

Manage login permissions for secondary logins

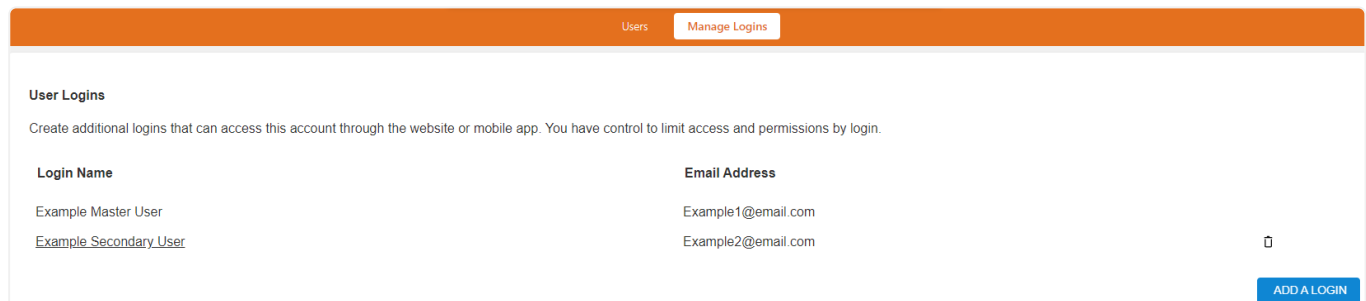
Login permissions for new and existing secondary accounts can only be managed using the customer website.

For more information about how to create a new secondary login for an account, see [Create a login for the customer website](#).

Important: Login management can only be done with a customer's login. Login management cannot be done using *Log In with Access*. For more information about logging in with access, see [Using Log In with Access](#).

To manage login permissions for secondary logins:

1. Log into the customer website.
2. Click **Users**.
3. Click **Manage Logins**.



Login Name	Email Address
Example Master User	Example1@email.com
<u>Example Secondary User</u>	Example2@email.com

ADD A LOGIN

4. In *Login Name*, click the desired login to change permissions for.

Note: Login names that are underlined can be edited.

5. Select which permission the login should be granted.
6. Click **Save**.

Permission	Description
Master Control	Users with Master Control will have all of the permissions of the primary account user, including the ability to manage website logins and change profile information such as the primary email address and phone number for the account. Master Control users will not receive certain types of account notifications that go only to the primary user (e.g., user code changes and invalid email addresses for secondary contacts).
Full Control	Users with Full Control will have all of the <i>Full Control</i> permissions described in the <i>Custom</i> permissions sections, along with most of the website and mobile app functionality available to the primary account user. Full Control users will not have the ability to manage website logins, view or edit Monitoring Station information, and they will not receive certain types of account notifications that go only to the primary user (e.g., user code changes and invalid email addresses for secondary contacts).
Read Only	Users with Read Only permissions will be able to see most of the website pages and settings for the account, including the User Codes and Live/Saved Video pages, but will not be able to make any changes to account settings, arming state, device status or view saved video. These users cannot see the Manage Logins page.
Limited Device Access	Users with limited device access will only be able to control and observe the specified devices. Note: Access to view the account's activity (i.e., Activity, Reports, Wellness, etc.) is restricted on the website and app when the Limited Device Access permission is chosen.

Permission	Description
Custom	Create a custom role to fit the exact requirements for the user. Use checkboxes to include a specific type of permission and then decide what level of control to provide the user (i.e., Read Only or Full Control). These settings can be adjusted after the login is created. Note: Custom users are able to view additional website and mobile content not listed in the Custom permissions, such as current system status, system history, their own password settings, and the system equipment list.