stryker

REF   910-01947

Directions For Use (DFU)
Version 2.3.0

Notice

Stryker Corporation or its divisions or other corporate affiliated entities own, use or have applied for the following trademarks or service marks: Stryker, Vocera. All other trademarks are trademarks of their respective owners or holders. The absence of a product or service name or logo from this list does not constitute a waiver of Stryker's trademark or other intellectual property rights concerning that name or logo. Copyright © 2023 Stryker.

Last modified: 2023-02-15 11:59

DFU-230-Docs build 104

Contents

Introduction

The Vocera Engage Medical Device Alarm Notification is manufactured by Vocera Communications, 1950 West Cook Road, Suite 101, Fort Wayne, IN 46818 (1-877-207-3753)

Warning: The Vocera Engage Medical Device Alarm Notification is contraindicated as a primary alarm notification system for medical devices or medical device system alarms.

Warning: All alerts delivered to mobile devices by Vocera Engage Medical Device Alarm Notification are secondary alerts.

Warning: Vocera Engage Medical Device Alarm Notification data is designed to manage and notify using a subset of the patient data that is available from the medical device data aggregator and related central station displays. Do not solely use Engage Medical Device Alarm Notification data for patient monitoring.

Warning: Do not rely solely on Vocera Engage Medical Device Alarm Notification to indicate medical device alerts. Always continue to monitor patients at primary patient monitors and central station (if applicable) and respond to patient monitor equipment alerts.

Caution: Federal law restricts this device to sale by or on the order of a licensed medical practitioner.

This website contains the Vocera Engage Medical Device Alarm Notification Directions For Use (DFU) documentation. The DFU information is provided to assist users to understand the expectations and limitations of the product, and to use the service effectively in performing their responsibilities. You can access the following information in this website:

- **Description Information:** Brief description of the device, intended use and expectations, contraindications, risks and benefits, etc.
- **Warnings:** List of safety warnings, cautions, and notes
- **Operation Information:** Device checkout, operation, monitoring, cleaning, disposal, etc.
- **User Assistance:** User support details including levels of support, levels of severity, contact information, hours of coverage

This DFU documentation is presented electronically. Navigate to details using the menu, or the tabs at the top of the page. Simply click the PDF icon on any page to produce a printable version.

Site-wide search is available at the bottom of the navigation menu. Select **All Documentation PDF** in the left menu to view a PDF of the website. Note that this PDF takes several minutes to generate. You can also view the entire site structure by selecting **All Documentation HTML**.

For ease of use, this website replicates the structure described in the FDA guidance document titled Guidance on Medical Device Patient Labeling.

Description

The indications for use for the Vocera Engage Medical Device Alarm Notification product version 2.1, released 2019.

Introduction

This section of the Directions For Use is intended to describe the FDA cleared or approved indications for use for this medical device.

Indications for Use

Warning: All alerts delivered to mobile devices by Vocera Engage Medical Device Alarm Notification are secondary alerts.

Warning: Do not rely solely on Vocera Engage Medical Device Alarm Notification to indicate medical device alerts. Always continue to monitor patients at primary patient monitors and central station (if applicable) and respond to patient monitor equipment alerts. In these specific examples, Directions For Use may not deliver clinical alert notifications:

- A clinician is not assigned to the location.
- The mobile device is turned off or the battery is depleted.
- The mobile device volume is turned down too low or turned off.
- The mobile device is not receiving communications due to being obstructed or out of wireless coverage range.
- The assigned clinician has exited the Unit.
- The assigned clinician is logged out of the Vocera application.
- The mobile device is not communicating with the Vocera appliance.
- The medical device or medical device aggregator is not communicating with the Vocera appliance.

Vocera Engage Medical Device Alarm Notification is a closed loop communications system that interfaces with health care information systems and medical devices to provide a secondary means of enunciating and displaying patient alarm text and other information to mobile health care workers that is important to patient care, nursing vigilance and overall hospital operations.

Vocera Engage Medical Device Alarm Notification alerts and informs the clinician about critical patient alarms by drawing an identified individual's attention to a defined patient condition in a timely manner without requiring them to be at or near the bedside medical devices or central station displays. Vocera Engage Medical Device Alarm Notification is not intended to replace any part of the patient monitoring system or procedures already existing for the medical devices interfaced with Vocera Engage Medical Device Alarm Notification .

Vocera Engage Medical Device Alarm Notification is limited to use by qualified medical professionals who have been trained on the use of the device. It is intended for use in hospital and hospital type acute care environments and is not for home use.

Description of the Solution

The description of the Vocera Communication Vocera EMDAN product.

Description of Vocera Engage Medical Device Alarm Notification

Vocera Communication's Vocera EMDAN platform is a highly configurable, hospital-wide communication and workflow engine.Vocera Engage Medical Device Alarm Notification is designed to deliver event-driven communications across multi-disciplinary teams and physical boundaries.

Vocera Engage Medical Device Alarm Notification receives alarms from patient monitors and uses staff assignment information to target the delivery of secondary alert messages for critical alarms to clinician's mobile devices and desk phones (fixed devices). Vocera Engage Medical Device Alarm Notification uses admission information to augment alert messages with patient information.

Vocera Engage Medical Device Alarm Notification requires the use of a supported nurse call system for real-time staff assignment, an enterprise phone management system to deliver to mobile and fixed devices, and a medical device data aggregator to collect alarm data from patient monitors. For example, a facility may use Rauland-Borg Responder 5, Cisco Unified Communications Manager, and Philips IntelliVue Information Network Database for these respective functions. Vocera Engage Medical Device Alarm Notification requires an Admit Discharge Transfer (ADT) feed for patient information to be available with alert messages.

Linking the medical device data aggregator with the local Admissions/Discharges/Transfer (ADT) application and mobile or fixed devices enables a key benefit of the device, context aware communication. The design goal for alert notifications is to enable any user to benefit by not only receiving an alert, but by receiving as much context as feasible (contained within the alert notification message or available via one or two button operations) in order to respond in the most efficient manner to aid the delivery of care.

Clinicians can interact with alerts delivered to mobile or fixed devices through workflows that allow the user to accept, decline, or get additional contextual information for an alert. Administrators can interact with browser workflows to maintain users, devices, and other facility information in the system.

The implementation and installation process is supervised by Vocera's Professional Service group. A structured consultative approach is used to examine both a customer's existing workflow practices and stated goals. Any changes to workflow or process re-engineering are reviewed with the customer's clinical management and implementation team before integrating the Vocera workflow into a customer's operating environment.

Vocera Engage Medical Device Alarm Notification is not intended to replace any part of the patient monitoring system or patient monitoring procedures already existing for the medical devices working with Vocera Engage Medical Device Alarm Notification .

Manufacturer's Responsibility

Vocera is responsible for the effects of safety, reliability and performance only if:

- Assembly operations, installations, modifications or repairs are carried out by authorized service personnel
- The electrical installation of the relevant room complies with the requirements of the appropriate regulations
- The equipment is used in accordance with the instructions for use

System Components

1. Medical Device
2. Medical Device Data Aggregator
3. HIS for ADT
4. Workstation / Engage Workflow Access
5. Engage Medical Device Alarm Notification Solution
6. SmartPhone
7. Fixed Device
8. Mobile Device
9. Enterprise Phone Management System
10. Staff Assignment System
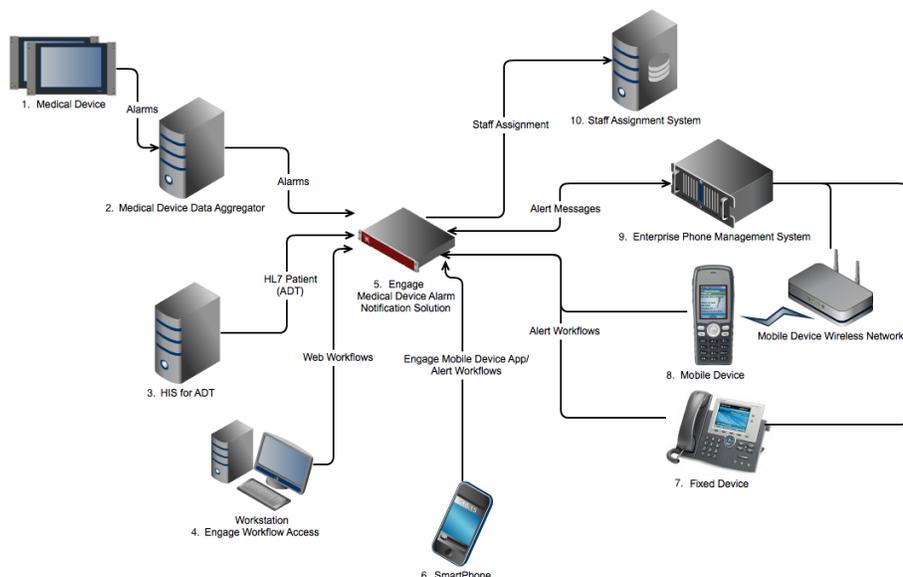
1. Medical Device
2. Medical Device Data Aggregator
3. Health Information System
4. Vocera Workflow System
5. Vocera Engage Medical Device Alarm Notification
6. Smartphone
7. Fixed Device
8. Mobile Device
9. Enterprise Phone Management System
10. Staff Assignment System

Vocera Engage Medical Device Alarm Notification Configuration

All Vocera Engage Medical Device Alarm Notification configuration is completed by Vocera staff. Any adjustments must be made and validated by Vocera.

Critical alarms can be different for each unit. The customer determines the list of critical alarms to deliver as alerts.

Alerts can follow up to seven different escalation paths; two of the seven paths are designed to be used with a Monitor Technician. Each escalation path has three escalation steps; primary, secondary, and tertiary. The customer determines the path for each alarm type, the tone for each step, and the delay before the secondary and tertiary steps.

Note: If the facility uses Mirth CAN channels with the EMDAN version 1.8 solution, the 'extension-solutions-mdan-logrotate' RPM must be installed in order to create necessary permissions for a functional logrotate.

Planning and Training Considerations

The planning and training considerations for the Vocera Engage Medical Device Alarm Notification product.

Planning and Training Considerations

Vocera Engage Medical Device Alarm Notification is to be used by licensed health care professionals using standard institutional procedures and good clinical practice guidelines for patient monitoring.

Staff training in the operation of Vocera EMDAN is essential for optimal use. Users should be skilled at the level of clinicians, clinical administrators and hospital administrators, with the knowledge and experience to acquire and interpret patients' vital signs. Each of these roles is assigned and associated with specific privileges and scopes. Access privileges to a central administrative/staff assignment console and the individual communications devices are controlled through passwords. Individuals using Vocera EMDAN should be familiar with the detailed operation as described in this manual, and they should understand all warnings and cautions in the manual.

System-Level Planning Considerations

The Vocera EMDAN configuration is guided by a series of workflow decisions made by the customer. Each feature of Vocera EMDAN affects a workflow currently in place within the operating environment.

