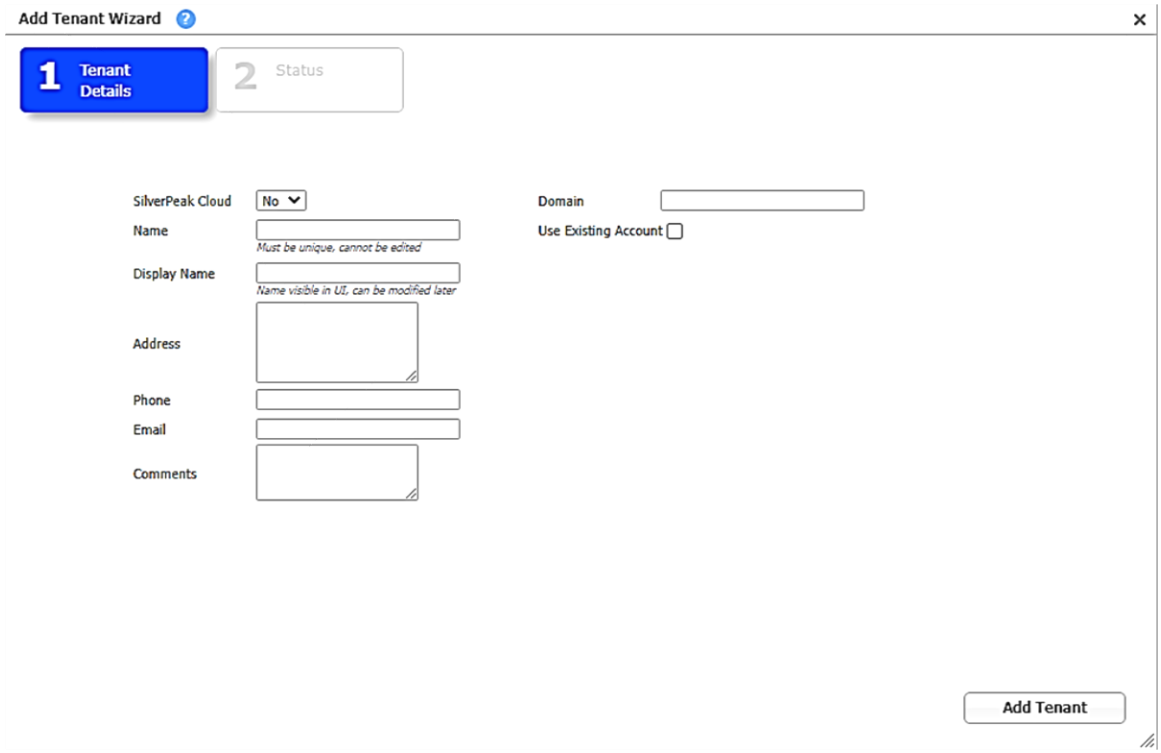
   After clicking **Add Tenant**, you can check the progress on the **Provisioning Status** page. After successful provisioning, the Orchestrator is ready for configuration.

   NOTE: If the status returns a "Failure" message, it is best to click the "Retry" option. This is preferable to deleting this job and starting over.

Procedure: Add A New Tenant with an On-Prem Orchestrator

Use the Add Tenant Wizard to provision a tenant Orchestrator initially.

1. In Orchestrator^{SP}, go to **Tenants > Add Tenant**.



- Select **No** from the **SilverPeak Cloud** menu.
- The Tenant Name is the name known to the portal. It will be used to create a sub-account for the tenant. Specify a unique Name. The name cannot be edited afterward.

Figure 28: Add Tenant Wizard

- The Display **Name** is the name you assign to be visible in the user interface.
- This **Email** address receives the Orchestrator and appliance alarms.

- You specify a **Domain** for your network, which would be your Orchestrator's IP address or FQDN.

2. Click **Add Tenant**. Step 2 of the Wizard displays the creation tenant process's status, which completes quickly. Alternatively, you can check the status in the **Tenants > Provisioning Tenant Status** screen.

   After clicking **Add Tenant**, you can check the progress by accessing the **Provisioning Status** page. After successful provisioning, the Orchestrator is ready for configuration.
   NOTE: If the status returns a "Failure" message, it is best to click the "Retry" option. This is preferable to deleting this job and starting over.

3. The on-prem tenant is added to the end of the Tenant Summaries list with a blue bar on its left that indicates it is on-prem.

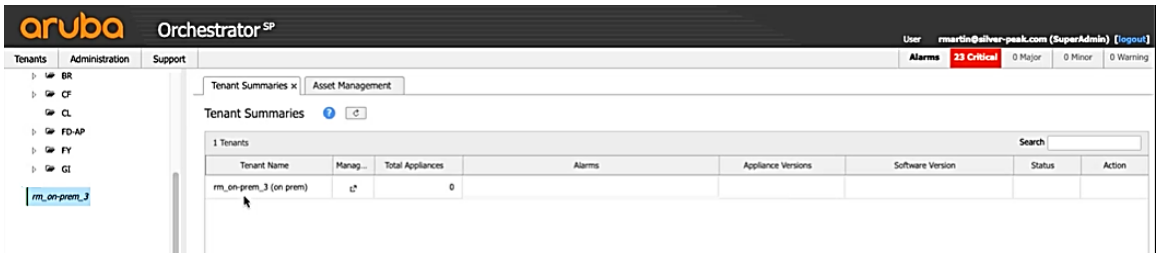


Figure 29: On-prem Tenant

4. Load a VM image onto your Orchestrator server and bring it up.

5. In the tenant tree, right-click on the on-prem tenant you created and click **Details**.

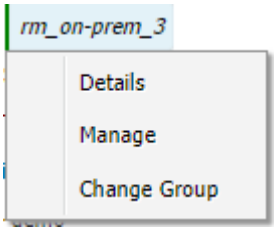


Figure 30: Tenant Details

6. Record the Account Name and Account Key information from the Tenant Details dialog box.

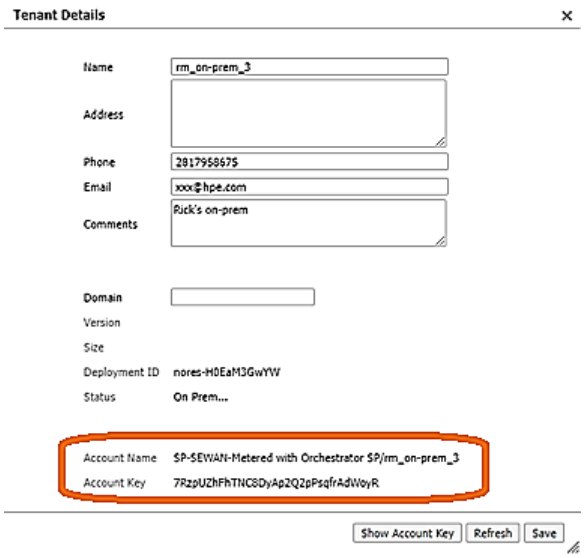


Figure 31: Tenant Account Name and Key for Tenant Details Dialog Box

After the Orchestrator registers with the Cloud Portal, Domain, Version, and Size will automatically populate in the Tenant Details dialog box.

