Vocera Badge Configuration Guide

Vocera Voice Server Version 5.2.2

Firmware 4.3 - B3000n

Notice

Vocera Communications, Inc.
www.vocera.com
tel :: +1 408 882 5100
fax :: +1 408 882 5101

Last modified: 2018-12-10 14:26

Docs_VS_522Rel build 216

Contents

Introduction

Learn about the information in this guide.

Welcome to Vocera!

About this Guide

Learn about the information in this guide and the supported Vocera product versions.

Table 1: Supported Releases in this Guide

Vocera Firmware	Supported Badge
Up to Firmware Release 4.3	B2000, B3000, and B3000n

This Guide describes how to set up a Vocera configuration computer, configure badges using the Badge Properties Editor and the Badge Configuration Utility, and update badge properties and firmware.

Important: All voice commands and features mentioned in this guide are supported in Vocera 4.0 or later unless otherwise indicated.

While this document discusses how to set up a Vocera Voice Server configuration computer, configure badges using the Badge Properties Editor and the Badge Configuration Utility, and update badge properties and firmware it does not provide information about the badge properties you need to set to support your network environment, or details on specific badge features, and commands. See the *Vocera Infrastructure and Planning Guide* and the *Vocera Badge User Guide*for a complete description of these topics.

Configuring New Badges

This chapter summarizes the procedures for configuring an initial test badge, troubleshooting it if necessary, and then configuring the remaining badges.

To an end user, a badge is a convenient communication device. To your wireless network, however, a badge is a network client—it requires minor configuration before it can communicate with your network, as any wireless device does. For example, you must specify properties for your badge, such as the SSID your wireless network uses, and any security settings your network may require.

The first time you configure badges, you will need to refer to subsequent chapters in this manual for complete information. After you have configured badges once or twice, you can use this chapter by itself as a reminder of the basic steps in badge configuration.

Configuring a Test Badge

When you perform the initial badge configuration, set up a single test badge first, confirm that it connects to the network the way you intended, and troubleshoot your `badge.properties` file if it does not. After you can successfully connect with this test badge, you can configure the remaining badges.

Important: Make sure a single test badge can connect to your network before you configure all your badges. If you download incorrect properties to your badges and they cannot connect, you may need to reset the factory defaults on each individual badge—a labor-intensive process.

1. Set up a configuration computer using the network settings required to connect to badges that have factory default settings. See **Installing and Setting Up** on page 10 for details.
2. Use the Badge Properties Editor on the configuration computer to create a `badge.properties` file that specifies how your badges connect to your network.
   See **About Property Files** on page 19.

   Tip: Use the Badge Properties Editor to specify that a DHCP server is assigning IP addresses to the badges dynamically. If your badges require static IP addresses, see **About Assigning Static IP Addresses** on page 8.
3. Make sure the production Vocera Voice Server is running and the badge is within range of the wireless network to which it is trying to connect.
   The badge will attempt to connect to the Vocera Voice Server after updating itself from the Badge Configuration Utility.
4. On the Vocera configuration computer, choose Programs > Vocera > Badge Utilities > Badge Configuration Utility.
   The Badge Configuration Utility opens in a command window, displaying a list of firmware components and properties that the utility will download.
5. Attach a charged battery to a new badge (a badge that has never been configured).

A new badge automatically looks for the configuration computer (because the IP address of the configuration computer is set to 10.0.0.1) and connects to it. The Badge Configuration Utility displays the **start session** message, then it automatically starts downloading firmware and properties to the badge.

The Badge Configuration Utility continues to display messages as it downloads the firmware and properties. When the download is complete, the badge reboots and tries to connect to the network using the SSID and other network properties that you specified in the `badge.properties` file.

If the badge successfully connects to the network, it then tries to connect to the production Vocera Voice Server using the Vocera Voice Server IP Address that you specified in the `badge.properties` file.

6. Look at the screen of the badge:
   - The message "Logged Out" indicates that the badge is configured properly and has connected to the Vocera Voice Server.

     Continue with **Configuring the Remaining Badges** on page 7.
   - If the badge does not display "Logged Out" within 30 seconds to one minute, the badge is not configured properly and did not connect to the Vocera Voice Server.

     Continue with **Troubleshooting Badge Configuration** on page 40.
7. Shut down the Badge Configuration Utility.
   a. On the configuration computer, click the close icon in the upper-right corner of the command window in which the Badge Configuration Utility is running.
   The Badge Configuration Utility session ends, and the command window closes.
8. Copy the `badge.properties` file you created on the configuration computer to the `\vocera \config` directory of your production Vocera Voice Server.
9. Do either of the following:
   - If your production Vocera Voice Server is running, stop it and then restart it to load the `badge.properties` file into memory.
   - If your production Vocera Voice Server is not running, start it to load the `badge.properties` file into memory.

Configuring the Remaining Badges

After you have successfully configured and tested one badge, configure the remaining badges for your site. The procedure for configuring these badges is essentially the same as the procedure described in **Configuring a Test Badge**; you simply use the Badge Configuration Utility to connect to each of your remaining badges.

1. From the Windows **Start** menu on the configuration computer, choose **Programs > Vocera > Badge Utilities > Badge Configuration Utility**.
   The Badge Configuration Utility opens in a command window, displaying a list of firmware components and properties that the utility will download.
2. Attach a charged battery to a new badge.
   The following events occur:
   - The badge connects to the configuration computer.
   - The Badge Configuration Utility downloads firmware and properties to the badge.
   - The badge reboots and tries to connect to the production Vocera Voice Server.

   When the badge displays "Logged Out", configuration is complete.
3. Continue configuring the remaining badges.
4. When you are finished, shut down the Badge Configuration Utility.
5. To shut down the Badge Configuration Utility, click the close icon in the upper-right corner of the command window in which the Badge Configuration Utility is running.
   The Badge Configuration Utility session ends, and the command window closes.

About Assigning Static IP Addresses

You cannot use the Badge Properties Editor to assign static IP addresses, because each static address must be unique. Therefore, each badge that uses a static IP address must be configured manually. Because this is a slow and potentially error-prone process, use a DHCP server to assign IP addresses to badges whenever possible.

Use static IP addresses only in the following situations:

- You are setting up a small evaluation system.
- Static IP addresses are mandatory at your site.

Tip: If you are configuring badges with static IP addresses, DO NOT copy the the `badge.properties` file to the Vocera Voice Server.

Configuring Badges with Static IP Addresses

Assigning a static IP address cannot be performed in the Badge Properties Editor and must be configured manually.

To configure badges with static IP addresses:

1. Set up the configuration computer.
   See **Setting Up the Configuration Computer** on page 10.
2. Set up the isolated access point.
   See **Setting Up an Isolated Access Point** on page 14.
3. On the configuration computer, use the Badge Properties Editor to specify the badge properties required by your site, as described in **Using the Badge Properties Editor** on page 22.
   a. Select the badge type you are configuring.
      You can specify properties for multiple badge types during each Badge Properties Editor session.
   b. On the General, Security, and Wireless tabs of the Badge Properties Editor, specify properties for your wireless network.
   c. Click OK to save these values and close the Badge Properties Editor.
4. On the configuration computer, use Notepad to add the badge IP address property to the `\vocera\config\badge.properties file`:
   a. Open the `badge.properties` file in Notepad.
   b. Add or edit the badge IP address properties that corresponds to the type of badge you are configuring. The following table shows you the properties for each Vocera badge type:

Badge Type	Properties
B3000n	B3N.ConfigStaticIP B3N.BadgeIPAddr B3N.SubnetMask B3N.GatewayIPAddr B3N.DNS1IPAddr
B3000	B3.ConfigStaticIP B3.BadgeIPAddr B3.SubnetMask B3.GatewayIPAddr B3.DNS1IPAddr
B2000	B2.ConfigStaticIP B2.BadgeIPAddr B2.SubnetMask B2.GatewayIPAddr B2.DNS1IPAddr

For details of these badge properties, see Badge Property Reference on page 51.

Note: Be careful not to add any extra carriage returns, unnecessary spaces, or any special characters.

c. Save the `badge.properties` file, and leave Notepad open.

5. On the configuration computer, choose **Start > Programs > Vocera > Badge Utilities > Badge Configuration Utility**.
   The Badge Configuration Utility opens in a command window, displaying a list of firmware components and properties that the utility will download.
6. Insert a fully-charged battery into a new badge (one that has never been configured).
   A new badge automatically connects to a configuration computer with the IP address 10.0.0.1. When the badge connects, the Badge Configuration Utility displays the start session message, and then it starts downloading firmware and properties to the badge.
   If the badge fails to connect to the configuration computer, try resetting defaults. See Restoring Factory Default Settings on page 46.
7. When the download is complete, the badge reboots and tries to connect to the network.
   After the badge reboots, look at the badge screen:
   - The message “Logged Out” indicates that the badge is configured properly and has connected to the Vocera Voice Server.
   - If the badge does not display “Logged Out” within 30 seconds to one minute, the badge is not configured properly and did not connect to the Vocera Voice Server. See Troubleshooting Badge Configuration on page 40
8. If the badge was configured successfully, take the battery out of the badge, and set the badge aside.
9. Close the Badge Configuration Utility window.
10. Repeat steps Step 4 through Step 9 for as many badges as you need to configure.
11. When all badges are completely configured, switch to the Notepad window that you left open in step Step 4c. Remove lines beginning with B3.BadgeIPAddr, B2.BadgeIPAddr, or BadgeIPAddr, or type the pound sign (#) on the first column of that line.
12. Save the file and exit Notepad.

Tip:

If you are configuring badges with static IP addresses, do not copy the `badge.properties` file to the Vocera Voice Server.

Setting Up the Configuration Computer

A badge requires basic configuration information, such as an SSID and security settings, to connect to your wireless network. Because a badge has no keyboard, you cannot configure it directly. Instead, you must configure it from a special computer called a **configuration computer**.

This section describes how to set up the computer and other equipment needed to configure Vocera badges.

About Installation and Setup

A new badge is factory-programmed to establish a wireless connection to a computer with the IP address of 10.0.0.1 using an SSID of *vocera* (all lower-case), with open authentication and no encryption. After the badge connects to the configuration computer, you can use this computer to customize badge settings for your specific network requirements and security.

The configuration computer must be a stand-alone computer that is not connected to your site's network.

Tip: Any notebook, laptop, or desktop computer running Windows with an an Ethernet network card is typically sufficient for use as the configuration computer. If a Windows firewall or antivirus software with firewall capabilities is installed on this computer, either disable it or open UDP ports 54000 and 5555.

Installing and Setting Up

1. Install the Badge Utilities on the configuration computer. The Badge Utilities let you specify badge properties in a text file, then download the properties to your badges.
   See **Installing Badge Configuration Utilities** on page 11.
2. Assign a specific IP address (10.0.0.1) and subnet mask (255.0.0.0) to the configuration computer. When you boot a new badge, it looks for a computer with these properties that is running the Badge Configuration Utility.
   See **Specifying TCP/IP Properties** on page 13.
3. Cable the configuration computer directly to an access point that is set up without security requirements. Any access point security will prevent unconfigured badges from connecting.
   See **Setting Up an Isolated Access Point** on page 14.

Configuration Hardware Requirements

The requirements needed to create a dedicated server used for configuring Vocera devices is discussed in this topic.

The *configuration hardware* is the computer and other equipment that configures Vocera devices. The configuration computer is the computer on which you run the Vocera Badge Configuration Utility (BCU), so it is referred to as the BCU computer.

Vocera requires the following hardware configurations for badges and phones:

Component	Requirement
Configuration Computer	Refer to **Vocera Voice Server Sizing Matrix**.
Access Point	An isolated access point that is not connected to the installation network of the site.
Cable	An Ethernet crossover cable to connect the configuration computer and the access point.

Installing Badge Configuration Utilities

If the Badge Configuration Utilities from a previous version of Vocera are installed on the configuration computer, remove them before installing the current Badge Configuration Utilities. Vocera does not support more than one version of the Badge Configuration Utilities on a configuration computer. The Badge Configuration Utilities version and Vocera Voice Server version must be the same.

Use the following steps to install the Badge Configuration Utilities.

1. Log in to the computer with administrator privileges.
2. Locate and double click the Vocera Launcher file.

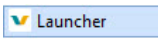


Figure 1: Vocera Launcher file

The Welcome window opens.

3. In the Welcome window, click Next to continue with the installation program.

Figure 2: Welcome Window

The License Agreement window opens.

4. Review the license agreement before accepting the terms and click Next.

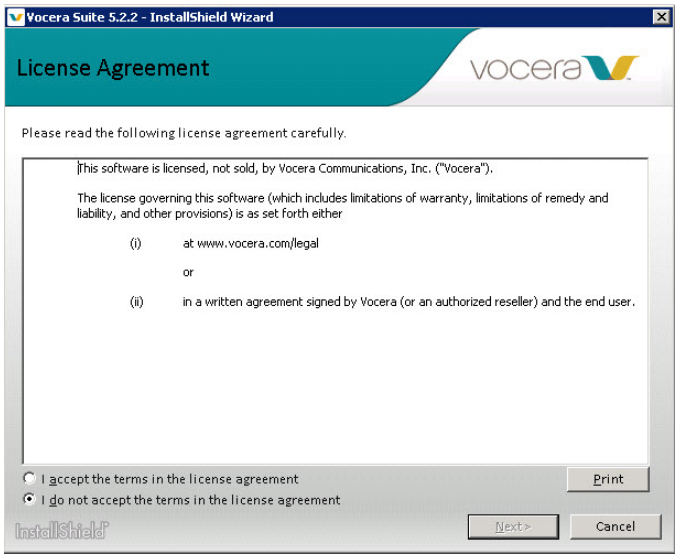


Figure 3: License Agreement Window

The Custom Setup Window opens.

5. In the Custom Setup window, select the Badge Configuration Utility radio button and click Next.

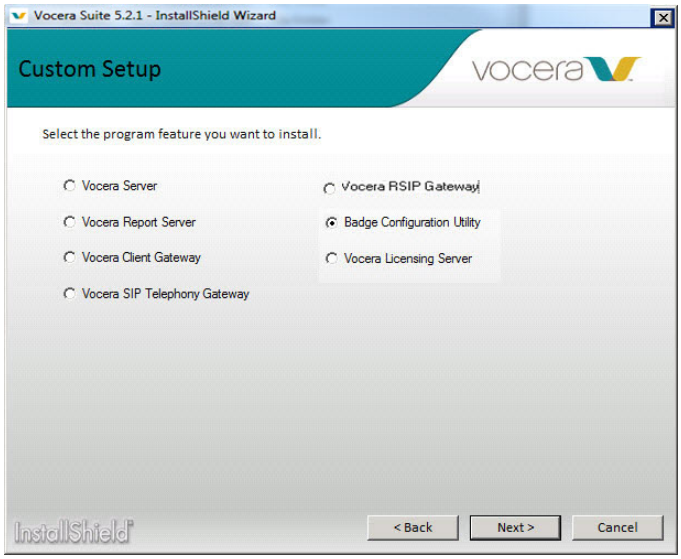


Figure 4: Custom Setup installation window

The Installation Configuration window opens.

6. In the Installation Configuration window, enter the IP address 10.0.0.1 and the drive where you want the Badge Configuration Utilities installed. Click Install.

