Wireless Network Configuration

For the Smart-hopping MX40s (865350, 865351), wireless network configuration happens as a part of the equipment label assignment procedure. The MX40s are shipped from the factory with an Equipment Label of "NEW_DEVICE" and an RF Access Code of "0". This allows basic wireless connectivity to any Smart-hopping Access Point. After the MX40 has basic connectivity to the Smart-hopping network, the "Label Assignment" procedure can be performed at the Information Center. The "Label Assignment" procedure configures the RF Access Code and Equipment Label into the MX40 without the need for any additional tools.

For the 802.11 a/b/g MX40s (865350), wireless network configuration must be completed before the equipment label assignment procedure can be performed. The WLAN configuration is done using the IntelliVue Support Tool – Mark2. See Chapter 9 of this document and also the IntelliVue Support Tool Instructions for Use for details.

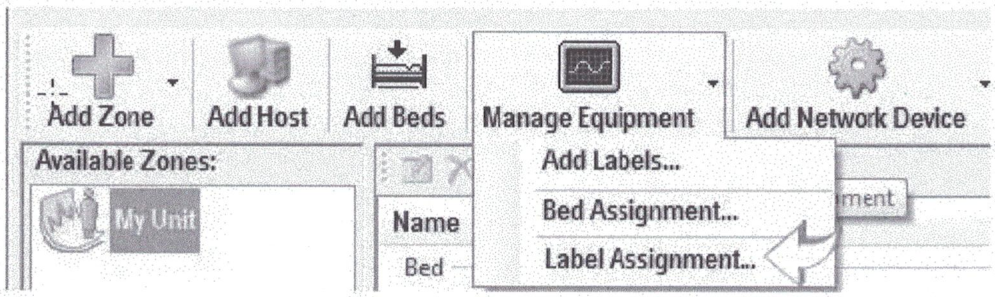
Need to Config before "label assignment"

Assigning an Equipment Label - IIC iX

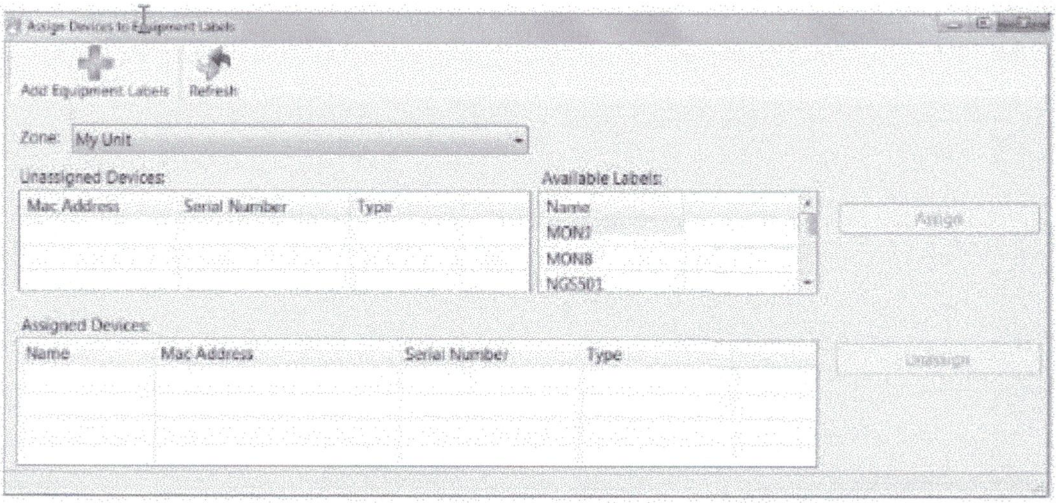
PIIC iX

➢ *To assign an equipment label to a device:*

Go to **Manage Equipment** > **Label Assignment**.



The **Assign Devices to Equipment Labels** dialog window opens.



Zone: My Unit

Name
MON3
MON8
NGS501

Click the desired label in the **Available Labels** list, then click the desired **Unassigned Device**.

Click the **Assign** button.

