Vocera B3000 Badge Guide

Version 4.4

vocera

Vocera Communications, Inc.
www.vocera.com
tel :: +1 408 882 5100
fax :: +1 408 882 5101
2013-12-12 14:07:39

Contents

Getting Started..... 7

Introduction..... 9
About This Guide..... 9
System Requirements..... 10
Getting Started with a B3000 Badge..... 10

B3000 End-User Features..... 13
Comparing Vocera Devices..... 13
Enhanced Durability..... 15
Enhanced Display..... 16
Increased Speaker Volume..... 17
Integrated Noise Cancellation..... 17
Smart Battery and Power Efficiency..... 18
Handset Mode..... 18
Improved Attachments..... 19
The Badge Menus..... 19
Main Screen..... 20
Info Menu..... 21
Power Off Menu..... 22
Messages Menu..... 23
Settings Menu..... 23
Volume Menu..... 23
Font Menu..... 23
Handset Menu..... 23
Group Mode Menu..... 24
Flip Screen Menu..... 24
Custom Settings..... 24
Adjusting the Message Font..... 24
Adjusting the Volume..... 25
Turning Handset Mode On or Off..... 26
Specifying the Group Mode Setting..... 27
Flipping the Screen..... 28
Anti-Microbial Protection..... 28

Maintaining Your Badge..... 29
When to Charge the Battery..... 29
Preparing the Charger..... 29
Preparing the B3000 Charger..... 30
Charging the B3000 Battery..... 31
Cleaning the Badge and Accessories..... 32

B3000 Device Management..... 35
Automatically Loading B3000 Badges into the System..... 35
Labeling B3000 Badges..... 36
Monitoring Active Devices..... 37
Managing B3000 Badges..... 37
Reporting on B3000 Badges..... 37

Configuring Badges..... 39

Configuring New Badges..... 41
Configuring a Test Badge..... 41
Configuring the Remaining Badges..... 43
Configuring Badges with Static IP Addresses..... 44

Setting Up the Configuration Computer..... 47
Configuration Hardware Requirements..... 47
Installation and Setup..... 48
Removing Earlier Versions of the Badge Configuration Utilities..... 48
Installing Badge Configuration Utilities..... 49
Specifying TCP/IP Properties..... 49
Setting Up an Isolated Access Point..... 50

Creating a Property File to Download..... 53
About Badge Profiles..... 53
Using the Badge Properties Editor..... 54
Setting General Properties..... 55
Setting Security Properties..... 57
Setting Wireless Properties..... 66

Using the Badge Configuration Utility..... 71
About the Badge Configuration Utility..... 71
Running the Badge Configuration Utility..... 72

Infrastructure Topics..... 75

B3000 Wireless Features..... 77
802.11b/g Support..... 77
Access Point Settings..... 78
Data Rates..... 78
SSID and Security..... 79
Acceptable Voice Quality..... 79
The Roaming Policy Property..... 81

B3000 Security Features..... 83
Security Support..... 83
Security and Roaming Delays..... 85
Authentication Delays..... 85
Optimizing WPA-PEAP, LEAP, EAP-FAST, and EAP-TLS..... 86
Other Wireless Security Topics..... 87

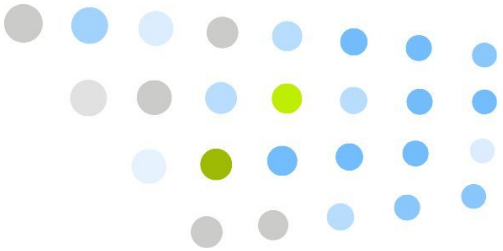
Appendixes..... 89

Agreements, Specifications, and Notices..... 91
Third-Party Software Agreements..... 91
System Specifications for B3000..... 91
B3000 Regulatory Notices..... 94

Important Safety Instructions..... 105
Warning Definition..... 106
Badge and Battery Charger Safety..... 107
Important Information About Use in Certain Areas..... 111
Additional Instructions for B3000 Battery Safety..... 111
Product Disposal Warning..... 112
National Safety Statement of Compliance – CE Marking..... 113

IP Port Usage..... 115
Opening Ports for Communication..... 115

Index..... 119



Getting Started

This section provides an introduction to the *Vocera B3000 Badge Guide* and information about the new end-user features in the B3000 badge:

- **Introduction** on page 9

  Discusses the organization of this manual, provides system requirements for the B3000 badge, and describes how to get started using the B3000 badge.

- **B3000 End-User Features** on page 13

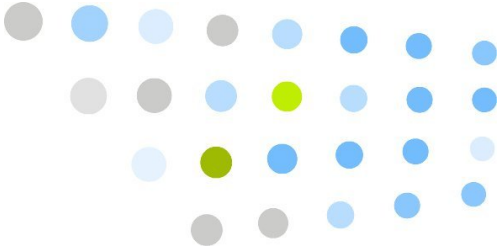
  Summarizes the new end-user features of the B3000 badge.

- **Maintaining Your Badge** on page 29

  Describes how to charge B3000 batteries and clean the B3000 badge.

- **B3000 Device Management** on page 35

  Describes Vocera device management features for B3000 badges.



Introduction

This guide contains all the information about the B3000 badge, its firmware, and its related server software that is new or different from the B2000. If you are familiar with the B2000, you can use this guide to learn about the new features and differences quickly.

About This Guide

All the information in the *Vocera B3000 Badge Guide* also appears in other books in the Vocera documentation set. For example, information for end users appears in the *Vocera Badge User Guide* and information about badge configuration appears in the *Vocera Badge Configuration Guide*.

The *Vocera B3000 Badge Guide* simply collects all the new documentation for the convenience of experienced users. If you do not have previous experience with Vocera badges, the other guides in the Vocera documentation set may be more useful.

The information in this guide is organized into the following parts:

- **Getting Started** on page 7 provides an introduction to this guide, discusses system requirements for the B3000 badge, describes end-user features of the B3000 badge, describes how to charge and clean the B3000 badge, and describes B3000 device management features.
- **Configuring Badges** on page 39 describes how to configure the B3000 and troubleshoot your badge configuration.
- **Infrastructure Topics** on page 75 provides updated information about infrastructure requirements and recommendations for the B3000 badge.
- **Appendixes** on page 89 provides additional information and reference material for the B3000 badge.

System Requirements

To use the B3000 badge, your Vocera system must meet the following requirements:

- Vocera Server 4.1 SP7 or later
- Vocera Server 4.2 SP1 with HF14799 or later

Getting Started with a B3000 Badge

If this is the first time you are using a Vocera badge, you can get started right away by following these simple steps:

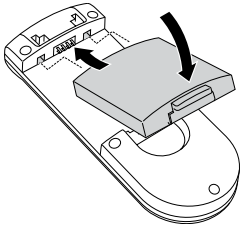
To get started with a B3000 badge:

1. Charge the battery, if necessary.

   New batteries must be charged before use. If the badge has already been used by someone else, check the battery level indicator on the badge display to make sure the battery has sufficient power.

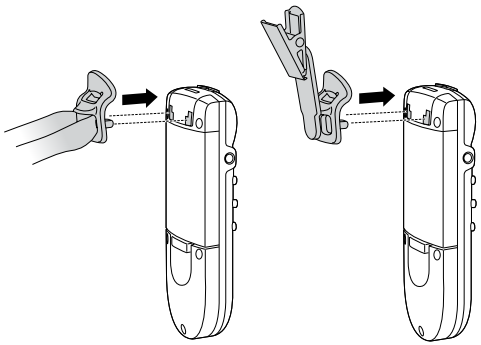
   See **Maintaining Your Badge** on page 29 for other ways to determine whether the battery needs charging and for instructions on how to charge the battery.

2. Install the battery. To do this, slide the pegs at the top of the battery into the two holes in the badge's battery compartment, and then press down gently to seat the battery.

   The badge will begin a startup sequence. Wait until the badge display reads Logged Out or shows someone's name.

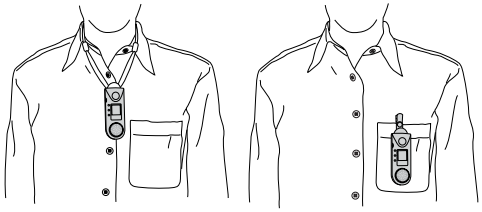
3. Choose the lanyard or universal clip attachment, and connect it to the badge.



You also can connect the lanyard or clip to the badge *before* installing the battery.

4. Put the badge on, and make sure it is in the proper position.

   For optimal speech recognition, the top of the badge should be approximately 6 inches (15 centimeters) from your chin. Any sound coming from another direction or beyond that distance is reduced or eliminated by the noise canceling microphones.



5. Log in: Press the Call button and wait for the Genie to answer.
   - **If the Genie asks for your name**, say your first and last names.
   - **If the Genie answers by saying "Vocera" or by playing a tone**, another user may already be logged in. If so, say "Log me out," wait for the chime, and then press the Call button again to log in.
6. Record your name: Press the Call button, wait for the Genie to answer, and then say "Record my name."

   The Genie will prompt you to record your name. If you do not record your name, the Vocera system uses speech synthesis to say your name.
7. Adjust the volume on the badge, if necessary. See **Adjusting the Volume** on page 25.

Your badge is now ready to use. You can press the Call button at any time, wait for the Genie to answer, and then give the Genie a voice command, such as:

"Call Jim Olsen."

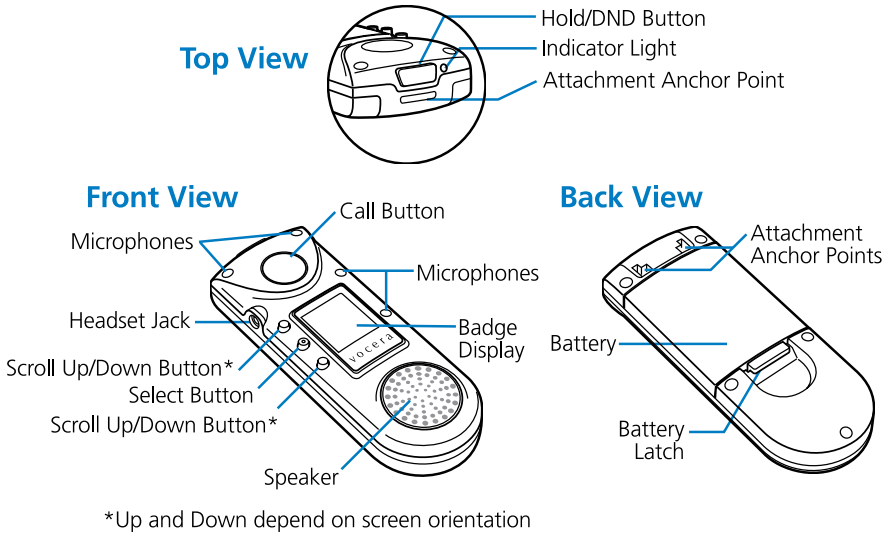
"Record my greeting."

"Play my messages."

For more information about Vocera commands, see **Basic Calling** in the *Vocera Badge User Guide* and **Advanced Commands** in the *Vocera Badge User Guide*.

B3000 End-User Features

This chapter describes the end-user features of the B3000 badge.



Comparing Vocera Devices

The following table lists the features of all Vocera devices, including the B3000:

Table 1. Features of Vocera Devices

Feature	B1000A	B2000	Smartphone	B3000
Rugged design			✓	✓
Louder speaker for noisy environments			✓	✓
Multiple noise-canceling microphones				✓

Feature	B1000A	B2000	Smartphone	B3000
Call button	✓	✓	✓	✓
DND button	✓	✓	✓	✓
Volume/menu selection buttons	✓	✓	✓	✓
LED indicators	✓	✓		✓[1]
Smart battery				✓
Single-bay and multi-bay chargers	✓	✓	✓	✓
Can charge battery while attached to device	✓	✓	✓	
Headset jack	✓	✓	✓	✓
Handset mode			✓	✓
MiniUSB interface			✓	
Read or play text messages	✓	✓	✓	✓
Send text messages			✓	
Background update support		✓		✓
802.11b support	✓	✓	✓	✓
802.11g support		✓	✓	✓
802.11a support			✓	
802.11d support		✓	✓	✓
802.11e QoS support		✓	✓	✓
Open, WEP, PSK, and PEAP authentication support	✓	✓	✓	✓
LEAP authentication support	✓	✓	✓	✓
EAP-FAST and EAP-TLS authentication support		✓	✓	✓
FIPS 140-2 certified		✓		
U-APSD support		✓	✓	✓

Feature	B1000A	B2000	Smartphone	B3000
CCKM support		✓	✓	✓
TCP-to-Genie support[2]		✓		✓
ASCII passphrase support for preshared key			✓	✓
Bluetooth support			✓	
Anti-microbial protection		✓		✓
Flippable display				✓
Screen saver		✓		
Protective sleeves	✓	✓		
Available colors	black	black and white	black	black and white

Notes:

1. B3000 has only one multicolor LED, green to indicate power is on and DND mode is off, amber to indicate power and DND mode are on
2. Requires Vocera Server 4.2 GA (or later).

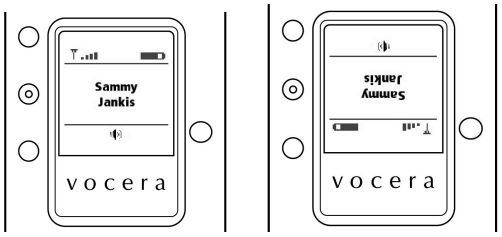
Enhanced Durability

The B3000 is more durable and rugged than its B2000 predecessor. All buttons on the badge now use dome switches instead of mechanical switches. Menu selection buttons have been moved from the side to the front of the badge, and the battery latch is now part of the battery. A metallic spine reinforces the shell and serves as the attachment point for accessories at the top of the badge. The B3000 has been tested to withstand dust, shock, and vibration. Like the B2000 badge, the B3000 is NOT water-resistant.

Enhanced Display

The B3000 badge display, which is 11% larger than the B2000 display but with nearly twice as many pixels, has been moved to the front of the badge and positioned in portrait orientation. To conserve power, the display is activated only when you press buttons, use menus, or are on a call. Otherwise, the display is powered off. You can choose to invert the screen, thus letting you conveniently read the text by tilting the bottom of the badge up.

The following figure show the B3000 screen in different orientations (right side up and upside down):



The following figure shows a user tilting his badge up to read the inverted screen:

Note: When you tilt the badge to read the screen, make sure your fingers do not block any of the four microphones.

