

ARISTA

Quick Start Guide

W-318/W-318 RW Access Point

Arista Networks

[*www.arista.com*](http://www.arista.com)

DOC-05847-02

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA +1-408-547-5500	+1-408-547-5502 +1-866-476-0000	+1-408-547-5501 +1-866-497-0000
www.arista.com/en/	support@arista.com	sales@arista.com

© Copyright 2024 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos, and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks is subject to Arista Network Terms of Use Policy, available at www.arista.com/en/terms-of-use. Use of marks belonging to other parties is for informational purposes only.

Contents

- Chapter 1: About This Guide..... 1**
- Chapter 2: Package Content.....2**
- Chapter 3: Overview of the Access Point..... 4**
 - 3.1 Right Panel of the Access Point..... 5
 - 3.2 Rear Panel of the Access Point..... 7
 - 3.3 Bottom Panel of the Access Point..... 8
- Chapter 4: Install the Access Point..... 10**
 - 4.1 Mount the Access Point..... 10
 - 4.1.1 Table Mount the Access Point..... 10
 - 4.1.2 Wall Mount the Access Point..... 12
 - 4.2 Connect the Access Point to the Network..... 12
 - 4.2.1 Connect the Access Point Using PoE..... 13
 - 4.3 Power On the Access Point..... 13
 - 4.3.1 Using the Access Point with Power Adapter..... 13
- Chapter 5: Access Point Troubleshooting..... 14**
- Chapter 6: Appendix A: AP-Server Mutual Authentication..... 15**
- Chapter 7: Appendix B: Product Compliance..... 16**
- Chapter 8: Appendix C: Regulatory Model Numbers..... 17**

About This Guide

This installation guide explains how to deploy the W-318/W-318 RW access point (AP).



Important: Please read the EULA before installing W-318/W-318 RW. You can download and read the EULA from <https://www.arista.com/en/support/product-documentation>.

Installing the AP constitutes your acceptance of the terms and conditions of the EULA mentioned above in this document.

Intended Audience

This guide can be referred by anyone who wants to install and configure the W-318/W-318 RW access point.

Document Overview

This guide contains the following chapters:

- [Package Content](#)
- [Overview of the Access Point](#)
- [Install the Access Point](#)
- [Troubleshooting](#)



Note: All instances of the term 'server' in this document refer to the Wireless Manager, unless the server name or type is explicitly stated.







Product and Documentation Updates

To receive important news on product updates, please visit our website at <https://www.arista.com/en/support/product-documentation>. We continuously enhance our product documentation based on customer feedback.

Package Content

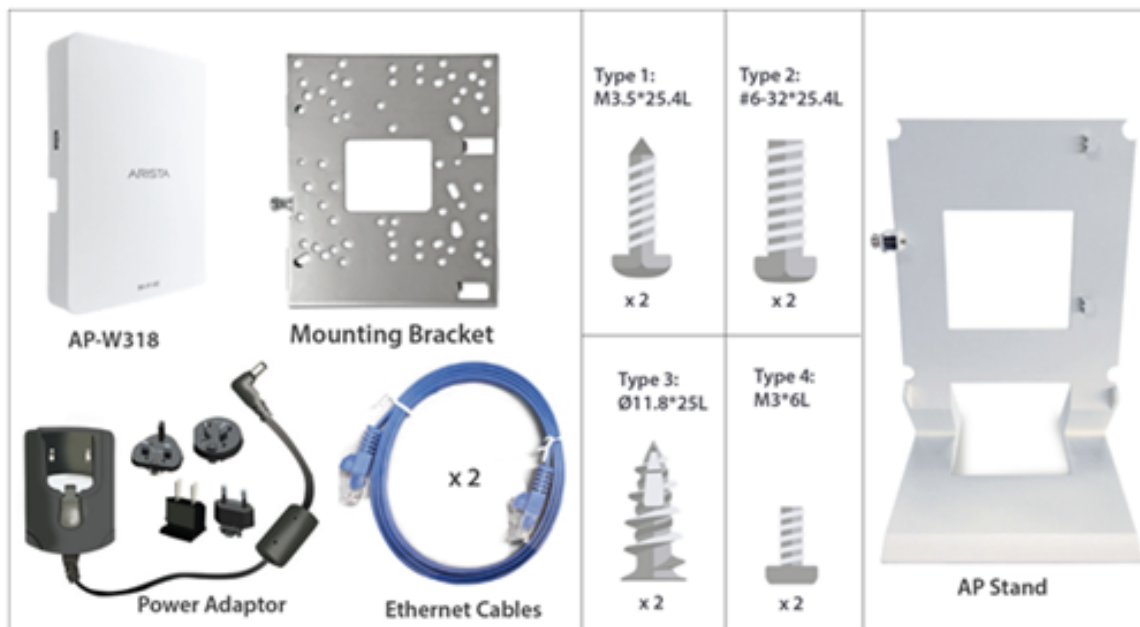
The W-318 package must contain the components shown in the following figure.

