

Vocera Device Configuration Guide

Version 5.3.0



Notice

Copyright © 2002-2021 Vocera Communications, Inc. All rights reserved.

Vocera® is a registered trademark of Vocera Communications, Inc.

This software is licensed, not sold, by Vocera Communications, Inc. ("Vocera"). The reference text of the license governing this software can be found at <https://www.vocera.com/legal/>. The version legally binding on you (which includes limitations of warranty, limitations of remedy and liability, and other provisions) is as agreed between Vocera and the reseller from whom your system was acquired and is available from that reseller.

Certain portions of Vocera's product are derived from software licensed by the third parties as described at <https://www.vocera.com/legal/>.

Microsoft®, Windows®, Windows Server®, Internet Explorer®, Excel®, and Active Directory® are registered trademarks of Microsoft Corporation in the United States and other countries.

Java® is a registered trademark of Oracle Corporation and/or its affiliates.

All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owner/s. All other brands and/or product names are the trademarks (or registered trademarks) and property of their respective owner/s.

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

Last modified: 2021-06-16 12:42

VS-530-Docs build 560



Contents

Introduction.....	5
About This Guide.....	5
Product Applicability.....	5
Configuration Hardware Requirements.....	5
Related Documentation.....	5
Badge Configuration Workflow.....	6
Setting Up the Configuration Computer.....	7
Installing Badge Configuration Utilities.....	7
Badge Configuration Files Overview.....	10
Property and Profile Files for the Badge.....	11
Specifying TCP/IP Settings.....	11
Setting up Isolated Access Point.....	12
Configuring a New Badge.....	13
Using the Badge Properties Editor.....	13
B2000 Badge Properties Configuration.....	14
B3000 Badge Properties Configuration.....	16
B3000N Badge Properties Configuration.....	21
Configuring a Test Badge.....	26
Assigning Static IP Addresses.....	26
Configuring the Remaining Badges.....	28
Using the Badge Configuration Utility.....	28
Running the Badge Configuration Utility.....	28
Maintaining Properties and Firmware.....	30
About Property and Firmware Maintenance.....	30
Updating Properties and Firmware.....	30
Using the Badge Background Updater.....	31
Background Updater and Vocera Clusters.....	31
Background Update Status.....	31
Using a Badge While a Background Update Is in Progress.....	32
Interrupting a Background Update.....	32
Troubleshooting Badge Configuration.....	33
Troubleshooting the Initial Badge Configuration.....	33
Troubleshooting the Badge Property Settings.....	34
Using the Badge Configuration Menu.....	34
Displaying the Badge Configuration Menu.....	34

Displaying the Badge Configuration Menu (Older Software).....	34
Navigating in the Badge Configuration Menu.....	35
Collecting Badge Data for Troubleshooting.....	36
Running the Quick Test.....	36
Repairing the File System.....	37
Restoring Factory Default Settings.....	38
Restoring a Badge to its Factory Image.....	38
Restoring the B3000n/B3000 Factory Image.....	38
Restoring the B2000 Factory Image.....	39

Introduction

This section introduces you to the details covered in this document, the product applicability, and the related documentation.

About This Guide

This document describes how to set up a Vocera Voice Server configuration computer, configure and update the firmware on badges using the Badge Properties Editor and Badge Configuration Utility.

Use the following information relevant to you:

- If you are on the Vocera Voice Server, use the Badge Properties Editor section in this document.
- If you are using the standalone configuration computer, use the Badge Configuration Utility section in this document.

This document does not provide information about the infrastructure planning details you need to set to support your network environment, or details on specific badge features, and commands. For a complete description of these topics, refer to Vocera B-Series Badge Guide and Vocera Infrastructure Planning Guide.

Product Applicability

This section describes the applicable products, the supported firmware releases, and the supported Vocera Software.

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

Configuration Hardware Requirements

Vocera requires specific hardware to set up the badges and the phones.

The following table provides details of the hardware required:

Component	Requirement
Configuration Computer	A dedicated computer that runs the Vocera Badge Configuration Utility (BCU). For more information, refer to Vocera Voice Server Sizing Matrix .
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.

Related Documentation

The documents supporting the Vocera Badge Configuration Guide is listed in this topic.

The following documents support the Vocera Badge Configuration Guide:

- *Vocera Infrastructure Planning Guide*—Specifies the recommended configuration of infrastructure to support Vocera. You can also refer to all the security information in the Vocera Infrastructure Planning Guide.
- *Vocera Badge User Guide*—Specifies the badge features and commands.



Badge Configuration Workflow

This section provides a workflow to configure badges.

To set up badges in your network, you must perform the following tasks:

1. **Setting Up the Configuration Computer**—In this step you set up a configuration computer, specify the TCP/IP properties and connect it to an access point. For more information, refer to [Setting Up the Configuration Computer](#) on page 7.
 - a. **Installing the Badge Configuration Utilities**—Install the Badge Configuration Utility that allows you to specify the settings and automatically generate a `properties.txt` file. You can then download the text file to your badges. For more information, refer to [Installing Badge Configuration Utilities](#) on page 7.
 - b. **Specifying TCP/IP Properties**—Specify TCP/IP properties in the configuration computer to allow a new badge to connect to it. For more information, refer to [Specifying TCP/IP Settings](#) on page 11.
 - c. **Setting Up an Isolated Access Point**—Connect the configuration computer directly to an access point that is set up without security parameters. For more information, refer to [Setting up Isolated Access Point](#) on page 12.
2. **Configuring a New Badge**—After you set up the configuration computer, you must specify properties for your badge before it can communicate with your network. You can then configure a test badge.
 - a. **Creating a Property File**—Use the Badge Properties Editor (BPE) to create a file specifying the property values your site requires. For more information, refer to [Using the Badge Properties Editor](#) on page 13.
 - b. **Configuring a Test Badge**—Set up a single test badge to confirm that it connects to the network the way you intended. For more information, refer to [Configuring a Test Badge](#) on page 26.
3. **Configuring the Remaining Badges**—After you have successfully configured and tested one badge, configure the remaining badges for your site using the Badge Configuration Utility (BCU).
 - a. **Using the BCU**—Use the BCU to download properties and firmware settings from the configuration computer to the rest of the badges. For more information, refer to [Using the Badge Configuration Utility](#) on page 28.

Setting Up the Configuration Computer

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

A badge has no keyboard, and cannot be configured directly. You must configure it from a computer that is referred to as a **configuration computer**. The configuration computer runs the Vocera Badge Configuration Utility (BCU) and is also called as the BCU computer.

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



Note: The configuration computer must be a standalone computer that is not connected to the network of your site.



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

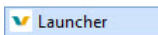
Installing Badge Configuration Utilities

The Badge Utilities let you specify badge properties using the web UI. You can then download the properties to your badges.

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

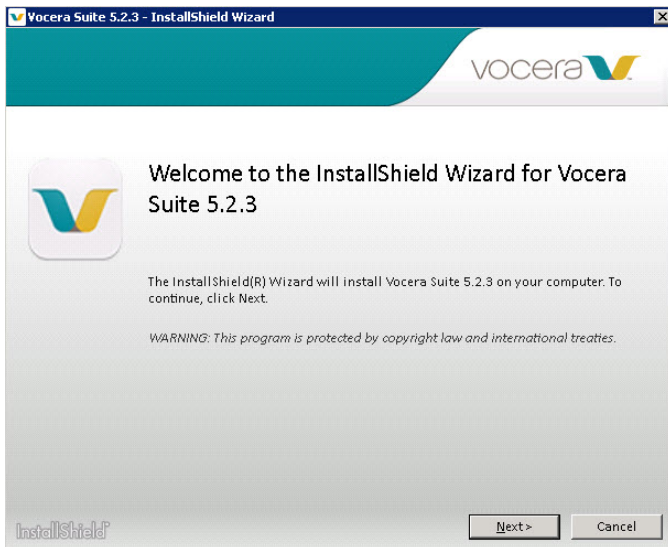
To install the Badge Configuration Utilities, perform the following steps:

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



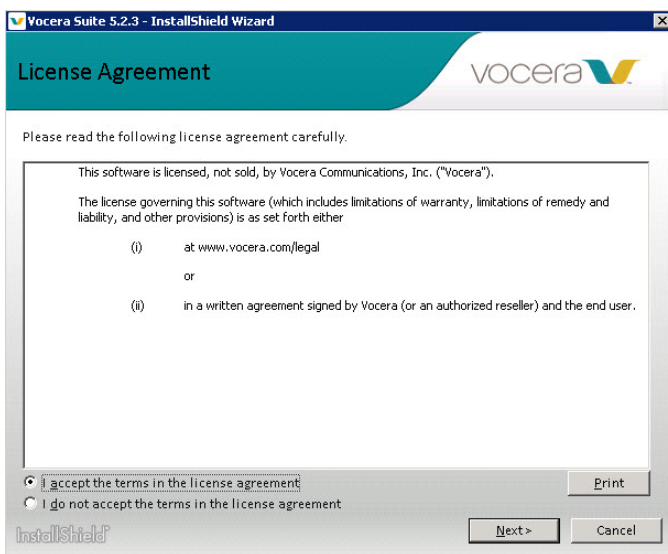
The Welcome window is launched.

3. Click Next to continue with the installation program.



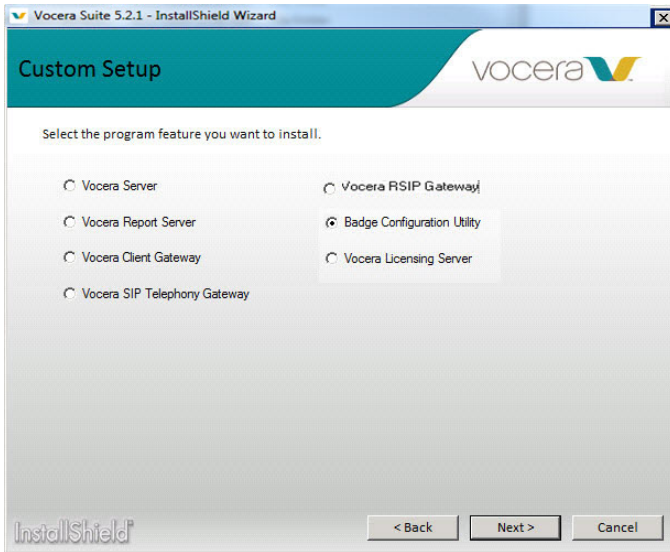
The License Agreement window is displayed.