7. Update the Orchestrator instance VM with the Account Name and Account Key.
8. Configure the Orchestrator in the Orchestrator Cloud Portal configuration dialog box.

Blueprint Overview

A Blueprint is a Tenant Orchestrator configuration template.

The primary goals for Blueprints are:

1. Export an Orchestrator configuration into a template that can be replicated to other Orchestrators and used as a starting point in the configuration process. Orchestrator-specific items, such as Netskope, stats, etc., are removed from the template.
2. Ability to export complete Orchestrator configurations to migrate between on-prem and cloud Orchestrators. Orchestrator-specific items would be kept, except stats, because those files are too big to migrate.

Use the Blueprint page to generate a template you can apply as a base configuration when creating new Tenant Orchestrators.

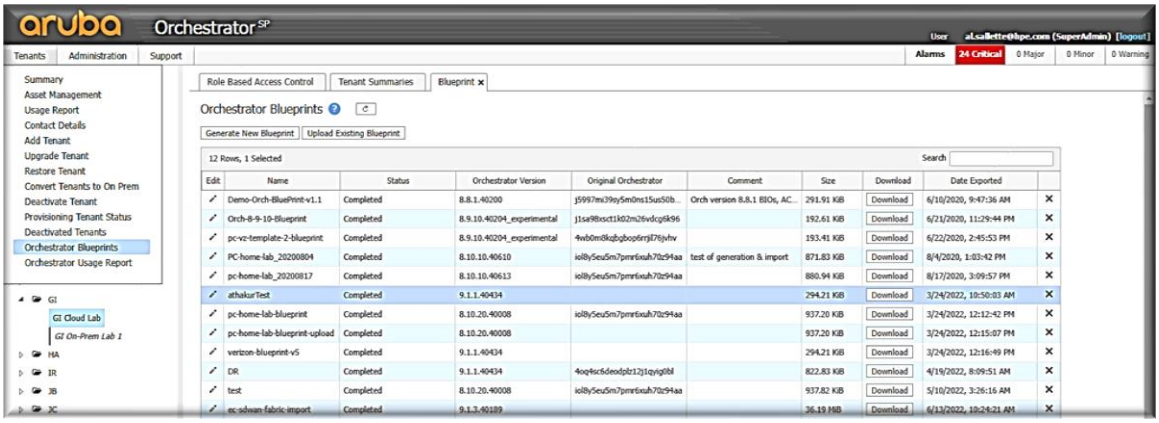
NOTE: Blueprints can only be created from Orchestrators that have no appliances associated with them. If the source Orchestrator manages any appliances, Blueprint creation will fail.

- You can create and store multiple Blueprints with the same Orchestrator.
- After creating as many Blueprints as needed, you can add appliances to the source Orchestrator.
- Blueprints *automatically exclude* the following information when created:
    - All stats and large historical data files (including audit logs, report histories, etc.).
    - Account information

After a Blueprint is created, there will be an option to use the Blueprint when creating a new Tenant. The blueprint will be automatically applied when the tenant Orchestrator is created.

Procedure: Create A Blueprint

1. In Orchestrator^{SP}, go to **Tenants > Orchestrator Blueprints**. The Blueprints tab opens, which displays a list of existing Blueprints.

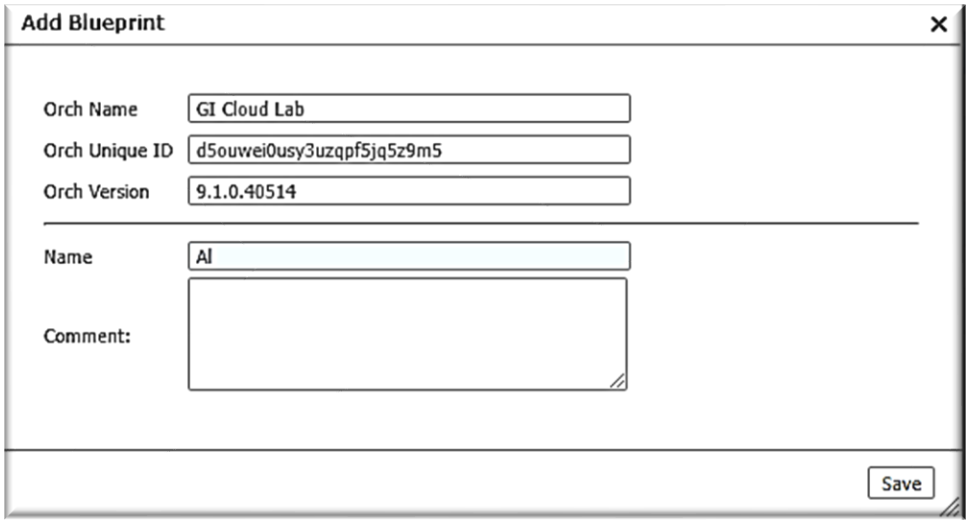


2. From the list of folders on the left, select the tenant Orchestrator you will use to create the template.

Figure 32: Blueprints Tab

NOTE: the Orchestrator must have no appliances.

3. Click **Generate New Blueprint** to open the Add Blueprint dialog.



4. Enter a name, add comments regarding the configurations in the Blueprint, and click **Save**. The Blueprint starts generating in the background. The status displays on the Blueprints tab.

Procedure: Add a Tenant Using a Blueprint

1. Under the Tenants menu, select Add Tenant. The Add Tenant Wizard opens.
2. Fill in the details for the Tenant, select a Blueprint from the dropdown list, and click **Add Tenant**. The Status page of the wizard displays. The applied Blueprint stops the Orchestrator and connects directly to the Orchestrator database to run the Blueprint SQL data.
3. After the Blueprint is applied, the Orchestrator will restart.