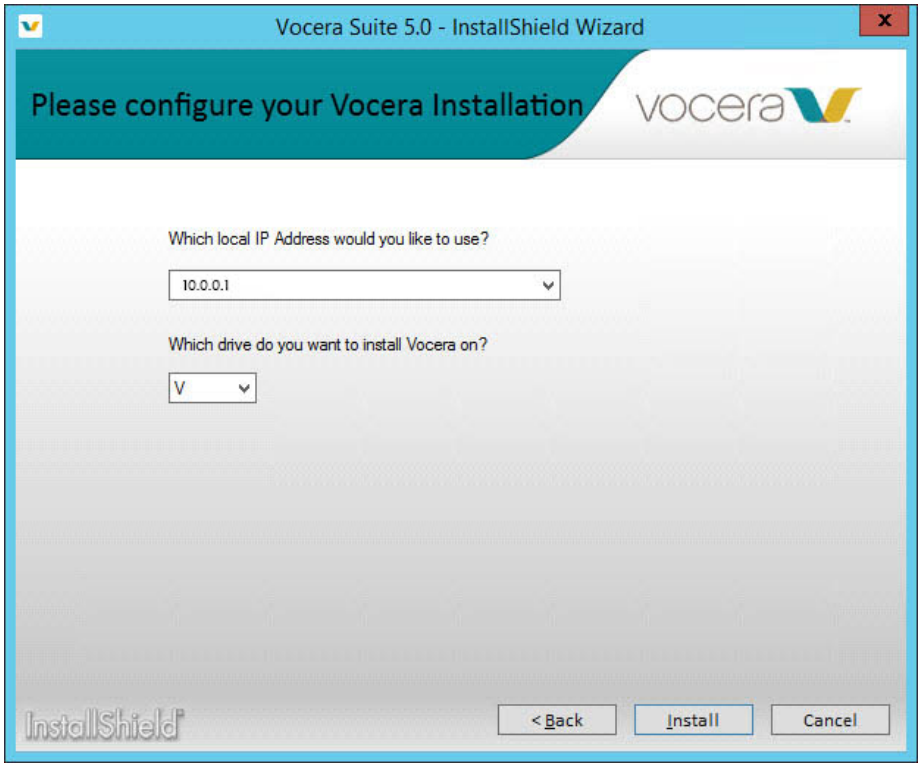
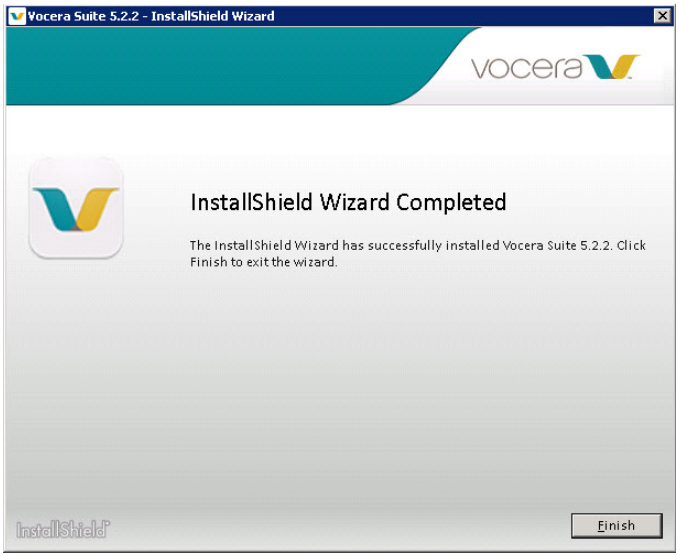


Figure 5: Installation Configuration window

The Vocera installer is launched with a progress bar showing the status of the installation.

7. When the installation is finished, a window appears announcing that the installation is complete. Click Finish.



Congratulations! Your installation is complete.

Specifying TCP/IP Properties

For a new badge to connect to the configuration computer properly, specify the following TCP/IP properties.

The exact procedure for setting your TCP/IP properties depends upon the version of the operating system. Refer to your Windows documentation for complete information.

In Windows, use the Network Connections control panel to specify the following TCP/IP properties for the network card in your configuration computer:

1. Set the **IP address** to 10.0.0.1.
   When you boot a new badge, it automatically looks for a computer with this address that is running the Badge Configuration Utility.
2. Set the **Subnet mask** to 255.0.0.0.

The exact procedure for setting your TCP/IP properties depends upon the version of the operating system. Refer to your Windows documentation for complete information. The exact procedure for setting your TCP/IP properties depends upon the version of the operating system. Refer to your Windows documentation for complete information.

Setting Up an Isolated Access Point

To set up a badge, connect the configuration computer to an isolated access point—one that is not connected to the site's network. The access point must be isolated from the rest of the network so you can set it up with a different SSID, and without compromising the site's security.

This isolated access point allows a badge to connect to the configuration computer using default factory settings. This access point is a temporary set up that you use only to configure badges. Configured badges can connect to your wireless LAN by using your existing SSID and security system.

When you are finished, your badge configuration hardware should be set up as follows:

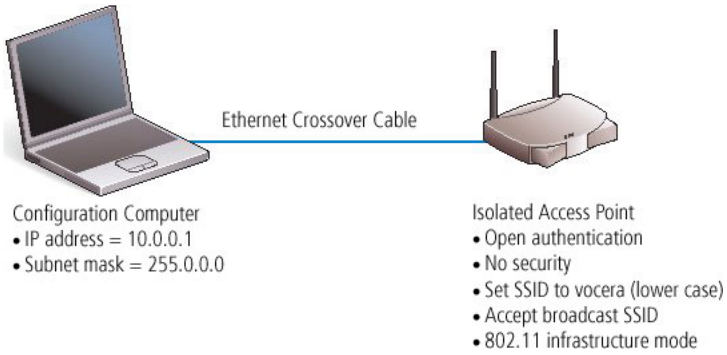


Figure 6: Badge configuration hardware

How to Set Up an Isolated Access Point

1. Attach an Ethernet crossover cable to the network port on the configuration computer.
2. Connect the other end of the cable to the Ethernet port on the access point.
3. If necessary, install configuration software for the access point on the configuration computer. Many access points require only a browser for configuration.
4. Using the access point configuration utility, make sure your access point is set up as follows:
   - Allow open authentication (typically the default)
   - Turn off all security (typically the default)
   - Assign the SSID value as `vocera`(using all lower-case letters)
   - Allow a broadcast SSID to associate (typically the default)
   - Configure as an access point in infrastructure mode (typically the default)

   The exact procedure for setting up your access point depends upon the hardware manufacturer. Refer to your access point documentation for complete information.

When Vocera badges come from the factory, their SSID property is set either to vocera or to <no value>. If you configure your access point as described above, both types of badges can connect to it.

Using the Badge Configuration Utility

The Badge Configuration Utility is a tool that can download properties and firmware from the configuration computer to:

- New badges that have never been configured.
- Badges that have been reset to factory defaults.
  See **Restoring Factory Default Settings** on page 46.

Because the Badge Configuration Utility is used with new badges, it must run on a stand-alone configuration computer. Each badge uses a built-in program called Updater during initial configuration. By default, the Updater program scans channels 1 through 11 attempting to connect to a Badge Configuration Utility on a machine whose IP address is 10.0.0.1. See **About Installation and Setup** on page 10.

After the badge downloads its properties and firmware, it reboots and attempts to connect to the network using the property values it has downloaded. If it connects to the network successfully, it then attempts to connect to the Vocera Voice Server.

Note: You can use the Badge Configuration Utility to configure all Vocera badge types simultaneously, up to a total of ten badges at one time.

About the Badge Configuration Utility

The `\vocera\config` directory on the configuration computer contains all the files used by the Badge Properties Editor and the Badge Configuration Utility. By default, the same set of files is also installed in this directory on the Vocera Voice Server computer.

The following directories and files in the `\vocera\config` directory are used by the Badge Configuration Utility:

Table 2: Directories and files used for configuration

Item	Description
gen2	Directory containing B2000 firmware, resources, and related files.
gen2\metadata\filelist	Auto-generated text file, created by both the Badge Configuration Utility and the Vocera Voice Server, containing the complete list of files for B2000 firmware. The Badge Configuration Utility and the Vocera Voice Server use this file to determine what files to download to a B2000 badge.
gen3	Directory containing B3000 firmware, resources, and related files.
gen3\metadata\filelist	Auto-generated text file, created by both the Badge Configuration Utility and the Vocera Voice Server, containing the complete list of files for B3000 firmware. The Badge Configuration Utility and the Vocera Voice Server use this file to determine what files to download to a B3000 badge.
gen3n	Directory containing B3000n firmware, resources, and related files.

Item	Description
gen3n\metadata\filelist	Auto-generated text file, created by both the Badge Configuration Utility and the Vocera Voice Server, containing the complete list of files for B3000n firmware. The Badge Configuration Utility and the Vocera Voice Server use this file to determine what files to download to a B3000n badge.
help	Directory containing help systems for the Badge Configuration Utility and the Badge Properties Editor.
lib	Directory containing the Badge Configuration Utility and the Badge Properties Editor applications.
badge.properties	Text file, created by the Badge Properties Editor, containing properties that determine badge behavior.
bcu.bat	Batch file that launches the Badge Configuration Utility.

Running the Badge Configuration Utility

1. From the Windows **Start** menu on the configuration computer, choose **Programs > Vocera > Badge Utilities > Badge Configuration Utility**.

   The Badge Configuration Utility opens in a command window.

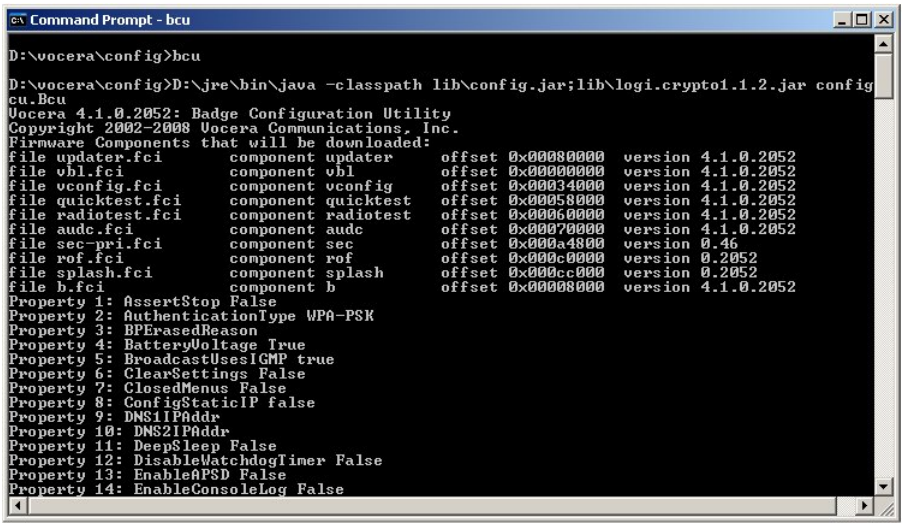


Figure 7: Badge Configuration Utility start-up

2. Attach a charged battery to either a new badge or a badge that has been reset to factory defaults.

   The badge automatically runs its Updater program because the `InstallDone` property is set to `False`. Updater looks for a Badge Configuration Utility running on 10.0.0.1 and connects to it.

3. The Badge Configuration Utility displays the **start session** message, and then the badge automatically starts the download process.
4. The Badge Configuration Utility continues to display messages as the badge downloads firmware and properties. When the download is complete, the Badge Configuration Utility displays the message **end session**.
5. The badge automatically reboots and tries to connect to the network, using the SSID and other network properties that it downloaded.

   If successful, the badge tries to connect to the Vocera Voice Server that was specified in the `ServerIPAddr` property.

6. Look at the screen of the badge:
   - The message “Logged Out” indicates that the badge is configured properly and has connected to the Vocera Voice Server.

     Continue with **Configuring the Remaining Badges** on page 7.

- If the badge does not display “Logged Out” within 30 seconds to one minute, the badge is not configured properly and did not connect to the Vocera Voice Server. Continue with **Troubleshooting Badge Configuration** on page 40

7. Shut down the Badge Configuration Utility. On the configuration computer, click the close icon in the upper-right corner of the command window in which the Badge Configuration Utility is running.
   The Badge Configuration Utility session ends, and the command window closes.

Property and Profile Files for the Badge

Badge properties tell a badge how to communicate on the wireless network deployed at your specific site. Use the Badge Properties Editor to create the `badge.properties` file to control general behavior and use the `profiles.txt` files for environments that require more than one wireless profile in a dynamic campus-type setting.

About Property Files

The `badge.properties` file tells a badge how to communicate on the wireless network deployed at your specific site.

Many of the properties that you specify determine how your badges connect to your network and behave in your specific environment. You can optimize many network settings to improve badge performance, and configure your badge accordingly.

See *Vocera Infrastructure Planning Guide* for information about how to configure your network infrastructure optimally to support the Vocera Communications System.

About Wireless LAN Properties

This section provides information related to WLANs created using the Vocera Badge Properties Editor.

Badge properties tell a badge how to communicate on the wireless network deployed at your specific site. Use the Badge Properties Editor to create a `badge.properties` file specifying the property values your site requires, and then use either the Badge Configuration Utility or the Vocera Voice Server to download these properties to all your badges.

Many of the properties that you specify determine how your badges connect to your network and behave in your specific environment. You can optimize many network settings to improve badge performance, and configure your badge accordingly.

A set of WLAN parameters can be scanned through for connectivity in different locations. Wireless clients learn about available APs by scanning other 802.11 channels for available APs on the same WLAN or SSID.

802.11r is the IEEE standard for fast roaming, where the initial authentication handshake with the target AP (that is, the next AP that the client intends to connect to) is done even before the client associates to the target AP. This is called Fast Transition (FT), and by default, fast transition is disabled.

See *Vocera Infrastructure Planning Guide* for information about how to configure your network infrastructure optimally to support the Vocera Communications System.

About Wireless Badge Profiles

A badge *profile* is the set of properties that specifies how that badge connects to your network. You can also create more than one profile which is listed in the `profiles.txt` file so you can enable Dynamic WLANs when badges are setup to connection to multiple wireless configurations moving from building to building in a campus environment .

Each type of Vocera badge has an independent profile, which allows different types of badges to run on VLANs/SSIDs that have different network and security settings. Consequently, you can tune different types of badges independently to optimize their performance, or give them any combination of different property settings for specific purposes.

You can set corresponding properties for each badge type to the same values or to different values, depending on the network security protocols you want to use.

For example, suppose different badge types use different SSIDs:

- B3000n badges connect to the *venus* SSID using PEAP.
- B3000 badges connect to the *mars* SSID using a pre-shared key.

Similarly, suppose all your badges reside on a single *voice* SSID using the same authentication and encryption settings. You would configure all badge types identically.

About Dynamic WLAN Profiles

This section contains information about Dynamic Wireless LAN profiles implementations for environments that requires more than one WLAN configuration.

Dynamic Wireless LAN profiles are intended for campus environments where the network administrator plans to deploy multiple WLAN configurations for different physical locations. This feature will permit the differing WLAN configurations to be provisioned in the B3000n where the badge is able to select the correct WLAN profile without requiring end user intervention.

You can also use this feature during WLAN transitions or upgrades where B3000n badges are moved dynamically to a new WLAN configuration when a previous WLAN configuration is disabled. This feature also benefits use cases where a facility's Wi-Fi is extended to home offices or remote offices where a different WLAN configuration is required, B3000n badges can dynamically select the appropriate configuration.

