Vocera Collaboration Suite Administrator Guide

Version 3.1.2

Notice

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

Last modified: 2018-11-27 07:37

VCS-312-Docs build 109

Contents

About Vocera Collaboration Suite

Vocera Collaboration Suite is an enterprise-wide solution that works inside and outside the walls of facilities to keep communication flowing between mobile workers in mission-control environments regardless of a user's location.

Vocera offers the flexibility to choose the right communication device for the environment and workflow. Vocera Collaboration Suite extends the Vocera platform to Android and iOS users anywhere they have Wi-Fi or cell phone coverage.

About This Guide

This guide provides information to administrators at sites where the Vocera Collaboration Suite solution is implemented.

Vocera Solution Comparison

Vocera smartphone and badge solutions offer secure messaging capability to any health care professional. Regardless of role or location, you can use Vocera to send secure, HIPAA-compliant messages to any member of your care team.

The following table lists the attributes and capabilities of the Vocera badge, Vocera Secure Texting and Vocera Collaboration Suite. Use this table to determine what solution is the best choice for you.

Attribute	Vocera Badge	Vocera Secure Texting		Vocera Collaboration Suite	
Network Supported	**Wi-Fi**	**Cellular**	**Wi-Fi**	**Cellular**	**Wi-Fi**
Supports Shared Devices	✓			✓	✓
Hands Free	✓				
Voice Automated	✓			✓	✓
Contact by Name, Role, Group	✓	✓	✓	✓	✓
Receive Group Call and Broadcast	✓				✓
Initiate Group Call and Broadcast	✓			✓	✓
Push-to-Talk	✓				✓
Contacts Directory Search		✓	✓	✓	✓
Favorites List		✓	✓	✓	✓
Presence/Availability Information		✓	✓	✓	✓
Select-to-Connect Commands		✓	✓	✓	✓
Keypad for extension dialing				✓	✓
Simple Paging	✓			✓	✓
Alarms/Alerts through integration	✓			✓	✓
Secure transmission and delivery of messages		✓	✓	✓	✓
Text Users and Groups		✓	✓	✓	✓
Web Console Messaging		✓	✓	✓	✓

The Vocera messaging solutions enable you to:

- Reach the **right person, instantly**.
- At the **right time**.
- On the **right device**.
- With the **right information**.
- In the **right place, anywhere**.

VCS Wi-Fi Configuration Best Practices

Smartphones are a necessary tool in today's workplace. Vocera Collaboration Suite is an essential smartphone application that allows users to securely stay connected. This documentation lists considerations to take into account before designing and deploying Vocera Collaboration Suite (VCS) as part of your workflow solution.

Wi-Fi Supported Settings

The Wi-Fi settings listed here are supported.

Setting	Recommendation
Wi-Fi Quality (2.4 and 5 GHz will be different)	Voice Grade
2.4 or 5 GHz	5 GHz only
MDM	Supported
Phone Model / OS	iPhone 5 or later / iOS 9.0.1 or later
	Android - Test
SSID Priority Queue	Highest
VPN / Per App VPN	No
Captive Portal	No
Session Timeouts	None
Wireless Authentication	WPA2 PSK
	802.1X w/ 802.11k/r
Client Exclusion Policies	Disabled

Site Survey

Vocera Collaboration Suite includes a voice application which connects over Wi-Fi. For best results, a Voice grade wireless network must be designed, and a site survey must be completed to verify proper coverage for the frequency band it will be deployed on.

If you have badges running on 2.4 GHz and plan to run VCS on 5 GHz, the 5GHz must be validated. The radio characteristics and planning of 2.4 and 5GHz are very different. Sufficient coverage on the 2.4 GHz network does not mean adequate coverage for 5 GHz. In both cases, the requirements are to have -65dBm power coverage with an SNR of 25 at 50mW or lower AP power output wherever the devices will be utilized.

Smartphones

One of the most important considerations when deploying Vocera Collaboration Suite is the capability of the smartphone platform.

Most smartphones are consumer grade devices and are limited in their Wi-Fi capabilities. Improvements come with each generation of the phone. For the best user experience, use a phone released in 2014 or later. Improvements have come in three main areas:

- Wi-Fi Roaming
- Wi-Fi Security
- Battery Management

Deployment Models

There are three typical models of smartphone use in the enterprise: Corporate Owned, BYOD, and Mixed.

Corporate Owned

The corporate owned model allows the business to completely secure the device and restrict applications and use for business needs.

A Mobile Device Management (MDM) solution is highly recommended to deploy and control these devices. With an MDM, the smartphone can be completely locked down so users can only use the necessary resources.

BYOD

Many employees have personal smartphones and use them at work. The challenge with this model is that it is difficult to know if the BYOD phone will perform well.

Use of an MDM can be highly beneficial in making sure the device meets the minimum technical and security requirements.

WLAN Settings

Many Vocera deployments are likely to have a combination of Vocera Badges and smartphones with the Vocera Collaboration Suite client installed. This section discusses the best practices for deploying for this mixture.

Wireless Priority and Applications

This table provides a list of priority classes and their associated data types and applications.

