Technical Document

JACE-9000 Wi-Fi Guide

February 26, 2025

niagara4

Legal Notice

Tridium, Incorporated

3951 Western Parkway, Suite 350

Richmond, Virginia 23233

U.S.A.

Confidentiality

The information contained in this document is confidential information of Tridium, Inc., a Delaware corporation (Tridium). Such information and the software described herein, is furnished under a license agreement and may be used only in accordance with that agreement.

The information contained in this document is provided solely for use by Tridium employees, licensees, and system owners; and, except as permitted under the below copyright notice, is not to be released to, or reproduced for, anyone else.

While every effort has been made to assure the accuracy of this document, Tridium is not responsible for damages of any kind, including without limitation consequential damages, arising from the application of the information contained herein. Information and specifications published here are current as of the date of this publication and are subject to change without notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia.

Trademark notice

BACnet and ASHRAE are registered trademarks of American Society of Heating, Refrigerating and Air-Conditioning Engineers. Microsoft, Excel, Internet Explorer, Windows, Windows Vista, Windows Server, and SQL Server are registered trademarks of Microsoft Corporation. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Mozilla and Firefox are trademarks of the Mozilla Foundation. Echelon, LON, LonMark, LonTalk, and LonWorks are registered trademarks of Echelon Corporation. Tridium, JACE, Niagara Framework, and Sedona Framework are registered trademarks, and Workbench are trademarks of Tridium Inc. All other product names and services mentioned in this publication that are known to be trademarks, registered trademarks, or service marks are the property of their respective owners.

Copyright and patent notice

Contents

About This Guide

This topic contains important information about the purpose, content, context, and intended audience for this document.

Product Documentation

This document is part of the Niagara technical documentation library. Released versions of Niagara software include a complete collection of technical information that is provided in both online help and PDF format. The information in this document is written primarily for Systems Integrators. To make the most of the information in this book, readers should have some training or previous experience with Niagara software, as well as experience working with JACE network controllers.

Document Content

This document provides basic information about configuring Wi-Fi options on the JACE-9000. Included in this document is a topic overview, as well as descriptions of requirements, operation notes, and configuration instructions for the WLAN-enabled models: North America, European Union or other regions (world wide). See Regions, SKUs, and Country Codes for related details.

This guide is intended for developers, systems engineers, and facility managers.

Document Change Log

This log provides the date this document was released and lists any subsequent document updates that have occurred.

February 26, 2025

- Initial release publication.

Related Documentation

Additional information is available in the following documents.

- *JACE–9000 (15885) Mounting and Wiring Guide*
- *JACE-9000 Install and Startup Guide*
- *JACE-9000 Backup and Restore Guide*

Chapter 1. Overview

Some models of the JACE-9000 platform feature an integrated IEEE 802.11 module for enabling wireless Ethernet communications to or from the platform. Both Client mode and Access Point mode are supported, however, the device cannot operate in both modes simultaneously.

WLAN/Wi-Fi Terms and Definitions

The following terms are important for understanding, configuring, and working with the capabilities of your specific JACE-9000 Wi-Fi features.

Term	Definition
Country Code	A two-letter code that represents the country where the Wi-Fi device is operating. It dictates the permissible channels and power levels for wireless transmission in that country.
Channel	A specific frequency within a frequency band that Wi-Fi devices use to communicate. Channels are typically designated by a number and can overlap with other channels in use.
Frequency	The specific electromagnetic wave frequency (measured in Hertz, MHz, or GHz) on which Wi-Fi signals are transmitted. Common frequencies for Wi-Fi are 2.4 GHz and 5 GHz.
Band	A range of frequencies used for wireless communication. Common Wi-Fi bands are the 2.4 GHz band (which has channels like 1 to 14) and the 5 GHz band (offering more channels and bandwidth).

Regions, SKUs, and Country Codes

It is important to understand the differences and relationships between a SKU, Region, and Country Code (CC) as they relate to the Wi-Fi capabilities and options on a JACE-9000.

NOTE: You cannot change the CC assigned to your JACE-9000 when your SKU is either US or EU. If your SKU is WW you can edit the CC from the system shell menu.

For JACE-9000 WLAN capability, a SKU code is used to identify and differentiate the controller WLAN capability based on regional requirements rather than strictly by CC. Grouping the CCs into regions helps to optimize the number of SKUs and reduce required configuration. So, for example, the Country Codes for both Canada and United States are in the "North America" Region which is identified by the SKU "US". As noted in the table below, CCs in this Region/SKU cannot be changed. However, CCs for Australia, New Zealand, and many other countries are in the "WW" SKU represented by the region "Rest of the world". Any Wi-Fi controller that is assigned a "WW" SKU has an editable CC that can be changed using the system shell menu.

The following table shows codes for all regions and some countries. SKU codes may be one of four options, as listed in the "SKU" column. Note that the "XX" SKU indicates that Wi-Fi is not supported on the controller.

Table 1.   Regions, SKUs, and Country Codes

Region	SKU	Country Code (CC)	CC Editable? YES/NO
North America	US	US - United States CA - Canada	NO
European Union	EU	CH - Switzerland GB - United Kingdom FR - France IT - Italy CZ - Czech Republic IE - Ireland ES - Spain NL - Netherlands DE - Germany	NO
Rest of the world	WW	AU - Australia NZ - New Zealand	Use a serial shell connection or Niagara workbench UI
No WLAN support	XX	CC is not applicable.	WLAN is not supported on this controller. There is no configuration option.