Dynamic Wireless LAN implementations are intrusive in that B3000n badges loses connectivity to an associated SSID before a scan for the new profile is initiated. It is intended for use cases where the B3000n is transported between locations during which it will lose connectivity, it is not intended for use inside a building where a rapid transition between SSIDs is desired.

Default Behavior and Restrictions

This topic describes the expected behavior and restrictions in an environment where dynamic profiles are implemented.

- There will be an interruption and communication delay of 60 seconds or longer as the Badge attempts to associate with a Wi-Fi network and transitions between multiple WLAN configurations.
- You can enable up to 4 WLAN profiles in your environment.
- This feature is available on B3000n only.

Wireless LAN Files

This section provides instructions for creating WLANs using the Badge Properties Editor.

The following directories and files in the `\vocera\config` directory are used and generated by the Badge Configuration Utility:

Table 3: Directories and files used for configuration

Item	Description
gen2	Directory containing B2000 firmware, resources, and related files.
gen2\metadata\filelist	Auto-generated text file, created by both the Badge Configuration Utility and the Vocera Voice Server, containing the complete list of files for B2000 firmware. The Badge Configuration Utility and the Vocera Voice Server use this file to determine what files to download to a B2000 badge.
gen3	Directory containing B3000 firmware, resources, and related files.
gen3\metadata\filelist	Auto-generated text file, created by both the Badge Configuration Utility and the Vocera Voice Server, containing the complete list of files for B3000 firmware. The Badge Configuration Utility and the Vocera Voice Server use this file to determine what files to download to a B3000 badge.
gen3n	Directory containing B3000n firmware, resources, and related files.
gen3n\metadata\filelist	Auto-generated text file, created by both the Badge Configuration Utility and the Vocera Voice Server, containing the complete list of files for B3000n firmware. The Badge Configuration Utility and the Vocera Voice Server use this file to determine what files to download to a B3000n badge.
help	Directory containing help systems for the Badge Configuration Utility and the Badge Properties Editor.
config	Directory containing the Badge Configuration Utility and the Badge Properties Editor applications.
badge.properties	Text file, created by the Badge Properties Editor, containing properties that determine badge behavior.
profiles.txt	(For B3000n only) Text file, generated by the Badge Properties Editor when you create dynamic wireless profiles for the badge. The profiles.txt file contains details of WLAN configurations, each with its own description and includes the priority used by WLAN profiles when selecting a profile and attempting to associate to the badge. The information in this file is populated with data from the badge.properties file and based on selections made when you create a new profile using the Badge Properties Editor user interface. **Note:** Vocera recommends that you do not edit these files manually.
bcu.bat	Batch file that launches the Badge Configuration Utility.
bpe.bat	Batch file that launches the Badge Properties Editor.

Using the Badge Properties Editor

The Badge Properties Editor is installed in the `\vocera\config` directory on both the configuration computer and the Vocera Voice Server computer. If you are performing the initial badge configuration, run the Badge Properties Editor on the configuration computer.

Tip: Use the Badge Properties Editor to create and modify the `badge.properties` file instead of using a text editor. Some values in `badge.properties` are encrypted; in addition, other properties are case sensitive or accept only a limited range of values. Using the Badge Properties Editor reduces the likelihood of creating incorrect property names or values.

1. Choose Start> Vocera> Badge Properties Editor.
   The Badge Properties Editor appears.
2. Select the badge type you are configuring.
   You can specify properties for multiple badge types during each Badge Properties Editor session. After you finish setting properties for one badge type, click Apply to save the properties, and then choose another badge type.
3. Set property values as described in the following topics:
   - **Setting General Properties** on page 24 describes the minimal set of properties you need to set for any badge in use at your site.
   - **Setting Security Properties** on page 26 describes how to make badges work with the security features implemented on your wireless network.
   - **Setting Wireless Properties** on page 35 describes properties that affect how the badge operates on you organization's wireless network.

   The Badge Properties Editor creates a text file called `badge.properties` in `\vocera\config`.

After you create the `badge.properties` file, you can upload the property values it contains to your badges.

- If you are configuring new badges, use the Badge Configuration Utility to download properties to the badges.
  See **About the Badge Configuration Utility** on page 16.
- If you are updating badges that are already connected to a Vocera Voice Server, use the Vocera Voice Server to download properties to the badges.
  See **Maintaining Properties and Firmware** on page 48.

Managing Dynamic WLAN Profiles

Learn how to manage Dynamic Wireless LAN profiles in environments that require more than one WLAN configuration.

To enable seamless wireless connections between different physical locations and Wireless LAN configurations in your environment, you can provision the badge to selects the correct WLAN profile while moving from wireless configuration to a new configuration without requiring end user intervention.

To create, edit, and delete Dynamic WLAN profiles, use the fields and buttons located at the top of the Badge Properties Editor User Interface.

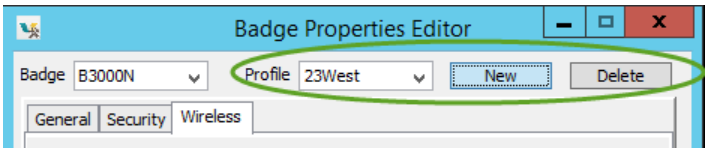


Figure 8: Wireless properties (B3000n)

Note: The Profile fields are greyed out for all badge types except B3000n.

The table below shows the available controls for managing multiple wireless profiles in your environment.

Control	Description
New	Click this button to create a new wireless profile.
Delete	Click this button after you select the desire profile from the Profile drop down menu if you want to delete it.
Profile selection drop down	Use the drop down box to select the badge profile that you want to review or edit.

Creating, Editing, and Deleting Dynamic Profiles

Follow these steps to create, edit, or delete a wireless configuration in your environment.

To create a new WLAN profile:

1. From the top of the Badge Properties Editor, click New. Be sure that `B3000n` is selected from the Badge drop down menu.

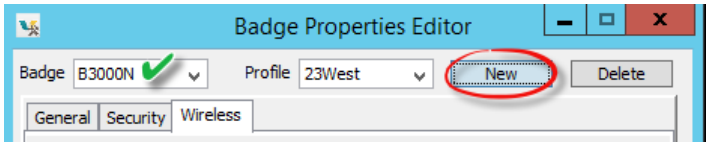


Figure 9: New profile creation (B3000n)

The Input dialog box displays.

2. Type the name of the new profile which must alphanumeric with no spaces.

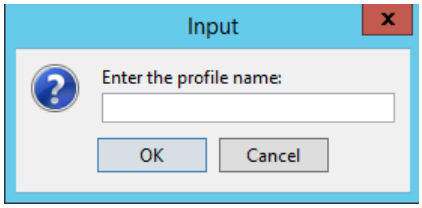


Figure 10: Input dialog box (B3000n)

3. Click OK. The new profile appears in the Profile drop down menu.
4. Open each tab on Badge Properties Editor dialog and enter the appropriate wireless settings for General, Security, and Wireless.

Note: Vocera strongly recommends that you use unique SSIDs for each new profile.

5. Click OK to save your changes and exit the Badge Properties Editor dialog or Apply to save your changes and remain in the application.

Note: Newly created WLAN profiles inherit parameters from the default WLAN Profile.

To edit a WLAN profile:

1. In the Badge drop down menu, click the down arrow and select the profile that you want to edit.
2. Open each tab on Badge Properties Editor dialog and enter the appropriate changes to the wireless settings for General, Security, and Wireless.
3. Click OK or Apply to save your changes.

To delete a WLAN profile:

1. In the Badge drop down menu, click the down arrow and select the profile that you want to delete.
2. From the top of the Badge Properties Editor, click Delete. A confirmation dialog box displays asking if you're sure.
3. Click OK. The profile is deleted and removed from the Profile drop down menu.

Setting General Properties

The general properties comprise the minimal set of properties needed by any badge at your site.

You must set values for all the general properties. Depending on the configuration of your site, you may have to set other properties as well.

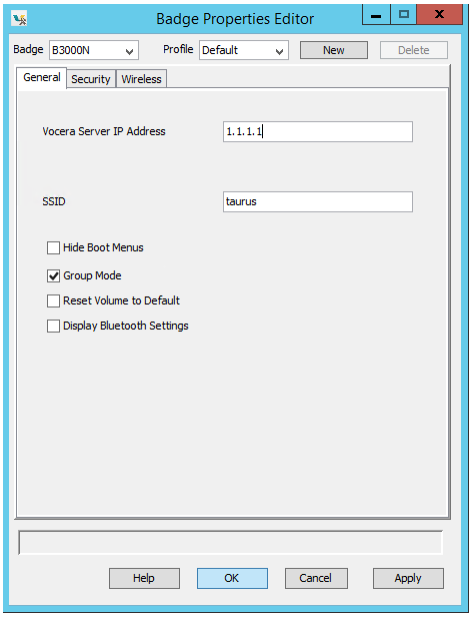


Figure 11: General properties (B3000n)

Table 4: Badge general properties

Property	Description	Badge Types Supported
Vocera Voice Server IP Address	Use the **Vocera Voice Server IP Address** field to specify the IP address of the computer which is running the Vocera Voice Server. This is a required field. Use dotted-decimal notation (such as 192.168.3.7) to specify this value. If you are configuring a cluster, enter the IP address of each machine in the cluster, separated by commas, with no spaces. Do not enter more than four comma-separated IP addresses. The Vocera Voice Server supports a maximum of four cluster nodes.	All
SSID	Use the **SSID** field to specify the SSID of the wireless network or subnet the Vocera badges will use. This is a required field. This value is case sensitive, and can be up to 32 characters in length. You can use initial or embedded spaces in the SSID value; trailing spaces cause an error message when the value is saved. Best Practice: Specify an SSID other than *vocera* (all lower-case) for your production server. Badges are factory-programmed to use the *vocera* SSID to establish a wireless connection to the configuration computer that you have set up for your Vocera system.	All
Hide Boot Menus	Check the **Hide Boot Menus** field to prevent a user from displaying the configuration menus on his or her badge. The badge configuration menus provide access to powerful utilities for maintenance and troubleshooting. Use these utilities only when you are working with Vocera Technical Support. **Note:** This property is ignored by the B3000 and B3000n badges, whose menus are always hidden.	B2000

Property	Description	Badge Types Supported
Group Mode	When checked, this property turns on Group Mode by default, which means that noise-canceling microphones are turned off when users are speaking to each other on a call. Group Mode widens the speech zone, allowing additional people to speak into the badge's primary microphone. By default, this property is selected. Uncheck it if you want to eliminate background noise when users are on a call. **Note:** B3000 and B3000n users can change the Group Mode setting on their badges, overriding the default. • For B3000: Group Mode is always off during Genie interactions and broadcasts. • For B3000n: Group Mode is automatically enabled when the badge is turned to a 105 degree angle to improve voice recognition when the badge is not placed in an optimal position.	B3000n, B3000
Reset Volume to Default	When this property is enabled, it resets the volume to the default at boot-up. Otherwise, the previous volume setting is maintained at boot-up. By default, this property is *not* selected.	B3000n, B3000, B2000
Display Bluetooth Settings	When this property is enabled, the Bluetooth settings will appear on the user's badge and are written to the badge.properties file.	B3000n

Setting Security Properties

Set badge security properties that correspond to the type of authentication and encryption employed by your wireless network.

If you are deploying multiple types of Vocera badges, you can configure them to reside on separate SSIDs and take advantage of the enhanced security support offered by newer badge models. If all your badges reside on the same SSID, the security you choose must be supported by all badge types. See **About Wireless Badge Profiles** on page 19 for information about configuring badges on separate SSIDs.

For more information about the security systems supported by Vocera, see the *Vocera Infrastructure Planning Guide*. The rest of this section describes how to use the Badge Properties Editor to configure badge security settings.

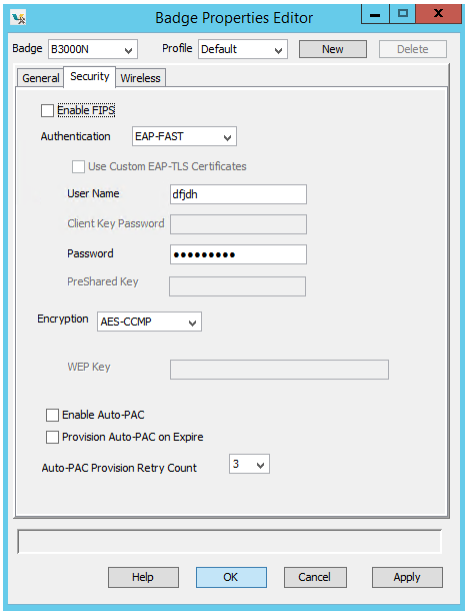


Figure 12: Security properties (B3000n)

Table 5: Badge security properties

Property	Description	Badge Types Supported
Enable FIPS	When enabled, this property causes the badge cryptographic security module to run in a secure mode that conforms with Federal Information Processing Standard (FIPS) 140-2. See **About Federal Information Processing Standard (FIPS)** on page 29. By default, this property is not selected. This property applies only to B2000 and B3000 badges currently. When the Enable FIPS box is checked, the B3000 requires WPA2-PSK, WPA2-PEAP, or WPA2-TLS. See **Enabling FIPS mode for B3000 badges** on page 29 for complete information on enabling these security profiles. For more information, see the *Vocera Infrastructure Planning Guide*. When the Enable FIPS box is checked, the B2000 requires WPA2-PSK or WPA2-PEAP. See **Enabling FIPS mode for B2000 badges** on page 30 for complete information on enabling these security profiles. For more information, see the *Vocera Infrastructure Planning Guide*.	B3000, B2000
Authentication	In the **Authentication** field, specify whether your wireless network requires authentication for access: • Specify **Open** if your wireless network does not require authentication. • If your wireless network requires authentication, specify the corresponding protocol. Important: If you are using EAP-FAST authentication, you can choose between automatic or manual PAC provisioning. If you choose manual PAC provisioning, you must create a `.pac` file on the Cisco ACS and copy it to the Vocera Voice Server and the Vocera configuration computer.	All
Use Custom EAP-TLS Certificates	When enabled, this property causes the badge to use custom EAP-TLS certificates rather than Vocera Manufacturer Certificates. If you use custom EAP-TLS certificates, you must generate your own self-signed certificates or obtain them from a trusted Certificate Authority (CA). If you check this box, additional configuration is required. You must install client-side certificates on the Vocera Voice Server and the configuration computer, install the server-side certificates on your authentication server, configure your authentication server for EAP-TLS, and specify the User Name and Client Key Password properties. Alternatively, uncheck this option to use the Vocera Manufacturer Certificates. Vocera badges are preconfigured with EAP-TLS client certificates that are automatically downloaded from the Vocera Voice Server or the Badge Configuration Unit. Vocera Manufacturer Certificates use 2048-bit RSA keys, which provide excellent security for today's enterprise and conform to industry standards and NIST recommendations. If you decide to use Vocera Manufacturer Certificates on the badge, you still need to install Vocera Voice Server-side certificates on your authentication server. By default, this property is not selected. This property is available only when the Authentication property is set to EAP-TLS.	B3000n, B3000, B2000

