Vocera WLAN Requirements and Best Practices

Notice

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

Last modified: 2021-05-05 23:08

ED-Device-Vseries-Production-Docs build 37

Contents

WLAN Requirements and Best Practices

This document summarizes the required settings and best practices for Vocera system implementations.

You can find more detailed information in the *Vocera Infrastructure Planning Guide*, available for download at: **https://pubs.vocera.com/device/vseries/production/help/vseries_vig_help/index.html**

Note: This document is not comprehensive and applies to the setting recommendations for Vocera only. See the documentation specific for each access point to get information on all the available settings.

WLAN Settings

The required and recommended WLAN settings and values are listed in this topic.

The following table displays the required WLAN settings.

Setting	Required Value
Voice Grade Site Survey	Required
Transmit Power	• B3000 (2.4 GHz)#Max 15dBm (30 mW) and Min 11 dBm (12.5 mW) • B3000n (2.4 GHz)[1]#Max 17dBm (50 mW) and Min 12dBm (16 mW) • B3000n (5 GHz)#Max 16 dBm (40 mW) and Min 13 dBm (20 mW) • V5000 (5 GHz)#Max 17 dBm (50 mW) and Min 13 dBM (20 mW)
Minimum Power Coverage	-65 dBm
Second Access Point Coverage	-65 dBm
Minimum SNR (B3000n Badge)	+ 25 dB
Minimum RSSI (V5000 Smartbadge)	-70 dB
Noise Floor	- 90 dB
Beacon Interval	100
DTIM	1
Priority Queue	Highest—Voice
Radio Channel Utilization	30%
Channel Width	B3000n Badge: • 2.4GHz—20 Mhz • 5 GHz—20Mhz or 40Mhz V5000 Smartbadge • 5 GHz—20MHz, 40MHz, or 80MHz Vocera recommends 20 MHz.

The following table displays the recommended WLAN settings.

[1] For 2.4GHz environments that include a combination of B3000 B3000n, and V5000 devices. Set the values provided for B3000 and not the values specified for B3000n.

Settings	Recommendations
Code Version	Vocera recommends that you use the most recent version of Controller and AP code with an assumption that code version is accurate.
Basic Data Rate	Data Rates Determine the rate as needed for each site.
Supported Data Rates	Determine the rate as needed for each site.
Channel Plan	• 2.4 GHz—1, 6, 11 • 5 GHz—36, 40, 44, 48, 149, 153, 157, 161[2] **Note:** Avoid channels 120, 124, 128, 144 if possible. Monitor DFS channels near an airport. If you are using DFS channels, broadcast the SSID in beacons for B3000n benefit.
Roaming Policy	2—May adjust based on AP density.
Max Number of SSIDs	5
Client Exclusions	Disabled
Authentication Timeouts	Add session timeout of at least 1 full shift.
Max Retries	4

The following table displays the multicast recommendations.

Setting	Recommended Value
Multicast Configuration	• PIM (Sparse Mode or Sparse Dense Mode) must be applied to all Vocera VLANs and the WLC management VLAN. • Enable IGMP Snooping on APs and all L2 devices in the multicast audio path. • Block all unnecessary multicast traffic.

The following table displays the association delays caused by authentication.

Authentication Type	Association Delay	Comments
Encrypted	Varies	Avoid using the options WEP, TKIP, and Mixed.
PSK	< 100 ms	PSK often provides the optimal trade-off between security and performance. **Note:** Vocera recommends using PSK.
EAP-FAST LEAP	200 ms	Frequent session timeouts can result in additional delays. **Note:** For EAP-FAST and LEAP, use CCKM (only for B3000n), OKC, or 802.11r to cache credentials and optimize roaming times.
PEAP EAP-TLS	Varies	The association delay caused by authentication varies based on the cipher strength (1024 bit or 2048 bit) and the depth of certificate chains. **Note:** For EAP-TLS and PEAP, use CCKM (only for B3000n), OKC, or 802.11r to cache credentials and optimize roaming times.

Cisco CAPWAP

The recommended values for Cisco CAPWAP are listed in this topic.

[2] For UK: Channel 149 - 161 are not available.

