RISCO GROUP

Creating Security Solutions. With Care.

RISCO Cloud

Remote Management Application

Installer Application Manual

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

Contents

Introduction

This guide provides information regarding the Remote Management Application (RISCO Cloud) and instructions on how to use the Installer Web Administration application. The target audience for the guide is the personnel responsible for installations and installer administration. The principle purpose of this guide is to provide the reader with the information necessary to manage RISCO Cloud installers and WEB based RP users and customers (subscribers).

Related Documents

The Agility™3 and LightSYS™2 User & Installer manuals provide additional information on some of the subjects addressed in this guide.

Abbreviations

Abbrev.	Description
CP	Control Panel, Security Panel or Control System
CPNS	Control Panel Notification Service
CPWS	Control Panel Web Service
CSR	Central Station Receiver
Proxy	RISCO Proxy Server
GPRS	General Packet Radio Service
IIS	Internet Information services
ISP	Internet Service Provider
RISCO Cloud/Proxy	RISCO Application/Proxy Server
RISCO Cloud	RISCO Application Server
PSTN	Public Switched Telephone Network
RP	Remote Programmer application
SIA	Security systems event reporting protocol
SP	Service Provider
WAApp	Web Administrative Application
WIApp	Web Installer Application
WUApp	Web User Application

Overview

Remote Management Application (RISCO Cloud) is the central component of RISCO's Web based service platform. Implementing secure TCP/IP network connectivity, RISCO Cloud provides high-speed central station reporting via a broadband interface. The predominant role of the RISCO Cloud is to handle and manage communications between security systems installed in the homes and businesses of subscribers and multiple alarm monitoring service providers. In addition to event reporting, RISCO Cloud enables the security system to be programmed and controlled via the Web by means of a number of Web applications and utilities.

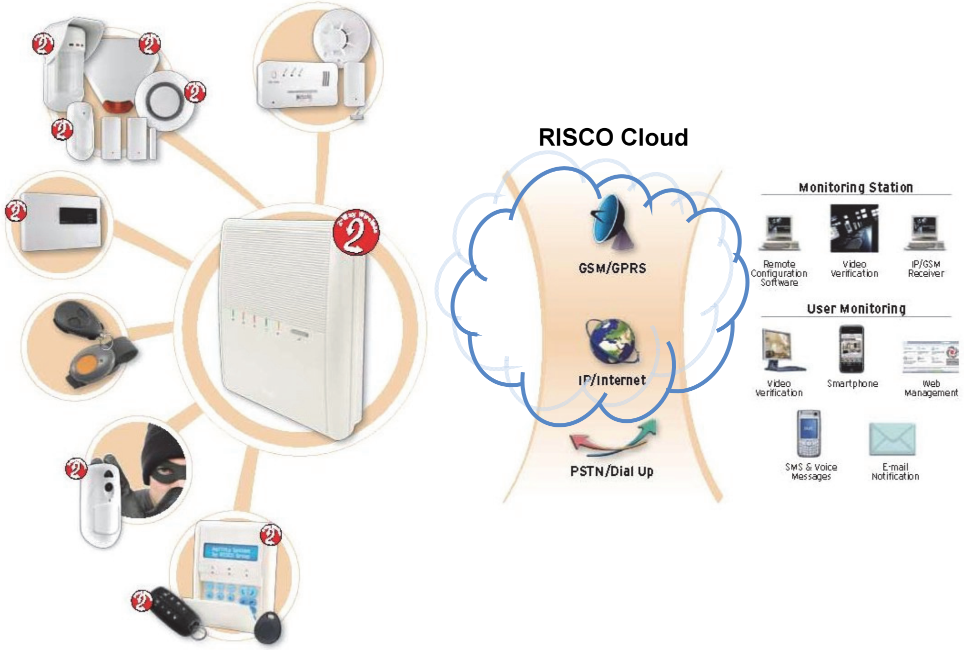


Figure 1 System Architecture

The main components of the system are:

- **RISCO Cloud/Proxy –** application/proxy server responsible for connection between end-users' control panels and service providers, for system management, and data transfer to the central station's alarm monitoring system
- **RISCO Security Panels –** Control panels with GSM/GPRS, IP or PSTN connection.

Installer Registration

The Installer Administration application is one of many components of the RISCO Application Server (RISCO Cloud) and requires the installer to register in order to gain access to this service.

NOTE – If your distributor has already registered you to the Installer Administration application and has provided you with a User Name and Password, then you can move straight onto the Logging In section.

Registering to the Installer Administration Application

1. Enter the Web page address supplied by your distributor (https://www.riscocloud.com/installer) into your browser and press Go. The Installer Login page is displayed.

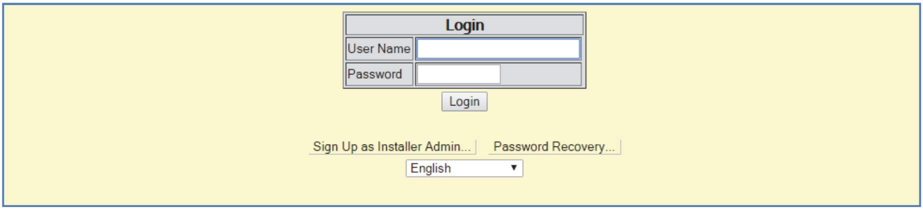


Figure 2 Installer Login page

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 Sign Up as Installer Admin link. The Installer Admin Self Registration page is displayed.

