RISCO Cloud

RISCO Application Server

Web Application User Guide

For more information about the control panels that are supported by the RISCO Cloud Web Application please refer to our Website: www.riscogroup.com

RISCO GROUP

Creating Security Solutions. With Care.

riscogroup.com

Table of Contents

1. Introduction

The Remote Management Solution is made up of a control system, various detectors and a number of optional peripheral devices. The Web Application is an important part of this system.

The **Control System** is the brain of the system. It communicates with all the devices connected to the system. For example, in the event of a burglary, a detector sends a signal to the control system indicating that it has sensed motion on the premises. On receiving this signal, the control system makes the decision to report the alarm to your monitoring service and activate the siren.

Detectors are the devices that protect your home, alerting the control system when there is a breach in security. Magnetic contacts protect your doors and windows while motion detectors with integrated cameras are able to detect and display an intruder moving across its field of view.

Keyfobs are hand-held transmitters that are used to operate the system. Various keyfobs are available providing a number of functions. For example, arming/disarming the system and sending panic alarms.

Keypads enable you to communicate with the control system in order to perform a number of different functions. The main function you can perform using a keypad is to arm the system when leaving your home and to disarm on your return.

The control system includes a built-in **Internal Siren** that is sounded during certain alarm conditions to warn you and deter intruders.

When an event occurs during **System Monitoring**, the control system sends a message to your monitoring service via the Web describing the exact nature of the event. This enables the monitoring service to take the required action.

The **Web Application (RISCO Cloud)** provides a full interface to your system from a local or remote PC. Via the Web you can perform a wide range of tasks such as arm/disarm, zone bypass, user code management and home automation control.

The **Smartphone Application (iRISCO)** provides access to the Web Application from your Smartphone (iPhone or Android).

2. Self Registration

The Web Application is part of the service provider's Web site and requires the end user to register in order to gain access to the Web site.

Note:

If your service provider has already registered you to the Web Application and has also provided you with a User Name and Password, then you can move straight onto the Logging In section.

To Register to the Web Application:

1. Enter the Web page address supplied by your service provider into your browser and press Go. The Login page is displayed.

Figure 1: Login Page

Note:

If you have already registered but forgotten your Login details, click the Password Recovery link and you can request that the password to be sent to your predefined email address.

2. Click the Self Registration link. The Self Registration page is displayed.

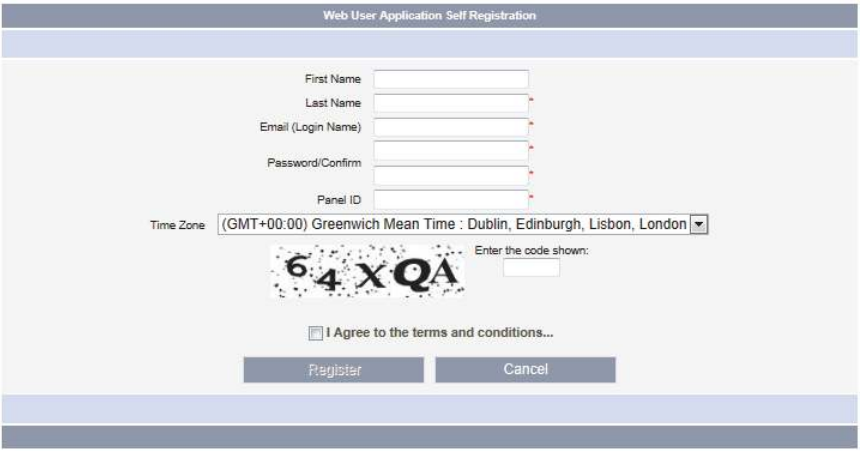

Figure 2: Self Registration Page

3. Enter the following registration details into the Self Registration page:

First/Last Name	Enter your First and Last Name
Email (Login Name)	Enter your chosen Login Name (i.e. email address)
Password/Confirm	Enter your chosen Password (2 times)
Panel ID	Enter your Panel ID (supplied by your service provider or as displayed on your control panel card)
Time Zone	Select your location time zone
Anti-Spam Code	Enter the displayed anti-spam code into this field
Terms and Conditions Agreement	Read the Terms and Conditions Agreement and check the checkbox to continue

4. Click Register. The Self Registration process sends a confirmation email to your specified email address.
5. From the received email, click the attached link to confirm your registration. The Login page is displayed and you can now login to the Web Application.

3. Logging In

To enter the Web Application from within your browser, enter the Web page address supplied by your service provider and press Go. The Login page is displayed.