Setting	Recommended Value
RRM—Dynamic Channel Assignment	Interval should be more than 8 hours. It is the typical duration of one nursing shift.
RRM—Dynamic Transmit Power Control	Enabled if the maximum and minimum transmit power levels meets Vocera's recommended settings.
Transmit Power Threshold	Adjust to fit site.
Coverage Hole	Disabled If Coverage Hole Detection is necessary, enable it with the following settings: • Set Voice RSSI (-60 to -90 dBm) to -70 • Set Min Failed Client Count per AP to 12
Aggressive Load Balancing	Disabled
Multicast Mode#Global	Enabled Disable Mobility Multicast Messaging if multicast is not properly enabled in network. It causes one-way audio or no audio.
AP Multicast Mode	Multicast
Flex Connect	Centralized Mode or Distributed mode. **Note:** For Vocera voice this option is not recommended. If you have a need to enable this option, contact Vocera Technical Support.
Multicast Tx Data Rate	Highest data rate. 12Mbps and 24Mbps as mandatory data rates. **Note:** Vocera highly recommends to disable 11b rates (1,2,5.5, 11) on the AP.
Unicast-ARP	Disabled
WMM	Enabled
U-APSD	Enabled
DHCP Address Assignment (required setting)	Disabled
Symmetric Mobility Tunneling	Enabled
Priority Queue	Platinum
Client Load Balancing	Disabled
Band Select	Disabled
Frame Aggregation	Disabled on transmit or receive for Traffic ID 6 (voice) and 7 (network control)

Aruba Networks

The recommended values for Aruba access points are listed in this topic.

Settings	Recommended Value
Minimum Controller Code	6.1.3 **Note:** Aruba Controller Code 6.3 and below does not support IGMP V3.
Role	Voice
ARM	Enabled if honoring maximum and minimum transmit power levels.
Voice Aware Scanning	Enabled
Tx Data Rates	2.4 GHz—6, 9, 11, 12, 18, 24 5 GHz—Data rates change depending on the site
Probe Retry	Disabled
Max Tx Failure	25

Settings	Recommended Value
Session ACL	vocera-acl
Mcast-rate-opt (needed for multicast to go at highest rate)	Enabled
Multicast Filters—Use the Aruba Policy Enforcement Firewall (PEF) to configure these multicast filters to block traffic.	netdestination HSRP Host 224.0.0.2 netdestination VRRP host 224.0.0.18 netdestination RIP host 224.0.0.9 netdestination OSPF host 224.0.0.5 host 224.0.0.6 netdestination PIM host 224.0.0.13 netdestination EIGRP host 224.0.0.10

Extreme Networks - Extreme Cloud Appliance

The recommended values for Extreme Networks - Extreme Cloud Appliance are listed in this topic.

Setting	Recommended Value
Minimum Basic Rate (MBR)	Based on Site Survey MIN 12
Radio Share Mode	Off
DTIM	1 To support multicast group calls
Multicast Bridging	Enabled
Multicast Rule	VLAN Predefined Multicast Rule **Vocera Mcst** added to rule list.
Radio Management (11k) support	Enabled
Admission Control	Disabled (Default)
Fast Transition (FT)	Disabled If Fast Transition is required, contact Vocera Technical Support.

Ruckus Networks

The recommended values for Ruckus access points are listed in this topic.

Setting	Recommended Value
QOS	High, Smartcast enabled on WLAN
Smart-Roam	Disabled
VLAN	Dedicated non-native VLAN
Authentication/Encryption	WPA2/AES (802.11i)
Wireless Client Isolation	Disabled
WLAN Background Scanning	Disabled
Power Level	2.4 GHz—25 mW 5 GHz—50 mW
Directed-Multicast and Broadcast	This setting is required. Turn off conversion of broadcast and multicast to unicast on the WLAN interface using the following commands: • **ruckus(config-wlan) #** no qos directed-multicast • **ruckus(config-wlan) #** qos directed-threshold 0
Band steering, load balancing	Disabled

Setting	Recommended Value
Mesh	Disabled
Proxy ARP and ARP Broadcast Filter	Enabled
DHCP Relay Agent	Enabled
Inactivity Timeout	720 (12 hrs)
Minimum BSS Rate	Depends on AP density
Hiding SSID in Beacons	Not recommended
Controller Code	Latest from Ruckus

Meru Networks

The recommend values for Meru Networks is listed in this topic.

