Technical Document

JACE-8000 WiFi Guide

June 24, 2021

niagara4

JACE-8000 WiFi Guide

Tridium, Inc.
3951 Westerre 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

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 the JACE-8000 WiFi option. Included are an overview, as well as descriptions of requirements, operation notes, and configuration instructions for the WLAN-enabled models (US or WW).

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

Document change log

June 24, 2021

Correction in Overview topic, updated WLAN capability and factory configuration of JACE-8000-CSE-003 XX model.

October 16, 2019

Minor correction in the "Overview" topic and edited Serial Shell information in the "WLAN factory configuration" topic.

September 19, 2019

In the "Overview" topic, added content describing WiFi capability for the different JACE-8000 models. In the "References" chapter, added the topic "WLAN factory configuration".

July 2, 2019

Removed a note related to Country Code from "Configuring WiFi Access Point Mode" and "Access Point mode tab" topics.

October 9, 2018: Niagara 4.7 updates:

Added information about configuring Access Point Dhcp Server Settings.

November 29, 2016

Updated controller images showing WLAN switch and antenna.

July 29, 2016

Added a cautionary note to "Configuring WiFi Access Point Mode", "Configuring WiFi Client Mode", "WiFi Configuration View", and "Access Point mode tab" topics alerting users that each enabled LAN port (LAN1, LAN2, and WiFi) must be configured on a different subnet.

May 6, 2016

Modified note in the "Overview" topic to include IEEE 802.1x and USB backup/restore as unsupported features when running AX.

April 6, 2016

- In the "Overview" topic, added a note explaining that starting in Niagara 4.2, JACE-8000 controllers can be converted to run AX-3.8U1–with some feature limitations. For any JACE-8000 running AX, WiFi functionality is not supported.
- In the "Switching WiFi modes" topic, added the note explaining "WiFi not supported/Switch position not monitored...."
- In the "WiFi Switch details" topic, added the note explaining "WiFi not supported/Switch position not monitored...."

December 2, 2015

- In the Specifications topic added a list of supported channels and unsupported DFS channels. Also in Specifications, added a note on unsupported security protocols: WPA2–enterprise, WEP, or no authentication.
- In the Configuring WiFi Client mode topic, added a paragraph prior to step 1, explaining the DFS restriction.
- In the supported WiFi configurations section on WiFi Client, added a note on the DFS restriction.

November 12, 2015

Added a new task to the guide: "Restarting the WiFi adapter after Inactivity Timeout shutdown". Also edited wording in the 1st note in the "WiFi Switch details" topic to include Inactivity Timeout shutdown.

November 5, 2015

Added prerequisite that the JACE be licensed and commissioned to each of the Configuring WiFi tasks.

October 23, 2015

Initial draft document.

Related documentation

- *JACE-8000 Install and Startup Guide*
- *JACE-8000 Backup and Restore Guide*
- *Niagara Platform Guide*

Chapter 1 Overview

Topics covered in this chapter

♦ WiFi Specifications

Some models of the JACE-8000 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 perform in both modes simultaneously.

Refer to the following table for the WLAN capability of each JACE-8000 model.

Table 1 WLAN capability of JACE-8000 models

Model name	Factory configuration	WLAN capability
JACE-8000-CSE-001 US	WLAN-enabled	You can turn on WiFi using the Selector Switch, and configure for US operation only.
JACE-8000-CSE-002 WW	WLAN-enabled	You can turn on WiFi using the Selector Switch, and configure for countries other than the US.
JACE-8000-CSE-003 XX	WLAN-not included	WiFi capability is not included with this model.

NOTE: The remainder of this document covers configuration details only for the WLAN-enabled models (US or WW).

By default, these devices ship with the WiFi feature turned OFF. You can enable WiFi using the Selector Switch, and configure the device for the country of operation. The process of enabling WiFi varies slightly depending on the country the device is shipped to. The initial WiFi setup requires Workbench or serial connectivity. When enabled, you can configure the device as a client to an already established IEEE 802.11 access point and network, or as an access point to establish a new network.

The WiFi feature adds a new platform view, the **WiFi Configuration** view for JACE-8000 platform (the only current Niagara 4 platform supporting WiFi). In addition, the JACE-8000 command line system console has a **Configure WiFi** option which you can use to initially configure WiFi, although this provides only a subset of the configuration parameters that are available via the platform view.

NOTE: Starting in Niagara 4.2, the JACE-8000 can be converted (downgraded) to run AX-3.8U1–with some feature limitations. For example, for any JACE-8000 running AX the WiFi functionality is not supported. In this configuration the WiFi switch position on the device is not monitored. Other unsupported features are IEEE 802.1X wired authentication and USB backup/restore.

NOTE: You can enable/disable the WiFi feature either via the WiFi Selector Switch on the enclosure or remotely via platform **WiFi Configuration** view.

WiFi Specifications

This section covers JACE-8000 WiFi specifications.

Disabled by default, the WiFi option (on factory configured WLAN-enabled models) can be enabled and configured to attach as a Client (CLT) to an already established IEEE 802.11 access point and network, or configured as an Access Point (ACC) to establish a new network.

- Supports IEEE 802.11a/b/g/n networks
- Configurable radio (OFF, ACC, CLT)
- Supports WPA-PSK, WPA2-PSK security protocols

NOTE: The JACE-8000 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.

    NOTE: The following Dynamic Frequency Selection (DFS) channels in the 5 GHz range are not supported: 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140.
- Single dual band 2.4/5.8 GHz antenna. The antenna may be remotely located using an extension cable.

Chapter 2 Common Tasks

Topics covered in this chapter

♦ Configuring WiFi Access Point mode
♦ Configuring WiFi Client mode
♦ Switching WiFi modes
♦ Adding a new wireless network
♦ Editing a wireless network
♦ Restarting the WiFi adapter after Inactivity Timeout shutdown

The following procedures describe how to configure the JACE-8000 WiFi adapter for Access Point mode or for Client mode.

You can configure WiFi communications using the platform **WiFi Configuration** view.

Configuring WiFi Access Point mode

This procedure describes the steps to configure the JACE-8000 WiFi subsystem to run in Access Point mode. This configuration can be used either as a network for WiFi enabled field bus devices, or to provide browser or Workbench access to local tools.

Prerequisites:

- JACE is licensed and commissioned
- Platform connection to the JACE
- WiFi Selector Switch in the Off (center) position

NOTE: The WiFi subsystem must be "stopped" before any WiFi process can be started.

