

User Management

Administration Guide

OneVue Sync Bluetooth

Publication date July 21, 2020

Table of Contents

Manage Users	3
About managing users	3
Overview of roles assigned to users	6
User role matrix by feature	7
Create a new user	12
Configure a user's access to data, system features, and device types (roles and device classes)	15
Set a user to be excluded from the account session timeout period	16
Resend a user their account invite notification	16
Deactivate or activate a user	17
Lock or unlock a user	18
Delete a user	19
Technical Support	20
Support through Primex Certified Sales and Service Partners	20
Primex Technical Support	20

Manage Users

About managing users

A User is someone who can log in to your OneVue account. Each user has a unique profile where you can manage what data and features they have access by assigning their Role and Device Class. From a user profile, you can also set their alert preferences and timeout exempt settings.

Only a user assigned to the Account Admin or Business Unit Admin role can view and manage user settings. A user assigned to the Business Unit Admin role can only manage the settings of users assigned to their Business Unit.

User management features

- **Add new users**

To access OneVue, a user must be added to OneVue. Once added, a user receives an email to activate their user account.

- **Manage user settings**

Settings include Roles, Device Classes, and Timeout Exempt. When a user views their profile these settings are not displayed.

- **Assign Roles to users**

Access to OneVue account data and the permissions to system features are granted by way of the Role(s) assigned to each user. Roles are designed to mirror common job functions.

A BU Admin can only assign a Business Unit at the time they create a new user. Only a user assigned to the Account Admin role can update a user's assigned Business Unit.

- **Change the email address for a user**

You may need to change a user's email address if, for example, they get married and their last name changes or their email address is not correct. For security purposes, changing or updating a user's email address can only be made by Primex Technical Support or by a user assigned to the Account Admin role.

- **Deactivate and reactivate users**

When deactivated a user cannot log in to OneVue and does not receive alert or system notifications. When deactivating a user, you can assign a user to re-assign the deactivated user's Alerts, Reports, and Custom Views. Commonly, a user is deactivated when they are not available for an extended period of time. When reactivated, a user's log in access, Alerts, Reports, and Custom Views are restored.

- **Lock a user**

When locked, a user is denied log in access to OneVue and continues to receive alert and system notifications.

- **Delete users**

Deleting a user permanently removes the user from OneVue. To delete a user, their profile is required to be deactivated.



TIP

There are User Reports that include data specific to users. These reports can only be generated manually and cannot be scheduled. Commonly, these reports are generated at the time the information is needed.

- **User Report**

The User Report provides details of each user, including their assigned Device Classes, Roles, and Alert Rules, and indicates if a User Profile is inactive.

If a staff member is leaving your organization and you need to reassign their responsibilities, this report provides what's needed to reassign their OneVue responsibilities to another user.

- **User Role Report**

The User Role Report provides details of the Roles and Device Classes assigned to each user.

If you need to understand who has access to account data and features, this report provides what's needed to identify who's assigned to specific Business Units or Locations and their assigned Roles.

User Profiles

To view users, go to **Admin > Users**. A list of all users is displayed.

1. To view a user's profile, from the list select the **Email link** of the user.
2. To manage the Role(s) assigned to the user, from their profile select **Assign Roles**. A BU Admin can only assign Roles to a user for their Business Unit when they create a new user. Only an Account Admin can update a user assigned roles.

User profile setting specifications

The following table provides the settings managed from a User Profile.

Setting	Definition
Avatar	Image displayed next to the User Profile name. Supported file types include GIF, JPEG, and PNG. The file size is limited to 5MB maximum.
Email	Email address of the user. The user is required to enter this email address to log in to OneVue and is the email address system and alert notifications are sent to. Only a user can update their profile's email address.
Title	Commonly the job title of the user; for reference use only.
First Name Last Name	The User Profile name is the value of the first name and last name. The User Profile name is displayed throughout the system and is viewable by other users.
Mobile Phone	Phone number the system uses to send the user text or voice alert notifications. A non-mobile number can be entered if the user is only to receive voice alert notifications. To only receive voice alert notifications, set the user's alert preferences to voice only.
Dialer Suffix	OneVue provides the ability to route voice alert notifications to an IVR system. You will commonly configure this setting when your organization's phone system requires that callers enter an extension number or select an option to reach a specific person, department, or central line.
Alert Preference	Alerts do not apply to the OneVue Sync Bluetooth or PoE solutions. Sets how the user receives alert notifications. The user receives alert notifications in the form of each method(s) selected. As an example, if all three methods are selected they will receive alert notifications by email, text, and voice.
Settings below can only be viewed and managed by a user assigned to an Admin Role.	
Device Classes	Identifies the types of devices the user has access to. By default, all classes are enabled. <ul style="list-style-type: none"> • Sensors: access to OneVue Sense devices and features. • Clocks/Bridges: access to OneVue Sync devices and features. • Transmitters: access to OneVue Sync Transmitters and features. • Bell Controllers/Message Boards: access to OneVue Notify Bell Scheduling devices and features. Ethernet only Message Boards discontinued in 2019. • InfoBoards: access to OneVue Notify InfoBoard and MiniBoard devices and features.
Is Locked?	When locked, the user is denied log in access and OneVue does continue to send the user alert and system notifications.