Setting	Recommended Value
SSID	Separate for Vocera.
IGMP Snooping	Enabled
QoS Rules	Enable QoS Rules 7 and 8. It is enabled by default.
Virtual Port	Disabled **Note:** Vocera recommends that you do not use Virtual Port.
Virtual Cell [3]	Enabled
Badge Roaming Policy	1
Silent Client Polling	Enabled
Vocera Location Feature	Disable Virtual Cell or divide APs into zone.
Multicast setting	Configure UDP Broadcast Port 5555 for Badge Discovery for Meru.

[3] A Transmit Power Asymmetry problem may arise at the edges of Virtual Cell coverage if the transmit power of an AP is higher than the Vocera device (~30mW). To avoid poor audio at the edges of the Virtual Cell, the RSSI of the Vocera device on the AP must be verified. The Vocera device should never drop below an RSSI of -75dBm.

IP Port Usage

The primary communication platforms provided by Vocera—the Vocera Platform, the Vocera Voice Server, and Engage Platform—require you to open specific IP ports to allow each server and its clients to communicate with each other.

Vocera Voice Server IP Ports

The port numbers that must be open for Vocera Voice Server IP communication are listed in this topic.

The following table indicates the ports that must be open for Vocera Voice Server communication.

Port Number	Protocol	Source	Destination	Direction
5002	UDP	Badge	Vocera Server Signaling	Bidirectional
5002	UDP	Badge	Vocera Server Signaling	Bidirectional
5001	TCP	Vocera SIP Telephony Gateway	Vocera Server Signaling	Outbound
5006	TCP	Vocera Client Gateway	Vocera Server Signaling	Outbound
5400	UDP	Badge/Badge Property Editor	Updater Signaling	Bidirectional
8011	TCP	Badge Property Editor	Localhost (127.0.0.1)	Bidirectional
5100	UDP	Badge	Vocera Server Audio	Outbound
7200-7263	UDP	Badge	Vocera Server Audio Recording	Inbound
80 and 443 (for SSL)	TCP	Browser	Apache Signaling	Bidirectional
8005	TCP	Tomcat	(Listening)	Inbound
8009	TCP	Apache Tomcat Connector	(Listening)	Inbound
8080	TCP	Tomcat HTTP Connector	(Listening)	Inbound
7500 - 8900 [4]	UDP	Vocera Server	Badge/VCG/VSTG Audio	Outbound
3306	TCP	MySQL Signaling	(Listening)	Inbound
5005	TCP	Vocera Server	VMI Clients	Bidirectional
5007	TCP	Vocera Server	VMI Clients (TLS)	Bidirectional
5251	TCP	Vocera Server	VAI Clients	Bidirectional
5251	TCP	Vocera Server	Vocera Report Server Signaling	Bidirectional
5251	TCP	Vocera Server Cluster Signaling	(Listening)	Inbound
5555 and 5556	UDP	Badge	Vconfig (Vch) Signaling during Discovery	Bidirectional
5555 and 5556	TCP	Badge	Vconfig (Vch) Signaling during Discovery	Bidirectional
7023	TCP	Nuance Watcher Telnet Client	(Listening)	Inbound
7890	UDP	Nuance Watcher	(Listening)	Inbound

[4] Only even-numbered ports are used. The range is configurable in `\vocera\nuance\SpeechServer\config\NSSserver.cfg`.

Port Number	Protocol	Source	Destination	Direction
27000	TCP	Nuance License Manager	(Listening)	Inbound
5060, 5062	TCP	Nuance Speech Server (listens)	(Listening)	Inbound
5060, 5062	TCP	Nuance Speech Server (allows UDP connections)	(Listening)	Inbound
8200	TCP	Nuance Recognition Server (nuance-server.exe)	(Listening)	Inbound
7777	TCP	Nuance Resource Manager; used only when multiple recognition servers are configured	(Listening)	Inbound
8202, 8204, and 8206	TCP	Nuance Recognition Server (nuance-server.exe); each additional port used only when dual/triple/quad recognition servers are configured	(Listening)	Inbound
7780	TCP	VA Flume agent	Vocera Analytics	Bidirectional
9091	TCP	Administration Console	Vocera Server	Bidirectional
9445	TCP	VA Service Monitor	Vocera Analytics	Bidirectional

The following table indicates the ports that must be open for Vocera SIP Telephony Gateway communication.