Assigning an Equipment Label - IIC

Non iX

➢ *To assign an equipment label to a device:*

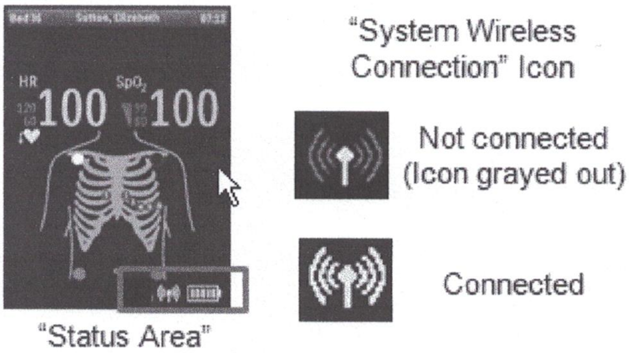
1 Select **All Controls** > **Label Assignment**.

2 Enter password (tele)

3 Insert battery power into the MX40 and if attached, disconnect the patient cable.

4 Select **Refresh**.

5 Confirm the connection to the wireless network as follows:


"System Wireless Connection" Icon
HR
SpO2
100
100
Not connected (Icon grayed out)
Connected
"Status Area"

6 Select the MAC address of the device from the **New Devices** list. If the address does not appear, remove battery power and re-insert. Select **Refresh**.

Note — The MAC address appears on the rear label of the MX40.

7 Select the desired equipment label from the **Equipment Label** list.

8 Select **Assign Label** to initiate programming of the equipment label and RF Access Code into the MX40.

9 When prompted, press **Confirm** on the MX40 to accept the assignment. The confirmation must occur within 30 seconds of the prompt.

10 On the MX40, wait for the New_Device label to change to the selected equipment label.

11 Confirm the label assignment by viewing the waveform in the Patient Sector at the Information Center.

WLAN Troubleshooting

Problem	Possible Cause	Solution
The MX40 fails to connect to Surveillance PIIC iX. MX40 displays inop **'No Central Monitor'** and Connection Status is in state **'None.'**	Status indicates that the MX40 does not have a network connection, or a radio "association" to the Access Point. There are several possible causes for this including: AP not turned on, or not connected to customer-supplied infrastructure properly.	Verify the AP is powered on and connected to the customer-supplied infrastructure properly.
	MX40 is not configured for the correct 802.11 radio modality (for the SSID setup (802.11a, 802.11bg, 802.11abg).	Check the configuration of the MX40 and verify radio modality is configured (refer to the MX40 service documentation). After the MX40 settings have been set via the IntelliVue Support Tool, make sure setting are Confirmed to ensure the settings are retained.
	MX40 not configured for the correct SSID. It must be the same as configured on the WLAN Controller.	Check the configuration of the MX40 and verify that the correct, case sensitive SSID is configured. Also, check the configuration of the SSID on the WLAN Controller. See "Step 1: Configure the ICN WLAN." on page 4-15 for the procedure. After the MX40 settings have been set via the Support Tool, make sure setting are Confirmed to ensure the settings are retained.
	MX40 not configured for the correct WPA/WPA2 pre-shared key, must be the same as configured on the WLAN Controller.	Check the configuration of the MX40 and verify that the correct WPA or WPA2 pre-shared key is configured. Check the configuration of the WPA/WPA2 key on the WLAN Controller. The default pre-shared key must not be used. See "Step 1: Configure the ICN WLAN." On page 4-15 for the procedure.
	MX40 is not seeing strong enough signals (-67 dBm or higher **when not body blocked**).	Deploy additional APs or adjust AP power levels to accommodate the required signal strength.
	MX40 was cloned and wireless settings were lost.	Configure the MX40 with the correct settings: SSID, WPA key, radio modality.
	MX40 not configured for the correct Country Code.	Do not change the MX40 country code from its default setting (1000). The default setting causes the monitor to use the country code provided by the AP to which it associates.
	Defective MX40.	If MX40 self test fails: 1. Verify issue persists with other MX40s. If so, verify CSCN WLAN settings. 2. If all settings are correct, replace MX40.

