HPE Aruba Networking EdgeConnect SD-WAN Orchestrator

Resolution to CVE-2024-3596

Instructions for vulnerability resolution for EdgeConnect SD-WAN Orchestrator in both self-hosted/on-prem and Orchestrator-as-a-Service deployment models.

A new vulnerability has been uncovered in the RADIUS protocol

HPE Product Security Advisory ID: **HPESBNW04662** published July 12, 2024

CVE: CVE-2024-3596

Version 1.0 – Initial Release, August 1, 2024

Contents

EdgeConnect SD-WAN Orchestrator Deployment Models

Vulnerable Orchestrator Deployments

Orchestrator Model	Deployment Model	Affected Releases
HPE Aruba Networking EdgeConnect SD-WAN Orchestrator	Self-hosted On Prem	All existing Orchestrator instances running CentoOS 7 or Rocky Linux using RADIUS are affected.
	Self-hosted Public Cloud IaaS	All Self-hosted Orchestrators running IaaS: AWS, Azure, and Google Cloud Platform (GCP) using RADIUS are affected.
Aruba EdgeConnect Orchestrator-as-a-Service (OaaS)	Enterprise, Single Tenant OaaS	OaaS using RADIUS is affected
	Orchestrator-SP Tenant OaaS	Orchestrator-SP tenant Orchestrators using RADIUS are affected
	Orchestrator Global Enterprise Tenant OaaS	Orchestrator Global Enterprise tenant Orchestrators using RADIUS are affected

Security Resolution Summary for Orchestrator

Depending on the Orchestrator deployment mode, actions must be completed as detailed here.

- It is recommended to use SAML or OAuth for Orchestrator-user administration and authentication instead of TACACS or RADIUS.
- Customers who rely on RADIUS for Orchestrator-user authentication must enable CHAP authentication. RADIUS servers must be configured to enable message authentication. RADIUS control plane should run over secure SD-WAN fabric if possible.
- Orchestrators in FIPS mode cannot use RADIUS.

Self-hosted Orchestrators, Rocky Linux, FIPS mode enabled

- RADIUS cannot be enabled because FIPS mode disallows MD5 authentication on which RADIUS depends.
- FIPS is enabled by default on all new self-hosted Orchestrators created starting with release 9.4. This applies to both on-prem/hypervisor-based and IaaS (Azure and GCP) deployments.
- FIPS-mode is not applicable for self-hosted/IaaS Orchestrators in AWS.
- FIPS-mode is not applicable for Orchestrator-as-a-Service instances.

Verify if Orchestrator is in FIPS mode

Starting with release 9.4, all new Orchestrator virtual images (not upgrades from previous CentOS installations) will be FIPS-enabled by default.

To verify this, enter the ***fips-mode-setup*** CLI command:

```
Check, enable, or disable the system FIPS mode.
usage: /bin/fips-mode-setup --enable|--disable [--no-bootcfg]
usage: /bin/fips-mode-setup --check
usage: /bin/fips-mode-setup --is-enabled

[admin@orchestrator ~]$ fips-mode-setup --check
FIPS mode is enabled.
```