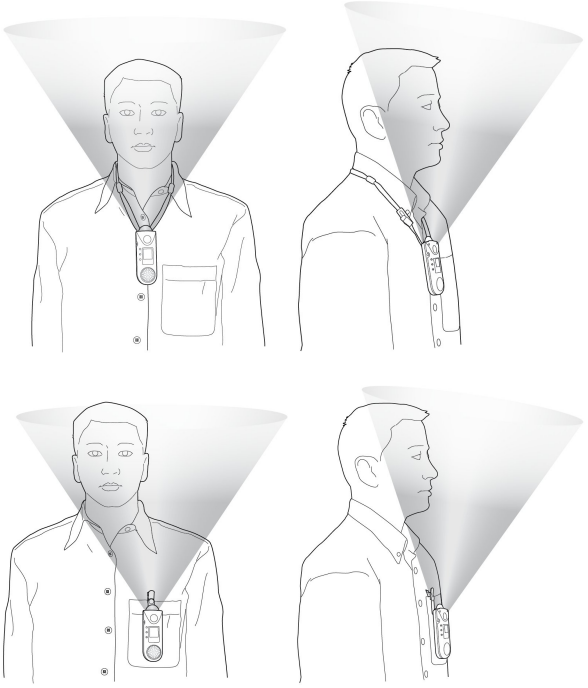
Increased Speaker Volume

The B3000 has a speaker with 85 dBSPL peak loudness, more than 10 dB louder than the B2000 speaker, making it easier to use without a headset in noisy areas or areas with persistent background noise.

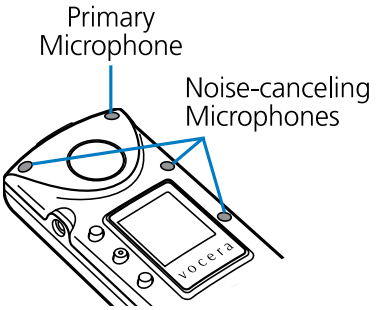
Integrated Noise Cancellation

The B3000 has enhanced noise cancellation as well as better acoustic echo cancellation. The badge has an array of four directional microphones (two at the top and two along the right front side), each with their own echo cancellor, reducing background noise while you speak.

The following figures illustrate B3000 microphone sensitivity. They show front and side views of someone wearing the badge using a lanyard or a universal clip. The shaded area above the badge is the *speech zone*, the region in which audio can be detected.



The following figure shows the primary B3000 microphone and the three noise-canceling microphones.



The noise cancellation features of the B3000 badge have been designed to provide significant improvement in speech recognition accuracy in environments with background noise compared to the older B2000 model.

Smart Battery and Power Efficiency

The lithium-ion polymer smart battery continuously monitors battery life and is able to accurately report remaining capacity. Due to improvements in power efficiency in the B3000 badge, a fully charged B3000 standard battery should provide 3 hours of talk time (U-APSD enabled) and up to 45 hours of standby time. A fully charged B3000 extended battery should provide 5 hours of talk time and 60 hours of standby time. Unlike the B2000 battery, you must remove the B3000 battery from the badge to charge it.

Handset Mode

Version: Vocera 4.3 SP2 or later

The B3000 lets users switch to handset mode to ensure privacy or use the badge in a high noise environment without a headset. When the badge is in handset mode, you can use it like a telephone handset. Press the Call button to make a call or answer a call, and then put the badge speaker to your ear and speak into the primary microphone located on the front of the badge at the top right corner. Only the primary microphone is enabled in handset mode; the three noise-canceling microphones are automatically disabled. For information on how to switch the badge to handset mode, see **Turning Handset Mode On or Off** on page 26.

Note: When you hold the badge speaker up to your ear, do not cover the primary microphone with your fingers. Otherwise, the Genie will not hear anything you say.

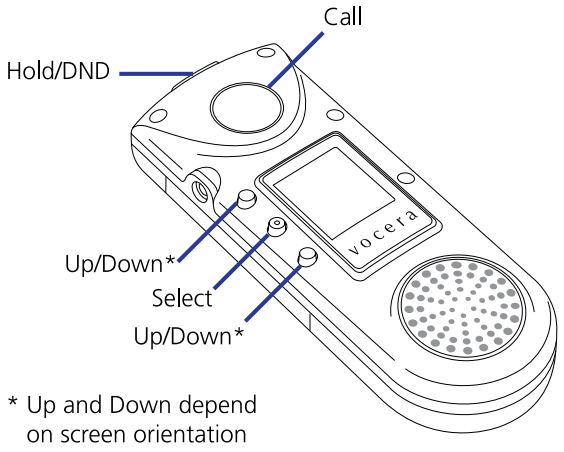
Improved Attachments

B3000 lanyards and clips attach easily and securely to the metal spine at the top of the badge, letting you remove the attachment without removing the battery, and vice versa.

The Badge Menus

The display on the *front* of the badge shows a series of menu screens that comprise the top level of the menu system. Press the Select button to display the menu, and then use the Up or Down buttons to navigate.

The Up, Select, and Down buttons are on the front of the badge. Up and Down depend on the orientation of the screen.



Use the Select button to choose a displayed item. To return to the main screen at any time, press and hold the Select button until the badge beeps.

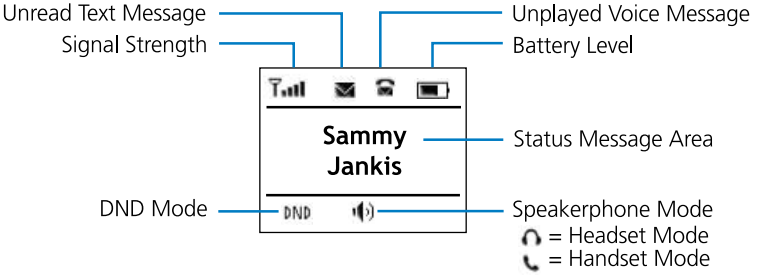
The top-level menu consists of the following choices: Info, Power Off, Messages, Settings, and Return Home. The Settings menu has the following submenu: Volume, Font, Handset, and Flip Screen.

The following sections describe your badge's display menu choices.

Main Screen

The main screen appears when you turn on the badge. This screen has a status message area with symbols that show you the wireless network signal strength, the battery charge level, whether you are in speakerphone or headset mode, and whether you have unread text messages or unplayed voice messages.

The following figure shows the B3000 main screen:



The status message area may show one of the following alerts:

Status Message	Meaning
Name—not blinking	The name of the person who is logged in to the Vocera system using this badge.
Name—blinking	If someone is trying to call you, this shows you the name of the person who is calling. If you are already on a call, this shows the name of the person with whom you are currently speaking. If you are already on a call and you hear the Call Waiting tone, this displays the name of the person who is trying to call you. If you are in a conference, this shows its name. If you are receiving a broadcast, this shows the name of the person making the broadcast. If you received a message, this shows the name of the person who sent the message for 15 seconds.
Vocera	Your badge is communicating with the Genie.
Logged out	No one is logged in with this badge.
Searching for Access Points *or* Off Network	The badge is out of network range or is not able to connect with the network. If you are sure you are within range of your network, contact your system administrator.
Searching for Server	The badge is within network range, but it is not communicating with the Vocera Server. See **Why does my device display say "Searching for Server"?** in the *Vocera Badge User Guide*.
Authenticating	The badge's credentials are being authenticated for network security.
Requesting IP Address	The badge is requesting an IP address from the DHCP server.

Info Menu

The Info menu gives you information about the badge you are using and how it is connected to the network.

Most of this information is intended to be used by your system administrator for diagnostic purposes.

The Info menu provides the following information:

- Battery. The battery strength is given in volts (V). The badge operates correctly when the battery level is 3.5 V or greater.
- Badge MAC. The MAC address is a unique identifier for your badge that the Vocera server uses as the Badge ID. On a B3000 badge, this screen also displays the Vocera serial number.
- Location. The name of the location or the physical network address of the access point with which your badge is currently communicating.
- Label. A label that uniquely identifies the device in the Vocera system for device management purposes.
- Badge IP. The Internet Protocol (IP) network address of the badge. The Badge IP command also shows the subnet mask—or netmask— and the gateway IP address.
- Version. The version of the firmware that your badge is using.
- FIPS Mode. Whether FIPS 140-2 mode is enabled. For more information about FIPS, see the *Vocera Badge Configuration Guide*.

  Note: FIPS mode is certified for B2000 badges only.

- Server IP. The IP network address of the Vocera Server or the active node of the Vocera Server cluster.
- Cluster. The IP network addresses of the nodes in the Vocera Server cluster, if one exists. If all the Vocera Server cluster IP addresses don't fit on one screen, you can scroll to the next screen by pressing Down.
- AP MAC. The physical ID of the access point to which the badge is currently connected.
- User. The name of the person who is currently logged in to your network with this badge.
- Radio. If the badge is connected to the network, displays the message "Connected" and the channel that the radio is using; otherwise, displays the message "Powering off."

  This screen also displays the signal-to-noise ratio (SNR) of the connection and plays a beep for the built-in survey tool.
- SSID. The SSID of the access point the badge is connected to.

Power Off Menu

Power Off turns off all power to the badge and the badge display to preserve the battery charge when you are away from the network.

Press the Call button to turn the power on again.

Messages Menu

Your badge can display text messages that were sent from email accounts, the Vocera User Console, or an application that integrates with the Vocera system, such as a nurse call system.

When you select **Messages**, the display shows one subject line for each text message. On a B3000 badge, the subject line for only one message is shown at a time. A closed envelope symbol next to a subject means you have not yet read that message; an open envelope means you have already read that message. An [S] means you have already read and saved that message. See **Reading Text Messages** in the *Vocera Badge User Guide* for more information.

Settings Menu

The Settings menu (available only on B3000 badges) displays the following submenus for personal settings: Volume, Font, Handset, Group Mode, Flip Screen, and Return Home. The Vocera Server preserves these settings whenever you log into a different B3000 badge.

Volume Menu

The Volume menu independently adjusts the sound level for speakerphone and headset modes. On B3000 badges, you can also set the volume for handset mode. See **Adjusting the Volume** on page 25 for instructions.

Font Menu

The Font menu lets you display all uppercase letters or mixed case letters in text messages. See **Adjusting the Message Font** on page 24 for instructions.

Handset Menu

Version: Vocera 4.3 SP2 or later

The Handset menu (available only on B3000 badges) lets you turn handset mode on or off. In handset mode, you can press the Call button to make a call or answer a call, and then put the badge speaker to your ear and speak into the primary microphone located on the front of the badge at the top right corner. This ensures privacy and lets you use the badge in a high noise environment without a headset. See **Turning Handset Mode On or Off** on page 26 for instructions.

Group Mode Menu

Version: Vocera 4.3 GA or later

The Group Mode menu (available only on B3000 badges) lets you turn off noise-canceling microphones while you are on a call, thus widening the speech zone and letting other people speak into the badge's primary microphone. If you are in a noisy environment, you can disable Group Mode to eliminate background noise while you are on a call.

Flip Screen Menu

Version: Vocera 4.1 SP7 or later

The Flip Screen menu (available only on B3000 badges) lets you invert the screen, turning it upside down. When the screen is inverted, you can conveniently read the text by tilting the bottom of the badge up.

Custom Settings

Vocera badges let you to customize for Volume, Font, Handset, Group Mode, and Flip Screen for each user. When you log into a different B3000 badge, your personal settings are preserved.

Adjusting the Message Font

You can adjust the way that the badge displays text messages. If you receive a lot of text messages—for example, if your site integrates with a messaging system such as a Nurse Call System—you may want to choose the display that is most readable for you.

To adjust the font used by badge messages on a B3000:

1. Hold the badge, and orient it so that you can read the screen.
2. Press the Select button to see the menu, then press the Up button until you see the **Settings** icon.
3. Press the Select button to choose the Settings menu.
4. Press the Up button until you see the **Font** icon.
5. Press the Select button to choose the Font menu.

   The display prompts you to select either all uppercase letters (UPPERCASE MSG ON) or sentence-style mixed case letters (UPPERCASE MSG OFF).

6. If necessary, press the Up or Down buttons to move the highlight, then press the Select button to set the text message display and return to the main screen.

Adjusting the Volume

You can adjust the sound level for speakerphone or headset mode independently. On B3000 badges, you can also set the volume for handset mode. There are two procedures for adjusting the volume: one for when the badge is idle, and one for when you are on a call.

When you use the Up and Down buttons to adjust the volume rather than using the Volume menu, the change affects only the listening mode in use at the time. That is, if you are using a headset and you adjust the volume during a call, you change the volume for the headset only. If the Announce Through Speaker property is enabled (see **Using the Announce through Speaker Commands** in the *Vocera Badge User Guide*), you change the volume for the badge speaker only (even if you're using a headset).

To adjust the volume when you are on a call:

- Do either of the following:
  - Press the Up button as many times as necessary to increase the volume to the level you prefer.
  - Press the Down button to decrease the volume.

To adjust the volume when the badge is idle on a B3000:

1. Hold the badge, and orient it so that you can read the screen.
2. Press the Select button to see the menu, and then press the Up button until you see the **Settings** icon.
3. Press the Select button to choose the Settings menu.
4. Press the Select button again to choose the Volume menu.

   The display prompts you to select one of the following modes:

   - **Speaker**
   - **Headset**
   - **Handset**
5. If necessary, press the Up or Down buttons to move the highlight, then press the Select button to set the volume for the specified mode.
6. Do either of the following:

- Press the Up button as many times as necessary to increase the volume to the level you prefer.
- Press the Down button to decrease the volume.

  The display changes accordingly.

7. Press the Select button to set the new volume level and return to the main screen.

Turning Handset Mode On or Off

Version: Vocera 4.3 SP2 or later

You can turn handset mode on or off for a B3000 badge. After you answer a call in speakerphone mode, you can put the caller on hold, switch to handset mode, and then resume the call.

To turn handset mode on or off for a B3000:

1. Hold the badge, and orient it so that you can read the screen.
2. Press the Select button to see the menu, then press the Up button until you see the **Settings** icon.
3. Press the Select button to choose the Settings menu.
4. Press the Up button until you see the **Handset** icon.
5. Press the Select button to choose the Handset menu.
6. Press the Up or Down buttons to switch between **Handset Mode Off** or **Handset Mode On**, and then press the Select button to make your selection and return to the main screen.

   When handset mode is on, the handset mode icon appears at the bottom of the screen.

To use a B3000 badge in handset mode:

- Press the Call button to make a call or answer a call, and then put the badge speaker to your ear and speak into the primary microphone located on the front of the badge at the top right corner.

To switch to handset mode while on a call:

1. Press the DND button on the top of the badge to put the call on hold.
2. Hold the badge, and orient it so that you can read the screen.