Figure 3: Login Page

To login to the Web Application:

1. Enter your User Name and Password that was supplied to you by your service provider or that you supplied during the self registration process.
2. Enter your Pass Code (User Code) and click the Enter/Login button.

Note:

For your system security reasons, you must change the password immediately at first login. You can change your password on the Change Password page that is accessible from the Settings menu. Your new password should be a minimum of 6 characters, with at least 1 digit.

When using the Smartphone application service, the Login page may look similar to the following examples:

Figure 4: Login Page (iPhone)

Figure 5: Login Page (Android)

Note:

You can discuss the Smartphone capability with your security service provider to determine if it is applicable to your system.

4. The Main Page

After logging in, your system's home page is displayed. The following diagram shows the Main page and explains the main elements of the Web application's interface

Figure 6: Main Page

4.1. Menu Bar

The Menu Bar includes the Main Menu options as well as the Log Off button. The Main Menu offers the user links to various pages in the Web Application. Use the Logoff button on the right side of the menu to close the session.

The following options are available from the Main Menu:

- Home – pressing the Home button allows the user to return to the Home page at any time.
- Arm/Disarm – provides access to the System Operation Area page.
- Settings – offers various options including user code and contact management, event log viewing and zone bypass.
- History – enables you to view the system's event log.
- Video – provides access to Video Monitoring and Stored Events (only available if supported devices are installed).
- Automation – allows you to control and schedule automated electrical appliances in your home (only available if supported devices are installed).
- Help/Download – offers online explanations on how to use the Web Application plus FAQ and customer support options.

4.2. Status Bar

The Status bar displays information on your system's status and the name of the user currently logged in. Above the status bar, the time when the system status display was last updated is shown. This information is displayed according to the local time at the control system. The system status refreshes automatically, and can also be refreshed manually. To refresh the current system status, click the Refresh Status button on the right-hand side of the Status bar.

4.3. Workspace

The workspace offers additional links to the following pages of the application: System Operation, Settings, History, Video and Automation. When you choose a page, either from the Main Menu, or from the workspace, the page is displayed in the workspace. For example, if you choose Arm/Disarm from the Main Menu, System Operation Area page and System Status area are displayed in the workspace (see the example below).

Figure 7: Workspace Example Page

You can arm and disarm the system using the Arm/Disarm drop-down box (upper-right part of the page) or using the buttons in the System Operation Area.

- The Web Application allows you to arm and disarm your system using any of the available arming methods.
- On the Status Bar below on the page you can see the current status of the system (in our example it is Disarmed and System Ready, which means that the system and all the detectors are working properly and there are no events to report). It is possible to check if there were alarms in the system.

Note:

It is important to note that when you are using the Web application, the system is armed with the programmed delay.

4.4. Home Button

Press the Home button on the Main menu to return to the Main page at any time.

4.5. Main Page (Smartphone)

When using the Smartphone application service, the Main page may look similar to the following examples:

Figure 8: Home Page (iPhone)

Figure 9: Home Page (Android)

Note:

You can discuss the Smartphone capability with your security service provider to determine if it is applicable to your system.

5. Arming and Disarming

Arming can be defined as turning the system on. When the system is armed, it monitors the zones that are protected by the detectors. If a detector detects an intrusion, the system generates an alarm. Certain detectors can be programmed by your installer to be active 24 hours a day. These detectors are always active regardless of system status.

To display the System Operation Area page:

On the Menu Bar, click Arm/Disarm. The System Operation page is displayed.

Figure 10: System Operation Area Page

Two arming modes are available: Away and Part. These modes enable you to arm your system accordingly to suit different circumstances.

Full Arming	Full Arming activates the entire system. This arming method is used when you intend to leave your home, leaving the premises empty.
Part Arming	Part Arming enables you to arm a section of your home while remaining on a different part of the premises. For example, at night your family is upstairs while the area downstairs is armed.

Before arming the system, check that all doors and windows are closed so that the system is ready for arming. System status is displayed on the status bar at the bottom of the page. If you are arming from a remote location and the system status is "Not Ready", you may temporarily bypass any zone that is causing this condition.

Disarming can be regarded as turning the security system off. When the system is disarmed only zones that are defined as active 24 hours are monitored (e.g. Flood, Gas and Panic zones).

6. Web Application Settings

The Web Application Settings area offers various options including system/Web user codes, contact and password management, user interface appearance and descriptors, event log viewing and zone bypass capabilities.

6.1. System Users and Codes

The System Users and Codes page enables you to manage your system's users. The page displays a table of the system's current users and enables you add, edit and delete users as required.

Note:

This capability is available only to a user with a Master code, the highest level of authorization.