Property	Description	Badge Types Supported
User Name, Password	If your network uses either LEAP, WPA-PEAP, or EAP-FAST authentication with TKIP-WPA encryption, enter appropriate values in the User Name and Password fields. If your network uses EAP-TLS authentication with external certificates (instead of the Vocera Manufacturer Certificates), enter a value for the User Name field but not the Password field. Otherwise, skip both these fields. Each badge on a Vocera Voice Server must use the same user name and password for LEAP, WPA-PEAP, or EAP-FAST authentication. The user name format depends on requirements set by the RADIUS authentication server. For example, when using LEAP with Cisco ACS and Windows Active Directory, enter *domain\userid* in the User Name field, where *domain* is a Windows domain name and *userid* identifies the user. Other RADIUS servers may require the user name only. The password value is case sensitive. You can use initial or embedded spaces in either of these values; trailing spaces cause an error message when the values are saved. The badge supports a maximum of 128 alphanumeric characters for the User Name and 32 alphanumeric characters for the Password. In addition, the badge supports the following characters for LEAP passwords: `^ # ! * @ % & $` Note: If you are using EAP-FAST authentication and you change the User Name or Password values, you must also generate a new PAC file. With manual PAC provisioning, this means you must generate a new PAC file on the Cisco ACS and then copy it to the Vocera Voice Server and the Vocera configuration computer. With automatic PAC provisioning, you must restore the factory settings on the badge and then reconfigure it; see **Restoring Factory Default Settings** on page 46. When the badge reconnects, it retrieves the new PAC file automatically from the ACS.	All
Client Key Password	If your network uses EAP-TLS authentication and you checked the Use Custom EAP-TLS Certificates box, enter the password used to encrypt the client key. Otherwise, skip this field. The maximum length of the password is 32 alphanumeric characters.	All
PreShared Key	If your network uses WPA-PSK authentication, specify a 64-character, hexadecimal value in the **PreShared Key** field. Otherwise, skip this field. If you are configuring B3000n or B3000 badges, you can specify the ASCII passphrase for your wireless network instead of a hexadecimal value.	All
Encryption	In the **Encryption** field, choose a value from the drop-down list to specify the type of data encryption your wireless network requires. The list includes different values depending on the value in the **Authentication** field. If necessary, check access point settings to see which type of encryption to use. See "Master Security Table" in the *Vocera Infrastructure Planning Guide* for a summary of the authentication and encryption combinations supported by Vocera.	All
WEP Key	If you specified either **WEP64** or **WEP128** encryption, specify a value for the **WEP Key** field corresponding to the first WEP key slot. Use hexadecimal characters to enter the key that the access point is using. See **Configuring WEP Encryption** on page 31. **Note:** The WiFi Alliance (WFA) has deprecated support for WEP, and newer versions of wireless controllers may not have configuration options for TKIP. Even though the B3000n and B3000 badges support WEP or TKIP, Vocera recommends not using them.	All

Property	Description	Badge Types Supported
Enable Auto-PAC	Enables automatic provisioning of the Protected Access Credential (PAC) for EAP-FAST authentication. This replaces the manual method of creating a new PAC on the Cisco ACS when it expires and then copying it to the Vocera Voice Server and the Vocera configuration computer. By default, this property is not selected. In order to take advantage of this feature, you must also select EAP-FAST authentication. Note: If you enable automatic PAC provisioning, you must increase the EAP request timeout on your access points to 15 seconds. Otherwise, automatic PAC provisioning will not work. See the *Vocera Infrastructure Planning Guide* for additional information.	B3000n, B3000, B2000
Provision Auto-PAC on Expire	Enables the automatic provisioning of a new PAC when it expires. If this property is unchecked, a badge whose PAC has completely expired will display the following message: "Expired or invalid PAC credentials." **Note:** This message should appear only if a badge has been powered off or did not roam at all for a while and the master key and the retired master key on the Cisco ACS have expired. If this happens, the badge needs to be reconfigured. By default, this property is not selected. In order to take advantage of this feature, you must also select EAP-FAST authentication.	B3000n, B3000, B2000
Auto-PAC Provision Retry Count	Limits the number of times a badge attempts to retry retrieving a PAC from the Cisco ACS after the first attempt failed (for example, due to wireless network problems). Select a number from 0 to 5. If a badge exceeds the retry count, it displays the following message: "Too many retries for Auto-PAC provisioning." By default, this property is set to 0 (meaning no retries). In order to take advantage of this feature, you must also select EAP-FAST authentication.	B3000n, B3000, B2000

About Federal Information Processing Standard (FIPS)

The National Institute of Standards and Technology (NIST) issues Federal Information Processing Standards (FIPS) for Federal computer systems. The FIPS 140 Publication Series coordinate the requirements and standards for cryptographic modules (both hardware and software components).

For more information about Vocera FIPS support and the FIPS 140-2 standard, see the following documents:

- http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2107.pdf
- http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1287.pdf
- http://csrc.nist.gov/groups/STM/index.html

If you use Microsoft Internet Authentication Service (IAS) for your authentication server and your wireless network is configured for WPA-PEAP authentication, you need to download and install a Microsoft update for your IAS server to support FIPS 140-2. This update adds support for additional AES cipher suites in the `Schannel.dll` module. For details, see http://support.microsoft.com/kb/948963.

Enabling FIPS mode for B3000 badges

To enable FIPs mode on B3000 Vocera badges:

1. Configure an SSID on your wireless network for WPA2-PSK, WPA2-PEAP, or WPA2-TLS, the security settings required for running the badge in FIPS mode.
2. Start the Badge Properties Editor on the badge configuration computer.

3. In the Badge Type list, select B3000.
4. On the General tab, select the SSID that has been configured for WPA-PSK, WPA-PEAP, or EAP-TLS authentication and AES-CCMP encryption.
5. Click the Security tab.
6. Ensure that the checkbox next to Enable FIPS is selected.
7. Specify one of the following security profiles:
   a. To enable WPA2-PSK for Vocera badges:
      - Select WPA-PSK authentication in combination with AES-CCMP encryption
      - Specify the PreShared Key value
      - Select other badge properties as appropriate
   b. To enable WPA2-PEAP for Vocera badges:
      - Select WPA-PEAP authentication in combination with AES-CCMP encryption
      - Specify the User Name and Password values. Each badge must use the same user name and password.
      - Select other badge properties as appropriate
   c. To enable WPA2-TLS for Vocera badges:
      - Select EAP-TLS authentication in combination with AES-CCMP encryption
      - Configure the certificates as described in **Configuring Badge EAP-TLS Authentication Certificates** on page 31
      - Select other badge properties as appropriate
8. Click OK to save these values and close the Badge Properties Editor.
9. Configure a test badge to make sure it can connect to your network. See **Configuring a Test Badge** on page 6.
10. If the test badge connected successfully, copy the `badge.properties` file to the `\vocera\config` folder of the active Vocera Voice Server computer.
11. Use the Vocera Control Panel to stop and start the active Vocera Voice Server. When the Vocera Voice Server restarts, it pushes the updated badge properties to the badges.

Note: To see whether FIPS mode is currently enabled on a B3000 badge, select the Info menu, and then select FIPS Mode.

Enabling FIPS mode for B2000 badges

To enable FIPs mode on B2000 Vocera badges:

1. Configure an SSID on your wireless network for WPA2-PSK or WPA2-PEAP, the security settings required for running the badge in FIPS mode.
2. Start the Badge Properties Editor on the badge configuration computer.
3. In the Badge Type list, select B2000.
4. On the General tab, select the SSID that has been configured for WPA-PSK or WPA-PEAP authentication and AES-CCMP encryption.
5. Click the Security tab.
6. Ensure that the checkbox next to Enable FIPS is selected.
7. Specify one of the following security profiles:
   a. To enable WPA2-PSK for Vocera badges:
      - Select WPA-PSK authentication in combination with AES-CCMP encryption
      - Specify the PreShared Key value
      - Select other badge properties as appropriate
   b. To enable WPA2-PEAP for Vocera badges:
      - Select WPA-PEAP authentication in combination with AES-CCMP encryption

- Specify the User Name and Password values. Each badge must use the same user name and password.
- Select other badge properties as appropriate

8. Click OK to save these values and close the Badge Properties Editor.
9. Configure a test badge to make sure it can connect to your network. See **Configuring a Test Badge** on page 6.
10. If the test badge connected successfully, copy the `badge.properties` file to the `\vocera\config` folder of the active Vocera Voice Server computer.
11. Use the Vocera Control Panel to stop and start the active Vocera Voice Server. When the Vocera Voice Server restarts, it pushes the updated badge properties to the badges.

Note: To see whether FIPS mode is currently enabled on a B2000 badge, select the Info menu, and then select FIPS Mode.

Configuring WEP Encryption

When you provide Vocera security with WEP encryption, your access points and badges transmit data using hexadecimal keys. WEP uses 64-bit or 128-bit keys (sometimes called 40-bit or 104-bit keys, respectively) to encrypt and decrypt data. Although there are four WEP key slots, Vocera badges always use the first WEP key slot. To configure WEP encryption, specify the hexadecimal key in the WEP Key field.

Entering a Pre-shared Key for WPA-PSK

With WPA-PSK authentication, each wireless network device encrypts network traffic using either a WPA passphrase or a 256-bit hexadecimal key.

- If you are configuring B3000 or B3000n badges, specify either the WPA passphrase or the hexadecimal key for your network as the value of the PreSharedKey property.

  If you are specifying a WPA passphrase, it must be 63 or fewer characters in length. The Badge Properties Editor treats all entries of 64 or more characters as a hexadecimal value.
- If you are configuring B2000 badges, you must specify a 256-bit hexadecimal key as the value of the PreSharedKey property.

  You can generate the appropriate hexadecimal key from the combination of your WPA passphrase and your SSID with a tool such as the one provided by Wireshark at the following location:

  http://www.wireshark.org/tools/wpa-psk.html

Note: The encrypted value of the hexadecimal B2000 PreSharedKey property that appears in the `badge.properties` file is different than the encrypted value of the passphrase for the B3000 or B3000n property, even if all the other security settings are the same.

Because the length of the unencrypted passphrase and hexadecimal key are different, the corresponding lengths of their encrypted values in `badge.properties` also differ considerably.

Configuring Badge EAP-TLS Authentication Certificates

Learn how to configure Vocera Badges using certificates for authentication

The badge supports EAP-Transport Layer Security or EAP-TLS, which provides excellent security, relying on client and server-side certificates. EAP-TLS is an IETF open standard, and is universally supported by WLAN vendors. It provides strong security by requiring both the badge and an authentication server to prove their identities via public key cryptography, or digital certificates. The EAP-TLS exchange is encrypted in a TLS tunnel, making it resistant to dictionary attacks.

To simplify EAP-TLS configuration, Vocera supplies client- and server-side EAP-TLS certificates called Vocera Manufacturer Certificates. To use Vocera Manufacturer Certificates, uncheck the Use Custom EAP-TLS Certificates box. You can also generate your own self-signed certificates or obtain them from a trusted Certificate Authority (CA).

If you are implementing EAP-TLS, you will need to install certificates on one of the following authentication servers:

- Microsoft Internet Authentication Services (IAS)
- Cisco Access Control Server (ACS)

The Security properties you need to specify for EAP-TLS vary depending on whether you choose to use Vocera Manufacturer Certificates or custom EAP-TLS certificates.

Table 6: EAP-TLS certificate details

Using Vocera Manufacturer Certificates	Using Custom EAP-TLS Certificates
Authentication = EAP-TLS Use Custom EAP-TLS Certificates = unchecked Encryption = TKIP-WPA or AES-CCMP	Authentication = EAP-TLS Use Custom EAP-TLS Certificates = checked User Name = Username created on the authentication server Client Key Password = Password used to encrypt the client key Encryption = TKIP-WPA or AES-CCMP

For information about configuring EAP-TLS for Cisco ACS, see the *Vocera Infrastructure Planning Guide*.

Configuring Badge EAP-TLS Authentication for Unique Certificates

Learn how to configure Vocera Badges using unique certificates for each badge.

For added security and increased control over badges in your network, you can configuring Vocera badges to use unique certificates. Although not necessarily recommended by Vocera, some wirelesses environments warrant the additional security that unique certificates provide in the network. In most cases, this extra layer of security is not needed where a single certificate for all badges is sufficient. However, if your organization desires greater security and granularity of control you can use individual certificates.

If you decide to utilize unique certificates in your environment, you must preform a series of manual steps before running the BCU to update and provision your Vocera badges. In addition to the manual steps, you'll also need to apply maintenance differently than in environments configured to use a single certificate.

Installing OpenSSL on the BCU Computer

Learn the steps to install OpenSSL on your dedicated BCU computer.

Prerequisite: Install the Badge Configuration Utility which is available with Vocera Voice Server or from Technical Support. For information about using about using the Badge Configuration Utility, see "Using the Badge Configuration Utility" in *Badge Configuration Guide*.

Vocera recommends that you use OpenSSL to convert certificates from one format to another since the badges recognize PEM files rather than PFX. After you complete the manual configuration steps, and wile running the BCU, the BCU uses OpenSSL to perform the needed conversion.

To install OpenSSL on the dedicated BCU computer.

1. Download and install the latest version (Win32 OpenSSL v1.0.2f) of OpenSSL. For example, http://slproweb.com/products/Win32OpenSSL.html.
2. Proceed through the OpenSSL installation, accepting all the defaults. If a message appears stating that Visual C++ 2008 is required, exit the OpenSSL installation and download Visual C++ 2008 from this link: http://www.microsoft.com/downloads/en/confirmation.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF&displaylang=en
3. After OpenSSL is installed, copy openssl.exe from the installation path into the Vocera config directory. For example, `C:\OpenSSL-Win32\bin` and paste into `%vocera_drive%\vocera\config`.

Manual Configuration Steps for the Badge Properties Editor

Learn the manual steps that must be performed before running the Badge Properties Editor.

1. Create the following folders in the following location: **%vocera_drive%\vocera\config\certs\files**.
2. Place ALL client certificates (.pfx files) into the following folder:**%vocera_drive%\vocera\config\certs\files**.

   Note: Each certificate MUST contain the MAC address of the corresponding badge in the following format:
   - *00-09-ef-01-02-03.pfx*
   - *0009ef010203.pfx*
   - *Mchapman_0009EF01ABCD.pfx*

   Providing the MAC address using this format allows the BCU to determine the corresponding badge.
3. Navigate to **%vocera_drive%\vocera\config\gen3\badge\res\certificates\EAP-TLS** and perform the following:
   - Create two empty files and label them as follows; **client_key** and **client_cert** .

     Note: Do not provide an extension for these file.
   - Obtain the root CA certificate (for example, rootca.pem), then rename the certificate to **rootca_cert**.

     Note: Do not provide an extension for the certificate file.
   - Copy these three files and paste into the following locations:
     - %vocera_drive%\vocera\config\gen3n\badge\res\certificates\EAP-TLS
     - %vocera_drive%\vocera\config\gen2\badge\res\certificates\EAP-TLS
4. Open Badge Properties Editor (BPE):
   - Select the Badge Type (B2000 / B3000 / B3000N)
   - On the Security tab, configure the following for EAP-TLS:
     1. Authentication: *EAP-TLS*
     2. Select the check box next to Use Custom EAP-TLS Certificates:
     3. User Name: *x*
     4. Client Key Password: *y*
     5. Encryption: *AES-CCMP or TKIP-WPA*
   - Configure the remaining values for your badge properties
   - Click OK

Deploying Badges with Unique Certificates

Learn how to deploy Vocera Badges with unique certificates.

The BCU provides benefits beyond loading badge firmware and updates to the badge properties file. Although not necessarily recommended, you can use the BCU to accept PFX (PCKS12) format client certificate files and convert them to a PEM format which is supported by Vocera badges. This is achieved by using the MAC address referenced on the certificate file name, so that certificates are pushed to the provisioned badges.

