

# Network Management

---

## Administration Guide

OneVue Sense Environmental Monitoring

Publication date June 13, 2022

Copyright ©2022 Primex. All rights reserved.

Printed in the USA.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical or otherwise, for any purpose, without the prior written permission of Primex.

OneVue is a trademark of Primex. All other trademarks are the property of their respective owners.

Primex is the leading provider of solutions to automate and maintain facility compliance, increase efficiencies, enhance safety and reduce risk for enterprise organizations in the healthcare, education, manufacturing and government vertical markets. Primex delivers solutions that utilize a facility's existing network infrastructure to automate, monitor, document and report essential activities performed by facility staff. Our solutions include synchronized time, automated critical notifications and bell scheduling, and environmental and event monitoring.



Corporate Headquarters

965 Wells Street

Lake Geneva, WI 53147

Phone: 1-262-729-4853

[info@primexinc.com](mailto:info@primexinc.com)

# Table of Contents

About managing networks used by Primex network devices .....	4
Network management overview .....	4
Manage sensor gateway settings .....	5
Change the network assigned to a device .....	6
OneVue network requirements .....	7
Create, view, edit, and delete network profiles .....	10
Network Profile requirements .....	10
Create a new network profile .....	10
View all network profiles .....	12
View a network profile .....	13
Edit a network profile .....	15
Delete a network profile .....	16
View devices assigned to a network profile .....	17
Change network assigned to devices (migrate to new network) .....	18
Available device network migration methods .....	18
Migrate devices to new network from OneVue .....	18
Migrate sensor to a new (updated) network with the Primex Device Configuration software .....	21
Migrate sensor to a new (updated) network when networks are not managed in OneVue .....	23
OWDC app: Migrate Sensor to a new network .....	25
Upload EAP TLS certificate to Primex network device .....	29
Requirements .....	29
Install EAP-TLS certificate .....	29
Technical Support .....	30

## ABOUT MANAGING NETWORKS USED BY PRIMEX NETWORK DEVICES

A Network Profile in OneVue represents a network at your facility and each Primex network device is assigned to a network. Once assigned, the network settings are downloaded to the Primex device, which allows the device to connect to your facility's network to transmit data to and download settings from OneVue. For OneVue devices that receive time from an NTP time source, its assigned network also allows its connection to an NTP Server.

A Primex network device has an internal gateway, a component that manages its network connection and firmware. From a device's profile, you can manage its settings and also its settings available from its gateway profile. To view a device's gateway settings, from its profile select its Gateway ID link.

The sections below provide an overview of managing the networks assigned to your Primex network devices and the settings managed from a device's gateway profile.

### Network management overview

- **Device network requirements**

There are specific network requirements to allow Primex network devices to connect to your facility's network and transmit data to and download settings from OneVue.

Be sure to share the OneVue network requirements with your facility's IT staff.

- **Manage who has access to network profiles**

A user must be assigned to the Account Admin or Network Admin role to view or manage networks.

- **Create network profiles**

A Network Profile is a wireless or wired Ethernet network at your facility. A Primex device connects to its assigned network to transmit data to and download settings from OneVue.

If your organization's information security policies do not allow network setting data to be managed in third-party applications, device network settings can be configured from the Primex Device Configuration software.

- **Update a network profile**

If a Network Profile is assigned to a device, only the network label, location, and notes can be updated. If the network is not assigned to a device any of its settings can be updated.

- **Update or change the network assigned to a device**

Due to the importance of Primex network devices connecting to your facility's network, network settings are stored locally in each device. A change to a device's assigned network is required to be completed using one of the device network migration methods.

- **View devices assigned to a network profile**

You may need to view what devices are assigned to a Network Profile when planning a network change. Before making a change to a network in use by a Primex device, it's critical to first migrate your devices to another network to avoid a device losing its network connection.

- **Deleting a network profile**

You can only delete a Network Profile that is not assigned to a device. It's recommended to delete networks that are not in use by your Primex devices.

## Manage sensor gateway settings

The following settings are managed from the gateway profile of a sensor. To view these settings, from a sensor's profile select its Gateway ID link.

- **Network**

During its check-in sequence to OneVue, the device attempts to connect to this network first. If the connection fails, the device automatically attempts to connect to its alternate network.

- **Alternate Network**

This network serves as a backup network. When a device cannot establish a connection to its primary network, it automatically attempts to connect to its assigned alternate network.

- **Migration Network**

This network is assigned to the device when migrating the device to a new network. The migration network is what the device is to be migrated to. When the device establishes a connection to its assigned migration network, OneVue automatically sets the migration network profile to its primary network and clears its migration network.

- **Keep Micro Firmware at**

Identifies the current firmware version. When set to Latest, the device automatically downloads new firmware released by Primex. If not set to Latest, displays the device's current installed version. Primex strongly recommends that firmware is set to Latest (default setting). To view firmware release notes, select **View Change Log**.

- **Logging Interval**

Sets the frequency readings are logged and stored in the sensor's local internal memory. All logged readings are transmitted to OneVue at the frequency set in its Check-In Interval setting.

Although a sensor's Logging Interval sets how often readings are logged by the sensor and all logged readings are transmitted to OneVue during each check-in, a sensor continuously monitors its sampled readings. When a sampled reading is out of range, the sensor connects to the network and the out-of-range reading is automatically transmitted to OneVue.

- **Check-In Interval**

Sets the frequency the sensor connects to your facility's network to transmit its logged readings to OneVue.

- **Unresponsive Timeout**

The Unresponsive Timeout sets the maximum amount of time a Primex device can go without a check-in to OneVue. When this time limit is exceeded, the device is set to an Alarm state with an Unresponsive status.

- **Enable Audio Alert**

Primex sensors have an audio alert that is activated when in a reading Alarm state. The audio alert emits a series of beeps to notify the surrounding staff of the reading alarm condition. By default, set to disabled.

- **Resume Audio Alert After**

Duration of time the sensor's audio alert should resume after the silence button is pressed during a reading alarm.

- **Manual Configuration File**

File downloaded when manually configuring a device's network settings with the Primex Device Configuration software. The file contains the OneVue account ID and current assigned network settings.

## Change the network assigned to a device

A Primex network device requires a network connection to operate over your facility's network. During each network connection, a device transmits its data to and downloads data from your OneVue account. Due to the importance of devices connecting to your facility's network, network settings are downloaded and stored locally at each device. To avoid a device losing its connection to your facility's network, changes to a device's network is managed by performing a network migration procedure.