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

Step 1 Click the **Access Point Mode** tab and if desired, modify the **`Adapter IPv4 Address`** and/or **`Adapter IPv4 Netmask`** values.

This sets the address that a client uses to make an IP connection to this unit over WiFi 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 Config** area, in the **`SSID`** field enter a name for this access point. 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 **`Passkey`** for the unit.

This sets a password 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.

Step 7 In the **`Inactivity Timeout`** field, enter the desired value (minutes).

This sets a limit on the amount of time a client connection can be inactive. On reaching the timeout limit, the WiFi adapter is shutdown completely. To restart it you must move the WiFi Selector Switch on the unit to "OFF". Once the WiFi Current State shows "Stopped", move the WiFi Selector Switch back to "ACC".

NOTE: If the intended WiFi usage is for tool connectivity, then set this value to some small number of minutes. If the intended WiFi usage is for field bus integration, then set this value to "`0`" to disable the Timeout functionality.

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 a **`Whitelist`**, click the **Enable Whitelist** checkbox and then click the**Whitelist** button to enter MAC addresses that will be permitted to join the network (up to 16 addresses).

A "whitelist" is an inventory of known MAC addresses that are permitted (or denied) access to the WiFi access point, functioning as an added layer of protection for the WiFi network. The format is six HEX addresses separated by a colon, for example: `08:00:69:E2:01:FE`

Step 9 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 **County Code** dropdown list and select the appropriate two-digit country code.

b. Click the **Radio Mode** dropdown list and select an appropriate 802.11 type for the devices connecting to the network.

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

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

Step 10 In the DHCP Server Settings pane, **`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.

Step 11 In the **`Max Number of Clients Allowed`** field, enter the maximum number of WiFi clients that can attach at a given time (maximum limit is 16).

NOTE: The WiFi adapter supports a maximum of 3 user interface devices such as, a laptop, PC, or WiFi phone, at a given time. However, this limit is not enforced.

Step 12 Click **Save**.

NOTE: The saved configuration changes take effect the next time WiFi is started.

Step 13 In the platform **WiFi Configuration** view, click on the **WiFi Enabled** dropdown list and select `True`.

Step 14 Move the WiFi Selector Switch on the controller to the **ACC** (left) position to start the WiFi adapter.

The WiFi subsystem is enabled in Access Point mode. In the **WiFi Configuration** view, the **`Current WiFi State`** field should reflect only the states that are valid for access point mode, such as `SAP starting`, `SAP running`.

Configuring WiFi Client mode

This procedure describes the steps to configure the JACE-8000 WiFi subsystem to run in Client Mode.

Prerequisites:

- JACE is licensed and commissioned
- Platform connection to the JACE
- WiFi Selector Switch on the unit is in the Off (center) position
- TCP/IP Configuration does not have DHCP Enabled (checked) on any adapter

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

NOTE: The WiFi subsystem must be "stopped" before any WiFi process can be started.

For JACE-8000 units deployed in the U.S. (and in countries that accept U.S. certification) an important consideration is determining whether or not the access point that the JACE will connect to is using Dynamic Frequency Selection (DFS). The JACE cannot connect to an access point that uses DFS channels in the 5 GHz range. The unsupported channels are listed here: 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140.

Step 1 In the platform **WiFi Configuration** view, click the **WiFi Enabled** dropdown list and select `True`.

The Wireless State pane displays read only values for the WiFi attach state, client adapter name, client MAC address and DHCP address as well as last access point.

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's configuration and this will conflict with your wired LAN settings. Note, this situation does not occur when connecting to JACE-8000 access point.

Step 2 In the Discovered Networks pane, click **Discover** to identify available networks.

Step 3 Select the SSID for the network that you want to connect to and click the **Add** button (or right-click the SSID and click **Add**).

Step 4 In the **Add a Wireless Network** dialog, enter values for the following parameters:

- **`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.
- **`Network Key`** (Passkey) needed to connect to the access point.

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

Step 6 Move the WiFi Selector Switch on the unit to the **CLT** (right) position.

In the platform **WiFi Configuration** view, the value for the **`WiFi Switch Position`** changes to `Client`.

WiFi subsystem is now running in Client mode and connected to the selected network. The **`Current WiFi State`** field should reflect only the states that are valid for client mode. For example, "Scanning", "Supplicant Running".

Switching WiFi modes

Switching from one WiFi mode to another is done only with the WiFi configuration switch on the JACE enclosure.

NOTE: Starting in Niagara 4.2, the JACE-8000 can be converted (downgraded) to run AX-3.8U1–with some feature limitations. For example, for any JACE-8000 running AX the WiFi functionality is not supported. In this configuration the WiFi switch position on the device is not monitored. Other unsupported features are IEEE 802.1X wired authentication and USB backup/restore.

When switching modes, always move the switch to "Off" (center), then wait for the WiFi subsystem to shutdown (less than one minute). Once WiFi is stopped, the JACE can be switched to another mode.

NOTE: You can switch modes without first opening the platform configuration view, provided you have already configured WiFi for the JACE. For example, if you want to turn the WiFi Access Point on or off, you might walk up to the unit and change the switch position without opening the platform configuration view.

Step 1 On the JACE enclosure, move the WiFi switch to the Off (center) position.

If you have the platform **WiFi Configuration** view open, the **`WiFi Current State`** value changes to `Stopping`.

Step 2 Wait while the WiFi subsystem shuts down.

In the platform **WiFi Configuration** view, the **`WiFi Current State`** value changes to `Stopped`. Also, the WiFi LED on top of the enclosure is off.

Step 3 On the enclosure, move the WiFi switch to:

- ACC (left) position for Access Point mode
- CLT (right) position for Client mode

Adding a new wireless network

When the access point for a preferred network is not configured to broadcast its SSID, you can still add the network to the WiFi Client configuration provided you know the necessary credentials to connect.

Prerequisites:

- The SSID and Network Key (passkey) of the desired access point.

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

Step 2 In the **Create a New Wireless Network** dialog, 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

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

Editing a wireless network

In the Client mode configuration, you can edit connection properties for a previously accessed wireless network listed in the Network Database table.

Prerequisites:

- WiFi Selector Switch in CLT position
- Previously configured WiFi network

Step 1 In the WiFi Configuration view, on the Client Mode tab, select a network listed in the Network Database pane and click **Edit**.

Step 2 In the **Edit a Wireless Network** dialog, modify values as needed.

NOTE: In this dialog the **Show Password** checkbox is activated once you edit the current **`Network Key`** value.