Port Number	Protocol	Source	Destination	Direction
5060	UDP	IP PBX	Vocera SIP Telephony Gateway Signaling	Bidirectional
5300-5555[5]	UDP	Vocera Server	Vocera Sip Telephony Gateway Audio	Outbound
8700 - 9467 [6]	UDP	IP PBX	Vocera Sip Telephony Gateway Audio (RTP/RTCP)	Outbound
Any free port	UDP	Vocera Server	Vocera SIP Telephony Gateway Signaling	Outbound

The following table indicates the ports that must be open for Vocera Client Gateway communication.

Port Number	Protocol	Source	Destination	Direction
6300-5200	TCP[7]	Smartphone	Vocera Client Gateway Signaling	Bidirectional
5200 - 6300[8]	UDP	Badge	Vocera Client Gateway Audio	Outbound
6300 - 6555 [9]	UDP	Vocera SIP Telephony Gateway	Vocera Client Gateway Audio	Outbound
7700 - 8467 [10]	UDP	Smartphone	Vocera Client Gateway Audio (RTP/RTCP)	Outbound
any free port	TCP	Vocera Server	Vocera Client Gateway Signaling	Outbound

The following table indicates the ports that must be open for Vocera Report Server comunication.

Port Number	Protocol	Source	Destination	Direction
5251	TCP	Vocera Server	Vocera Report Server Signaling	Bidirectional
8080	TCP	Report Console (Browser)	Apache Tomcat	Bidirectional

[5] Only even-numbered ports are used. The range is configurable in `\vocera\nuance\SpeechServer\config\NSSserver.cfg`.
[6] The number of ports used is based on the number of lines configured. The maximum number of lines is 256 with 2 ports (RTP and RTCP) for each, or 512 total. The server multiplies 512 by 1.5 to reserve additional ports in case some ports are already in use, resulting in 768 ports. The base port for this range is configurable.
[7] If the Use VCG client connection management option is set, the protocol is TCP. Otherwise, it is UDP.
[8] The number of ports used is based on the number of lines configured.
[9] The number of ports used is based on the number of lines configured.
[10] The number of ports used is based on the number of lines configured.

Port Number	Protocol	Source	Destination	Direction
9090	TCP	Report Console	Report Server	Bidirectional
80	TCP	Report Results	(Listening)	Inbound
3306	TCP	MySQL port	(Listening)	Inbound

The following table indicates the ports that must be open for Badge communication.

Port Number	Protocol	Source	Destination	Direction
5002	UDP	Badge	Server Signaling	Bidirectional
5200	UDP	Vocera SIP Telephony Gateway	Badge Audio	Outbound
5400	UDP	Badge	Updater	Outbound
5555 and 5556	UDP	Badge	Updater Signaling	Bidirectional
5555 and 5556	UDP	Badge	Vconfig (Vch) Signaling during Discovery	Bidirectional
5555 and 5556	TCP	Badge	Vconfig (Vch) Signaling during Discovery	Bidirectional

The following table indicates the ports that must be open for Vocera Collaboration Suite communication.

Port Number	Protocol	Source	Destination	Direction
80 or 443 (for SSL)	TCP	Vocera Collaboration Suite Push Notification	(Listening)	Inbound
5060-5080 (SIP)	TCP[11]	iPhone and Android Smartphone	Vocera Client Gateway Signaling	Bidirectional
7700-8467	UDP	iPhone Audio	(Listening)	Inbound
7700-8467 32768-65536	UDP	Android Audio	(Listening)	Inbound

The following table provides the details of the WLAN ports used by Vocera clients.

Port Number	Protocol	Client	Direction	Server/Client	Type
5002	UDP	Badge	Inbound and Outbound	Voice Server	Signaling
5200	UDP	Badge	Inbound and Outbound	Badge, Voice Server, and Vocera SIP Telephony Gateway	Audio
5300-5555	UDP	Badge	Inbound	Vocera SIP Telephony Gateway	Audio
5400	UDP	Badge	Inbound and Outbound	Updater	Signaling
5555 and 5556	UDP	Badge	Inbound and Outbound	Voice Server	Discovery
5555 and 5556 [12]	TCP	Badge	Inbound and Outbound	Voice Server	Connection
6300-6555 [13]	UDP	Badge	Inbound	Vocera Communication Gateway	Audio
7500-8700	UDP	Badge	Inbound	Voice Server	Audio
80 or 8080 (for NIO)	TCP	Vocera Collaboration Suite for Android and iPhone	Inbound	Vocera Messaging Platform	Signaling (Data)
5060, 5888-5889	UDP	Vocera Collaboration Suite for Android and iPhone	Inbound/Outbound	Vocera Client Gateway	Signaling
32768-65536	UDP	Vocera Collaboration Suite for Android	Inbound and Outbound	Vocera Devices	Audio

[11] If the Use VCG client connection management option is set, the protocol is TCP. Otherwise, it is UDP.
[12] Ensure that you allow packets from TCP port 5556 to be received on any available port on the Vocera Voice Server.
[13] The base port for this range is configurable.