Listed below are the methods available to migrate a device to another network. The method used is dependent on how your organization manages the networks used by Primex devices and if you are locally at the device.

Method	Overview	When to use
OneVue network migration	A migration network is assigned to the device gateway. During its next check-in, the device attempts to connect to the migration network. If the migration network connection is successful, its primary network is updated to the migration network and the migration network is cleared.	<ul style="list-style-type: none"><li>• Networks are managed from your OneVue account.</li><li>• Current assigned network and migration network are both operating on network.</li></ul>
OneVue Wired Device Configurator (OWDC) app	The new network is added to OneVue. The Primex device is connected to an Android device with OWDC app. From the app, its assigned network is updated (migrated). Once connected to the new network, it checks-in to OneVue and its network is updated.	<ul style="list-style-type: none"><li>• Onsite at facility and locally at a device.</li><li>• Networks are managed from your OneVue account.</li><li>• Troubleshooting a network connection and testing network connection onsite.</li></ul>

Method	Overview	When to use
Primex Device Configuration software	<p>Device connects to computer with software installed.</p> <p>To change (migrate) a device's assigned network.</p> <ul style="list-style-type: none"> <li>• Add a Network Profile with the updated network settings.</li> <li>• Set the device's migration network to the new Network Profile.</li> <li>• From the device's gateway profile, download the manual configuration file.</li> <li>• Connect the device to your computer. From the software, enter the new network settings directly into the software and then upload the file downloaded from the device's gateway profile.</li> <li>• Once the device connects to the new network, it checks-in to OneVue and its assigned network is updated and its migration network is cleared.</li> </ul>	<ul style="list-style-type: none"> <li>• Onsite at facility and locally at a device.</li> <li>• Troubleshooting a network connection and testing network connection onsite.</li> <li>• Current assigned network is no longer available or not correct, which requires migrating the device to a new network.</li> <li>• Networks are managed from your OneVue account or networks are not managed or stored in your OneVue account. When not managed, this is commonly due to information security policies restrict storing network setting data in third-party applications.</li> <li>• Device requires EAP-TLS certificate to authenticate with network. Certificates are uploaded to device using the software.</li> </ul>

## OneVue network requirements

The information below provides the details required to allow Primex network-enabled devices to communicate over a facility's network to OneVue. Details include device Wi-Fi, PoE, and Ethernet network communication protocols, and network port and firewall requirements.

### Network communication protocols

The OneVue platform is designed, developed, and managed in-house, allowing Primex to control the user experience and provide the highest level of reliability and security.

To support the myriad of network security and protocol standards in today's business environment, Primex network-enabled devices offer an array of options for secure network connectivity. This ensures our customers can use and leverage our full line of products without adding costly additional IT infrastructure.

#### Wi-Fi specifications

- Wireless Networking Protocols: 802.11b, 11g, 11n single stream (2.4 GHz)
- Wireless Security Protocols: WEP (Open & Shared), WPA (TKIP & AES), WPA2 (TKIP & AES)
- Wireless Authentication Protocols: None, EAP-TLS, EAP-TTLS (MSCHAPv2), PEAP v0 (MSCHAPv2), PEAP v1 (GTC)

- Network Communication Protocols: Hypertext Transfer Protocol Secure (HTTPS)/TLS 1.2
- IP Addressing: Dynamic Host Configuration Protocol (DHCP), static IP addressing
- Data Packet Size: typically less than 5 kilobytes (kB)

Power over Ethernet (PoE) and Ethernet specifications

- Power over Ethernet (PoE): Compliant with IEEE 802.3af standard
- Ethernet: 10/100 Mbps
- Network Communication Protocols: Hypertext Transfer Protocol Secure (HTTPS)/TLS
- IP Addressing: Dynamic Host Configuration Protocol (DHCP), static IP addressing
- Data Packet Size: typically less than 5 kilobytes (kB)

### Network port requirements

Primex Ethernet, PoE, and Wi-Fi enabled devices communicate to OneVue over a facility's network using the Hypertext Transfer Protocol Secure (HTTPS) protocol. OneVue client and device data is encrypted in transit and all sensitive data is encrypted at rest. An outbound HTTPS connection is established by each device and once complete the IP address is released.

The following ports must be open to allow for outgoing OneVue device communication from the facility network.

- **Port TCP 443:** required to be open to allow Hypertext Transfer Protocol over TLS/SSL (HTTPS) communication with OneVue and Wi-Fi, Power over Ethernet (PoE)/Ethernet enabled devices.
- **Port UDP 123:** used by Wi-Fi, Power over Ethernet (PoE)/Ethernet devices to access an external NTP Server. Port is required to be open for use with external Network Time Protocol (NTP) Servers. Use of internal NTP Servers is also supported.



## Network firewall requirements

The OneVue platform runs on the Amazon Web Services (AWS) cloud infrastructure. Organizations with network firewalls in place must proactively allow outbound network communication and file downloads through specific OneVue Domains and URLs. The files downloaded include the Sync device clock list, Notify device schedules, and device setting updates.

OneVue is a high-availability (HA) platform that may change IP addresses at any time, therefore OneVue does not support the use of firewall IP address filtering.

### If the firewall support wildcards:

<b>Domain filters</b>	*.primexonevue.com
	us-east-1-production.s3.amazonaws.com
<b>URL filters</b>	https://*.primexonevue.com
	https://us-east-1-production.s3.amazonaws.com

### If the firewall does not support wildcards:

<b>Domain filters</b>	console.primexonevue.com
	deviceapi-alt.primexonevue.com
	deviceapi.primexonevue.com
	onevueapi.primexonevue.com
	us-east-1-production.s3.amazonaws.com
<b>URL filters</b>	https://console.primexonevue.com
	https://deviceapi-alt.primexonevue.com
	https://deviceapi.primexonevue.com
	https://onevueapi.primexonevue.com
	https://us-east-1-production.s3.amazonaws.com

## Email, text (SMS), and voice communication

OneVue generates email, text (SMS), and voice notifications. Be sure to add **support@primexonevue.com** to your email program's safe senders list. Text and voice alert notifications are sent from phone number (608) 709-7043.

## CREATE, VIEW, EDIT, AND DELETE NETWORK PROFILES

A Network Profile is a network at your facility that a Primex network device connects to. Each device is assigned to a network, allowing it to connect to your facility's network to send data to and download settings from OneVue.