Procedure: Blueprint Export

You can use a blueprint when creating a new Orchestrator or migrating an existing Orchestrator to on-prem or cloud. After creating as many blueprints as you need, you can add appliances to the source Orchestrator. A typical scenario is for an organization to provision an Orchestrator^{SP} instance for a test environment and a separate Orchestrator^{SP} instance for their production environment. Blueprints enable creating a Blueprint in the test environment that they then export to an SQL file that they import as a Blueprint in their production environment.

To export an Orchestrator Blueprint, complete the following steps:

1. In the Orchestrator Blueprint Export dialog box, select the blueprint type: **Template** or **Migration**.
2. Click **Export**.
   Export downloads an SQL file to your local desktop.

   NOTE: Importing a Blueprint SQL file to a tenant completely replaces the configuration of the existing tenant Orchestrator.

Procedure: EdgeConnect Appliance Asset Management

Orchestrator^{SP} enables asset management of EdgeConnect appliances. Orchestrator^{SP} manages the following:

- A pool of EdgeConnect appliances.
- Assigning assets to different customers.
- Moving assets between customers.

Use the Asset Management page to assign assets to tenants. To perform a task, you must select an individual tenant.

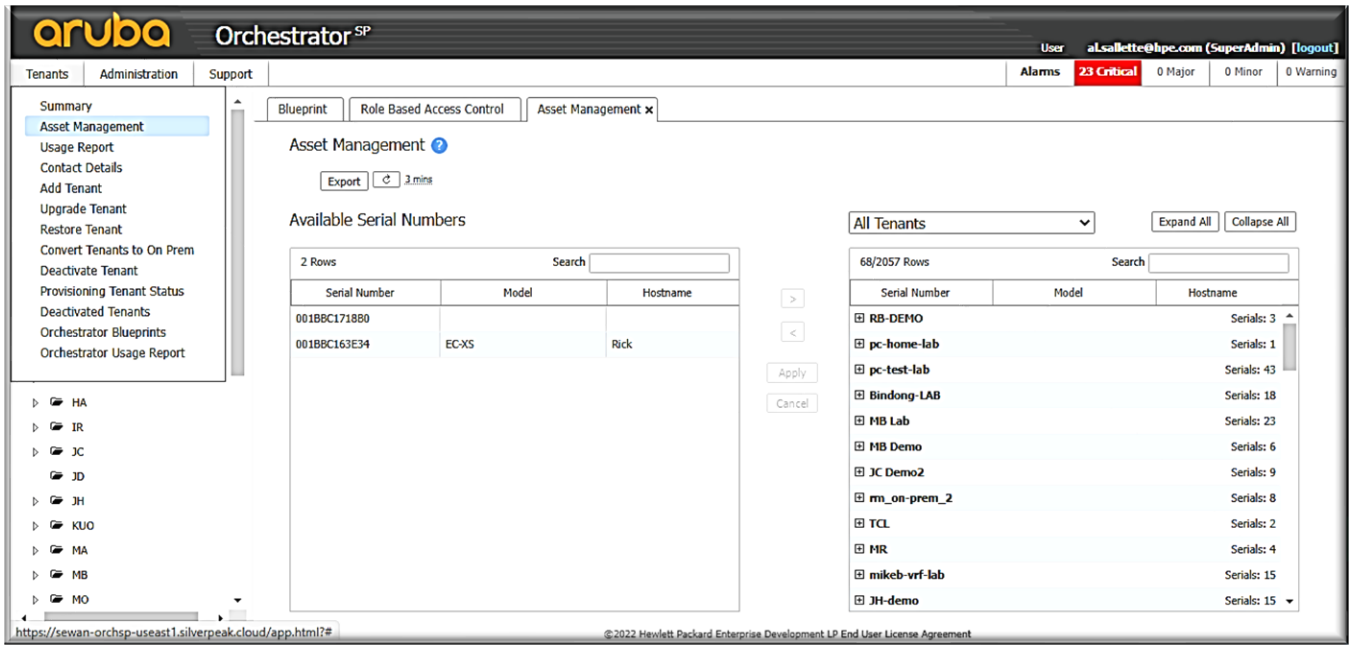


Figure 33: Asset Management

The Cloud Portal activates EdgeConnect appliances. That activation process identifies the Orchestrator^{SP} instance to which an EdgeConnect appliance belongs.

NOTE: Virtual appliances are greyed out and cannot be selected or moved.

To allocate a physical appliance to a tenant, do the following:

1. In Orchestrator^{SP}, go to **Tenants > Asset Management**. The Asset Management tab opens.
2. Select and move an appliance (Serial Number) from the Available Serial Numbers table to a tenant selected from the drop-down list.
3. The EdgeConnect appliance is in the Tenant. It would be best if you went to the Discovered Appliances tab of the tenant Orchestrator to approve it.
   NOTE: Any EdgeConnect appliance must be approved within the Tenant Orchestrator.
4. Once approved, the **Appliance Wizard** opens. Use the wizard to apply policies and select other configuration options.

To move a physical appliance from one tenant to another, do the following:

1. Go to the Asset Management list.
2. Select the tenant containing the asset you want to move from the Tenants drop-down list.
3. Select the asset, click the left arrow to move it to the Available Serial Numbers table, and then click **Apply**. Virtual appliances are greyed out and cannot be selected or moved.
4. From the Tenants drop-down list, select the destination tenant.

5. In the Available Serial Numbers table, select the asset. Click the right arrow to move it to the tenant chosen, then click **Apply**.
6. The EdgeConnect appliance is in the Tenant. It would be best if you went to the “Discovered Appliances” tab of the tenant Orchestrator to approve it.
   NOTE: Any EdgeConnect appliance must be approved within the Tenant Orchestrator.
7. Once approved, the Appliance Wizard opens. Use the wizard to apply policies and select other configuration options.
8. Use the **Export** button to create a CSV file for either the Appliance Serial Numbers page or the Licenses page.

To remove a physical appliance from a tenant, do the following:

1. Go to the Asset Management list.
2. Select the tenant containing the asset you want to remove from the Tenants drop-down list.
3. Select the asset, click the left arrow to move it to the Available Serial Numbers table, and then click **Apply**.
4. Use the **Export** button to create a CSV file for either the Appliance Serial Numbers page or the Licenses page.

