stryker

Vocera Device Configuration Guide

Version 5.3.3

Notice

Last modified: 2023-02-21 12:45

VS-533-Docs build 330

Contents

Introduction

This section introduces you to the details covered in this document, product applicability, configuration hardware requirements, and 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 (BPE) and Badge Configuration Utility (BCU).

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 up your network environment, details on specific device features, or commands. For a complete description of these topics, refer to Vocera B-Series Badge Guide and Vocera Infrastructure Planning Guide.

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

Product Applicability

This section describes the applicable products and the supported firmware releases.

Vocera Firmware	Supported Devices
Up to Firmware Release 5.0.3 and 5.1.1	B3000, B3000n, and V5000

Configuration Hardware Requirements

Vocera requires specific hardware to set up the device.

The following table provides details of the hardware required:

Component	Requirement
Configuration Computer	A dedicated computer that runs the 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 network of the site.

Component	Requirement
Cable	An Ethernet crossover cable to connect the configuration computer and the access point.

Related Documentation

The documents supporting the Vocera Device Configuration Guide are listed in this topic.

The following documents support the Vocera Device Configuration Guide:

- Vocera Infrastructure Planning Guide—Specifies the recommended configuration of infrastructure to support Vocera. You can also refer to the security information in this document.
- Vocera B-Series Badge User Guide—Specifies the Badge features and commands.
- Vocera V-Series Smartbadge User Guide—Specifies how to use your Vocera Smartbadge It starts with the basics, such as placing and receive calls. It also helps you understand how to use the Smartbadge features.
- Vocera Voice Commands Reference Guide—Specifies the details of the voice commands that you can use on your Vocera device and smartphones to communicate.
- Vocera Device Safety and Regulatory Guide—Specifies the safety details for electrical, magnetic, radio, wireless, chemical, chargers, along with your power supply safety.

Device Configuration Workflow

This section provides a workflow to configure devices.

To set up devices 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 8.
   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 device. For more information, refer to Installing Badge Configuration Utilities on page 8.
   b. **Specifying TCP/IP Properties**—Specify TCP/IP properties in the configuration computer to allow a new device to connect to it. For more information, refer to Specifying TCP/IP Settings on page 13.
   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 13.
2. **Configuring a New Device**—After you set up the configuration computer, you must specify properties for your device before it can communicate with your network. You can then configure a test device.
   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 15.
   b. **Configuring a Test Device**—Set up a single test device to confirm that it connects to the network the way you intended. For more information, refer to Configuring a Test Device on page 34.
3. **Configuring the Remaining Devices**—After you have successfully configured and tested one device, configure the remaining devices 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 devices. For more information, refer to Using the Badge Configuration Utility.

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 a supported version of 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 5400 and 5555.

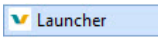
Installing Badge Configuration Utilities

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

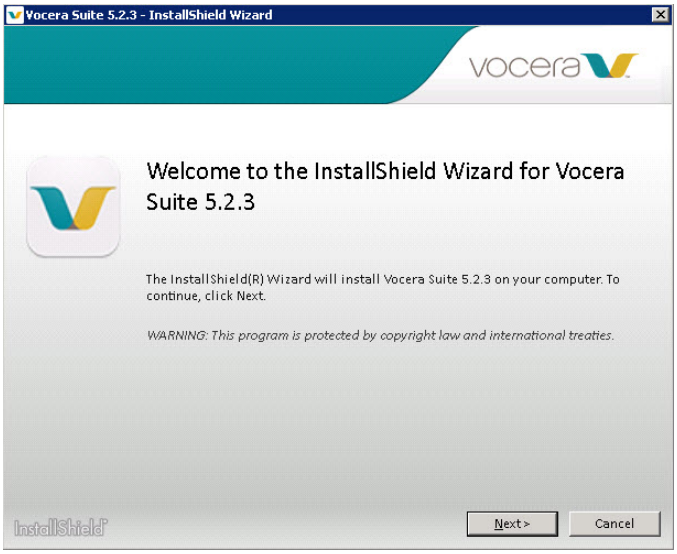
If the Badge Configuration Utilities (BCU) from a previous version of Vocera is installed on the configuration computer, remove it before installing the current Badge Configuration Utility. Vocera does not support more than one version of the Badge Configuration Utilities on a configuration computer. 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.

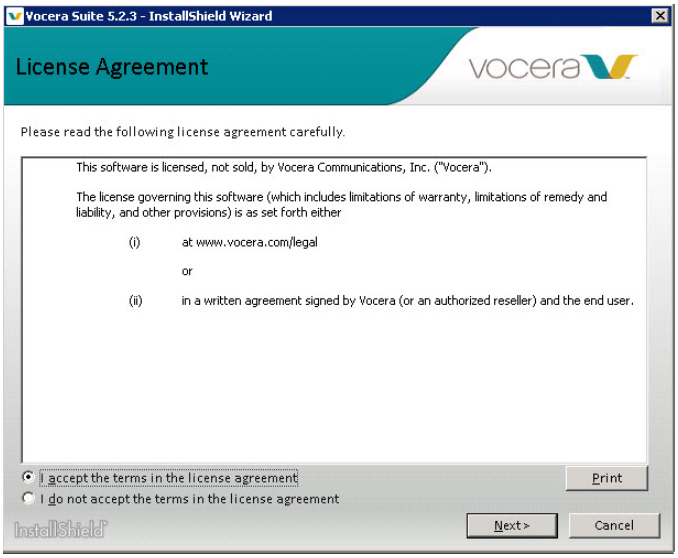
   

   The Welcome window is launched.
3. Click **Next** to continue with the installation program.



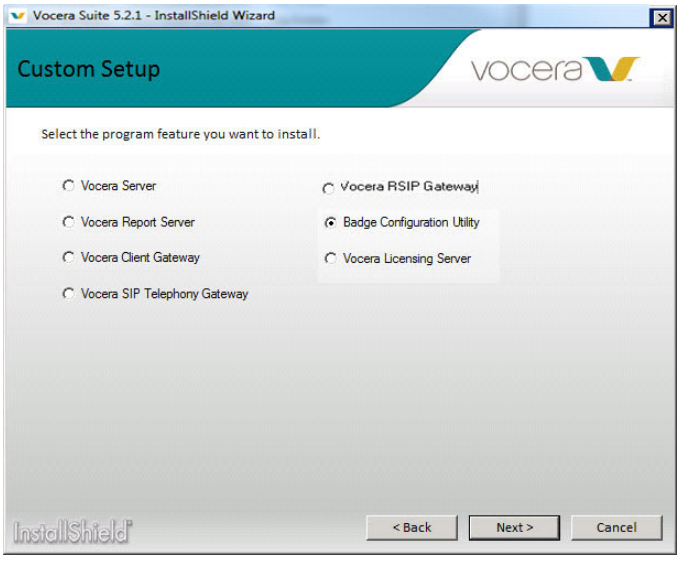
The License Agreement window is displayed.