Setting	Definition
Timeout Exempt	When the timeout exempt setting is enabled, the account level timeout session does not apply to the user. When enabled the user is not logged out by the system due to inactivity.

Overview of roles assigned to users

Access to OneVue account data and the permissions to system features are granted by way of the Role(s) assigned to each user. Roles are designed to mirror common job functions.

Considerations when assigning roles

- **Role requirements**

When a new user is created, if a role is not selected, they are automatically assigned to the account Business Unit as a BU (Business Unit) user Role.

At minimum, a user is required to be assigned to one Business Unit or Location. A user can also be assigned to multiple Business Units or Locations.

A user can only be assigned to one role by Business Unit or Location.

- **Parent-child Role structure**

Depending on your account structure, a user can be assigned a Role to one or multiple Business Units or Locations.

Your OneVue account is the parent to all Business Units. If a user is assigned to the account Business Unit, the highest level in the parent-child hierarchy structure, the user is granted the same Role to all child Business Units. If required, a different Role can be assigned to the child Business Unit(s) or Locations.

- **Account Admin Role**

Assign to a user(s) that is responsible for managing your OneVue account. It's recommend to have a minimum of two users assigned to the account Admin Role.

By default, the Admin Role is granted the permissions of the network Admin Role. To only allow a network admin to have access to network profile settings the Account Admin is Network Admin setting, located in the networks view, should be disabled.

- **Each Role has predefined permissions**

Roles determine what a user can do and cannot do and the data they can view. Roles are designed to mirror common job functions. All users have access to the Dashboard and their User Profile, and creating and managing their custom views.

- BU Admin role is commonly assigned to a user that is responsible for managing components and users of their assigned Business Unit.
- BU User and Facility User roles are commonly assigned to users responsible for monitoring devices, including viewing current and historical data.
- Network Admin role is commonly assigned to users that are responsible for managing the networks assigned to devices.
- Facility Admin role is commonly assigned to users responsible for the maintenance of your Primex devices.

- **ODC and OWDC app**

A user is required to be assigned to the Account Admin or Network Admin role to access the OWDC and ODC app.

OWDC app: configure sensors, bridges, Bell Controllers, and PoE digital clocks onsite.

ODC app: configure OneVue Sync Transmitters and Notify InfoBoards.

Roles overview

Account admin	Business Unit Admin	(BU) Business Unit User	Scheduler (OneVue Notify with Bell Scheduling solution)
<p>Complete access to all account data, system features, and the OWDC and ODC app.</p> <p>*The Account Admin Role is granted access to create and edit network and gateway profiles only if the Account Admin is Network Admin setting is enabled. This setting is managed from Devices > Networks list view.</p>	<p>Complete access to all system features and restricted to the data associated to their assigned Business Unit.</p> <p>Only when adding a new user, BU Admin can assign the user to their Business Unit.</p>	<p>View only access to Sync Bluetooth devices and reports associated to their assigned Business Unit. Users can also review and approve reports.</p>	<p>Complete view and edit access to manage the settings of Zones, ring types, Alert Rules, Teams, Bell Controller relays, and reports. View only access to the list of networks and device gateway profiles.</p>

Location Roles overview

Facility admin & Facility network admin	Facility user
<p>Complete access to all account data, system features, and OWDC and ODC app.</p>	<p>View only access to Sync Bluetooth devices and reports assigned to the Location.</p>

User role matrix by feature

Access to OneVue account data and the permissions to system features are granted by way of the Role(s) assigned to each user. Roles are designed to mirror common job functions.

All users

Each user has permission to manage their own User Profile settings, view the Dashboard, view and acknowledge alerts, and manage their custom views.