3. Press the Select button to see the menu, then press the Up button until you see the **Settings** icon.
4. Press the Select button to choose the Settings menu.
5. Press the Up button until you see the **Handset** icon.
6. Press the Select button to choose the Handset menu.
7. Press the Up or Down buttons to switch to **Handset Mode On**, and then press the Select button to make your selection and return to the main screen.
8. Put the badge speaker to your ear, and press the DND button to resume the call on hold.

Specifying the Group Mode Setting

Version: Vocera 4.3 GA or later

The Group Mode setting, which is available only on a B3000 badge, lets you disable the noise canceling microphones while you are on a call. By disabling the noise canceling microphones, the speech zone is effectively widened, thus letting people other than you speak into the badge's primary microphone.

The Group Mode setting affects the badge's speech zone only when you are on a badge-to-badge call. Group Mode is always off during Genie interactions and broadcasts.

To specify the Group Mode setting:

1. Hold the badge, and orient it so that you can read the screen.
2. Press the Select button to see the menu, then press the Up button until you see the **Settings** icon.
3. Press the Select button to choose the Settings menu.
4. Press the Up button until you see the **Group Mode** icon.
5. Press the Select button to choose the Group Mode menu.

   The display prompts you to select either **Enabled** or **Disabled**.

   The default setting is **Enabled**, meaning Group Mode is enabled only while on a call. Choosing **Disabled** turns on the noise-canceling microphones while you are on a call, thus eliminating background noise.
6. Press the Up or Down buttons to switch between settings, and then press the Select button to make your selection and return to the main screen.

Flipping the Screen

You can invert the B3000 screen, turning it upside down, thus making it easy to tilt up to read.

To flip the B3000 screen:

1. Hold the badge, and orient it so that you can read the screen.
2. Press the Select button to see the menu, then press the Up button until you see the **Settings** icon.
3. Press the Select button to choose the Settings menu.
4. Press the Up button until you see the **Flip Screen** icon.
5. Press the Select button to flip the screen and return to the main screen.

Anti-Microbial Protection

Most exterior surfaces of badges incorporate an antimicrobial additive from BioCote® to inhibit the growth of odor-causing bacteria, mold, and fungi. This additive is molded into the badge material, and you cannot wear it off or remove it by scratching the badge, protecting the product's surface from deterioration.

A topical solution, also from BioCote, is applied to the buttons and the plastic display screen of badges. The battery compartment, the inner surface of the battery, and the microphone screen do not incorporate antimicrobial protection.

Maintaining Your Badge

The Vocera badge requires very little maintenance: just recharge the battery when the power gets low, and clean the badge when necessary. The following sections describe how to charge the battery and how to clean the badge.

When to Charge the Battery

You must charge a new battery before you can use it. After that, you must recharge the battery as needed for the badge to operate properly.

There are several easy ways to check whether you need to recharge the battery:

1. On a B2000 badge, the green indicator light on the top of the badge turns red and blinks rapidly. B3000 badges do not have a red indicator light.
2. The battery-level indicator on the badge display shows empty.

3. An alert signal plays at regular intervals.

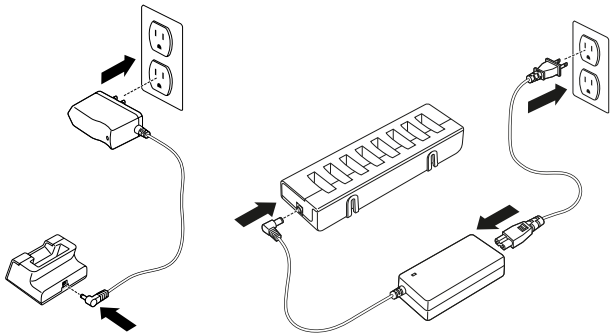
   Note: This signal may be disabled by the system administrator on request.

Preparing the Charger

Important: Before you use a charger, read **Important Safety Instructions** on page 105.

To prepare the charger for use, insert the single-pronged plug into the outlet in the charger, and plug the two-pronged power plug into a 110V or 220V AC outlet depending on the Vocera-supplied power adapter for your country.

Preparing the B3000 Charger



There are two indicator lights on the front of the B3000 charger. The capacity indicator is a blue light, and the charge status indicator is a red or green light. The following table describes the meaning of the indicator lights.

Indicator	Light	Meaning
Capacity (Blue)	Light off -or- Blue light for one second, then off	There is no battery in the charger, the battery is not seated properly, or the battery exceeds 80% capacity.
	Blinking blue	Capacity is between 80 % and 60%. Prepare to replace the battery soon.
	Steady blue	Capacity is less than 60% or the battery is beyond its useful life. If this happens, replace the battery.
Charge Status (Red/Green)	Light off	There is no battery in the charger, or the battery is not seated properly.
	Blinking green	The battery is charging.
	Steady green	The battery is fully charged.
	Blinking red	The battery failed to charge after 4 hours.

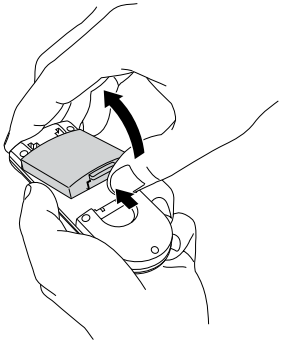
Indicator	Light	Meaning
	Steady red	The battery is unable to charge, or there is a problem with the charger. If the charger works when you try to charge a different battery, dispose of the original battery and charge a new one.

Charging the B3000 Battery

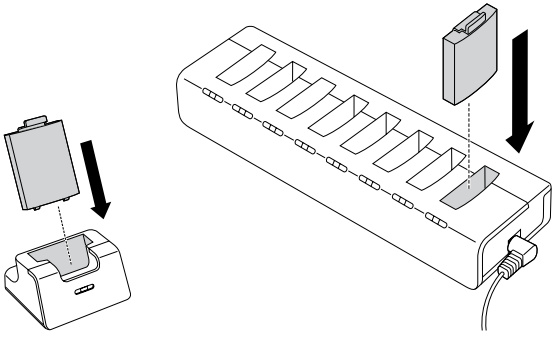
The B3000 battery can only be charged after it has been removed from the badge. It cannot be charged while it is attached to the badge. When you remove the battery, you do not need to remove an attached lanyard or clip from the badge.

To charge the B3000 battery:

1. Use your thumb to press the battery latch and lift it up, and then remove the battery.



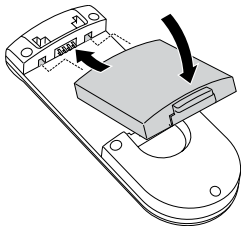
2. Insert the battery into the charger, and press down on the battery until you see the blue indicator light turn on.



If battery capacity exceeds 80%, the blue indicator light will turn off after a second.

The green indicator light on the front of the charger will begin to blink when the battery is positioned correctly, and it will continue to blink while the battery is charging. When the indicator glows steadily, the battery is fully charged. Charging normally takes only a few hours.

3. Remove the battery from the charger.
4. Slide the pegs at the top of the battery into the two holes in the badge's battery compartment.



5. Press down gently to seat the battery in the badge.

Cleaning the Badge and Accessories

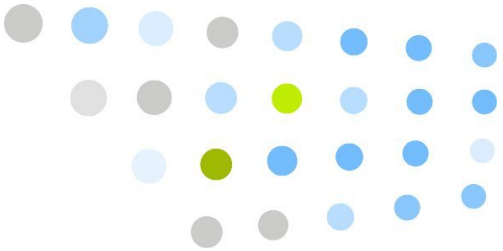
To clean a Vocera badge, battery, universal clip, protective sleeve, and battery charger, use a soft cloth dampened with water, isopropyl alcohol, or a germicidal solution, or use a commercially available cleaning wipe containing only those recommended cleaning agents.

To clean a standard Vocera lanyard, wash it in a commercial washing machine, and then allow it to air dry.

Important:

- Unplug the battery charger before cleaning.
- DO NOT machine-wash the Vocera headset-ready lanyard. Hand-wipe it instead.
- DO NOT use Clorox wipes, strong detergents, or abrasive cleansers to clean the badge. Such cleansers can damage the badge's finish.
- DO NOT pour liquid directly onto the badge or immerse it in water. The badge speaker, microphone, and battery pack are not watertight.
- DO NOT open the badge for any reason. Opening the badge voids all warranties.

- DO NOT attempt to clean a badge that has been dropped into body fluids. Dispose of biohazardous materials properly.



B3000 Device Management

Vocera device management features allow you to manage, track, and maintain the hardware devices that connect to the Vocera system. If your Vocera system includes device management features, you can use them to do the following things:

- Maintain an inventory of Vocera devices
- Increase accountability of organizations that use Vocera devices
- Track Vocera devices through their life cycle
- Prevent loss and control damage to Vocera devices
- Report on the status and usage patterns of Vocera devices

For more information about Vocera device management features, see the *Vocera Administration Guide*. This section provides information on device management features that are specific to the B3000 badge.

Automatically Loading B3000 Badges into the System

Vocera automatically loads new devices into the system the first time they connect to the Vocera Server. This feature ensures that every device that connects to the Vocera Server is recorded by the system for inventory purposes.

When the server automatically loads a new device, it records the following device information:

- MAC Address
- Serial Number
- Site
- Type
- Color

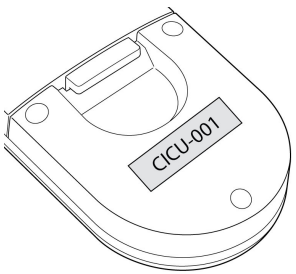
By default, the status given to devices automatically loaded by the server is "Unregistered." The system device manager should use the **Devices** page of the Administration Console to assign unregistered devices to an owning group and change the status from "Unregistered" to "Inventory" or "Active." See **Adding or Editing a Device** in the *Vocera Administration Guide*.

Labeling B3000 Badges

When you label devices, follow these guidelines:

- The **Label** field that you enter for devices in the Administration Console is limited to 20 characters and the value must be unique. Keep this in mind before you create the physical labels that will be applied to devices.
- Prefix the label text for each device with the abbreviation of the group (for example, RAD for radiology and CICU for cardiac intensive care unit) that owns the device. Other visual cues such as different colored labels, dots, or stickers can help quickly identify the group.
- Labels should be applied directly to the *back* of a B3000 badge, beneath the battery compartment.

Figure 1. B3000 badge with a label



- **DO NOT use metallic or magnetic labels to label the device.** Metallic or magnetic labels—including labels that use metal-based dye—can adversely affect the device's radio.
- If the device is shared between multiple users, the label should have a unique sequential identifier, such as RAD-001, RAD-002, and so on. The sequential numbering of devices makes it easier for the device manager to identify whether a device is missing from the sequence.
- If the device is not shared and you know the user's name, the label could have the user's initials, such as RAD-001-JP.

- If you want to use the same label as a device that has been retired, you must change the **Label** field for the retired device first. You can prepend the label of the retired device with the string "RETIRED-" or "RET-".

Monitoring Active Devices

After a device has been added to the system and assigned to a group, system device managers, group device managers, and system administrators can use the Device Status Monitor page of the Administration Console to monitor all active devices on the system. Devices are listed by group.

For information about using the Device Status Monitor page, see **Device Status Monitor** in the *Vocera Administration Guide*.

Note: Unregistered devices, that is, devices that have not yet been recorded by the system device manager and assigned to a group, can be used to log into the Vocera system. However, unregistered devices are not listed in the Device Status Monitor.

Managing B3000 Badges

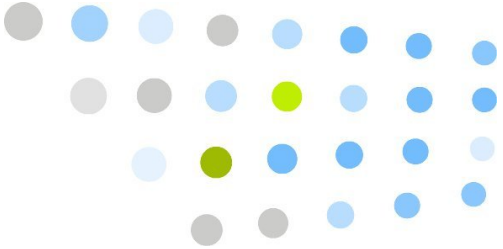
When you click Devices in the navigation bar, you can view devices currently in the Vocera system, including B3000 badges.

Vocera uniquely identifies B3000 badges by the MAC Address field, an alphanumeric value. The Vocera system can derive the MAC address for a B3000 badge from the serial number, also an alphanumeric value. When you enter the serial number for a B3000 badge in the Administration Console, the MAC Address field is populated automatically.

Most MAC addresses for B3000 badges have the following 6-character prefix: 0009ef. The last 6 characters of the B3000 MAC address are identical to the last 6 characters of the serial number.

Reporting on B3000 Badges

B3000 is listed as one of the Device Types in the Vocera Report Server console. This allows you to filter reports to show only B3000 badges.



Configuring Badges

The following topics explain how to configure new badges, update existing badges, and troubleshoot your badge configuration:

- **Configuring New Badges** on page 41

  Provides best practices for performing the initial configuration of new badges.

- **Setting Up the Configuration Computer** on page 47

  Describes how to set up a computer and connect it to an access point so you can download configuration settings to new badges.

- **Creating a Property File to Download** on page 53

  Shows you how to run the Badge Properties Editor and create a **badge.properties** file that determines specific badge properties and behavior.

- **Using the Badge Configuration Utility** on page 71

  Describes how to run the Badge Configuration Utility to download the properties to new badges.

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.

To configure a test badge:

1. Set up a configuration computer using the network settings required to connect to badges that have factory default settings.

   See **Setting Up the Configuration Computer** on page 47 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 **Creating a Property File to Download** on page 53.

   Best Practice: 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 **Configuring Badges with Static IP Addresses** on page 44. This section assumes you are using a DHCP server to assign IP addresses to the badges.

3. Make sure the production Vocera Server is running and the badge is within range of the wireless network it is trying to connect to.

   The badge will attempt to connect to the Vocera 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 Server using the Vocera 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 Server.

     Continue with **Configuring the Remaining Badges** on page 43.

- 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 Server.

  Continue with **Troubleshooting Badge Configuration** in the *Vocera Badge Configuration Guide*.

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.

8. After you are finished troubleshooting, copy the **badge.properties** file you created on the configuration computer to the **\vocera\config** directory of your production Vocera Server.
9. Do either of the following:
   - If your production Vocera Server is running, stop it and then restart it to load the **badge.properties** file into memory.
   - If your production Vocera Server is not running, start it to load the **badge.properties** file into memory.

   See **Using the Vocera Control Panel** in the *Vocera Installation Guide*.

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** on page 41; you simply use the Badge Configuration Utility to connect to each of your remaining badges.

To configure the 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 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.

   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.

Configuring Badges with 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.

To configure badges with static IP addresses:

1. Set up the configuration computer.

   See **Setting Up the Configuration Computer** on page 47.

2. Set up the isolated access point.

   See **Setting Up an Isolated Access Point** on page 50.

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 54.