### Network Profile requirements

- **IP addressing (servers)**

It's recommended to use a local DHCP and DNS servers rather than a remote DNS server on the internet. A local DHCP server provides better response times compared to a remote server, thus reducing network connection times and conserving device battery life.

- **Wi-Fi data transmission**

The minimum wireless access point signal strength of -60 dBm is required to support reliable wireless operation. If signal strength is not reliable, the use of a wireless access point in closer proximity of the sensor device installation location is recommended. The data packet size is typically less than 5 kilobytes (kB).

- **WEP Open and WEP Shared security types**

Network settings do not support the use of an ASCII passphrase. It's required to convert an ASCII passphrase to a WEP Hex passkey; provide the Hex Key and Confirm Hex Key.

- **Guest network or open network use**

Primex devices cannot respond to landing pages, nor agree to any terms of service to connect to a network.

- **Proxy Servers**

Primex devices cannot authenticate through a proxy server. If a HTTPS proxy server is used, the Primex device 12-character Gateway ID (MAC address) for each device is required to be whitelisted.

### Create a new network profile

1. Go to **Devices > Networks**.
2. From the bottom menu, select **+ New**.
3. Network Label

Name that uniquely identifies the network. Allows up to a maximum of 40 characters.

4. Enter the **settings**. To view all settings, select **Show Advanced Settings**.

By default, the profile type is set to Wireless with the Security Type of WPA2 AES. You can change these settings to the type of network you are creating.

Devices → Networks → Configure Network

Guest networks requiring confirmation through a browser, and no passphrases will require customer I.T. involvement.

### Configure Network

[Hide Advanced Options](#)

Network Label \*

Location Select a...

Profile Type: **Wireless**

SSID \*

Passphrase

Confirm Passphrase

Security Type: **WPA2 AES**

Notes

Authentication

Authentication

Username

Password

Confirm Password

TCP/IP

Use DHCP ☒

[Save](#) [Cancel](#)

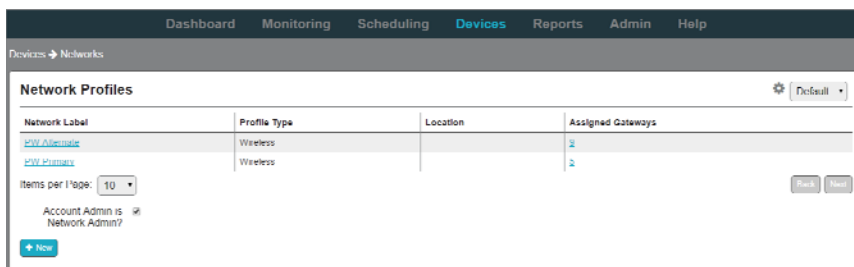
Setting	Definition
Gateways assigned to network (link)	Quantity of Primex devices assigned to the network. Selecting the link opens the list of gateways assigned to the network.
Network Label	Name that uniquely identifies the network. Allows up to a maximum of 40 characters.
Profile Type	Identifies the type of network, either Wireless (Wi-Fi) or Wired.
Location	The Location assigned to the network.
Wireless (Wi-Fi) Network settings	
SSID	Service Set Identifier (SSID) of the network. Case sensitive and allows up to a maximum of 40 characters.
Passphrase	Security key of the wireless network. Leave this field blank if you have selected "None" for the Security Type.
Hex Key	WEP Open and WEP Shared security types - network settings do not support the use of an ASCII passphrase. It's required to convert an ASCII passphrase to a WEP Hex passkey; provide the Hex Key and Confirm Hex Key.
Confirm Passphrase	Re-enter the security key of the wireless network; validates the Passphrase entered.
Hex Key	

Setting	Definition
Security Type	<p>Security mode of the wireless network. Select None if the network is an open network with no security. By default, WPA2 AES is selected.</p> <p>Does the network require EAP-TLS authentication certificates? If yes, certificates are required to be uploaded to each Primex device using the Primex Device Configuration Software.</p>
<b>Advanced settings.</b> Below settings are only viewable when <b>Show Advanced Options</b> is selected.	
Notes	
Authentication	<p>The type of authentication protocol of the Wireless network. If None is selected, additional settings are not displayed.</p> <p>Username and password are required.</p>
TCP/IP	<p>The type of network communication protocol of the network; either DHCP or a non-DHCP IPv4 protocol.</p> <p>If Wired Network, TCP/IP settings are required.</p> <p>DHCP (Dynamic Host Configuration Protocol): select option if the network is DHCP; network allocates dynamic IP addresses to devices in the network.</p> <p>IPv4 Address protocol: deselect Use DHCP option and enter the settings. Primex devices support Internet Protocol version 4 (IPv4).</p> <ul style="list-style-type: none"> <li>• Subnet Mask: subnet mask for of the network.</li> <li>• Gateway: gateway of the network</li> <li>• DNS1: primary Domain Name Server (DNS)</li> <li>• DNS2: secondary Domain Name Server (DNS)</li> </ul> <p>The IPv4 address is entered into each device's gateway profile that are assigned to the Non-DHCP network.</p>

- Once all settings are entered, select **Save**. The network can now be assigned to a device.

## View all network profiles

- Go to **Devices > Networks**.



- All networks are displayed.

Column	Definition
Network Label	<p>Name that uniquely identifies the network. This is not name provided in the SSID setting.</p> <p>Selecting the link opens the network profile.</p>
Profile Type	Indicates if the profile is a wireless (Wi-Fi) or wired network.
Location	Location assigned to the network.
Assigned Gateways	Quantity of device gateways assigned to the network. To view the detailed list of the assigned gateways, select the link.
Account Admin is Network Admin?	<p>When enabled only a user assigned to the account Admin Role or network Admin Role can view this setting. When this setting is disabled, only a user assigned to the network Admin Role can view this setting.</p> <p>Indicates if a user(s) assigned to the account Admin Role has the permission to manage network profiles. By default, this setting is enabled.</p> <ul style="list-style-type: none"> <li>• When enabled, as indicated by a check mark, a user assigned to the account Admin Role is granted permission to view, create, and edit network profiles.</li> <li>• When disabled, only a user assigned to the network Admin Role can view, create, and edit network profiles.</li> <li>• A user assigned to the network Admin Role can enable or disable this setting.</li> <li>• A user assigned to the account Admin Role can only disable this setting.</li> </ul>

## View a network profile

1. Go to **Devices > Networks**.
2. Select the **Network Label** link of the network to view.

The network settings are displayed. To view all of the settings, select Show Advanced Options.

