Quick Start Guide

W-118 Access Point

Arista Networks

www.arista.com

DOC-03485-01

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	support-wifi@arista.com	sales@arista.com

Chapter 1. About This Guide

This installation guide explains how to deploy the W-118 access point (AP).

Important: Please read the EULA before installing W-118. 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-118 access point.

Document Overview

This guide contains the following chapters:

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

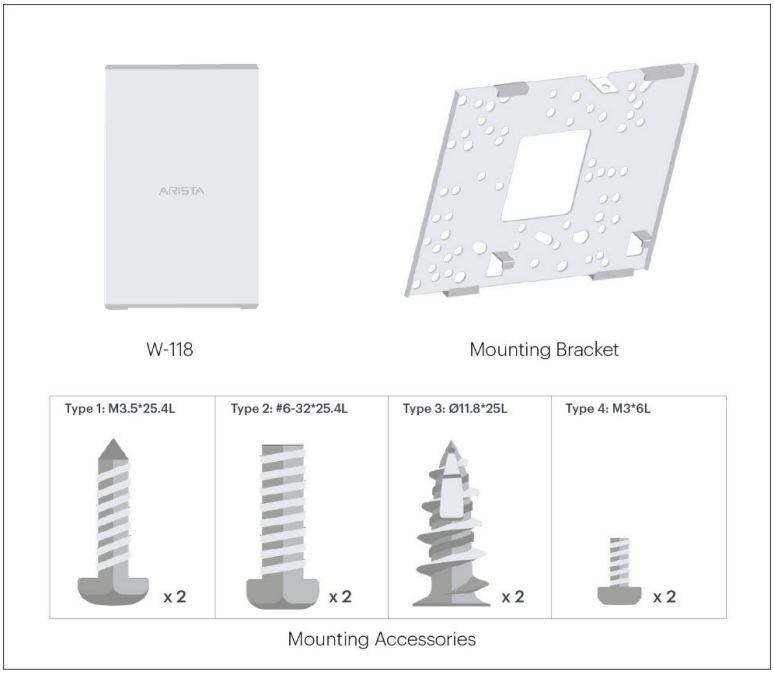
Product and Documentation Updates

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.

Chapter 2. Package Content

The W-118 package must contain the components shown in the figure below.

Figure: W-118 Mounting Accessories



⚠ **Important:** The MAC address of the device is printed on a label at the bottom of the product and the packaging box. Note down the MAC address, before mounting the device on the ceiling 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-wifi@arista.com, or return the package to the vendor or dealer where you purchased the product.

Chapter 3. W-118 Overview

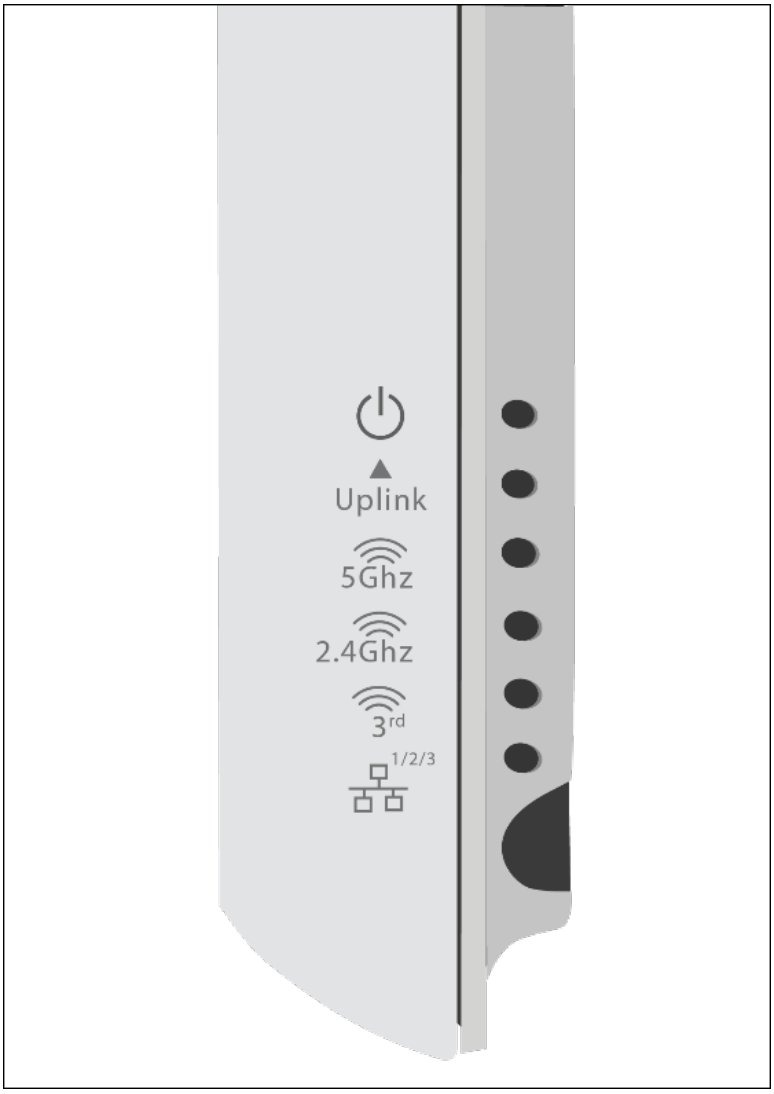
W-118 is a 2x2 MU-MIMO tri-radio 802.11a/b/g/n/ac access point.