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



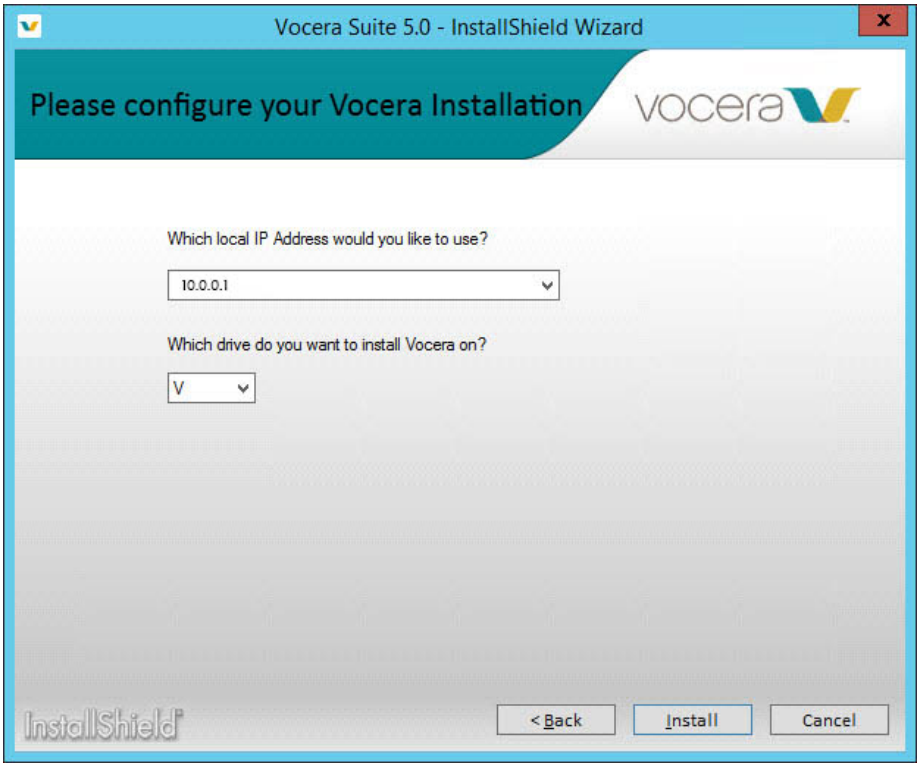
The Custom Setup Window opens.

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

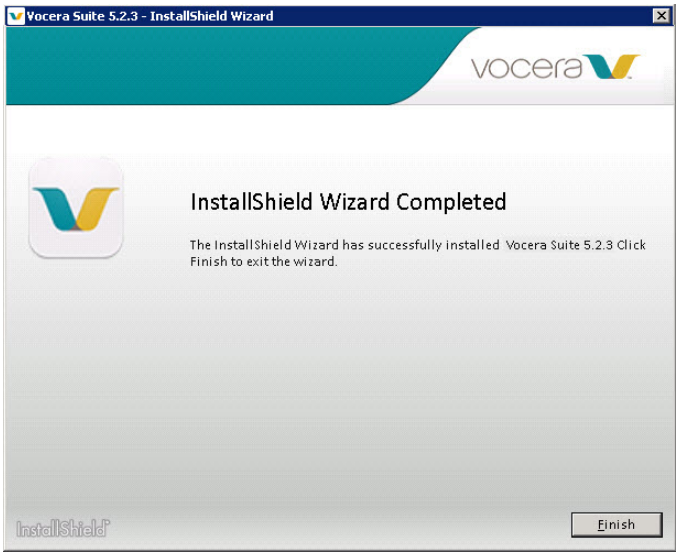


The **Installation Configuration** window is displayed.

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 message appears displaying 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 `filelist` to determine the list of 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 `filelist` to determine the list of files to download to a B3000 badge.
B3000n	
gen3n	Directory containing B3000n firmware, resources, and related files.

Item	Description
gen3n\metadata\filelist	Auto-generated text file, created by both the Badge Configuration Utility and the Vocera Voice Server, contains the complete list of files for B3000n firmware. The Badge Configuration Utility and the Vocera Voice Server use `filelist` to determine the files to download to a B3000n badge.
profiles.txt	For B3000n, a text file, is generated by the Badge Properties Editor at `gen3\badge\config` when you create dynamic wireless profiles for the badge. The `profiles.txt` 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 `badge.properties` file and based on selections made when you create a new profile using the Badge Properties Editor user interface. **Note:** Vocera recommends that you do not edit these files manually.
V5000	
gen5	Directory containing V5000 firmware, resources, and related files.
gen5\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 V5000 firmware. The Badge Configuration Utility and the Vocera Voice Server use `filelist` to determine the files to download to a V5000 badge.
Common Files	
lib	Directory containing the Badge Configuration Utility and the Badge Properties Editor applications.
badge.properties	A text file, is generated by the Badge Properties Editor at `<gen3/gen3n/v5000>\badge\config` contains properties that determine badge behavior. **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. For B3000n badges, use the `profiles.txt` files for environments that require more than one wireless profile in a dynamic campus-type setting.

Each B3000n 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.

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 because 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 on the version of the operating system. Refer to your Windows documentation for complete information.

For 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 searches for a computer with this address that executes the Badge Configuration Utility.
2. Set the **Subnet mask** to 255.0.0.0.

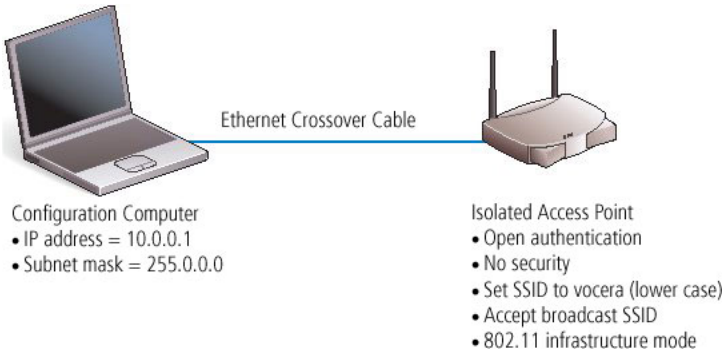
Note: The exact procedure for setting your TCP/IP properties depends on the version of the operating system. Refer to your Windows documentation for more information.

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).

Note: The prefered IP address of the AP is 10.0.0.<x> series to connect with the IP address of the configuration computer .

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 are shipped from the factory, the 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 Device

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

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*	Specifies the IP address of the computer that runs the Vocera Voice Server. This is a required field. Use dotted-decimal notation to specify this value. For example, `192.168.3.7`. If you are configuring a cluster, enter the IP address of each machine in the cluster, separated by commas, with no spaces. **Note:** Do not enter more than four comma-separated IP addresses. The Vocera Voice Server supports a maximum of four cluster nodes.
SSID*	Specify an SSID other than vocera (all lower-case) for your production server. Badges are factory-programmed to use the vocera SSID to establish a wireless connection to the configuration computer that you have set up for your Vocera system.
Hide Boot Menus	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. **Note:** This property is ignored by the B3000 and B3000n badges, with menus always hidden.
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.
WPA-PSK	Specifies that your wireless network uses the WiFi Protected Access Pre-Shared Key protocol for authentication.
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.
Username and Password*	Enter appropriate values in the **Username** and **Password** fields if your network uses either LEAP, WPA-PEAP, or EAP-FAST authentication. 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. 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 domain \ userid in the **Username** field, where domain is a Windows domain name and userid identifies the user. Other RADIUS servers may require the username only. The password value is case sensitive. You can use initial or embedded spaces in either of these values; trailing spaces cause an error message when the values are saved. The badge supports a maximum of 128 alphanumeric characters for the **Username** and 32 alphanumeric characters for the **Password**. In addition, the badge supports the following characters for LEAP passwords: `^ # ! * @ % & $` **Note:** If you are using EAP-FAST authentication and you change the 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.
Encryption Type	The encryption types available are: • 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 Use hexadecimal characters to enter the key that the access point uses.
Wireless Settings	

Fields	Description
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.
B2.ClosedMenus	Specifies whether the badge configuration menus are hidden, or if they can be easily accessed through the DND button: • **FALSE** specifies that you can access the configuration menus by pressing the DND button. Within three seconds, 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	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. • **FALSE** specifies that U-APSD is disabled. • **TRUE** specifies that U-APSD is enabled. 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.