When a network is assigned to a gateway only the Network Label, Location, and Notes can be edited.

Setting	Definition
Gateways assigned to network (link)	Quantity of Primex devices assigned to the network. Selecting the link opens the list of gateways assigned to the network.
Network Label	Name that uniquely identifies the network. Allows up to a maximum of 40 characters.
Profile Type	Identifies the type of network, either Wireless (Wi-Fi) or Wired.
Location	The Location assigned to the network.
Wireless (Wi-Fi) Network settings	
SSID	Service Set Identifier (SSID) of the network. Case sensitive and allows up to a maximum of 40 characters.
Passphrase Hex Key	Security key of the wireless network. Leave this field blank if you have selected "None" for the Security Type.  WEP Open and WEP Shared security types - network settings do not support the use of an ASCII passphrase. It's required to convert an ASCII passphrase to a WEP Hex passkey; provide the Hex Key and Confirm Hex Key.
Confirm Passphrase Hex Key	Re-enter the security key of the wireless network; validates the Passphrase entered.
Security Type	Security mode of the wireless network. Select None if the network is an open network with no security. By default, WPA2 AES is selected.  Does the network require EAP-TLS authentication certificates? If yes, certificates are required to be uploaded to each Primex device using the Primex Device Configuration Software.
<b>Advanced settings.</b> Below settings are only viewable when <b>Show Advanced Options</b> is selected.	
Notes	For information purposes and commonly provides additional details needed to be shared with system users.
Authentication	The type of authentication protocol of the Wireless network. If the type of None is selected, additional settings are not displayed.  Username and password are required.

Setting	Definition
TCP/IP	The type of network communication protocol of the network; either DHCP or a non-DHCP IPv4 protocol.
If Wired Network, TCP/IP settings are required.	<p>DHCP (Dynamic Host Configuration Protocol): select option if the network is DHCP; network allocates dynamic IP addresses to devices in the network.</p> <p>IPv4 Address protocol: deselect Use DHCP option and enter the settings. The system and devices support Internet Protocol version 4 (IPv4).</p> <ul style="list-style-type: none"> <li>• Subnet Mask - subnet mask for of the network.</li> <li>• Gateway - gateway of the network</li> <li>• DNS1 - primary Domain Name Server (DNS)</li> <li>• DNS2 - secondary Domain Name Server (DNS)</li> </ul> <p>The IPv4 address is entered in the gateway profile(s) assigned to the network.</p>

## Edit a network profile

If a network profile is assigned to a device, only its network label, Location, and notes can be edited. If the network is not assigned to a device, all of its settings can be edited.

To edit a network that is assigned to a device, you will need to create a new network profile and then migrate the device to the new network profile.

1. Go to **Devices > Networks**.
2. Edit the settings. To view all settings, select **Show Advanced Options**.

Setting	Definition
Gateways assigned to network (link)	Quantity of Primex devices assigned to the network. Selecting the link opens the list of device gateways assigned to the network.
Network Label	Name that uniquely identifies the network. Allows up to a maximum of 40 characters.
Profile Type	Identifies the type of network, either Wireless (Wi-Fi) or Wired.
Location	The Location assigned to the network.
Wireless (Wi-Fi) Network settings	
SSID	Service Set Identifier (SSID) of the network. Case sensitive and allows up to a maximum of 40 characters.

Setting	Definition
Passphrase	Security key of the wireless network. Leave this field blank if you have selected “None” for the Security Type.
Hex Key	WEP Open and WEP Shared security types - network settings do not support the use of an ASCII passphrase. It's required to convert an ASCII passphrase to a WEP Hex passkey; provide the Hex Key and Confirm Hex Key.
Confirm Passphrase	Re-enter the security key of the wireless network; validates the Passphrase entered.
Hex Key	
Security Type	<p>Security mode of the wireless network. Select None if the network is an open network with no security. By default, WPA2 AES is selected.</p> <p>Does the network require EAP-TLS authentication certificates? If yes, certificates are required to be uploaded to each Primex device using the Primex Device Configuration Software.</p>
<b>Advanced settings.</b> Below settings are only viewable when <b>Show Advanced Options</b> is selected.	
Notes	For information purposes and commonly provides additional details needed to be shared with system users.
Authentication	<p>The type of authentication protocol of the Wireless network. If the type of None is selected, additional settings are not displayed.</p> <p>Username and password are required.</p>
TCP/IP	The type of network communication protocol of the network; either DHCP or a non-DHCP IPv4 protocol.
If Wired Network, TCP/IP settings are required.	<p>DHCP (Dynamic Host Configuration Protocol): select option if the network is DHCP; network allocates dynamic IP addresses to devices in the network.</p> <p>IPv4 Address protocol: deselect Use DHCP option and enter the settings. The system and devices support Internet Protocol version 4 (IPv4).</p> <ul style="list-style-type: none"> <li>• Subnet Mask: subnet mask for of the network.</li> <li>• Gateway: gateway of the network</li> <li>• DNS1: primary Domain Name Server (DNS)</li> <li>• DNS2: secondary Domain Name Server (DNS)</li> </ul> <p>The IPv4 address is entered in the gateway profile(s) assigned to the network.</p>

3. Select **Save**.

## Delete a network profile

You can only delete a network profile that is not assigned to a device gateway. It's recommended to delete networks that are not in use by your Primex network devices.



1. Go to **Devices > Networks**.
2. Select the **Network Label** link of the network to delete.
3. Select **Delete This Network**.
4. From the Delete This Network confirmation window, select **Yes**.

The network profile is deleted from your OneVue account.

## View devices assigned to a network profile

Each Primex network device is assigned to a Network Profile. The network profile settings are stored locally in the Primex device, allowing it to authenticate and connect to your facility's network. You may need to view this information when you are planning to migrate devices to another network.

1. Go to **Devices > Networks**.
2. Select the **Network Label** link of the network to view.

The quantity of devices assigned to the network is displayed.