Port Number	Protocol	Client	Direction	Server/Client	Type
5005	TCP	VMI Clients	Inbound and Outbound	Vocera Server	Connection
5251	TCP	VAI Clients (Including Staff Assignment)	Inbound and Outbound	Vocera Server	Connection
8080	TCP	Vocera Collaboration Suite for Android and iPhone	Inbound	Vocera Server	Signaling

The following table indicates the ports that must be open for Vocera Analytics communication.

Port Number	Protocol	Source	Destination	Direction
9445	TCP	Voice Server (Remote Agent)	(Listening)	Inbound
4040	TCP	VA Server	Spark UI	Inbound
7778	TCP	VA Server (VMP Flume agent)	Spark	Bidirectional
7779	TCP	VA Server (Engage Flume agent)	Spark	Bidirectional
7780	TCP	Voice Server (VS Flume Agent)	Spark	Bidirectional
8443 (default) or user defined	TCP	VA Server (Reporting service)	(Listening)	Inbound
3306	TCP	Maria DB Signaling	(Listening)	Inbound

The following table indicates the ports that must be open for ASL communication.

Port Number	Protocol	Source	Destination	Direction
22	TCP	Each Vocera Server	Vocera ASL Server (asl.vocera.com)	Inbound (for ASL update) Outbound (for sending logs)

The following table indicates the ports that must be open for ASR Broker communication.

Port Number	Protocol	Source	Destination	Direction
443	TCP / HTTP2 / GRPC	ASR Broker	GCP Services	Outbound
5060	UDP / SIP	ASR Broker	Nuance	Bidirectional
6060	UDP / SIP	Voice Server	ASR Broker	Bidirectional
6060	TCP / MRCPv2	Voice Server	ASR Broker	Inbound
6075	TCP / MRCPv2	ASR Broker	Nuance	Inbound
6080	TCP / HTTP	Operational/Monitoring	ASR Broker	Inbound
6100-6499 (only even-numbered ports)	UDP / RTP	Badge	ASR Broker	Bidirectional
0/*	TCP / HTTP	ASR Broker	Voice Server(Grizzly HTTP Server)	Inbound
0/*	UDP / RTP	ASR Broker	Nuance	Bidirectional

Engage IP Ports

The port numbers that must be opened on the Engage Linux 5.x machine for effective communication are listed in this topic.

Port Number	Protocol	Source	Destination	Interface/Feature	Purpose
443	TCP	Engage Middleware Module	svc.ext-inc.com 199.180.201.227	-	Provisioning APNS certificate retrieval
22	TCP	Engage Middleware Module	svc.ext-inc.com 199.180.201.227	-	Remote Support

Port Number	Protocol	Source	Destination	Interface/Feature	Purpose
443	TCP	Engage Middleware Module	yum.ext-inc.com 199.180.201.238	-	Repository access for installing Ubuntu and Engage Middleware Module software updates
2196	TCP	Engage Middleware Module	feedback.push.apple.com 17.0.0.0/8	XMPP	Retrieve list of failed devices from Apple Push Notification Service (APNS) Outbound, to Apple
5223	TCP	Engage Mobile App, iOS device	*.push.apple.com 17.0.0.0/8	XXMP	Receive push notifications on Engage Mobile App, iOS device . According to Apple, the iOS device is using Wi-Fi, port 5223 must be open outbound and inbound to the Wi-Fi. If all devices are using 4G port 5223 is not required.
443	TCP	Engage Mobile	Engage Mobile	-	Workflow page access for Android and Engage Mobile App, iOS device s using a reverse proxy in a DMZ. Traffic from any address to Engage Middleware Module on port 443 must be open unless a reverse proxy is used.
443	TCP	Engage Middleware Module (all networks)	Reverse proxy	-	Workflow page access for Android and Engage Mobile App, iOS device s using a reverse proxy in a DMZ. Traffic from any address to the proxy on port 443 must be open. Using a reverse proxy also has an internal requirement for the proxy to access Engage Middleware Module.
443	TCP	External browser access (all networks)	Engage Middleware Module	-	When workflow page access for browsers outside the network is desired not using a reverse proxy. Traffic from any address to Engage Middleware Module on port 443 must be open unless a reverse proxy is used.
443	TCP	External browser access (all networks)	Reverse proxy	-	When workflow page access for browsers outside the network is desired not using a reverse proxy. Traffic from any address to Engage Middleware Module on port 443 must be open unless a reverse proxy is used.