Roles by feature

The following provides detail by each system feature and Role. An x in the column indicates the Role has permission to the feature.

Device Preconfiguration

	Account Admin	BU (Business Unit) Admin	BU (Business Unit) User	Scheduler	Network Admin	Facility Admin	Facility Network Admin	Facility User
Complete Device Preconfiguration - including assigning network profile to devices	x	x			x	x	x	
Create a new network, including assigning IPv4 address to a device	x				x		x	

OWDC and ODC app

	Account Admin	BU (Business Unit) Admin	BU (Business Unit) User	Scheduler	Network Admin	Facility Admin	Facility Network Admin	Facility User
Assign network and provide primary settings	x				x			

Report Profiles & Reports

	Account Admin	BU (Business Unit) Admin	BU (Business Unit) User	Scheduler	Network Admin	Facility Admin	Facility Network Admin	Facility User
To view a report, a user is required to be assigned to the Business Unit or Location for what's included in the report.								

	Account Admin	BU (Business Unit) Admin	BU (Business Unit) User	Scheduler	Network Admin	Facility Admin	Facility Network Admin	Facility User
View reports, generate report, view report profile settings	x	x	x	x	x	x	x	x
Create and edit Report Profile	x	x			x	x		
Create, generate, and view OneVue Audit Report	x							
Create, generate, and view User Report, User Role Report, & User Alert Rule Report	x							
Acknowledged a Report Audit Review	x	x	x		x	x	x	x
Create, edit, and archive a Report Profile	x	x		x	x	x	x	

Account and User settings

	Account Admin	BU (Business Unit) Admin	BU (Business Unit) User	Scheduler	Network Admin	Facility Admin	Facility Network Admin	Facility User
View and edit account profile	x							

	Account Admin	BU (Business Unit) Admin	BU (Business Unit) User	Scheduler	Network Admin	Facility Admin	Facility Network Admin	Facility User
Create, edit, and view User Profiles	x	x*			x	x	x	
* assign users to their Business Unit when creating a new user only.								
Create , edit and view Business Units	x	x*			x			
Create, edit, and view Locations	x				x	x	x	
Create, edit, and delete User Announcements and view history	x				x			

Devices - Sync Bluetooth Clocks, Bridges, Repeaters

BU roles: required to be assigned to Business Unit assigned to devices; grants access to parent Business Unit and its child Business Unit.

	Account Admin	BU (Business Unit) Admin	BU (Business Unit) User	Scheduler	Network Admin	Facility Admin	Facility Network Admin	Facility User
View devices (list view and device profiles)	x	x	x		x	x	x	x

	Account Admin	BU (Business Unit) Admin	BU (Business Unit) User	Scheduler	Network Admin	Facility Admin	Facility Network Admin	Facility User
Edit all device profile settings	x	x				x	x	

Network Profiles and Gateways

System Feature	Account Admin	BU (Business Unit) Admin	BU (Business Unit) User	Scheduler	Network Admin	Facility Admin	Facility Network Admin	Facility User
Devices > Gateways								
*The Account Admin Role is granted access to create and edit network and gateway profiles only if the Account Admin is Network Admin setting is enabled. This setting is managed from Devices > Networks list view.								
View list of gateways and profiles	x	x	x	x	x	x	x	
Edit profile settings	x*	x			x	x	x	
Edit the IPv4 address of a gateway	x*				x		x	
Download manual configuration file from gateway profile	x*				x		x	
Devices > Networks								
*The Account Admin Role is granted access to create and edit network and gateway profiles only if the Account Admin is Network Admin setting is enabled. This setting is managed from Devices > Networks list view.								

System Feature	Account Admin	BU (Business Unit) Admin	BU (Business Unit) User	Scheduler	Network Admin	Facility Admin	Facility Network Admin	Facility User
View the list of all networks.	x	x	x	x	x		x	
Create, edit, view, and delete a network profile	x*				x		x	
View and disable the Account Admin is a Network Admin setting	x*							
View, enable, and disable the Account Admin is a Network Admin setting					x		x	

Create a new user

You must create a User Profile for anyone that requires access to your OneVue account.