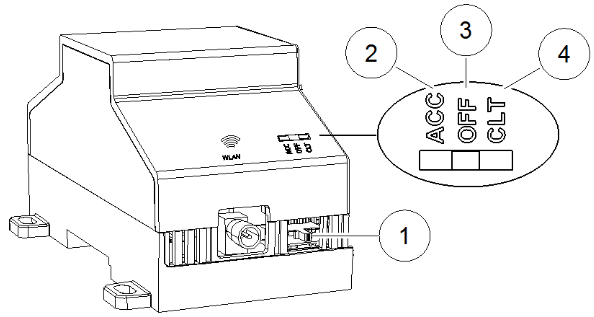
Restarting the WiFi adapter after Inactivity Timeout shutdown

To restart the WiFi adapter after an Inactivity Timeout shutdown, you must physically move the WiFi Selector Switch. You cannot restart the adapter from the **WiFi Configuration** View.

Prerequisites:

- WiFi adapter is shutdown due to exceeding the amount of time configured for the **`Inactivity Timeout`** property.

NOTE: The **`WiFi Enabled`** setting in the **WiFi Configuration** view cannot be used to re-enable WiFi on a unit which has experienced an **`Inactivity Timeout`**. You must move the WiFi Selector Switch on the unit to the "Off" position (as shown here) in order to reset the timeout.



1	Selector switch
2	ACC — Access Point mode
3	OFF — WLAN off
4	CLT — Client mode

Step 1 Move the WiFi Selector Switch on the enclosure from "ACC" to the "OFF" (center) position.

In the **WiFi Configuration** view, the **`Current WiFi State`** transitions to "Stopped".

Step 2 Once "Stopped", move the WiFi Selector Switch on the enclosure back to the "ACC" (left) position.

Step 3 If disabled in the **WiFi Configuration** view, click **`WiFi Enabled`** dropdown and select "true".

The WiFi adapter is re-enabled in Access Point mode. In the **WiFi Configuration** view, the **`Current WiFi State`** field should show either "SAP starting" or "SAP running".

Chapter 3 References

Topics covered in this chapter

♦ WLAN factory configuration
♦ Secure storage and the SD card
♦ WiFi Switch details
♦ WiFi Configuration view
♦ Supported WiFi configurations

The topics that follow provide additional details on the SD card, the WiFi switch, the WiFi Configuration view, as well as supported WiFi configurations.

WLAN factory configuration

JACE-8000 WiFi capability is pre-configured by the factory as either “WLAN-enabled” or “WLAN-disabled”. For models that are factory configured as WLAN-enabled (e.g. JACE-8000-CSE-001 US, JACE-8000-CSE-002 WW), additional steps must be taken to configure the adapter. Conversely, for models that are factory-configured as WLAN-disabled (e.g. JACE-8000-CSE-003 XX), WiFi is permanently disabled. The WLAN adapter cannot be used or configured.

You can verify the WLAN factory configuration either with the product packaging or via the Serial Shell. If disabled, the packaging will be labeled with “`WLAN DISABLED`”, or “`JACE-8000-CSE-003`”, or with both. If packaging is already removed, you can check the configuration using the **Serial Shell**.

1. At the prompt in the **Serial Shell Main Menu**, type: ‘`sh`’.

   The shell `$` prompt appears.

2. At the `$` prompt, type the command: `wifi-skuread` and press **Enter**.

   This will return the one of the following codes for your device. The returned code indicates the device’s WLAN capability:

   `US` =United States (WiFi enabled for the US only)

   `WW` = World Wide (WiFi enabled for countries other than the US)

   `XX` = Disabled (WiFi is permanently disabled)

Secure storage and the SD card

On JACE-8000, the SD card is the primary storage media for all data and configuration related to the Niagara installation. Since the SD card can be easily removed and the data duplicated, the sensitive data is encrypted when stored on the card. Files are stored in encrypted format, but decoded on the fly as they are accessed.

Sensitive data include the following:

- Credentials for accessing a WiFi network
- Niagara key material
- Private key files
- OS account credentials

The system is designed in a way that protects this data, while at the same time allowing you to move an SD card from a unit that suffered a hardware failure to a new unit with minimal effort.

In this scenario, the SD card inserted into the replacement unit contains the system passphrase for the original unit, which does not match the one in the replacement unit. This results in the boot sequence failing due to the passphrase mismatch (indicated by Stat LED flashing with a 50% duty cycle with a 1 second period).

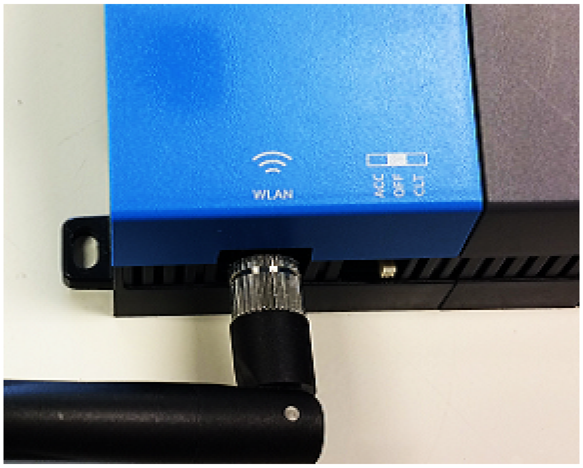
You are then prompted to enter the system passphrase (for the original unit which is stored on the SD card) via serial connection. You must first authenticate with platform credentials, before you can update the system password.

NOTE: Pre-configuring (via serial connection) the replacement JACE-8000 unit with a system passphrase matching the one stored on the SD card (swapped out of the other unit) facilitates commissioning the replacement unit. In this situation, the commissioning process does not prompt for a passphrase since it detects a passphrase match.

WiFi Switch details

The JACE-8000 enclosure has a 3-position slide switch, the WiFi Selector Switch, as shown here.

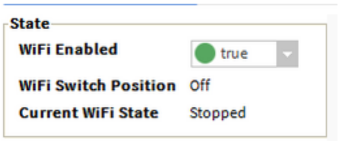
Figure 1 Antenna and switch location on enclosure



NOTE: Starting in Niagara 4.2, the JACE-8000 can be converted (downgraded) to run AX-3.8U1–with some feature limitations. For example, for any JACE-8000 running AX the WiFi functionality is not supported. In this configuration the WiFi switch position on the device is not monitored. Other unsupported features are IEEE 802.1X wired authentication and USB backup/restore.

Use the WiFi Selector Switch on the enclosure to turn the WiFi subsystem on or completely off. Once you set the switch to either Access Point or Client mode, the **`WiFi Enabled`** property in the platform **WiFi Configuration** view allows you to enable or disable WiFi functionality.