These configuration decisions will be presented in pre-installation site planning sessions by Vocera Communication's Professional Service personnel. Prior to installation day, you will have reviewed many detailed operational alternatives, including the following topics:

- Selecting ringtones to suit your environment
- Escalation Paths
- Group Alerts
- Alert Priorities
- Integration with a nurse call system
- Integration with an enterprise phone management system
- Integration with a medical device data aggregator
- Vocera User Account creation

Unit-Level Planning Considerations

The Vocera EMDAN configuration is populated with local locations, room numbers, sectors, preferred labels/vocabulary, user and roles.

Two accounts, a phone user account and a web user account, must be created before mobile and fixed devices can be used with Vocera EMDAN .

Vocera EMDAN provides permissions and roles. The **Administrator Role** allows users to manage Vocera at the application level, granting the user the ability to manage other users and view audit logs. The **Clinician Role** is designed for users who do not need to manage the system; the Clinician is the primary user of the system with permissions to receive alerts, use interactive features to respond to alerts, look up physiological details for a patient, and view staff assignment. The **Supervisor Role** is designed for Clinical Supervisors and includes access to the administrative menu. The Administrative User can manage staff assignments, check the status of alerts and receive escalated alerts.

User Training Considerations

All staff members using or administering Vocera EMDAN will receive standardized training modules based on their job assignment and role.

Before their first shift using Vocera EMDAN , all staff will be trained in the day-to-day use of the solution. Custom training modules and Quick Reference Guides may be created to match the local operation environment. All staff will be familiar with the following concepts/procedures:

- Always use a fully charged mobile device
- Importance of logging in at the beginning of each shift
- Importance of logging out at the end of each shift
- User credentials and procedure to login at the start of each shift

- Importance of identifying and maintaining possession of your assigned mobile device
- Ring tones in use within the facility and their priority
- Vibration alerts (if supported)
- Common abbreviations used in alerts
- Alert banner priority codes
- Recognizing a handset low battery alert
- How to respond to an alert notification
- How to view physiological detail associated with an alert
- How to decline an alert notification
- Escalation path for all alerts in use in your environment
- How to review accepted/declined alerts using your mobile or fixed device
- Review of any system downtime procedures

System Specifications

The system specifications for the Vocera Engage Medical Device Alarm Notification product.

System Specifications

The system specifications listed here are the minimum settings that Vocera Engage Medical Device Alarm Notification (EMDAN) requires to function. Installation planning, configuration, and other system related activities should be managed by Vocera Communications personnel.

In this Vocera EMDAN documentation, the term "appliance" refers to the Vocera software and any hardware that may be required to run Vocera EMDAN .

Supported Browsers

The Vocera application is managed via a browser-based interface. A supported browser is required to install, support, and manage Vocera EMDAN .

Supported browsers include:

- Microsoft Internet Explorer version 10 or later
- Firefox version 47 or later
- Apple Safari version 10.10 or later
- Chrome version 53 or later

Virtual Host

Vocera will provide the appliance as an .ovf file containing the entire Virtual Machine (VM) and application. See Virtual Machine Installation on page 27 for the current VM requirements.

Physical Appliance

Vocera may provide a physical appliance. See Appliance Installation on page 21 for the current requirements for the appliance environment.

Network

All network segments from the monitor to the fixed or mobile communication device should have a network latency for an 8000 byte packet of no more than 70 milliseconds, or an end-to-end latency of no more than 500 milliseconds.

The following table describes the firewall requirements which should be configured in order to successfully install, update, and support the Vocera application and its operating system.

Port	Destination	Purpose
22	svc.ext-inc.com (199.180.201.227)	Remote Support (SSH)
443	svc.ext-inc.com (199.180.201.227)	Initial Server Provisioning Port must be left open for Remote Support
443	yum.ext-inc.com (199.180.201.238)	Upgrade repository for OS & Application

ADT

An ADT HL7 feed is required for patient information to be available in alert messages. Vocera will manage the installation settings.

Medical Device

Vocera EMDAN does not interact directly with medical devices, such as patient monitors. Medical device interaction with a medical device data aggregator is managed outside of Vocera EMDAN .

Nurse Call System

Vocera EMDAN integrates with a nurse call system.

Enterprise Mobile Device Management System

Vocera EMDAN integrates with an enterprise mobile device system, such as a Cisco Unified Communications Manager system, to deliver messages. Vocera will manage the Vocera EMDAN installation settings. The minimum setup requirements are dependent on the enterprise mobile device management system selected.

Devices

Vocera EMDAN integrates with mobile devices, such as the Cisco IP wireless phone, to display information which the mobile device requests.

Vocera EMDAN also integrates with fixed devices, such as Cisco 7945 and 7962 desk phones.

Daylight Savings Time Observation

A detailed description of how Vocera Communications handles DST for the Vocera EMDAN product.

Introduction

The seasonal occurrences of Daylights Savings Time (DST) requires an observation from Vocera in order to properly maintain on time message delivery, rather than inappropriately continuing to deliver in the no longer accurate hour. When the local time gains an hour in the fall or loses an hour in the spring, messaging systems must mirror the respective time change for proper delivery times to be maintained. The Vocera appliance manages both DST occurrences in the calendar year for all internal conditions and rule triggers that dictate changes to a delivery.

Vocera stores time stamps in Coordinated Universal Time (UTC), and the cron software utility handles the timestamp change for jobs. For example, an alert received at 1:01 -0400 UTC and an alert received at 1:01 -0500 UTC will be rendered into the same '1:01' timestamp by Vocera. An alert received at 2:01 -0200 UTC and an alert received at 2:01 -0100 UTC are also rendered into the same '2:01' timestamp as well.

Conditions

Any conditions attempting to add or subtract from a timestamp in the changing time zone are also correctly rendered by the appliance. For example, if a raw timestamp of 1:00:00 -0500 AM is under the condition '#{timestamp - 1.hours}', the result is 1:00:00 -0400 AM. An as_time display will show '1:00:00' for both the -0400 AM and -0500 AM timestamps. This also works with a '#{timestamp + 1.hours} condition and Vocera will still correctly merge the timestamp.

Rule Delay

A Rule trigger that delays a delivery will still perform properly through a DST change. For example, a Rule with a 30 second delay that is triggered at 1:59:45 -0100 AM in the fall will correctly delay to 1:00:15 -0200 AM for the gained hour. A delay trigger may also occur in the spring when the local time loses an hour, but will still calibrate the time change during the event. For example, a Rule with a 30 second delay triggered at 3:59:50 -0400 AM will observe the DST change to correctly deliver at 5:00:20 -0300 AM.

The duration of these delays overlap with the local time change, but the appliance recognizes the DST observation and appropriately adjusts in real time for the delay to properly postpone the alert delivery. The adjustments made by Vocera will happen for Rule delays regardless of when DST occurs. No triggers and conditions within the appliance will be affected by the actual time change from any DST occurrence.

Warnings

The Danger, Warning, Caution, and Note safety messages that are used in this documentation.

Introduction to Warnings

This section of the Directions For Use is intended to describe the specific hazard alert information that you should know before using the device.

Safety Message Signal Words

Safety message signal words designate the severity of a potential hazard.

- DANGER indicates an imminently hazardous situation, which, if not avoided, will result in death or serious injury.
- WARNING indicates a potentially hazardous situation, which, if not avoided, could result in death or serious injury.
- CAUTION indicates a potentially hazardous situation, which, if not avoided, will result in minor or moderate injury.
- NOTE indicates an informational message that does not pertain directly to a hazard.

DANGER Safety Message

No danger safety messages apply to this system.

WARNING Safety Message

The following warning safety messages apply to this system.

 Warning: **Risk of Failure if Dropped or Subjected to Vibration** Avoid dropping the appliance. Do not expose the appliance to vibration. Complete all Customer Acceptance Testing after installation to ensure proper functioning of the appliance.

 Warning: Alerts will not pop up or play a sound if the device time is more than 10 seconds in the future of the actual time. The badge counter will increase and is displayed in the Notification Tray.

 Warning: The Vocera Engage Medical Device Alarm Notification is contraindicated as a primary alarm notification system for medical devices or medical device system alarms.

 Warning: Setting the notification type to None for iOS devices will preclude Vocera Engage Medical Device Alarm Notification from effectively notifying the user of alerts, and could result in patient injury or death.

 Warning: All alerts delivered to mobile devices by Vocera Engage Medical Device Alarm Notification are secondary alerts.

Warning: Federal law restricts this device to sale by or on he order of a licensed medical practitioner.

Warning: Document all Vocera appliance device settings that were configured during installation of Vocera Engage Medical Device Alarm Notification software. Modifying, deleting or replacing any Vocera appliance files or changing any of the device settings can result in sub-optimal Vocera Engage Medical Device Alarm Notification performance, including inhibition of alert notification delivery, system time settings, alert type, alert volume and wireless network connection.

Warning: When a system sending alerts to Engage manages the alerts, that system assumes the role and responsibilities of alarm manager.

Warning: Turning down or off phone ringer/vibrate will preclude Vocera Engage Medical Device Alarm Notification from effectively notifying the user of alerts, and could result in patient injury or death.

Warning: Accuracy – If the data intended to be transmitted is not available or the accuracy of the transmitted data is questionable, the caregiver should access the data from the source device, such as the primary patient monitor for physiological data or the EMR/HIS for patient demographic information. The data provided via the Vocera Engage Medical Device Alarm Notification device is not intended to be the sole source for patient data and is to be used in conjunction with the data at the patient monitor or central station. The primary patient monitor should always be referenced before making any patient care decisions.

Warning: Vocera Engage Medical Device Alarm Notification is dependent upon your facility's ADT solution for patient demographic and location information.

Warning: Caregivers must be trained on proper action instructions for alerts, and hospitals must schedule routine equipment inspection and calibration. If a patient monitor goes into a fail state, it may generate an alarm cancelled message but the alarm actually remains active.

Warning: System configuration must be performed only by qualified personnel who are trained and familiar with the Vocera appliance and relevant communication standards, and with local implementation of the medical device aggregator. Improper configuration of Vocera adapters can cause unexpected and unintended behavior of the clinical alert notification service.

Warning: Vocera Engage Medical Device Alarm Notification data is designed to manage and notify using a subset of the patient data that is available at the medical device aggregator and related central station displays. Do not rely solely on Vocera Engage Medical Device Alarm Notification data for patient monitoring.

Warning: Do not rely solely Vocera Engage Medical Device Alarm Notification to indicate medical device alerts. Always continue to monitor patients at primary patient monitors and central station (if applicable) and respond to patient monitor equipment alerts. In these specific examples, Vocera Engage Medical Device Alarm Notification may not deliver clinical alert notifications:

- A clinician is not assigned to the location.
- The mobile device is turned off or the battery is depleted.
- The assigned clinician has exited the Unit.
- The assigned clinician is logged out of the Vocera application.
- The mobile device is not communicating with the Vocera appliance.
- The medical device or medical device aggregator is not communicating with the Vocera appliance.