The System Users and Codes page provides a useful tool for managing your system's users. In this area you can add, delete, or change System Users and the User Codes for your system (for example, add/edit codes for family members).

The following System User types are available:

Grand Master	The Grand Master Code is used by the system's owner and is the highest Authority Level. The owner can set/change the Grand Master Code.
Users	There are no restrictions in the number of User Codes (as long as they do not exceed the number of codes remaining in the system). The User has access to the following: ➢Arming and disarming ➢Bypassing zones ➢Viewing system status, trouble, and alarm memory ➢Activating designated Utility Outputs ➢Changing his/her own User Code ➢Setting keypad's settings.
Cleaner	The Cleaner Code is a temporary code, which is to be immediately deleted from the system as soon as it is used to arm. This code is typically used for maids, home attendants, and repairmen who must enter the premises before the owner(s) arrive. These codes are used as follows: ➢ For one-time arming in one or more partitions ➢ If first used to disarm the system, the code may be used once for subsequent arming

Arm Only	There are no restrictions in the number of Arm Only Codes (as long as they don't exceed the number of codes remaining in the system). Arm Only Codes are useful for workers who arrive when the premises are already open, but because they are last to leave, they're given the responsibility to close the premises and arm the system. The users with Arm Only Codes have access for arming one or more partitions.
Duress	When coerced into disarming the system, the user can comply with the intruder's wishes while sending a silent duress alarm to the Central Station. To do so, a special duress code must be used, which when used, will disarm the system in the regular manner, while simultaneously transmitting the duress alarm. In any other situation the Duress authority level behaves as the same as the User authority level.

To display the System Users and Codes page:

1. On the Menu Bar, click Settings.
2. Click System Users and Codes. The System Users and Codes page is displayed.

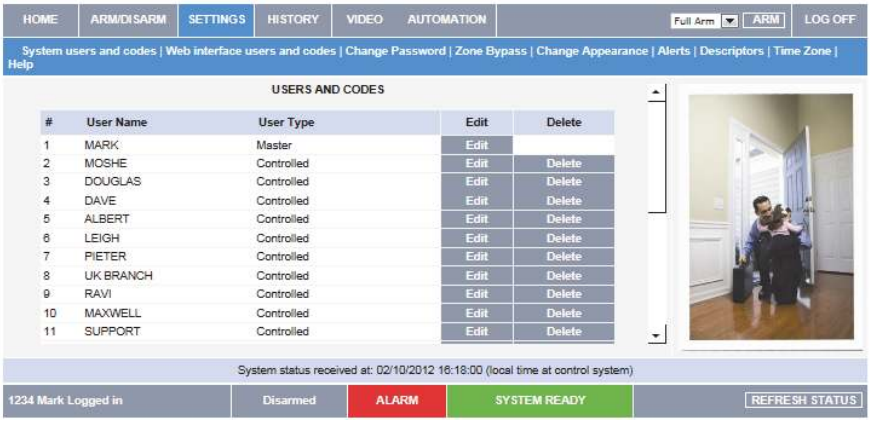

Figure 11: System Users and Codes Page

To add a new system user:

1. Click Add New User at the bottom of the table; the Add New System User page opens.

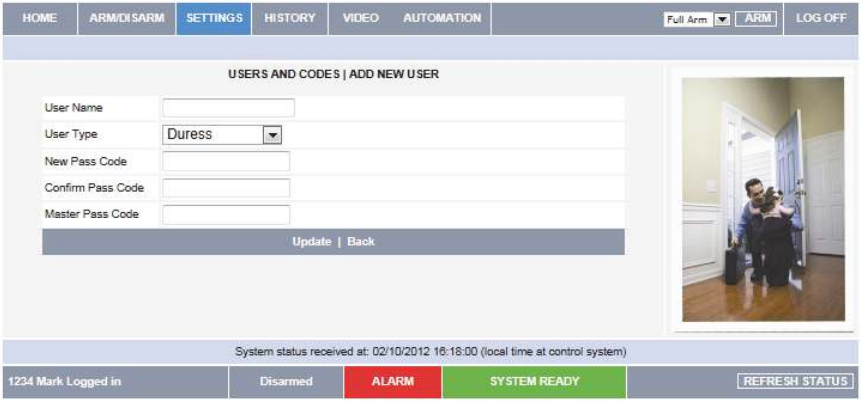

Figure 12: Add New System User Page

2. Enter the user's name in the field provided (16 characters max.).
3. Choose the user type from the available options.
4. Enter the new user's passcode.
5. Enter the new user's passcode again for confirmation.
6. Enter your Master code.
7. Click Update.