NOTE: By design, the **`WiFi Enabled`** setting (in the platform **WiFi Configuration** view) has no effect whenever the WiFi Selector Switch on the enclosure is in the **OFF** (center) position, or when the unit has experienced an **`Inactivity Timeout`** shutdown.



State

WiFi Enabled	● true
WiFi Switch Position	Off
Current WiFi State	Stopped

Switching from one WiFi mode to another is done only with the WiFi Selector Switch on the enclosure.

WiFi Selector Switch positions

- **ACC** (left position)

  Starts the WiFi subsystem in Access Point mode if all of the following conditions are satisfied:

  - The switch is in the ACC position.
  - WiFi is enabled (via the platform **WiFi Configuration** view in Workbench, or the system shell in JACE console window).
  - A country code is configured. For US models, the country code is pre-configured at the factory. For other models, the county code must be set.
  - A valid configuration for the adapter IP, access point, and Dhcp server have been specified and saved (either through Workbench via the platform **WiFi Configuration** view or system shell menu).

    NOTE: If not configured correctly, the access point mode attempts to start but fails to complete successfully.

- **OFF** (center position)

  The Off setting disables the WiFi subsystem, keeping it from starting. If already running, the Off setting shuts down the WiFi subsystem. While the switch is in this position, neither client mode nor access point mode can be started, even if enabled from within the Niagara platform **WiFi Configuration** view.

- **CLT** (right position)

  Starts the WiFi subsystem in Client mode if all of the following conditions are satisfied:

  - Switch is in the CLT position.
  - WiFi is enabled (from the platform **WiFi Configuration** view in Workbench, or from the system shell in JACE console window).
  - The country code is configured. For US models, the country code is pre-configured at the factory. For other models, the county code must be set.
  - If an available access point is specified and configured correctly in the Workbench view (or via system shell menu), then the Client mode starts and attempts to connect to an access point.

    NOTE: If not configured correctly, or if out of range of the access point, then connection to that access point fails.

NOTE: For factory-configured "WLAN-disabled" models only (e.g. JACE-8000-CSE-003 XX), WiFi is permanently disabled. The WLAN adapter cannot be used or configured..

WiFi Configuration view

The **WiFi Configuration** view is the main view for configuring WiFi communications for JACE-8000 platform (the only current Niagara 4 platform supporting WiFi). The view includes tabs for configuring the JACE to run in both Client mode and Access Point mode. However, the unit cannot perform in both modes at the same time.

CAUTION: When enabling more than one LAN port (applies to LAN1, LAN2, WiFi) the IP address for each must be configured on different subnets, otherwise the ports will not function correctly. For example, with a typical "Class C" subnet mask of 255.255.255.0, setting Interface 1=192.168.1.99 and Interface 2= 192.168.1.188 is an invalid configuration, as both addresses are on the same subnet. Note that when the controller is configured for WiFi Client mode, typically the IP address is DHCP-assigned by a WiFi router. Be sure to confirm that the WiFi router is configured to assign addresses on a different subnet than that used in the controller's LAN1 and/or LAN2 configuration. Additionally, if configuring the controller for Access Point mode using syssh, be sure you configure it for a different subnet than that used in either the LAN1 and/or LAN2 configuration.

State Properties

WiFi State properties appear in the upper portion of the view.

Property	Value	Description
WiFi Enabled	true, false (default)	Selecting True, enables WiFi functionality. **NOTE:** The **`WiFi Enabled`** setting in the **WiFi Configuration** view is ignored whenever the unit's WiFi Selector Switch is in the **OFF** (center) position.
WiFi Switch Position	Access Point, Off, Station	Read only value. Indicates the current position of the WiFi Selector Switch on the unit: Access Point = ACC (left position). OFF (center position) turns the WiFi subsystem completely off. Station = CLT (right position).

Current WiFi States

General **`Current WiFi State`** values listed in the following table may occur when using either Client mode or Access Point mode.

Current WiFi State Value	Condition	Additional Notes
Stopping	WiFi processes are stopping	This is the result of moving the 3-position switch from **ACC** or **CLT** to **OFF**, or of toggling the "**Wifi Enabled**" control from "true" to "false" in the platform WiFi Configuration view, or an Access Point Inactivity Timeout. In the case of inactivity timeout, the next state will be "Inactivity Timeout" after WiFi is stopped. In all other cases, the next state will be "Stopped".
Stopped	WiFi drivers are not loaded, and no Client or Access Point mode processes are running.	WiFi LED on top of unit should be off in this state. The state must be "Stopped" before any WiFi process can be started. This state can be entered from a "failed" state or "stopping" state. As a special case for Access Point mode, if "Inactivity Timeout" is used AND inactivity timer is expired AND user moves the 3-position switch from ACC position, then Stopped state can be entered.
Failed	WiFi process (either Client or Access Point) was not able to successfully complete.	Usually indicates an invalid configuration. A "failed" state will kick off an attempted shutdown of the WiFi processes and drivers, after which the state should transition to "Stopped".

Client Mode WiFi states

The following current WiFi states are specific to Client mode.

Current WiFi State Value	Condition	Additional Notes
Supplicant Running	The supplicant is running, and loading the "Client Mode" network database to search for an Access Point to connect to.	After verification to ensure that no other adapter is using the Dhcp.client service, the "tiw_sta0" adapter is started, an IP address is assigned, and the "wpa_supplicant" process is started; the state will transition to the "Supplicant Running" state.
Sta Scanning	The Client mode WiFi adapter is looking for an Access Point to connect to by scanning available frequencies	This can happen if the WiFi network (ssid/password, etc) is not configured correctly or is unavailable because the Access Point is off or out of range.
Sta Trying to Associate	A configured Access Point has been located, and the supplicant is trying to associate with the access point.	If a whitelist is configured in the access point, the MAC address of this client adapter must pass the whitelist filters.
Sta Negotiating	The Client mode supplicant is negotiating capabilities and credentials with the access point	If successful, the next transition will be "Sta Running"
Sta Association Success	The Client has successfully associated with an Access Point	The Client and Access Point will begin a 4-way handshake process to validate credentials and establish common security protocol suites (see "Sta Negotiating")
Sta Disconnected	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, will not progress past this point. Every 15 seconds, the network database is reloaded, so configuration changes made during this state will be picked up.
Sta Error: Dhcp enabled on another adapter	The Client Mode could not be started.	Client mode WiFi could not be started because another adapter is using Dhcp to get it's IP address. Only one adapter is allowed to have a Dhcp assigned address, and WiFi Client mode always uses Dhcp to get an address for the client-mode adapter.