- The patient monitor is not communicating with the medical device aggregator.
- The patient is disconnected from the patient monitor.

Warning: Loss of Functionality/Data Loss – Do not change Vocera system components or configuration without approval by Vocera. Such changes could degrade system performance and affect patient monitoring.

Warning: Only Vocera authorized personnel are allowed to change alert timing delays. A delay can result in harm to the patient, and the facility must sign-off on workflows that include a delay in the initial notification.

Warning: If Vocera is installed on a secure network, the device must be on the same secure network to receive alerts. Be aware that connecting to a network other than the required network, either manually or automatically, will prevent the user from getting alerts.

Warning: TFTP Services Restart Restarting the TFTP Service for a Cisco Communications Manager will cause all of the phones connected to the Communications Manager to fail-over to a secondary Communications Manager. If there is no secondary Communications Manager available, all of the phones will restart.

Warning: Engage Mobile 5.X will not work properly without XMPP 3.X. Failure to install the correct versions will result in missed alarms and system failures.

Warning: Engage Mobile version 4.X is not compatible with later versions, and the customer facility must have the XMPP version 2.X adapter installed on their appliance.

Warning: Engage Mobile 5.0 or above will not work properly without XMPP 3.0. Failure to install the correct versions will result in missed alarms and system failures.

Warning: If an iOS device is not connected to the network and multiple alert notifications are generated during this time, the device may only receive the most recent alert notification from the Apple Push Notification Service.

Warning: Use of an RTLS integration will selectively deliver patient alarms. Continue to monitor patients at primary patient monitors.

CAUTION Safety Message

The following caution safety messages apply to this system.

Caution: Federal law restricts this device to sale by or on the order of a licensed medical practitioner.

Caution: Accuracy – A user must verify the accuracy of patient demographic information by confirming the transmitted alert data with a second source.

Caution: Automated or manual changes to the time or date settings of the attached medical device (including daylight savings time adjustments) may affect operation of the Vocera Engage Medical Device Alarm Notification device, such as loss of patient data history. Refer to the medical device product documentation for detailed information about the effects of time changes.

NOTE Safety Message

The following note safety messages apply to this system.

Note: Always recharge a mobile device when it is not in use and at first notification of low batteries. A device with low batteries will eventually fail as power is depleted.

Note: Engage Mobile is not compatible with the 3D Touch feature available on the iPhone 6s or 6s + models. Swiping through Engage Mobile with 3D Touch enabled may unexpectedly take the user outside of the application.

Note: Failure to disable the battery saving feature that temporarily turns off Wi-Fi when the Motorola MC40 (MC40-HC) goes to sleep will prevent the user from getting alerts.

Note: Failure to disable the battery saving feature that temporarily turns off Wi-Fi when the Zebra TC51 (TC51-HC) goes to sleep will prevent the user from getting alerts.

Note: A user must log out of their current device before logging into a different device. Failure to do so may cause unintended consequences such as alert notification failure.

Note: The Resynchronize Users and Groups button will require a significant amount of time to process. Pressing this button uploads all user and group information from the LDAP server, which is then read and updated in Vocera.

Note: Disable the Snapshot feature of VMWare. Leaving the Snapshot feature enabled can cause the VM to lose connectivity for an extended period of time. The client should manually take a snapshot of their VM immediately before and after any upgrades.

Note: When the facility uses Rauland-Borg ResponderSync for staff assignment, ResponderSync polling for assignment information may cause an inaccuracy in a Vocera assignment. In a facility where hourly polling takes multiple minutes to complete, it is possible that an assignment made while the system is polling will not be received, resulting in an incorrect assignment until the next poll event updates the assignment information.

Note: Loss of Functionality/Data Loss – Be extremely careful not to assign the same IP address to two different devices on the network. Duplicate IP addresses will cause erratic system communications and data loss.

Note: Loss of Functionality/Data Loss - It is important to limit the number of people in escalation paths and to not use groups as recipients when using OAI hardware. The OAI system has a set maximum number of access points, and will not allow any additional devices to connect when all points are in use. When the OAI network access points are maximized, additional mobile devices do not receive alerts and caregiver action is delayed.

Note: Swiping through Engage Mobile with 3D Touch enabled, a feature available on iPhone 6 models, may unexpectedly take the user outside of the application.

Note: Alerts delivered to mobile devices might be considered primary alarms by caregivers. Continue to remind users that Clinical Alert notification is secondary and always continue to monitor patients at primary patient monitors.

Note: User Interface – Only Vocera personnel are allowed to authorize network changes. Caregiver action may be delayed if unauthorized changes are made to the Vocera appliance network.

Note: Any hospital may include additional options to those described in this Administrator Menu documentation. Depending on the solution, you may have additional options. The Resynchronize Users and Groups button will require a significant amount of time to process. Pressing this button uploads all user and group information from the LDAP server, which is then read and updated in Vocera.

Note: Only external devices specifically designed to be connected to the Vocera appliance, or approved by Vocera for use with the Vocera appliance should be connected, as specified in this manual or as otherwise specified by Vocera. External equipment must be connected to the system only by qualified service personnel. Connecting external devices not approved for use with the Vocera appliance may cause loss of function or equipment damage.

Note: Shut down of the Vocera appliance will cause disruption of data flow between the appliance and the medical device aggregator and the supported mobile devices. Notify the affected users relying upon this data flow before shutting down the appliance, or if the appliance shuts down for any reason.

Note: If more than one ADT server exists on the accessible hospital network, intermittent failures may occur. Be sure to allow only one ADT server to operate on the accessible hospital network.

Note: Contact Vocera for information before connecting any devices to the equipment that are not specifically recommended in this manual.

Note: Periodically, and whenever the integrity of the medical device or patient data stream is in doubt, test all functions.

Note: In network configurations or IP address settings are changed; update the Vocera appliance with the new IP address settings. Failure to follow this instruction can cause loss of connectivity with the Vocera appliance.

Note: The Adapter engine backup procedure should be performed at regular intervals and/or whenever any adapter is changed to ensure complete adapter restoration if it should become necessary.

Note: Do not allow mobile devices to act as a Network Time Protocol (NTP) server. Mobile devices can drop communication packets that may cause communication problems resulting from time errors.

Note: The SpectraLink 8000 OAI Gateway is recommended and tested to be used with a TCP/IP connection only.

Note: The SpectraLink 6100 and 6300 Gateway may only be used with an RS-232 connection.

Note: The SpectraLink OAI adaptor supports a maximum of ten messages on the SpectraLink OAI devices. Only the ten most recent messages display on the phone.

Note: Vocera does not support soft-key functionality on the SpectraLink OAI 6020 device.

Note: The end user will not be able to receive Vocera alerts on their device if the MAC address is displayed in the Available Devices box. The device's MAC address must be shown in the Controlled Devices box.

Note: The Motorola MC40 handset device has a scan button feature that can be used to populate the 'Domain' field via a QR code.

Note: The bar code reader for the Motorola MC40 will not work with the Engage Mobile application.

Note: The bar code reader for the Zebra TC51 will not work with the Engage Mobile application.

Note: Any air gestures or eye gestures enabled in the Samsung Galaxy S4 device will not work within the Engage Mobile application.

Note: The facility name is added to the unit name when a single instance of Vocera supports users from several facilities, each of which may have a unit with the same name. For example, a Cardio unit may exist in General Hospital and Central Hospital. When a single Vocera instance supports both facilities, the facility name is pre-pended to the unit name, such as General Hospital Cardio.

Note: The application will not function as designed if "Don't Allow" is selected at the Use Current Location prompt, or if location services is turned off.

Note: A single character must be entered into the search function for results to begin to appear.

Note: When a user is configured on multiple escalation levels, they will not get an update via XMPP since they are already considered part of the conversation. For example, where a Charge Nurse is assigned to two escalation levels, Primary and Tertiary, this user will only get the Primary alert and no subsequent notifications, including the Tertiary level alert when no other caregivers can accept the alert.

Note: If your facility is using phones with an XMPP integration, you will not have the option to assign a user, assign a default unit, or remove a default unit as these options are managed automatically for XMPP devices.

Note: Users cannot be assigned to XMPP devices using Manage Phones. Users must log into Engage Mobile from the XMPP device, and that login serves the same purpose as assigning the user to the phone.

Note: Users cannot be unassigned from XMPP devices using Manage Phones. Users must log out of Engage Mobile from the XMPP device, and that logout serves the same purpose as unassigning the user from the phone.

Note: Only XMPP phones have a disconnected status. If your facility does not use phones with an XMPP integration, this option will always return no results.

Note: Asterisks are displayed when the system can find no corresponding information for the field.

Note: Three asterisks (***) display in place of the user name in the search results when the device that received the message was not associated with a user at the time of the message delivery.

Note: When the message is sent from a web browser, three asterisks (***) display in place of the phone number in the search results.

Note: Removing the alert will only remove it from the Cisco fixed device, not from any corresponding systems or records.

Note: Not all facilities opt for a full three level escalation path. Some facilities may choose to use one or two levels of assignment for alert notifications.

Note: The Administrator, Charge Nurse, Super User, and End User can track alerts and messages. The End User role can track messages only. Contact a System Administrator for assistance.

Note: The Administrator and Super User can manage message templates and template categories, and unit associations with categories; contact a System Administrator for assistance.

Note: Only the Administrator and Super User roles can manage phones; contact the System Administrator for assistance if needed.

Note: Only the Administrator role can manage user presence states; contact the System Administrator for assistance if needed.

Note: Only the Administrator role can manage the unit's rooms and beds; contact a System Administrator for assistance.

Note: Only the Administrator role can view the Manage Configurations functionality; contact a System Administrator for assistance.

Note: Only an Administrator can manage functional roles in the Administrator Menu; contact the System Administrator for assistance if needed.

Note: Only the Administrator role can view the Manage Locations functionality; contact a System Administrator for assistance.

Note: Only the Administrator can manage user groups; contact the System Administrator for assistance if needed.

Note: Only the Administrator role can manage a user's default unit, title and group; contact the System Administrator for assistance if needed.

Note: Only the Administrator role can manage the Monitor Technician in the system; contact a System Administrator for assistance.

Note: Only the Administrator role can view all configured units in a facility; contact the System Administrator for assistance if needed.

Note: Only the Administrator role can view all patients in the system; contact the System Administrator for assistance if needed.

Note: Only the Administrator role can view the Alarm System Status; contact a System Administrator for assistance.

Note: Only the Administrator role can view the Manage RTLS Locations functionality; contact a System Administrator for assistance.

Note: Only the Charge Nurse / Unit Secretary role can access this workflow to manage phone assignments for other users; contact a System Administrator for assistance if needed.

Note: Only the Charge Nurse/Unit Secretary, Super User, or Administrator role can view the Quick Staff Assignment functionality; contact a System Administrator for assistance.

Note: Only the Charge Nurse/Unit Secretary, Super User, and Administrator default roles can manage unit staff assignments; contact the System Administrator for assistance if needed.

Note: Only the Charge Nurse can access the Assign User Groups functionality. Contact an Administrator for assistance if needed.