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



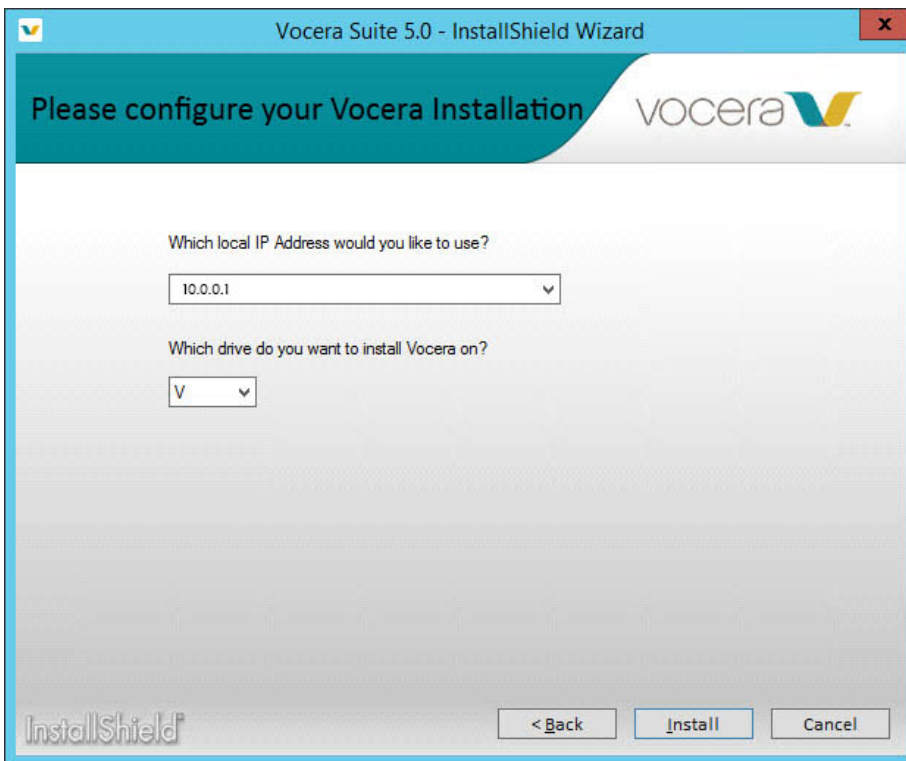
The Custom Setup Window opens.

5. Select the Badge Configuration Utility (BCU) radio button and click Next, in the Custom Setup window.

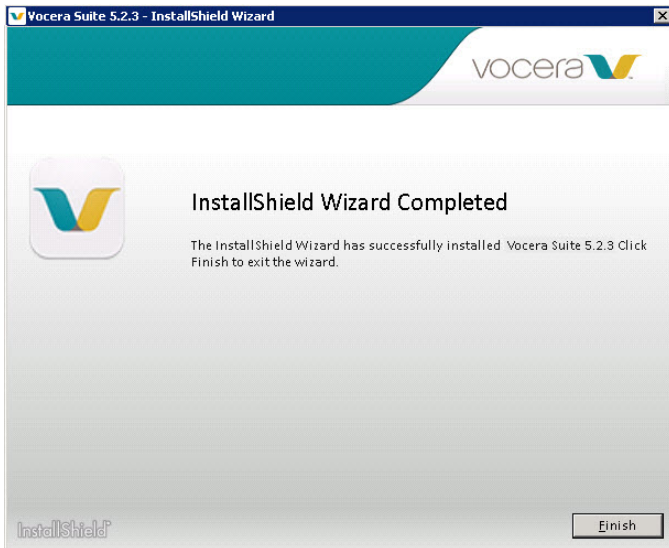


The Installation Configuration window is displayed.

6. Enter the IP address **10.0.0.1** and the drive where you want to install the Badge Configuration Utilities.



7. Click Install.



The Vocera installer launches with a progress bar that shows the status of the installation. When the installation is complete, a window appears announcing that the installation is complete.

8. Click Finish.

Your installation is complete, and a shortcut icon is created on the desktop to access Badge Property Editor (BPE). The installation creates some important badge configuration files at **Vocera\config**.



Badge Configuration Files Overview

The **\vocera\config** directory on the configuration computer contains the files used by the Badge Properties Editor and the Badge Configuration Utility.

By default, the same set of files is also installed in this directory on the Vocera Voice Server computer.

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

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

Item	Description
badge.properties	Text file, created by the Badge Properties Editor, contains properties that determine badge behavior.  Note: Vocera recommends that you do not edit these files manually.
profiles.txt	(For B3000n only) Text file, generated by the Badge Properties Editor when you create dynamic wireless profiles for the badge. The <code>profiles.txt</code> file contains details of WLAN configurations, each with its description and includes the priority used by WLAN profiles when selecting a profile and attempting to associate to the badge. The information in this file is populated with data from the <code>badge.properties</code> file and based on selections made when you create a new profile using the Badge Properties Editor user interface.  Note: Vocera recommends that you do not edit these files manually.
bcu.bat	A batch file that launches the Badge Configuration Utility.

Property and Profile Files for the Badge

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

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

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

For example, suppose different badge types use different SSIDs:

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

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

About Dynamic WLAN Profiles

Dynamic Wireless LAN profiles are intended for campus environments where the network administrator plans to deploy multiple WLAN configurations for different physical locations.

You can configure various WLAN configurations to be provisioned in the B3000n where the badge can select the correct WLAN profile without requiring end-user intervention.

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

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

An interruption and communication delay of 60 seconds or longer as the badge attempts to associate with a Wi-Fi network and transitions between multiple WLAN configurations is an expected behavior. You can enable up to 4 WLAN profiles in your environment.

Specifying TCP/IP Settings

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

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

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

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



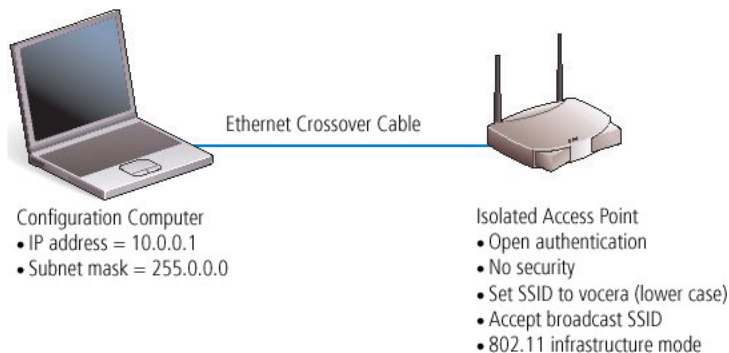
Note: The exact procedure for setting your TCP/IP properties depends upon the version of the operating system. Refer to your Windows documentation for more information.

Setting up Isolated Access Point

The isolated access point allows a badge to connect to the configuration computer using default factory settings.

This access point is a temporary set up that you use only to configure badges. Configured badges can connect to your wireless LAN by using your existing SSID and security system.

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



How to Set up an Isolated Access Point

The access point must be isolated so you can set it up with a different SSID, and without compromising the security of your site. Any access point security will prevent unconfigured badges from connecting.

To set up an isolated Access Point, perform the following tasks:

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. Install configuration software for the access point on the configuration computer.
Most access points require only a browser for configuration.
4. Ensure that your access point is set up as follows, using the access point configuration utility:
 - Authentication—Allow open (typically the default)
 - Security—Turn off all security (typically the default)
 - SSID—Assign the value as vocera (using all lower-case letters)
 - SSID broadcast—Allow a broadcast to associate (typically the default)
 - Configuration Mode—Configure the Access Point in the 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.

Configuring a New Badge

This section summarizes the procedures for creating a badge property file, using the Badge Properties Editor, and configuring a test badge.



Note: When you configure a badge, you must either assign it a fixed IP address or specify a DHCP server that assigns IP addresses dynamically. This IP address is one of the properties in the badge properties file. For more information, refer to [Assigning Static IP Addresses](#) on page 26.

Using the Badge Properties Editor

Badge Properties Editor (BPE) is a tool that allows you to set properties for the badge and lets it connect to the wireless network.

The Badge Properties Editor (BPE) is installed on both the configuration computer and the Vocera Voice Server computer. If you are performing initial badge configuration, use the Badge Properties Editor on the configuration computer.

To use the BPE, perform the following tasks:

1. Locate and double-click the Vocera BPE Launcher icon on the desktop the first time. For subsequent logins, access the Vocera BPE Launcher using the URL `http://127.0.0.1:8011/#/!` where **127.0.0.1** is the localhost and **8011** is the Voice Server IP port for BPE. The Badge Properties Editor UI appears.
2. Select a badge you want to configure, under Badges.

The badges you can configure are:

- B2000
- B3000
- B3000n
- V5000



Note: The B2000 badge is not supported on Vocera Platform 6.1.0

3. Set the following badge property values for your badge:
 - **Profiles**—This parameter is applicable only for B3000n badge. Specifies the name of the file to control general behavior. You must use the **profiles.txt** files for environments that require more than one wireless profile in a dynamic campus-type setting.
 - **General Settings**—Specifies the minimal set of properties you need to set for any badge in use 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.
 - **Security Settings**—Specifies how to enable badges to work with the security features that correspond to the type of authentication and encryption employed by your wireless network. If you are deploying different types of Vocera badges, you can configure them to reside on separate SSIDs and take advantage of the enhanced security support offered by newer badge models. If all the badges reside on the same SSID, the security you opt must be supported by all badge types.
 - **Wireless Settings**—Specifies the parameters that affect how the badge operates on the wireless network of your organization. A set of WLAN parameters can be scanned through for connectivity in different locations. Wireless clients learn about available APs by scanning other 802.11 channels on the same WLAN or SSID.
 - **Custom Properties**—Specifies the customized badge properties you want to upload to the badge. The options available are:
 - **Select**—Select the badge property that you want to configure.
 - **Key**—Enter the key in the following format-B2.<Property-Name>, B3.<Property-Name>, B3N.<Property-Name>, and V5.<Property-Name> for B2000, B3000, B3000n, and V5000 respectively.

- Value—Enter the value of the property.
- Comment—Add comments for your reference.



Note: Key and Value fields are mandatory.

4. Click one of the following:

- Submit—Allows you to submit the changes.
- Discard Changes—Allows you to discard the changes and re-enter the badge properties.



The Badge Properties Editor creates a **badge.properties** text file under `\vocera\config`.


You can now upload the badge properties to your badges.

B2000 Badge Properties Configuration

This section lists that badge properties that you can configure using the BPE on your B2000 Badge.