Fields	Description
B2.EnableWMM	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 • **FALSE** specifies that 802.11e QoS is disabled. • **TRUE** specifies that 802.11e QoS is enabled. 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.
B2.InstallDone	Specifies whether the Badge Properties Editor has performed the initial configuration for a badge: • **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	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.
B2.ResetVolumeToDefault	Specifies whether the badge resets the volume to the default at boot-up. • **FALSE** specifies that the badge maintains the previous volume setting at boot-up. • **TRUE** specifies that the badge resets the volume to the default at boot-up.
B2.SubnetMask	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.
B2.SubnetRoaming	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.

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.

Fields	Description
Create Profile	Allows you to create a new profile to control general behavior.
General Settings	
Server IP Address*	Specifies the IP address of the computer that runs the Vocera Voice Server. This is a required field. Use dotted-decimal notation to specify this value. For example, `192.168.3.7`. If you are configuring a cluster, enter the IP address of each machine in the cluster, separated by commas, with no spaces. **Note:** Do not enter more than four comma-separated IP addresses. The Vocera Voice Server supports a maximum of four cluster nodes.
SSID*	Specify an SSID other than vocera (all lower-case) for your production server. Badges are factory-programmed to use the vocera SSID to establish a wireless connection to the configuration computer that you have set up for your Vocera system.
Hide Boot Menus	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. **Note:** This property is ignored by the B3000 and B3000n badges, with menus always hidden.
Group Mode	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. Uncheck this option if you want to eliminate background noise when users are on a call. **Note:** B3000 and B3000n users can change the Group Mode setting on their badges, overriding the default. • For B3000: Group Mode is always off during Genie interactions and broadcasts. • For B3000n: Group Mode is automatically enabled when the badge is turned to a 105-degree angle to improve voice recognition.
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*	Enter appropriate values in the **Username** and **Password** fields if your network uses either LEAP, WPA-PEAP, or EAP-FAST authentication. 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. 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 domain \ userid in the **Username** field, where domain is a Windows domain name and userid identifies the user. Other RADIUS servers may require the username only. The password value is case sensitive. You can use initial or embedded spaces in either of these values; trailing spaces cause an error message when the values are saved. The badge supports a maximum of 128 alphanumeric characters for the **Username** and 32 alphanumeric characters for the **Password**. In addition, the badge supports the following characters for LEAP passwords: `^ # ! * @ % & $` **Note:** If you are using EAP-FAST authentication and you change the 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.
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	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." **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 to be reconfigured. To take advantage of this feature, you must also select EAP-FAST authentication.

Fields	Description
Auto-PAC Provision Retry Count	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. If a badge exceeds the retry count, it displays the following message: `Too many retries for Auto-PAC provisioning`. By default, this property is set to 0 (indicates no retries). To take advantage of this feature, you must also select EAP-FAST authentication.
EAP-TLS	Specifies that your wireless network uses Extensible Authentication Protocol-Transport Layer Security for authentication. 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. 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 Vocera Device Configuration Guide.
Use Custom EAP-TLS Certificates	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. 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. This property is available only when the **Authentication** property is set to EAP-TLS.
Encryption Type	The encryption types available are: • TKIP-WPA—Specifies your network uses TKIP as defined by WPA. • AES-CCMP—Specifies your network uses AES-CCMP as defined by WPA2 Use hexadecimal characters to enter the key that the access point is using.
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.

Fields	Description
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	
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: • **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. • **FALSE** specifies that U-APSD is disabled. • **TRUE** specifies that U-APSD is enabled. 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.

Fields	Description
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. • **FALSE** specifies that 802.11e QoS is disabled. • **TRUE** specifies that 802.11e QoS is enabled. 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.
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: • **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. • **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.
B3.SubnetRoaming	Specifies whether users can roam across subnet boundaries while using badges. If subnet roaming is enabled, a badge automatically obtains a new IP address as a badge user makes the transition to an access point on a different subnet. If you enable subnet roaming, you must use a DHCP server to supply your IP addresses. **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. **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.

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*	Specifies the IP address of the computer that runs the Vocera Voice Server. This is a required field. Use dotted-decimal notation to specify this value. For example, `192.168.3.7`. If you are configuring a cluster, enter the IP address of each machine in the cluster, separated by commas, with no spaces.  **Note:** Do not enter more than four comma-separated IP addresses. The Vocera Voice Server supports a maximum of four cluster nodes.
SSID*	Specify an SSID other than vocera (all lower-case) for your production server. Badges are factory-programmed to use the vocera SSID to establish a wireless connection to the configuration computer that you have set up for your Vocera system.
Hide Boot Menus	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.  **Note:** This property is ignored by the B3000 and B3000n badges, with menus always hidden.
Group Mode	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. Uncheck this option if you want to eliminate background noise when users are on a call.  **Note:** B3000 and B3000n users can change the Group Mode setting on their badges, overriding the default. • For B3000: Group Mode is always off during Genie interactions and broadcasts. • For B3000n: Group Mode is automatically enabled when the badge is turned to a 105-degree angle to improve voice recognition.
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	
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	

Fields	Description
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*	Enter appropriate values in the **Username** and **Password** fields if your network uses either LEAP, WPA-PEAP, or EAP-FAST authentication. 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. 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 domain \ userid in the **Username** field, where domain is a Windows domain name and userid identifies the user. Other RADIUS servers may require the username only. The password value is case sensitive. You can use initial or embedded spaces in either of these values; trailing spaces cause an error message when the values are saved. The badge supports a maximum of 128 alphanumeric characters for the **Username** and 32 alphanumeric characters for the **Password**. In addition, the badge supports the following characters for LEAP passwords: `^ # ! * @ % & $` **Note:** If you are using EAP-FAST authentication and you change the 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.
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.

Fields	Description
Provision Auto-PAC on Expire	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."  **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 to be reconfigured. To take advantage of this feature, you must also select EAP-FAST authentication.
Auto-PAC Provision Retry Count	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. If a badge exceeds the retry count, it displays the following message: `Too many retries for Auto-PAC provisioning`. By default, this property is set to 0 (indicates no retries). To take advantage of this feature, you must also select EAP-FAST authentication.
EAP-TLS	Specifies that your wireless network uses Extensible Authentication Protocol-Transport Layer Security for authentication. 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. 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 Vocera Device Configuration Guide.
Use Custom EAP-TLS Certificates	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. 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. This property is available only when the **Authentication** property is set to EAP-TLS.
Encryption Type	The encryption types available are: • TKIP-WPA—Specifies your network uses TKIP as defined by WPA. • AES-CCMP—Specifies your network uses AES-CCMP as defined by WPA2 Use hexadecimal characters to enter the key that the access point is using.

Fields	Description
Wireless Settings	
Wireless Band	Select the wireless bands used by the B3000n badge: • **ABGN**—Uses all 802.11 wireless bands (a, b, g, and n) at 2.4 GHz and 5 GHz. This is the default setting. • **AN**—Uses 802.11a and 802.11n wireless bands at 5 GHz. • **BGN**—Uses the 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)	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.
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.
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	Check **802.11w** box to support protected management frames. The options available are: • Disable • Optional • Mandatory **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. Enable 802.11w for WPA2-PSK-SHA256 profile to work.
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.

Fields	Description
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	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.
Custom Settings	
B3N.BroadcastUsesIGMP	Vocera broadcast is implemented as IP Multicast. If broadcast commands need to cross a subnet, IGMP must be supported in the switch or router, and this property must be set to `TRUE`. The B3000n badge auto-detects IGMP and changes its mode dynamically if IGMP is enabled in the infrastructure. Consequently, this property is deprecated in the B3000n badge.
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	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. • `FALSE` specifies that U-APSD is disabled. • `TRUE` specifies that U-APSD is enabled. To take advantage of this standard, your access points must also support it. **Important:** Both the `B3N.EnableAPSD` and `B3N.EnableWMM` properties must be set to the same value. The firmware and chip set changes in the B3000n badge make this property unnecessary. Consequently, this property is deprecated in the B3000n badge.
B3N.EnableWMM	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. • `FALSE` specifies that 802.11e QoS is disabled. • `TRUE` specifies that 802.11e QoS is enabled. 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. 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.
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.