Channels supported by country

Refer to the following table for a list of channels that each country supports. Countries are listed by country code (CC).

Table 2. 2.4 GHZ frequency

SKU	Countries	Supported Channels indicated by '•'													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
US	CA – Canada US – Unitied States	•	•	•	•	•	•	•	•	•	•	•			
EU	CH – Switzerland GB – United Kingdom FR – France DK – Denmark IT – Italy IE – Ireland CZ – Czech Republic ES – Spain NL – Netherlands DE – Germany	•	•	•	•	•	•	•	•	•	•	•	•	•	
WW	AU – Australia NZ – New Zealand	•	•	•	•	•	•	•	•	•	•	•	•	•	•

Table 3. 5GHZ frequency

SKU	Countries	Supported Channels indicated by '•'				DFS					
		36	40	44	48	52 - 144	149	153	157	161	165
US	US – United States CA – Canada	•	•	•	•	•	•	•	•	•	•
EU	CH – Switzerland GB – United Kingdom FR – France DK – Denmark IT – Italy IE – Ireland CZ – Czech Republic ES – Spain NL – Netherlands DE – Germany	•	•	•	•	•	•	•	•	•	•
WW	AU – Australia	•	•	•	•	•	•	•	•	•	•
	NZ – New Zealand	•	•	•	•	•	•	•	•	•	•

JACE-9000 Wi-Fi Specifications

This topic covers JACE-9000 WLAN (Wi-Fi) specifications.

Disabled by default, the Wi-Fi option (on factory configured WLAN-enabled models) can be enabled and configured to attach as a Client to an already established IEEE 802.11 access point and network, or configured as an Access Point to establish a new network. In addition, when configured as an Access Point, the controller can be set to "Off" or one of three active modes - using the `Switch Position` property in Workbench. Refer to the WiFi Configuration topic for more details about configuration options.

NOTE: Dynamic Frequency Selection (DFS) channels are not supported.

Following is a list of basic Wi-Fi specifications that apply to the JACE-9000:

- Supports Wi-Fi 5 (802.11ac)
- Supports IEEE 802.11a/b/g/n/ac networks
- Configurable radio with the following settings: (OFF, WAP/Controlled Access Point, Client)
- Supports WPA-PSK, WPA2-PSK security protocols

  NOTE: The JACE-9000 does not support enterprise-level authentication (such as WPA2-enterprise), WEP authentication, or using no authentication at all.
- Supports 2.4 or 5.8 GHz frequencies
  - 2.4 GHz channels: 1–11
  - 5.8 GHz channels: 36, 40, 44, 48,149, 153, 157, 161, and 165.
- Single dual band 2.4/5.8 GHz antenna. The antenna may be remotely located using an extension cable.
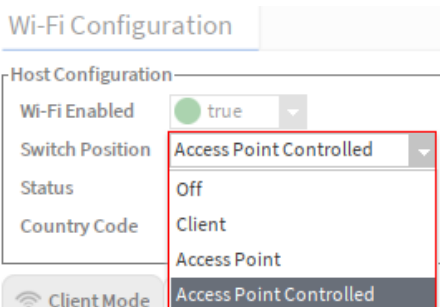
Wi-Fi modes and states - JACE-9000

The following topics describe the modes, states, and properties that are important for setting up and configuring the JACE-9000 Wi-Fi.

JACE-9000 Wi-Fi modes

The controller Wi-Fi service functions as either a Client or as an Access Point (one or the other but not simultaneously). Within these two categories of operation there are four basic modes for Wi-Fi on the JACE-9000. Select the desired mode using the `Switch Position` drop-down list in the Wi-Fi Configuration view of Workbench or by using the system shell menu using a serial terminal connection.

Figure 1. Select Wi-Fi mode

Wi-Fi mode configuration options:

Off
Disables Wi-Fi activity.

Client
Sets the controller Wi-Fi service to Client mode.

Access Point
Configures the Wi-Fi service to function as an `Access Point`.

Access Point Controlled
Sets Wi-Fi service to operate in the `Access Point Controlled` mode.

About `Access Point Controlled`

When `Access Point Controlled` mode is chosen, the mode status is indicated by the `Status` property value in the **Wi-Fi Configuration** view and by the led on front of the controller. The default `Status` value is `Stopped` with led color blinking steady green. You can change to a running status by pressing the Wi-Fi button to toggle `Status` to `Access Point Running` and a steady green light (no blinking). This `Access Point Running` status enables the use of an inactivity time limit for access point availability. Selecting this mode activates a configurable time limit property for inactivity as well as the use of the Wi-Fi button to continue to toggle on or off the Access Point availability while in this mode. Use this mode for convenience and to improve security by limiting the amount of time that your controller is available as an access point.

JACE-9000 Wi-Fi states

Wi-Fi **states** are visible in the **Wi-Fi Configuration** view as a **Status** value. They reflect the status of the Wi-Fi and include information relative to the mode that is currently running. Some examples of status values include the following:

- Stopped
- Client Running
- Client Trying to Associate
- Access Point Running
- Access Point Inactivity Timeout

Following are some common, expected statuses that you may see, following a reboot or an Access Point Timeout:

- Inactivity Timeout followed by Reboot: status=Stopped
- Inactivity Timeout expired: status=Access Point Inactivity Timeout
- Access Point Running followed by Reboot: status=Stopped

JACE-9000 Wi-Fi controls and indicators

There are three physical Wi-Fi related items on a JACE-9000 that has Wi-Fi capability: the Wi-Fi button, the Wi-Fi LED, and the Antenna.