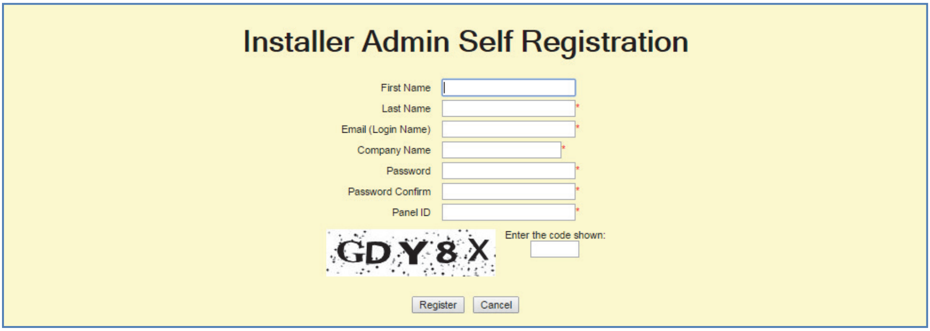


Figure 3 Installer Administration Self Registration page

3. Enter the following registration details into the provided fields:

Field	Description
First/Last Name	Enter your First and Last Name
Email (Login Name)	Enter your chosen Login Name (i.e. email address)
Company Name	Enter your company name into this field
Password Confirm	Enter your chosen Password (2 times)
Panel ID	Enter your Panel ID (supplied by your distributor or as displayed on your control panel) **NOTE** – Panel ID is required only on first time registration.
Anti-Spam Code	Enter the displayed anti-spam code into this field

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 Installer Administration Application.

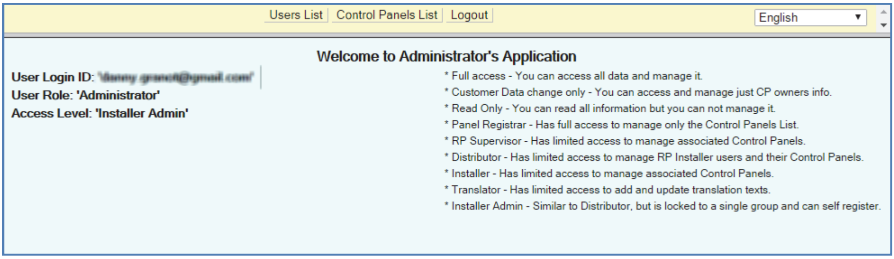
Login to the Installer Administration Application

To begin a session, the Installer Administration application requires that the Installer logs in.

Login

To log into the Installer Administration application:

1. Enter user name and password.
2. Click Login; the Main page is displayed.



Welcome to Administrator's Application

User Login ID: [redacted]
User Role: 'Administrator'
Access Level: 'Installer Admin'

* Full access - You can access all data and manage it.
* Customer Data change only - You can access and manage just CP owners info.
* Read Only - You can read all information but you can not manage it.
* Panel Registrar - Has full access to manage only the Control Panels List.
* RP Supervisor - Has limited access to manage associated Control Panels.
* Distributor - Has limited access to manage RP Installer users and their Control Panels.
* Installer - Has limited access to manage associated Control Panels.
* Translator - Has limited access to add and update translation texts.
* Installer Admin - Similar to Distributor, but is locked to a single group and can self register.

Figure 4 Main page

The Main page displays the details of the current user. At the top of the page, there is a menu offering links to the various pages of the application.

Logout

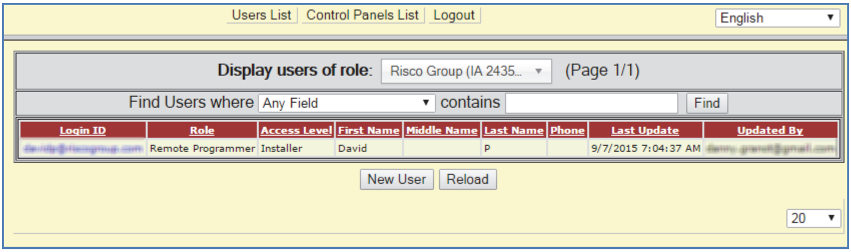
To end a session, the Installer Administration application requires that the Installer logs out.

Click Logout; you are automatically returned to the Log In page.

Installer Admin/WEB RP User Management

On the Users List page, you can view the list of users / installers who are authorized to enter the Installer Administration Application or the Web Remote Programmer (RP) application.

NOTE – For RP users, there is an option to display the list for each group of panels specifically



Display users of role: Risco Group (IA 2435... (Page 1/1)

Find Users where Any Field contains

Login ID	Role	Access Level	First Name	Middle Name	Last Name	Phone	Last Update	Updated By
[redacted]	Remote Programmer	Installer	David		P		9/7/2015 7:04:37 AM	[redacted]