Priority Class	Data Type	Application	Example
Voice	Voice only	Critical, voice only applications	Vocera Badges
Video	Video/mixed use	Latency sensitive, mixed voice/data	Smartphone running Vocera CS
Best Effort	Data	Data only applications	Web, email, chat
Background	Guest	Not business related	Guest chat, video, etc.

Quality of Service

In the wireless world, QoS is used to make sure the most important traffic will have priority over less sensitive traffic.

Voice traffic is sensitive to delays in audio delivery (latency) and to variations in the timing of the audio delivery (jitter). Voice over wireless is especially challenged because it is a shared medium. For the best user experience, all audio traffic must be tagged with the appropriate QoS markings on the wired infrastructure and be allocated to the appropriate wireless priority queue. The recommendations described here focus on wireless prioritization, as it is typically more constricted.

Tip: An important thing to remember about Quality of Service (QoS) is that it is only important if there is contention on the media. Traffic metering lights on freeway entrances are a type of quality of service. When there is no traffic on the freeway there is no need to restrict traffic coming on. When the freeway is very busy, the metering lights are used to restrict the cadence of adding more traffic. This restriction prevents the freeway from coming to a standstill.

Wireless prioritization is usually done at the SSID level. Vocera recommends that all voice only applications, such as the Vocera Badge, be allocated to the voice SSID.

Mixed use devices, such as smartphones running Vocera Collaboration Suite (VCS), should use an SSID with highest priority. Because the smartphone can only associate to one SSID, it cannot send voice packets to the voice SSID and other packets to a lower priority SSID. It allows VCS voice packets to have higher priority over other data traffic. The data packets from VCS will not impact voice quality on the voice only SSID.

All other data applications in the environment should use an SSID with Best Effort priority. Data applications typically use TCP and HTTP, which have protocol layer redundancy. Latency and jitter that would seriously impact a voice application have no discernable effect on data applications.

The Background priority should be used for traffic that is least important to business. While Guest access is important to patient and family satisfaction, it is less important than most business traffic. Care should be taken to provide a balance for guest access to the wireless network.

2.4 vs 5 GHz Frequency Bands

The current generation of Apple and Android smartphones contain Wi-Fi radios that support both the 2.4 and 5 GHz frequency bands.

The 2.4 GHz band is typically overutilized because there are fewer channels and it is used by more devices. It also has more common interference sources, such as microwave ovens, wireless security cameras, and Bluetooth devices.

It is highly recommended that VCS enabled smartphones be deployed on a voice quality 5GHz infrastructure only.

5GHz Channels and Dynamic Frequency Selection (DFS)

Depending on location, some channels may not be available in the 5GHz frequency band. Channel use is limited by each country's regulatory agency.

Some of the 5 GHz channels are sometimes not available, as other applications (primarily RADAR) have priority use. If the Wi-Fi is using one of these channels and the AP detects it is being used by RADAR, the AP will change channels. When this happens, the clients associated with that AP will be forced to look for another AP. If a voice call is active during the channel change, voice audio will be interrupted.

If your facility is near an airport or a weather station (common users of RADAR), you should disable DFS channels.

Security

Wireless security is an important consideration, especially when deploying a BYOD model.

Captive Portal

Wi-Fi Captive Portals require the user to log in through a web page before getting full access to the Wi-Fi network.

The granted access is usually for a limited time. When that time expires, you must login again through the web page.

A Captive Portal should not be used when deploying VCS. If it must be deployed, set the session timeout to longer than a shift so that users do not have to re-login during their shift.

Virtual Personal Network (VPN)

VPNs are typically used to create a secure connection to a network. Using a VPN with VCS is not recommended.

- The VCS client is already on a secure network. Unless the VCS client is on the guest network (not recommended), it is already secure.
- VPN can be computationally intensive, which may cause delay or jitter in the audio packets.

iOS 7 Per App VPN

With iOS 7, Apple introduced a way to initiate a VPN on a per-application basis. Unfortunately, the implementation limits traffic over the VPN tunnel to TCP and HTTP traffic.

VCS uses UDP for both audio and signaling, and therefore will not work over a Per App VPN.

802.1X

Before a smartphone can use the Wi-Fi network, it must associate with the network and be validated.

The easiest way to do this is to configure a key on the smartphone. After it is configured and when it comes on the network, or when it roams between APs, the smartphone uses the key to get on the network.

A more secure method is to use an Authentication server (such as RADIUS, IAS, ICS, AAA). Authentication uses the 802.1X protocol to validate the user by using an Extensible Authentication Protocol (EAP) type. There are many EAP types, but they are all similar in that they communicate to the Authentication server before allowing access to the network. While 802.1X and EAP are more secure, they take time to perform the authentication. The authentication can take several seconds and occurs when the device first comes on the network and every time the smartphone roams between APs. If a smartphone is in a VCS call while roaming, there could be several seconds of lost audio on each roam.

802.11k/r

If 802.1X is required, 802.11k/r must be used. 802.11k/r are protocols that improve the roaming times drastically when using 802.1X.

Legal Notices

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

Download PDF Documentation

For your convenience, the *Vocera Collaboration Suite Administrator Guide* is also available as a PDF you can download.

Vocera Collaboration Suite Administrator Guide