Note: Only the End User role can log in or out of a phone using this workflow; contact a System Administrator for assistance.

Note: Use the Unit Staff Assignment workflow for advanced assignments.

Note: Enter a user login that was previously uploaded to the system. Failure to do so will create a user with no associations and alerts cannot be passed to that user.

Note: The system cannot delete a facility if there are units, rooms, or locations assigned to the facility.

Note: You CANNOT delete a unit if there are rooms assigned to it.

Note: You CANNOT delete a room if there are beds assigned to it.

Note: A Room Name is NOT required when creating a room.

Note: When message templates are created, edited, or removed in the system, some end users will not see the changes until they log out and then log back into their device.

Note: Assignments are defined as needed for the facility and are created in the Manage Configurations workflow. Contact an Administrator for assistance.

Note: It is recommended that ALL users have a default unit assigned. Without a default unit, there will be unintended errors.

Note: Vocera does not support sending group messages using SpectraLink OAI devices.

Note: Alert message may be truncated causing the alert status to not visible on a SpectraLink OAI device screen. When an alert is accepted or declined, the update message sent to recipients may be too long to fit the screen, however, an audit event is logged with the details.

Note: A user must be connected to wifi to download the Engage Mobile application.

Note: **Additional Information** For additional information on restarting services, see the Cisco Unified Serviceability Administration Guide for the version of Communications Manager being used. For additional information on uploading files to the TFTP server, see the Cisco Unified Communications Operating System Administration Guide for the version of Communications Manager being used.

Note: Mindray Panorama delivers an alarm only once. As a result, the adapter will process only one alert per Mindray alarm.

Note: An additional Mindray adapter will need to be set up on the appliance for every Mindray Central Network in the facility.

Note: If you want to store the recipient, select the checkbox for Store Message Recipient and enter clinical.to**.number** in the Recipient field.

Note: The values in the regular expression mappings should be updated based on the messages received from the Mindray monitor and the facility configuration.
- Facility: value is not received and must be hardcoded. The Implementation Specialist may configure this.
- Bed Number: mapped to clinical.bed.room.room_number. If the value received is not consistent with the naming used by the facility, the Implementation Specialist may hardcode a value such as "1".
- Clinical ID: this is a unique identifier for the alert composed of an adapter prefix, location, alert type, and alarm time.
- Activity State: value is not received and must be set to ACTIVE for new alerts.
- Alarm Time: value is not received and must be set to current time for new alerts.

Note: The **pagers.ini** file is one of the files saved to the Emergency Disk. Create an Emergency Disk to save this file.

Note: When a user is configured on multiple escalation levels, they will not get an update via XMPP since they are already considered part of the conversation. For example, where a Charge Nurse is assigned to two escalation levels, Primary and Tertiary, this user will only get the Primary alert and no subsequent notifications, including the Tertiary level alert when no other caregivers can accept the alert.

Note: For each installation, update the regular expressions in the default adapter settings to work with the facility's patient monitor's current software version. See the Regular Expressions (Regex) configuration page for details. Refer to the CEI Alarm Messages document for expected message formats based on the software version.

Note: The SpectraLink 8000 OAI Gateway is recommended and tested to be used with a TCP/IP connection only.

Note: The SpectraLink 6100 and 6300 Gateway may only be used with an RS-232 connection.

Note: When using Cisco 8821 handsets use caution when navigating pages using the Back button. The last page viewed is not refreshed when the Back button is pressed; this may result in content that is outdated.

Note: If the facility uses Mirth CAN channels with the EMDAN version 1.8 solution, the 'extension-solutions-mdan-logrotate' RPM must be installed in order to create necessary permissions for a functional logrotate.

Note: Upgrading a device to the Android 6.0 Marshmallow operating system may create a different device ID in the registration history. This is an artifact of the new operating system and will not affect your service.

Note: Two or more characters must be entered into the search bar for results to begin to appear. The search will return results from both first and last names, title, and role.

Note: The plus icon on the top right corner of the screen will become gray when presenting an expired conversation.

Note: Some Status icons might not appear in the Status Bar if there are too many icons to display.

Note: When using Cisco 8821 handsets, use caution when navigating pages using the Back button. The last page viewed is not refreshed when the Back button is pressed; this may result in content that is outdated.

Note: Changing the device camera permissions for Engage Mobile while logged in as a user will cause the application to crash. When you restart the application, the most recent camera setting you chose will be stored in Vocera.

Note: While it is possible to deploy and update the Engage Mobile application on iOS devices via MDM or the Apple App Store, do not deploy devices in an enterprise using both methods. Deploying the Engage Mobile application using both MDM and the Apple App Store will result in APNS messages not being sent to all devices. Use only MDM to deploy and update devices in an enterprise environment.

Conclusion

This concludes the Warnings for the Vocera Directions For Use .

Installation

This section will guide a user through the installation information for the Vocera Engage Medical Device Alarm Notification product.

This section contains the Vocera appliance and virtual machine installation procedures.

Appliance Installation

This page contains the requirements and steps for a customer to install a physical appliance containing the Vocera Engage Medical Device Alarm Notification (Vocera EMDAN) product.

Overview

Follow the steps in this document to assemble an appliance rack to hold an Vocera appliance at the customer facility.

Be aware that there are a variety of rack units on the market, which may mean the assembly procedure will differ slightly. Refer to the installation instructions that came with the rack unit you are using.

For additional details on the appliance rack used in this page, see the SC512 User Manual.

Minimum Requirements for Appliance Environment

- A server rack capable of housing a 1U rack mountable enterprise appliance, 1.68"(w) x 14"(d) x 1.75" (h) and 25 lbs.
- 120VAC Switching, 4A max, 260 Watts
- 10 to 35 C (50 to 95 F) operating temperature
- 90% non-condensing operating relative humidity
- 887 BTU output, 12,000 hours, RFTB
- EMI Safeguards

⚠️ **Warning:** **Risk of Failure if Dropped or Subjected to Vibration.** Avoid dropping the appliance. Do not expose the appliance to vibration. Complete all Customer Acceptance Testing after installation to ensure proper functioning of the appliance.

Installing the Chassis into a Fixed Bracket Rack

In this process, first install the inner rail to the chassis, then install the outer rail to the rack, and finally install the chassis in the rack.

The chassis package includes two rack rail assemblies in the rack mounting kit. Each assembly consists of two sections: an inner fixed chassis rail that secures directly to the server chassis, and an outer fixed rack rail that secures directly to the rack itself. The package comes with "chassis ears" that allow the chassis to use generic rails.
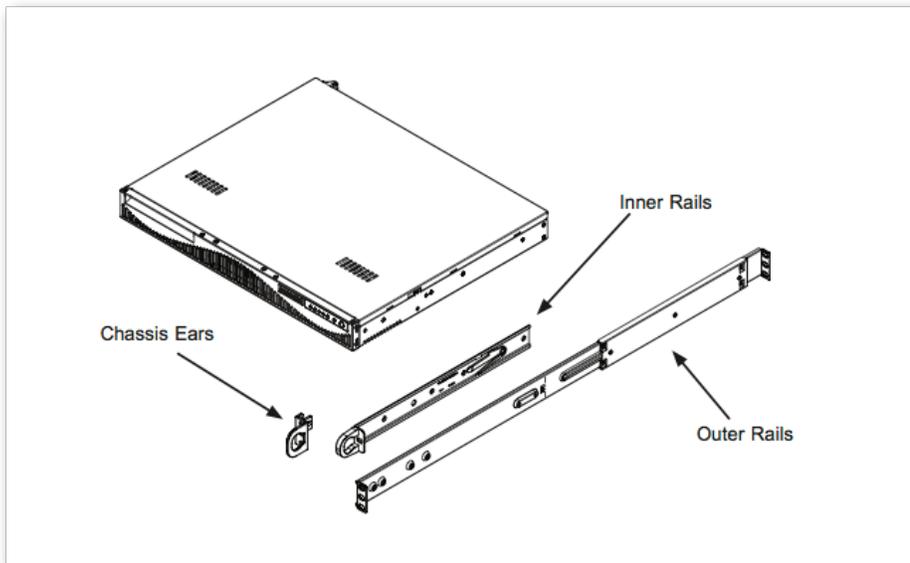
Warning: Electrical Hazard – Do not open the appliance case. Opening the case exposes personnel to the risk of electrical shock from contact with electrical components. Contact support and return the appliance to Vocera if needed.

Installing the Inner Rail Vocera

First locate and remove the three screws holding the chassis ear in place. Remove both chassis ears.

Then place the inner rail on the side of the chassis, aligning the hooks of the chassis with the rail holes. Use the figure below as a guide to position the rails on the chassis.
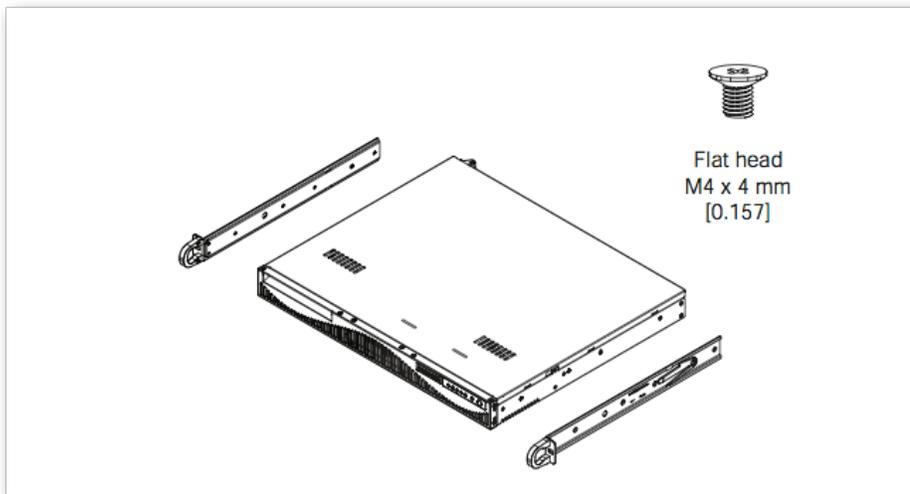
Slide the rail toward the front of the chassis to secure the rail in place. Secure the chassis with four flathead screws.

Repeat these steps for the other inner rail Vocera.

Installing the Outer Rails into the Rack

Attach the short bracket to the outside of the long bracket, aligning the pins with the slides as shown below. Both bracket ends must face the same direction.