Figure 5 Users List page

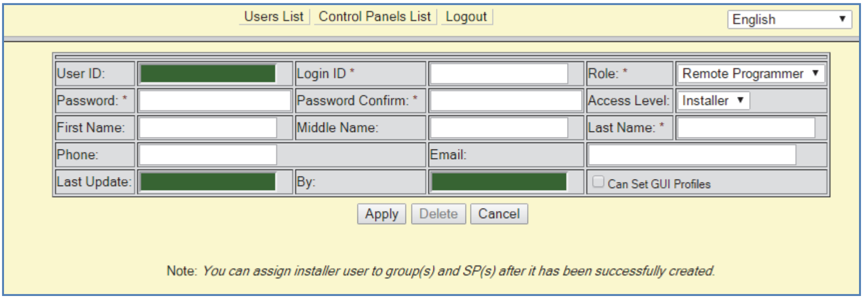
Column	Description
Login ID	The user name that is entered when logging in.
Role	The type of user. The role can only be Remote Programmer (RP user).
Access Level	The authorization level of the user. The access level can only be Installer.
First/Middle/Last Name	User's personal details for identification purposes.
Phone	User’s telephone number for reference purposes.
Last Update	The date when the user’s details were last edited.
Updated By	The RISCO Cloud WAApp operator who last updated the user’s details. (If Deleted displayed in the Update By column, meaning this Administrator User was deleted from the RISCO Cloud DB)

Column	Description
Display List Filtering	The users display list can be filtered by selection of the list length on the foot of the page on the right, or by selecting the Display Installers assigned to group from the dropdown list on the top of the table.

Adding a New User / Installer

To add a new user / installer:

1. On the Users List page, click New User (located at the foot of the list); the User Update page is displayed.



User ID:		Login ID *		Role: *	Remote Programmer ▾
Password: *		Password Confirm: *		Access Level:	Installer ▾
First Name:		Middle Name:		Last Name: *	
Phone:			Email:		
Last Update:		By:		□ Can Set GUI Profiles	

Note: *You can assign installer user to group(s) and SP(s) after it has been successfully created.*

Figure 6 New User page

NOTE – Mandatory fields are indicated by an asterisk (*).

2. Enter the new user's login ID, password (twice) and personal details in the appropriate fields.

NOTE – The User ID is automatically assigned once the new user is saved in the system.

3. Select the Can Set GUI Profiles checkbox to enable the user to set functionality profiles for control panels. Functionality profiles are used to define what the end user can see and do with their app or web application.
4. Click Apply to save.

Editing an Existing User / Installer

To edit the existing user / installer's details:

1. On the Users List page, click the Login ID Name of the user / installer you wish to edit (colored in blue); the User Update page is displayed.
2. Edit the user / installer's details as required.
3. Click OK to save.

Deleting a User

To delete a user / installer:

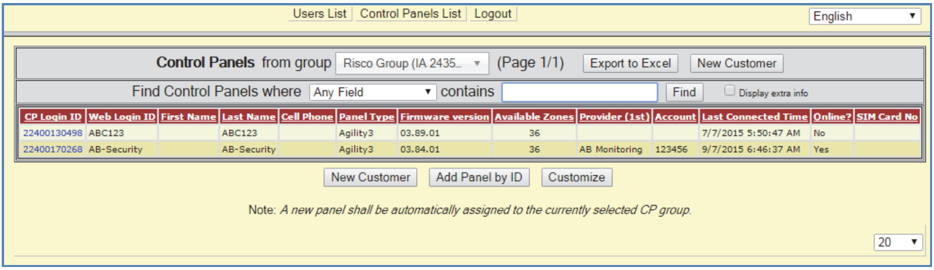
1. On the Users List page, click the Login ID of the user / installer you wish to delete; the User Update page is displayed.
2. Click Delete and then OK; the user is deleted.

Control Panels List

The Control Panels List is an inventory of the installers' control panels. A control panel must appear in the list in order to be recognized by RISCO Cloud.

To view the Control Panels List:

1. Open the Control Panels List page.
2. Choose the appropriate search filters for the control panels you wish to view and click Find; the required entries in the Control Panels List are displayed.



Control Panels from group Risco Group (IA 2435... (Page 1/1)

Find Control Panels where Any Field contains

CP Login ID	Web Login ID	First Name	Last Name	Cell Phone	Panel Type	Firmware version	Available Zones	Provider (1st)	Account	Last Connected Time	Online?	SIM Card No
22400130498	ABC123		ABC123		Agility3	03.89.01	36			7/7/2015 5:50:47 AM	No	
22400170268	AB-Security		AB-Security		Agility3	03.84.01	36	AB Monitoring	123456	9/7/2015 6:46:37 AM	Yes	

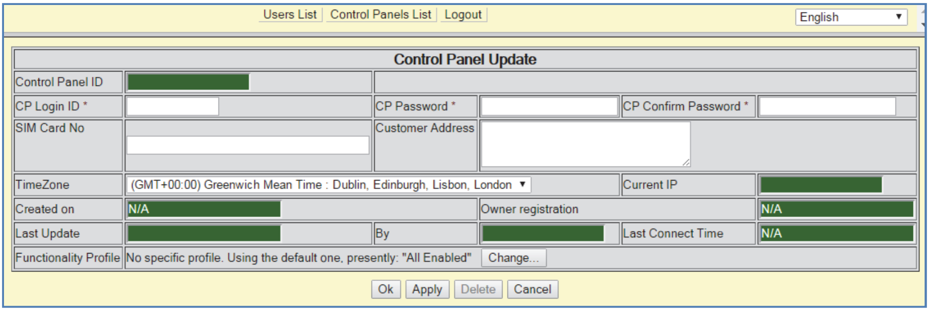
Note: *A new panel shall be automatically assigned to the currently selected CP group.*

Figure 7 Control Panels List page

Adding a New Control Panel

To add a new control panel:

1. On the Control Panels List page, click New Customer; the New Control Panel page is displayed.



Control Panel Update

Control Panel ID					
CP Login ID *		CP Password *		CP Confirm Password *	
SIM Card No		Customer Address			
TimeZone	(GMT+00:00) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London			Current IP	
Created on	N/A		Owner registration		N/A
Last Update		By		Last Connect Time	N/A
Functionality Profile	No specific profile. Using the default one, presently: "All Enabled"				

Figure 8 New Control Panel page

2. Enter the new customer’s details in the appropriate fields. The available fields are described in the following table.