Enter the information or check the following badge properties:

Fields	Description
General Settings	
Server IP Address*	<p>Specifies the IP address of the computer that runs the Vocera Voice Server. This is a required field.</p> <p>Use dotted-decimal notation to specify this value. For example, 192.168.3.7.</p> <p>If you are configuring a cluster, enter the IP address of each machine in the cluster, separated by commas, with no spaces.</p> <p> Note: Do not enter more than four comma-separated IP addresses. The Vocera Voice Server supports a maximum of four cluster nodes.</p>
SSID*	<p>Specify an SSID other than <i>vocera</i> (all lower-case) for your production server. Badges are factory-programmed to use the <i>vocera</i> SSID to establish a wireless connection to the configuration computer that you have set up for your Vocera system.</p>
Hide Boot Menus	<p>Specifies the option to prevent configuration menus to be displayed on a badge. The menus provide access to powerful utilities for maintenance and troubleshooting. Use these utilities only when you are working with Vocera Technical Support.</p> <p> Note: This property is ignored by the B3000 and B3000n badges, with menus always hidden.</p>
Security Settings	
Enable FIPS	<p>Specifies the option to enable the badge cryptographic security module to run in a secure mode that conforms with Federal Information Processing Standard (FIPS) 140-2.</p> <p>When <i>Enable FIPS</i> field is checked, it requires WPA2-PSK, WPA2-PEAP, or WPA2-TLS.</p>
Authentication Type	
Open	<p>Specifies that your wireless network does not require authentication.</p>
LEAP	<p>Specifies that your wireless network implements the Cisco LEAP protocol for authentication.</p>
WPA-PSK	<p>Specifies that your wireless network uses the WiFi Protected Access Pre-Shared Key protocol for authentication.</p>
WPA-PEAP	<p>Specifies that your wireless network uses the WiFi Protected Access Protected Extensible Authentication Protocol for authentication.</p>
EAP-FAST	<p>Specifies that your wireless network uses Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling for authentication. EAP-FAST authentication enables you to select between automatic or manual PAC provisioning.</p>




Fields	Description
Username and Password*	<p>Enter appropriate values in the <i>Username</i> and <i>Password</i> fields if your network uses either LEAP, WPA-PEAP, or EAP-FAST authentication with TKIP-WPA encryption.</p> <p>If your network uses EAP-TLS authentication with external certificates (instead of the Vocera Manufacturer Certificates), enter a value for the <i>Username</i> field but not the <i>Password</i> field. Otherwise, skip both these fields.</p> <p>Each badge on a Vocera Voice Server must use the same username and password. The username format depends on the requirements set by the RADIUS authentication server. For example, when you use LEAP with Cisco ACS and Windows Active Directory, enter <i>domain \userid</i> in the <i>Username</i> field, where <i>domain</i> is a Windows domain name and <i>userid</i> identifies the user. Other RADIUS servers may require the username only.</p> <p>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.</p> <p>The badge supports a maximum of 128 alphanumeric characters for the <i>Username</i> and 32 alphanumeric characters for the <i>Password</i>. In addition, the badge supports the following characters for LEAP passwords:</p> <p>^ # ! * @ % & \$</p> <p> Note: If you are using EAP-FAST authentication and you change the username or password values, you must also generate a new PAC file. With manual PAC provisioning, you must generate a new PAC file on the Cisco ACS and copy it to the Vocera Voice Server and the Vocera configuration computer. With automatic PAC provisioning, you must restore the factory settings on the badge and reconfigure it. When the badge reconnects, it retrieves the new PAC file automatically from the ACS.</p>
Encryption Type	<p>The encryption types available are:</p> <ul style="list-style-type: none"> • None—Species that no encryption type is required. • WEP64—Specifies the WEP 64 bit key with 10 hexadecimal digits • WEP128—Specifies the 128-bit WEP key with 26 hexadecimal digits • TKIP-WPA—Specifies your network uses TKIP as defined by WPA. • AES-CCMP—Specifies your network uses AES-CCMP as defined by WPA2 <p>Use hexadecimal characters to enter the key that the access point uses.</p>
Wireless Settings	
2.4 Ghz Channels	
Set to Defaults (1, 6, 11)	Specifies the option to force badges to scan the three non-overlapping 2.4 GHz channels of 1, 6, and 11.
Specify Channels	Specifies the option to specify up to four arbitrary channels to scan. If the access points on your network are set either to four channels, three channels, or to fewer than three channels other than 1, 6, and 11, select Specify Channels and enter the specific channel numbers in a comma-separated list. Ensure that you specify only channels that are supported for your locale.
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, as communication may be interrupted. Lower values allow a badge to tolerate lower signal quality before searching. The optimal threshold value varies from one 802.11 network to another, depending on how the network is configured. Select a value from 1 to 5. The default value is 2.
CCKM	Check CCKM box if you want to enable Cisco Certified Key Management. CCKM is a form of fast roaming supported on Cisco access points and various routers. Using CCKM, Vocera devices can roam from one access point to another without any noticeable delay during reassociation. After the RADIUS authentication server initially authenticates a Vocera device, 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. To take advantage of this feature, your access points must also support CCKM, and you must use either LEAP, WPA-PEAP, EAP-FAST, or EAP-TLS authentication.
802.11d	Check 802.11d box if you are in a country where systems that use other standards in the 802.11 family are not allowed to operate.
Custom Settings	
B2.BroadcastUsesIGMP	Vocera broadcast is implemented as IP Multicast. If broadcast commands must cross a subnet, IGMP must be supported in the switch or router. Set this property to TRUE.



Fields	Description
B2.ClosedMenus	<p>Specifies whether the badge configuration menus are hidden, or if they can be easily accessed through the DND button:</p> <ul style="list-style-type: none"> FALSE specifies that you can access the configuration menus by pressing the DND button. Within three seconds, it displays the boot countdown timer. TRUE specifies that you must use the special sequence of button presses to display the configuration menus. This value prevents displaying configuration menus and inadvertently causes configuration problems in a badge.
B2.EnableAPSD	<p>Specifies whether the badge takes advantage of the Unscheduled Automatic Power Save Delivery Subset (U-APSD) of 802.11e. U-APSD improves power management and potentially increases the talk time of 802.11 clients.</p> <ul style="list-style-type: none"> FALSE specifies that U-APSD is disabled. TRUE specifies that U-APSD is enabled. <p>To take advantage of this standard, your access points must also support it. Important: Both the B2.EnableAPSD and B2.EnableWMM properties must be set to the same value.</p>
B2.EnableWMM	<p>Specifies whether the badge takes advantage of the WiFi Multimedia (WMM) subset of 802.11e. The 802.11e QoS for prioritizing voice over data traffic and ensuring high-level voice quality</p> <ul style="list-style-type: none"> FALSE specifies that 802.11e QoS is disabled. TRUE specifies that 802.11e QoS is enabled. <p>To take advantage of this standard, your access points must also support it, switches and routers must be configured to honor DSCP markings, and the Vocera QoS Manager service must be enabled on the Vocera Voice Server. Important: Both the B2.EnableAPSD and B2.EnableWMM properties must be set to the same value.</p>
B2.InstallDone	<p>Specifies whether the Badge Properties Editor has performed the initial configuration for a badge:</p> <ul style="list-style-type: none"> TRUE specifies that the badge boots the normal Vocera application when it powers up. FALSE specifies that the badge attempts to connect to a machine at IP address 10.0.0.1 running the Vocera Voice Server when it powers up. If successful, the badge downloads properties and firmware from the Vocera Voice Server.
B2.ListenInterval	<p>An access point broadcasts a management frame called a beacon at a fixed interval (required to be set to 100 ms by Vocera). The B2.ListenInterval property specifies the frequency with which badges "wake up" and listen for a beacon. When the beacon interval is 100 ms and B2.ListenInterval is 5; the default listen interval is 500 ms.</p>
B2.ResetVolumeToDefault	<p>Specifies whether the badge resets the volume to the default at boot-up.</p> <ul style="list-style-type: none"> FALSE specifies that the badge maintains the previous volume setting at boot-up. TRUE specifies that the badge resets the volume to the default at boot-up.
B2.SubnetMask	<p>Specifies a subnet mask that indicates the bits in the IP address corresponding to the subnet, and uses standard dotted notation. For example: 255.255.255.0. You must specify this property if you are using static IP addresses. Leave this field blank if a DHCP server assigns IP addresses.</p>
B2.SubnetRoaming	<p>Specifies whether users can roam across subnet boundaries while using badges. If subnet roaming is enabled, a badge automatically obtains a new IP address when a user transitions to an access point on a different subnet. If you enable subnet roaming, you must use a DHCP server to supply your IP addresses. TRUE specifies that the access points on your wireless LAN are divided into multiple subnets, and you want to allow users to roam across subnet boundaries. FALSE specifies that all the access points on your wireless LAN are within a single subnet. Set this property to minimize DHCP traffic and reduce the chance of a momentary loss of audio when roaming between access points. The subnet where the Vocera Voice Server is located is not relevant to this property.</p>

B3000 Badge Properties Configuration

This section lists the badge properties that you can configure using the BPE on your B3000 Badge.

Enter information or check the following badge properties:

Fields	Description
Profiles	
Selected Profiles	Specifies the name of the profile you selected to control general behavior. You must use the profiles.txt files for environments that require more than one wireless profile in a dynamic campus-type setting.
Create Profile	Allows you to create a new profile to control general behavior.
General Settings	
Server IP Address*	<p>Specifies the IP address of the computer that runs the Vocera Voice Server. This is a required field.</p> <p>Use dotted-decimal notation to specify this value. For example, 192.168.3.7.</p> <p>If you are configuring a cluster, enter the IP address of each machine in the cluster, separated by commas, with no spaces.</p> <p> Note: Do not enter more than four comma-separated IP addresses. The Vocera Voice Server supports a maximum of four cluster nodes.</p>
SSID*	Specify an SSID other than <i>vocera</i> (all lower-case) for your production server. Badges are factory-programmed to use the <i>vocera</i> SSID to establish a wireless connection to the configuration computer that you have set up for your Vocera system.
Hide Boot Menus	<p>Specifies the option to prevent configuration menus to be displayed on a badge. The menus provide access to powerful utilities for maintenance and troubleshooting. Use these utilities only when you are working with Vocera Technical Support.</p> <p> Note: This property is ignored by the B3000 and B3000n badges, with menus always hidden.</p>
Group Mode	<p>Specifies the option to ensure noise-canceling microphones are turned off while users are on a call. Group Mode widens the speech zone, allowing additional people to speak into the primary microphone of the badge.</p> <p>Uncheck this option if you want to eliminate background noise when users are on a call.</p> <p> Note: B3000 and B3000n users can change the Group Mode setting on their badges, overriding the default.</p> <ul style="list-style-type: none"> • For B3000: Group Mode is always off during Genie interactions and broadcasts. • For B3000n: Group Mode is automatically enabled when the badge is turned to a 105-degree angle to improve voice recognition.
Reset Volume to Default	Specifies the option to reset the default volume at boot-up. Otherwise, the previous volume setting is maintained at boot-up.
Security Settings	
Enable FIPS	Specifies the option to enable the badge cryptographic security module to run in a secure mode that conforms with Federal Information Processing Standard (FIPS) 140-2. When Enable FIPS field is checked, it requires WPA2-PSK, WPA2-PEAP, or WPA2-TLS.
Authentication Type	
Open	Specifies that your wireless network does not require authentication.
LEAP	Specifies that your wireless network implements the Cisco LEAP protocol for authentication.