Figure 2. JACE-9000 Wi-Fi controls and led indicator light
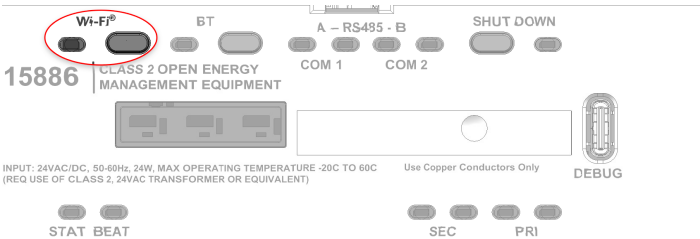
Wi-Fi button

The Wi-Fi button is located on the controller front panel. The button is functional only when the Wi-Fi service is configured to operate in `Controlled Access Point` mode. When this mode is active, pressing the button toggles the Access Point state between "Access Point Running" and "Stopped". See JACE-9000 Wi-Fi modes for more details about configuring modes.

Wi-Fi LED indicator light

The Wi-Fi LED is located on the controller front panel. The light blink patterns indicate the status of the Wi-Fi service. The following table shows led color and blink pattern for different states.

Table 4. LED mode and status indicators

| Color	Blink pattern	Mode	Status (state)
Green	Blinking (ON: 0.5 sec / OFF: 1.0 sec)	Access Point or Controlled Access Point	Stopped (access point is not running)
Green	ON (not blinking)	Access Point or Controlled Access Point	Running (access point is available)
Green	Blinking (ON: 0.1 sec / OFF: 2 sec)	Access Point or Controlled Access Point	Inactive (no client connected)
Green	Blinking (ON: 0.2 sec / OFF 0.2 sec / ON: 0.2 sec / OFF: 3.0 sec)	Access Point or Controlled Access Point	Wi-Fi Error
Yellow	Blinking (ON: 0.5 sec / OFF: 1.0 sec)	Client	Stopped or Disconnected: Client mode configured but not connected to a wireless network
Yellow	ON (not blinking)	Client	Client mode configured and connected to a wireless network
Yellow	on for 0.1 sec, off for 0.1 sec	Client	Client mode is scanning for an access point. Check status of targeted access point network.
Yellow	Blinking (ON: 0.2 sec / OFF 0.2 sec / ON: 0.2 sec / OFF: 3.0 sec)	Client	Wi-Fi Error

Antenna

The antenna has no user configurable features or displays. It must be installed for proper Wi-Fi operation. It is attached to the bottom of the JACE-9000 unit and is adjustable by hand. No tools are required for installation or adjustment.

Figure 3. JACE-9000 Wi-Fi antenna
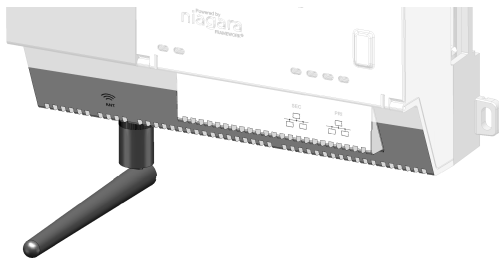
Chapter 2. Configuring JACE-9000 Wi-Fi

The following procedures describe how to enable and configure the JACE-9000 Wi-Fi adapter to operate in Access Point mode, Access Point Controlled mode, and Client mode. Also covered are instructions on how to discover, add, and connect to available access point networks.

You can configure WLAN communications using the platform **Wi-Fi Configuration** view in Workbench. Connect to (login) your desired target platform, right-click on the platform icon and choose **Views** > **Wi-Fi Configuration** from the popup menu. The **Wi-Fi Configuration** view displays.
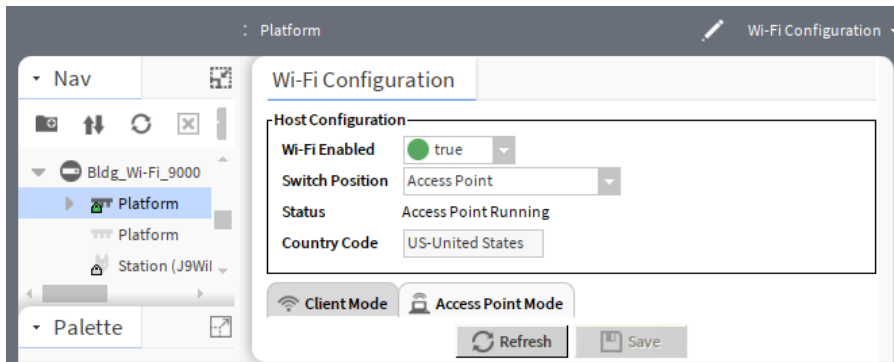
Configure a JACE-9000 as Wi-Fi Access Point or Access Point Controlled

This procedure describes the steps to configure the JACE-9000 Wi-Fi subsystem to run in Access Point mode or in Access Point Controlled mode. This configuration can be used either as a network for Wi-Fi enabled field bus devices, or to provide browser or Workbench access to local tools.

Prerequisites:

- The controller has a SKU and Country Code that supports Wi-Fi. For more details, see "Regions, SKUs, and Country Codes".
- The controller is licensed and commissioned
- You are connected to the the JACE platform.

CAUTION: When enabling more than one LAN port (applies to LAN1, LAN2, Wi-Fi) the IP address for each must be configured on different subnets, otherwise the ports will not function correctly.

NOTE: The controller can only operate in one mode at a time. For example, a controller in Access Point mode cannot also operate as a Client at the same time.