Flat head
M5 x 12 mm [0.472]

Washer for M5

Secure to the
Rear of the Rack

Attach Outer Rack Rails
together

Secure to the
Front of the Rack
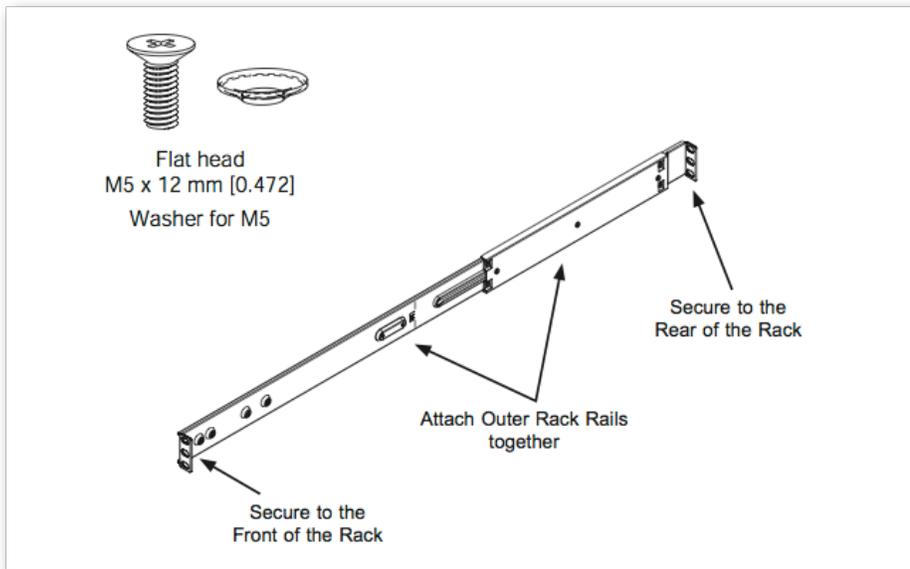
Adjust both the short and long brackets to the proper distance so that the rail fits snugly into the rack. Secure the long bracket to the front side of the outer rail with two M5 screws and the short bracket to the rear side of the outer rail with three M5 screws, as shown below. Use a washer with each screw.
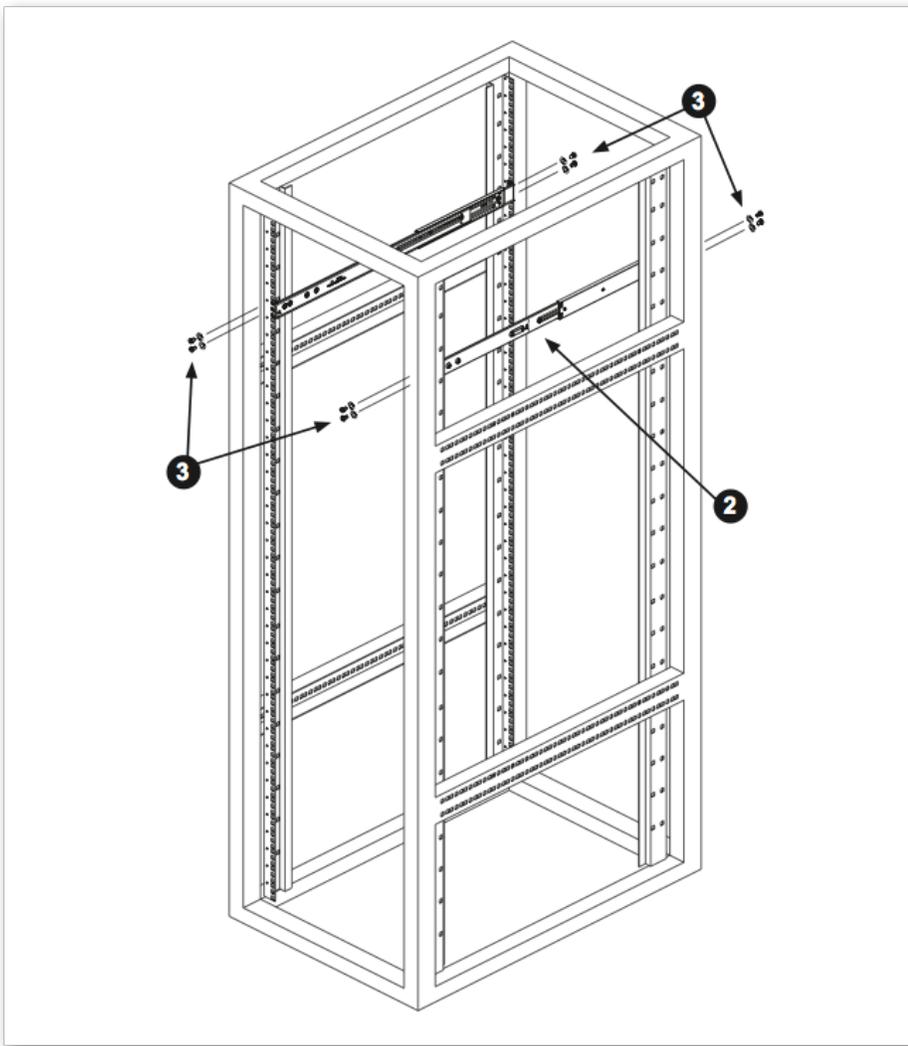
Repeat these steps for the other outer rail.

Installing the Chassis into the Rack

⚠️ **Warning:** Electrical Hazard – Protect the Vocera appliance power cord from fraying and any wiring from exposure. Prevent service or clinical personnel from receiving electrical shock due to contact with exposed wiring or power cords.

⚠️ **Warning:** Thermal Hazard – Ensure that there is adequate ventilation. Adequate ventilation is required to prevent the appliance from overheating, or a mechanical failure generating excessive heat. Inadequate ventilation may result in personnel receiving a burn from the appliance.

At this point, the inner rails are attached to the chassis and the outer rails are attached to the rack unit.

Now align the chassis rails with the front of the rack rails, as shown below.
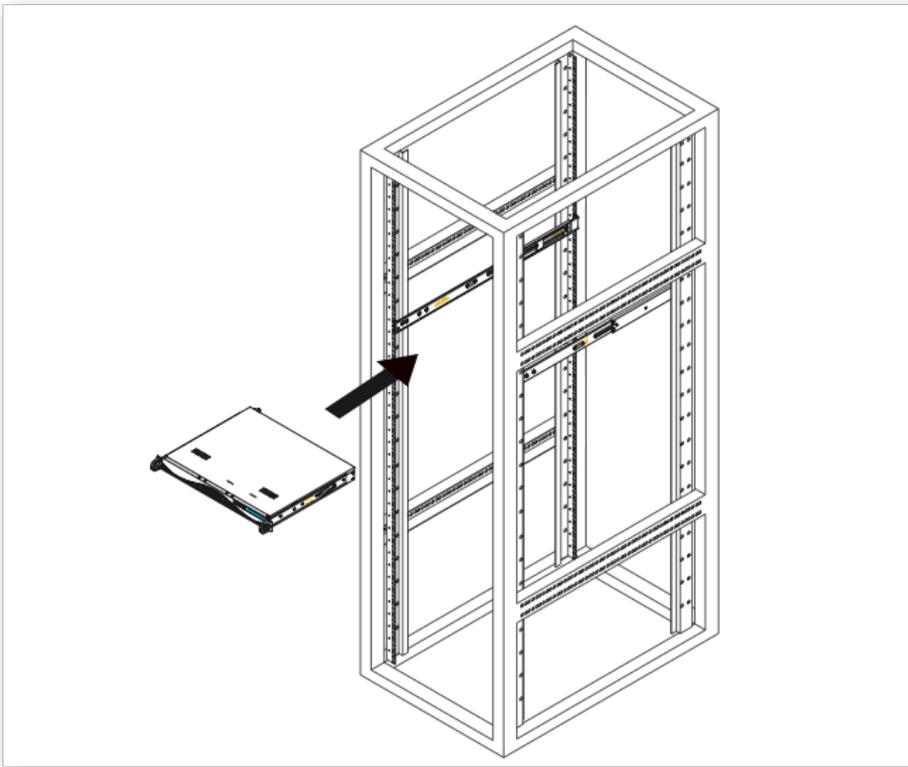
Slide the chassis rails into the rack rails, keeping the pressure even on both sides. It may be necessary to depress the locking tabs when inserting. When the server has been pushed completely into the rack, you should hear the locking tabs "click" into the locked position.

Insert and tighten the thumbscrews that hold the front of the server to the rack.

Installing the Chassis into a Telco Rack

The compact design allows the chassis to be installed into a Telco rack without use of rails. These steps describe how to install the chassis into a mid-mount Telco rack.

First, remove the chassis rails and the chassis ears if the ears are installed at the front of the chassis.

Locate the three screw holes in the middle of the chassis and secure the ears to the chassis with three flat head screws. Make sure the screws are secure, but do not over tighten the screws.
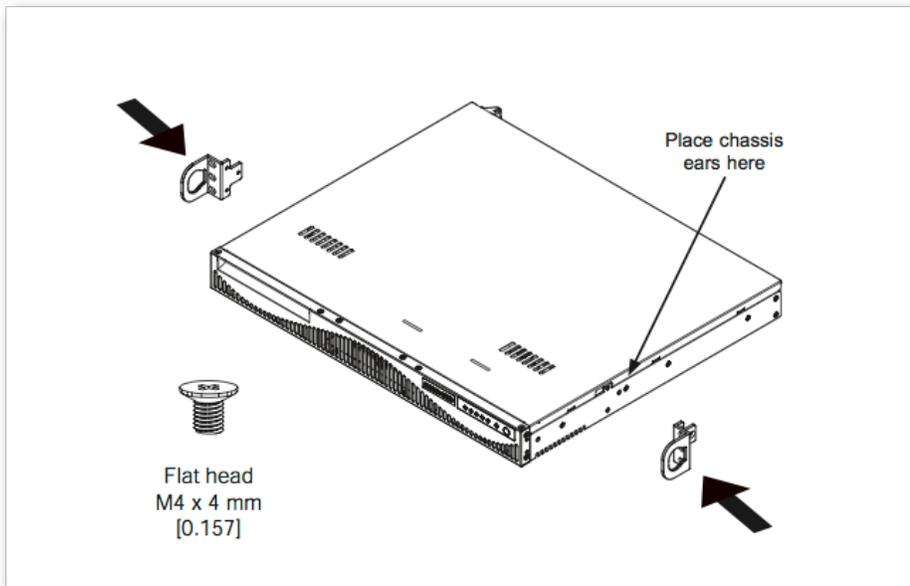
Hold the chassis in the telco rack and screw the chassis to the rack using the three screw holes located in the chassis ears, as shown below. Now the chassis is held in place by the chassis ears and does not slide in and out of place.
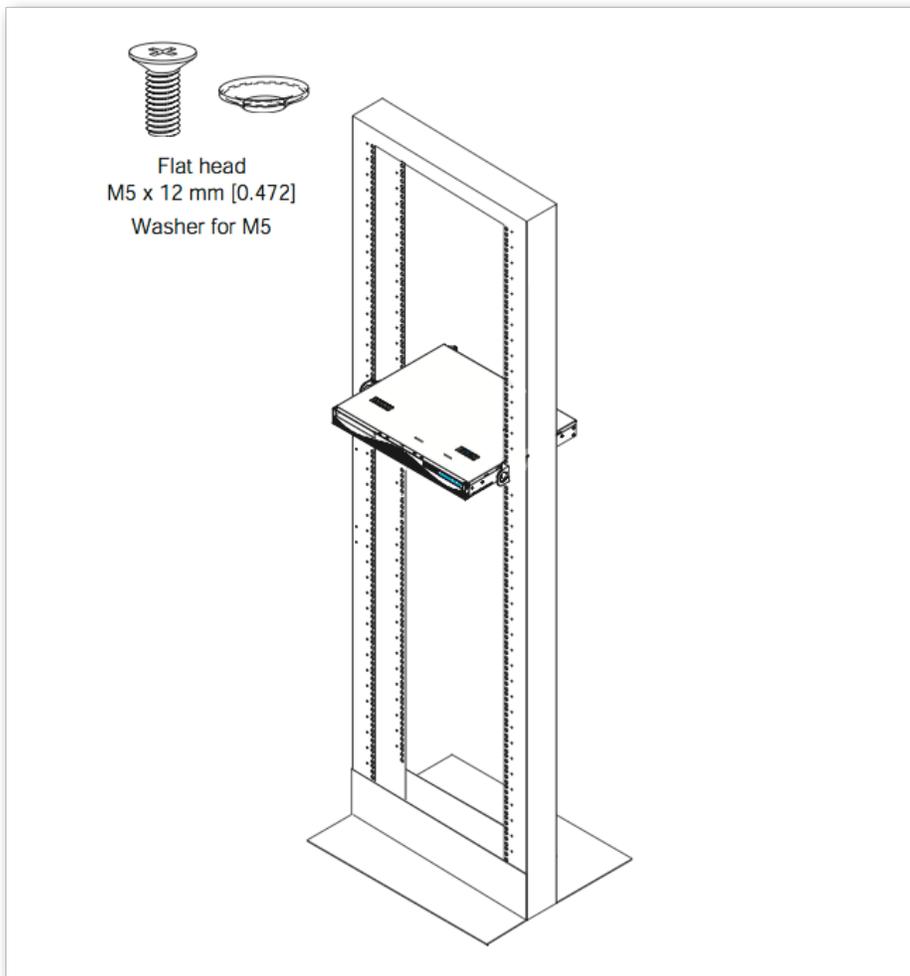
Conclusion