1. Go to **Admin > Users**.
2. Select **+ New**.

New User



Upload Avatar Choose File No file chosen

Email *

Title

First Name *

Last Name *

Mobile Phone

Dialer Suffix

Alert Preference Email
 Text
 Voice

Set Business Unit Roles manually

Save Cancel

3. Enter the user's settings and assign a Role to the user.

Setting	Definition
Avatar	Image displayed next to the User Profile name. Supported file types include GIF, JPEG, and PNG. The file size is limited to 5MB maximum.
Email	Email address of the user. The user is required to enter this email address to log in to OneVue and is the email address system and alert notifications are sent to.
Title	Commonly the job title of the user; for reference use only.
First Name	The User Profile name is the value of the first name and last name. The User Profile name is displayed throughout the system and is viewable by other users.
Last Name	

Setting	Definition
Mobile Phone	<p>Phone number the system uses to send the user text or voice alert notifications.</p> <p>A non-mobile number can be entered if the user is to only to receive voice alert notifications. To only receive voice alert notifications, set the user's alert preferences to voice only.</p>
Dialer Suffix	<p>OneVue provides the ability to route voice alert notifications to an IVR system. You will commonly configure this setting when your organization's phone system requires that callers enter an extension number or select an option to reach a specific person, department, or central line.</p>
Alert Preference	<p>Sets how the user receives alert notifications.</p> <p>The user receives alert notifications in the form of each of method(s) selected. As an example, if all three methods are selected they will receive alert notifications by email, text, and voice.</p>
Set Business Unit Roles Manually (only displayed when creating a new user)	<p>When selected, assign a Role to the new user.</p> <p>By default, a user is assigned to the account Business Unit and the Business Unit (BU) Role.</p>
 NOTE When creating a new user, the settings below are only available after the User Profile is saved.	
Device Classes	<p>Identifies the types of device the user has access to. By default, all classes are enabled.</p> <ul style="list-style-type: none"> • Sensors: access to OneVue Sense devices and features. • Clocks/Bridges: access to OneVue Sync devices and features. • Transmitters: access to OneVue Sync Transmitters and features. • Bell Controllers/Message Boards: access to OneVue Notify Bell Scheduling devices and features. Ethernet only Message Boards discontinued in 2019. • InfoBoards: access to OneVue Notify InfoBoard and MiniBoard devices and features.
Is Locked?	<p>When locked, user is denied log in access and OneVue does continue to send the user alert and system notifications.</p>
Timeout Exempt	<p>When the timeout exempt setting is enabled, the account level timeout session does not apply to the user. When enabled, the user is not logged out by the system due to inactivity.</p>

4. Select **Save**.

The user receives a system-generated email providing the instructions to activate their OneVue user account. During activation, they establish their password and accept the OneVue terms and conditions.

5. Next, assign the user a Device Class, which is commonly based on the OneVue solution(s) deployed at your facility.

To view the user's profile, go to **Admin > Users >** select the **user email** link.

- **Sensors:** access to OneVue Sense devices and features.
- **Clocks/Bridges:** access to OneVue Sync devices and features.
- **Transmitters:** access to OneVue Sync Transmitters and features.
- **Bell Controllers/Message Boards:** access to OneVue Notify Bell Scheduling devices and features. Ethernet only Message Boards discontinued in 2019.
- **InfoBoards:** access to OneVue Notify InfoBoard and MiniBoard devices and features.

Configure a user's access to data, system features, and device types (roles and device classes)

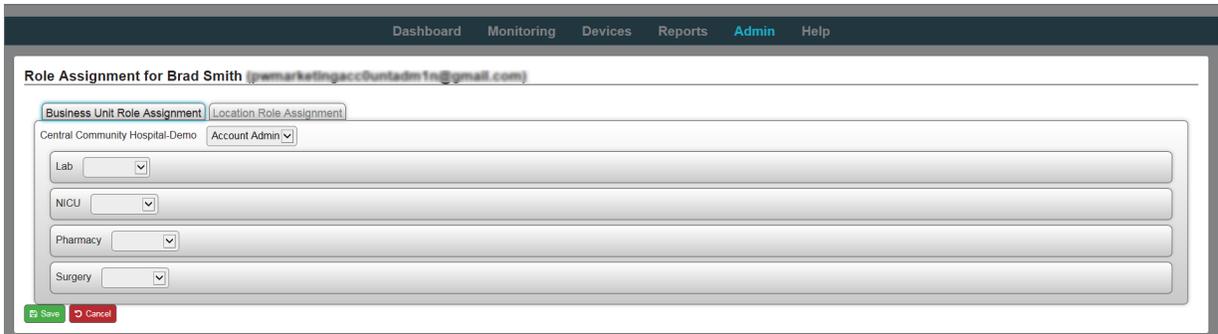
Access to OneVue account data and the permissions to system features are granted by way of the Role(s) assigned to each user. Roles are designed to mirror common job functions.