Field	Description
Control Panel ID	The serial number of the control panel that is allocated automatically when the customer is created.
CP Login ID	The digits used by the control panel for identification when connecting to RISCO Cloud. This parameter must be identical to the CP ID programmed at the control panel. To edit this field, click the Change button to the right of the field then click OK in the confirmation dialog box. The maximum number of characters you should enter for the CP ID is 11.
CP Password/ CP Confirm Password	Used by the control panel for authentication when connecting to RISCO Cloud. This parameter must be identical to the CP Password programmed at the control panel. The maximum number of characters you should enter for the CP Password is 16. Confirmation field for the previously entered CP Password.
SIM Card No.	Unique number of the SIM card used in the Control Panel
Customer Address	The customer's physical address details for identification purposes.

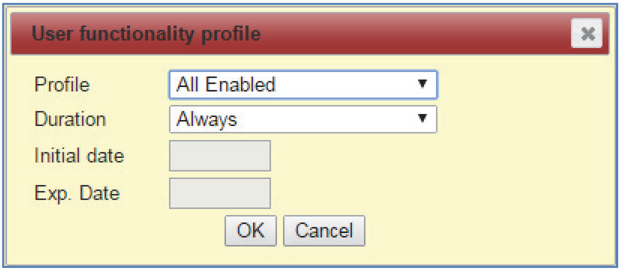
Field	Description
Time Zone	The UTC offset and time zone in which the control panel is located (offset from GMT)).
Current IP	IP address of the control panel (this parameter is displayed after the first connection between the control panel and RISCO Cloud).
Last Update/By	Last time the control panel fields were updated and details of the user/administrator that performed the changes.
Last Connect Time	Last time the control panel connected to RISCO Cloud.

Enabling Functionality Profile for a Control Panel

On the Control Panel page you can enable/disable functionality profiles for control panels. Functionality profiles are created by the administrator and can be used to define what the end user can see and do with their app or web application.

To enable functionality profile for a control panel:

1. Click the Functionality Profile Change button. The User Functionality Profile dialog window is displayed.



User functionality profile

Profile	All Enabled
Duration	Always
Initial date	
Exp. Date	

Figure 9 User Functionality Profile

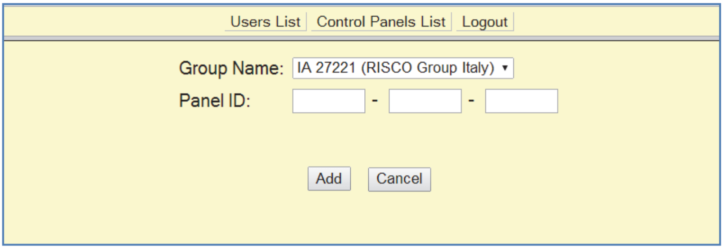
2. Select the profile type.
3. Select the duration of the profile.
4. Define the profile start and end date (for Custom duration only).
5. Click OK to confirm.

Adding an Existing Control Panel by Panel ID

This allows you to add an exisiting control panel but has not yet been associated with a group/installer.

To add an existing control panel by Panel ID:

1. On the Control Panels List page, click Add Panel by ID button; the Add Panel by ID dialog box is displayed.



Group Name: IA 27221 (RISCO Group Italy) ▾

Panel ID: - -

Figure 10 Adding existing control panel

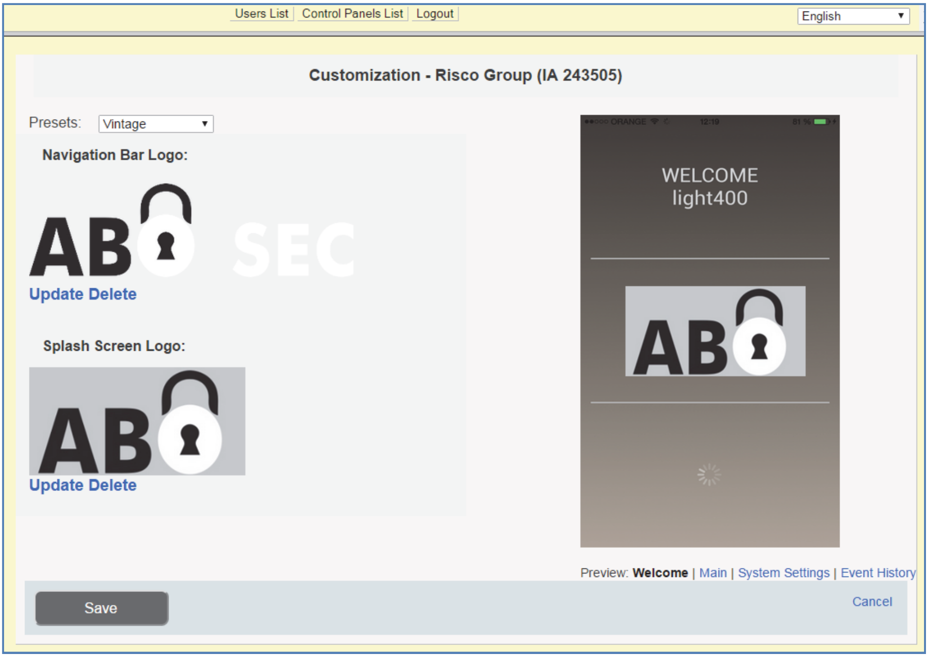
2. Enter the Control Panel ID number in the Panel ID fields.
3. Select the associated group from the Group Name drop-down and click Add. The control panel will be added to the list of panels associated with the selected group installer.