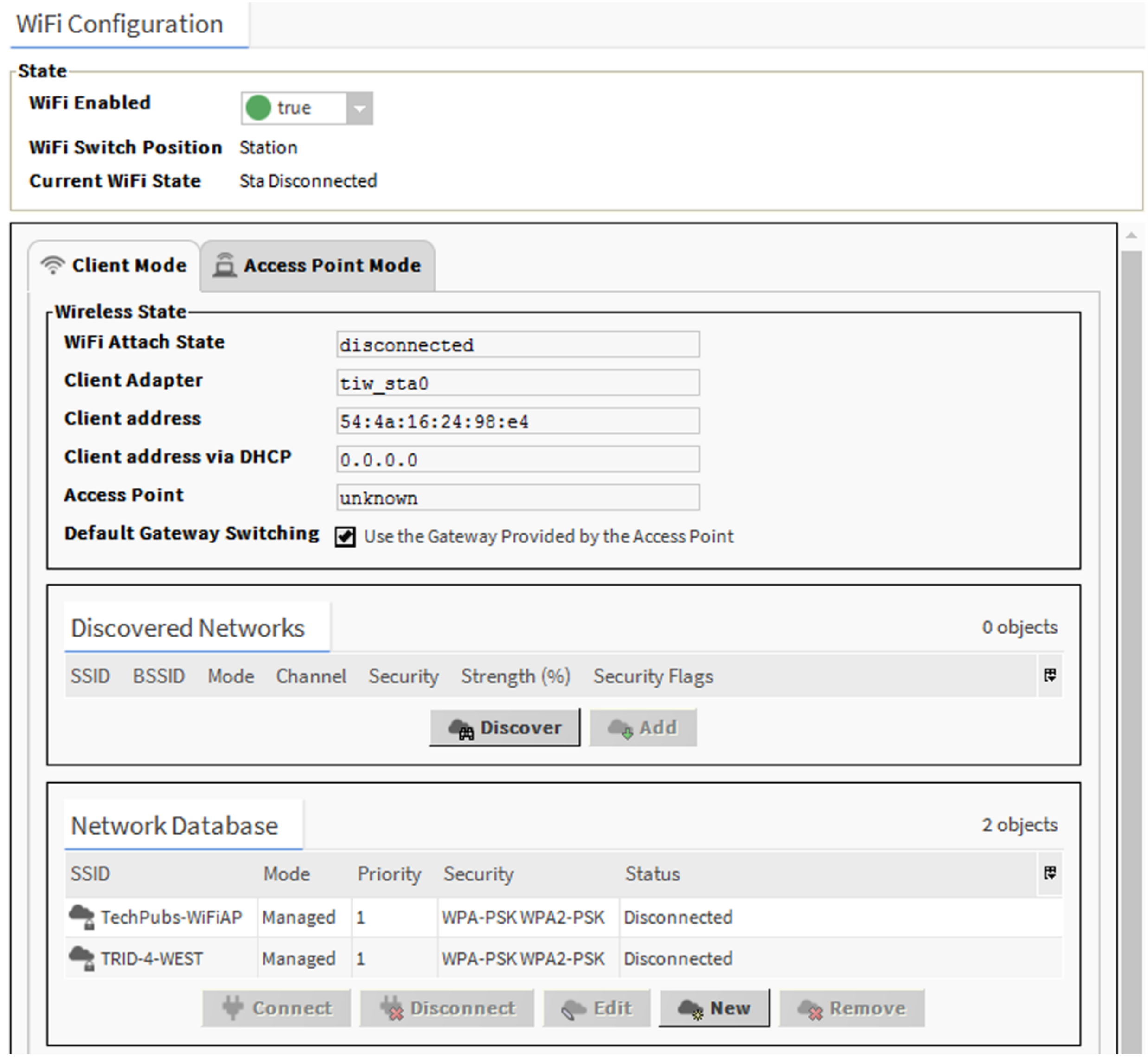
Access Point WiFi states

The following current WiFi states are specific to Access Point mode.

Current WiFi State Value	Condition	Additional Notes
SAP Starting	Access Point processes are starting. Access point mode is enabed in the **WiFi Configuration** view, and the 3-position switch on the unit is in the "ACC" (left) position.	Start WiFi driver which adds a "`tiw_sap0`" adapter, bring the adapter up and assign an IP address to it, start Hostapd, and start Dhcp server on the adapter. This state can only be entered from the "Stopped" state.
SAP Running	Adapter is up, IP assigned, Hostapd started, and Dhcp server started on the adapter.	SAP is Running
Inactivity Timeout	In Access Point mode, a non-zero "Inactivity Timeout" has been configured, and for the specified amount of time the adapter neither sends nor receives non-broadcast packets to/from attached clients. The adapter is shut down in this state.	Inactivity timeout is only used in Access Point mode. To restart the WiFi adapter after an Inactivity Timeout shutdown, you must physically move the WiFi selector switch from "ACC" to "OFF" in order for the state to transition to "Stopped". Once stopped, move the selector switch back to "ACC".

Client Mode tab

Figure 2 WiFi Configuration view, Client Mode tab



WiFi Configuration

State

WiFi Enabled ● true

WiFi Switch Position Station

Current WiFi State Sta Disconnected

Wireless State

WiFi Attach State disconnected

Client Adapter tiw_sta0

Client address 54:4a:16:24:98:e4

Client address via DHCP 0.0.0.0

Access Point unknown

Default Gateway Switching ☑ Use the Gateway Provided by the Access Point

Discovered Networks 0 objects

SSID	BSSID	Mode	Channel	Security	Strength (%)	Security Flags

Network Database 2 objects

SSID	Mode	Priority	Security	Status
TechPubs-WiFiAP	Managed	1	WPA-PSK WPA2-PSK	Disconnected
TRID-4-WEST	Managed	1	WPA-PSK WPA2-PSK	Disconnected

Wireless State configuration properties

Properties listed in the following table appear in the Wireless State pane of the **Client Mode** tab in the **WiFi Configuration** view.

Property	Value	Description
WiFi Attach State	Disconnected, Connected	Read only value.
Client Adapter	tiw_sta[*n*]	Read only value. Client Adapter name appended with number 0 through the maximum number of clients configured for the Access Point. For example: `tiw_sta0`, `tiw_sta1`, `tiw_sta2`, etc.
Client address	`00:00:00:00:00:0`	MAC address of the client device. Format is six HEX addresses separated by a colon, for example: `08:00:69:E2:01:FE`.