1. From the Windows Start menu on the configuration computer, choose Programs > Vocera > Badge Utilities > Badge Configuration Utility. The Badge Configuration Utility opens in a command window.
2. Once command prompt window appears, press any key to continue.
3. For each certificate located in the **certs\files** folder, enter the PFX import password when prompted.

   Note: If the wrong import password is entered, the script will continue to run but the certificate will not be converted. If this occurs, restart the process by running the Badge Configuration Utility again.

   Result: After all the passwords are entered, the Badge Configuration Utility runs automatically were badges are provisioned with the needed firmware and properties, and each badge with a unique EAP-TLS certificate.

   In addition, the PFX converted certificates can be removed from the **certs/files** folder since the converted certificates are loaded automatically when the BCU is restarted.

   Note: These converted badge certificates are located in their own mac address folder here:**%vocera_drive%\vocera\config\certs\badges**

Maintenance for Badges with Unique Certificates

Learn how to apply maintenance for Vocera badges using unique certificates.

In most environments after the initial badge configuration is performed using the BCU, you can use the Vocera Voice Server to push certificate and firmware updates to the badges in your environment. However, in an environment where unique certificates are configured, you are required to use the BCU for some firmware and certificate updates and ***cannot*** perform these tasks using the Vocera Voice Server.

For updating badge firmware and properties:

- Badge firmware updates can be safely applied on your Vocera Voice Server. The firmware updates will not overwrite or remove your unique EAP-TLS certificate information when the badges are updated.
- The badge properties file on your Badge Configuration Computer can be copied onto your Vocera Voice Server: **%vocera_drive%\vocera\config**.

  You can safely apply system-wide badge property updates from the Vocera Voice Server and will not impact your badges unique EAP-TLS certificate information unless you are changing WLAN network security properties.

To renew certificates:

- When your badges approach the time to renew EAP-TLS certificates, they can only be updated using the Badge Configuration Utility.
- Follow the steps in Manual Configuration Steps for the Badge Properties Editor on page 33 and Deploying Badges with Unique Certificates on page 34 to convert and re-provision your new EAP-TLS badge certificate.

Setting Wireless Properties

The wireless properties affect how the badge operates on you organization's wireless network.

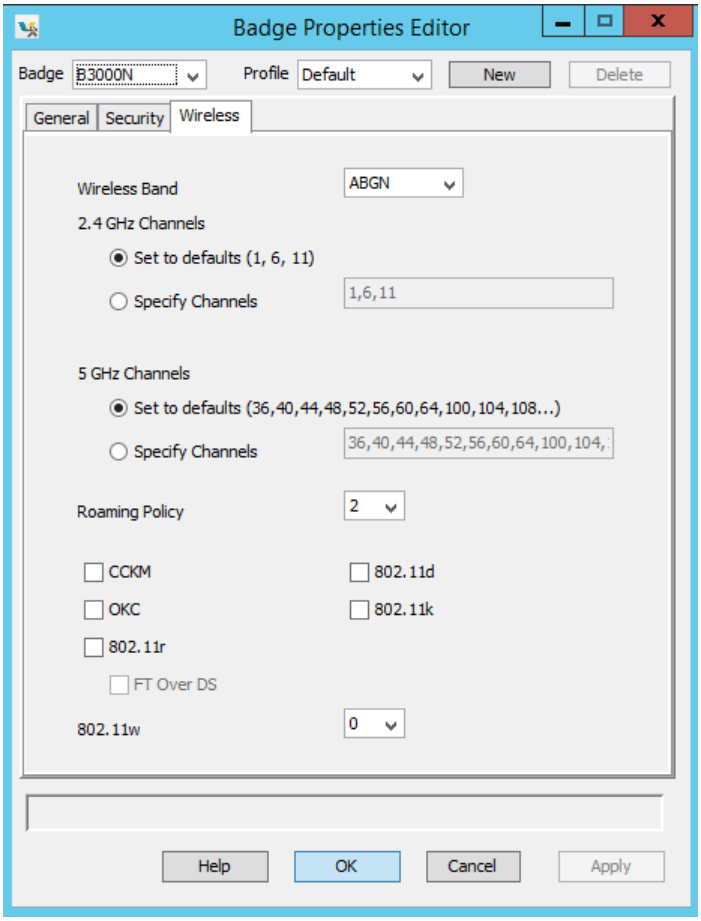


Figure 13: Wireless properties (B3000n)

Table 7: Wireless properties

Property	Description	Badge Types Supported
Wireless Band	Select the wireless bands used by the B3000n badge: • ABGN—Uses all 802.11 wireless bands (a, b, g, and n) at 2.4 GHz and 5 GHz. This is the default setting. • AN—Uses 802.11a and 802.11n wireless bands at 5 GHz. • BGN—Uses the the 802.11b, 802.11g, and 802.11n wireless bands at 2.4 GHz. • A—Uses the 802.11a wireless band at 5 GHz. • BG—Uses the 802.11b and 802.11g wireless bands at 2.4 GHz.	B3000n
2.4 GHz Channels: Set to Defaults (1, 6, 11)	Select this option to force badges to scan the three non-overlapping 2.4 GHz channels of 1, 6, and 11.	B3000n, B3000, B2000

Property	Description	Badge Types Supported
2.4 GHz Channels: Specify Channels	By default, B3000 and B2000 badges scan only channels 1, 6, and 11 unless you select the Specify Channels option. Selecting Specify Channels allows you to specify up to four arbitrary channels to scan. If the access points on your network are set either to four channels, to three channels other than 1, 6, and 11, or to fewer than three channels, select **Specify Channels** and enter the specific channel numbers in a comma-separated list. Make sure you specify only channels that are supported for your locale.	B3000n, B3000, B2000
5 GHz Channels: Set to Defaults (36, 40, 44, 48)	Select this option to force B3000n badges to scan the four 5 GHz channels of 36, 40, 44, and 48.	B3000n
5 GHz Channels: Specify Channels	By default, B3000n badges scan only channels 36, 40, 44, 48 unless you select the Specify Channels option. Selecting Specify Channels allows you to specify any number of the following channels in the 5 GHz band to scan: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165 Enter the specific channel numbers in a comma-separated list. Make sure you specify only channels that are supported for your locale. Also, make sure the 5Ghz channels available in the wireless controller match the ones defined in this property. See **Wireless Channels** on page 37.	B3000n
Roaming Policy	The **Roaming Policy** property specifies how quickly a badge searches for an access point when signal quality drops. Higher values cause a badge to search sooner, and may correct problems with choppy audio. However, a badge cannot send or receive audio packets while searching for an access point, so communication may be interrupted. Lower values allow a badge to tolerate lower signal quality before searching. The optimal threshold value varies from one 802.11 network to another, depending on how the network is configured. Select a value from 1 to 5. The default value is 2.	B3000n, B3000, B2000
CCKM	Use the **CCKM** field to specify whether you want to enable Cisco Certified Key Management. CCKM is a form of fast roaming supported on Cisco access points and on various routers. Using CCKM, Vocera devices can roam from one access point to another without any noticeable delay during reassociation. After a Vocera device is initially authenticated by the RADIUS authentication server, each access point on your network acts as a wireless domain service (WDS) and caches security credentials for CCKM-enabled client devices. When a Vocera device roams to a new access point, the WDS cache reduces the time it needs to reassociate. By default, this property is not selected. In order to take advantage of this feature, your access points must also support it, and you must use either LEAP, WPA-PEAP, EAP-FAST, or EAP-TLS authentication.	B3000n, B3000, B2000
802.11d	Use the **802.11d** field to specify whether you want badges to select AP channels based on the country code broadcast by access points and the channels entered in the Specify Channels fields. By default, this property is not selected. In order to take advantage of this feature, your access points must also support it.	B3000n, B3000, B2000
802.11k	Use the **802.11k** field to specify whether you want badges to make more informed roaming decisions, by discovering the best available access point. By default, this property is not selected. In order to take advantage of this feature, your access points must also support it.	B3000n

Property	Description	Badge Types Supported
802.11r	Use the **802.11r** field to specify whether you want badges to permit continuous connectivity for devices in motion. The default 802.11r roaming request takes place over the air (over Wi-Fi), but another option is to request that 802.11r roam request through the distribution system or wired network. Select FT Over DS, if you prefer to use a wired network over the default.	B3000n
802.11w	Use the **802.11w** field to specify whether you want badges to support protected management frames. By default, this property is not selected. In order to take advantage of this feature, your access points must also support it. In the drop down, select the number corresponding to how you want the badge to handle protected management frames (MFP): • Select 1: Makes MFP optional • Select 2: Makes MFP required	B3000n

Wireless Channels

Table 8: Wireless channels per locale

Country/Region	Radio Band / Channel Range					
	2400 to 2483.5 MHz	5.150 to 5.250 GHz (Band 1)	5.250 to 5.350 GHz (Band 2)	5.470 to 5.725 GHz (Band 3)	5.725 to 5.825 GHz (Band 4)	5.825 to 5.850 GHz (Band 4+)
	1-13	36-48	52-64	100-140	149-161	165
U.S., Canada, French Canada	1-11 (max 18 dBm)	36, 40, 44, 48 (max 16 dBm)	52, 56, 60, 64 (max 16 dBm - DFS and TPC)	100, 104, 108, 112, 116, 132, 136, 140 (max 16 dBm - DFS and TPC)	149, 153, 157, 161 (max 16 dBm)	165 (max 16 dBm)
Austria, Belgium, Bulgaria, Croatia, Cyrus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, UK	1-13 (max 18 dBm)	36, 40, 44, 48 (max 16 dBm)	52, 56, 60, 64 (max 16 dBm - DFS and TPC)	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 (max 16 dBm - DFS and TPC)	Not applicable	Not applicable
Australia New Zealand, Singapore	1-13 (max 18 dBm)	36, 40, 44, 48 (max 16 dBm)	52, 56, 60, 64 (max 16 dBm - DFS and TPC)	100, 104, 108, 112, 116, 132, 136, 140 (max 16 dBm - DFS and TPC)	149, 153, 157, 161 (max 16 dBm)	165 (max 16 dBm)
Saudi Arabia	1-13 (max 18 dBm)	36, 40, 44, 48 (max 16 dBm)	52, 56, 60, 64 (max 16 dBm - DFS and TPC)	100, 104, 108, 112, 116, 132, 136, 140 (max 16 dBm - DFS and TPC)	149, 153, 157, 161 (max 16 dBm)	Not applicable

Country/Region	Radio Band / Channel Range					
	2400 to 2483.5 MHz	5.150 to 5.250 GHz (Band 1)	5.250 to 5.350 GHz (Band 2)	5.470 to 5.725 GHz (Band 3)	5.725 to 5.825 GHz (Band 4)	5.825 to 5.850 GHz (Band 4+)
	1-13	36-48	52-64	100-140	149-161	165
United Arab Emirates	1-13 (max 18 dBm)	36, 40, 44, 48 (max 16 dBm)	52, 56, 60, 64 (max 16 dBm - DFS and TPC)	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 (max 16 dBm - DFS and TPC)	149, 153, 157, 161 (max 16 dBm)	165 (max 16 dBm)
Malaysia, Bahrain	1-13 (max 18 dBm)	36, 40, 44, 48 (max 16 dBm)	52, 56, 60, 64 (max 16 dBm - DFS and TPC)	Not applicable	149, 153, 157, 161 (max 16 dBm)	165 (max 16 dBm)
Qatar	1-13 (max 18 dBm)	Not applicable	Not applicable	Not applicable	149, 153, 157, 161 (max 16 dBm)	165 (max 16 dBm)
Kuwait	1-13 (max 18 dBm)	36, 40, 44, 48 (max 16 dBm)	52, 56, 60, 64 (max 16 dBm - DFS and TPC)	Not applicable	Not applicable	Not applicable
Oman	1-13 (max 18 dBm)	36, 40, 44, 48 (max 16 dBm)	52, 56, 60, 64 (max 16 dBm - DFS and TPC)	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 (max 16 dBm - DFS and TPC)	Not applicable	Not applicable

Enabling 802.11d

If you enable 802.11d and you roam with a badge to an access point that does not have 802.11d enabled, the badge will passively scan for beacons to discover what country it's in. If it finds beacons but the beacons do not identify the country, the badge will display the following message:

```
COUNTRY INFO NOT FOUND IN BEACONS
```

If this happens, press the Call button to clear the message, and then make sure that 802.11d is enabled on all access points.

Bluetooth Recommendations for B3000n

This topic describes Vocera recommendations for the radio frequency spectrum on the badge.

For optimal use in a wireless environment, Vocera recommends that you set B3000n badges to 5GHz radio frequency. By adjusting the spectrum to 5GHz, you can avoid the congestion and interference that can occur at lower frequencies such 2.4 GHz which is the standard range for wi-fi and Bluetooth.

To adjust the radio frequency:

- Open the Badge Properties Editor.
- On the Wireless Tab, in the Wireless Band dropdown menu select AN.
- Click OK or Apply.

Note: The 5GHz radio frequency is only available on B3000n badges. However, your wireless environment can include badges utilizing 5GHz and 2.4GHz.

When you select AN and change the badge frequency to 5GHz, BPE also enables APSD (Automatic Power Save Delivery). APSD is a power saving mechanism implemented in wi-fi standards. Utilizing APSD on the badge and network allows your mobile devices to save battery power when connected to the wi-fi network. It works by allowing your mobile devices to enter standby or sleep mode, and therefore it conserves battery. The APSD allows smooth transition in and out of sleep mode by allowing the mobile devices to signal the router of its status.

Troubleshooting Badge Configuration

This topic describes how to troubleshoot badge configuration problems using different diagnostic and configuration tools.

Troubleshooting the Initial Badge Configuration

If you complete the steps described in **Configuring a Test Badge** on page 6 and the screen of the test badge does not display the "Logged out" message, you need to troubleshoot it. The badge may not be configured properly, or there may be a problem with some of the other hardware and software you are using.

When the badge does not successfully connect to the production Vocera Voice Server at the end of its configuration cycle, one or more of the following problems may have occurred:

- The production Vocera Voice Server is not running.
- The badge is not within range of an access point used by the production server.
- The badge properties are not set correctly.

The screen of the badge displays a message that helps you diagnose the problem:

Badge Message	Typical Problems and Solutions
Searching for access points	The badge cannot connect to an access point on the wireless LAN used by the production server, possibly because: • The badge is not within range of an access point. If you configured the test badge in a remote area, make sure you are within range of the wireless network, then remove the battery from the badge and insert it again. • The SSID setting of the badge is incorrect. See **Badge Property Reference** on page 51. • The security settings of the badge are incorrect. See **Badge Property Reference** on page 51.
Requesting IP address	The badge is connected to an access point, but it cannot receive an IP address from a DHCP server, possibly because: • The security settings of the badge are incorrect. See **Badge Property Reference** on page 51. • The DHCP server is not active or cannot be reached from the badge. • The badge is associated with an access point that is not on the production network.

Badge Message	Typical Problems and Solutions
Searching for server	The badge is connected to an access point and has received an IP address, but it cannot connect to the Vocera Voice Server, possibly because: • The Vocera Voice Server is not running. Make sure the Vocera Voice Server is running, then remove the battery from the badge and insert it again. • The subnet that the badges are on cannot reach the subnet that the Vocera Voice Server is on. This situation can occur if you have set up an isolated subnet for the badges. Make sure the switch and router settings allow the badge subnet access to the server subnet, then remove the battery from the badge and insert it again. • The IP address of the Vocera Voice Server that you specified for the badge is incorrect.