Customizing a Control Panel Group (Branded App only)

On the Control Panel page you can customize a control panel group. This option is otherwise referred to as the Branded App (FreeControl). Branded App customization can be used to define how the app or web application is displayed to the end user.

To customize a control panel group:

1. On the Control Panel List page, click the Customization button; the Add Panel by ID Control Panel Group Customization page is displayed.



Customization - Risco Group (IA 243505)

Presets: Vintage

Navigation Bar Logo:

Splash Screen Logo:

Users List | Control Panels List | Logout
English
AB SEC
Update Delete
AB
Update Delete
WELCOME
light400
AB
Preview: Welcome | Main | System Settings | Event History
Save
Cancel

Figure 11 Control Panel Group Customization page

2. Select a predefined template from the Presets dropdown list.
3. Click Update to change the Navigation Bar or Splash Screen logo accordingly.
4. Click Browse and choose a file to open.

NOTE – For best display, please select images with the following dimensions: Navigation bar logo: 220*73 or 186*62 and Splash screen logo: 972*486 or 912*456.

5. Click Save to confirm.

You can preview your selection by clicking the relevant Preview link:

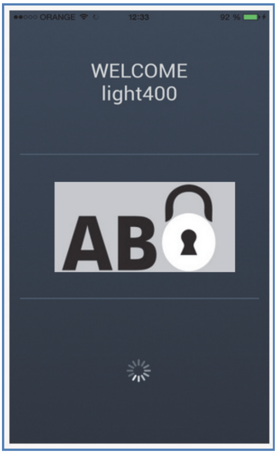


Figure 12 Preview – Welcome

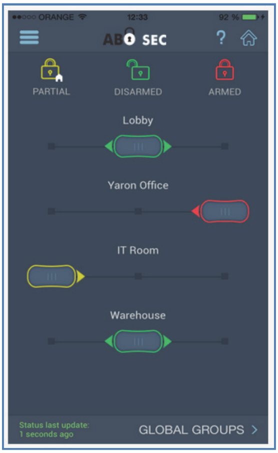
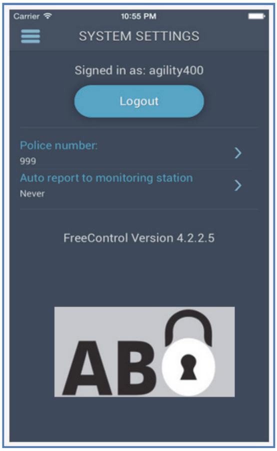


Figure 13 Preview – Main



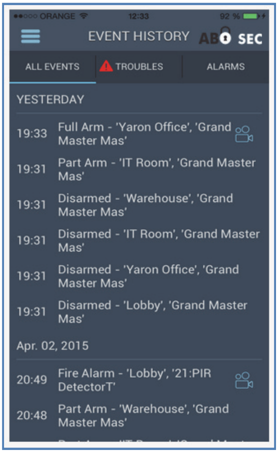
Signed in as: agility400

Police number:
999

Auto report to monitoring station
Never

FreeControl Version 4.2.2.5

Figure 14 Preview – System Settings



YESTERDAY

19:33 Full Arm - 'Yaron Office', 'Grand Master Mas'

19:31 Part Arm - 'IT Room', 'Grand Master Mas'

19:31 Disarmed - 'Warehouse', 'Grand Master Mas'

19:31 Disarmed - 'IT Room', 'Grand Master Mas'

19:31 Disarmed - 'Yaron Office', 'Grand Master Mas'

19:31 Disarmed - 'Lobby', 'Grand Master Mas'

Apr. 02, 2015

20:49 Fire Alarm - 'Lobby', '21:PIR DetectorT'

20:48 Part Arm - 'Warehouse', 'Grand Master Mas'

Figure 15 Preview – Event History

6. Click Save to complete.

Editing an Existing Control Panel

To edit an existing control panel:

1. On the Control Panels List page, click the CP Login ID of the customer you wish to edit; the Control Panel Update page is displayed.
2. Enter the control panel's details as required.
3. Click OK to save.

Deleting a Control Panel

To delete a control panel:

1. On the Control Panels List page, click the CP login ID of the control panel you wish to delete; the Control Panel Update page is displayed.
2. Click Delete and then OK; the control panel is deleted.

Additional Control Panel Options

On opening the Control Panel Update page, the column on the left hand side offers a number of additional options relevant to each control panel.
These are as follows:

Event Forwarding – allows the user to enable or disable the event forwarding groups that are available for the Alerts event forwarding feature in the Web User Application.

Service Providers – allows the user to define the service provider (monitoring service) to which events are reported.

Network Cameras – allows the user to define the IP cameras in use with the control panel.

Web Users – allows the user to add additional Sub users for the security panel.

Group Membership – allows the user to view the panel groups assigned.

User Video Events – on this page the user can define additional user video event parameters and view a log of the video events removed by the web user.

CP Statistics – allows the user to view general statistical information about the selected control panel and associated Web and Smartphone user

Smartphone List – allows the user to view the list of registered Smartphone's associated to the selected control panel.