   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 **\vocera\config\badge.properties** file in Notepad.

   b. Add or edit the badge IP address properties that corresponds to the type of badge you are configuring:

Badge Type	Properties
B3000	B3.ConfigStaticIP B3.BadgeIPAddr B3.SubnetMask B3.GatewayIPAddr B3.DNS1IPAddr
B2000	B2.ConfigStaticIP B2.BadgeIPAddr B2.SubnetMask B2.GatewayIPAddr B2.DNS1IPAddr
B1000A	BadgeIPAddr SubnetMask GatewayIPAddr DNS1IPAddr DNS2IPAddr

   For details of these badge properties, see **Badge Property Reference** in the *Vocera Badge Configuration Guide*.

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

   c. Save the edited file, but DO NOT close Notepad.

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** in the *Vocera Badge Configuration Guide*.

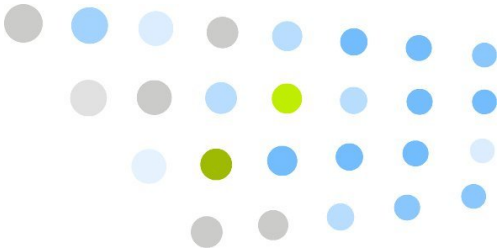
7. When the download is complete, the badge reboots and tries to connect to the network.

   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 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 Server. See **Troubleshooting Badge Configuration** in the *Vocera Badge Configuration Guide*.

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 4.Step 4.c. Remove any line beginning with B3.BadgeIPAddr, B2.BadgeIPAddr, or BadgeIPAddr, or put a pound sign (#) on the first column of that line.
12. Save the file and exit Notepad.

Best Practice: If you are configuring badges with static IP addresses, DO NOT copy the the **badge.properties** file to the Vocera 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 chapter describes how to set up the computer and other equipment needed to configure Vocera badges.

Configuration Hardware Requirements

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 configuration hardware for badges and phones:

Table 2. Configuration hardware requirements

Component	Requirement
Configuration Computer	See the **Vocera Voice Server Sizing Matrix**[1].
Access Point	An isolated access point that is not connected to the installation site's network.
Cable	An Ethernet crossover cable to connect the configuration computer and the access point.

[1] http://www.vocera.com/products/documents/VoceraServerSizingGuidelines.pdf

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. Here is the procedure for setting up the configuration computer:

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 49.

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 49.

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 50.

Any notebook or desktop computer running Windows 2003 Server or Windows XP and containing an Ethernet network card is typically sufficient for use as the configuration computer.

Removing Earlier Versions of the 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 Server version must be the same.

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.

Installing Badge Configuration Utilities

You can install the Badge Configuration Utilities after selecting **Vocera Server** from the main Vocera installation screen. In the installation program, you must specify the drive to install on and the country.

To install the Badge Configuration Utilities:

1. Log in to the computer with administrator privileges.
2. **Electronic Software Distribution:** Navigate to the folder where you extracted the contents of the Vocera ISO file, and run the **vocera.hta** file. For details on downloading the software, see **Electronic Software Distribution** in the *Vocera Installation Guide*.

   DVD Media: Insert the Vocera Software DVD in the drive. The main installation screen appears automatically. If this screen does not appear, run the **vocera.hta** at the root of DVD.
3. Click **Vocera Server**.
4. On the Welcome screen, click **I Agree** to continue with the installation program.

   The Available Features screen appears.
5. Clear the **Vocera Server** checkbox, and make sure the **Badge Configuration Utilities** checkbox is selected. Click **Next**.
6. Continue following the prompts in the installation program.

   Use the **Help** button on any screen for further information.

   Click **Install** on the final installer screen to install the software.
7. When you are finished, select **Yes, I want to restart my computer now**, and click **Finish**.

Specifying TCP/IP Properties

You need to specify certain TCP/IP properties in the configuration computer to allow a new badge to connect to it properly.

To specify TCP/IP properties:

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

- 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.

- 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.

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.

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.

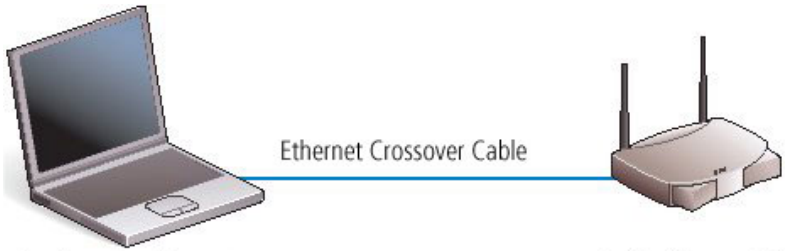
   Many access points require only a browser for configuration.
4. Using the access point configuration utility, make sure your access point is set up as follows:
   - Allow open authentication (typically the default)
   - Turn off all security (typically the default)
   - Assign the SSID value as **vocera** (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.

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

Figure 2. Badge configuration hardware



Configuration Computer
- IP address = 10.0.0.1
- Subnet mask = 255.0.0.0

Isolated Access Point
- Open authentication
- No security
- Set SSID to vocera (lower case)
- Accept broadcast SSID
- 802.11 infrastructure mode

Creating a Property File to Download

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 Server to download these properties to all your badges.

Important: 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 Badge Profiles

A badge *profile* is the set of properties that specifies how that badge connects to your network. Each type of Vocera badge has an independent profile, which allows different types of badges to run on VLANs 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 wish to use.

For example, suppose different badge types use different VLANs:

- B3000 and B2000 badges connect to the *venus* VLAN using PEAP.
- B1000A badges connect to the *mars* VLAN using a pre-shared key.

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

Using the Badge Properties Editor

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

Note: 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.

To use the Badge Properties Editor:

1. Choose **Start > Programs > Vocera > Badge Utilities > 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 55 describes the minimal set of properties you need to set for any badge in use at your site.
   - **Setting Security Properties** on page 57 describes how to make badges work with the security features implemented on your wireless network.
   - **Setting Wireless Properties** on page 66 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 **Using the Badge Configuration Utility** on page 71.

- If you are updating badges that are already connected to a Vocera Server, use the Vocera Server to download properties to the badges.

  See **Maintaining Properties and Firmware** in the *Vocera Badge Configuration Guide*.

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 3. General properties (B3000)

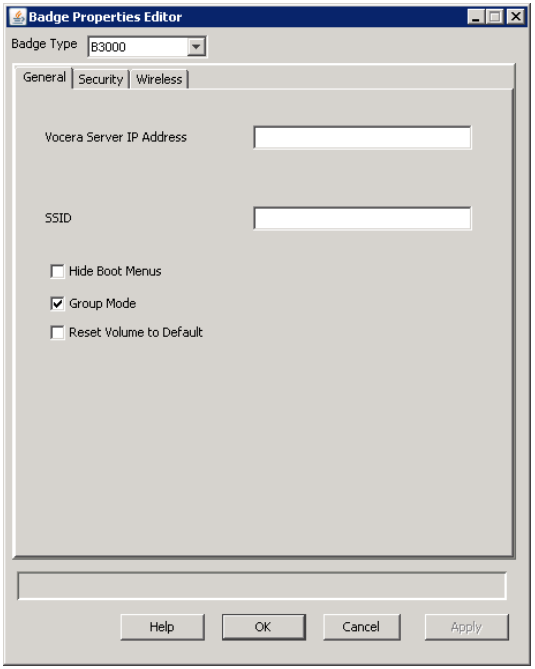


Table 3. General properties

Property	Description	Badge Types Supported
Vocera Server IP Address	Use the **Vocera Server IP Address** field to specify the IP address of the computer which is running the Vocera 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 badge supports a maximum of 63 characters for the members of the cluster list. This limit allows you to enter up to four numeric IP addresses, separated by commas, with no spaces between them.	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.	All

Property	Description	Badge Types Supported
Group Mode	When checked, this property turns on Group Mode, which means that noise-canceling microphones are turned off when users are on a call. Group Mode widens the speech zone, allowing other 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 badge users can change the Group Mode setting on their badges. Group Mode is always off during Genie interactions and broadcasts.	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.	B3000, B2000

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 VLANs and take advantage of the enhanced security support offered by newer badge models. If all your badges reside on the same VLAN, the security you choose must be supported by all badge types. See **About Badge Profiles** on page 53 for information about configuring badges on separate VLANs.

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

Figure 4. Security properties (B3000)

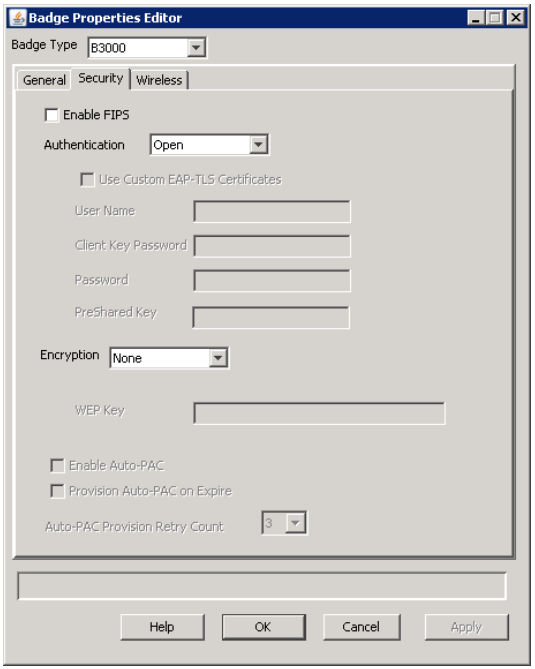


Table 4. Security properties

Property	Description	Badge Types Supported
Enable FIPS	When enabled, this property causes the B2000 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 64. By default, this property is not selected. This property applies only to B2000 badges currently. When the **Enable FIPS** box is checked, WPA2-PSK or WPA2-PEAP is required. To enable WPA2-PSK and WPA2-PEAP for Vocera badges, please select WPA-PSK or WPA-PEAP authentication in combination with AES-CCMP encryption.	B3000, B2000

Property	Description	Badge Types Supported
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 Server and the Vocera configuration computer. See **Configuring EAP-FAST Authentication** in the *Vocera Infrastructure Planning Guide*.	All

Property	Description	Badge Types Supported
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 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 Server or the configuration computer. 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 server-side certificates on your authentication server. By default, this property is not selected. This property is not available for the B1000A badge. It is also not available when the **Authentication** property is NOT set to EAP-TLS.	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 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 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** in the *Vocera Badge Configuration Guide*. When the badge reconnects, it retrieves the new PAC file automatically from the ACS.	All

Property	Description	Badge Types Supported
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 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 **Table 11, "Vocera security support"** on page 83 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 65.	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 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 **Increasing the EAP Request Timeout for Automatic PAC Provisioning** in the *Vocera Infrastructure Planning Guide*.	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.	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.	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/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**.

Note: FIPS Mode is not certified for the B3000 badge yet.

To enable FIPS mode for B2000 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. Make sure the **Enable FIPS** checkbox is checked.
7. To enable WPA2-PSK and WPA2-PEAP for Vocera badges, please select WPA-PSK or WPA-PEAP authentication in combination with AES-CCMP encryption.
   - If you select WPA-PSK, specify the **PreShared Key** value.
   - If you select WPA-PEAP, specify the **User Name** and **Password** values. Each badge must use the same user name and password.
8. Select other badge properties as appropriate.
9. Click **OK** to save these values and close the Badge Properties Editor.

10. Configure a test badge to make sure it can connect to your network. See **Configuring a Test Badge** on page 41.
11. If the test badge connected successfully, copy the **badge.properties** file to the **\vocera\config** folder of the active Vocera Server computer.
12. Use the Vocera Control Panel to stop and start the active Vocera Server. When the Vocera 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 Hexadecimal Pre-shared Key for WPA-PSK

With WPA-PSK authentication, each wireless network device encrypts the network traffic using a 256-bit key (a 64-character hexadecimal string). Many access points have drivers that allow you to enter an ASCII passphrase that is then internally converted to a 256-bit key. However, the **PreSharedKey** property for B1000A and B2000 badges in the Badge Properties Editor requires the raw hexadecimal value.

If you know the ASCII passphrase used by your wireless network, you can convert the passphrase to the hexadecimal key using a Web-based tool found at the following location:

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

Configuring Badges for EAP-TLS 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.

Note: B1000A badges do not support EAP-TLS authentication.

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 5. Security properties needed for EAP-TLS

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 **Configuring EAP-TLS Authentication** in the *Vocera Infrastructure Planning Guide*.

Setting Wireless Properties

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

Figure 5. Wireless properties (B3000)

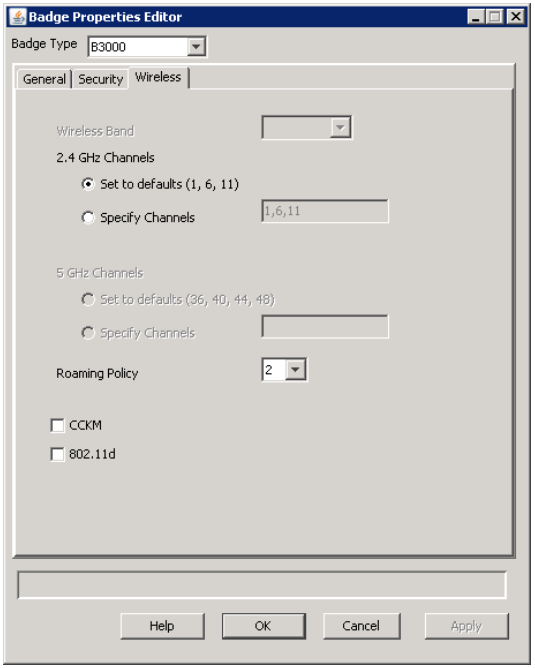


Table 6. Wireless properties

Property	Description	Badge Types Supported
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.	B3000, B2000
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.	B3000, B2000

Property	Description	Badge Types Supported
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 0 to 3. The default value is 2.	B3000, B2000, B1000A
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.	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.	B3000, B2000

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.

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** in the *Vocera Badge Configuration Guide*.

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 **Setting Up the Configuration Computer** on page 47.

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 Server.

Note: You can use the Badge Configuration Utility to configure all Vocera badge types simultaneously.

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 Server computer.

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

Table 7. Directories and files used for configuration

Item	Description
fci	Directory containing B1000A firmware.
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 Server, containing the complete list of files for B2000 firmware. The Badge Configuration Utility and the Vocera 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 Server, containing the complete list of files for B3000 firmware. The Badge Configuration Utility and the Vocera Server use this file to determine what files to download to a B3000 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.