Problem	Possible Cause	Solution
MX40 fails to connect to Surveillance PIIC iX.	MX40 has a radio connection to the wireless infrastructure but has not been recognized by the Surveillance PIIC iX. Possible causes include:	
	MX40 not assigned to Surveillance PIIC iX. No Monitor label assigned to MX40 from Surveillance PIIC iX.	Assign patient monitor in to the Surveillance PIIC iX. Assign the Monitor Label to MX40 from Surveillance PIIC iX.
	Configuration problem using WEP, WPA(PSK), WPA2(PSK), or 802.1x. Authentication.	Verify the Mode, SSID, Country and Security settings in the MX40 match your installation.
	Configuration problem using WPA Enterprise or WPA2 Enterprise including 802.1x Authentication.	1. Check the connection Status. (Status message ... Conn.Status). If the state only shows "Scanning," make sure that the Mode, SSID, Country and Security settings in the MX40 Status screen are accurate. If not correct, correct the configuration using the IntelliVue Support Tool.
		2. Check the connection status. If the MX40 shows the state "Authenticating," the SSID, Mode, Country and Security settings are correct. If a WLAN connection to the Access Point is established, but the MX40 fails to authenticate, check the authentication server and WLAN controller error logs.
		3. As an investigation step, disable the CertificateCheck via the IntelliVue Support Tool (Configuration -> Hardware -> Network -> WLAN). If authentication is now possible, proceed with step 4. Otherwise, verify the authentication server configuration, WLAN controller configuration and the user credentials (User Name, Password, Anonymous Identity). If the previously used credential settings were incorrect, the MX40 is perhaps on the exclude list of the WLAN Controller. Resolve this issue on the WLAN controller. Note: Do not forget to re- enable the certificate check.
		4. Check the installed CA certificate using the support tool. - Task -> Clone from Medical Device - Open the cloned file using Configuration -> Configuration Editor - In Configuration Editor check Configuration -> Hardware -> Network -> WLAN -> Certificate 1 for validity (Valid from, Valid until).
		5. Make sure that the installed CA certificate is the root certificate of the authentication server certificate chain.

9. MX40 WLAN (P/N 865352)

This section provides information specific to the operation of the WLAN version of the MX40.

Important — MX40 WLAN (865352) requires compliance with Phillips Customer-supplied Clinical Network Specifications.

Short-range Radio and WLAN

Because at least 20 MHz separation is needed between the SRR channels and 802.11b/g (2.4 GHz ISM band) channels in order to source real-time waves over the SRR link, the MX40 WLAN device should only be used with Short-range radio when operating on the 802.11a (5.6 GHz) band. See Smart-hopping and SRR Channel Selection for 2.4GHz Smart-hopping Networks p. 2-15.

WLAN Configuration Parameters

1. First Highlight MX40
2. Click "Read from Device"
3. Save File in easy Place
4. Click "Configuration Editor"
5. Select File you Saved in Step 3

The MX40 WLAN configuration is loaded into the MX40 using the IntelliVue Support Tool - Mark2 (IVST Mark2). The parameter values are changed using the IntelliVue Support Tool Configuration Editor which is accessed from the IVST Mark2 "Configuration/Reports" table. The WLAN parameters can be found under **Hardware > Network**. There are two menu pages, **Network** and **WLAN**.

1 on MX40

Network

Many of the configuration parameters on the **Network** menu page do not apply to the MX40. See the table below.

Parameter	Applicable to MX40?	Available Selections	Comments
LAN IP Config			
Enabled	No	No	
Mode	No	No	
IP Address	No	No	
Subnet Mask	No	No	
Default Gateway	No	No	
WLAN IP Config			
Enabled	Yes	Off, On	Must be "On" for WLAN connection to function.
Mode	Yes	Off, DHCP, Manual, Bootp	The MX40 only supports "DHCP".
IP Address	No	No	
Subnet Mask	No	No	
Default Gateway	No	No	
DNS Config 1			
DNS Mode	No	No	
DNS Server 1	No	No	
DNS Server 2	No	No	
DNS Server 3	No	No	
IGS Server 1			
CI Mode	No	No	
CI Address	No	No	
CI TTL	No	No	

Parameter	Applicable to MX40?	Available Selections	Comments
IGS Server 2			
CI Mode	No	No	
CI Address	No	No	
CI TTL	No	No	
IGS Server 3	No	No	
CI Mode	No	No	
CI Address	No	No	
CI TTL	No	No	
IP Address Configuration			
IGMP	No	No	
CI Mode	No	No	
CI Address	No	No	
CI TTL	No	No	
QoS State	Yes	On, Off	To enable QoS, this must be configured "On", and WMM Mode on the WLAN page must be set to "Enabled".
QoS Level	Yes	0-7	A level of 6 is recommended.
Directory Mode	No	No	
Directory Address	No	No	

WLAN

Here are the parameters listed on the **WLAN** menu page.