Fields	Description
Username and Password*	<p>Enter appropriate values in the <i>Username</i> and <i>Password</i> fields if your network uses either LEAP, WPA-PEAP, or EAP-FAST authentication with TKIP-WPA encryption.</p> <p>If your network uses EAP-TLS authentication with external certificates (instead of the Vocera Manufacturer Certificates), enter a value for the <i>Username</i> field but not the <i>Password</i> field. Otherwise, skip both these fields.</p> <p>Each badge on a Vocera Voice Server must use the same username and password. The username format depends on the requirements set by the RADIUS authentication server. For example, when you use LEAP with Cisco ACS and Windows Active Directory, enter <i>domain \userid</i> in the <i>Username</i> field, where <i>domain</i> is a Windows domain name and <i>userid</i> identifies the user. Other RADIUS servers may require the username only.</p> <p>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.</p> <p>The badge supports a maximum of 128 alphanumeric characters for the <i>Username</i> and 32 alphanumeric characters for the <i>Password</i>. In addition, the badge supports the following characters for LEAP passwords:</p> <p>^ # ! * @ % & \$</p> <p> Note: If you are using EAP-FAST authentication and you change the username or password values, you must also generate a new PAC file. With manual PAC provisioning, you must generate a new PAC file on the Cisco ACS and copy it to the Vocera Voice Server and the Vocera configuration computer. With automatic PAC provisioning, you must restore the factory settings on the badge and reconfigure it. When the badge reconnects, it retrieves the new PAC file automatically from the ACS.</p>
WPA-PSK	Specifies that your wireless network uses the WiFi Protected Access Pre-Shared Key protocol for authentication.
Pre shared Key	If Authentication Type is set to WPA-PSK , the pre-shared field appears. The pre-shared key that the badge supplies for authentication is a 64-character, hexadecimal value.
WPA-PEAP	Specifies that your wireless network uses the WiFi Protected Access Protected Extensible Authentication Protocol for authentication.
EAP-FAST	Specifies that your wireless network uses Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling for authentication. EAP-FAST authentication enables you to select between automatic or manual PAC provisioning.
Enable Auto-PAC	Specifies the option to enable automatic download of a PAC from the Cisco ACS, and the ACS periodically refreshes the PAC to ensure it does not expire. To take advantage of automatic PAC provisioning, you must configure badges correctly by setting Auto-PAC properties. If you enable manual PAC provisioning, you must create a <code>.pac</code> file on the Cisco ACS and copy it to the Vocera Voice Server and the Vocera configuration computer.
Provision Auto-PAC on Expire	<p>Specifies the option to enable automatic provisioning of a new PAC when it expires. If this property is unchecked, a badge with an expired PAC displays the following message: "Expired or invalid PAC credentials."</p> <p> Note: This message appears 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 must be reconfigured.</p> <p>To take advantage of this feature, you must also select EAP-FAST authentication.</p>
Auto-PAC Provision Retry Count	<p>Specifies the option to limit the number of times a badge attempts to retry retrieving a PAC from the Cisco ACS after the first attempt failed. For example, the badge attempts to retry retrieving a PAC due to wireless network problems. Select a number from 0 to 5.</p> <p>If a badge exceeds the retry count, it displays the following message: Too many retries for Auto-PAC provisioning.</p> <p>By default, this property is set to 0 (indicates no retries). To take advantage of this feature, you must also select EAP-FAST authentication.</p>

Fields	Description
EAP-TLS	<p>Specifies that your wireless network uses Extensible Authentication Protocol-Transport Layer Security for authentication.</p> <p>Check the EAP-TLS field to enable the badge to use custom EAP-TLS certificates rather than Vocera Manufacturer Certificates. If you use custom EAP-TLS certificates, you must generate your self-signed certificates or obtain them from a trusted Certificate Authority (CA). If you check this box, additional configuration is required. You must install client-side certificates on the Vocera Voice Server and the configuration computer, install the server-side certificates on your authentication server, configure your authentication server for EAP-TLS.</p> <p>Alternatively, uncheck this box to use the Vocera Manufacturer Certificates. Vocera badges are preconfigured with EAP-TLS client certificates that are automatically downloaded from the Vocera Voice Server or the Badge Configuration Computer. Vocera Manufacturer Certificates use 2048-bit RSA keys that provide excellent security for enterprise and conform to industry standards and NIST recommendations. If you decide to use Vocera Manufacturer Certificates on the badge, you still need to install Vocera Voice Server-side certificates on your authentication server. For more information on security certificates, refer to <i>Vocera Device Configuration Guide</i>.</p>
Use Custom EAP-TLS Certificates	<p>Specifies the option to enable the badge to use custom EAP-TLS certificates rather than Vocera Manufacturer Certificates. If you use custom EAP-TLS certificates, you must generate your self-signed certificates or obtain it from a trusted Certificate Authority (CA). If you check this box, additional configuration is required. You must install client-side certificates on the Vocera Voice Server and the configuration computer, install the server-side certificates on your authentication server, configure your authentication server for EAP-TLS, and specify the Username and Client Key Password properties.</p> <p>Alternatively, uncheck this box to use the Vocera Manufacturer Certificates. Vocera badges are preconfigured with EAP-TLS client certificates that are automatically downloaded from the Vocera Voice Server or the Badge Configuration Computer. Vocera Manufacturer Certificates use 2048-bit RSA keys that provide excellent security for enterprise and conform to industry standards and NIST recommendations. If you decide to use Vocera Manufacturer Certificates on the badge, you still need to install Vocera Voice Server-side certificates on your authentication server.</p> <p>This property is available only when the Authentication property is set to EAP-TLS.</p>
Encryption Type	<p>The encryption types available are:</p> <ul style="list-style-type: none"> • TKIP-WPA—Specifies your network uses TKIP as defined by WPA. • AES-CCMP—Specifies your network uses AES-CCMP as defined by WPA2 <p>Use hexadecimal characters to enter the key that the access point is using.</p>
Wireless Settings	
2.4 GHz Channels	
Set to Defaults (1, 6, 11)	Specifies the option to force badges to scan the three non-overlapping 2.4 GHz channels of 1, 6, and 11.
Specify Channels	<p>Specifies the option to specify up to four arbitrary channels to scan.</p> <p>If the access points on your network are set either to four channels, three channels, or to fewer than three channels other than 1, 6, and 11, select Specify Channels and enter the specific channel numbers in a comma-separated list.</p> <p>Ensure that you specify only channels that are supported for your locale.</p>
Roaming Policy	<p>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, as communication may be interrupted. Lower values allow a badge to tolerate lower signal quality before searching. The optimal threshold value varies from one 802.11 network to another, depending on how the network is configured. Select a value from 1 to 5. The default value is 2.</p>
CCKM	<p>Check CCKM box if you want to enable Cisco Certified Key Management.</p> <p>CCKM is a form of fast roaming supported on Cisco access points and various routers. Using CCKM, Vocera devices can roam from one access point to another without any noticeable delay during reassociation. After the RADIUS authentication server initially authenticates a Vocera device, 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.</p> <p>To take advantage of this feature, your access points must also support CCKM, and you must use either LEAP, WPA-PEAP, EAP-FAST, or EAP-TLS authentication.</p>
802.11d	Check 802.11d box if you are in a country where systems that use other standards in the 802.11 family are not allowed to operate.




Fields	Description
Custom Settings	
B3.BroadcastUsesIGMP	Vocera broadcast is implemented as IP Multicast. If broadcast commands must cross a subnet, IGMP must be supported in the switch or router. Set this property to TRUE.
B3.ClosedMenus	Specifies whether the badge configuration menus are hidden, or if they can be easily accessed through the DND button: <ul style="list-style-type: none"> FALSE specifies that you can access the configuration menus by pressing the DND button within three seconds displaying the boot countdown timer. TRUE specifies that you must use the special sequence of button presses to display the configuration menus. This value prevents displaying configuration menus and inadvertently causes configuration problems in a badge.
DefaultHandsetVolume	Lists the default volume level of Privacy Mode when no users are logged in.
DisplayHandsetMode	Displays Privacy Mode on the badge menu under Settings.
B2.EnableAPSD	Specifies whether the badge takes advantage of the Unscheduled Automatic Power Save Delivery Subset (U-APSD) of 802.11e. U-APSD improves power management and potentially increases the talk time of 802.11 clients. <ul style="list-style-type: none"> FALSE specifies that U-APSD is disabled. TRUE specifies that U-APSD is enabled. <p>To take advantage of this standard, your access points must support it. Important: Both the B3.EnableAPSD and B3.EnableWMM properties must be set to the same value.</p>
B3.EnableWMM	Specifies whether the badge takes advantage of the WiFi Multimedia (WMM) subset of 802.11e. The 802.11e QoS provides standards-based QoS to prioritize voice over data traffic and ensure high-level voice quality. <ul style="list-style-type: none"> FALSE specifies that 802.11e QoS is disabled. TRUE specifies that 802.11e QoS is enabled. <p>To take advantage of this standard, your access points must support it, switches and routers must be configured to honor DSCP markings, and the Vocera QoS Manager service must be enabled on the Vocera Voice Server. Important: Both the B3.EnableAPSD and B3.EnableWMM properties must be set to the same value.</p>
EnableHandsetQuickEntry	Enables Easy Access entry to Privacy mode.
HandsetMode	Enables or disables Privacy mode using Easy Access.
HandsetQuickEntryPromptPlay	Plays an audible alert, "Entering Handset Mode" while switching to Privacy Mode using Easy Access.
B3.InstallDone	Specifies whether the Badge Properties Editor has performed the initial configuration for a badge: <ul style="list-style-type: none"> TRUE specifies that the badge boots the normal Vocera application when it powers up. FALSE specifies that the badge attempts to connect to a machine at IP address 10.0.0.1 running the Vocera Voice Server when it powers up. If successful, the badge downloads properties and firmware from the Vocera Voice Server.
B3.ListenInterval	An access point broadcasts a management frame called a beacon at a fixed interval (required to be set to 100 ms by Vocera). The B3.ListenInterval property specifies the frequency with which badges "wake up" and listen for a beacon. When the beacon interval is 100 ms and B3.ListenInterval is 5, the default listen interval is 500 ms.
B3.ResetVolumeToDefault	Specifies whether the badge resets the volume to the default at boot-up. <ul style="list-style-type: none"> FALSE specifies that the badge maintains the previous volume setting at boot-up. TRUE specifies that the badge resets the volume to the default at boot-up.
B3.SubnetMask	Specifies a subnet mask that indicates the bits in the IP address that correspond to the subnet, using standard dotted notation. For example: 255.255.255.0. You must specify this property if you are using static IP addresses. Leave this field blank if a DHCP server is assigning IP addresses.