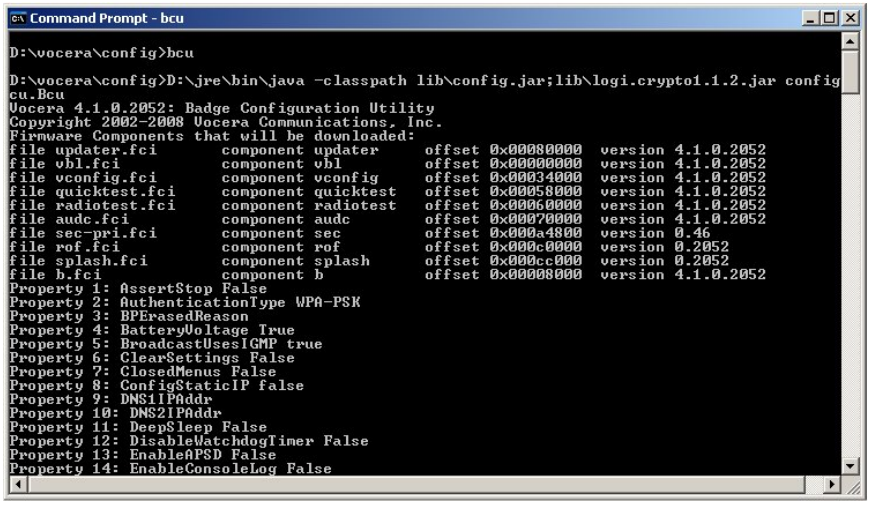
Running the Badge Configuration Utility

To use 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 6. 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 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 Server.

     Continue with **Configuring the Remaining Badges** on page 43.

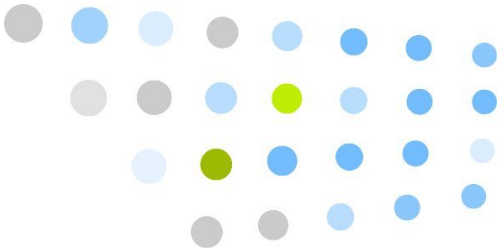
   - If the badge does not display "Logged Out" within 30 seconds to one minute, the badge is not configured properly and did not connect to the Vocera Server

Continue with **Troubleshooting Badge Configuration** in the *Vocera Badge Configuration Guide*.

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.



Infrastructure Topics

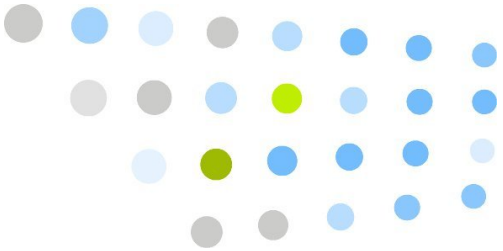
The following topics provide updated information about infrastructure requirements and recommendations for the B3000 badge:

- **B3000 Wireless Features** on page 77

  Discusses the network and badge configuration topics you need to address when integrating the B3000 badge into your wireless infrastructure.

- **B3000 Security Features** on page 83

  Discusses the security support that the B3000 provides.



B3000 Wireless Features

This chapter presents the following topics:

- **802.11b/g Support** on page 77.
- **Access Point Settings** on page 78.
- **Acceptable Voice Quality** on page 79.
- **The Roaming Policy Property** on page 81.

802.11b/g Support

The B2000 and B3000 badges support both 802.11b and 802.11g, although they cannot be configured to use *either* 802.11b or 802.11g data rates. Both the B2000 and B3000 automatically use the 802.11b and 802.11g data rates that have been enabled on the access points. For optimal coverage, Vocera recommends that you enable all 802.11b and 802.11g data rates on the access points.

The B1000A badge is an 802.11b client. It is compatible with 802.11b access points or 802.11g access points that are configured in either of the following ways:

- To support 802.11b clients only.
- To support a mixed 802.11b and g environment.

A mixed 802.11b and g environment, rather than a dedicated 802.11g environment, lowers the throughput for your 802.11g clients, but it still provides them with better throughput than a dedicated 802.11b environment.

Note: For information on Vocera's position regarding the proposed 802.11n standard, which promises significantly higher speed and range than 802.11b/g, search for **`802.11n`** in the Vocera Technical Support Knowledge Base.

Access Point Settings

Vocera requires specific settings for the following access point features:

Table 8. Required AP settings for Vocera

AP Feature	Setting
Beacon Interval	**100 milliseconds** (typically the default). See **Beacon and DTIM Intervals** in the *Vocera Infrastructure Planning Guide*.
DTIM Interval	**1**. See **Beacon and DTIM Intervals** in the *Vocera Infrastructure Planning Guide*.
Data Rates	Enable all 802.11b/g data rates, and set one or more to Basic. See **Data Rates** on page 78.
SSID	The same for all access points on a VLAN. You can configure badge profiles to use different SSIDs for different badge types. See **SSID and Security** on page 79.
Security Settings	The same for all access points on a VLAN. You can configure badge profiles to use different security settings for different badge types. See **SSID and Security** on page 79.
Peer-To-Peer Communication	**Enabled** on the access point or on the WLAN controller (if using lightweight access points). See **Peer-To-Peer Communication** in the *Vocera Infrastructure Planning Guide*.

Data Rates

For optimal reliability, Vocera recommends that you enable all 802.11b/g data rates on your network. When all data rates are enabled, the badge can switch among them if necessary to maintain a connection, minimizing the likelihood of lost packets. You must also set one or more data rates as Basic. See **Data Rates and Overlapping Cells** in the *Vocera Infrastructure Planning Guide* and **Configuring AP Radio Data Rates** in the *Vocera Infrastructure Planning Guide* for additional information.

SSID and Security

The badges are centrally maintained by the Vocera server from a single configuration file. Because the badge does not have a keyboard, this centralized management is practical and minimizes maintenance that would otherwise be time-consuming and error-prone.

You can use the Badge Properties Editor to specify properties for all Vocera badges. In addition, you can specify different network profiles for different badge types, allowing them to reside on different VLANs. See the *Vocera Badge Configuration Guide*.

See **Security** in the *Vocera Infrastructure Planning Guide* for additional information about configuring badge security.

Acceptable Voice Quality

Each type of Vocera badge provides a different utility for evaluating the communication quality of the signal you are receiving from an access point.

The survey tools use a logarithmic scale to measure communication quality, but the values are normalized differently. Consequently, communication quality is measured in *SNR* (for Signal-to-Noise Ratio) on B3000 and B2000 badges and in *CQ* (for Communication Quality) on a B1000A badge. An SNR value is similar but not equivalent to a CQ value. The SNR and CQ values are not equivalent to traditional SNR values, which are normally measured in decibels. Instead, SNR and CQ values are based on a logarithmic scale ranging from 0 to 92, where 0 represents no signal and 92 is the strongest possible signal with essentially no background noise.

Depending on what type of Vocera badge you have, use the appropriate tool to confirm that your access point coverage is sufficient to support the badge in all areas where it will be used. The Vocera system can maintain good voice quality in all places where the SNR value is greater than or equal to 16 and the CQ value is greater than or equal to 20.

The Vocera utilities for evaluating communication quality are Layer 2 applications that do not require the badge to connect to the Vocera server or to acquire an IP address. Consequently, you can use it to confirm network coverage early in the implementation process, before the Vocera system is physically deployed.

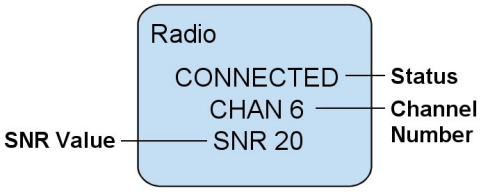
Note: To use the B1000A badge in survey mode, you must make sure that the badge VLAN at least temporarily allows open authentication while you conduct the survey. The B3000 and B2000 badge survey tools do not require open authentication.

To confirm communication quality levels throughout a site using a B3000 badge:

1. Press the Hold/DND button to put the badge in Do Not Disturb (DND) mode.
2. On the main menu of the badge, scroll to display the info icon.
3. Use the Select button to display the Info menu.
4. Scroll down until **RADIO** appears, then select it.

   The badge displays information similar to the following:

Figure 7. Radio Info screen



5. The badge begins beeping at the following rate to indicate the SNR value:

Table 9. B3000 badge beep rates in survey mode

Roaming Policy	SNR Value	Beep Rate
0	SNR > 16	1 beep / 5 seconds
	16 >= SNR >= 12	1 beep / second
	12 >= SNR >= 0	2 beeps / second
1	SNR > 18	1 beep / 5 seconds
	18 >= SNR >= 12	1 beep / second
	12 > SNR >= 0	2 beeps / second
2	SNR > 20	1 beep / 5 seconds
	20 >= SNR >= 12	1 beep / second
	12 > SNR >= 0	2 beeps / second
3	SNR > 22	1 beep / 5 seconds
	22 >= SNR >= 12	1 beep / second
	12 > SNR >= 0	2 beeps / second

6. Wear the badge normally.

   Use a lanyard or one of the other badge attachments to wear the badge properly. Do not handle the badge or read the display as you perform the test, or it will not measure access point signal strength correctly.

   Note: You may want to perform a survey with two badges, both in survey mode. Wear the first badge normally and listen for beeping tones that indicate the general SNR range. Hold the second badge to display the SNR value, but turn down the badge volume so the tones do not distract other people.

7. Connect a headset to the badge.

   The badge emits a tone during the test to indicate the communication quality. In certain environments, such as hospitals, this tone can be mistaken for the emergency sound made by life-support equipment.

8. Walk slowly through the entire coverage area and listen to the tones made by the site survey tool. You must perform the test in two directions offset by 180 degrees (while facing one direction, and then while facing the direction 180 degrees opposite).

   Don't forget to include stairways, elevators, kitchens, bathrooms, and other areas where Vocera usage exposes gaps in conventional site surveys.

9. To exit from the Radio Info screen, press the badge Select button.

10. Note any area where the tone from the Radio Info tool indicates that the coverage is less than or equal to the acceptable level for the current roaming policy, somewhere between 16 and 22.

    You must improve the coverage in these areas in order to have a successful deployment.

The Roaming Policy Property

The **Roaming Policy** property determines how aggressively the badge attempts to roam as the signal-to-noise (SNR) ratio of the transmission from an access point deteriorates. The badge assesses the SNR in terms of the SNR metric for B2000 and B3000 badges and the proprietary Communications Quality (CQ) metric for B1000A badges, as discussed in **Acceptable Voice Quality** on page 79. The badge begins to look for another access point when the SNR value or CQ value drops to a level specified by the **Roaming Policy** value.

The **Roaming Policy** value is an integer from 0 to 3, where 0 specifies the least aggressive roaming and 3 is most aggressive. By default, **Roaming Policy** is set to 2. The following table shows the relationship between badge SNR and CQ values and **Roaming Policy**:

Table 10. Roaming policy and badge SNR/CQ values

Roaming Policy Value	Typical B2000/B3000 SNR when Roaming	Typical B1000A CQ when Roaming	Comments
0	16	16	Typically not used because voice quality may have already deteriorated when roaming is initiated.
1	18	20	The lowest value typically used, since voice quality is maintained when roaming is initiated.
2	20	24	The default value, initiates roaming while voice quality is good on most networks.
3	22	28	Initiates roaming while voice quality is high. This value usually causes roaming that is too aggressive, but it may help roaming on a network with densely deployed APs. See **Data Rates and Overlapping Cells** in the *Vocera Infrastructure Planning Guide* for information about data rates.

The previous table shows the typical SNR and CQ values at which the badge initiates roaming. The actual SNR and CQ values may vary somewhat, due to environmental factors and dynamic changes in coverage.

If you are not satisfied with the roaming behavior of the badge, you can experiment by adjusting the Roaming Policy property. Make sure you test any changes thoroughly before implementing them on all badges in a production system.

To specify the Roaming Policy property:

- Use the Badge Properties Editor to set the **Roaming Policy** property to the appropriate value on all badges.

  See **Setting Wireless Properties** on page 66 for more information about how to set the **Roaming Policy** property.

B3000 Security Features

Security is a critical concern for any enterprise application. In particular, the data transmitted on a wireless network is often considered to be at risk because radio waves can be monitored without physical access to the network.

Vocera supports well-known industry standards for wireless security. This chapter summarizes the security support provided by Vocera and discusses the network overhead introduced by various security methodologies.

Note: You must configure properties in the Vocera badges to support the security requirements of your wireless network. See **Setting Security Properties** on page 57 for additional information.

Security Support

Vocera supports industry standard security systems as well as popular proprietary security methods such as Cisco LEAP. The following table summarizes the security support in Vocera:

Table 11. Vocera security support

Authentication	Encryption	B1000A Support	B2000 Support	B3000 Support	Smartphone Support
Open	None	✓	✓	✓	✓
	WEP64	✓	✓	✓	✓
	WEP128	✓	✓	✓	✓
PEAP (MS-CHAP v2)	TKIP	✓	✓	✓	✓
PSK	TKIP	✓	✓	✓	✓
EAP-FAST	TKIP		✓	✓	✓
EAP-TLS	TKIP		✓	✓	✓

Authentication	Encryption	B1000A Support	B2000 Support	B3000 Support	Smartphone Support
PEAP (MS-CHAP v2)	AES-CCMP		✓	✓	✓
PSK	AES-CCMP		✓	✓	✓
EAP-FAST	AES-CCMP		✓	✓	✓
EAP-TLS	AES-CCMP		✓	✓	✓
LEAP	TKIP-Cisco	✓			
	WEP64	✓	✓	✓	✓
	WEP128	✓	✓	✓	✓
	TKIP		✓	✓	✓
	AES-CCMP		✓	✓	✓

The LEAP, PEAP, EAP-FAST, and EAP-TLS protocols typically require each user in a network environment to be authenticated with a unique set of credentials. However, each badge in a profile must have the same security properties so the Vocera server can automatically update all badges when necessary. Consequently, Vocera supports device authentication for PEAP, LEAP, EAP-FAST, and EAP-TLS, not user authentication. All badges must present the same set of credentials for network authentication. See **About Badge Profiles** on page 53.

Vocera has tested the following authentication servers:

Table 12. Authentication servers

Model	Manufacturer	Supported Authentication
ACS (Access Control Server)	Cisco	EAP-TLS, EAP-FAST, LEAP, PEAP, and mixed LEAP/PEAP client environments
IAS (Internet Authentication Service)	Microsoft	EAP-TLS, PEAP (badge only)
Steel-Belted Radius	Juniper Networks	LEAP

Note: If you are using PEAP authentication on B1000A badges with Cisco ACS, do not enable EAP-GTC on the server, as this setting will interfere with authentication.

Security and Roaming Delays

In general, increasing levels of security increase the amount of time required for a client to associate with the network. The overhead introduced by security can cause performance problems with Vocera. This overhead is not noticeable the first time a badge associates with an access point, but it may cause a noticeable interruption in speech if a badge roams and re-associates while a call is active.

While encryption techniques such as WEP introduce a certain amount of overhead to each packet, the required processing is minimal and does not affect Vocera. The overhead introduced by authentication techniques, however, can be significant and may affect the performance of the badge as it roams.