Overview Of Adding Appliances to a Tenant Orchestrator

The following figure shows the process of installing and provisioning an EdgeConnect appliance.

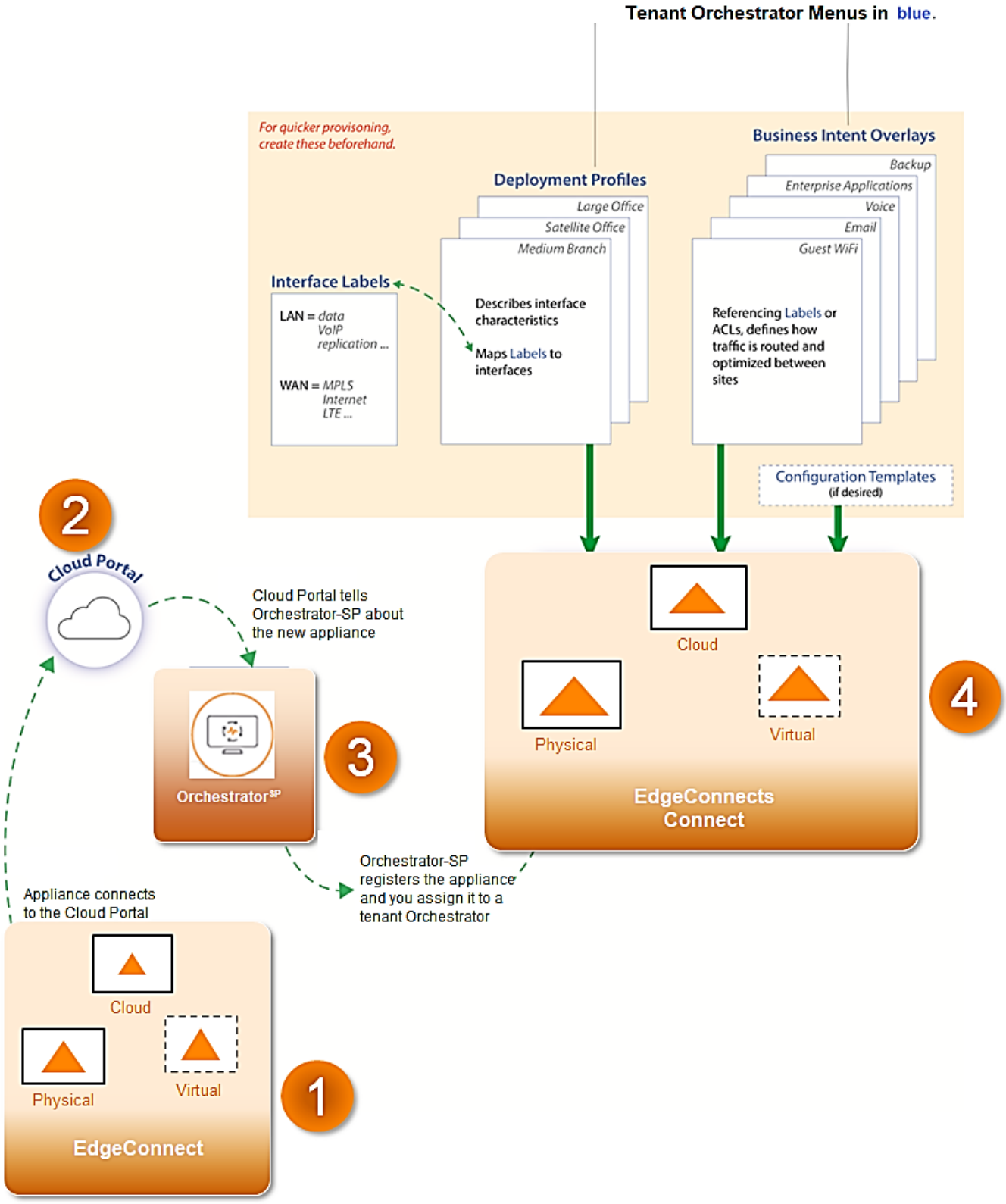


Figure 34 Appliance Provisioning Flow

EdgeConnect appliances are added via Orchestrator^{SP} and then assigned to a tenant Orchestrator. Adding a new appliance to a tenant consists of four basic steps:

1. **Registration and discovery.** The EdgeConnect appliance registers with the Cloud Portal.
2. **The Cloud Portal** assigns the appliance to the appropriate Orchestrator^{SP} Instance.
3. You **accept** the discovered appliance in Orchestrator^{SP}.
4. You **assign** it to a tenant Orchestrator. In the tenant Orchestrator, you accept the assignment of the appliance, and the **Configuration Wizard** opens. Because the wizard prompts you to select profiles, it is easier to create these ahead of time.

Follow the instructions in the SD-WAN documentation to add EdgeConnect appliances via Orchestrator.

RMA

The RMA (Return Merchandise Authorization) Wizard automates the RMA process for an exchange or replacement of your appliance if needed. It includes appliance discovery, the version of the appliance, and a backup selection. Please note the following before you begin the RMA process.

- Upgrade or downgrade the new appliance to the same software version before shipping to the site. This will save time.
- Perform a backup of the Orchestrator and EdgeConnect appliances.
- Install the new EdgeConnect onsite.

NOTE: When Orchestrator discovers the new device, do not approve it. Use the tenant **Orchestrator > Support > RMA** dialog to start the following RMA process to move the license to the new EdgeConnect.