This chapter provides an overview of the W-118 and describes:

Right Panel of W-118

The right panel of the W-118 has 6 LEDs that indicate the functioning state of the device.

Figure: W-118 Right Panel



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

Table 1. W-118 LED Status Description

LED	Status	Description
Power	Solid Green	Power ON
	OFF	Power OFF
Uplink	Solid Green	Device connected through WAN port (Ethernet port) at 10/100/1000 Mbps
	Blinking Green	Activity on WAN port
5 GHz	Solid Green	No activity on 5 GHz radio
	Blinking Green	Wireless activity on 5 GHz radio

LED	Status	Description
2.4 GHz	Solid Green	No activity on 2.4 GHz radio
	Blinking Green	Wireless activity on 2.4 GHz radio
Radio 3	Blinking Green	Activity on third radio
LAN1/2/3	Solid Green	Device connected to LAN port 1/2/3 on the bottom of the device at 10/100/1000 Mbps

Rear Panel of W-118

The rear panel of the W-118 has an Ethernet port labeled WAN, that enables you to connect the device to a wired LAN through a switch or a hub and provides the power for the device by using the 802.3af standard.

Figure: W-118 Rear Panel

Table 2. W-118 Rear Panel

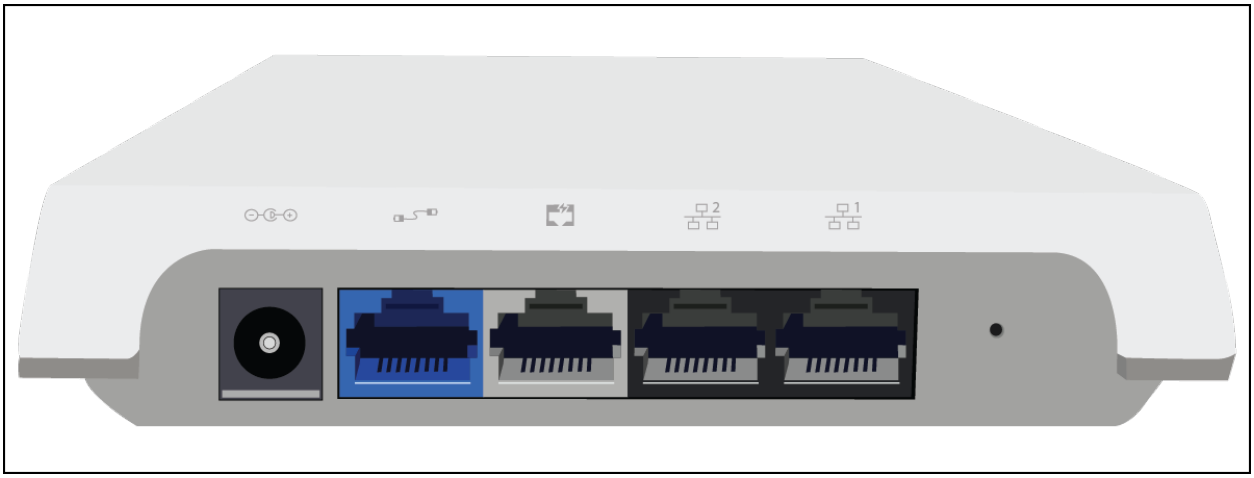
Port	Description	Connector Type	Speed/Protocol
PASSTHROUGH	This is a wired port that facilitates extension of the wired network after the AP is mounted on the wall. Another device can be plugged in to the pass-through port on the bottom of the W-118 device. The traffic on the pass-through port does not interfere with the AP traffic. No policies can be applied on the pass-through port traffic.	RJ45	-