Fields	Description
B3.SubnetRoaming	<p>Specifies whether users can roam across subnet boundaries while using badges.</p> <p>If subnet roaming is enabled, a badge automatically obtains a new IP address as a badge user makes the transition to an access point on a different subnet. If you enable subnet roaming, you must use a DHCP server to supply your IP addresses.</p> <p>TRUE specifies that the access points on your wireless LAN are divided into multiple subnets, and if you want to allow users to roam across subnet boundaries.</p> <p>FALSE specifies that all the access points on your wireless LAN are within a single subnet. Set this property to minimize DHCP traffic and reduce the chance of a momentary loss of audio when roaming between access points.</p> <p>The subnet where the Vocera Voice Server is located is not relevant to this property.</p>

B3000N Badge Properties Configuration


This section lists the badge properties that you can configure using the BPE on your B3000N Badge.

Enter information or check the following badge properties:

Fields	Description
Profiles	
Selected Profiles	Specifies the name of the profile you selected to control general behavior. You must use the profiles.txt file for environments that require more than one wireless profile in a dynamic campus-type setting.
Create Profile	Allows you to create a new profile to control general behavior.
General Settings	
Server IP Address*	<p>Specifies the IP address of the computer that runs the Vocera Voice Server. This is a required field.</p> <p>Use dotted-decimal notation to specify this value. For example, 192.168.3.7.</p> <p>If you are configuring a cluster, enter the IP address of each machine in the cluster, separated by commas, with no spaces.</p> <p> Note: Do not enter more than four comma-separated IP addresses. The Vocera Voice Server supports a maximum of four cluster nodes.</p>
SSID*	Specify an SSID other than <i>vocera</i> (all lower-case) for your production server. Badges are factory-programmed to use the <i>vocera</i> SSID to establish a wireless connection to the configuration computer that you have set up for your Vocera system.
Hide Boot Menus	<p>Specifies the option to prevent configuration menus to be displayed on a badge. The menus provide access to powerful utilities for maintenance and troubleshooting. Use these utilities only when you are working with Vocera Technical Support.</p> <p> Note: This property is ignored by the B3000 and B3000n badges, with menus always hidden.</p>
Group Mode	<p>Specifies the option to ensure noise-canceling microphones are turned off while users are on a call. Group Mode widens the speech zone, allowing additional people to speak into the primary microphone of the badge.</p> <p>Uncheck this option if you want to eliminate background noise when users are on a call.</p> <p> Note: B3000 and B3000n users can change the Group Mode setting on their badges, overriding the default.</p> <ul style="list-style-type: none"> For B3000: Group Mode is always off during Genie interactions and broadcasts. For B3000n: Group Mode is automatically enabled when the badge is turned to a 105-degree angle to improve voice recognition.
Reset Volume to Default	Specifies the option to reset the default volume at boot-up. Otherwise, the previous volume setting is maintained at boot-up.
Display Bluetooth Settings	Check the Display Bluetooth Settings box to display the Bluetooth configuration menu on the badge.
Security Settings	

Fields	Description
Enable FIPS	Specifies the option to enable the badge cryptographic security module to run in a secure mode that conforms with Federal Information Processing Standard (FIPS) 140-2. When Enable FIPS field is checked, it requires WPA2-PSK, WPA2-PEAP, or WPA2-TLS.
Authentication Type	
Open	Specifies that your wireless network does not require authentication.
LEAP	Specifies that your wireless network implements the Cisco LEAP protocol for authentication.
Username and Password*	<p>Enter appropriate values in the Username and Password fields if your network uses either LEAP, WPA-PEAP, or EAP-FAST authentication with TKIP-WPA encryption.</p> <p>If your network uses EAP-TLS authentication with external certificates (instead of the Vocera Manufacturer Certificates), enter a value for the Username field but not the Password field. Otherwise, skip both these fields.</p> <p>Each badge on a Vocera Voice Server must use the same username and password. The username format depends on the requirements set by the RADIUS authentication server. For example, when you use LEAP with Cisco ACS and Windows Active Directory, enter <i>domain \userid</i> in the Username field, where <i>domain</i> is a Windows domain name and <i>userid</i> identifies the user. Other RADIUS servers may require the username only.</p> <p>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.</p> <p>The badge supports a maximum of 128 alphanumeric characters for the Username and 32 alphanumeric characters for the Password. In addition, the badge supports the following characters for LEAP passwords:</p> <p>^ # ! * @ % & \$</p> <p> Note: If you are using EAP-FAST authentication and you change the username or password values, you must also generate a new PAC file. With manual PAC provisioning, you must generate a new PAC file on the Cisco ACS and copy it to the Vocera Voice Server and the Vocera configuration computer. With automatic PAC provisioning, you must restore the factory settings on the badge and reconfigure it. When the badge reconnects, it retrieves the new PAC file automatically from the ACS.</p>
WPA-PSK	Specifies that your wireless network uses the WiFi Protected Access Pre-Shared Key protocol for authentication.
Pre shared Key	If Authentication Type is set to WPA-PSK , the pre-shared field appears. The pre-shared key that the badge supplies for authentication is a 64-character, hexadecimal value.
WPA-PEAP	Specifies that your wireless network uses the WiFi Protected Access Protected Extensible Authentication Protocol for authentication.
EAP-FAST	Specifies that your wireless network uses Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling for authentication. EAP-FAST authentication enables you to select between automatic or manual PAC provisioning.
Enable Auto-PAC	Specifies the option to enable automatic download of a PAC from the Cisco ACS, and the ACS periodically refreshes the PAC to ensure it does not expire. To take advantage of automatic PAC provisioning, you must configure badges correctly by setting Auto-PAC properties. If you enable manual PAC provisioning, you must create a .pac file on the Cisco ACS and copy it to the Vocera Voice Server and the Vocera configuration computer.
Provision Auto-PAC on Expire	<p>Specifies the option to enable automatic provisioning of a new PAC when it expires. If this property is unchecked, a badge with an expired PAC displays the following message: "Expired or invalid PAC credentials."</p> <p> Note: This message appears 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 must be reconfigured.</p> <p>To take advantage of this feature, you must also select EAP-FAST authentication.</p>
Auto-PAC Provision Retry Count	<p>Specifies the option to limit the number of times a badge attempts to retry retrieving a PAC from the Cisco ACS after the first attempt failed. For example, the badge attempts to retry retrieving a PAC due to wireless network problems. Select a number from 0 to 5.</p> <p>If a badge exceeds the retry count, it displays the following message: Too many retries for Auto-PAC provisioning.</p> <p>By default, this property is set to 0 (indicates no retries). To take advantage of this feature, you must also select EAP-FAST authentication.</p>

Fields	Description
EAP-TLS	<p>Specifies that your wireless network uses Extensible Authentication Protocol-Transport Layer Security for authentication.</p> <p>Check the EAP-TLS field to enable the badge to use custom EAP-TLS certificates rather than Vocera Manufacturer Certificates. If you use custom EAP-TLS certificates, you must generate your self-signed certificates or obtain them from a trusted Certificate Authority (CA). If you check this box, additional configuration is required. You must install client-side certificates on the Vocera Voice Server and the configuration computer, install the server-side certificates on your authentication server, configure your authentication server for EAP-TLS.</p> <p>Alternatively, uncheck this box to use the Vocera Manufacturer Certificates. Vocera badges are preconfigured with EAP-TLS client certificates that are automatically downloaded from the Vocera Voice Server or the Badge Configuration Computer. Vocera Manufacturer Certificates use 2048-bit RSA keys that provide excellent security for enterprise and conform to industry standards and NIST recommendations. If you decide to use Vocera Manufacturer Certificates on the badge, you still need to install Vocera Voice Server-side certificates on your authentication server. For more information on security certificates, refer to <i>Vocera Device Configuration Guide</i>.</p>
Use Custom EAP-TLS Certificates	<p>Specifies the option to enable the badge to use custom EAP-TLS certificates rather than Vocera Manufacturer Certificates. If you use custom EAP-TLS certificates, you must generate your self-signed certificates or obtain it from a trusted Certificate Authority (CA). If you check this box, additional configuration is required. You must install client-side certificates on the Vocera Voice Server and the configuration computer, install the server-side certificates on your authentication server, configure your authentication server for EAP-TLS, and specify the Username and Client Key Password properties.</p> <p>Alternatively, uncheck this box to use the Vocera Manufacturer Certificates. Vocera badges are preconfigured with EAP-TLS client certificates that are automatically downloaded from the Vocera Voice Server or the Badge Configuration Computer. Vocera Manufacturer Certificates use 2048-bit RSA keys that provide excellent security for enterprise and conform to industry standards and NIST recommendations. If you decide to use Vocera Manufacturer Certificates on the badge, you still need to install Vocera Voice Server-side certificates on your authentication server.</p> <p>This property is available only when the Authentication property is set to EAP-TLS.</p>
Encryption Type	<p>The encryption types available are:</p> <ul style="list-style-type: none"> • TKIP-WPA—Specifies your network uses TKIP as defined by WPA. • AES-CCMP—Specifies your network uses AES-CCMP as defined by WPA2 <p>Use hexadecimal characters to enter the key that the access point is using.</p>
Wireless Settings	
Wireless Band	<p>Select the wireless bands used by the B3000n badge:</p> <ul style="list-style-type: none"> • ABGN—Uses all 802.11 wireless bands (a, b, g, and n) at 2.4 GHz and 5 GHz. This is the default setting. • AN—Uses 802.11a and 802.11n wireless bands at 5 GHz. • BGN—Uses the 802.11b, 802.11g, and 802.11n wireless bands at 2.4 GHz. • A—Uses the 802.11a wireless band at 5 GHz. • BG—Uses the 802.11b and 802.11g wireless bands at 2.4 GHz.
2.4 GHz Channels	
Set to Defaults (1, 6, 11)	<p>Specifies the option to force badges to scan the three non-overlapping 2.4 GHz channels of 1, 6, and 11.</p>
Specify Channels	<p>Specifies the option to specify up to four arbitrary channels to scan.</p> <p>If the access points on your network are set either to four channels, three channels, or to fewer than three channels other than 1, 6, and 11, select Specify Channels and enter the specific channel numbers in a comma-separated list.</p> <p>Ensure that you specify only channels that are supported for your locale.</p>
CCKM	<p>Check CCKM box if you want to enable Cisco Certified Key Management.</p> <p>CCKM is a form of fast roaming supported on Cisco access points and various routers. Using CCKM, Vocera devices can roam from one access point to another without any noticeable delay during reassociation. After the RADIUS authentication server initially authenticates a Vocera device, 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.</p> <p>To take advantage of this feature, your access points must also support CCKM, and you must use either LEAP, WPA-PEAP, EAP-FAST, or EAP-TLS authentication.</p>