Any changes to the Wi-Fi Configuration, including enabling or disabling Wi-Fi, require a controller reboot after saving changes.

In the following steps, a reboot prompt appears any time you save a change to a property value. In order to save time, you can choose to not save until you make final changes in the **Wi-Fi Configuration** view.

Step 1. From the **Wi-Fi Configuration** view, click the **Access Point Mode** tab and set the `Adapter IPv4 Address` and/or `Adapter IPv4 Netmask` values, as needed.
This sets the address that a client uses to make an IP connection to this unit over Wi-Fi while the unit is functioning as an access point.

NOTE: The IP address and subnet must not conflict with IP addresses used for wired Ethernet connections.

Step 2. In the **Access Point Configuration** area, find the `SSID` field and enter a name for this access point. A best practice is to replace the default name with a unique, meaningful network name.

   a. Click the `Broadcast SSID` checkbox *only* if configuring the Access Point for field bus devices so that the devices can detect the access point signal and connect as needed. Otherwise, for security purposes do not click the checkbox.

Step 3. Enter a `Passphrase` for the unit (10 character minimum).
This sets an access word or phrase that a client must enter to connect to this network.

Step 4. Click the `Wpa Mode` dropdown list and select the preferred mode. WPA WPA2 (default) will accommodate most devices.

Step 5. Click the `Key Management Algorithms` dropdown list and select an encryption algorithm appropriate for the devices connecting to this network.

Step 6. Click the `Pairwise Cipher Suites` dropdown list and select an encryption suite appropriate for the devices connecting to this network.
Pairwise Cipher Suites are algorithms and protocols for ensuring a secure connection between two devices in a wireless network. They define how data is encrypted and authenticated, so that communication stays protected from interception.

Step 7. In the `Inactivity Timeout` field, enter the desired value (minutes).
This value applies to Access Point Controlled mode only and sets a limit on the amount of time that the Access Point can be inactive. When the Wi-Fi mode is Access Point Controlled mode and the Access Point is inactive for a time greater than the Inactivity Timeout value, the Wi-Fi adapter is shut down. To restart it you can press the Wi-Fi button on the front cover. The Wi-Fi service will restart and operate under the same Inactivity Timeout property value. If you are in Access Point mode, no inactivity limit is enforced.

   NOTE: If you intend to use Wi-Fi for tool connectivity, Access Point Controlled mode is a good option. Choose this mode and set the Inactivity Value to some reasonably small number of minutes that makes sense for your use case. If the intended Wi-Fi usage is for field bus integration, then you should consider using the "Access Point" mode that disables the Inactivity Timeout property

   CAUTION: An Access Point represents a potential target for a cyber attack. Leaving the Access Point disabled by default is a recommended security best practice.

Step 8. To configure `Mode and Channel` properties, click the **Config Channel** button and select from the following:

   NOTE: For WW models, if the country code is not pre-configured then you must set it. For US models, the country code is pre-configured at the factory and cannot be changed.

   a. Click the **Mode** dropdown list and select an appropriate IEEE 802.11 type: (a, b, g,or n) to match your needs for the devices connecting to the network.

   b. Click the **Bandwidth** dropdown list and select the preferred frequency band. The HT20 HT40 (default) option accommodates most devices.

   c. Click the **Channel** dropdown list and select the least congested channel number for your network.

Step 9. To configure an `Allow List`, click the **Enable Allow List** checkbox and then click the **Allow List** button to enter MAC addresses that will be permitted to join the network (up to 8 addresses).
An "Allow List" is an inventory of known MAC addresses that are permitted access to the Wi-Fi access point, functioning as an added layer of protection for the Wi-Fi network. The format for an address group is six bytes, each separated by a colon, for example: `08:00:69:E2:01:FE`.

Step10. In the DHCP Server Settings area, `in the Client Range Low` field , enter the lowest IP address for the range.

   NOTE: The adapter IP should be in the same subnet, but not in the range of addresses defined here.

Step11. In the `Max Number of Clients Allowed` field, enter the maximum number of concurrent Wi-Fi clients that you will allow to attach to this access point (maximum number is 8), then click **Save** to keep your change.
Changes are saved but changes are applied only after reboot, so you are prompted for a reboot, however, there is no need to reboot until you complete all changes.

Step12. In the platform **Host Configuration** group, click on the **Wi-Fi Enabled** dropdown list and select `True`.

Step13. In the **Switch Position** dropdown field, select **Access Point** or **Controlled Access Point**.

NOTE: There is no physical "Switch" to move on the JACE-9000, this property value sets the mode for Wi-Fi operation.

After selecting a mode, you are presented with the **Reboot Now?** prompt.

Step14. Check the values in your **Access Point Mode** tab and Host Configuration fields. If you are satisfied with the settings, click **Yes** to reboot or **No** to make changes and reboot later.

Result
After a reboot, the controller will operate using the updated configuration and mode.

Configure a JACE-9000 as a Wi-Fi Client

This procedure describes the steps to configure the JACE-9000 Wi-Fi subsystem to run in `Client Mode` and connect to a Wi-Fi access point network.

Prerequisites:
• The JACE-9000 controller is licensed and commissioned.
• You have a platform connection to the controller.
• TCP/IP Configuration with DHCP Enabled does not conflict with other adapters

CAUTION: When configured for Wi-Fi Client mode, typically the IP address is DHCP-assigned by a Wi-Fi router. Be sure to confirm that the Wi-Fi router is configured to assign addresses on a different subnet than that used in either of the controller's Ethernet LAN configurations, otherwise the ports will not function correctly.