Parameter	Applicable to MX40	Available Selections	Comments
General			
Country	Yes	1000	Not modifiable. A country code of 1000 allows the MX40 to adapt to the country code of the access point.
IP Address	Yes	0.0.0.0 can't change	Not modifiable. Uses DHCP for IP address.
WMM Mode	Yes	Disabled, Enabled	To enable QoS, this must be set to "Enabled", and QoS State on the Network menu page must be set to "On".

Parameter	Applicable to MX40	Available Selections	Comments
Security Mode	Yes	NotConfigrd, WEP, WPA (PSK), WPA2 (PSK), WPAEnterpr, WPA2Enterpr	WPA2-Enterprise is not recommended due to increased handover times.
Mode	Yes	None, Auto, 802.11ah, 802.11bg, 802.11g	
SSID	Yes	****	1-32 characters
WEP			
WEP Key Index	Yes	1, 2, 3, 4	This selects which WEP Key will be used.
WEP Key Size 1	Yes	104 Bit, 40 Bit	
WEP Key 1	Yes	****	10 or 26 hex characters based on Key Size 1,2,3,4,5,6,7,8,9,A,B,C,D,E,F
WEP Key Size 2	Yes	104 Bit, 40 Bit	
WEP Key 2	Yes	****	10 or 26 hex characters based on Key Size 1,2,3,4,5,6,7,8,9,A,B,C,D,E,F
WEP Key Size 3	Yes	104 Bit, 40 Bit	
WEP Key 3	Yes	****	10 or 26 hex characters based on Key Size 1,2,3,4,5,6,7,8,9,A,B,C,D,E,F
WEP Key Size 4	Yes	104 Bit, 40 Bit	
WEP Key 4	Yes	****	10 or 26 hex characters based on Key Size 1,2,3,4,5,6,7,8,9,A,B,C,D,E,F
WPA (PSK) / WPA2 (PSK)			
WPA Password	Yes	****	8-63 characters
WPA Enterprise / WPA2 Enterprise			
Authentication	Yes	NotConfigrd, PEAP, TTLS	If WPA / WPA2 Enterprise is selected, must select PEAP or TTLS.
Inner Authentication	Yes	NotConfigrd, PAP, CHAP, MSCHAP, MSCHAPv2	The MX40 only supports MSCHAPv2.
PEAP Version	Yes	Default, Version 0, Version 1	
PEAP Label	Yes	Default, EAP, PEAP	

Parameter	Applicable to MX40	Available Selections	Comments
Certificate Check	Yes	Disabled, Enabled	Should be "Enabled" is using a certificate. "Disabled" is provided for troubleshooting purposes.
User Name	Yes	****	0-63 characters
Password	Yes	****	0-63 characters
Anonymous Identity	Yes	****	0-63 characters
Certificate 1			
Friendly Name	Yes	****	0-32 characters
File	Yes	Add, Delete	
File Size	Yes		Not modifiable, reflects file chosen
Valid from	Yes		Not modifiable, reflects file chosen
Valid until	Yes		Not modifiable, reflects file chosen
PEAP Version	Default, Version 1, Version 2		
User name, Password	Yes	****	In EAP, PEAP mode this entry needs a User name and Password with 0-63 alpha-numeric characters. This identity is optionally used for the first authentication phase to hide the real user identity and four routing purposes. If the length is 0, "Not configured" is shown.
IGMP Mode (no user config required)	Yes	On	Enables IGMP support. No use of streaming multicast. IGMP is required to support IP Multicasting. Set to On with CI configured to Multicast. No user control.

WLAN Configuration Parameter Definitions

Network Parameter Definitions

These definitions are for the parameters that apply to the MX40.

WLAN IP Config – these are parameters that apply specifically to the wireless network adapter.

- "Enabled" under the WLAN IP Config section refers to the wireless network adapter in the MX40. When "Enabled" is configured "on" the wireless network adapter is on and active. When configured "Off", the wireless network adapter is in a low power sleep state.

- "Mode" under the WLAN IP Config section refers to the network configuration protocol the device uses when communicating over the 802.11 link. Although other selections may be available on the IntelliVue Support Tool Configuration Editor, the only network configuration protocol that the MX40 supports is DHCP.