Property	Value	Description
Client address via DHCP	unknown	Read only value.
Access Point	unknown, last access point	Read only value. “Unknown” indicates the unit has never connected to an access point. Otherwise, display the name of the last access point the unit connected to.
Default Gateway Switching	enabled, disabled	When enabled (checked), uses the gateway provided by the Access Point. **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 JACE-8000 access point. When disabled (not checked), keep the gateway as assigned in **TCP/IP Configuration** view.

Discovered Networks table

Once the WiFi Selector Switch on the unit is in the CLT position, setting the WiFi Enabled property to “true” activates the **Discover** button.

Control buttons	Description
Discover	Scans for WiFi signals, displays a list of discovered networks in the table.
Add	Invokes the **Add a Wireless Network** dialog which allows you to configure connection properties for the selected network.

Network Database table

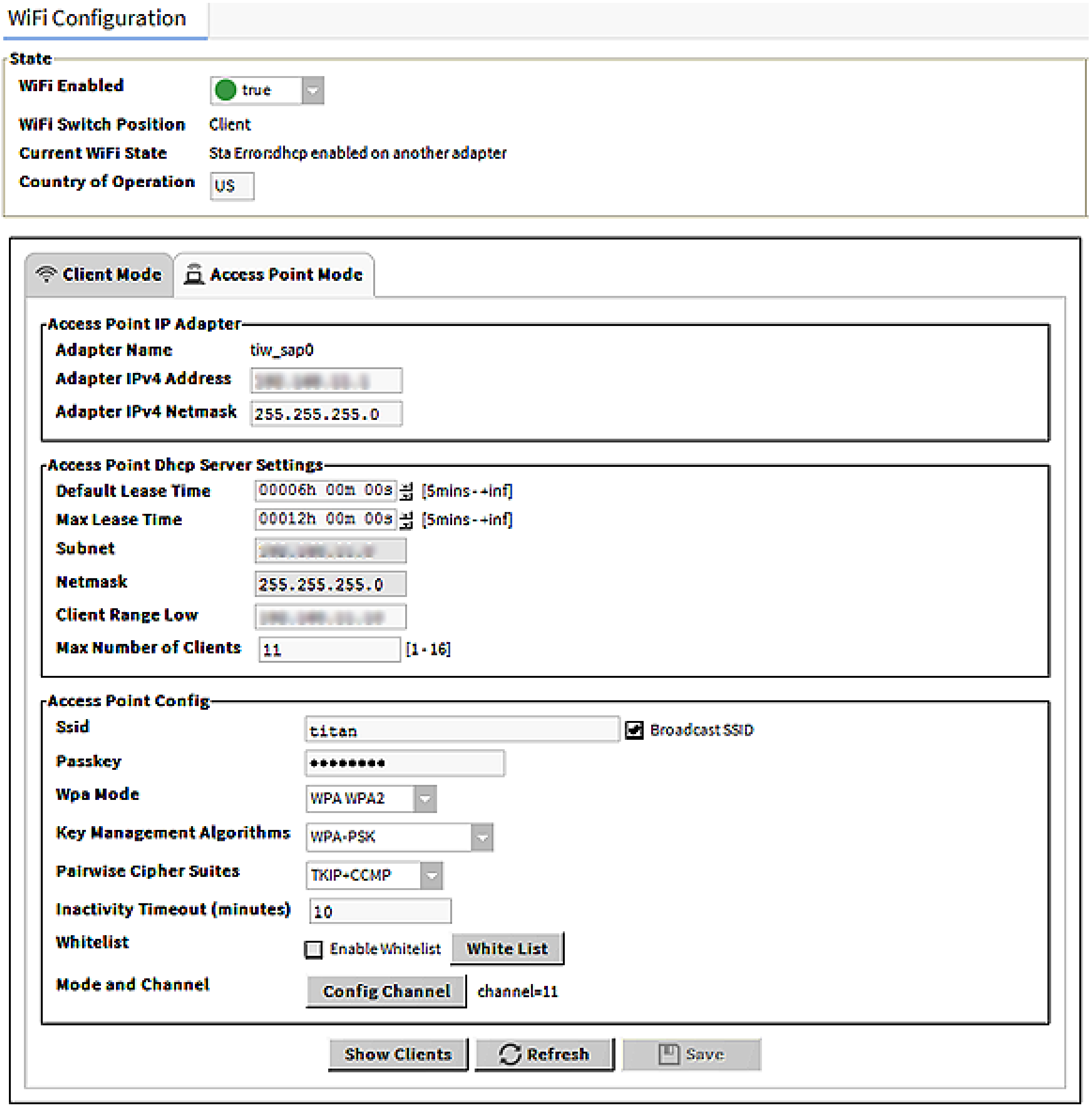
Lists added WiFi networks.

Control buttons	Description
Connect	Inactive (dimmed) until you select a network in the table to connect to.
Disconnect	Inactive (dimmed) until the unit is currently connected to an access point.
Edit	Inactive (dimmed) until you select a network. Invokes the **Edit a Wireless Network** dialog which allows you to change configured connection priority and/or access point passkey.
New	Invokes the **Create a New Wireless Network** dialog which allows you to configure access point properties and add the new network to the Network Database table.
Remove	Inactive (dimmed) until you select a network to delete. Clicking Remove invokes a confirmation dialog.

Access Point Mode tab

The figure shown here shows the Access Point Mode configuration properties with the controller's secondary LAN port configured for DHCP.

Figure 3 WiFi Configuration view, Access Point Mode tab



WiFi Configuration

State

WiFi Enabled: ● true

WiFi Switch Position: Client

Current WiFi State: Sta Error:dhcp enabled on another adapter

Country of Operation: US

Client Mode | Access Point Mode

Access Point IP Adapter

Adapter Name: tiw_sap0

Adapter IPv4 Address: [redacted]

Adapter IPv4 Netmask: 255.255.255.0

Access Point Dhcp Server Settings

Default Lease Time: 00006h 00m 00s [5mins-+inf]

Max Lease Time: 00012h 00m 00s [5mins-+inf]

Subnet: [redacted]

Netmask: 255.255.255.0

Client Range Low: [redacted]

Max Number of Clients: 11 [1-16]

Access Point Config

Ssid: titan ☑ Broadcast SSID

Passkey: •••••••••

Wpa Mode: WPA WPA2

Key Management Algorithms: WPA-PSK

Pairwise Cipher Suites: TKIP+CCMP

Inactivity Timeout (minutes): 10

Whitelist: □ Enable Whitelist [White List]

Mode and Channel: [Config Channel] channel=11

[Show Clients] [Refresh] [Save]

Access Point IP Adapter fields

Property	Value	Description
Adapter name	tiw_sap0 (default)	Read only value.
Adapter IPv4 Address	IP address	This sets the IP address of the WiFi adapter. A client uses this to make an IP connection over WiFi while the unit is functioning as an Access Point.
Adapter IPv4 Netmask	IP address	This sets the netmask of the WiFi adapter.