NOTE:

In the following steps, changes you make to the fields cause a **Reboot Now** prompt to open. You can select **No** until you have made all your changes. However, you must reboot before changes are applied to the controller.

Step 1. In the platform **Wi-Fi Configuration** view, under the Host Configuration group, select `True` from the **Wi-Fi Enabled** dropdown list .

The `Status` and Country Code fields display read-only values that are updated after saving changes and rebooting the controller.

Under the **Client Configuration** group, the following properties are read-only fields: `Status`, `Adapter Name`, `Access Point SSID`, `MAC Address`, and `Ipv4 Address`.

CAUTION: If the Default Gateway Switching property is enabled (checked) when connecting to a third party access point (such as Cisco), the gateway changes to whatever is provided by the access point configuration and this will conflict with your wired LAN settings. Note, this situation does not occur when connecting to JACE-9000 access point.

Step 2. In the Discovered Networks pane, click **Discover** , choose from the filtering options presented in the **Search for Access Points** window and click click the **Discover** button to initiate the discovery process.
The discovery process begins and access points populate the Discovered Networks table.

Step 3. From the Discovered Networks table, select the SSID for the network that you want to connect to

and click the **Add Network** button (or right-click the SSID and click **Add Network**) to add the access point.

Step 4. In the **Add a Wi-Fi Network** window, enter values for the following parameters:

Option	Description
SSID	read-only field with ID of selected access point
Priority	(0–9) to indicate which access point to try first. If all added networks have the same priority the client chooses the strongest signal.

Step 5. In the Network Database pane, select the added network and click **Connect**.

Step 6. Save any unsaved changes and reboot the controller.
After reboot, you can reconnect to the platform, select the **Wi-Fi Configuration** view, and confirm that the values for `Switch Position` and **Status** are correct.

Result

The Wi-Fi subsystem is now running in Client mode and connected to the selected network. The `Status` field should reflect only the states that are valid for client mode. For example, "Scanning", "Client Running".

Add a new Wi-Fi network - JACE-9000

Prerequisites:

- You know the SSID and Network Key (passkey) of the desired access point.
- Your JACE-9000 has Wi-Fi "enabled".

When the access point for a preferred network is not configured to broadcast its SSID, you can still add the network to the Wi-Fi Client configuration if you know the necessary credentials for that access point.

Step 1. In the Network Database pane of the Client Mode tab, click **New Network**.

Step 2. In the **Create a New Wireless Network** window, configure the following properties for the access point and then click **OK**.

- Enter the `SSID` for the access point
- Enter a `Priority` for connecting to the access
- Modify the default security options as needed
- Enter the `Network Key` (passkey) for the access point

Result

The new wireless network is added to the Network Database table.

Chapter 3. Wi-Fi references

Wi-Fi Configuration view
The topics that follow provide details about JACE-9000 Wi-Fi setup, configuration options and status monitoring using Niagara 4.15.

Wi-Fi Configuration view - Niagara 4.15

The **Wi-Fi Configuration** view is the primary view for configuring Wi-Fi communications on both the JACE-8000 and the JACE-9000 controllers. The view includes tabs for configuring the controller to run in both Client mode and Access Point mode. However, a controller unit cannot perform in both modes at the same time.

The topics that follow provide additional details about the JACE-9000 **Wi-Fi Configuration** view in Niagara 4.15 Workbench: **Platform** > **Views** > **Wi-Fi Configuration**.
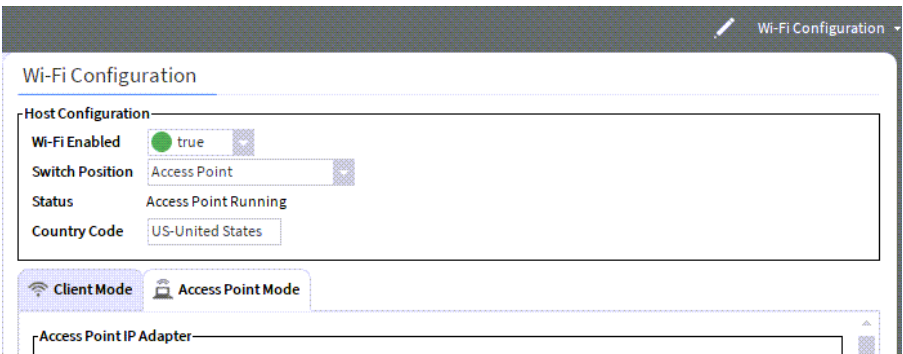
The information in this view is organized in three major groups: Host Configuration, Client Mode tab, Access Point Mode tab. Values are shown in each view but are editable only when appropriate, based on the current active Wi-Fi state (Enabled: true or false) and mode (Switch Position), as selected and shown in the Host Configuration group properties.

Host Configuration properties
The Host Configuration property group is located at the top of the **Wi-Fi Configuration** view. These properties are described in the following table.