See **Vocera Tech Support Knowledge Base article 1246** for more information on troubleshooting.

Troubleshooting the Badge Property Settings

Troubleshooting the badge property settings is an iterative process. If you did not successfully configure a badge the first time, you can reset the factory defaults and configure the badge again. You can repeat this process as many times as necessary.

1. Display the badge configuration menus.
   See **Displaying the Badge Configuration Menu (Older Software)** on page 42.
2. Reset all the badge properties to the factory default settings.
   See **Restoring Factory Default Settings** on page 46.
3. Launch the Badge Properties Editor again.
   When you launch the Badge Properties Editor after the initial configuration, it reloads your working settings from the `badge.properties` file. See **Using the Badge Properties Editor** on page 22 for information about launching the Badge Properties Editor.
4. Use the Badge Properties Editor to change the incorrect property values.
   Refer to the table in **Troubleshooting the Initial Badge Configuration** on page 40 for hints about what property values are incorrect. Then change the values as described in **Using the Badge Properties Editor** on page 22.
5. Configure the badge by running the Badge Configuration Utility again.
   See **Configuring a Test Badge** on page 6.

Using the Badge Configuration Menu

The badge configuration menu lets you access a set of diagnostic and configuration tools that are built into the badge. These tools are powerful—they are intended only for use when troubleshooting badge configuration.

Do not confuse the badge *configuration* menu with the *top-level* badge menu:

- The configuration menu contains utilities for configuration and troubleshooting, and it is only available *before* the badge fully boots.
- The top-level menu contains information and controls for end users, and it is only available *after* the badge fully boots.

The procedures for displaying the configuration menu in different badge models are similar, although the screens displayed by each are different.

How to Display the Badge Configuration Menu

Newer badge software (B3000n 4.0.0, B3000 3.1.1, or later) provides simplified access to the configuration menu. The configuration menu is hidden to prevent badge users from inadvertently accessing it, yet easy for administrators to display.

1. Remove the battery from the badge, then insert it again.
   The screen displays the word vocera.
2. Press and hold both the Hold/DND button (the button on top of the badge) and also the Call button (the large button on front of the badge).
   When the badge boots, the screen displays the following top-level configuration menu items:

Top-Leve Configuration Menu Item
APPS & TESTS
VERSIONS
ALL FILES...
REPAIR FILESYSTM
RESTART VBL
TO CONSOLE
REBOOT BADGE
RESET DFLT EAPTLS
RESET DEFAULTS

Displaying the Badge Configuration Menu (Older Software)

The Hide Boot Menus property determines whether the badge configuration menu is hidden, or if it can be easily accessed through the Hold/DND button.

Displaying the Badge Configuration Menu when Hide Boot Menus is True

Use the following steps to display the badge configuration menu when the Boot Menu is set to `TRUE`.

1. Remove the battery from the badge, then insert it again.
   The screen displays the name **vocera**.
2. Press and hold the **Hold/DND** button (the button on top of the badge). When the countdown timer appears (after about 15 seconds), release the button.
3. During the three-second countdown timer, use the following special sequence of button presses to display the badge configuration menus:

   DND Select Select Call Call Select Select Select Call

   This sequence consists of clicking the **Hold/DND** button, the **Select** button (the middle button on the side of the badge), and the **Call** button (the big button on the front of the badge). See Navigating in the Badge Configuration Menu on page 43 for an illustration showing the button locations.

   The screen of the badge displays the following top-level configuration menu items:

B3000 Menu	B2000 Menu
APPS & TESTS	APPS & TESTS
VERSIONS	VERSIONS
ALL FILES...	ALL FILES...
REPAIR FILESYSTM	RESTART VBL
RESTART VBL	TO CONSOLE
TO CONSOLE	REBOOT
REBOOT BADGE	RESET DFLT EAPTLS
RESET DFLT EAPTLS	RESET DEFAULTS
RESET DEFAULTS	

Displaying the Badge Configuration Menu when Hide Boot Menus is False

Use the following steps to display badge configuration menus when Hide Boot Menus is set to FALSE.

1. Remove the battery from the badge, then insert it again.
   The screen displays the name **vocera**.
2. Press and hold the **Hold/DND** button (the button on top of the badge). When the countdown timer appears (after about 15 seconds), release the button.
3. During the three-second countdown timer, press and release the **Hold/DND** button. See Navigating in the Badge Configuration Menu on page 43 for an illustration showing the button locations.
   The screen of the badge displays the following top-level configuration menu items:

B3000 Menu	B2000 Menu
APPS & TESTS	APPS & TESTS
VERSIONS	VERSIONS
ALL FILES...	ALL FILES...
REPAIR FILESYSTM	RESTART VBL
RESTART VBL	TO CONSOLE
TO CONSOLE	REBOOT
REBOOT BADGE	RESET DFLT EAPTLS
RESET DFLT EAPTLS	RESET DEFAULTS
RESET DEFAULTS	

Navigating in the Badge Configuration Menu

Because the screen of the badge is small, all the menu items are not visible at the same time. You can scroll to display more menu items at the same level, or you can select a menu item to view a nested set of items related to the upper-level menu choice.

Use the following buttons to navigate in the badge menus:

- The **Scroll Up** button (the top button on the side of the B2000 badge and on the front of the B3000n/B3000 badge)
  Press this button to scroll up through menu items.

  Note: On the B3000n/B3000 badge, the Scroll Up and Scroll Down buttons depend on the screen orientation.

- The **Scroll Down** button (the bottom button on the side of the B2000 badge and on the front of the B3000n/B3000 badge)
  Press this button to scroll down through menu items.
- The **Select** button (the middle button on the side of the B2000 badge and on the front of the B3000n/B3000 badge)
  Press this button to select a menu item. Depending on the selection you make, any of the following things can happen:
  - A lower-level set of menu items appears.
  - An action occurs (such as connecting to the vconfig utility).
  - A value is set (such as **TRUE** or **FALSE**).
- The **Call** button (the big button on the front of the badge)
  Press this button to navigate to an upper-level set of menu items. If you are already in the top-level set of menus, pressing the **Call** button does not navigate further.

The following illustration shows the location of the buttons on the B3000n badge (B3000 buttons are in the same location):

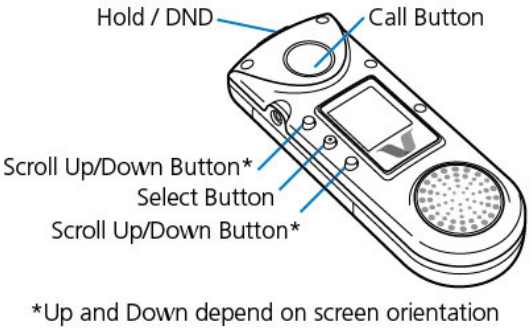


Figure 14: B3000n Badge buttons

Collecting Badge Data for Troubleshooting

The Vocera Badge Log Collector service and the `Sendlogs` utility allow you to collect all debug information from a B3000n, B3000, or B2000 badge and upload it directly to the Vocera Voice Server computer as a single file. While the Vocera Badge Log Collector service is running on the Vocera Voice Server, you can use it as an unattended log collection service to collect debug information from multiple badges. If you are working with Vocera Technical Support to troubleshoot problems you are having with a badge, you can send the file containing debug information to Vocera.

Note: If it is not possible to send badge logs to the Vocera Voice Server, you can send them to the Badge Configuration Utility machine. Contact Vocera Technical Support for assistance.

When a badge connects to the host using the `Sendlogs` utility, the following files are uploaded to the host computer. These files are helpful when troubleshooting problems with a badge.

- `log.txt, log.old1.txt (B3000n)`
- `log.txt, log.txt.old (B3000, B2000)`
- `badge.properties`
- `*.erbin`
- Other related files

Note: The `Sendlogs` utility uses a unicast connection to the host computer, so it allows you to upload badge information on a wireless network that blocks broadcast traffic.

To collect badge data using the `Sendlogs` utility:

1. On a B3000n or B3000 badge, press and hold the Select button for about 10 seconds until the `Sendlogs` utility starts (about 5 seconds on the B2000 badge).
   The Select button is the middle button of the three small buttons on the front of the B3000n/B3000 badge and on the side of the B2000 badge.

   Note: You can start `Sendlogs` when the badge is on a call, but the call will be dropped.
2. The badge connects directly to the Vocera Voice Server computer using a Vocera Voice Server unicast transmission.
3. The badge assembles a package of files into a single `.tar.gz` file and uploads it to the `\vocera\logs\BadgeLogCollector\uploads` directory on the host. If you have a Vocera Voice Server cluster, the logs may be located in any of the nodes identified in ServerIpAddr (not necessarily the active node). The format of the filename is `DATETIME-USERNAME-BADGEMACudd.tar.gz`.
4. After uploading the badge data (about a minute), the badge restarts.

Note: You can also launch the `Sendlogs` utility from the badge configuration menu. After you display the configuration menu, choose APPS & TESTS > SENDLOGS.SH. See **Using the Badge Configuration Menu** on page 41.

Running the Quick Test

If you suspect that a B3000n/B3000 badge is not working properly, you can run the Quick Test utility to diagnose possible problems. Vocera recommends that you run the Quick Test before contacting Vocera Technical Support to report a problem with the badge.

Note: The Quick Test is not available on badges earlier than the B3000.

The Quick Test utility tests badge features in the following sequence:

- The OLED screen
- The speaker and microphones
- The battery
- The green and amber indicator lights
- The red, green, and blue halo lights (B3000n only)
- The WLAN radio
- The badge's buttons (Call, DND, Up, Select, and Down)

You should run the Quick Test in a quiet room. Otherwise, the audio test will not be accurate. Also, make sure you do not cover any of the microphones with your fingers.

Important: If you encounter a failure in any portion of the Quick Test, contact Vocera Technical Support for further assistance.

To run the B3000n/B3000 Quick Test:

1. Remove the battery from the badge, then insert it again.

   The screen displays the word vocera and proceeds to count from 1 to 6.
2. When the screen reaches 6, press and hold the Call button (the large button on the front of the badge) for about 5 seconds. When you see patterns on the OLED screen, the Quick Test has started and you can release the Call button.
3. The Quick Test proceeds through the following tests:
   a. OLED test: When the OLED test starts (the pixels will go from off to on), make sure you remove your fingers from the microphones because the audio test starts next. You must watch the OLED screen during the test to identify any problems; the Quick Test will not report an OLED failure. What sort of problems should you look for? Check to see whether a significant portion of the screen is on or off at all times, which would interfere with your ability to read the screen.
   b. Audio test: Be quiet during the audio test. Sound will play for 5 seconds, and the screen will indicate whether the four microphones are working.

      Note: If the Quick Test reports that one or more of the microphones has failed, you may have inadvertently covered the microphones with your fingers while holding the badge. Try running the Quick Test again, and this time be careful not to cover the microphones.
   c. Battery test: Shows information about the battery temperature, voltage, current, and power.
   d. LED test: You must watch the green and amber lights to identify any problems. Make sure they turn on and off.
   e. Halo test: Watch the halo lights to identify any problems. Make sure they turn on and off (B3000n only).

f. WLAN test: Shows the radio configuration, AP table, and IP table. The badge will associate with an AP, and, if using DHCP, request an IP address.

g. Button test: Prompts you to press and release each of the buttons to make sure they are working.

4. When you are finished with the button test, press and hold the Call button to exit the Quick Test.
5. After the badge restarts, you can send logs of the Quick Test to the server using the `Sendlogs` utility. See **Collecting Badge Data for Troubleshooting** on page 44.

Note: If you encounter a failure in any portion of the Quick Test, contact Vocera Technical Support for further assistance.

Repairing the File System

The B3000n/B3000 badge is designed to automatically recover from problems that may occur with its file system. Despite this safeguard, in very rare circumstances one or more files on a badge may become corrupted. When this happens, your badge may continuously reboot, or a badge program may not start. To correct a problem with a corrupted file, you can run the REPAIR FILESYSTM utility, which is available on the badge configuration menu.

The B3000n/B3000 badge has two partitions: the main partition which is read/write, and a backup partion which is read-only. When you run the REPAIR FILESYSTM utility, the badge checks the file system and repairs any corrupted files.

Note: You cannot repair the file system of badges earlier than the B3000.

1. Display the badge configuration menu.
   See **Using the Badge Configuration Utility** on page 16.
2. Press the Down button to highlight the REPAIR FILESYSTM command.
3. Press the Select button. The badge displays three choices:
   - NO - CANCEL!
   - YES - REPAIR!
   - YES - WIPE N REPA
4. Do one of the following:
   - Press the Down button to highlight YES - REPAIR!
     The badge will check the file system and repair any corrupted files by copying files from the backup partition to the main partition.
   - Press the Down button to highlight YES - WIPE N REPA
     The badge will delete all files from the main partition and copy all files from the backup partition to the main partition.
5. Press the Select button.
6. Wait while the badge reboots and then proceeds to update the file system. When the update is complete (after a minute or two), the badge reboots.

Restoring Factory Default Settings

When you use the Badge Configuration Utility, you download property values that specify how a badge connects to your network and the way it behaves when it is connected. If one or more of these values are incorrect, you can restore all the factory default settings and configure the badge again. After you restore factory default settings on the badge, it automatically connects to the machine running the Badge Configuration Utility when it powers up.

1. Display the badge configuration menu.

See Using the Badge Configuration Menu on page 41.

2. Scroll down and select the **RESET DEFAULTS** menu item.
   The screen displays a confirmation menu.
3. Select **YES - RESET!**
   Any existing badge property values are erased, and the factory default values are restored. The badge reboots and tries to connect to the configuration computer at the IP address 10.0.0.1.

   Note: If the Badge Configuration Utility is running, the badge automatically downloads the current property values when it reboots. If you are not ready to download properties, make sure you exit the Badge Configuration Utility before resetting the badge defaults.
4. When you see the Vocera splash screen, remove the battery from the badge.

Restoring a Badge to its Factory Image

Only restore a badge to its factory image if the badge is not performing normally or if you think the firmware image may have been corrupted. It takes much longer to perform this procedure than it does to restore factory default settings on the badge.

How to Restore the B3000n/B3000 Factory Image

1. Make sure you start with a fully charged battery.
2. Remove the battery from the badge.
3. Press and hold the Select button, and then insert the battery again.
   The Badge U-boot screen appears.
4. Press the Hold/DND button to see the factory reset menu.
   The badge prompts, Reset badge?
5. Press the Select button to confirm that you want to restore the factory image on the badge. Otherwise, press any other button to cancel restoring the factory image.
   Once you confirm, the badge displays the following prompt: "Warning: Leave the badge powered on for 10 min and wait. Do not interrupt."
6. When the update is finished, the default settings are restored and the badge can be configured again.

How to Restore the B2000 Factory Image

1. Make sure you start with a fully charged battery.
2. Remove the battery from the badge.
3. Press and hold the Select button, and then insert the battery again. The badge menu appears, and the badge performs a quick test.
4. Wait a couple seconds until the test is complete.
5. Press the Hold/DND button to see the factory reset menu. The badge prompts, "Reset badge?"
6. Press the Select button to confirm that you want to restore the factory image on the badge. Otherwise, press any other button to cancel restoring the factory image.
   Once you confirm, the badge displays the following prompt: "Warning: Leave the badge powered on for 10 min and wait. Do not interrupt."
7. Wait a few minutes until the badge displays the following prompt: `WAITING AT IP ADDR 10.213.213.213` At this point, the badge does not have any proper settings.
8. Restore the default settings on the badge so that you can configure it again. See Restoring Factory Default Settings on page 46.