Port Number	Protocol	Source	Destination	Interface/Feature	Purpose
5222	TCP	Engage Mobile iOS	Engage Middleware Module	XMPP	Client to server XMPP traffic use the well known port 5222.
5222	TCP	Engage Mobile iOS	Edge> Engage Middleware Module	XMPP	External XMPP traffic communicates with Engage Middleware Module through the Edge XMPP proxy on port 5222.
5269	TCP	Federated XMPP Server	Engage Middleware Module	XMPP	Federated server communication uses port 5269. Federation can be initiated in either direction. This does not need to be opened externally if only federating with servers on the internal network.
5269	TCP	Engage Middleware Module	Federated XMPP Server	XMPP	Federated server communication uses port 5269. Federation can be initiated in either direction. This does not need to be opened externally if only federating with servers on the internal network.

The following table indicates the internal network requirements

Port	Protocol	Source	Destination	Interface/feature	Purpose
443	TCP	Reverse proxy	Engage Middleware Module	-	Reverse proxy access to Engage Middleware Module when a proxy is used in a DMZ for external smart phone or external browsers.
22	TCP	Any SSH client	Engage Middleware Module	-	SSH access.
80	TCP	Any HTTP client	Engage Middleware Module	-	Admin Console and workflow access via HTTP.
80	TCP	Cisco Phones SpectraLink Phones	Engage Middleware Module	-	Workflow access from mobile devices.
443	TCP	Any HTTP client	Engage Middleware Module	-	Admin Console and workflow access via HTTPS.
8888	TCP	Any HTTP client	Engage Middleware Module	Mirth	HTTP access to Mirth client download and login.
8443	TCP	Mirth Client	Engage Middleware Module	Mirth	Mirth administration once client is downloaded.
389	TCP	Engage Middleware Module	LDAP Server	LDAP	LDAP default configuration for Active Directory.
2021	TCP	Engage Middleware Module	DigiBox	TAP / Serial Devices	Default non-secure DigiBox port.

Port	Protocol	Source	Destination	Interface/feature	Purpose
1322	TCP	Engage Middleware Module	Unite Connectivity Manager (UCM)	Ascom	Push interactive messages to Ascom devices.
5000 - 5004	TCP	UCM	Engage Middleware Module	Ascom	UCM responses to message delivery.
27015	TCP	Engage Middleware Module	Vocera Server	Vocera	Communicate with Vocera server.
25	TCP	SMTP Client	Engage Middleware Module	Incoming e-mail	Inbound SMTP messages for the incoming e-mail interface.
25	TCP	Engage Middleware Module	SMTP	Outgoing e-mail	Outbound SMTP messages from the outgoing e-mail interface.
6661	TCP	HL7 (LLP)	Engage Middleware Module	HL7	Inbound HL7 messages. This is the default port configured in Mirth. This might be changed or additional connections added. Any additional connections require opening the ports.
12000	TCP	Navicare Server	Engage Middleware Module	Navicare	Inbound Hill-Rom Navicare messages
2000	UDP	Carescape Network	Engage Middleware Module	Carescape	Time synchronization.
7000	UDP	Carescape Network	Engage Middleware Module	Carescape	Device discovery
7000	UDP	Carescape Network	Engage Middleware Module	Carescape	Alarm Messages
161	UDP	SNMP Client	Engage Middleware Module	SNMP	Query Engage Middleware Module for SNMP parameters.
161	UDP	Engage Middleware Module	SNMP Manager	SNMP	Send SNMP traps for audit events.

The following table indicates the inbound Engage Middleware Module ports.

Port	Protocol	Purpose
22	TCP	SSH access
80	TCP	HTTP access
443	TCP	HTTP access
6661	TCP	Default HL7 port
8443	TCP	Mirth HTTPS administrative access
8888	TCP	Mirth HTTP client access
161	TCP	SNMP