This completes the steps for installing the physical appliance in a facility.

Virtual Machine Installation

This page contains the complete set of instructions required for a customer to download and install a virtual machine (VM) containing the Vocera application.

Overview

In addition to the set of instructions on this page, Vocera will provide the FTP site and login credentials to access the appliance. The virtual machine (VM) is provided as an .ovf file containing the entire VM and application.

Requirements

A virtual machine host is required. This document contains instructions for installing the Vocera VM on a host system running VMWare using the vSphere client program. Please refer to the instructions for your facility's VM host program.

Browser Requirements

- Microsoft Internet Explorer version 10 or later
- Firefox version 47 or later
- Apple Safari version 10.10 or later
- Chrome version 53 or later

Network Requirements

All network segments from the monitor to the fixed or mobile communication device should have a network latency for an 8000 byte packet of no more than 70 milliseconds, or an end-to-end latency of no more than 500 milliseconds.

The following table describes the firewall requirements which should be configured in order to successfully install, update, and support the Vocera Engage application and its operating system.

Port	Destination	Purpose
22	svc.ext-inc.com (199.180.201.227)	Remote Support (SSH)
443	svc.ext-inc.com (199.180.201.227)	Initial Server Provisioning Port must be left open for Remote Support
443	yum.ext-inc.com (199.180.201.238)	Upgrade repository for OS & Application

VM Requirements

The Vocera VM requires the following resources.

Component	Specification
Network Addresses	1 – Static IP address with network connectivity to required data sources
Remote Connectivity	Remote connectivity via VPN client from Vocera Engage
Operating System	Support for Linux 64-bit operating system

The allocation of resources for the Vocera VM server (i.e., processor, memory, etc.) for optimal performance will depend on factors such as the volume of inbound data, processing overhead of the data type, and the complexity of the solution implemented. It is not always practical to conduct a detailed analysis at the start of every project to determine the correct hardware selection. The table below provides recommendations for the VM resource allocation. It uses two factors as criteria for the resource allocation based on information that must be known at the time the customer quote is completed:

1. Number of Beds – As an indicator of the volume of inbound data to be processed

2. Number of PS Days for Implementation – As an indicator of the complexity of the implemented solution, (i.e., number of workflows, number of integrations, etc.)

Using the Number of Beds and Number of PS Days information for a project, find the server type recommendation in the able below. The server types will be defined in another table further below.

Hospital Size / Solution Complexity	100 Beds Or Less	100 To 500 Beds	500 Beds Or Larger
30 Days Implementation Or Less (Low Complexity Integration)	Small Server	Medium Server	Medium Server
30 To 50 Days Implementation (Medium Complexity Integration)	Medium Server	Large Server	Large Server
50 Days Implementation Or More (High Complexity Integration)	Large Server	Large Server	Large Server

When a deployment is expected to have multiple phases, the VM selection generally should allow for the computing requirements in all phases, not just the requirements expected in the first phase.

The ideal target for resource utilization when the server is running in steady state should be the CPU load at one or below, and the disk input/output average wait time per transaction should be less than 100 milliseconds. When the CPU load number approaches or exceeds the number of cores allocated to the server, it is an indication of an overloaded condition; possible overload causes can be either too low disk input/output throughput or under-powered CPUs for the given workload.

Resource Specifications

The following table of information is provided as a recommendation based on observations of existing customer installations. The installed hardware infrastructure in a customer's data center may not allow for an exact match to the specification below. When an exact match is not possible, the selected hardware should approach the performance of the recommended setup. The website http://www.cpubenchmark.net provides performance information on a wide span of processors, making it possible to compare a given customer's hardware against the recommendations listed below.

For photo storage information and resource specifications on the Media appliance, see the Media appliance and adapter documentation.

Server Size	CPU	Memory	Storage	CPU Benchmark
Small	Four Cores, Intel Xeon E3-1225 V2 @ 3.20GHz	8GBytes RAM	100GBytes HDD	http://www.cpubenchmark.net/cpu.php?cpu=Intel+Xeon+E3-1225+V2+%40+3.20GHz

Server Size	CPU	Memory	Storage	CPU Benchmark
Medium	Four Cores, Intel Xeon E5-2640 @ 2.50GHz	16GBytes RAM	300GBytes HDD	http://www.cpubenchmark.net/cpu.php?cpu=Intel+Xeon+E5-2640+%40+2.50GHz
Large	Eight Cores, Intel Xeon E5-2690 @ 2.90GHz	16GBytes RAM	500GBytes HDD	http://www.cpubenchmark.net/cpu.php?cpu=Intel+Xeon+E5-2690+%40+2.90GHz

Appliance Sizing Calculation

Active customer sites may want to calculate the database size that will work best for them, given their space and time parameters. The following information is provided to calculate High Availability (HA) capacity of the appliance's database size per active bed per unit time, and historical archive appliance needs.

Step	Process	Calculation
1.	Count the number of locations that alerts are delivered to	Locations = Beds + Tele-pack locations + Other (or, Locations = Beds * 130%)
2.	Determine how long data will stay on the primary appliance	Assume 1 year's worth of data
3.	Determine how long data will stay in long term storage on the reporting server or archive appliance	Assume 20 years' worth of data
Total	**Number of HA Appliances * Appliance Storage + Long Term Storage**	

Downloading the VM

Using a web browser, navigate to the FTP site and log in with the provided credentials.

Download the VM files to a location that can later be accessed by your VMWare vSphere client.

- The VM consists of three files; *.vmdk, *.mf, and *.ovf.
- Note that the download of these files could take several hours as they will total over 3 GB.
- Use an FTP client that supports "resuming downloads" due to the large size of the files to be downloaded.

Installing the VM

Install the Vocera VM via the virtual machine host program supported by your facility. The following steps describe importing the VM using VMWare's vSphere client.

Warning: Disable the Snapshot feature of VMWare. Leaving the Snapshot feature enabled can cause the VM to lose connectivity for an extended period of time. The client should manually take a snapshot of their VM immediately before and after any upgrades.

1. Launch the VMWare vSphere client and log into the ESX host on which you plan to install the Vocera Engage VM.
2. From the vSphere client, navigate the following path: File > Deploy OVF Template > Deploy from File.
3. Using the Browse button, navigate to the *.ovf file previously downloaded, select the file, and then select Next.
4. Enter an appropriate name for the Vocera appliance, such as "Vocera", and then select Next.

5. Select the appropriate networking options, and then select Next.
6. Revise the deployment settings to the required disk size, memory, and number of cores shown in the table above.
7. Select Finish.
8. Power on the VM.

Conclusion

The appliance is now ready for configuration by the Vocera Implementation Engineer (IE). Please reach out to your designated IE who will set the static IP address of the VM and enable your administrator login capabilities.

Vocera Backup Best Practices and Disaster Recovery

This page contains the best practices for backup procedures and disaster recovery to employ for a customer's Vocera appliance.

Introduction

Vocera recommends that customers follow these best practices for backup procedures and disaster recovery.

The Engine's Backup functionality creates backup files of the entire database, including stored patient data and configured adapters. The backup files provide insurance against loss of information and configuration.

In this page the Database Backup Configuration section lists the tasks necessary to ensure that backup files are captured and stored. The steps to perform these tasks are documented in the Engine's Backup Database wiki page for Vocera internal users.

Database Backup Configuration

Configure daily backups to complete on every primary production Vocera server, whether Virtual Machine (VM) or physical appliance.

Always export the daily backup to the secondary Vocera server; Vocera requires that customers provide a secondary production server.

Configure daily backups to export to an external, customer-provided by FTP, SFTP, or SMB.

Retain aminimum of 10 backups in the secondary appliance and external storage location.

Virtual Machines

Vocera strongly recommends that customers do not complete VMWare Snapshots or other forms of daily snapshots of the Vocera server. Customers should only complete VMWare Snapshots when an Vocera representative can watch the system. See the attached VM Snapshots Product Bulletin for additional information.

Vocera highly recommends that a VM backup is taken prior to the initial deployment, as well as before and after any major Vocera system changes.

Disaster Recovery

In the event of a catastrophic failure, complete the following steps to restore the Vocera system.

1. Restore the latest VM backup. (This backup would have been taken prior to any major changes, and while working with Vocera employees.)
2. Retrive and restore the latest available daily system backup from the external storage location.
3. With the assistance of Vocera Communications Support, bring the Engage application and adapters back up in the necessary order.
4. Test all system integrations and verify that they are working properly.

5. Test all clinical workflows to ensure they have been restored and are working properly.

Contraindications

Information about when the Vocera EMDAN product should not be used.

Introduction

This section of the Directions For Use is intended to describe when the device should not be used (contraindications). The device should not be used under known or reasonably foreseeable hazardous conditions where the risk of use clearly outweighs any possible benefit.

Contraindications

Vocera Communications Engage Medical Device Alert Notification is contraindicated as a primary alarm notification system for medical devices or medical device system alarms.