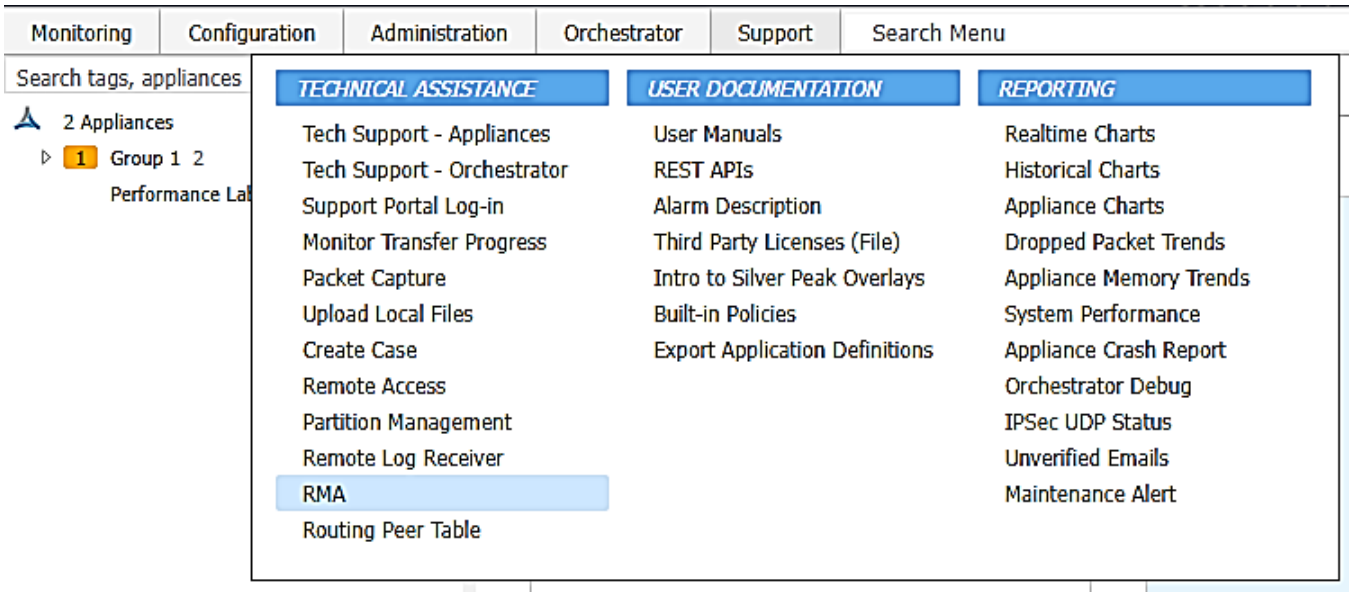


Figure 35 RMA

Procedure: RMA a Tenant Appliance

Complete the following steps to RMA your appliance.

1. Contact Aruba Support to open a ticket for the RMA. Aruba will then send a replacement appliance.
2. Install the replacement appliance, and let the Cloud Portal discover the appliance, which automatically recognizes that it belongs to the Orchestrator^{SP} instance. The replacement EdgeConnect Appliance shows up in the list of Available Serial Numbers in the Orchestrator^{SP} Asset Management tab.
3. Assign the replacement appliance to the tenant where the appliance to be returned for the RMA is located.
4. Navigate to the RMA tab in the Orchestrator UI.

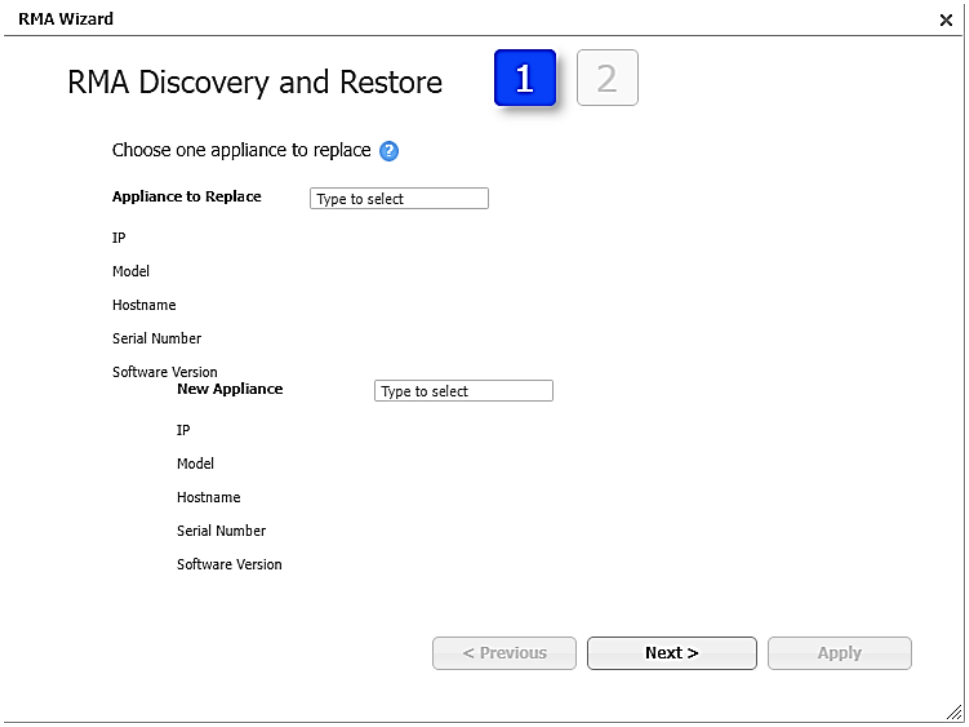


Figure 36 RMA Configuration Transfer

5. Select the appliance you want to replace from the menu.

   NOTE The IP address, appliance model, hostname, serial number, and software version will auto-populate once you select the appliance.
6. Select the incoming discovered appliance to replace the previous appliance.

   NOTE The IP address, appliance model, hostname, serial number, and software version will auto-populate once you select the appliance.
7. Select **Next >**.
8. If you do not choose to add a backup appliance, select **Apply**.
9. The **Applying Configuration** page will open if you This page lists the status of the upgrading appliance and restore configuration.

Complete the following steps if you add a backup appliance from the table.

1. Select the backup appliance from the table.

2. Select the version you want the backup appliance to have from the drop-down menu.

   NOTE: A backup must be provided if your selection results in a software downgrade.

Upgrade and Downgrade

If the software version you selected for your backup appliance is **higher** than that of the discovered appliance, you will need to do the following:

- Upgrade to the new version of Orchestrator
- Backup the appliance from a restore, if applicable

If the software version you selected for your backup appliance is **lower** than that of the discovered appliance, you will need to do the following:

- Install the desired version as the next boot on the appliance
- Restore from backup

BACKUP/RESTORE TENANT ORCHESTRATORS

Cloud Orchestrators automatically run backup jobs daily and as part of upgrades. Backups are relevant to these scenarios:

- Redundancy with hosting in two AWS availability zones
- Customer backups:
  - One daily
  - One monthly
  - During the end customer's orchestrator upgrade
- For decommissioned customers, one backup is maintained for 90 days

The flow chart below illustrates how the backup/restore operation progresses.