Maintaining Properties and Firmware

You can use the production Vocera Voice Server to change badge properties or update firmware any time after the initial badge configuration, instead of using the configuration computer. This is convenient because the Vocera Voice Server can update connected badges automatically, without requiring you to configure them manually again.

Although the production Vocera Voice Server can update your existing badges, you should continue to maintain the configuration computer after you complete the initial badge configuration. You will need the configuration computer to configure any new badges that you receive.

Tip: Copy the `badge.properties` file from the `\vocera\config` directory on the configuration computer to the same directory on the production Vocera Voice Server after you complete the initial badge configuration. You can use this file as a reference to see what property values the badges are currently using. In addition, if you need to change badge properties later, the Vocera Voice Server uses this file to update the badges automatically.

About Property and Firmware Maintenance

The Vocera Voice Server maintains a copy of the most recent badge firmware in its own directory structure in the following locations:

Badge type	Firmware location
B3000n	`\vocera\config\gen3n\badge`
B3000	`\vocera\config\gen3\badge`
B2000	`\vocera\config\gen2\badge`

The Vocera Voice Server can update badge properties and firmware at either of the following times:

- Immediately after a badge boots.

  When a badge boots, it connects to the Vocera Voice Server. The server compares the badge firmware and properties with its own copies as described in **How to Update Properties and Firmware** on page 49.
- Immediately after the server starts.

  You need to stop the server to install any upgrades or service packs that may contain new firmware. When you restart the server, it compares the badge firmware and properties with its own copies as described in **How to Update Properties and Firmware** on page 49.

The server downloads firmware even if a badge has a more recent version of the firmware than the server. If you receive a firmware upgrade from Vocera, install it on the Vocera Voice Server as described in the firmware release notes.

How to Update Properties and Firmware

Each time the Vocera Voice Server starts, it reads `badge.properties` into memory. If property values on the badge don't match the in-memory values, the server automatically updates the badges with the values from `badge.properties`.

Important: If you edit the `badge.properties` on the Vocera Voice Server, its values are not read into memory again until you restart the server. At that time, the server automatically downloads the new properties to badges that connect to it.

To update properties and firmware:

1. On the badge configuration computer, use the Badge Properties Editor to configure a test badge to confirm that WLAN security settings work properly. See **Configuring a Test Badge** on page 6.

   If the test badge works properly, you are ready to copy the `badge.properties` file to the Vocera Voice Server to update other badges.
2. Copy the `badge.properties` file in the `\vocera\config` directory on the badge configuration computer to the `\vocera\config` directory on the active Vocera Voice Server.
3. Use the Vocera Control Panel to restart the server, as described in the *Vocera Voice Server Installation Guide*.
4. As badges connect to the server, they synchronize with the Vocera Voice Server, if necessary.

   If a badge is offline, it will update as soon as the badge boots and connects to the server.

Using the Badge Background Updater

B3000n, B3000, and B2000 badges can download a firmware upgrade and/or modified settings in the background. After the files are downloaded, the badge switches to the new firmware image and/or settings automatically.

The badge functions normally during the update process, allowing you to make and receive calls when the update is going on in the background. This eliminates several minutes of downtime each time badge firmware is updated.

Background Updater and Vocera Clusters

After Vocera Voice Server 4.4 (or a more recent version) has been installed on your Vocera Cluster, you can take advantage of the background update feature to ensure that users experience minimal downtime during subsequent updates to badge properties or firmware. During a background update the badge will always download firmware and settings from the active server.

1. Update the `badge.properties` file in the `\vocera\config` directory on the *active* server. A minute or two later, the file will be synchronized with the standby server.
2. Update the standby node(s):
   a. On the standby node, shut down the Vconfig by choosing Run > Exit.
   b. Update the standby node by installing the latest Vocera Voice Server service pack.
   c. Reboot the standby node.
   d. Wait for the Vocera Voice Server on the standby node to rejoin the cluster and perform a remote restore.

      Important: After the Vocera Voice Server starts, it initially comes up as an active node, and then within a minute it rejoins the cluster and performs a remote restore. With a large database, a remote restore can take several minutes.
   e. On the active node, shut down the Vconfig by choosing Run > Exit.
   A standby node becomes active. Badges connect to it and download new firmware and settings in the background.
   f. Update the remaining Vocera Voice Server.

Background Update Status Icon

When a badge is performing a background update, the ▼ icon on the screen indicates that the update is in progress. After the files are downloaded, the badge restarts.

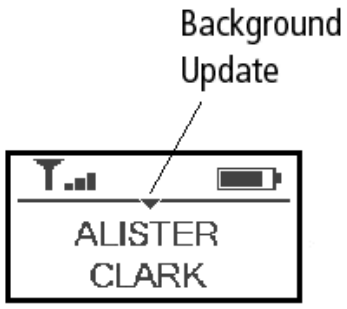


Figure 15: Background Update icon

If the badge screen saver is currently active, the ▼ icon appears to the right of the battery indicator:

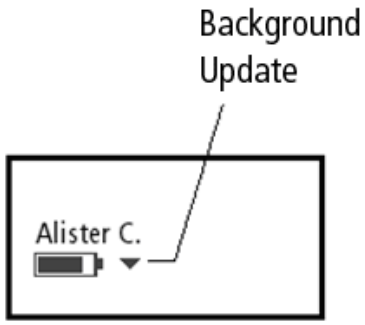


Figure 16: Badge screen saver with Background Update icon

If the update process is paused because the badge is being used to make or receive a call, the ▼ icon does not appear on screen until the call is finished and the update process resumes.

Using a Badge While a Background Update Is in Progress

All badge functionality is available while a background update is in progress. If you make or receive a call, the background update is automatically paused so that it does not affect call quality. While background update is paused, the ▼ icon does not appear on screen. When you finish the call, the background update process resumes and the ▼ icon appears on screen again until the update is finished.

The duration of the update varies based on whether the badge is used to receive or make calls during the update process. If you pause the update several times to make or receive calls, the update process will take longer. However, since the background update does not prevent users from using the badge, the duration of the update is insignificant. In fact, users may not even notice that an update has occurred.

Interrupting a Background Update

If you roam off network or the Vocera Voice Server fails over to another server while a background update is in process, the update stops and the badge restarts. When your badge reconnects to a Vocera Voice Server, the background update process will begin again.

Badge Property Reference

This section contains an alphabetical list of the most common badge properties. These property names appear in the **badge.properties** file. The list contains cross-references to the fields and pages you can use to set these properties in the Badge Properties Editor (BPE).

The properties for different types of Vocera badges have different names. In the `badge.properties` file, properties have the following prefixes:

Badge type	Prefix
B3000n	`B3N`
B3000	`B3`
B2000	`B2`

Important: Badges have many properties that are for internal use only. Setting the wrong value or the wrong property can cause unrecoverable damage to a badge. Use the Badge Properties Editor to set property values unless you are working with Vocera Technical Support. Otherwise, do not set any properties other than the ones listed in this chapter.

Table 9: List of Badge Properties

Property Name	Default Value	Description
• *B2000:* **B2.AuthenticationType** • *B3000:* **B3.AuthenticationType** • *B3000n:* **B3N.AuthenticationType**	Open	Specifies the type of authentication required by your wireless network: • **Open** specifies that your wireless network does not require authentication. • **LEAP** specifies that your wireless network implements the Cisco LEAP protocol for authentication. • **WPA-PEAP** specifies that your wireless network uses the WiFi Protected Access Protected Extensible Authentication Protocol for authentication. • **WPA-PSK** specifies that your wireless network uses the WiFi Protected Access Pre-Shared Key protocol for authentication. • **EAP-FAST** specifies that your wireless network uses Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling for authentication. • **EAP-TLS** specifies that your wireless network uses Extensible Authentication Protocol-Transport Layer Security for authentication. Use the **Authentication** field on the Security tab of the Badge Properties Editor to set this value.

Property Name	Default Value	Description
• *B2000:* **B2.BadgeIPAddr** • *B3000:* **B3.BadgeIPAddr** • *B3000n:* **B3N.BadgeIPAddr**	*Blank*	Specifies a static IP address for the badge using standard dotted notation (such as 192.168.3.7). Leave this value blank if a DHCP server is assigning IP addresses. If you are setting up badges for a production Vocera environment, allow a DHCP server to assign IP addresses to the badges. Static IP addresses are feasible only for small evaluation systems.
• *B2000:* ***Not available*** • *B3000:* ***Not available*** • *B3000n:* **B3N.DisplayBluetooth**	FALSE	Specifies whether the Bluetooth configuration menu is displayed on the badge.
• *B2000:* **B2.BroadcastUsesIGMP** • *B3000:* **B3.BroadcastUsesIGMP** • *B3000n:* ***Not available***	FALSE	Vocera broadcast is implemented as IP Multicast. If broadcast commands need to cross a subnet, IGMP must be supported in the switch or router, and this property must be set to TRUE. The B3000n badge auto-detects IGMP and changes its mode dynamically if IGMP is enabled in the infrastructure. Consequently, this property is deprecated in the B3000n badge. **Note:** This badge property is not available in the Badge Properties Editor.
• *B2000:* **B2.ChannelsToScan** • *B3000:* **B3.ChannelsToScan** • *B3000n:* **B3N.ChannelsToScan**	*Blank*	Allows B3000n (on 2.4 GHz networks), B3000, and B2000 badges to scan up to four arbitrary channels when the signal quality drops. By default, badges scan only channels 1, 6, and 11 unless this property is set. To set this property, enter the specific channel numbers in a comma-separated list. For optimal performance of the badge and other wireless clients, Vocera recommends that the access points on your network are set only to the three non-overlapping channels of 1, 6, and 11. Use the Specify Channels field in the 2.4 GHz Channels section of the Wireless tab in the Badge Properties Editor to set this value.
• *B2000:* *Not available* • *B3000:* *Not available* • *B3000n:* **B3N.ChannelsToScan5G**	*Blank*	Allows B3000n badges on 5 GHz networks to scan an arbitrary set of channels when the signal quality drops. By default, B3000n badges scan all available channels unless this property is set. To set this property, enter the specific channel numbers in a comma-separated list. Use the Specify Channels field in the 5 GHz Channels section of the Wireless tab in the Badge Properties Editor to set this value.
• *B2000:* **B2.ClientKeyPassword** • *B3000:* **B3.ClientKeyPassword** • *B3000n:* **B3N.ClientKeyPassword**	*Blank*	Specifies the password for the client private key. This is only needed if you are using external EAP-TLS certificates. The maximum length of the password supported by Vocera badges is 32 alphanumeric characters.

Property Name	Default Value	Description
• *B2000:* **B2.ClosedMenus** • *B3000:* **B3.ClosedMenus** • *B3000n:* **B3N.ClosedMenus**	FALSE	Specifies whether the badge configuration menus are hidden, or if they can be easily accessed through the DND button: • **FALSE** specifies that you can access the configuration menus by pressing the DND button within three seconds of the B3000, or B2000 badge displaying the boot countdown timer. • For B3000 and B2000 badges, **TRUE** specifies that you must use the special sequence of button presses to display the configuration menus. • To display the configuration menus on B3000n badges, press and hold the DND and Call buttons together while the countdown timer is displayed, regardless of the setting of this property. With B3000 and B2000 badges, set this value to TRUE to prevent users from displaying the configuration menus and inadvertently causing configuration problems in a badge. Use the **Hide Boot Menus** field on the General tab of the Badge Properties Editor to set this value.
• *B2000:* **B2.ConfigStaticIP** • *B3000:* **B3.ConfigStaticIP** • *B3000n:* **B3N.ConfigStaticIP**	FALSE	Specifies whether your badge has a static IP address, or whether it receives its address from a DHCP server. If a DHCP server is assigning IP addresses, leave this field blank. This value is necessary only if you are using static IP addresses. **Note:** This badge property is not available in the Badge Properties Editor.
• *B2000:* **B2.DNS1IPAddr** • *B3000:* **B3.DNS1IPAddr** • *B3000n:* **B3N.DNS1IPAddr**	*Blank*	Specifies the IP address of the DNS server that your site uses to resolve DNS queries, in standard dotted notation. If a DHCP server is assigning IP addresses, leave this field blank. This value is necessary only if you are using static IP addresses and the value of **ServerIPAddr** is specified as a DNS style name. **Note:** This badge property is not available in the Badge Properties Editor.
• *B3000n/B3000/B2000:* *Not available*	*Blank*	Specifies the IP address of the secondary DNS server that is used if the primary server is not available, in standard dotted notation. If a DHCP server is assigning IP addresses, leave this field blank. This value is necessary only if you are using static IP addresses and the value of ServerIPAddr is specified as a DNS style name. **Note:** This badge property is not available in the Badge Properties Editor.
• *B2000:* **B2.EAPTLSUseExtCert** • *B3000:* **B3.EAPTLSUseExtCert** • *B3000n:* **B3N.EAPTLSUseExtCert**	FALSE	Specifies whether to use external certificates instead of the Vocera Manufacturer Certificates. External certificates can be self-signed or signed by a trusted Certificate Authority (CA). • **FALSE** specifies that you are using the Vocera Manufacturer Certificates. • **TRUE** specifies that you are using external certificates. Additional configuration is required.

Property Name	Default Value	Description
• *B2000:* **B2.EFAutoPACProvRetryCount** • *B3000:* **B3.EFAutoPACProvRetryCount** • *B3000n:* **B3N.EFAutoPACProvRetryCount**	0	Limits the number of times a badge attempts to retry retrieving a PAC from the Cisco ACS after the first attempt failed (for example, due to wireless network problems). Enter a number from 0 to 5. By default, this property is set to 0 (meaning no retries). In order to take advantage of this feature, you must also select EAP-FAST authentication.
• *B2000:* **B2.Enable80211d** • *B3000:* **B3.Enable80211d** • *B3000n:* **B3N.Enable80211d**	FALSE	Specifies whether the badge will take advantage of the region-based channel selection capabilities of 802.11d. • **FALSE** specifies that region-based channel selection is disabled. • **TRUE** specifies that region-based channel selection is enabled. In order to take advantage of this standard, your access points must also support it.
• *B2000:* **B2.EnableAPSD** • *B3000:* **B3.EnableAPSD** • *B3000n:* *Not available*	FALSE	Specifies whether the badge will take advantage of the Unscheduled Automatic Power Save Delivery Subset (U-APSD) of 802.11e. U-APSD improves power management and potentially increases the talk time of 802.11 clients. • **FALSE** specifies that U-APSD is disabled. • **TRUE** specifies that U-APSD is enabled. In order to take advantage of this standard, your access points must also support it. Important: The B2.EnableAPSD, B3.EnableAPSD, B2.EnableWMM, and B3.EnableWMM properties should all be set to the same value. The firmware and chip set changes in the B3000n badge make this property unnecessary. Consequently, this property is deprecated in the B3000n badge. **Note:** This badge property is not available in the Badge Properties Editor.
• *B2000:* **B2.EnableCCKM** • *B3000:* **B3.EnableCCKM** • *B3000n:* **B3N.EnableCCKM**	FALSE	Specifies whether Cisco Certified Key Management is enabled for Vocera devices. CCKM is a form of fast roaming supported on Cisco access points and on various routers. Using CCKM, Vocera devices can roam from one access point to another without any noticeable delay during reassociation. After a Vocera device is initially authenticated by the RADIUS authentication server, each access point on your network acts as a wireless domain service (WDS) and caches security credentials for CCKM-enabled client devices. When a Vocera device roams to a new access point, the WDS cache reduces the time it needs to reassociate. • **FALSE** specifies that CCKM is disabled. • **TRUE** specifies that CCKM is enabled. In order to take advantage of this feature, your access points must also support it, and you must use either LEAP, WPA-PEAP, EAP-FAST, or EAP-TLS authentication.