**Network Profile**

Show Advanced Options

This network profile is currently in use; you may only edit the Network Label and Location

A total of 9 gateways assigned to network

Network Label \*

Profile Type:

SSID \*

Security Type \*

Password:

Confirm Password:

3. Select the **link** to view a detailed list of gateways assigned to the network.

Dashboard Monitoring Scheduling <b>Devices</b> Reports Admin Help						
Devices → Networks → PW Alternate → Assigned Gateways						
Assigned Gateways <span>Default</span>						
<input type="checkbox"/>	Gateway ID	Gateway Type	Last Check-in	Location	State	Update Pending
<input type="checkbox"/>	<a href="#">43:76:89:85:43:22</a>	PrimexIAQ	2016-07-07 4:39 AM		<span>●</span> Suspended	Yes
<input type="checkbox"/>	<a href="#">54:35:34:53:45:34</a>	PrimexIAQ	2016-09-20 1:28 AM		<span>●</span> Normal	No
<input type="checkbox"/>	<a href="#">65:46:54:45:65:65</a>	PrimexIAQ	2016-07-07 4:24 AM		<span>●</span> Alarm	No
<input type="checkbox"/>	<a href="#">65:76:57:56:66:66</a>	PrimexIAQ	2016-07-07 6:15 AM		<span>●</span> Normal	No
<input type="checkbox"/>	<a href="#">76:57:55:67:67:57</a>	PrimexIAQ	2016-07-01 6:08 AM		<span>●</span> Normal	No
<input type="checkbox"/>	<a href="#">FF:FF:FF:00:00:99</a>	PrimexTEMP Single Probe			<span>●</span> Normal	Yes
<input type="checkbox"/>	<a href="#">Unassigned</a>	PrimexIAQ			<span>●</span> Normal	Yes
<input type="checkbox"/>	<a href="#">Unassigned</a>	PrimexIAQ			<span>●</span> Normal	Yes
<input type="checkbox"/>	<a href="#">Unassigned</a>	PrimexTEMP Single Probe			<span>●</span> Normal	Yes
Items per Page: <input type="text" value="10"/>						
<input type="button" value="Edit Selected"/> <input type="button" value="Exit"/>						
<input type="button" value="Back"/> <input type="button" value="Next"/>						

## CHANGE NETWORK ASSIGNED TO DEVICES (MIGRATE TO NEW NETWORK)

A Primex network device requires a network connection to operate over your facility's network. During each network connection, a device transmits its data to and downloads data from your OneVue account. Due to the importance of devices connecting to your facility's network, network settings are downloaded and stored locally at each device. To avoid a device losing its connection to your facility's network, changes to a device's network is managed by performing a network migration procedure.

### Available device network migration methods

- **Migrate device to new network from OneVue**

If you need to change the network assigned to a device from OneVue, you can assign a migration network and the migration network is downloaded to the device during its next check-in. The current network must be operational to allow the device's check-in to OneVue. During a check-in, the device will download the new network settings.

- **Migrate device to new network with the OneVue Wired Device Configurator (OWDC) app**

The OWDC Android™ app provides the experience of managing Primex network devices locally at a device on a mobile platform. The app provides the flexibility to assign or migrate a device to another network. Once you download the app from the Google Play™ store (it's free!), you connect a Primex network device to your Android device and the app guides you through the entire process.

- **Migrate device to new network locally at device with OneVue manual configuration file**

Manually configuring the network settings of a Primex device can be performed with the Primex Device Configuration software. An encrypted file (.pwg extension) is downloaded from a device's gateway profile. The file includes your OneVue account ID and the network profile(s) assigned to the device's gateway profile.

- **Migrate device to new network when networks are not managed in OneVue**

If the networks used by your Primex devices are not managed from your OneVue account, network updates are required to be made locally at the device. Network settings are updated using the Primex Device Configuration software.

### Migrate devices to new network from OneVue

If you need to change the network assigned to a device from OneVue, you can assign a migration network and the migration network is downloaded to the device during its next check-in.

## WARNING

It's critical to ensure the current assigned network is operational on your network to allow devices to connect to the current assigned network to download the migration network settings. Once all devices successfully connect to the migration network, the previous assigned network is no longer required to be operational on your network.

It's recommended to perform this procedure on a single or test group of devices with both the current network and migration network operational on your network. This will allow you to validate the devices' connection to the migration network.

## Overview

The procedure can be performed for a single [19] or multiple devices [20] at the same time.

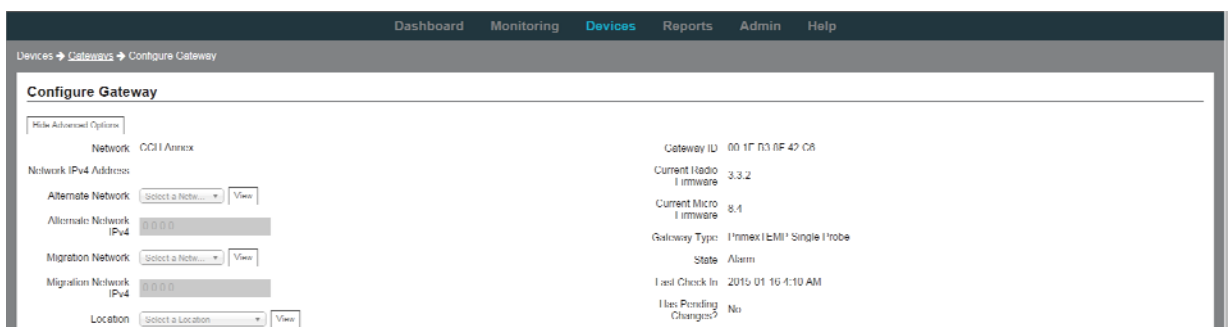
1. A migration network is assigned to the device's gateway.
2. During its next check-in to OneVue, the device downloads its assigned migration network settings.
3. At the device's next subsequent check-in, the device attempts to connect to the migration network first.
4. Once the device successfully connects to the migration network, the system automatically sets its network to the migration network set during this procedure and clears the migration network setting. If the connection to the migration network should fail, it attempts to connect to its current assigned network.

## How to set the migration network of a single device

Before you begin this procedure, verify the settings of the network you are migrating to are correct.

1. Go to **Devices** > select the **device type**.
2. From the list, select the **Gateway ID** of the device you are migrating. The device's gateway profile is displayed.
3. Select **Show Advanced Options**.
4. From the **Migration Network** drop-down, select the **network profile** the device is to be migrated to.

To change the IPv4 address, from the Migration Network IPv4 field, enter the IPv4 address the device is to be migrated to. To set the IPv4 migration network, the migration network must be a non-DHCP network with a specific subnet mask, gateway and DNS servers.