To edit an existing system user:

1. Click Edit for the user you want to modify; the Edit User page opens.
2. Edit the user's name in the field provided (16 characters max.).

Note:

When editing an existing user, you cannot change the user type.

3. Enter the user's passcode.
4. Enter the user's passcode again for confirmation.
5. Enter your Master code.
6. Click Update.

To delete a system user:

1. Click Delete for the user you want to remove from the table; the confirmation page opens.
2. Click Yes to confirm.

6.2. Web Interface Users and Codes

The Web Interface Users and Codes page enables you to manage your Web users. The page displays a table of the system's current users and enables you add, edit and delete users as required. You can even issue temporary (limited) codes to guests that will automatically expire after 24 hours.

To display the Web Interface Users and Codes page:

1. On the Menu Bar, click Settings.
2. Click Web Interface Users and Codes. The Web Interface Users and Codes page is displayed.

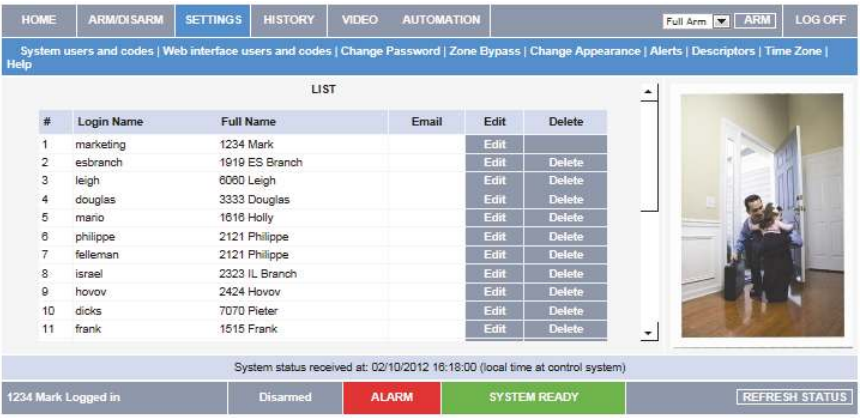

Figure 13: Web Interface Users and Codes Page

To add a new Web user:

1. Click Add New User at the bottom of the table; the Add New Web User page opens.

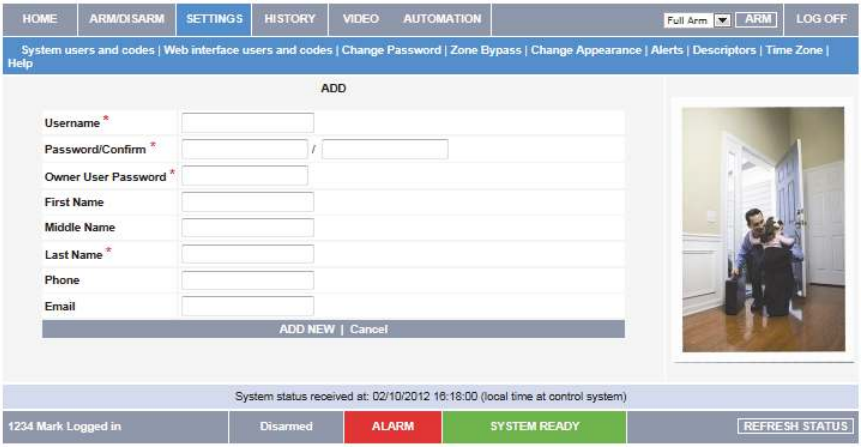

Figure 14: Add New Web User Page

2. Enter the user's name in the field provided (16 characters max.).
3. Enter the new user's password.
4. Enter the new user's password again for confirmation.
5. Enter the Owner User password.
6. Enter the First Name, Middle Name and Last Name of the new user in the fields provided.
7. Enter Phone and Email details of the new user into the fields provided.
8. Click Add New.

To edit an existing Web user:

1. Click Edit for the user you want to modify; the Edit User page opens.
2. Edit the user's name in the field provided (16 characters max.).
3. Enter the user's password.
4. Enter the user's password again for confirmation.
5. Enter the Owner User password.
6. Edit the First Name, Middle Name and Last Name of the user in the fields provided.
7. Edit the Phone and Email details of the user into the fields provided.
8. Click Update.

To delete a Web user:

1. Click Delete for the user you want to remove from the table; the confirmation page opens.
2. Click Yes to confirm.

6.3. Change Password

The Change Password page allows you to modify the password you use to log in to the Web Application.

To change the password:

1. On the Menu Bar, click Settings.
2. Click Change Password. The Change Password page is displayed.

Figure 15: Change Password Page

3. Enter the old password.
4. Enter a new password.

Note:

The new password should be a minimum of 6 characters, with at least 1 digit.