Fields	Description
OKC	Check the OKC box to enable authentication between multiple APs in a network when APs are under common administrative control.
802.11r	Check 802.11r box to permit continuous connectivity for devices in motion. 802.11r addresses the fast roaming and fast BSS transitions.
FT over DS	Check FT over DS box to configure fast transition roaming over the DS (distribution system).
802.11d	Check 802.11d box if you are in a country where systems that use other standards in the 802.11 family are not allowed to operate.
802.11k	Check 802.11k to discover the best available access point.
802.11w	<p>Check 802.11w box to support protected management frames.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Disable • Optional • Mandatory <p> Note: It is difficult to troubleshoot security of encryption-related issues if the management frames are encrypted. So, you have the option to disable it or make it optional.</p> <p>Enable 802.11w for WPA2-PSK-SHA256 profile to work.</p>
5 GHz Channels	
Set to Defaults (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165)	Specifies the option to force B3000n badges to scan 5 GHz channels of 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165.
Specify Channels	<p>Specifies the option to specify up to four arbitrary channels to scan.</p> <p>If the access points on your network are set either to four channels, three channels, or to fewer than three channels other than 1, 6, and 11, select Specify Channels and enter the specific channel numbers in a comma-separated list.</p> <p>Ensure that you specify only channels that are supported for your locale.</p>
Roaming Policy	<p>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, as communication may be interrupted. Lower values allow a badge to tolerate lower signal quality before searching. The optimal threshold value varies from one 802.11 network to another, depending on how the network is configured. Select a value from 1 to 5. The default value is 2.</p>
Custom Settings	
B3N.BroadcastUsesIGMP	<p>Vocera broadcast is implemented as IP Multicast. If broadcast commands need to cross a subnet, IGMP must be supported in the switch or router, and this property must be set to TRUE.</p> <p>The B3000n badge auto-detects IGMP and changes its mode dynamically if IGMP is enabled in the infrastructure. Consequently, this property is deprecated in the B3000n badge.</p>
DefaultHandsetVolume	Lists the default volume level of Privacy Mode when no user is logged in.
DisplayHandsetMode	Displays Privacy Mode in the badge menu under Settings.
B3N.EnableAPSD	<p>Specifies whether the badge takes advantage of the Unscheduled Automatic Power Save Delivery Subset (U-APSD) of 802.11e. U-APSD improves power management and potentially increases the talk time of 802.11 clients.</p> <ul style="list-style-type: none"> • FALSE specifies that U-APSD is disabled. • TRUE specifies that U-APSD is enabled. <p>To take advantage of this standard, your access points must also support it.</p> <p>Important: Both the B3N.EnableAPSD and B3N.EnableWMM properties must be set to the same value.</p> <p>The firmware and chip set changes in the B3000n badge make this property unnecessary. Consequently, this property is deprecated in the B3000n badge.</p>

Fields	Description
B3N.EnableWMM	<p>Specifies whether the badge takes advantage of the WiFi Multimedia (WMM) subset of 802.11e. The 802.11e QoS prioritizes voice over data traffic and ensures high-level voice quality.</p> <ul style="list-style-type: none"> • FALSE specifies that 802.11e QoS is disabled. • TRUE specifies that 802.11e QoS is enabled. <p>To take advantage of this standard, your access points must also support it. Switches and routers must be configured to honor DSCP markings, and the Vocera QoS Manager service must be enabled on the Vocera Voice Server.</p> <p>If 802.11n is enabled on both the network and the B3000n badge (through the B3N.WirelessBand property), the B3000n takes advantage of WMM and ignores this property. In legacy 802.11n environments, you can continue to use this property for the B3000n badge. This property is not tied to the use of APSD for the B3000n.</p>
EnableHandsetQuickEntry	Enables easy access entry to Privacy mode.
HandsetMode	Enables or disables Privacy mode using easy access.
HandsetQuickEntryPromptPlay	Plays an audible alert, Entering Handset Mode while switching to Privacy Mode using Easy Access.
B3N.InstallDone	<p>Specifies whether the Badge Properties Editor has performed the initial configuration for a badge:</p> <ul style="list-style-type: none"> • TRUE specifies that the badge boots the normal Vocera application when it powers up. • FALSE specifies that the badge attempts to connect to a machine at IP address 10.0.0.1 running the Vocera Voice Server when it powers up. If successful, the badge downloads properties and firmware from the Vocera Voice Server.
B3N.ListenInterval	<p>Specifies the frequency in which a badge "wakes up" and listen for a beacon. When the beacon interval is 100 ms and B3.ListenInterval is 5; the default listen interval is 500 ms.</p> <p>An access point broadcasts a management frame called a beacon at a fixed interval (required to be set to 100 ms by Vocera).</p>
B3N.ResetVolumeToDefault	<p>Specifies whether the badge resets the volume to the default at boot-up.</p> <ul style="list-style-type: none"> • FALSE specifies that the badge maintains the previous volume setting at boot-up. • TRUE specifies that the badge resets the volume to the default at bootup.
B3N.SubnetMask	Specifies a subnet mask that indicates the bits in the IP address corresponds to the subnet, and uses standard dotted notation. For example 255.255.255.0. You must specify this property if you are using static IP addresses. Leave this field blank if a DHCP server assigns IP addresses.
B3N.SubnetRoaming	<p>Specifies whether users can roam across subnet boundaries while using badges.</p> <p>If subnet roaming is enabled, a badge automatically obtains a new IP address when a user transitions to an access point on a different subnet. If you enable subnet roaming, you must use a DHCP server to supply your IP addresses.</p> <p>TRUE specifies that the access points on your wireless LAN are divided into multiple subnets and you want to allow users to roam across subnet boundaries.</p> <p>FALSE specifies that all the access points on your wireless LAN are within a single subnet. Set this property to minimize DHCP traffic and reduce the chance of a momentary loss of audio when roaming between access points.</p> <p>The subnet where the Vocera Voice Server is located is not relevant to this property.</p>
B3N.ChannelstoScan	Specifies the list of channels to be scanned in 2.4GHz. Use this property to scan channels other than 1,6,11 mentioned in the specific channel options. If you do not specify channel numbers all the channels are automatically scanned.
B3N.ChannelstoScan5G	Specifies the list of channels to be scanned in 5GHz. Use this property to scan channels other than 1,6,11 mentioned in the specific channel options. If you do not specify channel numbers all the channels are automatically scanned.
B3N.HeadsetMicSupport	Specifies the option to enable or disable the headset mic when a 2.5 mm headphone is used. Set the value to True if the headset has a mic and False if it does not have a mic. The default value of the property is true. This property option can also be enabled/disabled from the Badge Settings.

Configuring a Test Badge

Set up a single test badge to confirm that it connects to the network the way you intended, and troubleshoot your `badge.properties` file if needed and then configure the remaining badges.

Ensure that the production Vocera Voice Server is running and the badge is within range of the wireless network to which it is trying to connect. The badge will attempt to connect to the Vocera Voice Server after updating itself from the Badge Configuration Utility.



Important: If you download incorrect properties to your badges, you may need to reset the factory defaults on each badge.

To configure a test badge, perform the following tasks:

1. Locate and double-click the Vocera Badge Configuration Utility Launcher file on the desktop.
2. Attach a charged battery to a new badge (a badge that has never been configured).
A new badge automatically looks for the configuration computer (because the IP address of the configuration computer is set to 10.0.0.1) and connects to it. The Badge Configuration Utility displays the **start session** message; then it automatically starts downloading firmware and properties to the badge.
The Badge Configuration Utility continues to display messages as it downloads the firmware and properties. When the download is complete, the badge reboots and tries to connect to the network using the SSID and other network properties that you specified in the `badge.properties` file.
If the badge successfully connects to the network, it then tries to connect to the production Vocera Voice Server using the Vocera Voice Server IP Address that you specified in the `badge.properties` file.
3. On the screen of the badge:
 - The message “Logged Out” indicates that the badge is configured properly and has connected to the Vocera Voice Server. Continue with [Configuring the Remaining Badges](#) on page 28.
 - If the badge does not display “Logged Out” within 30 seconds to one minute, the badge is not configured properly and did not connect to the Vocera Voice Server. Continue with [Troubleshooting Badge Configuration](#) on page 33.
4. Shut down the Badge Configuration Utility.
The Badge Configuration Utility session ends, and the command window closes.
5. Copy the `badge.properties` file you created on the configuration computer to the `\vocera\config` directory of your production Vocera Voice Server.
6. Perform one of the following:
 - If your production Vocera Voice Server is running, stop it and then restart it to load the `badge.properties` file into memory.
 - If your production Vocera Voice Server is not running, start it to load the `badge.properties` file into memory.

Assigning Static IP Addresses

Badges that use static IP addresses must be configured manually.

You can also use static IP addresses in the following situations:

- When there is no DHCP server to provide the IP addresses.
- You are setting up a small evaluation system.
- Static IP addresses are mandatory at your site.

However, note that assigning static IP addresses manually to badges is a slow and potentially error-prone process. Hence, Vocera recommends that you use a DHCP server to assign IP addresses.

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

Configuring Badges with Static IP Addresses

To configure badges with static IP addresses, perform the following tasks:

1. Click the BPE launcher.

The BPE UI opens.

2. Select the badge type you want to configure.

The badge configuration page appears.


3. Select the profile and configure the general, security, and wireless settings. For more information, refer to [Using the Badge Properties Editor](#) on page 13.
4. Under Custom Setting, click New and enter the following :

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

For more information on the badge properties, refer to *Custom Settings* section of , [B2000 Badge Properties Configuration](#) on page 14, [B3000 Badge Properties Configuration](#) on page 16, and [B3000N Badge Properties Configuration](#) on page 21 respectively.

5. Click one of the following :

- Submit—Submits the changes.
- Discard Changes—Discards the changes.

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

Configuring the Remaining Badges

After you have successfully configured and tested one badge, you can 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](#). Use the Badge Configuration Utility to connect to each of your remaining badges.

Using the Badge Configuration Utility

Badge Configuration Utility is used with new badges. Hence 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 with IP address 10.0.0.1.