Dashboard Monitoring **Devices** Reports Admin Help

Devices > Gateways > Configure Gateway

### Configure Gateway

☐ Hide Advanced Options

Network	CGI Annex	Gateway ID	00:1F:03:0F:42:C8
Network IPv4 Address		Current Radio	1 firmware
Alternate Network	Select a Network...	Current Micro	1 firmware
Alternate Network IPv4	0.0.0.0	Gateway Type	1'rimex EIM  Single 1'robe
Migration Network	Select a Network...	State	Alarm
Migration Network IPv4	0.0.0.0	Last Check In	2010-01-10 4:10 AM
Location	Select a Location...	Has Pending Changes?	No

5. Select **Save**.

Its Updated Pending status is set to Yes and the network migration change is scheduled to be downloaded to the device during its next check-in to OneVue. Once the device has successfully connected to the migration network, the system automatically sets the primary network to the migration network selected during this procedure and the migration network setting is cleared.

### How to set the migration network of multiple devices at the same time

Before you begin this procedure, verify the settings of the network you are migrating to are correct.

This multi-edit procedure cannot be performed for devices assigned to a static IPv4 address.

1. Go to **Devices > Gateways**.
2. From the list, select the **devices' gateways** that are to be migrated from their current primary network to another network.

Gateway Id	Gateway Type	Last Check-In	Location	State	Update Pending
<input checked="" type="checkbox"/> 00-1F-R3-8P-4D-08	PrimexTFMP Single Probe	2015-01-16 4:10 AM		Alarm	No
<input checked="" type="checkbox"/> 00-1F-R3-8P-4D-4F	PrimexIAQ	2015-01-16 11:21 AM		Normal	No
<input checked="" type="checkbox"/> 00-1F-R3-8P-4D-55	PrimexIAQ	2015-01-16 11:15 AM		Normal	No
<input checked="" type="checkbox"/> 00-1F-R3-8P-4B-1R	PrimexTFMP Dual Probe	2015-01-16 11:07 AM		Normal	No
<input type="checkbox"/> 00-1F-R3-8P-4C-AD	PrimexTFMP Single Probe PoP	2015-01-16 11:24 AM		Suspended	No
<input type="checkbox"/> 00-1F-R3-8P-51-74	PrimexIAQ	2015-01-16 8:15 AM		Alarm	No

3. Select **Edit Selected**. The Mass Edit Gateway window is displayed.
4. From the **Migration Network** drop-down menu, select the **network profile** the selected gateways are to be migrated to.

5. Select **Update All Selected Gateways**.

All selected device's Updated Pending status is set to Yes and the network migration change is scheduled to be downloaded to each device during their next check-in to your OneVue account. Once a device has successfully connected to the migration network, the system automatically sets the primary network to the migration network selected during this procedure and the migration network setting is cleared.

## Migrate sensor to a new (updated) network with the Primex Device Configuration software

When a device cannot connect to the network, you can update its network settings with the Primex Device Configuration software. When a device cannot connect to the network, a device's OneVue status is **Unresponsive** and its LCD screen will display **No Signal**.

During this procedure, an encrypted file (.pwg extension) with your OneVue Account ID and the device's Migration Network (new/updated network) is downloaded from OneVue and uploaded to the device. You will need to be locally at the device to complete this procedure.

As an alternative, you can also use the OneVue Wired Device Configurator app (OWDC) to change a device's assigned network locally at the device.

### Requirements

- Primex Device Configuration software is installed on your computer.
- Primex device USB configuration cable (mini-USB supplied with each device order).
- Your OneVue User Profile is assigned to an Admin Role.
- For EAP-TLS authentication, the certificate .der file is required. The file is uploaded to the device during configuration.
- If your security policies restrict network settings to be stored in your OneVue account, in which your OneVue account does not have network profiles, the network settings can be entered directly within the Primex Device Configuration software.

### Step 1: From OneVue, set the device's migration network and download manual configuration file

This step is required to upload the correct network settings to a device, which will allow its connection to your facility's network and check-in to OneVue. When a device connects to its assigned Migration Network, OneVue automatically sets the Migration Network to its Primary Network and clears its Migration Network.

1. First, create a new **Network Profile** with the correct network settings. If a network with the correct settings already exists, proceed to the following step (assign Migration Network).  
Go to **Devices > Networks** > from the bottom, select **+ New**.
2. Assign the device's **Migration Network**. When a device connects to its assigned Migration Network, OneVue automatically sets the Migration Network to its Primary Network and clears its Migration Network.  
From OneVue, go to **Devices** > select the **device type** > from the list, select the **device's 12-character Gateway ID link** > from the Gateway Profile, select **Show Advanced Options** > set its **Migration Network** > select **Save**.  
If you have multiple devices to update, you will need to set the Migration Network for each device.
3. From the **Manual Configuration File** option, select **Download**. The manual configuration file contains your OneVue account ID and the network profile(s) assigned to a device. This file can be used for all devices to update.
4. From the **Download Manual Configuration File** window, enter the Configuration File Password.  
This password must match the password of the Primex Device Configuration software. **If you have not changed the Primex Device Configuration software password (Primex1) on your local computer, leave as is.**

If you require that a user cannot view the details of the network profile settings within the Primex Device Configuration software, select the Hide Configuration option. When Hide Configuration is selected, the network setting details are not displayed in the software.



5. Select **OK**.
6. From the system prompt, select **Save**.

By default, the file is saved to your computer's **Downloads** folder and is named device.pwg. To copy the file to another location, select Open Folder and copy the file to the desired location.

## Step 2: Upload manual configuration file to device with Primex Device Configuration software

1. Verify the device **does not have battery power** applied; remove the device cover and temporarily set the battery on/off switch to the Off (down) position or remove the batteries.
2. Plug the **Primex mini-USB configuration cable** into a **USB port on your computer**.
3. Plug the configuration cable **mini-USB connector** into the **device USB mini port**.  
The device automatically powers up, detects the connection to your computer and enters configuration mode. The LCD displays the letters **Con** and the **Config icon** is displayed indicating the device is in configuration mode.
4. Open the Primex Device Configuration software. Go to **All Programs > Primex > Primex Device Configuration** or from your computer desktop, double-click on the Primex Device Configuration icon.
5. From the **Enter Password** window, enter the password.  
Factory default password (case sensitive): **Primex1**
6. Select **Connect**. A connection between your computer and the device is established.
7. Verify the notification area located in the lower-left of the screen, displays **Connected to device on COMx**, which indicates the connection is established.
8. Next, open the **.pwg** file downloaded from the device's gateway profile. From the top menu, select **File**, browse to the file location and select the **device.pwg** file.
9. Select **Write Configuration >** from the Confirmation Needed window, select **Yes**. The settings of the .pwg file have been uploaded to the device, including your OneVue account ID and the network profile(s).