5. Enter the new password again for confirmation.
6. Click Set New Password.

6.4. Zone Bypass

A bypassed zone is ignored by the system and does not generate an alarm when triggered. To "unbypass" a zone is to restore the zone, effectively instructing the system to monitor activity from that zone.

Note:

All bypassed zones are automatically unbypassed when the system is disarmed.

The Zone Bypass page displays a list of the zones (i.e. detectors) in your system and allows you to bypass or unbypass them as required.

To bypass a zone:

1. On the Menu Bar, click Settings.
2. Click Zone Bypass. The Zone Bypass page is displayed.

Figure 16: Zone Bypass Page

The table of zones displays your system's detectors and their current bypass status.

3. Check the checkboxes for the zones you want to bypass.
4. Click Update.

Note:

To restore a bypassed zone to normal operation, you can "unbypass" the zone.

6.5. Change Appearance

The Change Appearance page allows you to choose a color scheme for the interface of the Web Application.

To change the interface color scheme:

1. On the Menu Bar, click Settings.
2. Click Change Appearance. The Change Appearance page is displayed.

Figure 17: Change Appearance Page

3. Click "Set" underneath the required color scheme or "Set Default" to restore the default color scheme.

6.6. Alerts

The Alerts feature allows those people included in your contact list to be notified by email or SMS when certain events occur. The page displays a table of the system's alert contacts and enables you add, edit, test and delete contacts as required.

To display the Alerts page:

1. On the Menu Bar, click Settings.
2. Click Alerts. The Alerts page is displayed.

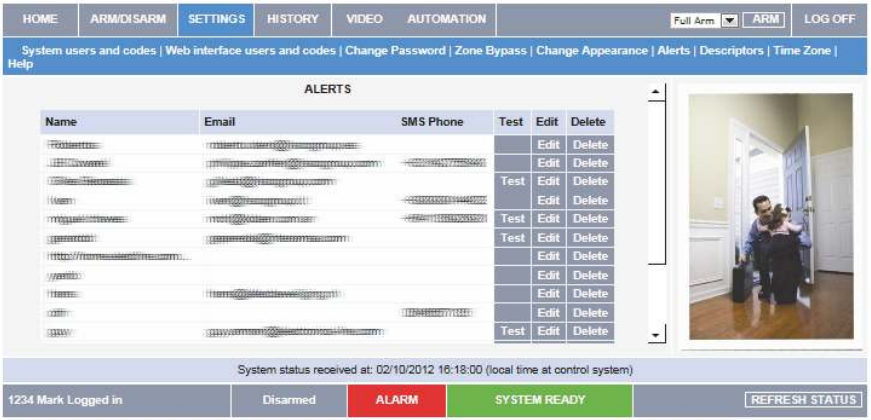

Figure 18: Alerts Page

To add new alert contact:

1. Click Add New at the bottom of the table; the Add New Alert Contact page opens.

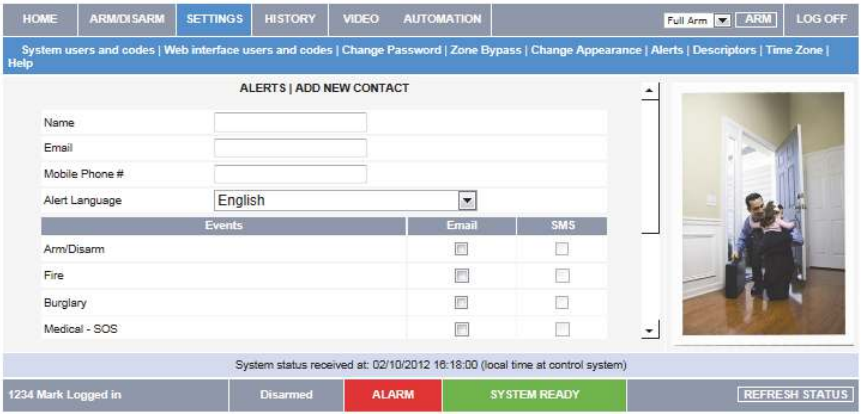

Figure 19: Add New Alert Contact Page

2. Enter the contact's name in the field provided.
3. Enter the new contact's email address.
4. Enter the new contact's mobile phone number
5. Select the alert language from the available list.
6. Choose the event and message type from the available options (Email, SMS).

Note:

SMS alert option is only available for selection if SMS functionality is supported

7. Click Update.

To send a test message:

1. Click Test for the contact to whom you want to send a test message; a confirmation page appears.
2. Click OK.

To edit an existing alert contact:

1. Click Edit for the contact you want to modify; the Edit Alert Contact page opens.
2. Edit the contact name, email address and mobile number as required.
3. Choose the event and message type from the available options (Email, SMS).
4. Click Update.