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.

For more information, refer to [Restoring Factory Default Settings](#) on page 38.

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



Note: You can use the Badge Configuration Utility to configure ten badges simultaneously.

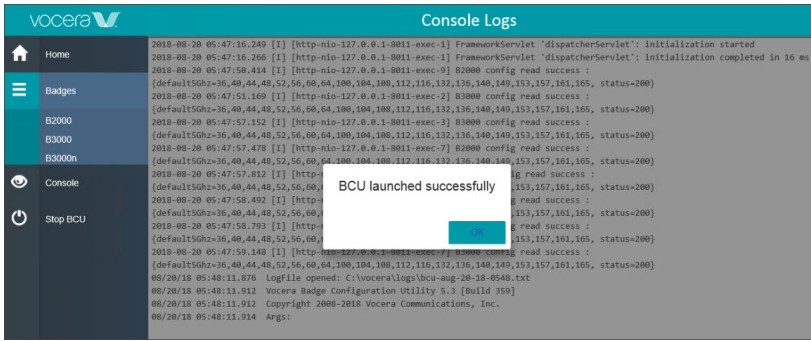
Running the Badge Configuration Utility

You can configure the remaining badges using the Badge Configuration Utility.

1. Using the BCU

To use the BCU, perform the following tasks:

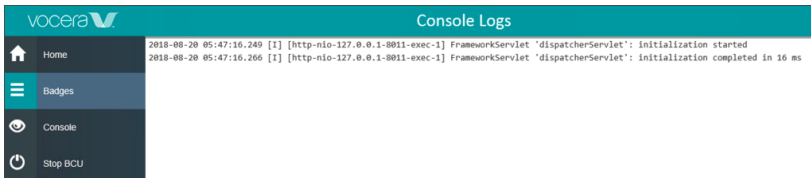
1. Locate and double-click the Vocera BPE Launcher icon on the desktop.
The Badge Properties Editor UI appears.
2. Attach a charged battery to either a new badge or a badge that has been reset to factory defaults.
The badge automatically runs its Updater program if the `InstallDone` property is set to `False`. The Updater searches for a Badge Configuration Utility running on 10.0.0.1 and connects to it.
3. Click Start BCU on the left pane.
The tab toggles to Stop BCU.



```

vocera Console Logs
Home
Badges
  B2000
  B3000
  B3000n
Console
  Stop BCU
2018-08-20 05:47:16.240 [I] [http-nio-127.0.0.1-8011-exec-1] FrameworkServlet 'dispatcherServlet': initialization started
2018-08-20 05:47:16.266 [I] [http-nio-127.0.0.1-8011-exec-1] FrameworkServlet 'dispatcherServlet': initialization completed in 16 ms
2018-08-20 05:47:58.414 [I] [http-nio-127.0.0.1-8011-exec-9] B2000 config read success :
[default15Ghz=36,40,44,48,52,56,60,64,100,104,108,112,116,132,136,140,140,149,153,157,161,165, status=200]
2018-08-20 05:47:51.169 [I] [http-nio-127.0.0.1-8011-exec-2] B3000 config read success :
[default15Ghz=36,40,44,48,52,56,60,64,100,104,108,112,116,132,136,140,140,149,153,157,161,165, status=200]
2018-08-20 05:47:57.152 [I] [http-nio-127.0.0.1-8011-exec-3] B3000n config read success :
[default15Ghz=36,40,44,48,52,56,60,64,100,104,108,112,116,132,136,140,140,149,153,157,161,165, status=200]
2018-08-20 05:47:57.478 [I] [http-nio-127.0.0.1-8011-exec-7] B2000 config read success :
[default15Ghz=36,40,44,48,52,56,60,64,100,104,108,112,116,132,136,140,140,149,153,157,161,165, status=200]
2018-08-20 05:47:58.793 [I] [http-nio-127.0.0.1-8011-exec-7] B3000 config read success :
[default15Ghz=36,40,44,48,52,56,60,64,100,104,108,112,116,132,136,140,140,149,153,157,161,165, status=200]
2018-08-20 05:47:59.148 [I] [http-nio-127.0.0.1-8011-exec-7] B3000n config read success :
[default15Ghz=36,40,44,48,52,56,60,64,100,104,108,112,116,132,136,140,140,149,153,157,161,165, status=200]
08/20/18 05:48:11.876 Logfile opened: C:\vocera\logs\bcu-aug-20-18-0548.txt
08/20/18 05:48:11.912 Vocera Badge Configuration Utility 5.3 [Build 359]
08/20/18 05:48:11.912 Copyright 2008-2018 Vocera Communications, Inc.
08/20/18 05:48:11.914 Args:
  
```

The Console displays the message **BCU launched successfully**, and the badge automatically starts the download process.



```

vocera Console Logs
Home
Badges
Console
  Stop BCU
2018-08-20 05:47:16.240 [I] [http-nio-127.0.0.1-8011-exec-1] FrameworkServlet 'dispatcherServlet': initialization started
2018-08-20 05:47:16.266 [I] [http-nio-127.0.0.1-8011-exec-1] FrameworkServlet 'dispatcherServlet': initialization completed in 16 ms
  
```

The Console continues to display messages **Initializing complete in <time taken to complete> ms** after the badge downloads firmware and properties.

- The badge automatically reboots and tries to connect to the network, using the SSID and other network properties that it downloaded. If successful, the badge tries to connect to the Vocera Voice Server that was specified in the **ServerIPAddr**.

2. Validating the Connection

To validate the connection, perform the following tasks:

- Look at the screen of the badge:
 - The message **Logged Out** indicates that the badge is configured properly and has connected to the Vocera Voice Server. Continue configuring the remaining badges. For more information, refer to [Configuring the Remaining Badges](#) on page 28.
 - If the badge does not display **Logged Out** within 30 seconds to one minute, the badge is not configured properly and did not connect to the Vocera Voice Server. Continue troubleshooting the badges. For more information, refer to [Troubleshooting Badge Configuration](#) on page 33.
- Shut down the BPE browser. The session ends.

Maintaining Properties and Firmware

You can use the production Vocera Voice Server to change badge properties or update firmware any time after the initial badge configuration, instead of using the configuration computer.

This is convenient because the Vocera Voice Server can update connected badges automatically, without requiring you to configure them again.

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



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

About Property and Firmware Maintenance

The Vocera Voice Server maintains a copy of the most recent badge firmware in its directory structure.

The locations are as follows:

Badge type	Firmware location
B3000n	<code>\vocera\config\gen3n\badge</code>
B3000	<code>\vocera\config\gen3\badge</code>
B2000	<code>\vocera\config\gen2\badge</code>

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

- Immediately after a badge boots.
When a badge boots, it connects to the Vocera Voice Server. The server compares the badge firmware and properties with its own copies as described in [Updating Properties and Firmware](#) on page 30.
- Immediately after the server starts.
You need to stop the server to install any upgrades or service packs that may contain new firmware. When you restart the server, it compares the badge firmware and properties with its own copies as described in [Updating Properties and Firmware](#) on page 30.

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

Updating Properties and Firmware

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



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

To update properties and firmware:

1. Use the Badge Properties Editor to configure a test badge to confirm that WLAN security settings work properly. For more information, refer to [Configuring a Test Badge](#) on page 26.
If the test badge works properly, you are ready to copy the `badge.properties` file to the Vocera Voice Server to update other badges.
2. Copy the `badge.properties` file in the `\vocera\config` directory on the badge configuration computer to the `\vocera\config` directory on the active Vocera Voice Server.
3. Use the Vocera Control Panel to restart the server, as described in the *Vocera Voice Server Installation Guide*.
4. As badges connect to the server, they synchronize with the Vocera Voice Server, if necessary.
If a badge is offline, it updates as soon as the badge boots and connects to the server.

Using the Badge Background Updater

B3000n, B3000, and B2000 badges can download a firmware upgrade and/or modified settings in the background.

After the files are downloaded, the badge switches to the new firmware image and/or settings automatically.

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

Background Updater and Vocera Clusters

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

During a background update, the badge always download firmware and settings from the active server.

To update the background updater, perform the following tasks:

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




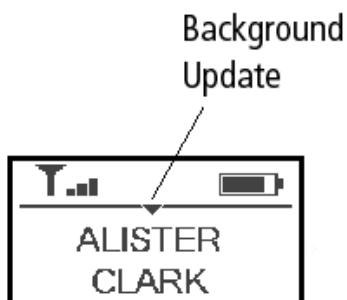
Important: After the Vocera Voice Server starts, it initially comes up as an active node, and then within a minute it rejoins the cluster and performs a remote restore. With a large database, a remote restore can take several minutes.

- e. On the active node, shut down the Vconfig by choosing `Run > Exit`.
A standby node becomes active. Badges connect to it and download new firmware and settings in the background.
- f. Update the remaining Vocera Voice Server.

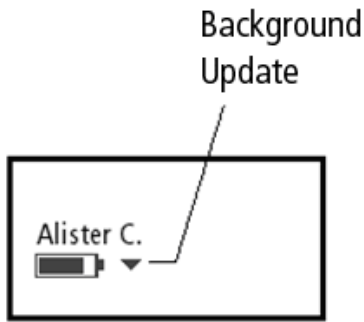
Background Update Status

The background update on the badge is indicated by an update icon.

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



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



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

Using a Badge While a Background Update Is in Progress

All badge functionality is available while a background update is in progress.

If you make or receive a call, the background update is automatically paused so that it does not affect call quality. While background update is paused, the

icon does not appear on the screen. When you finish the call, the background update process resumes and, the



icon appears on screen again until the update is finished.

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

Interrupting a Background Update

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

Troubleshooting Badge Configuration

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

Troubleshooting the Initial Badge Configuration

If you have configured a test badge and the screen of the test badge does not display the “Logged out” message, you need to troubleshoot it.

The badge may not be configured properly, or there may be a problem with some of the other hardware and software you are using.