Property	Value	Description
Wi-Fi Enabled	true, false (default)	The `true` option enables Wi-Fi and the `false` option disables Wi-Fi on the connected controller. Any change in this value requires a reboot to implement.
Switch Position	Off, Client, Access Point, Access Point Controlled	**NOTE:** There is no physical "switch" on the JACE-9000. • `Off` sets controller Wi-Fi operation off. • `Client` sets controller Wi-Fi to

Property	Value	Description
		function in Client mode. • `Access Point` sets Wi-Fi to function in Access Point mode. • `Access Point Controlled` sets controller Wi-Fi to function as an access point using the same properties as the `Access Point` option but with the added ability to act in response to the controller Wi-Fi button presses. See <u>Wi-Fi modes and states - JACE-9000</u> for more details.
Status	read-only field reports a current status	Values indicate current status, including the following steady and transitional states. • Stopped • Running • Access Point Running • Client Trying to Associate
Country Code	read-only field displays device Country Code	Based on your controller's SKU and Region, as described in <u>Regions, SKUs, and Country Codes</u>

Current Wi-Fi states

Current Wi-Fi State	Condition	Additional Notes
Stopping	Indicates that Wi-Fi processes are stopping.	This is the result of toggling the **Wi-Fi Enabled** control from `true` to `false` in the platform's **Wi-Fi Configuration** view, or an access point Inactivity Timeout occurred. In the case of an inactivity timeout, the next state will be `Inactivity Timeout` after which the Wi-Fi connection stops. In all other cases, the next state will be `Stopped`.
Stopped	Indicates that the Wi-Fi drivers are not loaded and no Client or Access Point mode processes are running.	The Wi-Fi LED on top of the unit should be in blinking mode. See <u>LED mode and status indicators</u> .
Failed	read-only field reporting a process failure.	Reports that a Wi-Fi process (either Client or Access Point) was not able to successfully complete. This usually indicates

Current Wi-Fi State	Condition	Additional Notes
		an invalid Wi-Fi configuration. A `Failed` state kicks off an attempted shutdown of the Wi-Fi processes and drivers, after which the state should transition to `Stopped`.

Client Mode Wi-Fi states

The following current Wi-Fi states are specific to Client mode.

Type	Value	Description
Client Supplicant Running	Indicates that Client mode is running but not active.	This status displays when Client mode is inactive and not connected to an Access Point.
Client Running	Reports that the adapter is up and the IP assigned.	Client successfully established the connection with Access Point.
Client Scanning	Indicates that the Client mode Wi-Fi adapter is looking for an access point to connect to by scanning available frequencies.	This can happen if the Wi-Fi network (ssid/password, etc) is not configured correctly or is unavailable because the access point is off or out of range.
Client Trying to Associate	Indicates that a configured access point has been located, and the supplicant is trying to associate with the access point.	If the Allow List is configured in the access point, the mac address of this client adapter must pass the list filters.
Client Negotiating	Indicates that the Client mode supplicant is negotiating capabilities and credentials with the access point.	If successful, the next transition will be to `Client Running`.
Client Association Success	Indicates that the Client has successfully associated with an access point.	The Client and access point begin a four-way handshake to validate credentials and establish common security protocol suites (see "Client Negotiating").
Client Disconnected	Reports a normal state transition on Client mode startup.	It is normal to see this during Client mode startup, but should transition to other states. If no configured access points are available, the connection does not progress past this point. Every 15 seconds, the network database is reloaded, so that configuration changes made during this state are picked up.
Client Fault	Indicates tha the Client mode is not currently capable of running.	This state displays when a client process encounters a faulty or unknown state. This state may also result from configuration errors or a

Type	Value	Description
		failure in the CC and SKU validation process.

Access Point mode Wi-Fi states

The following current Wi-Fi states are specific to Access Point mode.

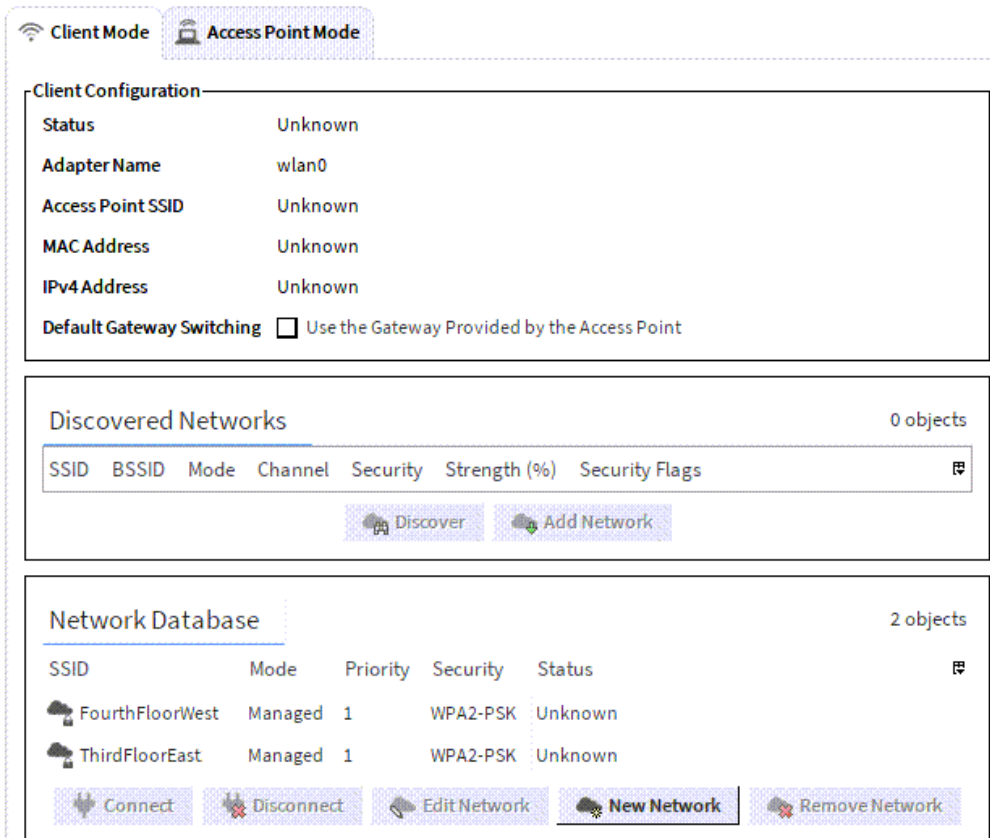| Type	Value	Description
Access Point Starting	Reports that the Access Point mode is enabled in the Wi-Fi Configuration view.	This starts the Wi-Fi driver, which adds a `wlan0` adapter, brings the adapter up and assigns an IP address to it, starts Hostapd, and starts the Dhcp server on the adapter. This state can only be entered from the `Stopped` state.
Access Point Running	Reports that the adapter is up and the IP address assigned.	The Hostapd started and the Dhcp server started on the adapter.
Inactivity Timeout	In Access Point Controlled mode, a non-zero Inactivity Timeout value is used to provide Access Mode capability. If, for the specified amount of time, no clients are connected or attached, the adapter is shut down in this state.	Inactivity timeout is only used in Access Point Controlled mode. **Active** An Access Point is considered "Active" if at least one client is connected, regardless of whether or not there are any current non-broadcast communications. **Inactive** An Access Point is considered "Inactive" if no clients are connected for the specified `<Inactivity Timeout>` value. To restart the Wi-Fi adapter after an Inactivity Timeout shutdown, you must press the Wi-Fi button on the controller. Timed access restarts using the current Inactivity Timeout setting.
Access Point Fault	Reports that there is a fault, unknown state or configuration error.	This state indicates that the service is not started because Wi-Fi properties are not correctly configured, service is not enabled or in some other fault state.