Licenses – currently not available

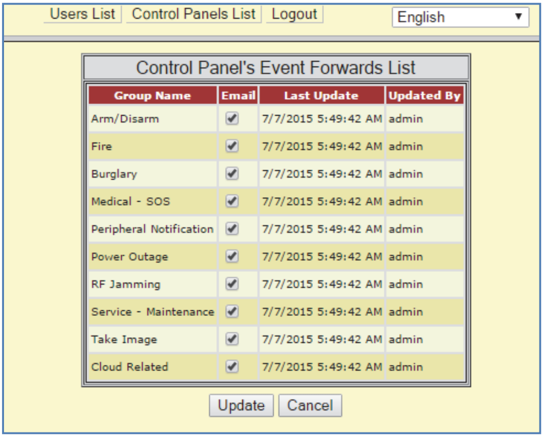
These options are explained in the following sections.

Event Forwarding

Alert notification is an event forwarding feature that allows notification by email after an event has occurred. The list of event forwarding options appears on the Control Panel Update page located below the customer details. This option in the Web Administration application is used for enabling or disabling email notification per event forwarding group. Contacts for event forwarding, however, are edited by the customer in the Alerts section of the Web User application. The user fills in contacts credentials and then chooses the desired events to be forwarded from the available groups, as chosen by the installer administrator on this page.

To edit event forwarding options:

1. Open the Control Panel Update page.
2. Click the Event Forwards link in the left-hand column; the Event Forwards table is displayed.



Control Panel's Event Forwards List

Group Name	Email	Last Update	Updated By
Arm/Disarm	☑	7/7/2015 5:49:42 AM	admin
Fire	☑	7/7/2015 5:49:42 AM	admin
Burglary	☑	7/7/2015 5:49:42 AM	admin
Medical - SOS	☑	7/7/2015 5:49:42 AM	admin
Peripheral Notification	☑	7/7/2015 5:49:42 AM	admin
Power Outage	☑	7/7/2015 5:49:42 AM	admin
RF Jamming	☑	7/7/2015 5:49:42 AM	admin
Service - Maintenance	☑	7/7/2015 5:49:42 AM	admin
Take Image	☑	7/7/2015 5:49:42 AM	admin
Cloud Related	☑	7/7/2015 5:49:42 AM	admin

Figure 16 Event Forwards table

3. Using the checkboxes that appear in the E-mail column, enable or disable event forwarding per event group as required.
4. Click Update to confirm.

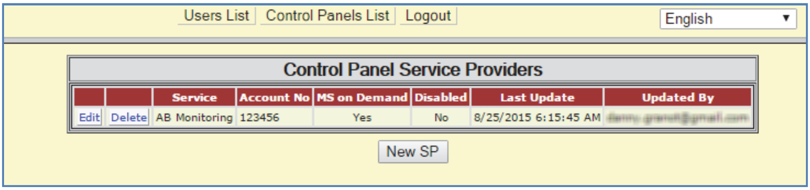
Service Provider

Service providers are monitoring stations to which RISCO Cloud forwards event data. This section explains how to allocate a service provider to a control panel. The list of service providers available for allocation to a control panel is determined by the administrator of the application.

Each control panel can be allocated with several service providers, Proxy or IP SIA. This ensures that the service provider to which the customer has subscribed will receive the relevant event messages generated by the customer's security system. The event will be filtered by the Event Forwarding as explained above.

To allocate a service provider to a control panel:

1. Open the Control Panel Update page.
2. Click the Service Providers link in the left-hand column; the Service Providers List is displayed.

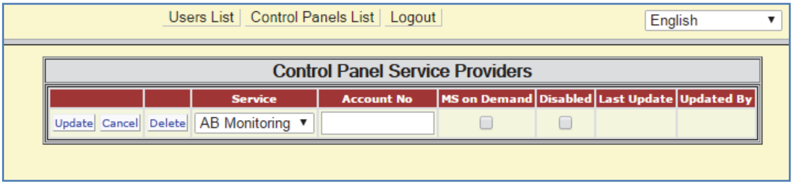


Control Panel Service Providers

		Service	Account No	MS on Demand	Disabled	Last Update	Updated By
Edit	Delete	AB Monitoring	123456	Yes	No	8/25/2015 6:15:45 AM	[redacted]

Figure 17 Service Provider List

3. Click on New SP button then choose an available service provider.



Control Panel Service Providers

		Service	Account No	MS on Demand	Disabled	Last Update	Updated By
Update Cancel	Delete	AB Monitoring ▼		□	□		

Figure 18 New Service Provider Allocation table

4. Enter the account number in the text field provided.

NOTE – This account will be reported in the events sent to service provider's monitoring system, regardless of the account number registered in the panel for other means of communication.

5. Select the MS on Demand checkbox to enable the monitor station monitoring option for the service provider's control panels. This allows the service provider the option to authorize monitoring station monitoring whenever the end user thinks it's necessary.
6. Select the Disabled checkbox to enable the disable option for the service provider's control panels.
7. Click Update.

To edit a control panel's service provider:

1. Open the Control Panels Update page.
2. Click the Service Providers link in the left-hand column; the Service Providers table is displayed.
3. Click the Edit link next to the control panel's service provider.
4. Edit the service provider details as required.