WAN	Enables you to connect the device to a wired LAN through a switch or a hub. The device can then communicate with the server. This port also provides the power for the device using the 802.3af standard	RJ45	10/100/1000 Mbps Ethernet Power over Ethernet

Bottom Panel of W-118

The bottom panel of W-118 and its corresponding ports are described below.

Figure: W-118 Bottom Panel



Port	Description	Connector Type	Speed/Protocol
DC IN	Enables you to connect to and power on device using 12 V DC power with 2 ampere.	5.5mm overall diameter/2.1mm center pin/ hole	--
Pass-through port	The pass-through port is used to plug in a device into another wired port that is available on the wall where the AP is installed. The pass-through port at the rear of the device and pass-through port on the bottom of the device are internally connected.	RJ45	--
Ethernet (LAN3/PSE)	Gigabit Ethernet port that can be used for wired extension for an SSID. This port also provides the power for the 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 (LAN1)	Gigabit Ethernet port that can be used for wired extension for an SSID.	RJ45	10/100/1000 Mbps Gigabit Ethernet
Reset	Resets the W-118 device to factory defaults. To reset the device, press and hold the Reset Pin Hole until all LEDs go off which indicates that the device has rebooted. Pressing the Reset Pin Hole while the device is booting up will not have any effect. You should perform this operation only when the device is running.	Pin hole push button	Hold down and power cycle the device to reset

When you reset the device, the following settings are reset:

- Config shell password is reset to **config**.
- Server discovery value is erased and changed to the default, **wifi-security-server**.
- All the VLAN configurations are lost.
- If static IP is configured on the device, the IP address is erased and DHCP mode is set. The factory default IP address of the device is 169.254.11.74.

Chapter 4. Install the W-118

This chapter contains the stepwise procedure to install the W-118 device.

Zero-Configuration of W-118 as Access Point

Zero-configuration is supported under the following conditions:

- The device has no SSID configured.
- A DNS entry **wifi-security-server** is set up on all the DNS servers. This entry should point to the IP address of the server. By default, the device looks for the DNS entry **wifi-security-server**.
- The device is placed on a subnet that is DHCP enabled.

Important: If the device is placed on a network segment that is separated from the server by a firewall, you must first open port 3851 for User Datagram Protocol (UDP) and Transport Control Protocol (TCP) bidirectional traffic on that firewall. This port number is assigned to Arista Networks. If multiple devices are set up to connect to multiple servers, zero-configuration is not possible. In this case, you must manually configure the APs. See the Access Point Configuration Guide on our website at https://www.arista.com/en/support/product-documentation .

Take a configured W-118, that is, ensure that a static IP is assigned to the device or the settings have been changed for DHCP. Note down the MAC address and the IP address of the device in a safe place before it is installed in a hard-to-reach location. The MAC address of the device is printed on a label at the bottom of the product.

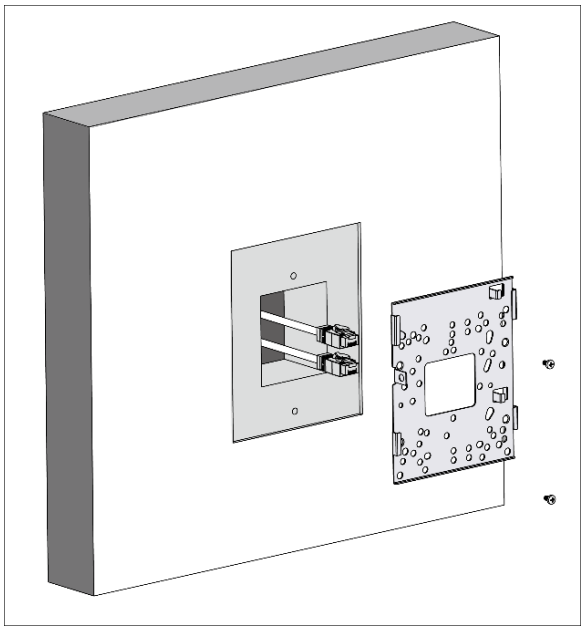
The steps to install the device with no configuration (zero-configuration) are as follows:

1. Mount the device. *(page 11)*
2. Power On the device. *(page 14)*
3. Connect device to the network. *(page 15)*

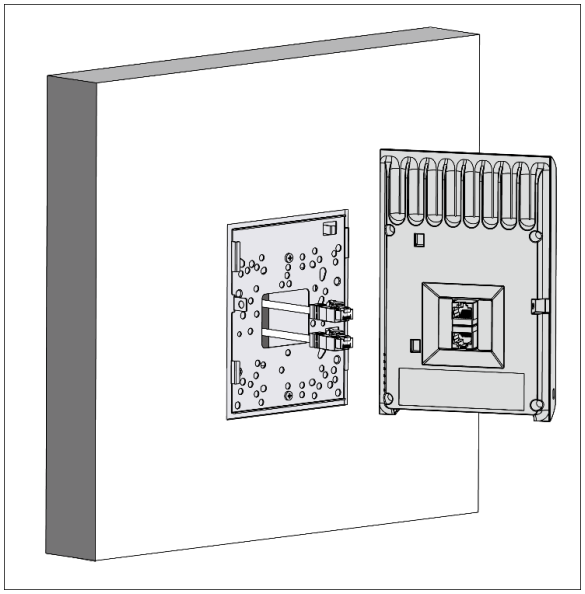
Mount the W-118

The steps to mount the W-118 are as follows:

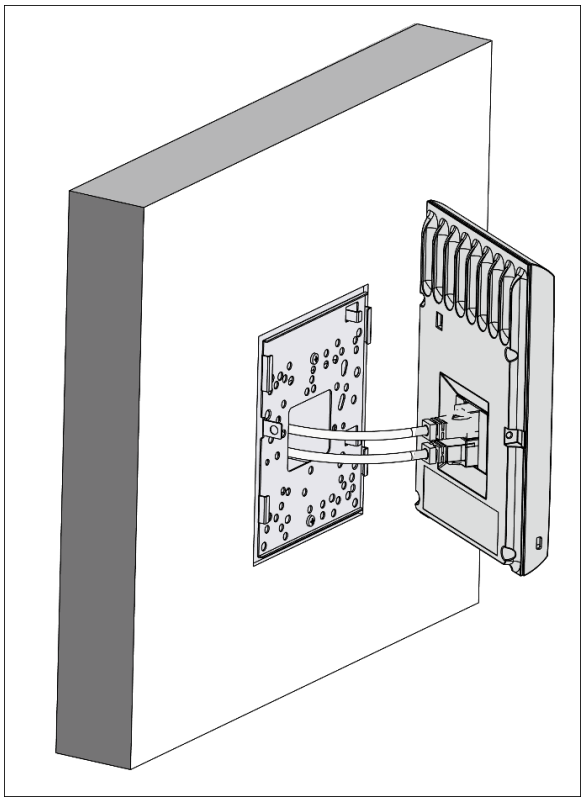
1. Attach the mounting bracket to the wall by using the mounting hardware kit as shown in the image below.