The delay in re-associating when roaming depends upon the specific configuration of your network and the type of security you implement. You may need to experiment to find the best balance between an appropriate level of security and acceptable performance.

Authentication Delays

The following table provides general guidelines for the amount of additional overhead different methods of security introduce when roaming. The specific performance you see may vary depending upon the access point you are using and your network configuration.

Table 13. Average additional association delays caused by authentication

Authentication Type	Association Delay	Comments
WPA-PSK	< 100 ms	WPA-PSK often provides the optimal trade-off between security and performance.
EAP-FAST	200 ms	Frequent session timeouts can result in additional delays. See **Optimizing WPA-PEAP, LEAP, EAP-FAST, and EAP-TLS** on page 86.
LEAP		
WPA-PEAP	Varies	The association delay caused by authentication varies based on the cipher strength (1024 bit or 2048 bit) and the depth of certificate chains.
EAP-TLS		

All forms of authentication introduce considerable overhead. In particular, WPA-PEAP and EAP-TLS add the most overhead due to the time required for connecting to an authentication server. WPA-PSK provides a considerable level of security while introducing only minimal overhead.

Optimizing WPA-PEAP, LEAP, EAP-FAST, and EAP-TLS

The WPA-PEAP, LEAP, EAP-FAST, and EAP-TLS protocols require back-end authentication servers to authenticate client credentials the first time a client connects to the network, each time the client roams, and at periodic intervals. Various properties control how often the authentication occurs, and in the case of WPA-PEAP and EAP-FAST, whether a full authentication or a fast authentication occurs.

The authentication that occurs the first time a client connects to the network is not noticeable to a badge user because it appears to be part of the general boot and connection procedure. However, the authentication that occurs during roaming or at a timeout interval can interrupt a conversation, due to packets that are lost while the authentication server processes credentials and re-authenticates the badge. You can optimize badge performance by allowing fast reconnects and setting a lengthy timeout interval, as described in the following sections.

Timeout Intervals

On authentication servers, a **Session Timeout** value specifies the duration of time that elapses before a client such as the badge is required to re-authenticate, regardless of whether it has roamed. Some vendors may refer to this timeout value as a group session timeout or a user session timeout.

Because a session timeout always triggers re-authentication, you can optimize performance by making sure that the timeout interval does not expire too frequently. For example, if your employees typically work eight-hour shifts, you could set the session timeout value to eight hours, ensuring that an authentication timeout does not occur during a shift.

Note: Do not confuse this session timeout, with the WPA-PEAP session timeout described in **PEAP Session Timeouts** on page 87.

Fast Reconnects

WPA-PEAP and EAP-FAST require a full authentication the first time a client connects to the network, but optionally allow a fast reconnect any other time an authentication occurs, up until the expiration of the PEAP session timeout interval for WPA-PEAP or the expiration of the authorization PAC time to live (TTL) for EAP-FAST. See **PEAP Session Timeouts** on page 87 and **EAP-FAST Stateless Session Resume** on page 87.

Because a fast reconnect reduces the time required for reauthentication by several seconds, you can optimize WPA-PEAP and EAP-FAST performance by enabling fast reconnects. For example, if a user roams during a conversation, the authentication that occurs causes the minimum possible interruption when fast reconnects are enabled.

PEAP Session Timeouts

When you are using WPA-PEAP authentication, an additional value called the **PEAP Session Timeout** interacts with fast reconnects. When the PEAP session timeout interval expires, a client is required to perform a full authentication, regardless whether fast reconnects are enabled, the next time any authentication occurs. Do not confuse the PEAP session timeout with the session timeout described in **Timeout Intervals** on page 86.

You can optimize performance by making sure that the PEAP session timeout interval does not expire too frequently, as you do with the regular session timeout. For example, if your employees typically work eight-hour shifts, you could set the PEAP session timeout value to eight hours, ensuring that a full authentication does not occur during a shift.

EAP-FAST Stateless Session Resume

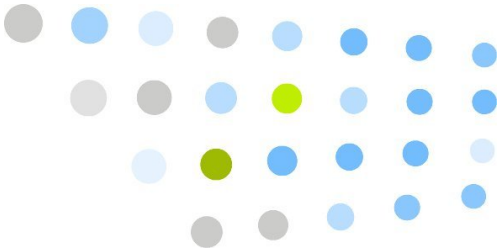
When you are using EAP-FAST authentication, an additional option called **Allow Stateless Session Resume** interacts with fast reconnects. This setting is similar to the **PEAP Session Timeout** setting. Make sure this option is selected, and specify a value for the **Authorization PAC Time to Live (TTL)** property. The **Authorization PAC TTL** value (in minutes or hours) sets the time after which the user authorization PAC expires. When ACS receives an expired authorization PAC, the stateless session cannot resume and phase two EAP-FAST authentication is performed. Therefore, you should set the **Authorization PAC TTL** property to a value that does not trigger a full authentication over the duration of a typical shift.

Other Wireless Security Topics

For additional wireless security information, see the following topics:

- **Configuring EAP-TLS Authentication** in the *Vocera Infrastructure Planning Guide*
- **Configuring EAP-FAST Authentication** in the *Vocera Infrastructure Planning Guide*

- **Configuring Microsoft IAS for WPA-PEAP** in the *Vocera Infrastructure Planning Guide*



Appendixes

The following topics provide reference information for the B3000 badge:

- **Agreements, Specifications, and Notices** on page 91

  This section contains information about third-party software agreements, system specifications, and regulatory notices.

- **Important Safety Instructions** on page 105

  Provides information about badge and battery safety, and information about use in certain areas.

- **IP Port Usage** on page 115

  Lists ports used by the Vocera system for IP communication.

Agreements, Specifications, and Notices

This section contains information about third-party software agreements, system specifications, and regulatory notices.

Third-Party Software Agreements

Certain portions of Vocera's product are derived from software licensed to Vocera by the third parties identified at **http://www.vocera.com/legal** under the heading "Communications." All such portions of Vocera's product are subject to the notices and restrictions specified at **http://www.vocera.com/legal**.

System Specifications for B3000

B3000 badge specifications:

Dimensions	3.9 x 1.4 x 0.7 in. (9.8, 3.6, 1.8 cm)
Weight	1.9 oz. (53.5 g), with battery
LED Indicators	Two indicators: green, amber
Display screen	80 x 82 OLED bit-mapped display Supports 5 lines of text, 9-16 characters per line, up to 150 characters per message (font dependent)
Controls	Call button
	Hold/Do Not Disturb (DND) button
	Volume and Menu Selection buttons

Headset Support *	2.5 mm headset jack * For headset guidelines, go to **www.vocera.com** and log into the Vocera customer portal.

B3000 network specifications:

Network Standard	IEEE 802.11b
	IEEE 802.11g
Frequency Band	2400–2483.5 MHz
Data Rates Supported	1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps
Wireless Medium	Direct Sequence Spread Spectrum (DSSS)
	Orthogonal Frequency Division Multiplexing (OFDM)
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation	DBPSK at 1Mbps
	DQPSK at 2Mbps
	CCK at 5.5 and 11Mbps
	BPSK at 6 and 9Mbps
	QPSK at 12 and 18 Mbps
	16-QAM at 24 and 36 Mbps
	64-QAM at 48 and 54 Mbps
Operating Channels	11 channels (FCC) 13 channels (ETSI)
Roaming	IEEE 802.11b compliant
	IEEE 802.11g compliant

Authentication	PSK PEAP EAP-FAST EAP-TLS LEAP
Encryption	64-bit WEP 128-bit WEP TKIP-WPA AES-CCMP

B3000 electrical specifications:

RF Output Power *	+16 dBm maximum
	* Results based on a controlled test environment. See the *Vocera Infrastructure Planning Guide* for network design guidelines.
RF Receive Sensitivity *	–82 dBm at 11 Mbps
	–65 dBm at 54 Mbps
	* Results based on a controlled test environment. See the *Vocera Infrastructure Planning Guide* for network design guidelines.
Microphone Frequency Range	350 Hz to 3.75 KHz
Microphone Directionality	Quad MEMS Microphone array
Speaker Frequency Range	500 Hz to 3.75 kHz
Peak Speaker Loudness	85 dBSPL at 25 cm
Batteries	
Battery Type	Lithium-ion Polymer
Battery Life	Standard: 3 hours talk time (U-APSD enabled); 45 hours of standby time. Extended: 5 hours of talk time (U-APSD enabled); 60 hours of standby time.

B3000 environmental specifications:

Operating Specifications	
Temperature Range	32° to 104° F (0° to 40° C)
Humidity Range	5% to 95% relative humidity, non-condensing

Storage Specifications	
Temperature Range	–4° to 104° F (–20° to 40° C)
Humidity Range	5% to 95% relative humidity, non-condensing

Drop Specification	1.5 meters onto concrete

B3000 Regulatory Notices

FCC Compliance for United States Users

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio or television reception. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio and television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Caution: Changes or modifications not expressly approved by Vocera could void the FCC compliance and negate your authority to operate the product.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

French Translation

Conformité aux normes FCC Cet équipement a été testé et trouvé conforme aux limites pour un dispositif numérique de classe B, conformément à la Partie 15 des règlements de la FCC. Ces limites sont conçues pour fournir une protection raisonnable contre les interférences nuisibles dans une installation résidentielle. Cet équipement génère, utilise et peut émettre des fréquences radio et, s'il n'est pas installé et utilisé conformément ment aux instructions du fabricant, peut causer des interferences nuisibles aux communications radio. Rien ne garantit cependant que l'interférence ne se produira pas dans une installation particulière. Si cet équipement provoque des interférences nuisibles à la réception radio ou de télévision, qui peut être déterminé en comparant et en l'éteignant, l'utilisateur est encouragé à essayer de corriger les interférence par une ou plusieurs des mesures suivantes:

1. Réorienter ou déplacer l'antenne de réception
2. Augmenter la distance entre l'équipement et le récepteur
3. Branchez l'appareil dans une prise sur un circuit différent de celui auquel le récepteur est connecté
4. Consultez votre revendeur ou un technicien radio / TV pour assistance

Précaution : Les changements ou modifications à cet appareil sans expressément approuvée par la partie responsable de conformité pourraient annuler l'autorité de l'utilisateur de faire fonctionner cet équipement.

Son fonctionnement est soumis aux deux conditions suivantes:

1. Ce dispositif ne peut causer des interférences, et
2. Ce dispositif doit accepter toute interférence, y compris les interférences qui peuvent causer un mauvais fonctionnement du dispositif.

Specific Absorption Rate (SAR) Exposure Guidelines

THIS BADGE MEETS THE FCC REQUIREMENTS FOR EXPOSURE TO RADIO FREQUENCY ENERGY (SAR).

Your wireless badge is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government. These limits are part of a set of comprehensive guidelines

that establish permitted levels of RF energy for the general population. The guidelines are based on standards that were developed by independent scientific organizations through periodic and thorough evaluation of scientific studies. The standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health. The exposure standard for wireless communications devices employs a unit of measurement known as the Specific Absorption Rate, or SAR. The SAR limit set by the FCC is 1.6W/kg. Tests for SAR are conducted using standard operating positions, as applicable to this device, specified by the FCC. The standard incorporates a substantial margin of safety to give additional protection for the public and to account for any variations in measurement. Before a badge is available for sale to the public, sample units must be tested by a certified regulatory lab to verify that they do not exceed the limit established by the government-adopted requirement for safe exposure.

USE ONLY APPROVED ACCESSORIES

RF exposure (SAR) tests have been performed on the Vocera badge when it is being worn correctly and used with the approved accessories. The SAR test results show that the badge complies with all FCC exposure requirements. When a properly-oriented badge is operated with the appropriate accessories, as directed in the *Vocera Badge User Guide*, the level of RF exposure is well below the FCC limit of 1.6W/Kg.

Therefore, to ensure compliance with FCC RF exposure guidelines when wearing the Vocera badge, the user should only use Vocera approved accessories (e.g., lanyard or universal clip). Accessories that have not been tested for RF exposure compliance with this product may not comply with the FCC RF exposure safety guidelines and should not be used.

To ensure RF exposure compliance of the badge when using the lanyard, position and maintain the call button, the speaker, and the antenna facing away from the body, as illustrated in **Getting Started with a B3000 Badge** on page 10. The badge and lanyard attachment have been designed specifically to maintain proper orientation during normal usage. Additionally, the lanyard clip can be secured to clothing to provide additional stability. Wearing the Vocera badge with the antenna facing the body may result in non-compliance with FCC RF exposure guidelines and must be avoided.

Use only the internal antenna which is part of this product. Any use of unauthorized antennas, any modifications to the supplied antenna, or any use of unauthorized attachments could damage the badge, violate FCC regulations, and void the user's authority to operate the product.

European Union Declaration of Conformity (DoC)

Standards:

B3000 Version CE ⓘ
EN 300-328
EN 301-489-1
EN 301-489-17
EN 60950-1
EN 50383
2011/65/EU

Responsible Party:

Responsible Party contact information is available at **www.vocera.com/legal/regulatory.aspx**.

CE Mark Restrictions:

- United Kingdom: System provider for third-party traffic may require a Wireless Telegraphy and/or Telecommunications Act License.
- France: French regulations require that you do not use this device outdoors.

English

Hereby, Vocera, Inc. declares that all CE Marked Vocera products incorporating Radio and Telecoms Terminal Equipment functionality are in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Français

Par la présente, Vocera, Inc. déclare que tous les produits Vocera incorporant la fonctionnalité d'Équipement terminal Radio et télécommunications et marqués du symbôle CE sont conformes aux exigences essentielles et autres dispositions pertinentes de la Directive 1999/5/EC.

Български

С настоящата, Vovera, Inc. декларира, че всички изделия на Vocera, маркирани със знака CE, включващи функционалност за терминално оборудване за радио и телекомуникации, съответстват на основните изисквания и на други съответни условия на Директива 1999/5/EC.

Ceština

Společnost Vocera, Inc. tímto prohlašuje, že všechny produkty společnosti Dell se značkou CE, které obsahují rádiová zařízení a telekomunikační koncová zařízení, vyhovují základním požadavkům i ostatním příslušným předpisům směrnice 1999/5/EC.

Dansk

Vocera, Inc. erklærer hermed, at alle CE-mærkede Vocera-produkter, som har indbygget tilslutningsfunktionalitet til radio- og telekommunikation, overholder de obligatoriske krav og andre relevante forudsætninger i Direktiv 1999/5/EU.