NOTE – If you want to disable the service provider without deleting it from the control panel's record, select the Disabled check box

5. Click Update.

To delete a service provider from a control panel record:

1. Open the Control Panel Update page.
2. Click the Service Providers link in the left-hand column; the Service Providers table is displayed.
3. Click the Delete link next to the control panel's service provider; the service provider is deleted.

NOTE – This procedure only deletes the service provider from the control panel record and does not delete the service provider from the RISCO Cloud database.

Network Cameras

The RISCO Cloud Installer Application provides an interface to your control panel from a local or remote PC via the Web. This enables you to add IP cameras and define camera and event alarm trigger settings.

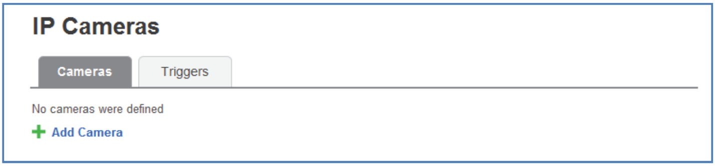
IMPORTANT – A control panel must first be defined in RISCO Cloud in order to accept IP cameras and define camera settings (Refer to Adding a New Control Panel).

Defining IP Camera Settings

Once you have connected the IP camera to the network (refer to, Connecting the IP Camera to the Network) you can define the camera settings.

To define IP camera settings:

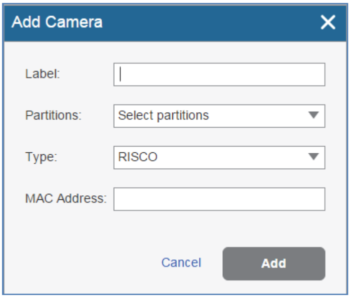
1. Open the Control Panel Update page.
2. Click the Network Cameras link in the left-hand column; the IP Camera List page is displayed (The list will be empty if no IP cameras have been defined).



No cameras were defined

Figure 19 IP Cameras List

3. Click Add Camera; the Add Camera dialog box is displayed.



Label:

Partitions: Select partitions

Type: RISCO

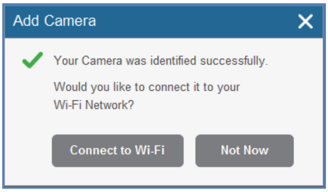
MAC Address:

Figure 8 Add Camera

4. Define the following fields in the Add Camera dialog box.

Field	Description	Camera Type
Label	Enter a name for the camera	RISCO cameras
Partitions	Select the partition(s) from the list of defined partitions	RISCO cameras
Type	Choose the RISCO camera type	RISCO cameras
MAC Address	Enter the MAC address as displayed on the box or on the back cover of the IP camera. The MAC address (media access control address) is the unique identifier assigned to the IP camera for communications on the physical network.	RISCO cameras

5. Click Add. The "Camera was identified successfully" message is displayed.



Add Camera

✓ Your Camera was identified successfully.

Would you like to connect it to your Wi-Fi Network?

Figure 20 Camera was identified successfully message

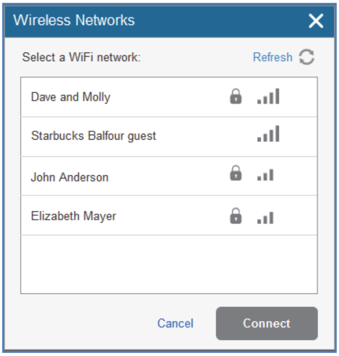
<u>NOTE</u> – This message is only relevant for IP cameras that need to be physically connected to the LAN network via the wireless router.

6. Select one of the following options:

   Connect to Wi-Fi – to establish a wireless network connection (go to step 9 to connect the IP camera to the wireless network).

   Not Now – to establish a LAN network connection (skip the wireless network connection steps 8, 9 and 10 and connect the IP camera to the LAN network).

7. If you selected the "Connect to Wi-Fi" option, a list of available wireless networks is displayed.



Wireless Networks

Select a WiFi network:

Dave and Molly

Starbucks Balfour guest

John Anderson

Elizabeth Mayer

Figure 21 List of available wireless networks

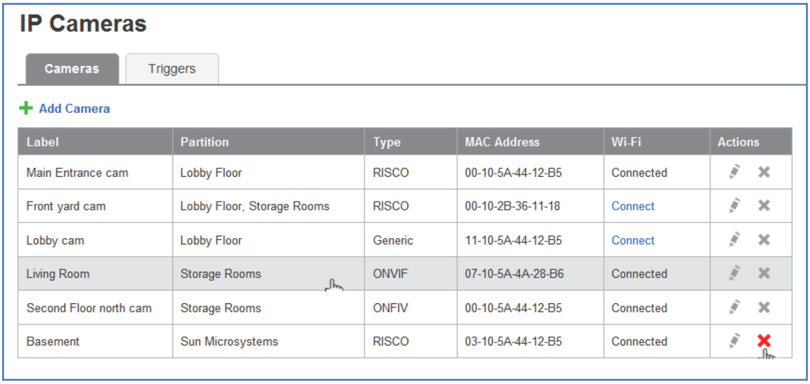
8. Select a wireless network from the available list and click Connect.

NOTE – If your network is password protected, a password must be entered into the displayed password screen.

9. Click OK to establish the wireless connection (Refer to Connecting to a Wireless Network using the RISCO Cloud).

IMPORTANT – Once a wireless connection has been established, don't forget to disconnect the IP camera from the router.

10. Once the "camera is ready for use" message is displayed, click OK. The defined IP camera is displayed in the IP Cameras page.