Fields	Description
B3N.InstallDone	Specifies whether the Badge Properties Editor has performed the initial configuration for a badge: • `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	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. An access point broadcasts a management frame called a beacon at a fixed interval (required to be set to 100 ms by Vocera).
B3N.ResetVolumeToDefault	Specifies whether the badge resets the volume to the default at boot-up. • `FALSE` specifies that the badge maintains the previous volume setting at boot-up. • `TRUE` specifies that the badge resets the volume to the default at 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	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.
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.

V5000 Smartbadge Properties Configuration

This section lists the Smartbadge properties that you can configure using the BPE on your V5000 Smartbadge.

Enter information or check the following Smartbadge properties:

Fields	Description
Profiles	
Selected Profiles	Specifies the name of the profile you have 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*	Specifies the IP address of the computer that runs the Vocera Voice Server. This is a required field. Use dotted-decimal notation to specify this value. For example, `192.168.3.7`. If you are configuring a cluster, enter the IP address of each machine in the cluster, separated by commas, with no spaces. **Note:** Do not enter more than four comma-separated IP addresses. The Vocera Voice Server supports a maximum of four cluster nodes.
SSID*	Specify an SSID other than vocera (all lower-case) for your production server. Badges are factory-programmed to use the vocera SSID to establish a wireless connection to the configuration computer that you have set up for your Vocera system.
Display Bluetooth Settings	Check the **Display Bluetooth Settings** box to display the Bluetooth configuration menu on the Smartbadge.
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.
WPA-PSK	Specifies that your wireless network uses the WiFi Protected Access Pre-Shared Key protocol for authentication.
WPA-EAP	Specifies that your wireless network uses the Wiki Protected Access Extensible Authentication Protocol for authentication. If this authentication type is set, EAP method options appear.
FT-PSK	Specifies that your wireless network uses the Fast Transition Pre-Shared Key protocol for authentication.
FT-EAP	Specifies that your wireless network uses the Fast Transition Extensible Authentication Protocol for authentication. If this authentication type is set, EAP Method options appear.
WPA-PSK-SHA256	Specifies that your wireless network uses the WiFi Protected Access Pre-Shared Key protocol with SHA-256 cryptographic hash functions for authentication.
WPA-EAP-SHA256	Specifies that your wireless network uses the WiFi Protected Access Extensible Authentication Protocol with SHA-256 cryptographic hash functions for authentication.

Fields	Description
	If **Authentication Type** is set to WPA-PSK, FT-PSK, WPA-PSK-SHA256, and WPA-EAP-SHA256, the pre-shared field appears. The pre-shared key that the badge supplies for authentication is a 64-character, hexadecimal value.
EAP Method	
TLS	Specifies that your wireless network uses Extensible Authentication Protocol-Transport Layer Security for authentication.
PEAP	Specifies that your wireless network uses the WiFi Protected Access Protected Extensible Authentication Protocol for authentication. The provisioning fields displayed are: • PEAP V0 • PEAP V1
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. The provisioning fields displayed are: • Disabled/manual • Unauthenticated • Authenticated • Unauthenticated and Authenticated
LEAP	Specifies that your wireless network implements the Cisco LEAP protocol for authentication.
Encryption Type	The encryption type available is • AES-CCMP—Specifies your network uses AES-CCMP as defined by WPA2
Username and Password*	Enter appropriate values in the **Username** and **Password** fields if your network uses either LEAP, WPA-PEAP, or EAP-FAST authentication. 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. 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 domain \ userid in the **Username** field, where domain is a Windows domain name and userid identifies the user. Other RADIUS servers may require the username only. The password value is case sensitive. You can use initial or embedded spaces in either of these values; trailing spaces cause an error message when the values are saved. The badge supports a maximum of 128 alphanumeric characters for the **Username** and 32 alphanumeric characters for the **Password**. In addition, the badge supports the following characters for LEAP passwords: `^ # ! * @ % & $` **Note:** If you are using EAP-FAST authentication and you change the 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.
Wireless Settings	
Wireless Band	Select the wireless bands used by the V5000 Smartbadge:

Fields	Description
	• **ABG**—Uses all 802.11 wireless bands (a, b, and g) at 2.4 GHz and 5 GHz. This is the default setting. • **A**—Uses the 802.11a wireless band at 5 GHz. • **BG**—Uses the 802.11b and 802.11g wireless bands at 2.4 GHz. **Note:** 802.11n and 802.11ac are enabled by default on the Vocera device. If the infrastructure does not support 802.11n or 802.11ac, the device radio automatically falls back to use legacy 802.11abg protocol.
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.
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** box to discover the best available access point. Vocera recommends enabling this option to advertise channels of both the bands.
OKC	Check the **OKC** box to enable authentication between multiple APs in a network when APs are under common administrative control.
802.11w	Check **802.11w** box to support protected management frames. The options available are: • Disable • Optional • Mandatory **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. Enable 802.11w for WPA2-PSK-SHA256 profile to work.
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, 144, 149, 153, 157, 161, 165)	Specifies the option to force V5000 Smartbadges 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, 144, 149, 153, 157, 161, 165.
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	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 3.
Custom Settings	

Fields	Description
V5.EnableConsoleLog	Specifies the option to enable or disable console log. Set the value to `FALSE`.
V5.MinimumVolume [0-6]	Specifies the option to enable volume to be set to 0 for all incoming calls, pages, alerts, and messages.
V5.EventDisplayActivate	Specifies the option to activate display notification based on incoming events. If the "Raise to Wake" option is also enabled on your Smartbadge, the badge property `V5.EventDisplayActivate` directly opens the notification. The default value of the property is `true`.
V5.EnableHotwordLedIndication	Specifies the option to enable or disable LED indication when hotword detection is active, and the screen is turned off. Set the value to `TRUE` to enable LED indication. Set the value to `FALSE` to disable LED indication.
V5.ForceIGMPVersion	Specifies the option for the Smartbadge to negotiate IGMP version to be used in the network. Default version is 3 and is backward compatible with version 1 and version 2.
v5._EnableDigitalHS_	Specifies the option for the Smartbadge to detect or not detect the USB-C Digital headset. The default value is false. Analog headsets continue to work as before regardless of the digital headset property.
V5.EnableHotword	Specifies the option to enable the voice command "OK Vocera" to initiate a Genie call. When the option is enabled, the V5000 Smartbadge listens for a spoken phrase. When that phrase is detected, the V5000 initiates a call to the Genie. The default value of the property is `false`.
V5.DirectCallEnabled	Specifies the option to enable direct calling. Set the value to true to enable direct calling. The default value of the property is `false`.
V5.ChannelsToScan	Specifies the list of channels to be scanned in 2.4GHz and 5GHz band together. Use this property to specify scan channels. If you do not specify channel numbers all the channels are automatically scanned. Vocera recommends using this badge property for scanning. For example: 36, 40, 44, 48, 149, 153, 157, 161, and 165.
V5.EnableAutoHandsetModeFt	Specifies the option to expose automatic handset mode. You can enable or disable automatic handset mode from the badge settings menu if the feature is enabled using the badge property. The option is set after the call is established and is active only when the badge is in the regular speaker mode. This feature is disabled for headset mode. If you take the device away from the ear during the call, the call remains in handset mode. You can use the screen options to change back to the handsfree mode when needed. The device returns to the handsfree mode after the call ends.
V5.UseSHA2cert	Specifies the option to switch between the SHA1 certificate and the new Vocera SHA2-256 certificate with 2048 bit RSA encryption. The default value is `V5.UseSHA2cert` is `true`.