### TO INSTALL A RADIUS EAP-TLS CERTIFICATE

1. Select the **RADIUS Certificate** tab.
2. For each of the certificates, select **Open** and select the certificate file (.der file required).
3. Select **Write Configuration >** from the **Confirmation Needed** window, select **Yes**. The network settings have been uploaded to the device. Proceed to step 10.
10. Select **Disconnect**. The connection between the software and device is ended.
11. Remove the USB connection between the device and your computer.
12. Apply power to the device; set the battery on/off switch back to the UP (On) position or insert batteries if removed.

When power was applied, the device automatically initiated a check-in to OneVue.

13. Verify the device LCD displays **Signal OK**, which indicates the device successfully checked-in to OneVue.

If there were pending changes downloaded during its check-in, the device will reset and check-in again before the **Signal OK** icon is shown.

14. If **No Signal** is displayed, initiate a manual check-in to OneVue by pressing and quickly releasing the device check-in button  (up arrow).

The device emits a series of audio beeps indicating its connection sequence.

1 beep: device booted

2 beeps: device connected to network

3 beeps: device connected to OneVue



#### NOTE

If you completed this procedure due to the settings of the network profile assigned during device preconfiguration were not correct and a migration network was assigned to the device's gateway profile, the migration network is downloaded to the device during its check-in. Upon a successful connection to the migration network, the OneVue automatically sets the primary network to the migration network.

### Migrate sensor to a new (updated) network when networks are not managed in OneVue

If your security policies restrict network settings to be stored in your OneVue account, in which your OneVue account does not have network profiles, the network settings can be entered directly within the Primex Device Configuration software.



#### WARNING

Do not begin this procedure if the device is not in your OneVue Account. If Device Preconfiguration was not completed before the order shipped from Primex, you will need to add the device to OneVue by using the OneVue Wired Device Configurator (OWDC) app.

### Requirements

- Primex Device Configuration software is installed on your computer.
- Primex device USB configuration cable (mini-USB supplied with each device order).



## Migrate device to another network

1. Verify the device does not have AC or battery power; remove the device cover and temporarily set the battery on/off switch to the Off (down) position or remove its batteries.
2. Plug the Primex USB configuration cable into a USB port on your computer.
3. Plug the configuration cable mini-USB connector into the device USB mini port.
4. The device automatically powers up, detects the connection to your computer and enters configuration mode. The LCD displays the letters **Con** and the **Config icon** is displayed indicating the device is in configuration mode.
5. Open the Primex Device Configuration software. Go to **All Programs > Primex > Primex Device Configuration** or from your computer desktop, double-click on the Primex Device Configuration icon.
6. From the Enter Password window, enter the **password**. Factory default password (case sensitive): **Primex1**
7. Select **Connect**. A connection between your computer and the device is established.
8. Verify the notification area located in the lower-left of the screen, displays **Connected to device on COMx**, which indicates the connection has been established.
9. Select **Read Configuration**. The device's current settings are displayed.

The screenshot shows the 'Primex Device Configuration' application window. The title bar is light blue with a gear icon and standard window controls. The menu bar includes 'File', 'Actions', and 'Help'. Below the menu is a toolbar with various icons. The main area has four tabs: 'Sensor Configuration' (selected), 'Firmware Upgrade', 'Tools', and 'Communication Log'. On the right, there are three buttons: 'Disconnect', 'Read Configuration', and 'Write Configuration'. The central display area shows the 'Primex Server' section with the 'ONEVUE' logo and a 'Change to AMP' button. To the right of the logo, device information is listed: Model: T101, MAC Address: 00:1E:B3:8F:59:1E, Sensor FW Version: 8.11, Radio FW Version: 3.3.2, Hardware Version: 5.0, and Regulatory Domain: FCC. Below this, there are three tabs: 'Wireless: Migration' (selected), 'Wired: Primary', and 'RADIUS Certificate'. The 'Wireless: Migration' tab contains fields for 'SSID', 'Security Type' (set to 'No Security'), 'Security Key', and a 'Use DHCP' checkbox (checked). The 'RADIUS' section has an 'Authentication' dropdown (set to 'No Authentication'), 'Username', and 'Password' fields. The 'Wired: Primary' tab contains fields for 'IP Address', 'Subnet Mask', 'Gateway', 'DNS 1', and 'DNS 2'. At the bottom, a status bar displays the message 'Configuration read OK.'

10. Verify the **OneVue logo** is displayed.



11. From the first drop-down menu, select **Wireless: Migration**.
12. Enter the settings of the network you are migrating the device to.
13. Select **Write Configuration**. From the Confirmation Needed window, select Yes. The settings have been uploaded to the device.
14. If the network is operational on your network, it's recommended to test the device's connection. Select **Tools > Connection Test**. The connection test attempts to connect to the network and the test results are displayed.
15. Select **Disconnect**. The connection between the software and device is ended.
16. Remove the USB connection between the device and your computer.
17. Apply AC power to the device and set the battery on/off switch back to the UP (On) position or insert batteries if removed.
18. When power was applied, the device automatically initiated a check-in to your OneVue account.
19. Verify the device LCD displays **Signal OK**, which indicates the device successfully connect to the network and checked-in to your OneVue account. If there were pending changes downloaded during its check-in, the device will reset and check-in a second time before the Signal OK icon is shown.

## OWDC app: Migrate Sensor to a new network

Learn how to update a sensor's assigned network with the OneVue Wired Device Configurator (OWDC) app. Commonly this procedure is performed when a sensor cannot connect to its current assigned network and requires a network update (migrate to a new network).

The OneVue Wired Device Configurator (OWDC) Android™ app provides the experience of adding a new Primex network device to OneVue and updating a device's primary settings on a mobile platform. Network devices include OneVue Sense Sensors, OneVue Sync Bridge, PoE Digital Clocks/Timers, and the OneVue Notify Bell Controller.