Figure 2-1: W-318 package content

 <p>ARISTA AP-W318</p>	<p>Type 1: M3.5*25.4L</p>  <p>x 2</p>	<p>Type 2: #6-32*25.4L</p>  <p>x 2</p>
 <p>Mounting Bracket</p>	<p>Type 3: Ø11.8*25L</p>  <p>x 2</p>	<p>Type 4: M3*6L</p>  <p>x 2</p>

The package content of W-318 RW access point includes an additional table mount stand, a power adaptor, and ethernet cables as shown in the following image:

Figure 2-2: W-318 RW package content with table mount stand



Important: The MAC address of the access point (AP) is printed on a label at the bottom of the product and the packaging box. Note the MAC address before mounting the AP on the wall or at a location that is difficult to access.

If the package is not complete, please contact the Arista Networks Technical Support Team at support-campus@arista.com, or return the package to the vendor or dealer where you purchased the product.

Overview of the Access Point

The W-318/W-318 RW access point (AP) is a 2x2:4 MU-MIMO, tri-band with multifunction radio, 802.11a/b/g/n/ac/ax access point.

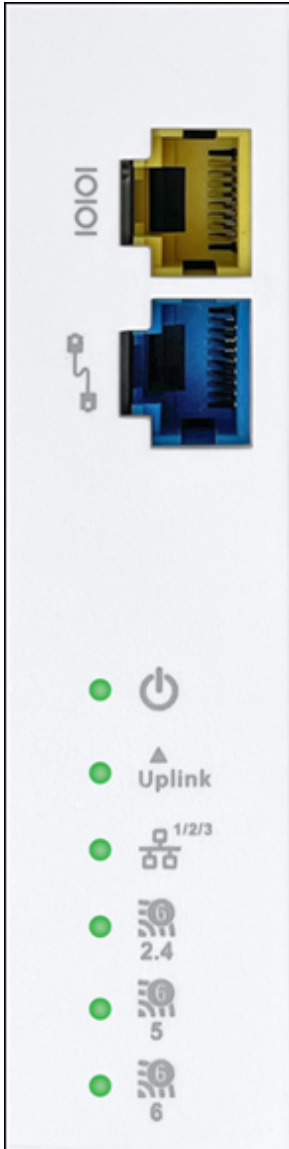
This chapter provides an overview of the AP and describes the following:

- [Right Panel of the AP](#)
- [Rear Panel of the AP](#)
- [Bottom Panel of the AP](#)

3.1 Right Panel of the Access Point

The right panel of the access point has 6 LEDs that indicate the functioning state of the device, one console port, and one passthrough port.

Figure 3-1: W-318/W-318 RW Right Panel



The following table describes the ports available on the right panel of the AP:

Table 1: Right Panel Ports and Description

Port	Description	Connector Type	Speed/Protocol
Console	Port to establish a 'config shell' terminal session via serial connection.	RJ-45	<ul style="list-style-type: none"> • RS 232 Serial (115200 bits per second) • Data bits:8; Stop bits: 1 • Parity: None • Flow Control: None
Passthrough	A wired port that facilitates extension of the wired network after the AP is mounted on the wall or stand. You can plug-in another device to the passthrough port of the AP. The traffic on the passthrough port does not interfere with the AP traffic. You cannot apply any policies on the passthrough port traffic.	Device connected through the Uplink port (Ethernet port) at 10/100/1000 Mbps	NA

The following table indicates the device states based on the LEDs.