Configuring a Test Device

Set up a single test device to confirm that it connects to the network the way you intended, and troubleshoot your `badge.properties` file as needed. Subsequently, configure the remaining devices.

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

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

To configure a test device, perform the following tasks:

1. Locate and double-click the Vocera **Badge Property Editor** Launcher file on the desktop and click **Start BCU**.
2. Attach a charged battery to a new device (a device that has never been configured).

   A new device automatically locates 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 device.

   The Badge Configuration Utility continues to display messages as it downloads the firmware and properties. When the download is complete, the device 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 device:
   - The message "Logged Out" indicates that the device is configured properly and has connected to the Vocera Voice Server.
     Continue with Configuring the Remaining Devices on page 37.
   - If the device does not display "Logged Out" within 30 seconds to one minute, the device is not configured properly and did not connect to the Vocera Voice Server.
     Continue with Troubleshooting Device Configuration on page 50.
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 Vocera Voice Server.
6. Perform one of the following:
   - If your Vocera Voice Server is running, stop it and then restart it to load the `badge.properties` file into memory.
   - If your 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.

Note: Assigning static IP addresses manually to badges is a slow and potentially error-prone process. 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 15.
4. Under **Custom Setting**, click **New** and enter the following properties:

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
V5000	V5.ConfigStaticIP V5.BadgeIPAddr V5.SubnetMask V5.GatewayIPAddr V5.DNS1IPAddr

   For more information on the badge properties, refer to Custom Settings section of , B2000 Badge Properties Configuration on page 16, B3000 Badge Properties Configuration on page 19, and B3000N Badge Properties Configuration on page 24 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 Devices

After you have successfully configured and tested one device, you can configure the remaining devices for your site.

The procedure for configuring these devices is the same as the procedure described in Configuring a Test Device. Use the Badge Configuration Utility to connect to each of your remaining devices.

Using the Badge Configuration Utility

Badge Configuration Utility is used with new devices. Hence it must run on a stand-alone configuration computer. Each device 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 device that have never been configured.
- Devices that have been reset to factory defaults.

For more information, refer to Restoring Device Factory Default Settings.

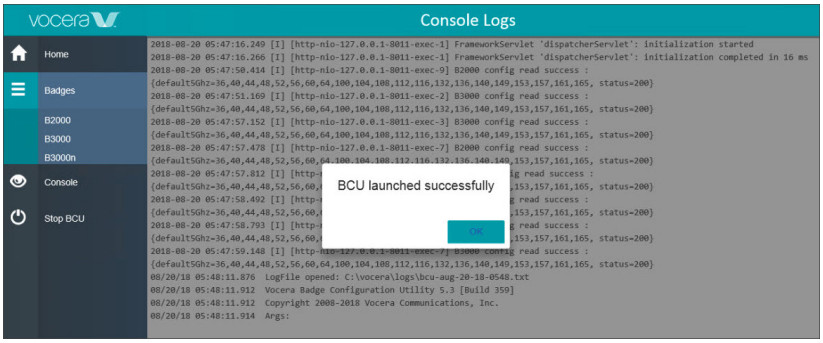
After the device downloads its properties and firmware, it reboots and attempts to connect to the network using the property values it has downloaded. If it connects to the network successfully, it then attempts to connect to the Vocera Voice Server.

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

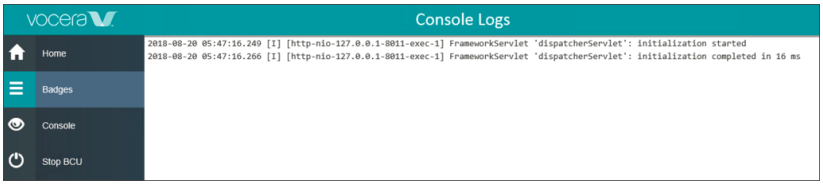
Running the Badge Configuration Utility

You can configure the remaining devices 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 device that has been reset to factory defaults.
   The device 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**.



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



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

4. 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:

5. Look at the screen of the device:
   - The message `Logged Out` indicates that the badge is configured properly and has connected to the Vocera Voice Server.
     Continue configuring the remaining devices. For more information, refer to Configuring the Remaining Devices on page 37.
   - If the device does not display `Logged Out` within 30 seconds to 60 seconds, 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 Device Configuration on page 50.

6. Shut down the BPE browser.
   The session ends.

Using Security Certificates

Using Security Certificates (SSL) is important to protect server-client communication. Installing SSL enables encrypting every bit of information. This section helps you understand security certificates and how to use them.

Security Certificates Overview

A public-key certificate or a digital security certificate is an electronic means that identifies a public key to a particular individual or an organization.

You could obtain a security certificate, by using your own certificate authority server (CA server) or by depending on an independent CA.

The certificate contains information about the identity of the user. For example, name, email address, the date the certificate was issued, and the name of the CA issuing the certificate. This is generally in the case of email encryption, code signing, and e-signature systems.

Transport Layer Security (TLS), typically has a computer or other device as the subject of the certificate. TLS is also called Secure Sockets Layer (SSL) and is known for being a part of the HTTPS protocol for securely browsing the web.

If you use custom Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) certificates, you must generate your self-signed certificates or obtain them from a trusted Certificate Authority (CA). In this case, 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.

Alternatively, you can use the Vocera Manufacturer Certificates. Vocera devices 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 1024, 2048, 4096, 7192, and 16384-bit keys 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 device, you still need to install Vocera Voice Server-side certificates on your authentication server. For more information, refer to Using External Certificates.

Certificate Authority Server

CA servers are built for identity management. It helps you create and store key pairs for encryption, decryption, signatures, and validation.

The CA generates a root certificate for digitally signing, signing firmware updates, code, and so on that require a digital signature.

Certificate Signatures

Vocera CA issues a certificate using hashing to generate a digest and then creates a certificate by encrypting the digest with its private key.

Hashing is a method used to obtain a hash, also known as the digital fingerprint of a message. The hash codes are unique and have a fixed length of 128 or 160 bits. Some examples are Message Digest 5 (MD5) and Secure Hash Algorithm. Vocera supports both Secure Hash Algorithm 1 (SHA-1) and (SHA-2). SHA-1 and SHA-2 are two different versions of the Secure Hashing Algorithm, and SHA-2 is an improvised version of SHA-1.

They differ in the following aspects:

- The way hash is created from the original data.
- The bit-length of the signature. SHA-1 is a 160-bit hash, and SHA-2 is a group of hashes and are created in a variety of lengths. The most popular hash is 256-bits.

Public Key Infrastructure

Public Key Infrastructure (PKI) helps organizations safeguard the identities of their users. It provides users with robust encryption, network authentication, and wireless network access.

PKI uses a sophisticated method of encrypting and decrypting information that supports the distribution, revocation, and verification of public keys used for encryption. It enables linking of identities with public key certificates. A PKI enables users and systems to securely exchange data over the internet and verify the authenticity of certificate-holding entities.

PKI supports the following high-level features:

- Generate a public-private key pair.
- Validate a certificate path

Configuring Device EAP-TLS Authentication Certificates

Vocera device supports EAP-Transport Layer Security or EAP-TLS, which provides excellent security, relying on the client and server-side certificates.

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

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

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

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

For more information, refer to the respective vendor documentation.

The security properties you need to specify for EAP-TLS vary depending on whether you choose to use Vocera Manufacturer Certificates or custom EAP-TLS certificates. For more information, refer to the **EAP Configuration Overview** section of the Vocera Infrastructure Planning Guide.