Nederlands

Vocera, Inc. verklaart bij deze dat alle Vocera-producten die van een CE-markering zijn voorzien en waar functionaliteit voor radio- en telecommunicatie-terminalapparatuur is ingebouwd, voldoet aan de essentiële vereisten en andere relevante bepalingen van Richtlijn 1999/5/EC.

Eesti keel

Käesolevaga teatab Vocera, Inc, et kõik CE-tähistusega tooted, mis hõlmavad raadio- ja telekommunikatsioonikeskuse seadmete funktsioone, vastavad direktiivi 1999/5/EÜ põhinõuetele ja teistele asjaomastele sätetele.

Suomi

Täten Vocera, Inc. ilmoittaa, että kaikki CE-merkityt radio- ja telealan laitteistojen toiminnallisuuksia sisältävät Vocera-tuotteet ovat direktiivin 1999/5/EY välttämättömien vaatimusten ja muiden relevanttien säännösten mukaisia.

Deutsch

Hiermit versichert Vocera, Inc., dass alle mit einem CE-Zeichen versehenen Vocera-Produkte, die Funktionalität von Radio und Telecoms Terminal-Geräten einbeziehen, die notwendigen Voraussetzungen und andere wichtige Bereitstellungen der Richtlinien 1999/5/EC erfüllen.

Ελληνικά

Δια του παρόντος η Vocera, Inc. δηλώνει ότι όλα τα προϊόντα της Vocera με τη σήμανση CE συμπερ. ραδιοεξοπλισμού και τηλεπικοινωνιακού τερματικού εξοπλισμού συμμορφώνεται με τις απαραίτητες απαιτήσεις και τις λοιπές σχετικές διατάξεις της Οδηγίας 1999/5/ΕΚ.

Magyar

Ezennel a Vocera, Inc. kijelenti, hogy az összes rádió és telekommunikációs egységeket tartalmazó CE jelzésű Vocera termék megfelel az 1999/5/EC szabvány és más vonatkozó előírás követelményeinek.

Português

Por meio deste, a Vocera, Inc. declara que todos os produtos Vocera com a marca CE que incorporar a funcionalidade de equipamentos terminais de rádio e telecomunicações cumprem os requisitos essenciais e outras provisões relevantes da directiva 1999/5/EC.

Italiano

Con la presente, Vocera, Inc. dichiara che tutti i prodotti Vocera con marchio CE che incorporano la funzionalità delle apparecchiature radio e delle apparecchiature terminali di telecomunicazione (R&TTE, Radio and Telecoms Terminal Equipment), sono conformi ai requisiti essenziali e ad altre importanti disposizioni della Direttiva 1999/5/CE.

Latviešu Valoda

Ar šo Vocera, Inc. apliecina, ka visi Vocera produkti, kam ir CE marķējums, ieskaitot radio iekārtu un telekomunikāciju gala iekārtu darbību, atbilst direktīvas 1999/5/EC pamatprasībām un citiem ar to saistītiem nosacījumiem.

Lietuvių kalba

„Vocera, Inc.“ pareiđkia, kad visi „CE“ paţymëti „Vocera“ produktai su „Radio and Telecoms Terminal Equipment“ funkcijomis atitinka svarbiausius ir kitus susijusius 1999/5/EC direktyvos reikalavimus.

Malti

Hawnhekk, Vocera, Inc. tiddikjara li l-prodotti kollha Vocera Immarkati b'CE li jinkorporaw il-funzjonalità tat-Tagħmir Terminali tar-Radju u tat-Telekomunikazzjonijiet, huma konformi mal-ħtiġijiet essenzjali u provvedimenti rilevanti oħrajn ta' Direttiva 1999/5/KE.

Polski

Niniejszym Vocera Inc. oświadcza, że wszystkie produkty oznaczone znakiem CE, zawierające radiowe i telekomunikacyjne urządzenia końcowe są zgodne z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.

Română

Vocera, Inc. declară, prin prezenta, că toate produsele Vocera marcate CE, care au integrată funcționalitatea de echipament terminal radio şi de telecomunicații sunt conforme cu cerințele principale şi cu alte dispoziții relevante ale directivei 1999/5/CE.

Slovenčina

Spol. Vocera, Inc. týmto vyhlasuje, že všetky produkty Vocera so značkou CE, ktoré obsahujú funkčnosť rádiových a telekomunikačných koncových zariadení, sú v súlade s hlavnými požiadavkami a inými príslušnými ustanoveniami smernice 1999/5/ES.

Slovenščina

S tem družba Vocera, Inc. izjavlja, da so vsi izdelki Vocera z oznako CE, ki vsebujejo funkcionalnost radijske in telekomunikacijske terminalne opreme, v skladu z bistvenimi zahtevami in drugimi primernimi odločbami direktive 1999/5/EC.

Español

Por la presente, Vocera, Inc. declara que todos los productos Vocera con la marca CE que incluyen la funcionalidad Equipos radioeléctricos y equipos terminales de telecomunicación cumplen con los requisitos esenciales y otras provisiones relevantes de la Directiva 1999/5/CE.

Svenska

Härmed försäkrar Vocera, Inc. att alla CE-märkta produkter från Vocera som innehåller radio- och teleterminalsfunktionalitet är i överensstämmelse med erforderliga föreskrifter och andra relevanta bestämmelser i direktiv 1999/5/EC.

Türkçe

Sonuç olarak, Vocera, Inc., CE ile Damgalı Vocera ürünlerin bünyesine dahil edilen Radyo ve Telekomların Terminal Araç fonksiyonelliklerin, 1999/5/EC direktiflerinin esas koşulları ve hükümlerine uygun olduğunu beyan eder.

Notice to Canada Users

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the radio interference regulations of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de Classe B prescrites dans le règlement sur le brouillage radioélectrique édicté par Industrie Canada.

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment.

Cet équipement est conforme à l'exposition aux rayonnements IC RSS-102 des limitesdéfinies pour un environnement non contrôlé.

Notice: The Industry Canada regulations provide that changes or modifications not expressly approved by Vocera, Inc. could void your authority to operate this equipment.

Avis: Dans le cadre des réglementations d'Industry Canada, vos droits d'utilisation de cet équipement peuvent être annulés si des changements ou modifications non expressément approuvés par Dell Inc. y sont apportés.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Canada Safety Code 6 Guidelines for Exposure to Radio Waves

THIS DEVICE MEETS HEALTH CANADA SAFETY CODE 6 GUIDELINES FOR EXPOSURE TO RADIO WAVES.

CET APPAREIL EST CONFORME AUX DIRECTIVES DU CODE 6 DE SÉCURITÉ DE LA SANTÉ CANADA POUR L'EXPOSITION AUX ONDES RADIO.

Your B3000 device is a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) recommended by international guidelines. The guidelines were developed by Health Canada and include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

Votre appareil B3000 est un émetteur-récepteur radio. Il est conçu pour ne pas dépasser les limites d'exposition aux ondes radio (champs électromagnétiques de fréquence radio) recommandées par les directives internationales. Les lignes directrices ont été élaborées par Santé Canada et comprennent une marge de sécurité importante destinée à assurer la sécurité de toutes les personnes, indépendamment de l'âge et de la santé.

The radio wave exposure guidelines use a unit of measurement known as the Specific Absorption Rate, or SAR. The SAR limit for radio devices is 1.6W/kg.

Les lignes directrices pour l'exposition aux ondes radio utilisent une unité de mesure appelée Débit d'Absorption Spécifique, ou DAS. La limite DAS pour les appareils radio est 1,6W/kg.

Tests for SAR are conducted using standard operating positions with the device transmitting at its highest certified power level in all tested frequency bands.

Les tests de DAS sont effectués en utilisant des positions standards de fonctionnement quand l'appareil fonctionne à son niveau de puissance maximum certifié dans toutes les bandes de fréquences testées.

During use, the actual SAR value for this device may be well below the value stated above. In general, the lower the power output by the device, the lower its SAR value.

En cours d'utilisation, la valeur de DAS réel de ce dispositif peut être bien inférieur à la valeur indiquée cidessus. En général, plus la puissance de sortie par le dispositif, plus sa valeur DAS.

The World Health Organization has stated that present scientific information does not indicate the need for any special precautions for the use of mobile devices. They recommend that if you are interested in further reducing your exposure then you can easily do so by limiting your usage or simply using a handsfree kit to keep the device away from the head and body.

L'Organisation mondiale de la Santé (OMS) a déclaré que l'information scientifique actuelle n'indique pas la nécessité de prendre des précautions particulières pour l'utilisation de dispositifs radio. Ils recommandent que si vous êtes intéressé à réduire encore davantage votre exposition, vous pouvez facilement le faire en limitant votre consommation ou tout simplement en utilisant un kit mains-libres pour maintenir le dispositif éloigné de la tête et du corps.

IC RSS-Gen, Sec. 7.1.3

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Notice to Australia and New Zealand Users

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to the Australian/New Zealand standard AS/NZS CISPR22: 2009 (Class B) set out by the Australian Communications and Media Authority and Radio Spectrum Management Agency.

New Zealand telecommunication statement (for products fitted with Telepermit approved modems):

The grant of a Telepermit for any item of terminal equipment indicates only that Telecom has accepted that the item complies with minimum conditions for connection to its network. It indicates no endorsement of the product by Telecom, nor does it provide any sort of warranty. Above all, it provides no assurance that any item will work correctly in all respects with another item of Telepermitted equipment of a different make or model, nor does it imply that any product is compatible with all of Telecom's network services.

This equipment shall not be set up to make automatic calls to the Telecom `111' Emergency Service.

Important: Under power failure conditions, this telephone may not operate. Make sure that a separate telephone, not dependent on local power, is available for emergency use.

Some parameters required for compliance with Telecom's Telepermit requirements are dependent on the equipment (PC) associated with this device. The associated equipment shall be set to operate within the following limits for compliance with Telecom's specifications:

a. There shall be no more than 10 calls to the same number within any 30-minute period for any single manual call initiation, and

b. The equipment shall go on-hook for a period of not less than 30 seconds between the end of one attempt and the beginning of the next attempt.

The equipment shall be set to make sure that automatic calls to different numbers are spaced such that there is no less than 5 seconds between the end of one call attempt and the beginning of another.

The equipment shall be set to make sure that calls are answered between 3 and 30 seconds of receipt of ringing.

Notice to Singapore Users

Complies with
IDA Standards
DA101094

Notice to Brazil Users

Important Safety Instructions

The Vocera badge (including its battery component) and the Vocera battery charger are electronic devices. Care appropriate to the use of any electronic device must be taken in using the badge and the battery charger in order to minimize the possibility of injury (e.g., from shock) and damage (e.g., from fire).

In addition, the Vocera badge is a wireless communication device that works by generating radio frequency (RF) signals. These signals, although generally lower in strength than a typical cellular telephone, can interfere with other electronic devices that are not appropriately shielded against RF signals. If the Vocera badge will be used in proximity to sensitive electronic devices for which interference could result in serious consequences, you must consult with the manufacturer of any such device in order to determine whether the Vocera badge can be safely operated in proximity to such device.

In order to ensure comfortable use of the badge and to avoid possible damage to hearing, do not bring the speaker within close proximity of the ear while the badge is powered on.

References below to the "badge" refer to the Vocera badge, including its battery component, while references to the "product" refer to the badge and the Vocera battery charger.

In addition to other basic safety precautions appropriate to the use of wireless electronic devices, please follow the safety and use instructions set forth below.

Warning Definition

Warning: This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Waarschuwing: Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.

Varoitus: Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.

Attention: Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents.

Warnung: Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt.

Avvertenza: Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.

Advarsel: Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.

Aviso: Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.

¡Advertencia! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.

Varning! Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.

Badge and Battery Charger Safety

1. PLEASE BE CERTAIN TO READ, UNDERSTAND, AND FOLLOW ALL WARNINGS AND INSTRUCTIONS IN THE PRODUCT DOCUMENTATION AND ON THE PRODUCT ITSELF.
2. A damaged battery may pose a risk of personal injury. Damage may include impact or shock that dents or punctures the battery, exposure to a flame, or other deformation. Do not disassemble the battery. Handle a damaged or leaking battery pack with extreme care. If the battery is damaged, electrolyte may leak from the cells or fire may result which may cause personal injury.

   Une batterie endommagée peut présenter un risque de blessures corporelles. Les dégâts peuvent résulter d'impacts ou de chocs provoquant des bosses ou des perforations de la batterie, de l'exposition au feu ou d'autres déformations. Ne démontez pas la batterie. Manipulez les batteries endommagées ou percées avec d'extrêmes précautions. Si une batterie est endommagée, de l'électrolyte peut s'échapper des cellules ou la batterie peut prendre feu, ce qui risque de provoquer des blessures corporelles.
3. Keep the battery away from children.

   Conservez la batterie hors de portée des enfants.
4. Do not expose (store or place) your badge or battery pack to a heat source such as a radiator, fireplace, stove, electric heater, or other heat-generating appliance or otherwise expose it to temperatures in excess of 65°C (149°F). When heated to excessive temperatures, battery cells could vent or explode, posing risk of fire.

N'exposez pas (ni ne rangez ou laissez) votre ordinateur ou batterie près d'une source de chaleur, telle qu'un radiateur, une cheminée, un poêle, un chauffage électrique ou tout autre appareil générateur de chaleur et ne l'exposez pas à des températures supérieures à 65 °C (149 °F). Lorsque les batteries atteignent une temperature excessive, les cellules de la batterie peuvent imploser ou exploser, représentant alors un risque d'incendie.

5. Do not carry a battery pack in your pocket, purse, or other container where metal objects (such as keys) could short-circuit the battery terminals. The resulting excessive current flow can lead to extremely high temperatures and may cause damage to the battery pack or surrounding materials, or personal injury, such as burns.

   Ne transportez pas de batterie dans votre poche, sac à main ou autre conteneur où des objets métalliques (comme des clés) pourraient court-circuiter les bornes de la batterie. L'excès de courant qui en résulterait pourrait entraîner des températures extrêmement élevées et endommager la batterie, ou les matériels à proximité, ou provoquer des blessures comme des brûlures.

6. Do not put anything other than a Vocera badge or Vocera battery into a Vocera charger slot, as other objects may touch dangerous voltage points or may short out parts, both of which conditions could result in fire or electric shock.

   Important: The B3000 badge cannot be placed into the charger.

7. Do not place the product on an unstable surface, as the product may fall and suffer serious damage.
8. Do not operate the charger in a cabinet or other enclosure unless proper ventilation is provided.
9. Do not position the badge or battery charger near any source of water such as a sink, wash bowl, or toilet. Do not spill liquid of any kind on the product, as doing so may short out parts, causing damage to the product and creating the risk of fire or electric shock.
10. Take the badge or charger to a qualified service provider in these circumstances:
    - If liquid has been spilled onto the badge or charger, or if rain or water has touched the badge or charger.
    - If the badge or charger does not operate normally after you follow the operating instructions.
    - If the badge or charger has been dropped or damaged.