Table 2: AP LED Status Description

LED	Status	Description
Power	Solid Green	Power ON
	OFF	Power OFF
Uplink	Solid Green	Device connected through the Uplink port (Ethernet port) at 10/100/1000 Mbps
	Blinking Green	Activity on the Uplink port
LAN1/2/3	Solid Green	Device connected to LAN port 1/2/3 on the bottom of the device at 10/100/1000 Mbps
2.4 GHz	Solid Green	No activity on 2.4 GHz radio
	Blinking Green	Wireless activity on 2.4 GHz radio
5 GHz	Solid Green	No activity on 5 GHz radio
	Blinking Green	Wireless activity on 5 GHz radio
6 GHz	Solid Green	No activity on 6 GHz radio
	Blinking Green	Wireless activity on 6 GHz radio

3.2 Rear Panel of the Access Point

The rear panel of the access point (AP) has an Ethernet port labeled Uplink that enables you to connect the AP to a wired LAN through a switch or a hub. The Uplink port powers the AP using the 802.3bt standard.

Figure 3-2: W-318/W-318 RW Rear Panel



Table 3: W-318/W-318 RW Rear Panel

Port	Description	Connector Type	Speed/Protocol
Passthrough	A wired port that facilitates extension of the wired network after the AP is mounted on the wall or stand. Another device can be plugged-in to the pass-through port of the AP. The traffic on the pass-through port does not interfere with the AP traffic. No policies can be applied on the pass-through port traffic.	RJ45	-
Uplink	Enables you to connect the AP to a wired LAN through a switch or a hub. The AP can then communicate with the server. This port also provides the power for the device using the 802.3bt standard	RJ45	10/100/1000 Mbps Power over Ethernet

3.3 Bottom Panel of the Access Point

The bottom panel of the access point and its corresponding ports are described below.

Figure 3-3: W-318/W-318 RW Bottom Panel

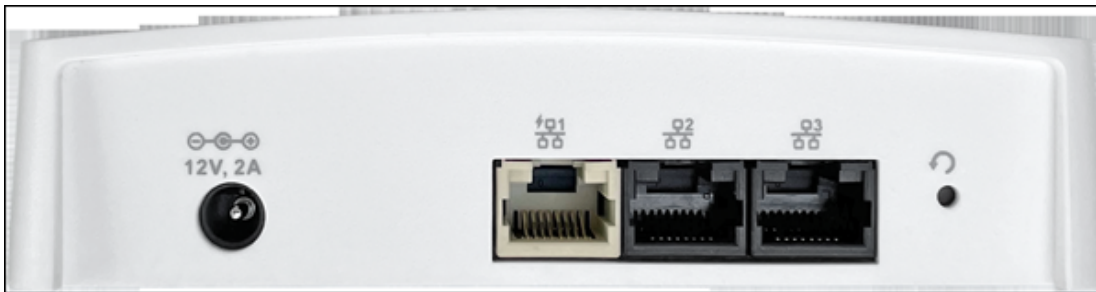


Table 4: W-318/W-318 RW Bottom Panel

Port	Description	Connector Type	Speed/Protocol
DC In	Enables you to connect to and power on the access point using 12 V DC power with 2 Ampere.	5.5mm overall diameter/2.1mm center pin/hole	NA
Ethernet (LAN1/PSE)	Gigabit Ethernet port that can be used for wired extension for an SSID. This Power Sourcing Equipment (PSE) port also provides the power to the connected device using the 802.3af standard.	RJ45	10/100/1000 Mbps Gigabit Ethernet
Ethernet (LAN2)	Gigabit Ethernet port that can be used for wired extension for an SSID.	RJ45	10/100/1000 Mbps Gigabit Ethernet
Ethernet (LAN3)	Gigabit Ethernet port that can be used for wired extension for an SSID.	RJ45	10/100/1000 Mbps Gigabit Ethernet
Reset	Resets the access point to factory defaults. To reset the access point, press and hold the Reset Pin Hole until all LEDs go off, which indicates that the access point has rebooted. Pressing the Reset Pin Hole while the access point is booting up will not have any effect. Perform this operation only when the access point is running.	Pin hole push button	Hold down and power cycle the access point to reset

Install the Access Point

This chapter explains the procedure to install the access point (AP).