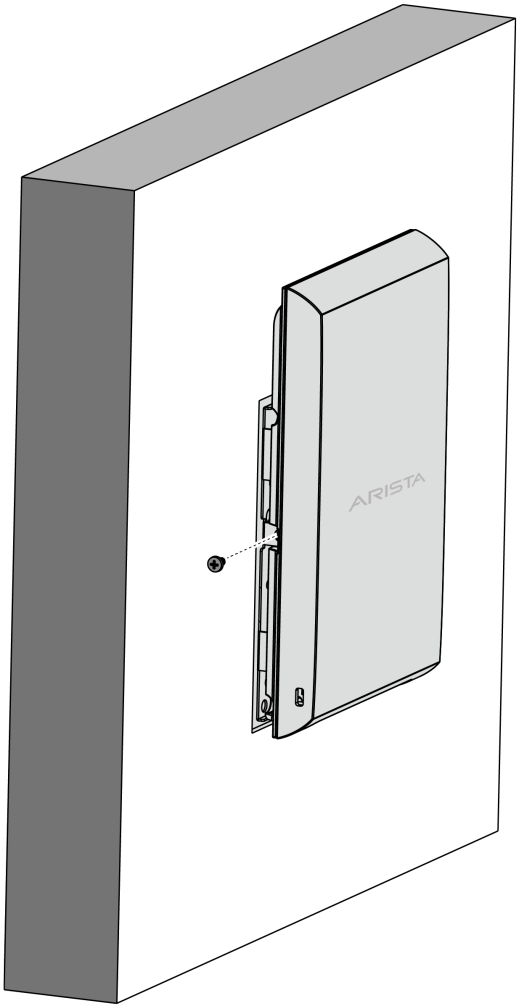
2. Affix the mounting bracket on to the wall using the appropriate screws from the mounting accessories included in the package.



3. Connect the cables to the appropriate ports in the rear-side of the device.



4. Mount the device on the bracket by aligning the two notches on the bracket with the two grooves on the rear panel of the device. Slide the device and tighten it onto the bracket with the screw provided in the package.



Important: To prevent disconnection or tampering by unauthorized personnel, it is extremely important to install the device such that it is difficult to unplug the device from the network or from the power outlet.

Note: You should label the devices using MAC addresses or at least your own convention. For example, use serial numbers, so that you can easily identify the devices.

Power On the W-118

The W-118 device can be powered on 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 W-118. Ensure the PoE source you are using is turned ON.

As an alternative to PoE, you can insert a compatible power adaptor plug into an AC power outlet and the other end into the power input port on the W-118.

Note: If you are not using PoE, ensure that you use only an AC power adaptor supported by the W-118 access point (AP).

Using the W-118 with Power Adapter

To power up the device with power adapter, perform the following steps:

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

Connect the W-118 to the Network

To connect W-118 to the network, perform the following steps:

1. Ensure that a DHCP server is available on the network to enable network configuration of the W-118.
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 device will be connected.
4. Check the status LEDs on the device. If all LEDs glow green, then the device 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 **Devices** tab in Wireless Manager and check whether the device is visible under the **Devices** tab.

The device is connected and ready to go operational.

Note: If the zero configuration is not successful, the device must be configured manually.

Important: If DHCP is not enabled on a subnet, the device 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 on our website at https://www.arista.com/en/support/product-documentation .

Connect the W-118 using PoE

If you are using a PoE injector, make sure the data connection is plugged into a suitable switch port with proper network connectivity.

Chapter 5. W-118 Troubleshooting

The table below lists some of the troubleshooting guidelines for W-118.

Diagnosis	Solution
The device 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 device is connected. If the device still fails to get a valid IP address, you can reboot it to see if the problem is resolved.
The Ethernet cable is loose. The device is probably disconnected from the network.	Ensure that the Ethernet cable is connected.
Unable to connect to the server.	Ensure that the server is running and is reachable from the network to which the device is attached. If there is a firewall or a router with ACLs enabled between the device and the server, ensure that the traffic is allowed on UDP port 3851. Use the server IP-based discovery and ensure that you have correctly entered the DNS name, **wifi-security-server** , on the DNS server. Also, ensure that the DNS server IP addresses are either correctly configured on the, or are provided by the DHCP server. It is also possible that the AP is unable to connect to the server because it has failed to authenticate with the server. In this case, an 'Authentication failed for ' event is raised on the server. Refer to the event for recommended action.
The AP has encountered a problem.	If you are using Arista Cloud Services, then open the TCP port 443 (SSL). If you have an on-premises installation, then open the ports UDP 3851 and port 80. If you are using a Proxy, Web Accelerator or URL Content Filter in between the AP and the Internet, ensure 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 Technical Support at support-wifi@arista.com.

Chapter 6. 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. All communication between the AP and server from this point on is encrypted using the session key.

The AP and server are shipped with the same default value of the shared secret. The CLI commands are provided on both server and AP for changing 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. APs that are not connected to the server at this time must be manually set up with the same communication key to enable communication with this server.

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