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

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

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

Badge Message	Typical Problems and Solutions
Searching for access points	<p>The badge cannot connect to an access point on the wireless LAN used by the production server, possibly because:</p> <ul style="list-style-type: none">• The badge is not within range of an access point. If you configured the test badge in a remote area, make sure you are within range of the wireless network, then remove the battery from the badge and insert it again.• The SSID setting of the badge is incorrect.• The security settings of the badge are incorrect. <p>For more information, refer to the B2000 Badge Properties Configuration on page 14, B3000 Badge Properties Configuration on page 16, and B3000N Badge Properties Configuration on page 21 depending on the badge you are configuring.</p>
Requesting IP address	<p>The badge is connected to an access point, but it cannot receive an IP address from a DHCP server, possibly because:</p> <ul style="list-style-type: none">• The security settings of the badge are incorrect. For more information, refer to the B2000 Badge Properties Configuration on page 14, B3000 Badge Properties Configuration on page 16, and B3000N Badge Properties Configuration on page 21 depending on the badge you are configuring.• The DHCP server is not active or cannot be reached from the badge.• The badge is associated with an access point that is not on the production network.
Searching for server	<p>The badge is connected to an access point and has received an IP address, but it cannot connect to the Vocera Voice Server, possibly because:</p> <ul style="list-style-type: none">• The Vocera Voice Server is not running. Ensure that the Vocera Voice Server is running, then remove the battery from the badge and insert it again.• The subnet that the badges are on cannot reach the subnet that the Vocera Voice Server is on. This situation can occur if you have set up an isolated subnet for the badges. Ensure that the switch and router settings allow the badge subnet access to the server subnet, then remove the battery from the badge and insert it again.• The IP address of the Vocera Voice Server that you specified for the badge is incorrect.

For more information on troubleshooting, refer to [Vocera Tech Support Knowledge Base article 1246](#).

Troubleshooting the Badge Property Settings

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

To troubleshoot the badge property settings, perform the following tasks:

1. Display the badge configuration menus.
For more information, refer to [Displaying the Badge Configuration Menu \(Older Software\)](#) on page 34.
2. Reset all the badge properties to the factory default settings.
For more information, refer to [Restoring Factory Default Settings](#) on page 38.
3. Launch the Badge Properties Editor again.
When you launch the Badge Properties Editor after the initial configuration, it reloads your working settings from the `badge.properties` file. For information about launching the Badge Properties Editor, refer to [Using the Badge Properties Editor](#) on page 13.
4. Use the Badge Properties Editor to change the incorrect property values.
For hints about what property values are incorrect, refer to [Troubleshooting the Initial Badge Configuration](#) on page 33. Then change the values as described in [Using the Badge Properties Editor](#) on page 13.
5. Configure the badge by running the Badge Configuration Utility again.
For more information, refer to [Configuring a Test Badge](#) on page 26.

Using the Badge Configuration Menu

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

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

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

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

Displaying the Badge Configuration Menu

Newer badge software provides simplified access to the configuration menu. The configuration menu is hidden to prevent badge users from inadvertently accessing it, yet easy for administrators to display.

To display the badge configuration menu, perform the following tasks:

1. Remove the battery from the badge, then insert it again.
The screen displays the word `vocera`.
2. Press and hold both the `Hold/DND` button (the button on top of the badge) and also the `Call` button (the large button on front of the badge).

When the badge boots, the screen displays the following top-level configuration menu items:

Top-Level Configuration Menu Item

```
APPS & TESTS VERSIONS ALL FILES... REPAIR FILESYSTEM RESTART VBL TO CONSOLE REBOOT BADGE RESET DFLT EAPTLS RESET
DEFAULTS
```

Displaying the Badge Configuration Menu (Older Software)

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

Displaying the Badge Configuration Menu When the hide boot menu is enabled

When the hide boot menu is enabled, the badge configuration menu is not displayed.

To display the badge configuration menu when the Boot Menu is enabled, perform the following tasks:

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

DND Select Select Call Call Select Select Select Call

This sequence consists of clicking the **Hold/DND** button, the **Select** button (the middle button on the side of the badge), and the **Call** button (the big button on the front of the badge). For an illustration showing the button locations [Navigating in the Badge Configuration Menu](#) on page 35.

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

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

Navigating in the Badge Configuration Menu

All the menu items are not visible on the badge at the same time, because the screen of the badge is small.

You can scroll to display more menu items at the same level, or you can select a menu item to view a nested set of items related to the upper-level menu choice. Use the following buttons to navigate in the badge menus:

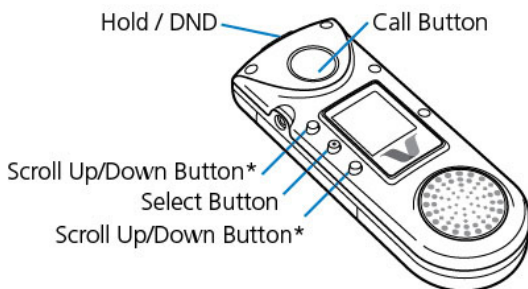
- The **Scroll Up** button (the top button on the side of the B2000 badge and on the front of the B3000n/B3000 badge)
Press this button to scroll up through menu items.



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

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

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



*Up and Down depend on screen orientation

Collecting Badge Data for Troubleshooting

The Vocera Badge Log Collector service and the **Sendlogs** utility allow you to collect all debug information from a B3000n, B3000, or B2000 badge and upload it directly to the Vocera Voice Server computer as a single file.

While the Vocera Badge Log Collector service is running on the Vocera Voice Server, you can use it as an unattended log collection service to collect debug information from multiple badges. If you are working with Vocera Technical Support to troubleshoot problems you are having with a badge, you can send the file containing debug information to Vocera.



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

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

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



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

To collect badge data using the **Sendlogs** utility:

1. On a B3000n or B3000 badge, press and hold the **Select** button for about 10 seconds until the **Sendlogs** utility starts (about 5 seconds on the B2000 badge).

The **Select** button is the middle button of the three small buttons on the front of the B3000n/B3000 badge and on the side of the B2000 badge.



Note: You can start **Sendlogs** when the badge is on a call, but the call will be dropped.

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



Note: You can also launch the **Sendlogs** utility from the badge configuration menu. After you display the configuration menu, choose **APPS & TESTS > SENDLOGS.SH**. For more information, refer to [Using the Badge Configuration Menu](#) on page 34.

Running the Quick Test

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



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

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

- The OLED screen
- The speaker and microphones
- The battery
- The green and amber indicator lights

- The red, green, and blue halo lights (B3000n only)
- The WLAN radio
- The badge's buttons (Call, DND, Up, Select, and Down)

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



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

To run the B3000n/B3000 Quick Test, perform the following tasks:

1. Remove the battery from the badge, then insert it again.
The screen displays the word `vocera` and proceeds to count from 1 to 6.
2. When the screen reaches 6, press and hold the `Call` button (the large button on the front of the badge) for about 5 seconds. When you see patterns on the OLED screen, the Quick Test has started and you can release the `Call` button.
3. The Quick Test proceeds through the following tests:
 - a. **OLED test:** When the OLED test starts (the pixels will go from off to on), make sure you remove your fingers from the microphones because the audio test starts next. You must watch the OLED screen during the test to identify any problems; the Quick Test will not report an OLED failure. What sort of problems should you look for? Check to see whether a significant portion of the screen is on or off at all times, which would interfere with your ability to read the screen.
 - b. **Audio test:** Be quiet during the audio test. Sound will play for 5 seconds, and the screen will indicate whether the four microphones are working.
 - c. **Battery test:** Shows information about the battery temperature, voltage, current, and power.
 - d. **LED test:** You must watch the green and amber lights to identify any problems. Make sure they turn on and off.
 - e. **Halo test:** Watch the halo lights to identify any problems. Make sure they turn on and off (B3000n only).
 - f. **WLAN test:** Shows the radio configuration, AP table, and IP table. The badge will associate with an AP, and, if using DHCP, request an IP address.
 - g. **Button test:** Prompts you to press and release each of the buttons to make sure they are working.
4. When you are finished with the button test, press and hold the `Call` button to exit the Quick Test.
5. After the badge restarts, you can send logs of the Quick Test to the server using the `SendLogs` utility.



Note: If the Quick Test reports that one or more of the microphones has failed, you may have inadvertently covered the microphones with your fingers while holding the badge. Try running the Quick Test again, and this time be careful not to cover the microphones.



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

Repairing the File System

The B3000n/B3000 badge is designed to automatically recover from problems that may occur with its file system. Despite this safeguard, in very rare circumstances one or more files on a badge may become corrupted. When this happens, your badge may continuously reboot, or a badge program may not start.

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



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

To correct a problem with a corrupted file, and run the `REPAIR FILESYSTEM` utility, available on the badge configuration menu, perform the following tasks:

1. Display the badge configuration menu.
For more information, refer to [Using the Badge Configuration Utility](#) on page 28.

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

Restoring Factory Default Settings

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

After you restore factory default settings on the badge, it automatically connects to the machine running the Badge Configuration Utility when it powers up.

To reset to factory setting, perform the following tasks:

1. Display the badge configuration menu.
For more information, refer to [Using the Badge Configuration Menu](#) on page 34.
2. Scroll down and select the **RESET DEFAULTS** menu item.
The screen displays a confirmation menu.
3. Select **YES - RESET!**
Any existing badge property values are erased, and the factory default values are restored. The badge reboots and tries to connect to the configuration computer at the IP address 10.0.0.1.



Note: If the Badge Configuration Utility is running, the badge automatically downloads the current property values when it reboots. If you are not ready to download properties, make sure you exit the Badge Configuration Utility before resetting the badge defaults.

4. When you see the Vocera splash screen, remove the battery from the badge.

Restoring a Badge to its Factory Image

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

Restoring the B3000n/B3000 Factory Image

To restore the factory image of B3000n/B3000, perform the following tasks:

1. Ensure that you start with a fully charged battery.
2. Remove the battery from the badge.
3. Press and hold the Select button, and then insert the battery again.
The Badge U-boot screen appears.
4. Press the Hold/DND button to see the factory reset menu.
The badge prompts, *Reset badge?*
5. Press the Select button to confirm that you want to restore the factory image on the badge. Otherwise, press any other button to cancel restoring the factory image.

Once you confirm, the badge displays the following prompt: "Warning: Leave the badge powered on for 10 min and wait. Do not interrupt."

6. When the update is finished, the default settings are restored and the badge can be configured again.

Restoring the B2000 Factory Image

To restore the factory image of B2000, perform the following tasks:

1. Ensure that you start with a fully charged battery.
2. Remove the battery from the badge.
3. Press and hold the **Select** button, and then insert the battery again. The badge menu appears, and the badge performs a quick test.
4. Wait a couple seconds until the test is complete.
5. Press the **Hold/DND** button to see the factory reset menu. The badge prompts, "Reset badge?"
6. Press the **Select** button to confirm that you want to restore the factory image on the badge. Otherwise, press any other button to cancel restoring the factory image.

Once you confirm, the badge displays the following prompt: "Warning: Leave the badge powered on for 10 min and wait. Do not interrupt."

7. Wait a few minutes until the badge displays the following prompt: **WAITING AT IP ADDR 10.213.213.213** . At this point, the badge does not have any proper settings.
8. Restore the default settings on the badge so that you can configure it again. For more information, refer to [Restoring Factory Default Settings](#) on page 38.