Zero-Configuration of the Access Point

Zero-configuration is supported under the following conditions:

- The device is in the AP mode with background scanning ON and no SSID configured.
- The DNS entry, **wifi-security-server**, is configured on all the DNS servers. This entry must point to the IP address of the server. By default, the AP looks for the **wifi-security-server** DNS entry.
- The AP is on a subnet that is DHCP enabled.



Important: If the AP is on a network segment that is separated from the server by a firewall, you must first open the port 3851 for bidirectional User Datagram Protocol (UDP) and Transport Control Protocol (TCP) traffic on that firewall. This port number is assigned to Arista Networks. Zero-configuration cannot work if multiple APs are set up to connect to multiple servers. In this case, the APs must be configured manually. For details on how to configure an AP manually, see the Access Point Configuration Guide on our website at <https://www.arista.com/en/support/product-documentation>.

Take a configured AP; that is, ensure that a static IP is assigned to the AP or the settings have been changed for DHCP. Note the MAC address and the IP address of the AP in a safe place before it is installed in a hard-to-reach location. The MAC address of the AP is printed on a label at the bottom of the product.

The steps to install the AP with no configuration (zero-configuration) are as follows:

1. [Mount the AP](#)
2. [Connect the AP to the network](#)
3. [Power ON the AP](#)

4.1 Mount the Access Point

You can place the W-318 AP on a wall or on a table depending on your requirements.

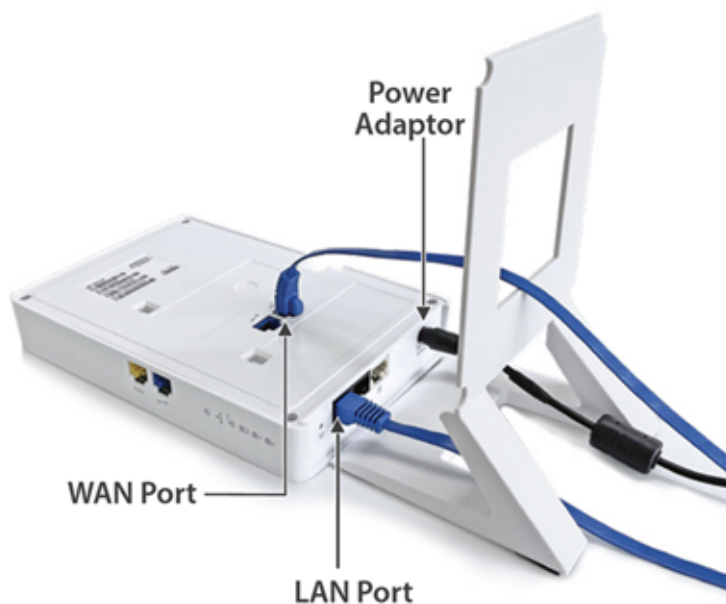
- [Table Mount the Access Point](#)
- [Wall Mount the Access Point](#)

4.1.1 Table Mount the Access Point

Use the following steps to table mount the access point:

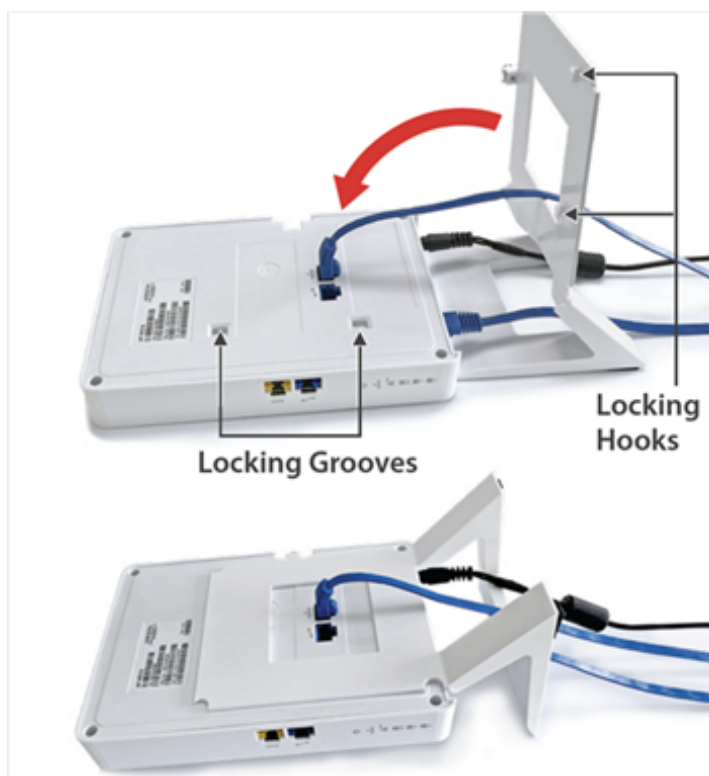
1. Plug the network cable (Ethernet cable) into the WAN port (PoE++) located at the back of the AP as shown below. If the network is not PoE enabled, plug the Power Adaptor at the DC Input port, as shown.