To deleting an alert contact:

1. Click Delete for the contact you want to remove from the table; the confirmation page opens.
2. Click Yes to confirm.

6.7. Descriptors

The Descriptors page allows you to edit descriptors of registered devices for the selected control panel.

To display the Descriptors page:

1. On the Menu Bar, click Settings.
2. Click Descriptors. The Descriptors page is displayed.

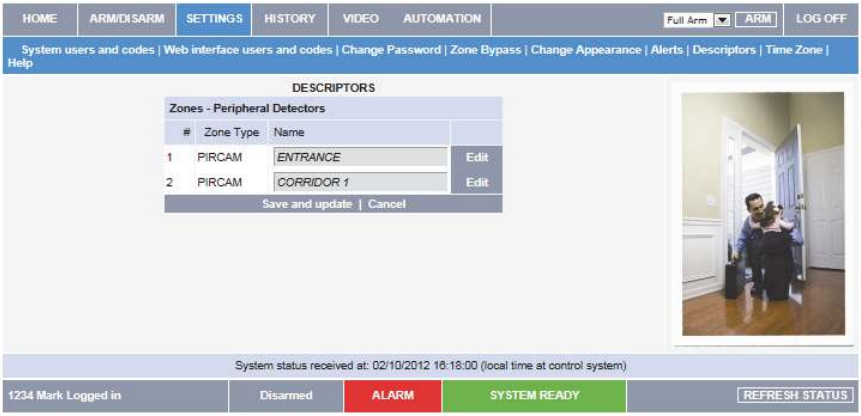

Figure 20: Descriptors Page

To edit a descriptor:

1. Click Edit for the descriptor you want to modify; the Edit Descriptor page opens.
2. Edit the descriptor as required.
3. Click Update.

6.8. Time Zone

The Time Zone page allows you to define the time zone for the control panel.

To display the Time Zone page:

1. On the Menu Bar, click Settings.
2. Click Time Zone. The Time Zone page is displayed.

Figure 21: Time Zone Page

3. Choose the applicable time zone from the available options.
4. Click Update.

7. Event Log History

The Event Log History page displays a log of events that have occurred within your system. For each event you can view the date and time that the event occurred, a description of the event, the user or device that caused the event and whether or not the event was reported to your monitoring service. In addition to viewing the event log, you can view any images related to an event. You can also save the log to a pre-formatted file or simply print the log.

To view the event log history:

On the Menu Bar, click History, the Event Log History Page is displayed:

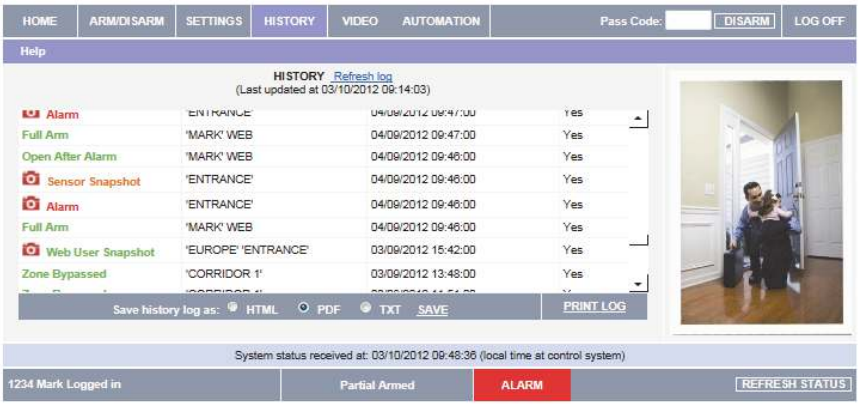

Figure 22: Event Log History Page

To view images related to an event:

Click on the Image icon displayed in front of the event. The selected event image is displayed.

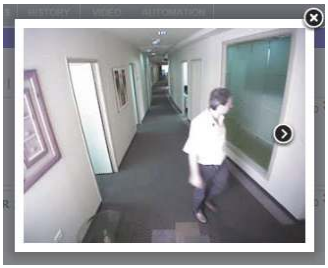

Figure 23: Event Image

To save the event log:

Select the type of file you want to save (HTML, PDF or RTF) and click Save.

To print the event log:

Click Print Log (located in the bottom right hand corner underneath the event log table).

8. Home Automation

Home Automation allows you to control and schedule automated lights and appliances in your home. The Web application offers a comprehensive interface that enables you to view the settings for all of your automated devices at once. Additionally, you can control devices from the system.