Vocera Engage Medical Device Alarm Notification is contraindicated in the event of any of the following foreseeable hazards of which users should become aware:

- when the network connection indication on the alarm notification device (e.g., mobile device) shows the absence of a network connection,
- in the event the alarm notification device appears to be inoperable or damaged in any way,
- in the event the alarm notification device is not turned on, correctly registered with Vocera Engage Medical Device Alarm Notification , or the user is not logged in to the mobile device, or
- in the occurrence of Vocera Engage Medical Device Alarm Notification system warnings indicating that system operation exceeds specifications or some error condition or the failure of some system on which Vocera Engage Medical Device Alarm Notification depends for proper functioning.

Risks and Benefits

The risks and benefits of the Vocera Communications EMDAN product.

Introduction

This section of the Directions For Use is intended to provide a thorough understanding of the effects and expectations associated with the appliance. The goal of this risk/benefit information is to aid you in deciding to use the appliance in a given situation, and to ensure that you use the appliance as labeled.

Risks and Benefits

Alarm notification is a function that is critical to patient safety and effective nursing vigilance. As the number of alarming medical devices used at the bedside has grown, concerns about effective alarm notification and response has likewise grown. For a summary of issues surrounding alarm notification, see the AAMI report on clinical alarms from the 2011 summit, convened by Association for the Advancement of Medical Instrumentation (AAMI), FDA, the Joint Commission, American College of Clinical Engineers (ACCE) and ECRI Institute.

Properly used, secondary alarm notification systems can be an effective tool in improving alarm notification responses. The following is a discussion of the risks and benefits associated with Vocera Engage Medical Device Alarm Notification and similar secondary alarm notification systems.

Risks

Warning: Alerts delivered to mobile devices might be considered primary alarms by caregivers. Continue to remind users that Clinical Alert notification is secondary and always continue to monitor patients at primary patient monitors.

- Vocera Engage Medical Device Alarm Notification is a secondary alarm notification system, and is not intended to replace the primary alarm notification provided by medical devices themselves or medical device systems (e.g., central stations). While caregivers are not always at the bedside or nursing station, and may use Vocera Engage Medical Device Alarm Notification for those brief periods away from, and possibly out of hearing of, medical device primary alarm notification, it is NOT RECOMMENDED that staff render primary medical device alarms inoperable or silent.

- Before a secondary alarm notification system is applied to manage medical device alarms, industry best practices should be followed in configuring the alarms on the medical devices themselves. Alarm parameters and limits should be reviewed, and where necessary, adjusted to ensure adequate alarming without producing nuisance alarms, i.e., a high volume of alarms that are false/positive or for which there is no clinical action required. Best practices for managing alarms at the medical device are outside the scope of these directions for use, but information is available from AAMI, the Joint Commission, the ACCE, and the National Patient Safety Foundation. Users of secondary alarm notification systems are strongly encouraged to review and optimize their medical device alarm policy and procedures prior to implementing Vocera Engage Medical Device Alarm Notification.

- Vocera Engage Medical Device Alarm NotificationVocera Engage Medical Device Alarm Notification is embodied in the Vocera appliance. The operation of Vocera Engage Medical Device Alarm Notification is dependent on the operation of this appliance. Installation specifications for the appliance for power, network connectivity, environmental controls, backup power, and SMTP and SNMP system monitoring should all be met at installation and maintained throughout the use of the system.

System Dependency Risks

The Operating Information Checkout procedure has been designed to provide users with a convenient validation process to ensure that all of the systems are working at the beginning of a shift. The use of this procedure is strongly encouraged.

An alarm may appeared to be canceled, but is not, when a patient monitor goes into a fail state and generates an alarm cancelled message. The caregiver training should include proper action instructions for alerts, and routine equipment inspection and calibration should be scheduled in the hospital.

To work properly, Vocera Engage Medical Device Alarm Notification is dependent on a number of other systems: the medical device system(s) communicating alarms, the system providing nurse to patient staff assignments, the staff-carried mobile device intended to communicate alarm notifications and responses, and the IT infrastructure (wired and wireless networks, servers, and computers) that supports all of these systems. The risks associated with each of these sub-systems will be discussed in the following sections.

Medical Device System

Vocera Engage Medical Device Alarm Notification can only annunciate alarms received from medical devices. Should the medical device system stop communicating alarms, Vocera Engage Medical Device Alarm Notification will no longer receive any alarms to communicate to staff. This risk can be mitigated by ensuring your medical device system is configured for high reliability (check with your medical device manufacturer for recommendations). To ensure that communications between the medical device system(s) and Vocera Engage Medical Device Alarm Notification are working, remote system monitoring is recommended so that staff is notified of any failures so that down-time procedures can be implemented and the failure corrected (check with your medical device manufacturer and IT department for recommendations).

Staff Assignment

The proper functioning of nurse to patient staff assignments is required to direct alarms to the responsible caregiver. Due to escalation features of Vocera Engage Medical Device Alarm Notification , alarms will be received by a caregiver on the unit, even when no nurse to patient staff assignment is made for a given patient. However, for optimal performance, it is important that nurse to patient staff assignments be made for each patient on the unit at each shift change. Staff should also be aware that receiving alarms for patients they are not assigned to cover may indicate incomplete or incorrect nurse to patient staff assignments. Should a caregiver receive alarms for patients they are not assigned to cover, a supervisor should be notified and nurse to patient staff assignments should be checked to ensure they are correct and complete for that shift.

Mobile Devices

Vocera Engage Medical Device Alarm Notification relies on properly configured and operating mobile devices (typically wireless phones) carried by staff receiving alarm notifications. Devices must be properly registered and configured within their own system (e.g., phones provisioned with their phone switch). Proper configuration is confirmed through user acceptance testing upon installation, and should be repeated by the customer, or Vocera, each time subsystems are changed in any way.

To ensure that staff receive the messages and alarms intended for them, it is critical that when staff comes on shift, that they "sign on" to their staff-carried device, and that they are registered within Vocera Engage Medical Device Alarm Notification . Staff-carried devices are wireless and only work when they are associated with the wireless network. These mobile devices provide a visual indicator (typically a stylized antenna icon, or signal strength indicator bars) that shows whether the device is connected to the network. Users should develop a habit of watching the wireless network visual indicator to know when they may be disconnected from the network and unable to receive alarms.

Vocera Engage Medical Device Alarm Notification is configured to escalate alarms that do not receive a response to back-up caregivers. When the mobile device is not configured correctly, then alerts cannot be delivered to the correct caregiver and caregiver action is delayed. This may occur when no user, or an incorrect user, is associated with the mobile device in the mobile device system, or when a hospital has multiple mobile device servers from different manufacturers and a mobile device is configured to work on the wrong mobile device system. Users should follow the mobile device OEM DFU for the mobile device system, and follow the checkout procedures in the Vocera DFU .

The Administrator should see the Vocera Installation instructions for device configuration. Built-in-escalations will alert secondary or tertiary caregivers in the event the primary or secondary caregivers fail to respond. Primary, secondary and tertiary recipients can be configured as groups. Caregivers cannot call one another if their phones are a part of a different phone system. When a hospital has multiple mobile device servers from different manufactures, a mobile device on one server cannot contact a phone on a different server. The Customer Acceptance testing before go-live should address multiple mobile device servers at the site, and should also require acknowledgement of a successful wireless site survey.

The SpectraLink OAI system has a set maximum number of access points that will not allow any additional devices to connect when all points are in use, creating the hazard where OAI network access points overload and caregiver action is delayed. It is important to limit the number of people in escalation paths when using OAI hardware, and to not assign groups to be recipients when using OAI hardware.

IT Infrastructure

Vocera Engage Medical Device Alarm Notification is dependent on properly working IT infrastructure to operate. This infrastructure includes the appliance, client computers, wired and wireless networks. Should any of these infrastructure components fail to meet Vocera Engage Medical Device Alarm Notification specifications, or fail completely, alarm notification may be delayed, interrupted, or become inoperable. It is important that IT monitoring best practices (typically with a variety of Simple Network Management Protocol (SNMP) monitoring tools) be followed to ensure that IT infrastructure continues to operate within specifications and that IT support is notified in the event of a failure so that users may adopt down time procedures and so that failures may be corrected.

Benefits

- Unlike with conventional alarms where every user is theoretically exposed to every medical device alarm on a unit, Vocera Engage Medical Device Alarm Notification conveys alarms to the responsible caregiver via a nurse carried mobile device that annunciates the alarm and vibrates.

- Vocera Engage Medical Device Alarm Notification is a closed loop alarm notification system; should the primary caregiver decline or not respond to an alarm, the system automatically escalates the alarm to a designated back up caregiver. Depending on the facility's configuration, should the backup caregiver not respond, then the alarm may be escalated again to a group. Each alarm notification includes information on the status of the alarm, whether it is a primary alarm, or escalated to the secondary or third level. For alarm systems that are designed to repeat an alarm, such as Philips, the alarm will be repeated and escalate until a response is made and the alarm condition ceases.

- Unlike audible alarms that include limited information in the alarm signal (typically just the type of medical device and alarm priority), Vocera Engage Medical Device Alarm Notification conveys clinical context about the alarm. This context includes the identity of the patient generating the alarm, alarm description text or label, alarm priority, and medical device contextual data that is available at the medical device.

- Vocera Engage Medical Device Alarm Notification log files provide a detailed timeline of alarm generation, delivery, and response to aid in sentinel event investigations and as a management tool to improve alarm responses across units.

Conclusion

This completes the risks and benefits discussion.

Expectations

This page describes what to expect with use of the Vocera Engage Medical Device Alarm Notification product.

Introduction

This section of the Directions For Use is intended to describe what to expect before, during, and after the use of the device.

Expectations of the Device

Vocera Engage Medical Device Alarm Notification is intended as a secondary alarm notification system where alarm notifications are received from medical devices and automatically dispatched to the responsible caregiver. Users may expect this solution to perform in a safe and effective manner when it is used and maintained in ways described in these directions for use. These user and customer responsibilities are divided between overall system specifications, configuration and performance that must be maintained continuously, and user operation of the system that occurs on a shift by shift basis.

The proper operation of Vocera Engage Medical Device Alarm Notification is dependent on meeting and maintaining basic system configuration and operating specifications that are of an ongoing nature, and are often the responsibility of Clinical Engineering and/or IT. The installation process of Vocera Engage Medical Device Alarm Notification ensures that these configuration and specifications requirements are met upon installation. User acceptance testing ensures that Vocera Engage Medical Device Alarm Notification is configured properly, and that the supporting IT infrastructure (servers, computers and networks) are operating at levels specified for safe and effective operation.