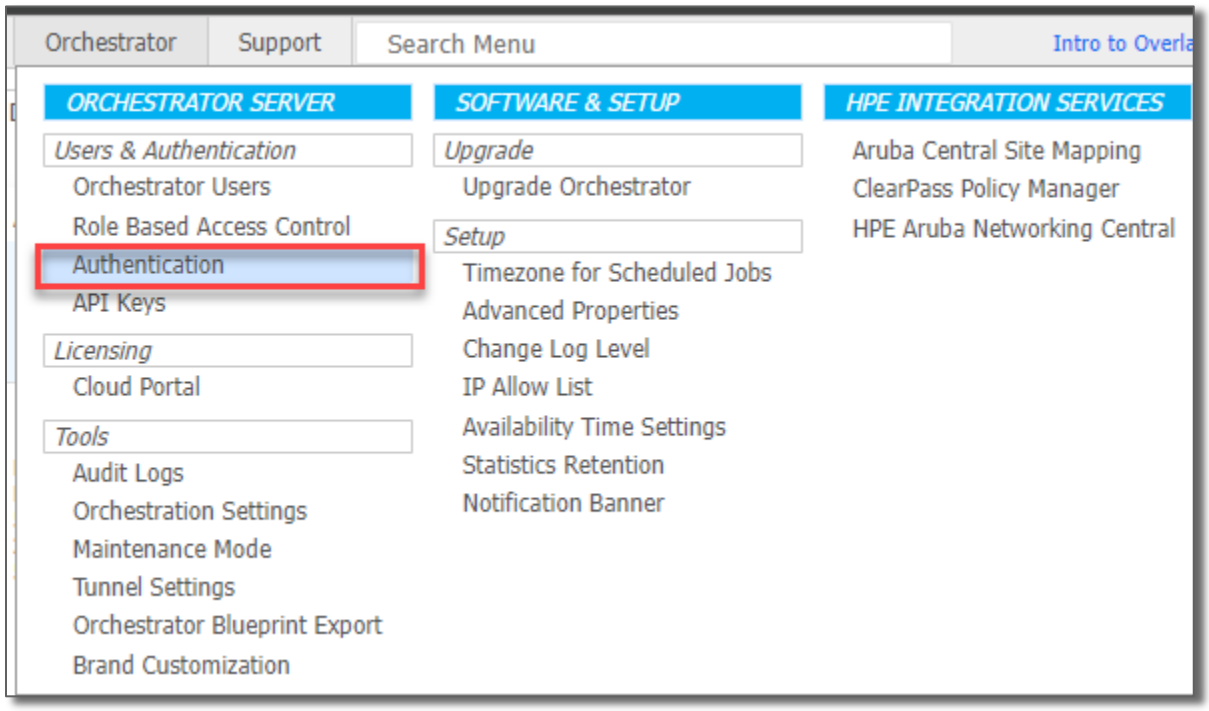
If the customer wants to use RADIUS for Orchestrator user administration and authentication and does not need Orchestrator to be in FIPS mode, then perform the following commands to disable FIPS mode:

1. Log into Orchestrator as the admin user and become the root user by entering '**`su -`**' and the root password.
2. Enter '**`fips-mode-setup -disable`**'.
3. Reboot the Orchestrator Virtual Machine.

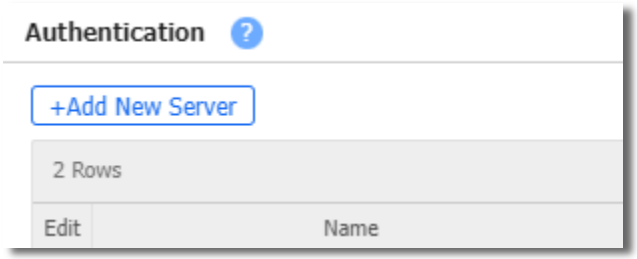
Adding a Remote Authentication (RADIUS) Server to Orchestrator (non FIPS mode)