- Each user is assigned a Role(s) by Business Unit and/or a Location.
- Device Classes grant a user access to specific Primex devices, which is set in their User Profile. Your OneVue users should only be assigned to the Device Classes that apply to the OneVue solution deployed at your organization. If you have multiple OneVue solutions, be sure to assign users to only the Device Classes they are responsible for.
- Only a user assigned to the Account Admin role can manage the Roles assigned to a user and a BU Admin can only assign a Role to a user when they create a new user for their Business Unit. An Account Admin and BU Admin (for users assigned to their Business Unit) can managed a users' assigned Device Classes and timeout exempt settings. A user cannot view these settings from their profile.

For an admin user these settings are required to be managed by another user assigned to the Account Admin role. It's recommended to have a minimum of two users assigned to the Account Admin role.

Assign user to a role

1. Go to **Admin > Users**.
2. Select the **Email link** of the user.
3. Select **Assign Roles**.
4. From the Business Unit or Location tab, select the **Role** to be assigned to the user. If applicable, assign a Role to each of the Business Units and/or Locations.



5. Select **Save**.

The User Profile has been assigned to the Role(s).

Assign a user to a device class

1. Go to **Admin > Users**.
2. Select the **Email link** of the user.
3. From **Device Classes**, select the checkbox for the devices the user is to have access to.
 - **Sensors:** access to OneVue Sense devices and features.
 - **Clocks/Bridges:** access to OneVue Sync devices and features.
 - **Transmitters:** access to OneVue Sync Transmitters and features.
 - **Bell Controllers/Message Boards:** access to OneVue Notify Bell Scheduling devices and features. Ethernet only Message Boards discontinued in 2019.
 - **InfoBoards:** access to OneVue Notify InfoBoard and MiniBoard devices and features.
4. Select **Save**.

The User Profile has been granted access to the selected Device Classes.

Set a user to be excluded from the account session timeout period

The account level session timeout period sets the amount of time the system automatically ends a user's OneVue login session due to inactivity. When a user is excluded from the account session timeout period, they are never logged out of OneVue due to inactivity.

1. Go to **Admin > Users**.
2. From the list, select the **Email link** of the user.
3. From the account level session timeout setting, select the **Timeout Exempt** checkbox.
4. Select **Save**.

Resend a user their account invite notification

If a user has not activated their OneVue account, an admin user can resend their new user account invite notification. During activation, the user establishes their password and accepts OneVue terms and conditions.



NOTE

A user can also select **Forgot Password** from the OneVue log in screen to resend their new account email invitation.

1. Go to **Admin > Users**.
2. Select the **Email link** of the user.
3. Select **Resend Invite**.

The user receives an email notification with the instructions to activate their OneVue user account.

Deactivate or activate a user

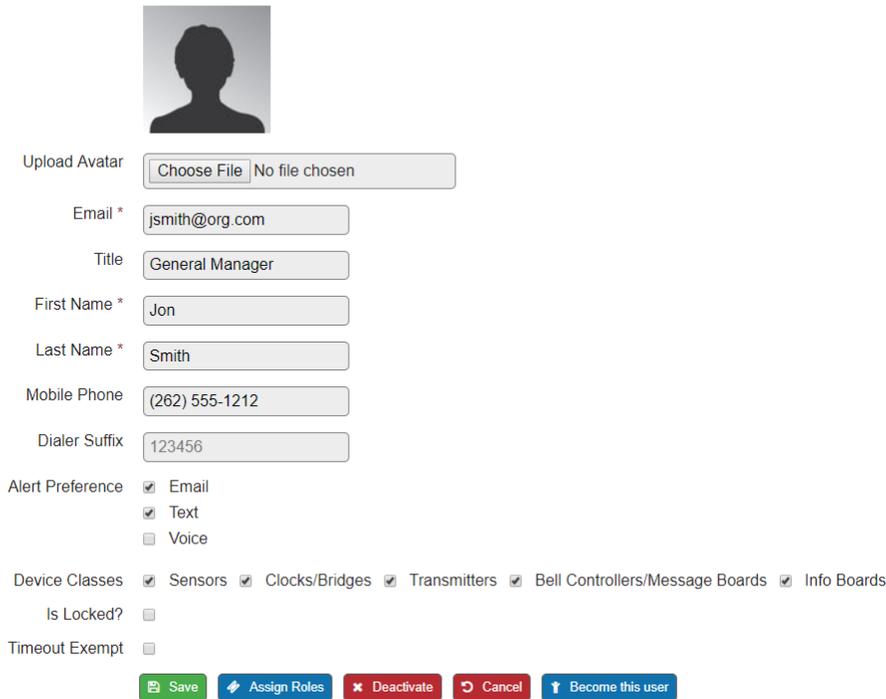
A User Profile can be deactivated to remove their access to OneVue. Once deactivated, the User Profile can either be deleted from your OneVue account or activated at a later date.