Once you download the app from the Google Play™ store (it's free!), you connect a Primex network device to your Android device and the app guides you through the entire process. It's a simple, easy process that provides onsite configuration.

### Configuration requirements

The following details what's required to configure a sensor with the OWDC app.

- **OWDC app installed on your Android mobile device**

Download the OWDC app or from the Google Play Store search for **OneVue Wired Device Configurator**.

- **Android mobile device requirements**

Android OS version 4.4 or later. Minimum 25% battery life remaining.

Supports USB Host or USB OTG mode. To verify USB support, check with the Android device manufacturer.

- **App log in**

Your OneVue user profile must be assigned to the Account Admin role. You will log in to the app with your OneVue username (email address) and password.

- **Connection cable (not supplied)**

The cable connects the Primex device to your Android device and also provides the power source to the Primex device during configuration.

A Sensor has USB Mini B (5 pin) connector interface and requires either a Mini-USB to Micro USB OTG adapter cable or Mini-USB to USB C adapter cable.

- **OneVue Network Profile**

From the OWDC app, you cannot create a new Network Profile. Before you begin, from OneVue verify a Network Profile exists or create a new Network Profile. From OneVue, go to Devices > Networks. To create a new network, from the bottom section select +New.

For a Non-DHCP network, during configuration you are required to provide the device's static IP address.



#### **NOTE**

OWDC cannot be used with devices that require EAP-TLS certificates for network authentication or any type of network certificate. Devices requiring this type of authentication must be configured through Device Preconfiguration, and when the devices arrive onsite the certificates are required to be uploaded to the devices using the Primex Device Configuration software. The devices will then be able to successfully authenticate to the facility's network and check-in to OneVue.

### [How to migrate a sensor to a new network](#)

1. From your Android device, open the **OWDC** app.



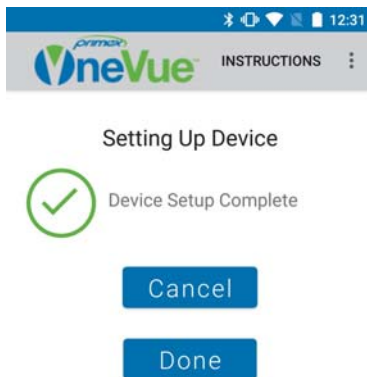
2. Enter your **OneVue username** > select **Next** > enter your **password** > select **Log In**.  
Are you a user for more than one OneVue account? When logging in to the app, it's critical to select the account you are adding a device to or editing.
3. **Remove AC power** from the sensor. During the next step, it receives power from its connection to your Android device. If battery power is enabled, leave this on.

4. Set the sensor into **configuration mode**. Connect the sensor to your Android device using a USB OTG or a USB C cable (dependent on your device).  
App displays "Add Device" and its LCD displays "Con", which indicates it's in configuration mode.



5. To assign or update its network > select a **Network Type** > select an available **Network** > and select **Next**.
6. The sensor's monitoring setting are displayed. You can optionally update if needed, otherwise select **Next**.
7. The app configures the Sensor and displays its configuration status.

Do not remove the connection between the Sensor and your Android device until prompted.



8. When the **Disconnect Device** message appears, **remove the wired connection** between the Sensor and your Android device and **reapply AC power** to the sensor.
  - Once disconnected, the app verifies the device successfully checked-in to OneVue. If after 15 minutes it does not check-in, the app displays a status message.

All sensor models: if a firmware update is available, it may also take time to download firmware (Sensor LCD displays UP).

You can now configure additional devices or close the app when you're done.

## UPLOAD EAP TLS CERTIFICATE TO PRIMEX NETWORK DEVICE

When the network that devices connect to require an EAP-TLS client certificate, the certificate must be uploaded to a Primex network device using the Primex Device Configuration software. This procedure is required during installation and when updating a device's certificate.

### Requirements

- Primex Device Configuration software is installed on your computer.
- Primex device USB configuration cable (supplied with each device order)
- EAP-TLS certificate file (.der)

### Install EAP-TLS certificate

1. If the device is battery-powered, temporarily remove its batteries.
2. Plug the Primex device USB configuration cable into a USB port on your computer.
3. Plug the configuration cable mini-USB connector into the device USB mini port.  
The device automatically powers up, detects the connection to your computer and enters configuration mode.
4. Open the Primex Device Configuration software. Go to **All Programs > Primex > Primex Device Configuration** or from your computer desktop, double-click on the Primex Device Configuration icon.
5. From the **Enter Password** window, enter the password.  
Factory default password (case sensitive): **Primex1**
6. Select **Connect**. A connection between your computer and the device is established.
7. Verify the notification area located in the lower-left of the screen, displays **Connected to device on COMx**, which indicates the connection has been established (x identifies the current COM port in use).
8. Select the **RADIUS Certificate** tab.
9. For each of the certificates, select **Open** and select the certificate file (.der file required).
10. Select **Write Certificates and Private Key**.
11. Select **Disconnect**. The connection between the software and the device is ended.
12. Remove the USB connection between the device and your computer.
13. Apply power to the device. When power is applied, the device automatically initiates a check-in to your OneVue account.
14. Verify that **Signal Ok** is displayed on its LCD screen and successfully checked-in to OneVue.

## TECHNICAL SUPPORT

You may require technical support when you have questions about product features, installation and configuration, or troubleshooting. Support services are delivered in accordance with your organization's support agreement, end-user license agreements, and warranties, either with a Primex Certified Sales and Service Partner or directly with Primex.

### **Support through Primex Certified Sales and Service Partners**

Ensuring our customers experience excellent service is of utmost importance to Primex. Our network of Certified Sales and Service Partners offers technical support services for Primex products.

If you have purchased Primex products or have a service agreement with a Primex Partner, they are your primary contact for all Technical Support inquiries.

### **When contacting Technical Support**

Make sure you have satisfied the system requirements specified in the product documentation. Also be at the computer or device on which the problem occurred, in case it's necessary to replicate the problem.

Please have the following information available:

- Customer ID/Account Name
- Problem description/error messages
- Device hardware information
- Troubleshooting performed

### **Primex Technical Support**

Hours: 7:00 AM to 7:00 PM CT, Monday through Friday

Phone: 1-262-729-4860

Email: [service@primexinc.com](mailto:service@primexinc.com)

Web: [www.primexinc.com/support](http://www.primexinc.com/support)