To view the Home Automation page:

On the Menu Bar, click Automation, the Home Automation Page is displayed:

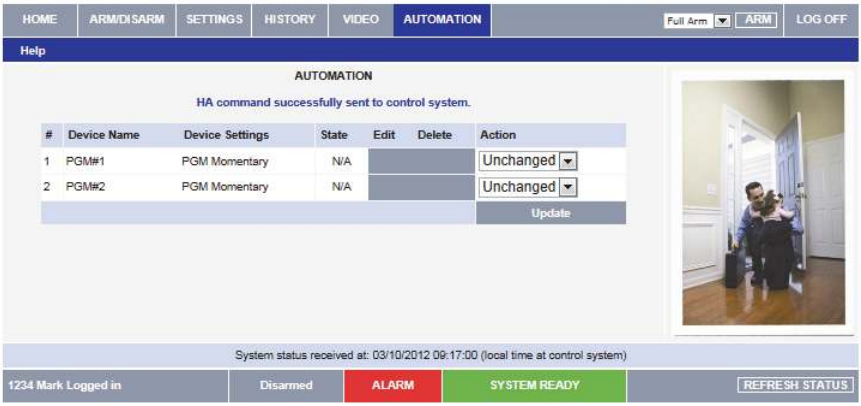

Figure 24: Home Automation Page

The Automation page displays a table of your automated devices and each device's scheduled settings.

To control automated devices:

1. In the Action column, choose Turn On or Turn Off for the devices you wish to control.
2. Click Update.

Note:

You can discuss the home automation capability with your security service provider to determine if it is applicable to your system.

9. Video Verification

Using the 2-way wireless PIR camera detectors installed in your home, the Web application enables you to view captured images over the Web in order to check your home and family while you are away.

To view the Video Verification page:

On the Menu Bar, click Video, the Video Verification Page is displayed:

Figure 25: Video Verification Page

The Video Verification page displays a list of your installed PIR camera detectors and each device's descriptor (see Descriptors). The Web application provides the capability to take an image on request for each PIR camera detector, view the stored image events log and define camera settings.

9.1. Image upon Request

A manual image capture option is available, for example, to test the installation location of each device as well as the quality of the captured image.

To perform image upon request:

Select the device that you would like to capture an image and click the associated Take Image button. The captured image is displayed.

Figure 26: Captured Image

For each image, the following is displayed; the date and time that the image occurred, the user or device that caused the event and the image location.

9.2. Stored Image Events

The Web application provides the capability to view the stored image events. The Stored Image Events page displays a log of image events that have occurred within your system. For each event you can view the date and time that the event occurred and the user or device that caused the event.

To view the image event log:

From the Video Menu Bar, click Images; the Image Event Log Page is displayed:

Figure 27: Stored Image Events Page

To view the stored event image:

Click the relevant stored image event. The Stored Event Image is displayed.

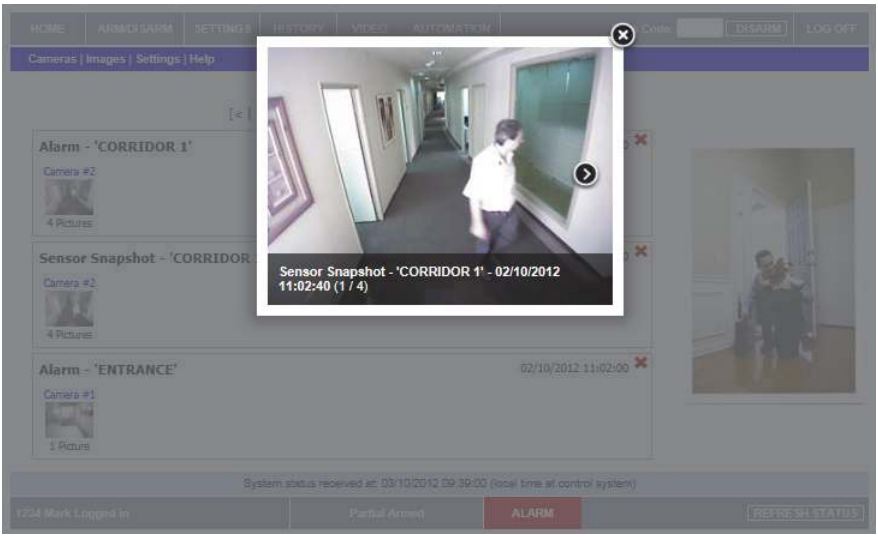

Figure 28: Stored Event Image

For each stored image, the following is displayed; the date and time that the event occurred, the user or device that caused the event and the event location.

