

Manage login permissions for secondary logins

GoSafer Security Knowledge Base

This operational reference is organized for GoSafer Security customers and staff. Alarm.com product names are retained where required for technical accuracy.

Overview

Login permissions for new or existing secondary accounts can be managed using the website.

Platform	App + Web
Content type	How-to / Configuration
Source last updated	2026-02-18

Procedure

Step-by-step guide: Screenshots and videos are placed with the instruction they illustrate.

Login permissions for new or existing secondary accounts can be managed using the GoSafer Security customer portal (powered by Alarm.com).

To manage login permissions for secondary logins:

1. Log in to the GoSafer Security customer portal (powered by Alarm.com).
2. Click **Users**.
3. Click **Manage Logins**.

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**.

Permi ssion	Description
Master Control	<p>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.</p> <p>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).</p>
Full Control	<p>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.</p> <p>Full Control users will not have the ability to manage website logins, 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).</p>
Read Only	<p>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, or device status. Read Only users cannot view saved video or SVR Timeline footage, and are unable to see the Manage Logins page.</p>

Permi ssion	Description
Limited Device Access	<p>Users with limited device access will only be able to control and observe the specified devices.</p> <p>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.</p>
Custom	<p>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.</p> <p>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.</p>

Source and support

For GoSafer Security assistance, visit gosaferssecurity.com.

Original Alarm.com reference:
https://answers.alarm.com/Customer/Website_and_App/User_Management/Web_App_Users/Manage_login_permissions_for_secondary_logins

Always verify safety, installation, compatibility, and current UI details against the original manufacturer documentation before operational use.

Revision #1

Created 2026-09-01 00:30:12 UTC by Jerdenn Calag

Updated 2026-09-01 16:52:24 UTC by Jerdenn Calag