- A deactivated user can no longer log in to OneVue.
- Alert or system notifications are not sent to a deactivated user.
- Deactivating a user does not remove any data created or associated to their User Profile.
- When deactivating a user, you can assign a user to receive the deactivated user's Alerts, Reports, and Custom Views.
- The user can be activated at a later date. Once activated, the user can log in to your OneVue account and all access to Alerts, Reports, and Custom Views is also reactivated.
- Once deactivated, the user can be deleted [19] from your OneVue account.

Deactivate a user

1. Go to **Admin > Users**.
2. Select the **Email link** of the user to deactivate.
3. From the bottom section, select **Deactivate**.

User Profile



The form displays a user profile for 'Jon Smith'. It includes an avatar upload section, a 'Choose File' button, and a 'No file chosen' message. The user's email is 'jsmith@org.com', title is 'General Manager', first name is 'Jon', and last name is 'Smith'. The mobile phone number is '(262) 555-1212' and the dialer suffix is '123456'. Alert preferences are checked for 'Email', 'Text', and 'Voice'. Device classes are checked for 'Sensors', 'Clocks/Bridges', 'Transmitters', 'Bell Controllers/Message Boards', and 'Info Boards'. The 'Is Locked?' and 'Timeout Exempt' checkboxes are unchecked. At the bottom, there are five buttons: 'Save' (green), 'Assign Roles' (blue), 'Deactivate' (red), 'Cancel' (red), and 'Become this user' (blue).

- Next, you will reassign a user to the deactivated user's custom Views, Alert Rules, and Reports. From the **Move Views To User** window, select a **user**.

Although the message displays Move Views, the selected user is also assigned to the deactivated the user's Alert Rules and Reports.

- Select **Deactivate**.

Activate a user

- Go to **Admin > Users**.
- Select the **Email link** of the user to activate.
- Select **Activate**.
- Select **Save**.

The User Profile is activated and they receive an email notifying them that their account has been activated. Their access to assigned Alert Rules, Reports, and Custom Views is also restored.

Lock or unlock a user

A User Profile can be set to locked to prevent them from logging in to your OneVue account. When a User Profile is set to locked, upon their attempt to log in the system displays a notification indicating their User Profile is locked. The user will continue to receive alert and system notifications.

Lock a user profile

1. Go to **Admin > Users**.
2. Select the **Email link** of the user.
3. From the **Is Locked** checkbox, select the checkbox. A checkmark indicates the user is locked.
4. Select **Save**.

The User Profile has been locked and cannot log in to your OneVue account.

Unlock a user profile

When a User Profile is set to locked it prevents the user from logging in to your OneVue account. Upon their attempt to log in, OneVue displays a notification indicating their User Profile is locked.

1. Go to **Admin > Users**.
2. Select the **Email link** of the user to unlock.
If the User Profile is locked, a checkmark appears in the Is Locked checkbox.
3. From the **Is Locked** checkbox, deselect the checkbox.
4. Select **Save**.

The User Profile has been unlocked and can now log in to your OneVue account.

Delete a user

A User Profile can be deleted to permanently remove the User Profile from your OneVue account.

To delete a user, the user's profile is required to be deactivated.

1. Go to **Admin > Users**.
2. Select the **Email link** of the user to delete.
3. Select **Delete**.

The User Profile is permanently deleted from your OneVue account.

Technical Support

You may require Technical Support when you have questions about product features, system 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.

Primex Technical Support

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

When you contact Primex Technical Support, please have the following information available:

- Customer ID/Account Name
- Problem description/error messages
- Device hardware information
- Troubleshooting performed before contacting Primex
- Recent network changes

PRIMEX TECHNICAL SUPPORT

Monday through Friday from 8:00 AM to 5:00 PM CT

Phone: 1-262-729-4860

Email: service@primexinc.com