Access Point Dhcp Server Settings pane

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	12 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	11 (default)	Maximum number of WiFi clients that can attach at a given time (maximum limit is 16).

Access Point Config pane

Type	Value	Description
Ssid	titan (default)	Service Set Identifier 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 WiFi signal so that devices can detect and connect. If disabled, the SSID is "hidden" and not discoverable, and a client must be manually configured with the correct SSID which matches the JACE's Ssid field above.
Passkey	text	Sets a password that a client must enter to connect to this network. Strong password required
Wpa Mode	WPA WPA2 WPA WPA2 (default)	WiFi 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) WPA-EAP WPA-PSK WPA-EAP	Methods 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.

Type	Value	Description
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 WiFi adapter is shutdown completely. To restart it you must move the WiFi Selector Switch on the unit to "OFF". Once the WiFi Current State shows "Stopped", move the WiFi Selector Switch back to "ACC". Note, if the intended WiFi usage is for tool connectivity, then set this value to some small number of minutes. If the intended WiFi usage is for field bus integration, then set this value to "0" to disable the Timeout functionality. **CAUTION:** An Access Point represents a potential target for cyber attack. Leaving the Access Point disabled by default is a security best practice.
Whitelist	list	Allows you to configure the access point with a range of device MAC addresses that can connect.
Enable Whitelist	disable (default), enable	If enabled, only an address in the configured whitelist can connect. If disabled, connection to the access point is not limited to a specific range of devices.
Mode and Channel	Country code: two digit code Radio mode: 802.11a/b/g/n Bandwidth: HT20, HT40, HT20 HT40 Channel number: (number of channel options depends on selected radio mode)	Once it is configured, County Code is a read only value. The **Config Channel** button invokes the **Configure Mode and Channel** dialog, which you can use to modify radio mode, bandwidth, and channel selections.

Supported WiFi configurations

WiFi client and access point modes add support for a number of new network configurations. Supported network configurations are described in the following examples.

NOTE: Although other network configurations may exist they are not necessarily supported.

The JACE-8000 controller does not support IP routing between any combination of Ethernet and WiFi ports. The controller will not forward IP packets from LAN1 to LAN2, LAN1 to WiFi, WiFi to LAN2, etc. If an installation requires IP routing between WiFi and Ethernet ports, it may be configured using standard IT networking infrastructure components.

In the following figures, different networks are represented by thick gray lines. The JACE-8000 does not route traffic between different networks. Data may be shared at the application level.

WiFi Access Point for local tool connections

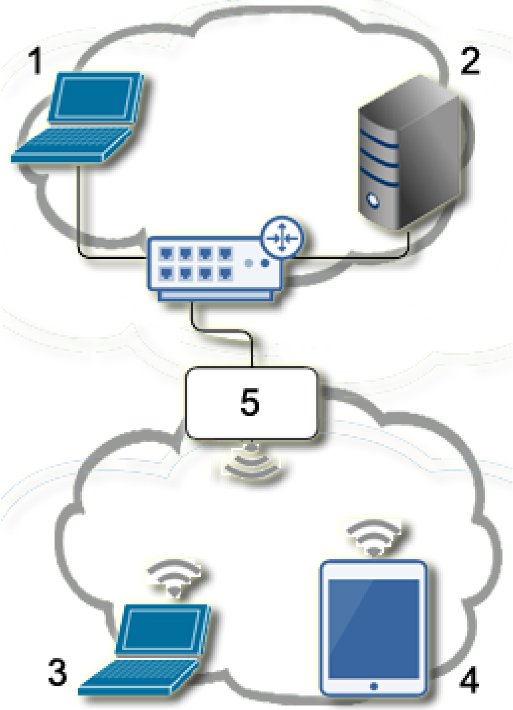
In this configuration, the JACE-8000 Access Point feature is turned on temporarily to provide a browser or Workbench with access to the platform and/or station running on the unit. The Access Point may support 3 or more simultaneous tool connections.

When configured for Access Point mode, tools such as laptops and mobile devices can connect to the WiFi adapter and access all features available over a wired Ethernet connection. For example, a tablet device can view web pages, or a laptop running Workbench can upgrade software.

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

When used for connecting tools, the WiFi may be left in disabled mode, then switch on (via physical switch) only when a user needs access to the unit.   Additionally, a timeout period can be configured to disable the AP mode after a certain period of inactivity. On reaching this timeout limit, the WiFi adapter is shutdown completely. To restart it you must move the WiFi Selector Switch on the unit to “OFF”. Once the WiFi Current State shows “Stopped”, move the WiFi Selector Switch back to “ACC”.

Figure 4 WiFi Access Point for local tools



1. Workbench B
2. Supervisor
3. Workbench A
4. Tablet A
5. JACE-8000 WiFi Access Point

In the above figure,

- Workbench A and Tablet A can access both the station and the platform on the controller.
- Workbench A and Tablet A cannot access the Supervisor since it is on a different network.
- Workbench B and Supervisor can access the station and the platform on the controller via the wired Ethernet connection.

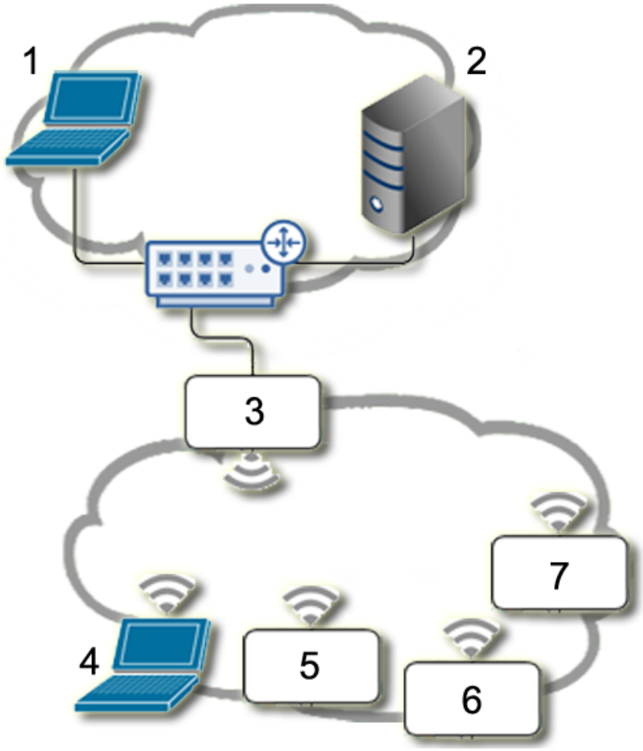
WiFi Access Point for field bus device integration

In this configuration, the JACE-8000 Access Point feature is turned on permanently in order to provide a network for WiFi enabled field bus devices, such as actuators, sensors, thermostats, etc. This Access Point can also be used by other JACE-8000 units that are configured for WiFi Client mode.