Using Vocera Manufacturer Certificates

You can use the Vocera Manufacturer Certificates if you do not want to manage EAP-TLS certificates for B3000, B3000n, and V5000 devices. Vocera Manufacturer Certificates are provided for client and server certificates.

Vocera Manufacturer Certificates use 2048-bit RSA keys, which provide excellent security for enterprise and conform to industry standards and National Institute of Standards and Technology (NIST) recommendations.

Vocera devices are preconfigured with EAP-TLS client certificates. They are automatically downloaded from the Vocera Voice Server or the configuration computer. However, you need to install Vocera server certificates on your authentication server.

To configure your authentication server for EAP-TLS using Vocera Manufacturer Certificates, perform the following:

1. Locate the following client certificates in the `\vocera\config\<gen3\gen3n\gen5>\badge\res\certificates\EAP-TLS\vi`.
   The following certificates are present:
   - `c_p#`This file is a root CA certificate.
   - `a_d#`This file is a client certificate.
   - `b_p#`This file is a client key.
2. Install all of the above certificates and configure the EAP-TLS part of your authentication server.
3. Add a username named `Vocera Manufacturer Certificate Client` to your authentication server database.
   The name must match; otherwise authentication will fail. Choose any password for this user.
4. Run the Badge Properties Editor on the configuration computer.
5. For B3000 and B3000n, click **Security**, and specify the following badge properties:
   - **Authentication**—EAP-TLS
   - **Use Custom EAP-TLS Certificates**—unchecked
   - **Encryption**—TKIP-WPA or AES-CCMP
6. For V5000, click **Security**, and specify the following badge properties:
   - **Authentication**—WPA-EAP
   - **EAP Method**—TLS
   - **Use Custom EAP-TLS Certificates**—unchecked
   - **Encryption**—CCMP or TKIP
7. Save the `badge.properties` file and copy it to your Vocera Voice Server computer.
8. Stop and start the Vocera Voice Server.
   Vocera devices are automatically updated, and are authenticated with the authentication server.

Using External Certificates

You can manage the EAP-TLS certificates either by generating your own self-signed certificates or obtaining certificates from a trusted Certificate Authority (CA) such as Microsoft Certificate Authority.

To configure your authentication server for EAP-TLS using external certificates, perform the following:

1. Generate the new EAP-TLS certificates.

Note: Note down the password used to encrypt the client key. You will need to enter this password for the Client Key Password property.

2. Download the server certificates to your authentication server.
3. Copy the Root CA certificate, the client certificate, and the client key to the `vocera\config\gen3\badge\res\certificates\EAP-TLS` and `vocera\config\gen5\badge\data\res\certificates\EAP-TLS` folder for B3000n and v5000 respectively, on the Vocera Voice Server and the configuration computer.

   Note: The certificates for the device must be in PEM format.

4. Rename the files with the following names:
   - `rootca_cert#`The root CA certificate
   - `client_cert#`The client certificate
   - `client_key#`The client-key
5. Add username to your authentication server database that the badges will use for authentication. Choose any password for this user.
6. Run the Badge Properties Editor on the configuration computer.
7. For B3000 and B3000n, click **Security**, and specify the following badge properties:
   - **Authentication**—EAP-TLS
   - **Use Custom EAP-TLS Certificates**—checked
   - **Encryption**—TKIP-WPA or AES-CCMP
8. For V5000, click **Security**, and specify the following badge properties:
   - **Authentication**—WPA-EAP
   - **EAP Method**—TLS
   - **Use Custom EAP-TLS Certificates**—checked
   - **Encryption**—CCMP or TKIP
9. Save the `badge.properties` file, and copy it to your Vocera Voice Server computers.
10. Stop and start the Vocera Voice Server.

    Vocera devices are automatically updated, and are authenticated with the authentication server.

    Note: To use unique certificate for the device, use the certificate generation tool that is provided with the BCU.

Configuring Badge EAP-TLS Authentication for Unique Certificates

To add security and increased control over devices in your network, you can configure Vocera devices to use unique certificates.

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

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

Installing the BCU for EAP-TLS with Unique Certificates

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

Prerequisite: Install the Badge Configuration Utility available with Vocera Voice Server or from Technical Support. For information about using the Badge Configuration Utility, refer to Using the Badge Configuration Utility.

To install OpenSSL on the dedicated BCU computer:

1. Download and install the latest version (Win32 OpenSSL v1.0.2f) of OpenSSL. For example, http://slproweb.com/products/Win32OpenSSL.html.
2. Proceed through the OpenSSL installation, accepting all the defaults. If a message appears stating that Visual C++ 2008 is required, exit the OpenSSL installation and download Visual C++ 2008 from this link: https://www.microsoft.com/en-in/download/details.aspx?id=29.
3. After OpenSSL is installed, update openssl path in the enviornment variable.
4. Place all client certificates (.pfx files) into the following folder: `%vocera_drive%\vocera\config\certs\files`.

   Note: Each certificate must contain the MAC address of the corresponding device. This allows the BCU to determine the corresponding device. The MAC address can be written in a number of formats:
   - 00-09-ef-01-02-03.pfx
   - 0009ef010203.pfx
   - Mchapman_0009EF01ABCD.pfx

   Incomplete MAC addresses result in an error.
5. For B3000n navigate to `%vocera_drive%\vocera\config\gen3\badge\res\certificates\EAP-TLS`. For V5000 navigate to `%vocera_drive%\vocera\config\gen5\badge\data\res\certificates\EAP-TLS`.
6. Create two empty files named `client_key` and `client_cert`. Ensure that there is no extension on the filename.
7. Obtain the root CA certificate `rootca.pem`, and rename to `rootca_cert`. Ensure that there is no extension on the filename.
8. Copy all the three files and paste it to the following locations: `%vocera_drive%\vocera\config\<gen3\gen3n\gen5>\badge\res\certificates\EAP-TLS`. For V5000 `%vocera_drive%\vocera\config\gen5\badge\data\res\certificates\EAP-TLS`.

Configuring BCU for EAP-TLS with Unique Certificates

The BCU provides benefits beyond loading badge firmware and updates to the badge properties file.

Although not necessarily recommended, you can use the BCU to accept PFX (PCKS12) format client certificate files and convert them to a PEM format, which is supported by Vocera devices. This is achieved by using the MAC address referenced on the certificate file name, so that certificates are pushed to the provisioned device.
To update the badge properties, perform the following steps:

1. Open Badge Properties Editor:
   - For B3000 and B3000n, click **Security**, and specify the following badge properties:
   - In the Security tab, configure the following settings:
     - Authentication#**EAP-TLS**
     - Use Custom EAP-TLS Certificates#**Checked**
     - User Name#<Enter username>

- Client Key Password#<Enter password>
- Encryption#**AES-CCMP or TKIP-WPA**
- Configure the remaining values for your badge properties
- Click **OK**

2. For V5000, click **Security**, and specify the following badge properties:
   - **Authentication**—**WPA-EAP**
   - **EAP Method**—**TLS**
   - **Use Custom EAP-TLS Certificates**—**Checked**
   - **Encryption**—**CCMP** or **TKIP**
   - Configure the remaining values for your badge properties
   - Click **OK**
3. Run the `bcu_certs.bat` from `%vocera_drive%\vocera\config`.

   Press any key to continue after the command prompt window appears. For each certificate located in the certs\files folder, you will be prompted to enter the pfx's import password if an import password has been set.

   Note: If the wrong import password is entered, the script will continue to run and the certificate will not be converted. You will need to rerun the program again.
4. After all the passwords are entered, the Badge Configuration Utility startups automatically and Vocera devices can be provisioned.