- If the badge or charger exhibits a distinct degradation in performance.
- If the power cord or plug on the charger is damaged or frayed.

11. Unplug the charger from the wall outlet before cleaning. To clean or disinfect the badge and charger, wipe with a cloth dampened with germicidal solution or isopropyl alcohol. Use of any other cleaners may damage the badge and void your warranty.
12. Use the battery charger indoors only.
13. Do not allow anything to rest on the charger's power cord. Do not locate the charger where the cord may be damaged or where the cord may cause someone to trip. Keep the power cord away from operating machinery.
14. Do not overload outlets or extension cords, because this may cause a fire or electrical shock.
15. Operate the charger only with a Vocera-approved power adapter.

    Utilisez le chargeur seulement avec un adaptateur de puissance approuvé par Vocera.
16. Use only the batteries supplied with the product or Vocera-approved replacements.
17. Do not use the battery to power any device other than the Vocera badge it is designed for.
18. Charge the battery only in its Vocera charger and according to the instructions in the *Vocera Badge User Guide*. These instructions are also included with the charger.
19. In limited circumstances, the badge may power off without any prior low battery warning or indication.
20. Do not charge the battery in a place where static electricity is generated or let the battery touch any object that is statically charged.
21. The battery can be stored at temperatures between –4° F and 104° F (between –20° C and 40° C), and can be charged or operated at temperatures between 32° F and 104° F (between 0° C and 40° C).
22. Do not put the battery into a microwave oven, conventional oven, dryer, or high-pressure container, or dispose of the battery in a fire. If you do so, the battery might explode.
23. Do not open or puncture the battery or subject the battery to strong physical shock.
24. Stop using the battery if it exhibits abnormal heat, odor, color, deformation, or is in an abnormal condition.

25. If you detect leakage or a foul odor, it is especially important to keep the battery away from fire. If battery liquid leaks onto your skin or clothes, immediately wash well with clean water. If liquid leaking from the battery gets into your eyes, do not rub your eyes. Instead, immediately rinse your eyes well with clean water, and consult a doctor.
26. If the contact points on a B3000 battery or a B3000 badge are damaged, the badge screen may display the following error: "Battery Communication Error." If this happens, do the following to determine whether the battery or badge is damaged:
    - Try using the battery in question on other badges that are working properly. If the "Battery Communication Error" message always appears on other badges, the battery is damaged and must be replaced.
    - Try using the badge in question with other batteries that are working properly. If the "Battery Communication Error" message always appears, the badge is damaged and must be replaced.
27. Handle batteries with care to avoid shorting the battery with conducting materials, such as rings, bracelets, and keys. If the battery shorts, it may overheat and burn you.
28. **Battery Disposal:** Dispose of used batteries properly. After Vocera batteries have reached the end of their useful life, we recommend recycling them at a recycling center in your community or by sending them to Vocera (or a designated Vocera partner for your locale) for an earth-friendly disposal. For Vocera recycling policy and instructions, search for "recycling" in Vocera Technical Support Portal Content. If you choose to dispose of batteries yourself, consult the regulations that are in force in your locale.
29. When recycling or discarding the battery, make it non-conductive by applying vinyl tape to the terminals. On B3000 batteries, apply tape to the top edge.

FAILURE TO FOLLOW THE FOREGOING INSTRUCTIONS COULD RESULT IN (A) DAMAGE TO EQUIPMENT, VOIDING YOUR WARRANTY AND/OR (B) PROPERTY DAMAGE AND/OR SERIOUS PERSONAL INJURY, INCLUDING DEATH.

ATTENTION: SI LES INSTRUCTIONS CI-DESSOUS NE SONT PAS SUIVIES, VOUS VOUS EXPOSEZ AUX RISQUES SUIVANTS: A) DOMMAGE À L'ÉQUIPEMENT, ANNULANT VOTRE GUARANTIE, B) DOMMAGES À LA PROPRIÉTÉ ET/OU RISQUES DE BLESSURES SÉRIEUSES, INCLUANT PERTE DE VIE.

Important Information About Use in Certain Areas

1. Turn your badge OFF in facilities when any posted notices instruct you to turn off all devices that emit a radio frequency. To turn the badge OFF, depress the Hold/DND button for 5 seconds or remove the battery. If the rules of your facility limit use of RF-emitting devices in certain areas, you must familiarize yourself with these rules and follow them strictly.
2. If you have any reason to suspect that the badge is interfering with sensitive equipment, turn the badge OFF immediately.
3. Turn your badge OFF and do not use the charger when you are in any area with potentially explosive materials in the atmosphere. Sparks in such areas could cause an explosion or fire, resulting in bodily injury or death. Areas with potentially explosive atmospheres include: fueling areas; transfer or storage facilities for fuel or chemicals; facilities with equipment using liquefied petroleum gas, such as propane or butane; and areas where the air contains chemicals or particles, such as grain, dust, or metal powders.

FAILURE TO FOLLOW THE FOREGOING INSTRUCTIONS COULD RESULT IN (A) DAMAGE TO EQUIPMENT, VOIDING YOUR WARRANTY AND/OR (B) PROPERTY DAMAGE AND/OR SERIOUS PERSONAL INJURY, INCLUDING DEATH.

ATTENTION: SI LES INSTRUCTIONS CI-DESSOUS NE SONT PAS SUIVIES, VOUS VOUS EXPOSEZ AUX RISQUES SUIVANTS: A) DOMMAGE À L'ÉQUIPEMENT, ANNULANT VOTRE GUARANTIE, B) DOMMAGES À LA PROPRIÉTÉ ET/OU RISQUES DE BLESSURES SÉRIEUSES, INCLUANT PERTE DE VIE.

Additional Instructions for B3000 Battery Safety

CAUTION: Using an incompatible battery may increase the risk of fire or explosion. Replace the battery only with a compatible battery purchased from Vocera that is designed to work with your B3000. Do not use a battery from other devices with your B3000. Dispose of used batteries properly. See Battery Disposal in this document.

PRÉCAUTION : L'utilisation d'une batterie non compatible peut accroître le risque d'incendie ou d'explosion. Remplacez la batterie uniquement par une batterie compatible achetée auprès de Vocera, conçue pour fonctionner avec votre Vocera B3000. N'utilisez pas de batterie provenant d'un autre périphériques. Évacuez les batteries usagées conformément à la réglementation. Reportez-vous à la section Mise au rebut de la batterie de ce document.

Product Disposal Warning

Warning: Ultimate disposal of this product should be handled according to all national laws and regulations.

Waarschuwing: Dit produkt dient volgens alle landelijke wetten en voorschriften te worden afgedankt.

Varoitus: Tämän tuotteen lopullisesta hävittämisestä tulee huolehtia kaikkia valtakunnallisia lakeja ja säännöksiä noudattaen.

Attention: La mise au rebut définitive de ce produit doit être effectuée conformément à toutes les lois et réglementations en vigueur.

Warnung: Dieses Produkt muß den geltenden Gesetzen und Vorschriften entsprechend entsorgt werden.

Avvertenza: L'eliminazione finale di questo prodotto deve essere eseguita osservando le normative italiane vigenti in materia.

Advarsel: Endelig disponering av dette produktet må skje i henhold til nasjonale lover og forskrifter.

Aviso: A descartagem final deste produto deverá ser efectuada de acordo com os regulamentos e a legislação nacional.

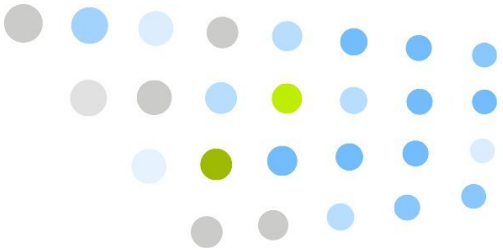
Advertencia: El desecho final de este producto debe realizarse según todas las leyes y regulaciones nacionales.

Varning: Slutlig kassering av denna produkt bör skötas i enlighet med landets alla lagar och föreskrifter.

National Safety Statement of Compliance – CE Marking

EN 60950 Statement:

This is to certify that the Vocera B3000 chassis and components installed within the chassis are in compliance with the requirements of EN 60950 in accordance with the Low Voltage Directive. Additional national differences for all European Union countries have been evaluated for compliance. Some components installed within the Vocera B3000 chassis may use a nickel-metal hydride (NiMH) and/or lithium-ion battery. The NiMH and lithium-ion batteries are long-life batteries, and it is very possible that you will never need to replace them. However, should you need to replace them, refer to the individual component manual for directions on replacement and disposal of the battery.



IP Port Usage

The following tables indicate the ports used by Vocera system components for IP communication:

Table 14. Badge IP port usage

Description	Protocol	Port No
Badge ↔ Server Signaling	UDP	5002
Vocera Server -> Badge Audio Telephony Server -> Badge Audio Vocera SIP Telephony Gateway -> Badge Audio Badge -> Badge Audio	UDP	5200
Badge ↔ Updater Signaling	UDP	5400
Badge ↔ Vconfig (Vch) Signaling during Discovery	UDP	5555 and 5556
Badge ↔ Vconfig (Vch) Signaling during Connection	TCP	5555 and 5556

Opening Ports for Communication

If a firewall separates Vocera servers from the wireless network, make sure the following ports are open for communication:

Table 15. WLAN Ports Used by Vocera Clients

Client	Direction	Server / Client	Type	Protocol	Ports
Badge	Inbound/ Outbound	VS	Signaling	UDP	5002
Badge	Inbound	VS	Audio	UDP / TCP	5100-5199 [a]

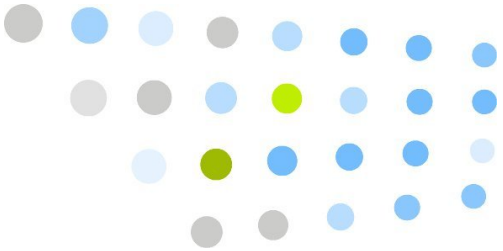
Client	Direction	Server / Client	Type	Protocol	Ports
Badge	Inbound/ Outbound	Badge/VS/VTS	Audio	UDP	5200
Badge	Inbound	VTS	Audio	UDP	5300-5399
Badge	Inbound/ Outbound	Updater	Signaling	UDP	5400
Badge	Inbound/ Outbound	VS	Discovery	UDP	5555 & 5556
Badge	Inbound/ Outbound	VS	Connection	TCP	5555 & 5556 [b]
Badge	Inbound	VCG	Audio	UDP	6300-6555 [c]
Smartphone	Inbound/ Outbound	VCG	Signaling	UDP	5060
Smartphone	Outbound	VCG	Audio	UDP	50000-50255
Smartphone	Inbound/ Outbound	FTP Server	MSP / FTP	TCP	20 & 21
Smartphone	Inbound/ Outbound	FTP Server	MSP / FTP	UDP	> 1023
Smartphone, Vocera Connect for Android and iPhone	Inbound	VCG	Audio	UDP	7700-8467
Smartphone, Vocera Connect for Android and iPhone	Inbound	VS	Signaling	TCP	80 or 443 (for SSL)
Vocera Connect for Android and iPhone	Inbound/ Outbound	VCG	Signaling	UDP	5060, 5888-5889
Vocera Connect for Android	Inbound/ Outbound	Vocera Devices	Audio	UDP	32768-65536
VMI Clients	Inbound/ Outbound	VS	Connection	TCP	5005

Client	Direction	Server / Client	Type	Protocol	Ports
VAI Clients (includes Staff Assignment)	Inbound/ Outbound	VS	Connection	TCP	5251
Vocera Devices (Dictation client)	Inbound	VS	Audio	UDP	8200
VS (Vocera Connect for Cisco)	Outbound	Cisco UCM	Signaling	TCP	2748

[a] This TCP range must be opened if TCP-to-Genie is enabled on the Vocera Server.

[b] Make sure you allow packets from TCP port 5556 to be received on any available port on the Vocera Server.

[c] The base port for this range is configurable.



Index

Symbols

2.4 GHz Channels: Set to Defaults (1, 6, 11) property, 67
2.4 GHz Channels: Specify Channels property, 67
802.11d property, 68
802.11g support, 77
802.11n support, 77

A

access point
    relationship to locations, 22
authentication
    optimizations, 86
    servers supported, 84
Authentication property, 59
Auto-PAC Provision Retry Count property, 63

B

badge
    configuring, 41, 43
Badge Configuration Utility, 41, 71
badge operation
    adjusting the volume, 25
    battery disposal, 110
    cleaning, 32
    safety recommendations, 95
Badge Properties Editor, 53
    General properties, 55
    Setting Security properties, 57
    starting, 54
badge.properties file, 54
battery
    disposal, 110
    removing from the badge, 31

replacing, 32
safety information, 110
battery charger, 31
beacon interval
required value, 78

C

CCKM property, 68
Cisco Certified Key Management, 68
cleaning accessories, 32
cleaning the badge, 32
Client Key Password property, 62
CQ value
Roaming Policy and, 81

D

data rates
required settings, 78
device management, 35
DTIM interval
required value, 78

E

EAP-TLS authentication, 65
Enable Auto-PAC property, 63
Enable FIPS Mode property, 64
Enable FIPS property, 58
Encryption Key property, 62

F

fast reconnect, 86
Federal Information Processing Standards (FIPS), 58, 64
firewall, opening ports, 115
font size, 24

G

group mode, 27

H

handset mode, 18, 23, 26
headset
volume adjustment, 25
Hide Boot Menus property, 56

I

indicators, battery charger, 31

L

labeling devices, 36

M

messages
    font size, 24

P

Password property, 61
PEAP session timeout, 87
peer-to-peer communication
    required setting, 78
PreShared Key property, 62
properties
    security, 79
    SSID, 79
Provision Auto-PAC on Expire property, 63

R

reporting, device management, 37
Reset Volume to Default property, 57
Roaming Policy property, 68

S

safety recommendations, 105
    battery disposal, 110
    SAR exposure, 95
SAR exposure guidelines, 95
screen, flipping, 28
security
    authentication servers supported, 84
    badge properties, 79
    optimizations, 86
    required settings, 78
    required settings discussed, 79
    standards supported, 83
Security properties
    setting, 57, 57
session timeout, 86
SNR
    CQ value and, 79
SNR value
    Roaming Policy and, 81
sound level, 25
speaker volume adjustment, 25

speech recognition
    proper badge position for, 11
speech zone, 17
SSID
    badge property, 79
    discussed, 79
    required setting, 78
SSID property, 56

T

timeout interval, 86

U

User Name property, 61

V

Vocera Server IP Address property, 56
volume adjustment, 25

W

WEP encryption, 65
WEP keys, 65