After installation and end user acceptance of the system, responsibility for maintaining system configurations and specifications becomes the responsibility of the customer. Other than the changes entailed with daily use, any time a change is made in Vocera Engage Medical Device Alarm Notification or related subsystems (medical devices, nurse-carried mobile devices, appliance/server, computers, wired and wireless networks) the user acceptance test should be repeated to ensure continued safe and effective operation. These changes include:

- redesign, reconfiguration, refurbishment or upgrade of existing IT infrastructure,
- replacing hardware with new models of the product, or models from different manufacturers,
- updating, patching or replacing application software in any system component,
- updating or patching firmware, system software or operating system software, or
- reconfiguring escalations or resources (e.g., units, rooms/locations and users) in Vocera Engage Medical Device Alarm Notification .

The configuration and specifications requirements for subsystems may be found in Vocera Engage Medical Device Alarm Notification installation guide. Any questions about the potential impact of changes to systems may be directed to Vocera Communications Customer Support.

The proper use of Vocera Engage Medical Device Alarm Notification is the responsibility of users and the system administrator(s). End user activities revolve around staff shifts. At the beginning of a shift, users must follow the Operating Information Checkout procedures. These procedures include:

- nurse to patient staff assignments for every patient, and
- staff must log onto their mobile devices so that each mobile device is associated with the staff person carrying it that shift.

During the shift, users are expected to respond to alarms through their mobile devices as described in these directions for use.

Importance of Adhering to the DFU

The importance of following instructions regarding the Vocera EMDAN product.

Introduction

This section of the Directions For Use is intended to explain the importance of following the instructions.

Importance of Adhering to the DFU

Vocera Engage Medical Device Alarm Notification requires certain configuration and user actions to provide safe and effective alarm notification. It is critical that the user review and understand the Directions For Use . Special attention should be directed to the warnings highlighted in this manual.

Adverse Events

Information about adverse events found in published literature related to the Vocera Engage Medical Device Alarm Notification product.

Introduction

This section of the Directions For Use (DFU) is intended to provide information about any adverse events found in published literature.

Adverse Events

Numerous adverse events are reported in the FDA MAUDE database for secondary alarm notification systems. In the majority of these adverse events, the outcome was patient death. The following sample reports are representative of adverse events occurring with secondary alarm notification systems:

- Misuse: alarm notification system was used as primary alarm notification rather than secondary alarm notification (report number 1218950-2003-00175)
- Misuse: nurse to patient assignment not made, resulting in alarms not going to the caregiver (report numbers 1218950-2005-00254, 2124823-2006-00017)
- Misuse: leads-off alarm not responded to during shift change (report number 1218950-2007-00485)
- System failure: nurse to patient assignment could not be completed due to latent software defect (report number 961193)

Users should be sure to be familiar with Vocera Engage Medical Device Alarm Notification Directions For Use and to review the section on Safety Warnings.

Warranty

Warranty information for the Vocera Engage Medical Device Alarm Notification product.

Introduction

This section of the Directions For Use (DFU) is intended to describe the warranty information for the medical device.

Warranty

Vocera Corporation warrants that for a period of thirty (30) days following the installation of the Software that the Software will perform in accordance with the applicable documentation when operated on the designated equipment and sufficient connectivity requirements; and Vocera Corporation will use reasonable commercial efforts consistent with industry standards to search for and remove any viruses from the Software before installation. If EXTENSION, LLC cannot substantially correct a breach of these warranties in a commercially reasonable manner within ninety days after receiving notice from you, you may terminate this EULA and obtain a refund of the applicable license fee. This paragraph states your exclusive remedy for a breach of the warranties set forth herein. EXTENSION, LLC DOES NOT GUARANTEE THAT THE SOFTWARE WILL PERFORM ERROR- FREE OR UNINTERRUPTED OR THAT EXTENSION HEALTHCARE WILL CORRECT ALL SOFTWARE ERRORS. EXCEPT AS SET FORTH HEREIN, NO OTHER WARRANTY WITH RESPECT TO THE SOFTWARE IS MADE BY Vocera Corporation AND Vocera Corporation EXPRESSLY DISCLAIMS ANY AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, DATA ACCURACY, INTEGRITY AND NONINFRINGEMENT. Vocera Corporation does not warrant the accuracy of codes, prices, or other data contained within the Software that has been integrated into or included in the Software. Pricing information provided by such Software does not constitute an offer to sell or to purchase. If you transfer or relocate the Software without the express permission of Vocera Corporation, all obligations under the warranties described in this section terminate. The warranties do not apply to your: (a) failure to follow, in all respects, our written recommendations or instructions; (b) using or combining the Software with products or services that are not specified as compatible with the products or services of Vocera Corporation and without Vocera Corporation's written consent;; (c) installation of the software outside the United States;; (d) breach of your obligations hereunder; or (e) third party Software.

Operating Information

This section of the Directions For Use contains information regarding the operation of Vocera Engage Medical Device Alarm Notification , such as maintenance and disposal.

Checkout Procedures

The steps to perform to ensure the equipment is working correctly at the start of a shift.

Introduction

This section of the Directions For Use is intended to describe the checkout steps required for safety and effectiveness in using this medical device.

Checkout Procedures

At the start of each shift, staff should check to be sure the equipment is working correctly before they begin to perform their tasks on the unit. The nursing staff should verify that their assigned mobile device is working correctly. Staff with management responsibility should ensure that the web browser is functioning as required. Contact support for assistance if problems occur.

Checkout procedures for the user consist of the following steps.

- Swap the device's batteries. Place the charged battery in the device, and put the used battery into the charger.
- If using a smartphone, place the device in the charging station. The user should select a fully charged unit.
- Check with Nurse Managers or House Supervisors to see if problems have been reported.
- Check the "Recent Deliveries" view of the Alert Tracking workflow in the Administrator Menu. If messages are listed, the system is at least partially functional. If no messages are listed, it may indicate a problem, depending on the hospital's message volume.
- Send a test alert and check the time between alarm initiation on the medical device equipment and the alert receipt on the mobile device. Total latency should be under 5 seconds.

Monitor the Device

This page describes the importance of monitoring device activity.

Introduction

Vocera provides facilities with alerting and device messaging functionality that allows staff to efficiently perform their responsibilities. Optimal use of EVocera Engage Medical Device Alarm Notification is dependent on a number of subsystems and the user actions and awareness. During use of the Vocera Engage Medical Device Alarm Notification solution, it is important that users maintain awareness regarding the operation of the overall solution.

This section of the Directions For Use is intended to describe the importance of monitoring the activity of the device.

Monitoring the Device

Vocera Engage Medical Device Alarm Notification will send a notification to your device when an alert is received. It is important to monitor the activity and use of your device. As you become more familiar with the solution and devices this will be easier as you will know what to expect on a day to day basis. This section will help you during the transition period while you familiarize yourself with the device and processes. Regardless of problem, if you feel that it has been too long since your last alert or message please refer to the Troubleshooting guide for common issues and solutions.

Connectivity of the Mobile Device

It is important to note the wireless coverage of your facility. For example, does the wireless coverage extend to inside an elevator? In many instances it will not; therefore you will not receive alerts or be able to send messages. While most of your activity will keep you within your coverage area, it is important to note that there may be areas of your facility that simply do not have coverage. If you feel that too much time has passed since your last message or alert, look at the device to see if you currently have connectivity to the wireless network. This can be determined by looking at the screen to see if you have a wireless icon on your mobile device.

In the event of a network failure, you may lose device connectivity to the wireless network. Again, being aware of the activity, or lack of activity from Vocera Engage Medical Device Alarm Notification via your device, and visually inspecting the wireless network icon on your device screen can help you identify a potential network failure and implement down time procedures. Please follow your facilities' down time procedures.

Vocera Engage Medical Device Alarm Notification monitors IT infrastructure, including the network, and will automatically generate messages notifying the staff of problems. Be aware that should you lose network connectivity of the device, you will not be able to receive messages from Vocera Engage Medical Device Alarm Notification until network connectivity is restored.

Handset Battery Life

In some instances the battery life of the mobile device may be the cause of not receiving alerts and messages. The instructions at shift change are to replace the battery in the device with the battery that is in the charging unit. For smartphones, the instructions are to place the device in the charging station and pick up a fully charged device. This may not have occurred. Additionally, towards the end of the life of the battery you may notice that the charge will not hold as long as it did at the beginning of its life. This can be checked by looking at the screen on the device and making note of the battery life icon.

Maintenance Instructions

The maintenance activities required for the device including maintenance, software updates, database backups.

Introduction

This section of the Directions For Use is intended to describe the maintenance activities required for the device.

Maintenance Instructions

Vocera Engage Medical Device Alarm Notification requires a mobile device, and a computer system with a web browser. There is minimal maintenance for the end user. All maintenance is completed via a push method. This allows Vocera to push necessary changes directly to the user without user intervention.

Software Updates

Periodically, Vocera will release updates to our software, and upgrades to the capability of our system. This is completed in a planned fashion with your facility's IT department. We will provide release notes detailing the proposed changes to current software, new functionality that will be released, and any known issues at the time of release. There is no action required on the part of the user. The software updates will be pushed out and take effect automatically.

Database Backup

Daily, at 4am, the server will create a backup of the Vocera database. This database is in a ready state and able to be restored to a client site. This may be necessary in the case of loss of data, loss of server hardware, or a similar situation which would require a restoration of the database. Vocera Support is able to provide this service at any time required, 24 hours per day, 7 days a week. As an extra precaution, in the event of a hardware failure, the database backup should be configured to export to a network shared drive on the customer's local network. This option is configured within the Vocera Admin Console.

Storage Instructions

The storage and storage conditions for the Vocera Engage Medical Device Alarm Notification product.

Introduction

This section of the Directions For Use is intended to describe the proper preparation for storage and storage conditions.

Storage Instructions

Vocera Engage Medical Device Alarm Notification requires a Virtual Machine (VM) or Physical Machine that will host the Vocera operating system and software.

Vocera Engage Medical Device Alarm Notification requires a mobile device and a computer system with a web browser. See the equipment manufacturers' websites for storage information on their products.

Disposal Instructions

How to safely dispose of the solution.

Introduction

This section of the Directions For Use is intended to explain how to safely dispose of the solution.

Disposal Instructions

The Vocera solution requires a physical machine that will host the Vocera operating system and software. Vocera realizes that a situation may arise that would include the disposal of the physical machine. It is important to note that some Personal Health Information (PHI) may still exist within the machine; therefore it is important to dispose of the system appropriately.

Virtual Machine Disposal

Vocera recommends following your internal procedures for the destruction of a virtual machine. There will be no physical hardware to dispose of, due to the nature of a virtual machine.

Conclusion

The prior recommendation should not be used in place of your facility's processes and procedures in regards to the destruction of data and disposal of machinery. This recommendation is provided in lieu of any processes or procedures in your facility and should be used as a guideline to develop your own.

User Assistance Information

Links to the publicly-accessed user assistance information for the Vocera Engage Medical Device Alarm Notification .

Introduction

This section of the Directions For Use corresponds to the Guidance on Medical Device Patient Labeling section that is intended to advise users on how to get help for problems with the device.

The Vocera User Assistance information is provided on the corporate website, where it is available to the public and allows easy access to the following important documents:

- General Terms and Conditions
- Assurance Policy
- End User License Agreement
- Privacy Policy