   The badge certificates converted from pfx format to PEM format and are located in their own mac address folder at: `%vocera_drive%\vocera\config\certs\badges.` PFX certificates can be removed from the certs/files folder after conversion. The converted certificates are kept and will be loaded automatically when the BCU is restarted.

Maintaining Devices with Unique Certificates

In most environments after the initial badge configuration is performed using the BCU, you can use the Vocera Voice Server to push certificate and firmware updates to the badges in your environment. However, in an environment where unique certificates are configured, you are required to use the BCU for some firmware and certificate updates.

You *cannot* perform these tasks using the Vocera Voice Server.

Updating Badge Firmware

Badge firmware updates can be safely applied to your Vocera Voice Server. The firmware updates will not overwrite or remove your unique EAP-TLS certificate information when the badges are updated.

The badge properties file on your Badge Configuration Computer can be copied onto your Vocera Voice Server: `vocera_drive\vocera\config\`.

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

Renewing Certificates

- When your badges approach the time to renew EAP-TLS certificates, they can only be updated using the Badge Configuration Utility.
- Follow the steps in Configuring BCU for EAP-TLS with Unique Certificates to convert and re-provision your new EAP-TLS badge certificate.

Supported Certificate Formats

Vocera has a specific list of certificate formats that are supported.

On the device, Vocera supports the SHA1 and SHA2 based PEM certificate file format.

Following are the supported certificate formats:

- SHA1
- SHA2
- SHA384
- SHA512

Public key sizes used are 1024, 2048, and 4096 bit keys.

Certificate Revocation

Certificate Authority (CA) provides a list of digital certificates that are revoked and should not be trusted.

Vocera badges do not check the revocation status of certificates, and therefore do not support Certificate Revocation Lists (CRLs) maintained on the authentication server.

Maintaining Properties and Firmware

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

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

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

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

About Property and Firmware Maintenance

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

The locations are as follows:

Badge type	Firmware location
V5000	`\vocera\config\gen5\badge`
B3000n	`\vocera\config\gen3n\badge`
B3000	`\vocera\config\gen3\badge`
B2000	`\vocera\config\gen2\badge`

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

- Immediately after a badge boots.
  When a device boots, it connects to the Vocera Voice Server. The server compares the device firmware and properties with its own copies as described in Updating Properties and Firmware on page 47.
- 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 47.

The server downloads firmware even if a device 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 at: https://www.vocera.com/ts/updates/rnotes/ReleaseNotes.html#fw_rnotes.

Updating Properties and Firmware

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

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

To update properties and firmware:

1. Use the Badge Properties Editor to configure a test device and confirm that WLAN security settings work properly. For more information, refer to Configuring a Test Device on page 34.
   If the test device works properly, you are ready to copy the `badge.properties` file to the Vocera Voice Server to update other devices.
2. Copy the `badge.properties` file in the `\vocera\config` directory on the device 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 devices connect to the server, they synchronize with the Vocera Voice Server, if necessary.
   If a device is offline, it updates as soon as the device boots and connects to the server.

Using the Badge Background Updater

Devices can download a firmware upgrade and modify settings in the background.

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

The badge functions normally during the update process, allowing you to make and receive calls when the update takes place in the background. This eliminates several minutes of downtime each time the 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 downloads 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. After approximately two minutes, 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.

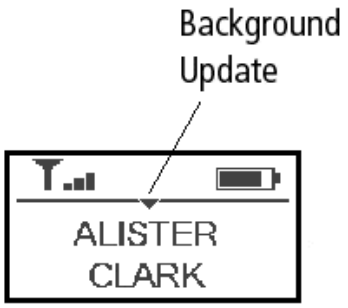
   Important: After the Vocera Voice Server starts, it initially comes up as an active node, and then within a minute it rejoins the cluster and performs a remote restore. With a large database, a remote restore can take several minutes.

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 nodes.

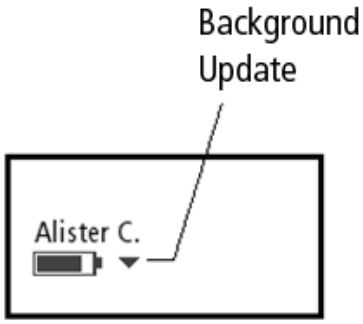
Background Update Status

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 functionalities of a badge are 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. The following icon represents the background updater:

▼

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 Device Configuration

This section describes how to troubleshoot device configuration problems using different diagnostic and configuration tools.

Troubleshooting the Initial Device Configuration

If a test device does not display the "Logged out" message, you need to troubleshoot it.

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

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

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

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

Badge Message	Typical Problems and Solutions
Searching for access points	The device cannot connect to an access point on the wireless LAN used by the Vocera Voice Server, possibly because: • The device is not within range of an access point. If you configured the test device in a remote area, ensure that you are within the wireless network range, then remove the battery from the device and insert it again. • The SSID setting of the device is incorrect. • The security settings of the device are incorrect. For more information, refer to the B2000 Badge Properties Configuration on page 16, B3000 Badge Properties Configuration on page 19, B3000N Badge Properties Configuration on page 24, and V5000 Smartbadge Properties Configuration on page 30 depending on the device configure.
Requesting IP address	The device is connected to an access point, but it cannot receive an IP address from a DHCP server, possibly because: • The security settings of the badge are incorrect. For more information, refer to the B2000 Badge Properties Configuration on page 16, B3000 Badge Properties Configuration on page 19, and B3000N Badge Properties Configuration on page 24, and V5000 Smartbadge Properties Configuration on page 30 depending on the device you are configuring. • The DHCP server is not active or cannot be reached from the device. • The device is associated with an access point that is not on the production server network.

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

For more information on troubleshooting a device, contact Customer Support.

Troubleshooting the Badge Property Settings

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

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

1. Display the device configuration menus.
   For more information, refer to Using the Device Configuration Menu on page 51.
2. Reset all device properties to factory default settings.
   For more information, refer to Restoring Device Factory Default Settings on page 58.
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 15.
4. Use the Badge Properties Editor to change the incorrect property values.
   For information about what property values are incorrect, refer to Troubleshooting the Initial Device Configuration on page 50. Then change the values as described in B2000 Badge Properties Configuration on page 16, B3000 Badge Properties Configuration on page 19, and B3000N Badge Properties Configuration on page 24, and V5000 Smartbadge Properties Configuration on page 30 depending on the device you are configuring.
   .
5. Configure the device by running the Badge Configuration Utility again.
   For more information, refer to Configuring a Test Device on page 34.

Using the Device Configuration Menu

Device 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 device configuration.

Do not confuse the Device configuration menu with the top-level device 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.

Badge Configuration Menu for B3000n

This section helps you understand how to display Badge Configuration Menu in the normal mode and in the hide boot menu for B3000n.

Displaying Badge Configuration Menu

B3000n 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 and the **Call** button.
   When the Badge boots, the screen displays the following top-level configuration menu items:
   - APPS & TESTS
   - VERSIONS
   - ALL FILES...
   - REPAIR
   - FILESYSTM
   - RESTART
   - VBL TO CONSOLE
   - REBOOT
   - BADGE RESET
   - DFLT EAPTLS
   - RESET
   - DEFAULTS

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 Hide Boot Menu is enabled, perform the following tasks:

1. Insert the battery
   The badge powers on, displays Vocera, and then start counting from 1 to 6.
2. When **6** appears on the screen, press and hold the **DND** and the **CALL** button at the same time.
   The hidden menus is displayed.

   Note: If the badge screen displays a username or `Logged Out`, you will not be navigated to the hidden menus. Try again starting from step 1.