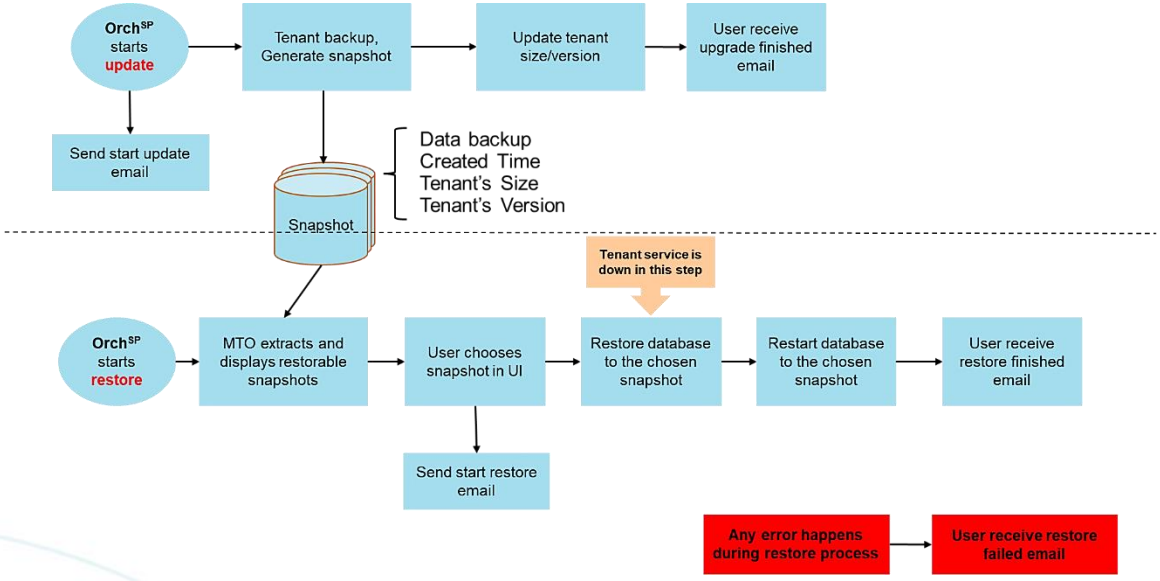


Figure 37 Restore Tenant Flow Overview

Restore Time Estimates

SIZE	APPROXIMATE DURATION
Small (50 appliances)	35 minutes
Medium (200 appliances)	40 minutes
Large (1000 appliances)	40 minutes

Version Dependencies

- Before v9.0.0
  - User can upgrade tenant to a larger size or newer version.
  - Cannot downgrade/rollback.
- After v9.0.0
  - User can downgrade/roll back to a previously defined state.
  - Previously defined state includes database snapshots, version, and size.
  - Can roll back to any snapshot within seven days.
  - Only the user with the privilege to upgrade can do tenant restore.
  - There will be downtime during the restore process.

Procedure: Restore a Tenant

1. In Orchestrator[SP],, go to **Tenants > Restore Tenant**. A list of restorable snapshots displays.

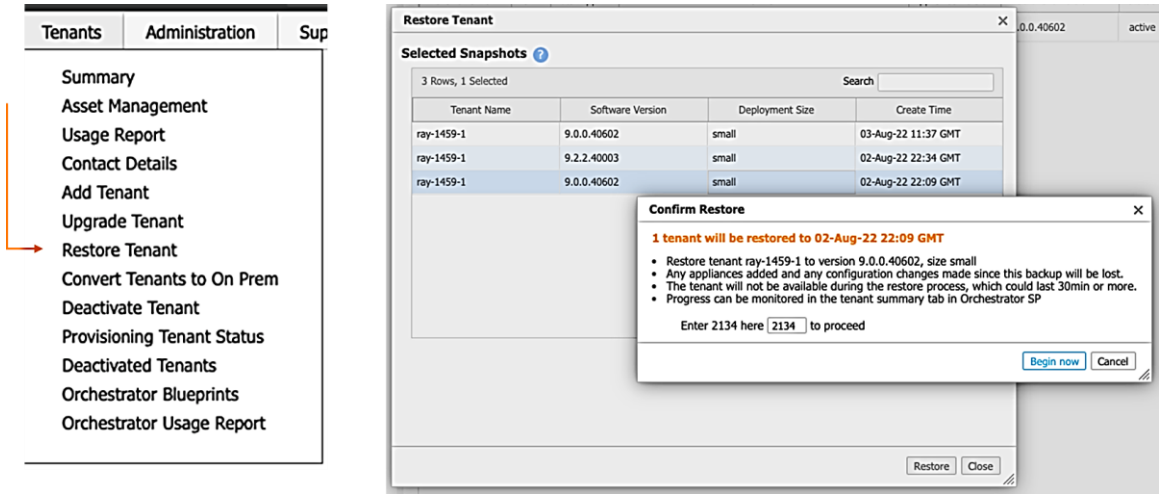


Figure 38 Select Snapshot

2. Select a snapshot in the list to restore.
3. Click **Restore.** A confirmation window opens.

   If the tenant's database is unavailable to restore, a warning message displays at the bottom of the window, and the Restore button will be inactive.

Make sure the target snapshot you chose is correct.

4. Enter the verification code in the box and click **Begin now**.
5. Once the process starts, you get a restore start email.
    - Sample Start Email

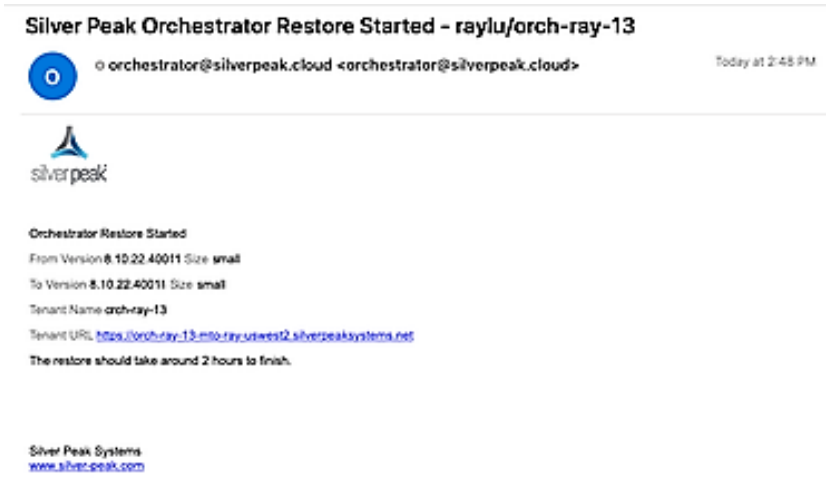


Figure 39 Start Email

    - Other email responses are sent for Restore Finish or Restore Fail

REST API

The set of REST APIs offered by Aruba provides differing levels of abstraction, facilitating multiple choices for programmatic integration, and spans the following systems:

- **Orchestrator^{SP}**: Aruba provides REST commands for performing all Orchestrator^{SP} operations.
- **Orchestrator**: Aruba provides REST commands for performing all operations at the SD-WAN service and network layers and serves as a single point of interaction to perform operations at the SD-WAN appliance layer.
- **EdgeConnect**: Aruba EdgeConnect supports a REST API that operates at the device level.