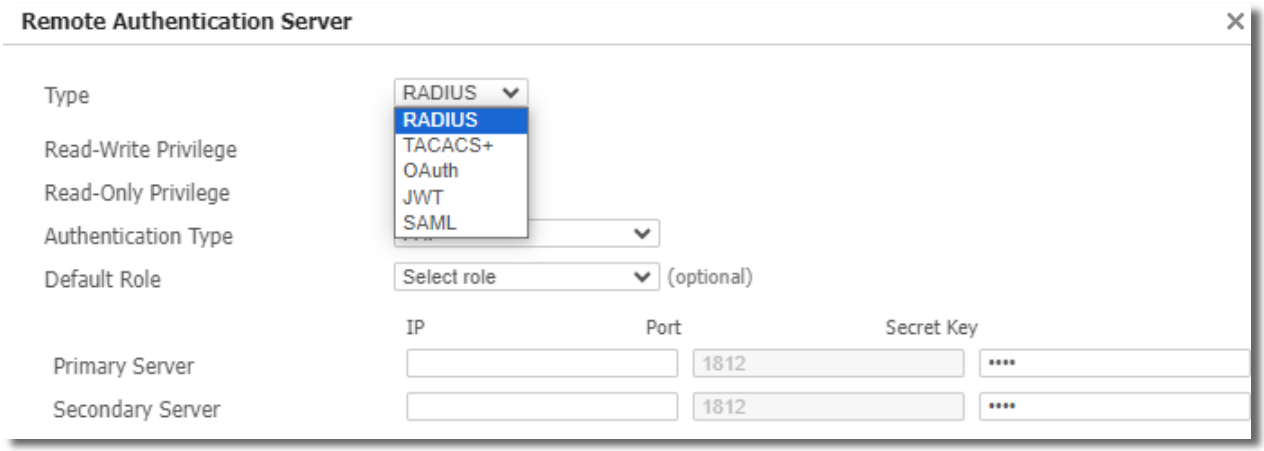
If there is no preexisting RADIUS server and the customer needs to add one, complete the following instructions.