Client mode tab - JACE-9000

The Client Mode tab provides properties for configuring the JACE-9000 Wi-Fi in Client mode.

Client Configuration group

The Client Mode tab displays configuration properties in a Client Configuration group and network management tools in separate discovery and database tables.

The following images and tables describe the different properties available in the Client mode tab of the **Wi-Fi Configuration**

Figure 4. Wi-Fi Configuration view, Client mode tab (Niagara 4.15)

Property	Value	Description
Status	read only text	Shows current Client mode state: Running, Not Running, etc.
Adapter Name	read only text	Name of the client Wi-Fi adapter
MAC Address	read only text	Client MAC address, if connected. "Unknown" if not connected.
IPv4 Address	read only IP address	Client IP address, if connected. "Unknown" if not connected.
Default Gateway Switching	check box (enabled, disabled)	When checkbox is selected, Wi-Fi is the preferred interface used for routing (as a default gateway) when multiple adapters in use.

Property	Value	Description
		CAUTION: When connecting to a third party access point (such as Cisco), the gateway changes to whatever is provided by the access point's configuration and this will conflict with your wired LAN settings. Note, this situation does not occur when connecting to a JACE access point.When disabled (not checked), keep the gateway as assigned in TCP/IP Configuration view

Network Discovery and Network Database groups

These groups provide the controls and displays for working with Wi-Fi access points. Use the button controls to discover, add, edit, connect and disconnect from reachable access points. The properties and features of this group work similar to typical Niagara network discovery tools.

Access mode tab - JACE-9000

The Access Mode tab provides properties for configuring the JACE-9000 Wi-Fi in Access mode.

The Access Mode tab displays properties in the following three groups:

- Access Point IP Adapter
- Access Point DHCP Server Settings
- Access Point Configuration

Figure 5. Wi-Fi Configuration view, Access Point Mode tab (Niagara 4.15)

Access Point IP Adapter group

Property	Value	Description
Name	read only text	Read only name of adapter
IPv4 Address	read only IP address	This sets the IP address of the Wi-Fi adapter. A client uses this to make an IP connection over Wi-Fi while the unit is functioning as an Access Point.
IPv4 SubnetMask	read only IP address	This sets the netmask of the Wi-Fi adapter.

Access Point DHCP Server Settings group

Type	Value	Description
Default Lease Time	6 hours (default)	Fixed duration (in hours, minutes, and seconds) for a DHCP IP address lease, before it expires the lease must be renewed.
Max Lease Time	6 hours (default)	Maximum duration (in hours, minutes, and seconds) for a DHCP IP address lease.
Subnet	address	The subnet of IP addresses assigned by the DHCP server. **CAUTION:** Configure this to assign addresses on a different subnet than that used in either of the controller's other LAN configurations, otherwise the ports will not function correctly.
Netmask	number	The Netmask of IP addresses assigned by the DHCP Server.
Client Range Low	address	Lowest IP address for the range. The order of assigning IPs from the Access Point DHCP is indeterminate. **NOTE:** The adapter IP should be in the same subnet, but not in the range of addresses defined here.
Max Number of Clients	8 (default)	Maximum number of Wi-Fi clients that can attach at a given time (maximum limit is 8).