Property Name	Default Value	Description
• *B2000:* **B2.EnableEFAutoPACProv** • *B3000:* **B3.EnableEFAutoPACProv** • *B3000n:* **B3N.EnableEFAutoPACProv**	FALSE	Enables automatic provisioning of the Protected Access Credential (PAC) for EAP-FAST authentication. This replaces the manual method of creating a new PAC on the Cisco ACS when it expires and then copying it to the Vocera Voice Server and the Vocera configuration computer. In order to take advantage of this feature, you must also select EAP-FAST authentication.
• *B2000:* **B2.EnableEFAutoPACProvOnExpiry** • *B3000:* **B3.EnableEFAutoPACProvOnExpiry** • *B3000n:* **B3N.EnableEFAutoPACProvOnExpiry**	FALSE	Enables the automatic provisioning of a new PAC when it expires. If this property is unchecked, a badge whose PAC has completely expired will display the following message: "Expired or invalid PAC credentials." In order to take advantage of this feature, you must also select EAP-FAST authentication.
• *B2000:* **B2.EnableFIPSMode** • *B3000:* **B3.EnableFIPSMode** • *B3000n:* *Not available*	FALSE	When set to TRUE, this property causes the cryptographic security module to run in a secure mode that conforms with Federal Information Processing Standard (FIPS) 140-2.
• *B2000:* **B2.EnableWMM** • *B3000:* **B3.EnableWMM** • *B3000n:* **B3N.EnableWMM**	FALSE	Specifies whether the badge will take advantage of the WiFi Multimedia (WMM) subset of 802.11e. 802.11e QoS provides standards-based QoS to prioritize voice over data traffic and ensure high level voice quality. • **FALSE** specifies that 802.11e QoS is disabled. • **TRUE** specifies that 802.11e QoS is enabled. In order to take advantage of this standard, your access points must also support it, switches and routers must be configured to honor DSCP markings, and the Vocera QoS Manager service must be enabled on the Vocera Voice Server. Important: The B2.EnableAPSD, B3.EnableAPSD, B2.EnableWMM, and B3.EnableWMM properties should all be set to the same value. If 802.11n is enabled on both the network and the B3000n badge (through the B3N.WirelessBand property), the B3000n takes advantage of WMM and ignores this property. In legacy 802.11n environments, you can continue to use this property for the B3000n badge. This property is not tied to the use of APSD for the B3000n. **Note:** This badge property is not available in the Badge Properties Editor.

Property Name	Default Value	Description
• *B2000:* **B2.EncryptionType** • *B3000:* **B3.EncryptionType** • *B3000n:* **B3N.EncryptionType**	None	Specifies the type of data encryption your wireless network requires. • **None** specifies your wireless network does not require encryption. • **WEP64** specifies your network uses 64-bit (sometimes called 40-bit) WEP keys. • **WEP128** specifies your network uses 128-bit (sometimes called 104-bit) WEP keys. • **TKIP-Cisco** specifies your network uses Cisco's proprietary TKIP encryption technique. • **TKIP-WPA** specifies your network uses TKIP as defined by WPA. • **AES-CCMP** specifies your network uses AES-CCMP as defined by WPA2. Use the **Encryption** field on the Security tab of the Badge Properties Editor to set this value.
• *B2000:* **B2.GatewayIPAddr** • *B3000:* **B3.GatewayIPAddr** • *B3000n:* **B3N.GatewayIPAddr**	*Blank*	Specifies the address of your gateway, if your LAN uses one, in standard dotted notation. Make sure you specify a default DHCP gateway by manually editing this property in the `badge.properties` file (this property is not currently exposed in the Badge Properties Editor. Vocera uses this property for multicast sessions even when badges and the Vocera Voice Server are in the same VLAN.
• *B2000:* *Not available* • *B3000:* **B3.GroupModeState** • *B3000n:* **B3N.GroupModeState**	1	Specifies whether Group Mode is turned on when users are on a call. Group Mode widens the speech zone, allowing other people to speak into the badge's primary microphone. • **1** specifies that Group Mode is enabled only while on a call. • **2** specifies that Group Mode is disabled to eliminate background noise when users are on a call. This setting is appropriate for noisy environments. **Note:** B3000n and B3000 badge users can change the Group Mode setting on their badges. • For B3000: Group Mode is always off during Genie interactions and broadcasts. • For B3000n: Group Mode is automatically enabled when the badge is turned to a 105 degree angle to improve voice recognition when the badge is not placed in an optimal position.
• *B2000:* *Not available* • *B3000:* **B3.HeadsetButtonSupport** • *B3000n:* **B3N.HeadsetButtonSupport**	FALSE	Specifies whether the in-line button on a wired headset is able to initiate or accept badge calls. • If this property is set to TRUE, a user can accept or initiate a call with either the headset button or the badge's Call button. • If this property is set to FALSE, a user must accept a call with the badge's Call button. This property is not available for the B2000 badge. The B2000 supports wired headsets, but does not support the use of the headset buttons. **Note:** This badge property is not available in the Badge Properties Editor.

Property Name	Default Value	Description
• *B2000:* **B2.InstallDone** • *B3000:* **B3.InstallDone** • *B3000n:* **B3N.InstallDone**	FALSE	Specifies whether the Badge Configuration Utility has performed the initial configuration for a badge: • If this property is **TRUE**, the badge boots the normal Vocera application when it powers up. • If this property is **FALSE**, the badge attempts to connect to a machine at IP address 10.0.0.1 running the Badge Configuration Utility when it powers up. If successful, the badge downloads properties and firmware from the Badge Configuration Utility. **Note:** This badge property is not available in the Badge Properties Editor.
• *B2000:* **B2.ListenInterval** • *B3000:* **B3.ListenInterval** • *B3000n:* **B3N.ListenInterval**	5	An access point broadcasts a management frame called a beacon at a fixed interval (required to be set to 100 ms by Vocera). The **B2.ListenInterval** property specifies the frequency with which badges "wake up" and listen for a beacon. When the beacon interval is 100 ms and **B2.ListenInterval** is 5, the default listen interval is 500 ms. **Note:** This badge property is not available in the Badge Properties Editor.
• *B2000:* **B2.Password** • *B3000:* **B3.Password** • *B3000n:* **B3N.Password**	*Blank*	If **AuthenticationType** is set to **LEAP**, **WPA-PEAP**, or **EAP-FAST**, specifies the password the badge supplies for authentication. Use the **Password** field on the Security tab of the Badge Properties Editor to set this value.
• *B2000:* **B2.PreSharedKey** • *B3000:* **B3.PreSharedKey** • *B3000n:* **B3N.PreSharedKey**	*Blank*	If **AuthenticationType** is set to **WPA-PSK**, specifies the 64-character, hexadecimal pre-shared key the badge supplies for authentication. Use the **PreShared Key** field on the Security tab of the Badge Properties Editor to set this value. The WPA-PSK standard uses a hexadecimal key to encrypt the association handshake. For B3000n and B3000 badges, you can enter the ASCII passphrase used by your wireless network. For other badges, enter a 64-character, hexadecimal value for the pre-shared key.
• *B2000:* **B2.ResetVolumeToDefault** • *B3000:* **B3.ResetVolumeToDefault** • *B3000n:* **B3N.ResetVolumeToDefault**	FALSE	Specifies whether the badge resets the volume to the default at boot-up. • FALSE specifies that the badge maintains the previous volume setting at boot-up. • TRUE specifies that the badge resets the volume to the default at boot-up.
• *B2000:* **B2.RoamingPolicy** • *B3000:* **B3.RoamingPolicy** • *B3000n:* **B3N.RoamingPolicy**	2	Specifies how quickly a badge searches for another access point when signal quality drops. Higher values cause a badge to search sooner, and may correct problems with choppy audio. However, a badge cannot send or receive audio packets while searching for an access point, so communication may be interrupted. Lower values allow a badge to tolerate lower signal quality before searching. The optimal threshold value varies from one 802.11 network to another, depending on how the network is configured. Use the **Roaming Policy** field on the Wireless tab of the Badge Properties Editor to set this value.

Property Name	Default Value	Description
• *B2000:* **B2.ServerIPAddr** • *B3000:* **B3.ServerIPAddr** • *B3000n:* **B3N.ServerIPAddr**	*Blank*	Specifies the IP address of the machine which is running the Vocera Voice Server. Use dotted notation (such as 192.168.3.7) to specify this value. For a Vocera Voice Server cluster, enter multiple IP addresses and separate them with commas. You must specify a value for this property. Use the **Vocera Voice Server IP Address** field on the General tab of the Badge Properties Editor to set this value.
• *B2000:* **B2.SSID** • *B3000:* **B3.SSID** • *B3000n:* **B3N.SSID**	vocera	Specifies the SSID of the wireless network or subnet the Vocera badges will use. This value is case sensitive. You must specify a value for this property. Use the **SSID** field on the General tab of the Badge Properties Editor to set this value.
• *B2000:* **B2.SubnetMask** • *B3000:* **B3.SubnetMask** • *B3000n:* **B3N.SubnetMask**	*Blank*	Specifies a subnet mask that indicates which bits in the IP address correspond to the subnet, using standard dotted notation (such as 255.255.255.0). You must specify this property if you are using static IP addresses. Leave this value blank if a DHCP server is assigning IP addresses. **Note:** This badge property is not available in the Badge Properties Editor.
• *B2000:* **B2.SubnetRoaming** • *B3000:* **B3.SubnetRoaming** • *B3000n:* **B3N.SubnetRoaming**	FALSE FALSE FALSE	Specifies whether users can roam across subnet boundaries while using badges. If subnet roaming is enabled, a badge automatically obtains a new IP address as a badge user makes the transition to an access point on a different subnet. If you enable subnet roaming, you must use a DHCP server to supply your IP addresses. Set this property to **TRUE** only if the access points on your wireless LAN are divided into multiple subnets, and if you want to allow users to roam across subnet boundaries. If all the access points on your wireless LAN are within a single subnet, set this property to **FALSE** to minimize DHCP traffic and reduce the chance of a momentary loss of audio when roaming between access points. The subnet where the Vocera Voice Server is located is not relevant to this property. **Note:** This badge property is not available in the Badge Properties Editor.
• *B2000:* **B2.UserName** • *B3000:* **B3.UserName** • *B3000n:* **B3N.UserName**	*Blank*	If **AuthenticationType** is set to **LEAP**, **WPA-PEAP**, or **EAP-FAST**, specifies the user name the badge supplies for authentication. Use the **User Name** field on the Security tab of the Badge Properties Editor to set this value.

Property Name	Default Value	Description
• *B2000:* **B2.WEPKey1** • *B3000:* **B3.WEPKey1** • *B3000n:* **B3N.WEPKey1**	*Blank*	Specifies a WEP key the badge can use to transmit or receive data, if EncryptionType is set to **WEP64** or **WEP128**. Enter the value in the following format: • If **EncryptionType** is set to **WEP64**, specify a key with 10 hexadecimal digits. • If **EncryptionType** is set to **WEP128**, specify a key with 26 hexadecimal digits. If either the access points or the badges are using the first WEP key to transmit data, the value you specify here must match the first WEP key in the access point. Use the **WEP Key** field on the Security tab of the Badge Properties Editor to set this value.
• *B2000:* **B2.WEPKey2** • *B3000:* **B3.WEPKey2** • *B3000n:* **B3N.WEPKey2**	*Blank*	Specifies a WEP key the badge can use to transmit or receive data, if EncryptionType is set to **WEP64** or **WEP128**. Enter the value in the following format: • If **EncryptionType** is set to **WEP64**, specify a key with 10 hexadecimal digits. • If **EncryptionType** is set to **WEP128**, specify a key with 26 hexadecimal digits. If either the access points or the badges are using the second WEP key to transmit data, the value you specify here must match the second WEP key in the access point. **Note:** This badge property is not available in the Badge Properties Editor.
• *B2000:* **B2.WEPKey3** • *B3000:* **B3.WEPKey3** • *B3000n:* **B3N.WEPKey3**	*Blank*	Specifies a WEP key the badge can use to transmit or receive data, if EncryptionType is set to **WEP64** or **WEP128**. Enter the value in the following format: • If **EncryptionType** is set to **WEP64**, specify a key with 10 hexadecimal digits. • If **EncryptionType** is set to **WEP128**, specify a key with 26 hexadecimal digits. If either the access points or the badges are using the third WEP key to transmit data, the value you specify here must match the third WEP key in the access point. **Note:** This badge property is not available in the Badge Properties Editor.
• *B2000:* **B2.WEPKey4** • *B3000:* **B3.WEPKey4** • *B3000n:* **B3N.WEPKey4**	*Blank*	Specifies a WEP key the badge can use to transmit or receive data, if EncryptionType is set to **WEP64** or **WEP128**. Enter the value in the following format: • If **EncryptionType** is set to **WEP64**, specify a key with 10 hexadecimal digits. • If **EncryptionType** is set to **WEP128**, specify a key with 26 hexadecimal digits. If either the access points or the badges are using the fourth WEP key to transmit data, the value you specify here must match the fourth WEP key in the access point. **Note:** This badge property is not available in the Badge Properties Editor.
• *B2000:* **B2.WEPKeySlot** • *B3000:* **B3.WEPKeySlot** • *B3000n:* **B3N.WEPKeySlot**	*Blank*	If **Encryption** is set to **WEP64** or **WEP128**, specifies which of the four WEP keys the badge uses to transmit data. Valid values are 1-4. **Note:** This badge property is not available in the Badge Properties Editor.

Property Name	Default Value	Description
• *B2000:* *Not available* • *B3000:* *Not available* • *B3000n:* **B3N.WirelessBand**	*ABGN*	Select the wireless bands used by the B3000n badge: • ABGN uses all 802.11 wireless bands (a, b, g, and n) at 2.4 GHz and 5 GHz. This is the default setting. • AN uses 802.11a and 802.11n wireless bands at 5 GHz. • BGN uses the the 802.11b, 802.11g, and 802.11n wireless bands at 2.4 GHz. • A uses the 802.11a wireless band at 5 GHz. • BG uses the 802.11b and 802.11g wireless bands at 2.4 GHz.
• *B2000:* *Not available* • *B3000:* **DefaultHandsetVolume** • *B3000n:* **DefaultHandsetVolume**	1	Lists the default volume level of Privacy Mode when no users are logged on.
• *B2000:* *Not available* • *B3000:* **DisplayHandsetMode** • *B3000n:* **DisplayHandsetMode**	True	Displays Privacy Mode in on the badge menu under Settings.
• *B2000:* *Not available* • *B3000:* **EnableHandsetQuickEntry** • *B3000n:* **EnableHandsetQuickEntry**	True	Enables Easy Access entry to Privacy mode.
• *B2000:* *Not available* • *B3000:* **HandsetMode** • *B3000n:* **HandsetMode**	False	Enables or disables Privacy mode using Easy Access.
• *B2000:* *Not available* • *B3000:* **HandsetQuickEntryPromptPlay** • *B3000n:* **HandsetQuickEntryPromptPlay**	True	Plays an audible alert, “Entering Handset Mode” while switching to Privacy Mode using Easy Access.