1. In Orchestrator, navigate to **Orchestrator > Orchestrator Server > Users & Authentication > Authentication**.

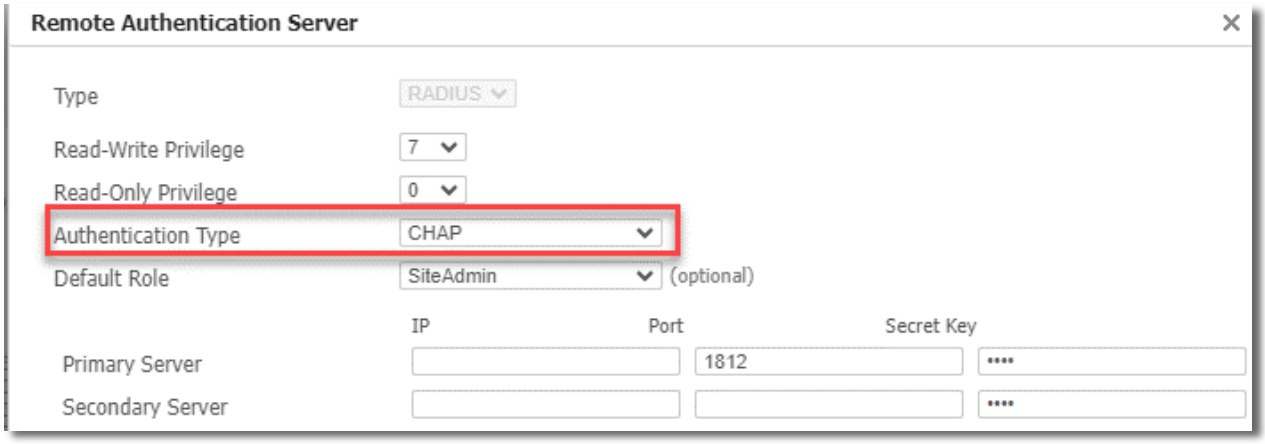


2. Click **+Add New Server** and select **RADIUS** from the Type menu.

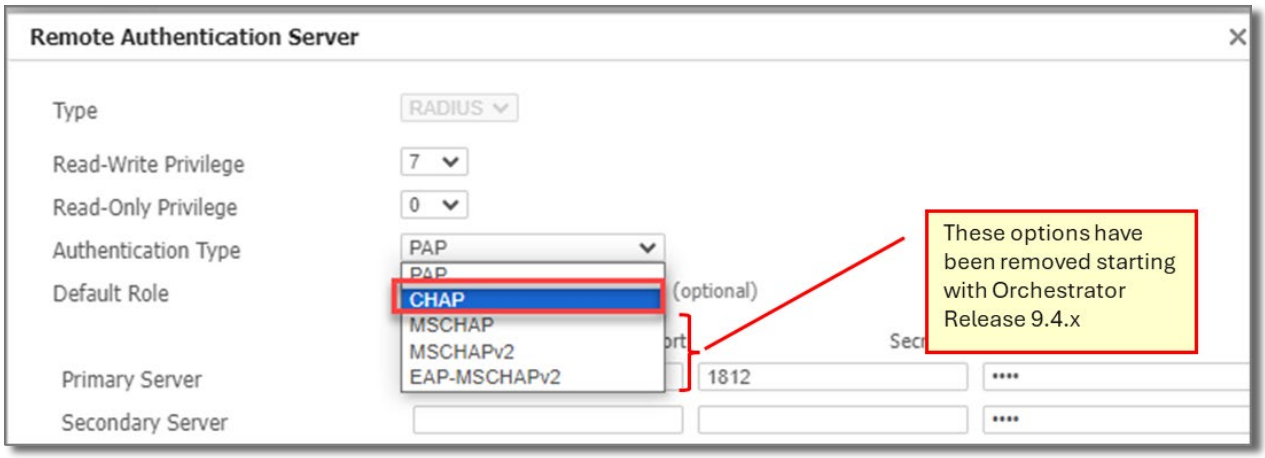




3. Select **CHAP** from the Authentication Type menu.

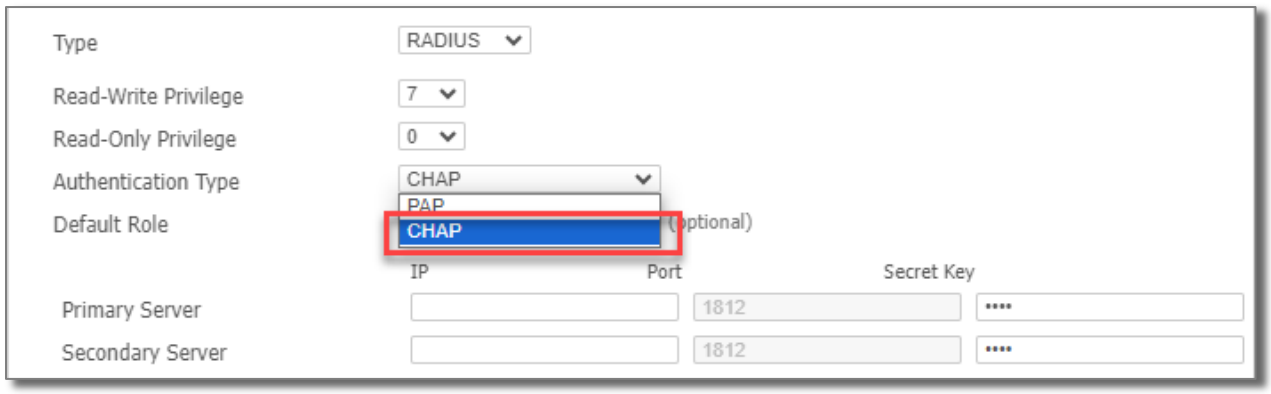


If the Orchestrator release is earlier than 9.4.1, the Authentication Type menu shows several options. Select **CHAP**.



If the Orchestrator Release is 9.4.1 or later, the only options in the Authentication Type menu are PAP and CHAP. Select **CHAP**.

See also, Engineering Alert 2024-0717. MSCHAP, MSCHAPv2, and EAP-MSCHAPv2 are all RADIUS authentication methods that depend on MD4. These authentication methods are no longer supported starting with Orchestrator Release 9.4.1 and later.



RADIUS Server Settings

Message-Authenticator must be enabled on the RADIUS server; configuration is dependent on the RADIUS server you are using.

For example, if you are using FreeRADIUS server, perform the following steps to enable Message-Authenticator:

- vi /etc/raddb/clients.conf
- require_message_authenticator = yes

Explore HPE GreenLake

© Copyright 2024 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.

All third-party marks are property of their respective owners.

Hewlett Packard Enterprise