IP Address Configuration – these parameters apply to the MX40 once the data reaches the wired network

- IGMP: IGMP (Internet Group Management Protocol) must be "On" to allow basic communication between the MX40 and the Information Center iX.
- QoS State: In order to enable Quality of Service for the MX40 data once it reaches the wired network, the "QoS State" parameter must be configured "On", and the "QoS Level" must be configured for a value greater than "0". Note: "WMM Mode" on the "WLAN" page must be configured for "Enabled" otherwise this setting will be ignored by the MX40.
- QoS Level: "QoS Level" sets the network QoS priority that the MX40 will use to tag packets. The QoS Level is used for both the wired and the wireless link. "0" is the lowest priority, "7" is the highest priority. A QoS Level of "6" is recommended for the MX40.

WLAN Parameter Definitions

General

- **Country**

  Not modifiable. A country code of 1000 allows the MX40 to adapt to the country code of the access point
- **IP Address**

  Not modifiable. The MX40 uses DHCP to obtain an IP address.
- **WMM Mode**

  This parameter enables or disables WMM (Wireless Multimedia Mode). Used for basic wireless quality of service. Note: "QoS State" on the "Network" page must be configured "On" and the "QoS Level" must be configured for a value greater than "0" otherwise this setting will be ignored by the MX40.
- **Security Mode**

  WEP, WPA(PSK) or WPA2(PSK), WPA-Enterprise and WPA2-Enterprise with either Protected EAP (PEAP) or Tunneled TLS (TTLS) as authentication methods. WEP is not recommended due to general security issues.
- **SSID**

  Service Set Identifier: Logical WLAN Network Name.

WEP

- **WEP Key Index**

  Defines the transmit WEP Key Index. This entry must match the WEP Key Index configured at the infrastructure device, i.e. on a WLAN Access Point, and ranges from 1 to 4.
- **WEP Key Size**

  The WEP Key Size 40 bit or 104 bit
- **WEP Key**

  The number of hex characters for the WEP key depends on the WEP key size chosen. For a 40 bit WEP key size the WEP key must be 10 hexadecimal characters long, for a 104 bit key the WEP key must be 26 hexadecimal characters long.

WPA

- **WPA Password**

  In WPA(PSK) or WPA2(PSK) mode this entry defines the Pre-Shared-Secret or Password with 8 to 63 alpha-numeric characters.

WPA Enterprise / WPA2 Enterprise

In WPA-Enterprise or WPA2-Enterprise mode the following parameters are used:

- **Authentication**

  The authentication method can be either Protected EAP (PEAP) or Tunneled TLS (TTLS).
- **Inner Authentication**

  For the MX40, PEAP and TTLS can only be used with MSCHAPv2 as the Inner Authentication method.
- **PEAP Version**

  This setting describes the PEAP protocol version to be used while authenticating against the authentication server. Valid values are Default, Version 0 and Version 1. If set to Default the decision is up to the wireless adapter. Version 0 or 1 forces the wireless adapter to use the protocol version required for a certain authentication server. This setting is intended for experts only.
- **PEAP Label**

  The PEAP label setting defines the string to be used to signal EAP-PEAP encryption to the authentication server. Valid values are Default, EAP or PEAP. Default leaves the decision up to wireless adapter. Both EAP and PEAP force the wireless adapter to use this setting. This setting is intended for experts only.
- **Certificate Check**

As long the Certificate Check is set to Enabled, the CA Certificate is used to verify the authenticity of the certificate chain delivered by the authentication server. The verification involves also the system time to check the validity period of every certificate in the chain. This item can only be set to Enabled, if an CA Certificate has been installed. Valid values are Disabled or Enabled.

- **Username**

  The username used in the encrypted tunnel with 1-63 alpha-numeric characters. It is also used as outer identity as long as the Anonymous Identity is not set.

- **Password**

  The password used in the encrypted tunnel with 8-63 alpha-numeric characters. Will be shown as four stars "****" after the user entered the password.

- **Anonymous Identity**

  The identity used for the outer PEAP or TTLS authentication, which may be "unprotected". Thus, the identity should be different to the Username for enhanced security. The Anonymous Identity contains

  1-63 characters. It can be set to NotConfigured by clearing it.

Certificate 1

- **Friendly Name**

  A certificate can be installed on the MX40, and when doing so, a "Friendly Name" of up to 32 characters can be assigned to it.