Both field bus devices and tools (laptop/mobile devices) can connect via the Access Point. Up to 16 devices are supported. However, if the maximum limit of 16 devices are connected then no tool access would be available.

In this configuration, the Access Point must always remain enabled so that tools and field bus devices can connect.

Figure 5 WiFi Access Point for WiFi Field Bus



1. Workbench B
2. Supervisor
3. JACE-8000 WiFi Access Point
4. Workbench A
5. WiFi Field Bus Device A
6. WiFi Field Bus Device B
7. WiFi Field Bus Device C

In the above figure,

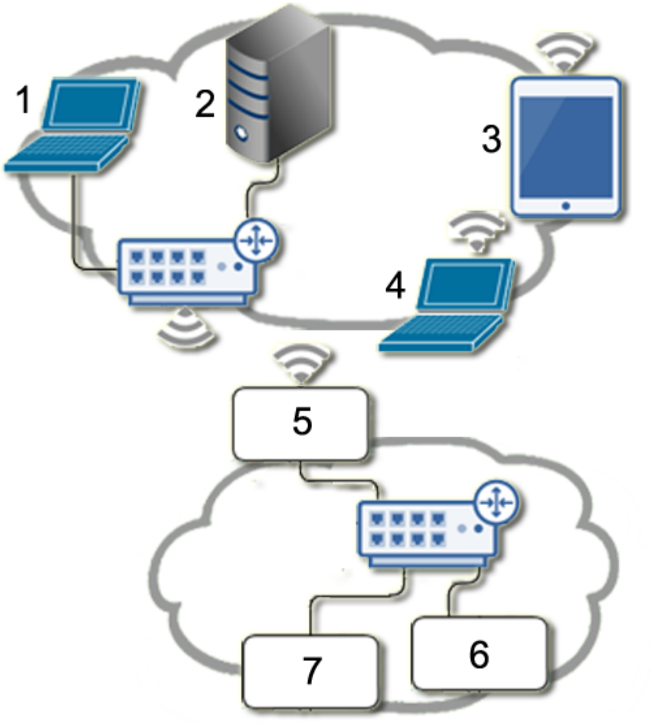
- Workbench A can access the controller. Also, the laptop can directly access WiFi field bus devices A, B and C using appropriate software. If the field bus devices are other JACE-8000 Clients, then Workbench A can also directly access.
- Workbench B and the Supervisor can access controller via the wired link, but do not have direct access to WiFi field bus devices.
- Additionally, JACE-8000 applications can read/write data from both networks.

WiFi Client

In this configuration, the JACE-8000 functions as a WiFi Client using an existing IT WiFi access point to gain access to a network. Also, one of the Ethernet ports on the JACE is used to connect some Ethernet-based field bus devices.

NOTE: JACE-8000 units deployed in the U.S. (and in countries that accept U.S. certification) and configured for Client mode cannot connect to an access point that uses Dynamic Frequency Selection (DFS) channels in the 5 GHz range. Unsupported DFS channels are listed here: 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140.

Figure 6 JACE-8000 as a WiFi Client



1. Workbench B
2. Supervisor
3. Tablet A
4. Workbench A
5. JACE-8000 WiFi Client
6. Ethernet Field Bus Device A
7. Ethernet Field Bus Device B

In the above figure,

- Workbench A, Tablet A, Workbench B and the Supervisor can all connect to the JACE using the IT networking infrastructure.

  All traffic not on the local subnet is routed through the default gateway on the JACE. This includes any broadcast traffic (Discovery) from the JACE. This means that if gateway switching is "enabled" on the JACE AND the Access Point provides a new default route in its configuration response to the JACE, then all non-local network traffic and broadcasts are routed to the Access Point and not to the field bus Ethernet when the JACE is attached to the WiFi network. It also means that the supervisor should be able to "discover and learn" the JACE.

  Conversely, if switching is disabled, the default gateway will stay pointing at the default gateway in the TCP/IP configuration of the JACE, regardless of any default route provided by the Access Point. This means that the supervisor/Workbench's need to be on the same subnet as the JACE, and any "discovery or learning" (which requires broadcasts and/or responses to broadcasts by the JACE) will not be possible because all the responses will be sent to the field bus network (which is still the default gateway).

  NOTE: Although discovery (broadcast) will not work, you can still add devices manually.

- The JACE can communicate with field bus devices.
- Other devices on the IT network cannot connect directly to the field bus devices, since they are on a separate network.

Glossary

access point	In a wireless local area network (WLAN), a wireless access point (WAP) is a hardware device, such as the JACE-8000, that allows wireless devices to connect to a wired network using WiFi, or related standards. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network.
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 WiFi phone. A client may be fixed, mobile or portable. Generally, in wireless networking terminology, a station, wireless client and node are often used interchangeably.
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.
IEEE 802.1x	An IEEE (Institute of Electrical and Electronics Engineers) standard for Port-based Network Access Control (PNAC) that is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism for devices seeking to attach to a LAN or WLAN.
PSK	Referred to as *WPA-PSK* (WiFi protected access-pre-shared key) mode, is a method of authentication key distribution.
SAP	In the context of the JACE-8000 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.
STA	In the context of the JACE-8000 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.
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.
TLS	Transport Layer Security is a cryptographic protocol that provides communication security over the Internet.
SSID	SSID (Service Set Identifier), an alphanumeric string (up to 32 characters), is a unique identifier for a specific WiFi 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.
whitelist	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 whitelist is an inventory of known MAC addresses that are permitted access to the Wi-Fi access point.
WPA WPA2	WPA (Wi-Fi Protected Access)/WPA2 (Wi-Fi Protected Access I) are two WiFi 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.

Index