Figure 4-1: Attach cables to AP



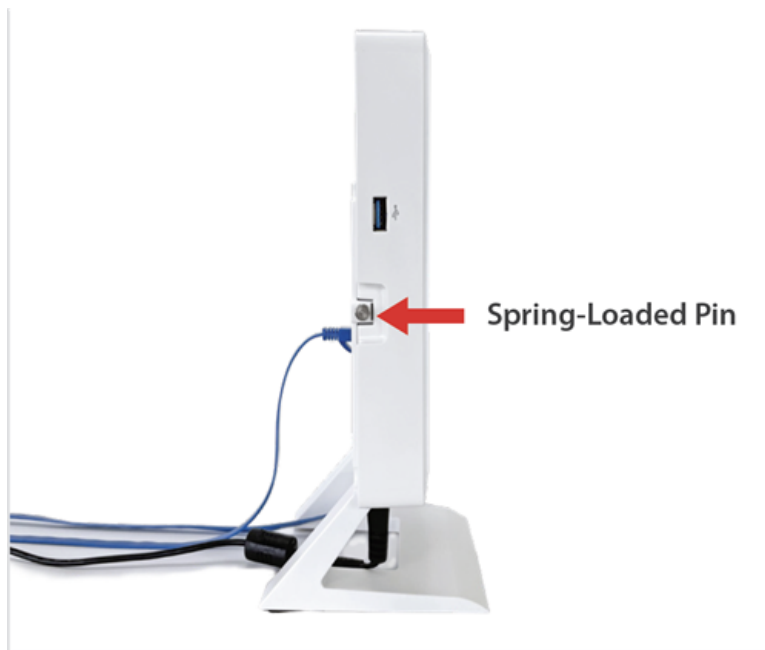
2. Flip the stand on the AP as shown, aligning the hooks on the stand to the grooves on the AP. Slide the hooks into the grooves to attach the AP to the stand.

Figure 4-2: Attach stand to AP



3. The spring-loaded pin will automatically lock into the locking hole of the AP. If the pin is not aligned, pull the pin and align it to the locking hole. **Note:** To remove the AP from the stand, pull the pin and then remove the AP.

Figure 4-3: Image showing the spring-loaded pin



Use LAN 1, LAN 2, and LAN 3 ports at the bottom of the AP to connect to local devices.

4.1.2 Wall Mount the Access Point



Note: The wall mounting accessory SKU (MNT-AP-FLAT-14CM) can be ordered and purchased separately.

For instructions on wall mounting the access point, refer to [Wall Mount the Access Point](#) article.

4.2 Connect the Access Point to the Network

To connect the access point (AP) to the network, perform the following steps:

1. Ensure that a DHCP server is available on the network to enable network configuration of the AP.
2. Add the DNS entry **wifi-security-server** on all DNS servers. This entry should point to the IP address of the server.
3. Ensure that DHCP is running on the subnet to which the AP will be connected.
4. Check the status LEDs on the AP. If all LEDs glow green, then the AP is operational and connected to the server.
5. Log on to the server using ssh and run the get sensor list command.

You will see a list of all Arista devices that are recognized by the server. Single Sign-On users can go to the **MONITOR > WiFi > Access Points** tab in CloudVision Cognitive Unified Edge and check whether the AP is visible under the **Access Points** tab.