Orchestrator[SP] user management API

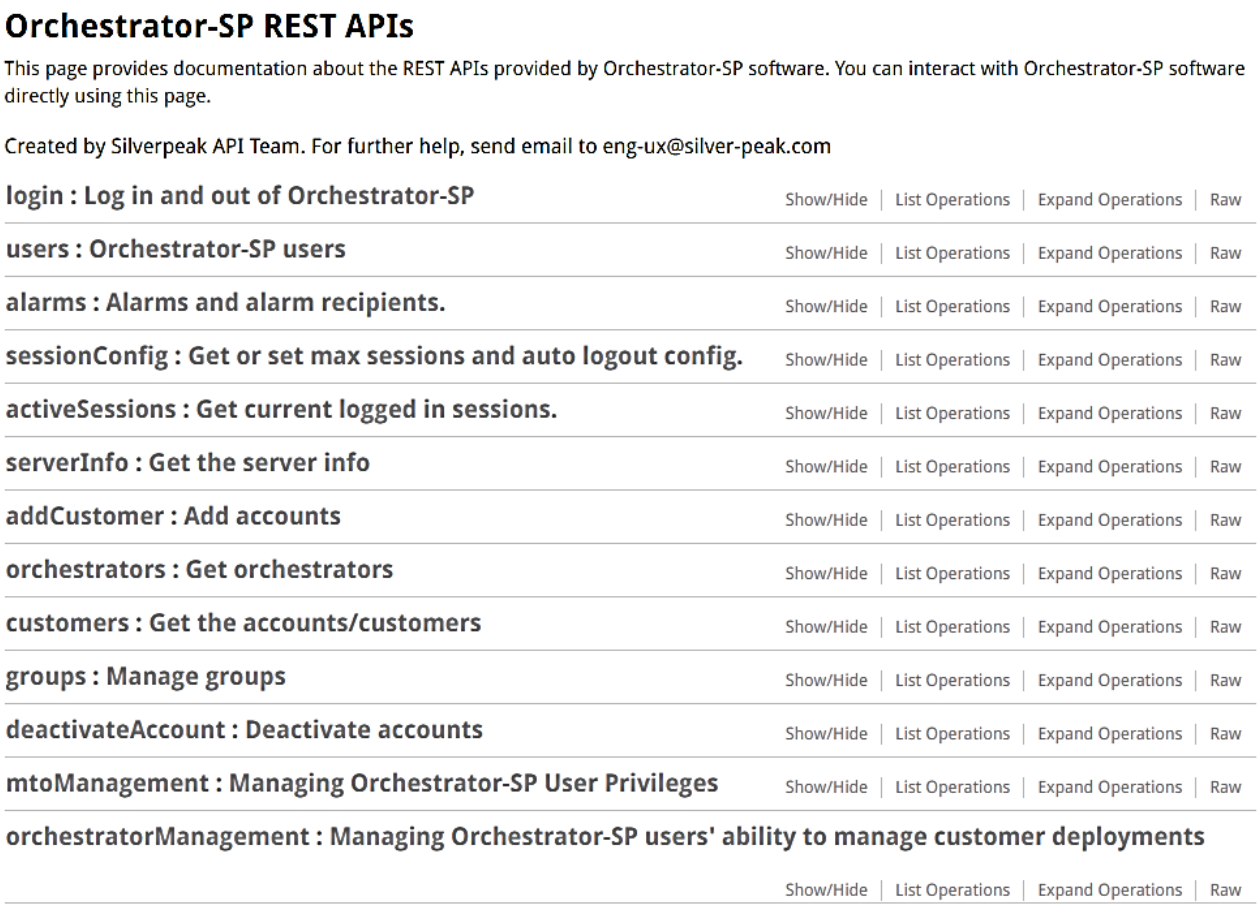


Figure 40 Orchestrator[SP] REST API

Tenant RBAC API

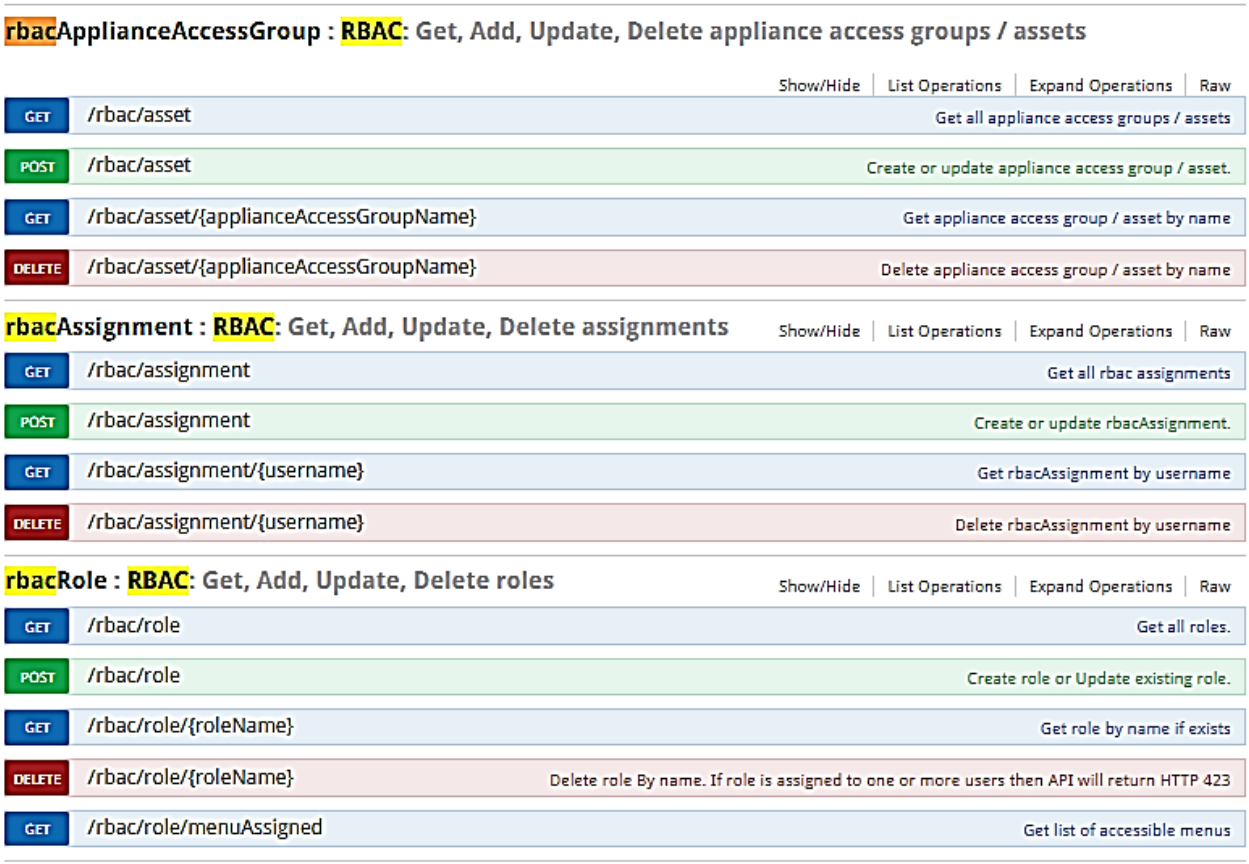


Figure 41 Tenant RBAC API

Tenant user API

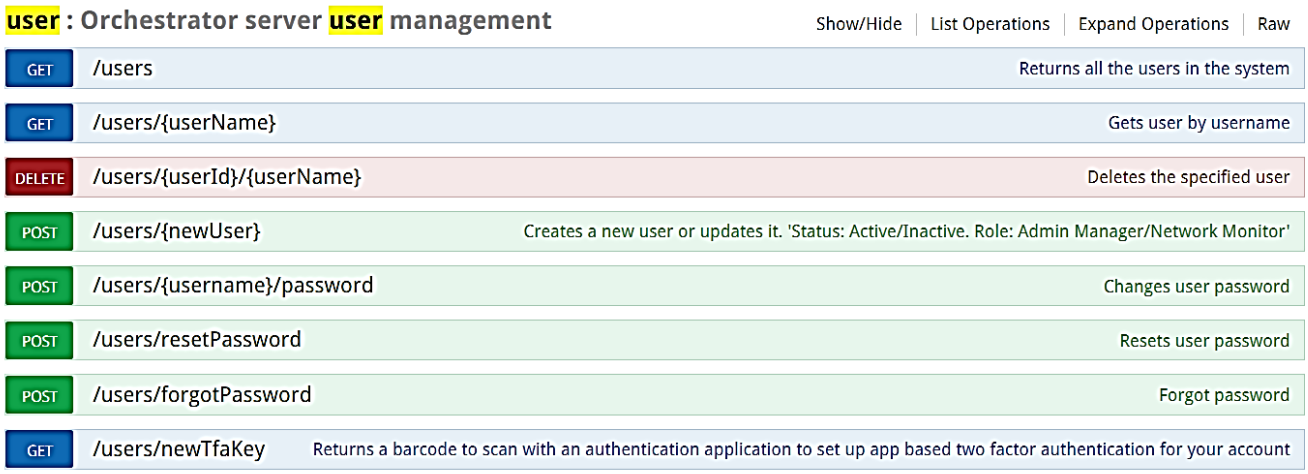


Figure 42 Tenant User API

INTEGRATING WITH PARTNERS

While open APIs provide service providers with the capability to customize the automation of the network with a high degree of flexibility, Aruba has an eco-system approach for those seeking a greater degree of overall lifecycle orchestration. You can leverage NFV MANO orchestration platforms available in the market. Rather than lock customers into a vertical, monolithically integrated single-vendor solution, Aruba works with any network or service orchestration vendor the service provider chooses. These partners leverage the open REST APIs to help bring pre-validated solutions to market based on customer deployment use-case scenarios and provide the expertise for extending automation across other 3rd party systems and VNFs that generally comprise the service provider infrastructure – e.g., firewall configuration, router configuration, additional VNF service chaining, etc. Aruba partners currently include:

- Cisco Tail-F
- NEC/Netcracker
- Ciena BluePlanet NFV Orchestration
- ADVA Ensemble
- WindRiver Titanium Cloud

Aruba is developing partnerships with systems integrators and service providers who provide turnkey, customized service provider SD-WAN solutions based on specific service and product requirements. Aruba offers partners do-it-yourself through this open ecosystem to complete turnkey solutions based on particular business needs.