9.3. Settings

The Web application provides the capability to modify the PIR camera detectors parameter settings according to your needs.

To view the video verification settings page:

From the Video Menu Bar, click Settings; the Video Verifications Settings Page is displayed:

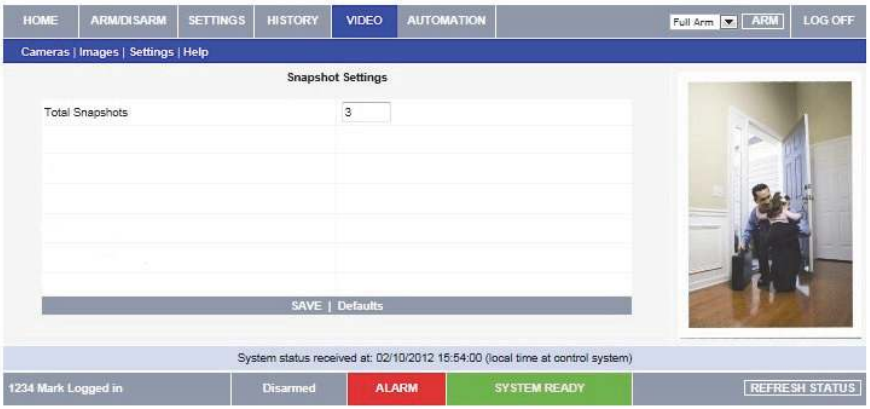

Figure 29: Video Verification Settings Page

To modify the PIR camera detectors parameter settings:

1. Enter the number of images that are required upon an alarm (1 to 7)
2. Click Save.

Note:

You can discuss this capability with your security service provider to determine if it is applicable to your system.

RISCO Group Limited Warranty

RISCO Group and its subsidiaries and affiliates warrants its products to be free from defects in materials and workmanship under normal use for 24 months from the date of production. Because Seller does not install or connect the product and because the product may be used in conjunction with products not manufactured by the Seller, Seller cannot guarantee the performance of the security system which uses this product. Seller's obligation and liability under this warranty is expressly limited to repairing and replacing, at Seller's option, within a reasonable time after the date of delivery, any product not meeting the specifications. Seller makes no other warranty, expressed or implied, and makes no warranty of merchantability or of fitness for any particular purpose.

In no case shall seller be liable for any consequential or incidental damages for breach of this or any other warranty, expressed or implied, or upon any other basis of liability whatsoever. Seller's obligation under this warranty shall not include any transportation charges or costs of installation or any liability for direct, indirect, or consequential damages or delay.

Seller does not represent that its product may not be compromised or circumvented; that the product will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the product will in all cases provide adequate warning or protection.

Seller, in no event shall be liable for any direct or indirect damages or any other losses occurred due to any type of tampering, whether intentional or unintentional such as masking, painting or spraying on the lenses, mirrors or any other part of the detector.

Buyer understands that a properly installed and maintained alarm may only reduce the risk of burglary, robbery or fire without warning, but is not insurance or a guaranty that such event will not occur or that there will be no personal injury or property loss as a result thereof. Consequently seller shall have no liability for any personal injury, property damage or loss based on a claim that the product fails to give warning. However, if seller is held liable, whether directly or indirectly, for any loss or damage arising under this limited warranty or otherwise, regardless of cause or origin, seller's maximum liability shall not exceed the purchase price of the product, which shall be complete and exclusive remedy against seller. No employee or representative of Seller is authorized to change this warranty in any way or grant any other warranty.

WARNING: This product should be tested at least once a week.

Contacting RISCO Group

RISCO Group is committed to customer service and product support. You can contact us through our website www.riscogroup.com or as follows:

United Kingdom
Tel: +44-(0)-161-655-5500
technical@riscogroup.co.uk

Italy
Tel: +39-02-66590054
support@riscogroup.it

Spain
Tel: +34-91-490-2133
support-es@riscogroup.com

France
Tel: +33-164-73-28-50
support-fr@riscogroup.com

Belgium
Tel: +32-2522-7622
support-be@riscogroup.com

USA
Tel: +1-631-719-4400
support-usa@riscogroup.com

Brazil
Tel: +55-11-3661-8767
support-br@riscogroup.com

China (Shanghai)
Tel: +86-21-52-39-0066
support-cn@riscogroup.com

China (Shenzhen)
Tel: +86-755-82789285
E-mail: support-cn@riscogroup.com

Poland
Tel: +48-22-500-28-40
support-pl@riscogroup.com

Israel
Tel: +972-3-963-7777
support@riscogroup.com