The AP is connected and operational.



Note: If the zero configuration is not successful, you must configure the AP manually.



Important: If DHCP is not enabled on a subnet, the AP cannot connect to that subnet with zero-configuration. If the DNS entry is not present on the DNS servers or if you do not have the DHCP server running on the subnet, you must manually configure the device. See the Access Point Configuration guide at <https://www.arista.com/en/support/product-documentation>.

4.2.1 Connect the Access Point Using PoE

If you are using a PoE injector, make sure one of the connectors is plugged into the Uplink port of the AP and the other end is plugged into a suitable switch port with proper network connectivity.

Figure 4-4: Back panel of the AP showing the network ports



4.3 Power On the Access Point

You can power-on the access point (AP) by plugging one end of the Ethernet cable into the PoE (802.3af) switch or injector, and the other end into the Ethernet/PoE port on the AP. Ensure the PoE source you are using is turned ON.

As an alternative to PoE, you can insert a compatible power adapter plug into an AC power outlet and the other end into the power input port on the AP.



Note: If you are not using PoE, ensure that you use only an AC power adapter supported by the AP.

4.3.1 Using the Access Point with Power Adapter

To power-on the access point (AP) with a power adapter, perform the following steps:

1. Plug the power cable into the DC power receptacle at the rear of the AP.
2. Plug the other end of the power cable into an 110V~240V 50/60 Hz AC power source.
3. Wait until the LED lights on the AP are lit. Refer to the LED details table.

Access Point Troubleshooting

The table below lists some of the troubleshooting guidelines for the access point (AP).

Problem	Solution
The AP did not receive a valid IP address via the DHCP.	Ensure that the DHCP server is on and available on the VLAN/subnet to which the AP is connected. If the AP still fails to get a valid IP address, you can reboot it to see if the problem is resolved.
Unable to connect to the server.	<ul style="list-style-type: none"> • Ensure that the server is running and is reachable from the network to which the AP is connected. If a firewall or a router has Access Control Lists (ACLs) enabled between the AP and the server, ensure that traffic on UDP port 3851 is allowed. • Use the IP-based server discovery method and ensure that you have correctly entered the DNS name, wifi-security-server, on the DNS server. • Ensure that the DNS server IP addresses are either correctly configured, or are provided by the DHCP server. • The AP might fail to authenticate with the server. In this case, an 'Authentication failed' event is raised on the server. Refer to the event for recommended action.
The AP has encountered a problem.	<ul style="list-style-type: none"> • If you are using Arista Cloud Services, then open the TCP port 443 (SSL). If you have an on-premises installation, then open UDP port 3851 and port 80. • If you are using a Proxy, Web Accelerator, or URL Content Filter between the AP and the Internet, ensure that the settings allow communication between the AP and Arista Cloud Services. • If your configuration requires you to specify an exact IP address or IP range for Arista Cloud Services, please contact http://support-wifi@arista.com.

Appendix A: AP-Server Mutual Authentication

The AP-server communication begins with a mutual authentication step in which the AP and server authenticate each other using a shared secret. The AP-server communication takes place only if this authentication succeeds.

After the authentication succeeds, a session key is generated. From this point on, all communication between the AP and server is encrypted using the session key.

The AP and server are shipped with the same default value of the shared secret. Both the server and the AP have CLI commands to change the shared secret.



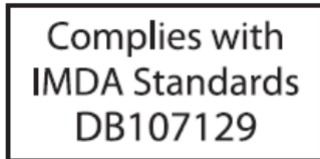
Note: After the shared secret (communication key) is changed on the server, all APs connected to the server will automatically be set up to use the new communication key. You must manually configure the new communication key on an AP if it is not connected to the server when the key is changed on the server.



Note: Although the server is backward compatible—that is, older version APs can connect to a newer version server—this is not recommended.

Appendix B: Product Compliance

Singapore IMDA Registration Mark



Appendix C: Regulatory Model Numbers

This appendix lists the Regulatory Model Numbers(RMN), where applicable, for the product models for the Access Points described in the document.

Table 5:

Regulatory Model Number (RMN)	Product Number
W-318	AP-W318
W-318	AP-W-318-RW