The Aruba EdgeConnect Enterprise Security App for Splunk Enterprise and Cloud Platforms enables users to search, analyze, and visualize the data gathered from Aruba EdgeConnect Enterprise Intrusion Detection System (IDS). Splunk Enterprise provides a dashboard view of all security event notifications exported from the EdgeConnect Enterprise SD-WAN platform, indexes the data stream, and parses it into a series of individual events that the user can view and search. Using the EdgeConnect Enterprise App for Splunk, users can filter, sort, navigate, and view the collective security event notifications generated across the SD-WAN, overall trends, and top talkers, to help customers pinpoint network events that warrant further investigation.

RESOURCES

Aruba provides essential service and support resources, including product documentation, training, and customer support.

Documentation And Training

If you have a product question or issue that you cannot resolve and is not time-sensitive, follow these guidelines to receive a quick and reliable solution on the Aruba Support Portal. It contains the following:

1. Airheads Community: Provides you with our state-of-the-art KB; join a community of network professionals and discuss issues, ideas, and tips. Or access the interactive Learning Portal, where you can access documents and videos on your area of interest. You can also upload your videos or content here: https://community.arubanetworks.com
2. Product documentation:
    - https://asp.arubanetworks.com/downloads
    - Aruba EdgeConnect SD-WAN Edge Platform documentation site.
3. The latest software updates: https://asp.arubanetworks.com/downloads
4. Training: Support Training | Silver Peak (silver-peak.com)

Support

To ensure you receive the best customer experience, Aruba, a Hewlett-Packard Enterprise Company, has developed expert support from Aruba.

Figure 43 Service and Support

Visit this link to learn about the service and support Aruba provides:

Aruba Support Services | Aruba (arubanetworks.com)