Access Point Configuration group

Type	Value	Description
SSID	atlas (default)	Service Set Identifier (SSID) is a unique alphanumeric identifier. Sets the name for this access point. Replace default name with a unique, meaningful network name. **NOTE:** It is important to change the default value to a unique name to avoid having multiple units with the same SSID in a particular area.
Broadcast SSID	enabled (default), disabled	If enabled, periodically broadcasts Wi-Fi signal so that devices can detect and connect. If disabled, the SSID is "hidden" and not discoverable. Also, a client must be manually configured with the correct SSID

Type	Value	Description
		which matches the controller SSID field above.
Passphrase	text	Sets a passphrase that a client must enter to connect to this network. A 10 character (minimum) phrase is required.
Wpa Mode	WPA, WPA2, WPA WPA2 (default)	Wi-Fi security protocols and security certification programs. WPA WPA2 will accommodate most devices. Devices with older network cards may only work with WPA security.
Key Management Algorithms	WPA-PSK (default)	Method of authentication key distribution and the encryption protocols that protect passwords via encryption using either a pre-shared key and/or an authentication server.
Pairwise Cipher Suites	TKIP, CCMP, TKIP+CCMP (default)	Encryption protocol options. TKIP CCMP will accommodate most devices.
Inactivity Timeout (minutes)	10 (default)	Sets a limit on the amount of time a client connection can be inactive. On reaching the Timeout limit, the Wi-Fi adapter is shutdown completely. To restart it you must press the Wi-Fi button while the **Switch Position** is in Access Point Controlled mode. Note, if the intended Wi-Fi usage is for tool connectivity, then set this value to some small number of minutes. If the intended Wi-Fi usage is for field bus integration, then use Access Point mode so the Wi-Fi is not timed out. **CAUTION:** An Access Point represents a potential target for cyber attack. Leaving the Access Point disabled by default is a security best practice.
Mode and Channel	**Config Channel** button invokes the **Configure Mode and Channel** window, which you can use to choose radio mode, bandwidth, and channel options.	• Mode IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, or IEEE 802.11n (default) • Bandwidth Two digit codeRadio mode: HT20, HT40, or HT20 HT40

Type	Value	Description
		• Channel Choose from list. Channel options depends on selected radio mode.
Allow List	Allow List button opens a window.	Opens a window that allows you to configure the access point with a set of device MAC addresses that are allowed to connect to this access point.
Enable Allow List	Enable Allow List checkbox. Select to enable or clear to disable (default).	If enabled, only an address in the configured Allow List can connect. If disabled, connection to the access point is not limited to a specific set of devices.
Clients	Show Clients button opens a window that displays all clients that are currently attached to the access point.	Open a window to show currently attached clients.

Chapter 4. Wi-Fi Troubleshooting - JACE-9000

This topic describes some possible issues with set up or configuring Wi-Fi on a JACE-9000 along with possible solutions.

Condition
Client Wi-Fi does not connect to a known SSID.

Cause
SSID name includes a special characters or non alpha-numeric characters.

If an access point has an SSID with an apostrophe or other possible non alpha-numeric character, the character may be displayed in Unicode by Workbench, preventing a successful client connection.

Remedy
- Do not create or connect to an SSID that contains a non-standard character, such as an apostrophe. If possible, rename the SSID with alpha-numeric characters only.

- If using Workbench, the 'discovered' access point name may show the SSID with one or more Unicode characters. You can edit the name in the SSID field to replace the Unicode characters with the corresponding special or non alpha-numeric character.
  For example, if you discover a network that displays as *Atlas\xe2\x80\x99s Access Point*, enter the following when adding the SSID in the New Network field: `Atlas's Access Point`, where the apostrophe replaces the Unicode characters.

Chapter 5. Glossary

The following glossary entries relate specifically to the topics that are included as part of this document.

To find more glossary terms and definitions refer to glossaries in other individual documents.

Alphabetical listing

access point
In a wireless local area network (WLAN), a wireless access point (WAP) is a hardware device, such as the JACE-9000, that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network.

allowlist
A layer of protection that can be added to a Wi-Fi network. An IP address can be re-assigned to any device but a MAC address is hard-coded to the device. A MAC allowlist is an inventory of known MAC addresses that are permitted access to the Wi-Fi access point.

EAP
EAP (Extensible Authentication Protocol) is an enterprise level authentication protocol that requires an authentication server. This is an additional security layer providing protection against attacks on passwords.

PSK
Referred to as *WPA-PSK* (Wi-Fi protected access-pre-shared key) mode, is a method of authentication key distribution.

SAP
In the context of a JACE access point mode of operation, the term SAP is synonymous with "access point", "host mode", or "hostapd". In this context, the terms may be used interchangeably.

client
A wireless client is a device that can use the 802.11 protocol. The JACE-8000 is such a device as is a laptop, a PC, and a Wi-Fi phone. A client may be fixed, mobile or portable. Generally, in wireless networking terminology, a station, wireless client and node are often used interchangeably.

STA
In the context of a JACE client mode of operation, the term STA is synonymous with "client", "station", "station mode", or "wpa_supplicant". In this context, these terms may be used interchangeably.

SSID
SSID (Service Set Identifier), an alphanumeric string (up to 32 characters), is a unique identifier for a specific Wi-Fi access point. The SSID differentiates one WLAN from another. If the access point is configured to periodically broadcast its SSID, the wireless devices that are within range can detect the network and connect to it. When broadcasting is disabled, a wireless client must be configured with the network's SSID in order to connect to it.

TKIP
TKIP (Temporal Key Integrity Protocol) is an encryption protocol. The RC4 stream cipher is used with a 128-bit per-packet key, dynamically generates a new key for each packet. Used by WPA.

WPA WPA2
WPA (Wi-Fi Protected Access)/WPA2 (Wi-Fi Protected Access II) are two Wi-Fi security protocols and security certification programs. They provide both security (you can control who connects) and privacy (the transmissions cannot be read by others) for communications as they travel across your network. WPA2 is newer, more secure and complex than WPA. Newer Wi-Fi devices (certified since 2006) support both the WPA and WPA2 security protocols. Devices that have older network cards may only work with WPA security.