Navigating the Menu Items in the Badge Configuration

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

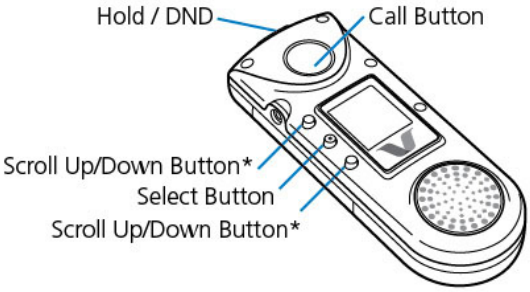
You can scroll to display more menu items at the same level, or you can select a menu item to view a nested set of items related to the upper-level menu choice. Use the following buttons to navigate in the badge menus:

1. Press the **Scroll Up** button to scroll up through menu items.

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

2. Press the **Select** button to select a menu item. Depending on the selection you make, one 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**).
3. Press the **Call** 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 B3000 and B3000n Badge:



*Up and Down depend on screen orientation

Badge Configuration Menu for V5000

This section helps you understand how to display the Smartbadge Configuration Menu for V5000.

V5000 Smartbadge 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 Smartbadge configuration menu, perform the following tasks:

1. Remove the battery from the Smartbadge, then insert it again.
   The Smart badge vibrates.
2. Press and hold both the **Hold/DND** button and the **Up Volume** button simultaneously.
   The Admin Menu Screen is displayed. The top level options are:
   - Apps
     - Send Logs
     - VCB
       - SSID
       - Authentication
       - EAP-Method
       - Encryption
       - Wireless Band
       - ACMode
       - NMode
       - WMW
       - UAPSDMode
       - 802.11d

    - Roaming Policy
    - Supplicant Loglevel
    - RadioLogLevel
    - PAC Provisioning
    - 802.11w
    - Neighbor Report
    - StaticIP
    - MFG Mode
    - Suppress FW download
    - Updater Off-Premise Profile
    - Updater Off-Premise Window Size
    - Updater Bytes Per Chunk
    - Direct Call Enabled
        - True
        - False
  - VCB Internal
  - Test
  - Updater
  - Version Info
  - Vocera only
- Reset to Defaults
- Break to Console
- Reboot Device
- Power Off

Device Data Overview

The Vocera Badge Log Collector service and the `Sendlogs` utility allow you to collect all debug information from a V5000 Smartbadge, B3000n and B3000 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 Smartbadge or a Badge, you can send the file containing debug information to Vocera.

Note: If you are not able to send badge logs to the Vocera Voice Server, you can send it to the Badge Configuration Utility machine and contact Vocera Technical Support for assistance.

When a device 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 device.

- `log.txt, log.old1.txt (B3000n)`
- `log.txt, log.txt.old (B3000)`
- `sys.messages(V5000)`
- `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.

Collecting Device Data

You need to collect device data to analyze issues encounter while using the Badge.

To collect device data using the `Sendlogs` utility:

To send logs perform the following steps:

1. Choose one of the following options based on your device.
   - On a Badge, press and hold the **Select** button for about 10 seconds until the `Sendlogs` utility starts.

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

   - On a Smartbadge, press and hold the **DND** button on the top of the Smartbadge for 3 seconds and release the **DND** button after first beep.
     The Smartbadge announces that message "Uploading badge diagnostic data, please wait.". After upload, Smartbadge announces that message "Badge diagnostic upload complete."
2. The device connects directly to the Vocera Voice Server computer using a Vocera Voice Server unicast transmission.
3. The device 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`.
   After uploading the device data (about a minute), the device 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 Device Configuration Menu.

Uploading Smartbadge Data

You need to collect device data to analyze issues encounter while using the Smartbadge.

To upload Smartbadge data, perform the following steps:

1. Locate the **DND** button on the top of the Smartbadge
2. Press and hold for about 3 seconds.
3. Release the **DND** button after first beep
   The Smartbadge announces that message "Uploading badge diagnostic data, please wait."
   After upload, Smartbadge announces that message "Badge diagnostic upload complete."

Running the Quick Test

If you suspect that a V5000 Smartbadge or B3000n or 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.

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.

Quick test for B3000 and B3000n

To run a Quick Test on B3000n B3000, preform 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, release the **Call** button.
   The Quick Test proceeds through the following tests:
   1. **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.
   2. **Audio test**: Be quiet during the audio test. Sound will play for 5 seconds, and the screen will indicate whether the four microphones are working.

      Note: If the Quick Test reports that one or more of the microphones has failed, you may have inadvertently covered the microphones with your fingers while holding the Badge. Try running the Quick Test again, and this time be careful not to cover the microphones.
   3. **Battery test**: Displays information about the battery temperature, voltage, current, and power.
   4. **LED test**: You must watch the green and amber lights to identify any problems. Make sure they turn on and off.
   5. **Halo test**: Watch the halo lights to identify any problems. Make sure they turn on and off (B3000n only).
   6. **WLAN test**: Displays the radio configuration, AP table, and IP table. The Badge will associate with an AP. If using DHCP, the Badge request an IP address.
   7. **Button test**: Prompts you to press and release buttons to ensure they are working.
3. Press and hold the **Call** button to exit the Quick Test.
4. Send logs of the Quick Test to the server using the `Sendlogs` utility after the Badge restarts.

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

Quick test for V5000

If you suspect that a V5000 Smartbadge 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.

To perform a Quick Test, following the steps:

1. Remove the battery from the Smartbadge, then insert it again.
   The Smart badge vibrates.
2. Press and hold both the **Hold/DND** button and the **Up Volume** button simultaneously.
   The Admin Menu Screen is displayed.
3. Navigate to **Apps**>**Test**.
   The Quick Test utility tests badge features in the following sequence:

- LED Test
- Backlight test
- Haptic effect
- Physical button
- Accelerometer test
- Proximity test
- Audio Test

Repairing the Badge File System

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

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

To correct a problem with a corrupted file and run the REPAIR FILESYSTM utility, perform the following tasks available on the Badge Configuration Menu:

1. Display the Badge Configuration Menu.
   For more information, refer to Using the Badge Configuration Utility.
2. Press the **Down** button to highlight the **REPAIR FILESYSTM** command.
3. Press the **Select** button. The Badge displays the following 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 checks 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 deletes 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.

Repairing the File System for B3000 and B3000n

To repair the file systems for B3000 and B3000n, perform the following tasks:

1. Display the Badge Configuration Menu.
   For more information, refer to Using the Badge Configuration Utility.
2. Press the **Down** button to highlight the **REPAIR FILESYSTM** command.
3. Press the **Select** button. The Badge displays three choices:

- **NO - CANCEL!**
- **YES - REPAIR!**
- **YES - WIPE N REPA**

4. Do one of the following:
   - Press the **Down** button to highlight **YES - REPAIR!**
     The Badge checks 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 deletes 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 Device Factory Default Settings

When you use the Badge Configuration Utility, you download property values that specify how a device 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 device again. After you restore factory default settings on the device, it automatically connects to the machine running the Badge Configuration Utility when it powers up.

Restoring Factory Default Settings for B3000 and B3000n

To reset to factory setting, perform the following tasks:

1. Display the Badge Configuration Menu.
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, ensure that 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 Factory Default Settings for V5000

To reset to factory setting, perform the following tasks:

1. Remove the battery from the Smartbadge, then insert it again.
   The Smart badge vibrates.
2. Press and hold both the **Hold/DND** button and the **Up Volume** button simultaneously.
   The Admin Menu Screen is displayed.
3. Navigate to **Reset to Defaults** and tap the option.
   Reset to Defaults? is displayed. The warning that **All settings will be lost** is also displayed.
4. Select one of the option:
   - **Cancel**—Cancels the selection.

- **Reset**—Resets the Smartbadge to the default settings.