IP Cameras

Label	Partition	Type	MAC Address	Wi-Fi	Actions
Main Entrance cam	Lobby Floor	RISCO	00-10-5A-44-12-B5	Connected	✎ ✖
Front yard cam	Lobby Floor, Storage Rooms	RISCO	00-10-2B-36-11-18	Connect	✎ ✖
Lobby cam	Lobby Floor	Generic	11-10-5A-44-12-B5	Connect	✎ ✖
Living Room	Storage Rooms	ONVIF	07-10-5A-4A-28-B6	Connected	✎ ✖
Second Floor north cam	Storage Rooms	ONFIV	00-10-5A-44-12-B5	Connected	✎ ✖
Basement	Sun Microsystems	RISCO	03-10-5A-44-12-B5	Connected	✎ ✖

Figure 22 IP Camera List

NOTE – You also have the option to edit ✎ or delete ✖ the selected IP camera.

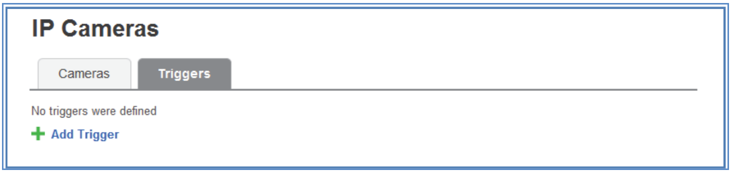
Defining Camera Trigger Settings

Any event from the following list can be defined to trigger an alarm.

Partition Events			
Fire Alarm	Panic Alarm	Medical Alarm	Alarm
Full Arm	Part Arm	Disarmed	Duress
Tamper	24 HR-X Alarm	Water Alarm	Gas Alarm
Environ. Alarm	No Motion Alarm	Exit Alarm	Low Temperature
Detector Events			
Alarm	Zone Bypassed	Zone Un-bypassed	Zone Tamper

To define camera trigger settings:

1. From the Control Panel Cameras page, click the Triggers tab, the Camera Triggers List page is displayed.

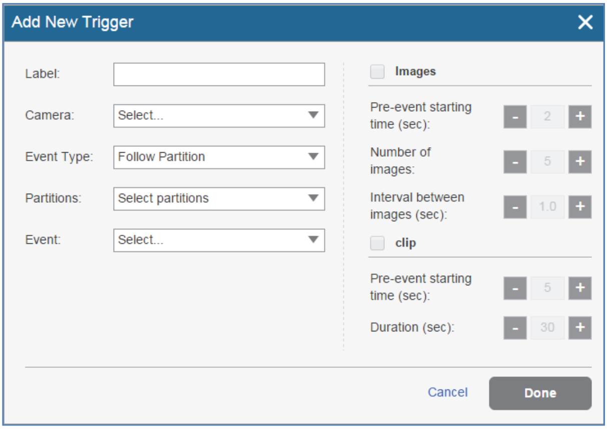


IP Cameras

No triggers were defined

Figure 23 Camera Triggers List

2. Click Add Trigger; the Add New Triggers dialog box appears.



Add New Trigger

Label:

Camera: Select...

Event Type: Follow Partition

Partitions: Select partitions

Event: Select...

□ Images

Pre-event starting time (sec): 2

Number of images: 5

Interval between images (sec): 1.0

□ clip

Pre-event starting time (sec): 5

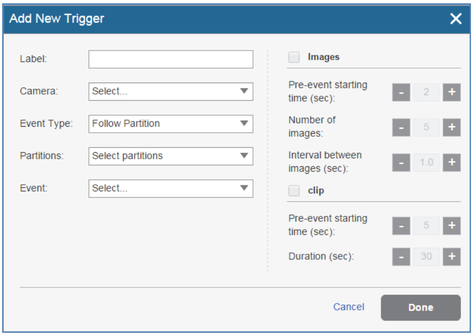
Duration (sec): 30

Figure 24 Add New Trigger

3. Define the following fields in the Add New Trigger dialog box:

Field	Description	Event Type
Label	Enter a name for the camera trigger	Partition and Detector events
Camera	Choose a camera from the list	Partition and Detector events
Event Type	Choose an event type from the list	Partition and Detector events

Additional fields are displayed in the Add Trigger dialog box according to the event type that you selected (see examples below for Partition and Detector event types).



Add New Trigger

Label:

Camera: Select...

Event Type: Follow Partition

Partitions: Select partitions

Event: Select...

□ Images

Pre-event starting time (sec): 2

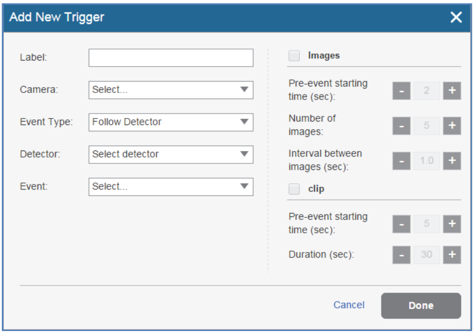
Number of images: 5

Interval between images (sec): 1.0

□ clip

Pre-event starting time (sec): 5

Duration (sec): 30



Add New Trigger

Label:

Camera: Select...

Event Type: Follow Detector

Detector: Select detector

Event: Select...

□ Images

Pre-event starting time (sec): 2

Number of images: 5

Interval between images (sec): 1.0

□ clip

Pre-event starting time (sec): 5

Duration (sec): 30

Figure 25 Add Partition Event Trigger

Figure 26 Add Detector Event Trigger

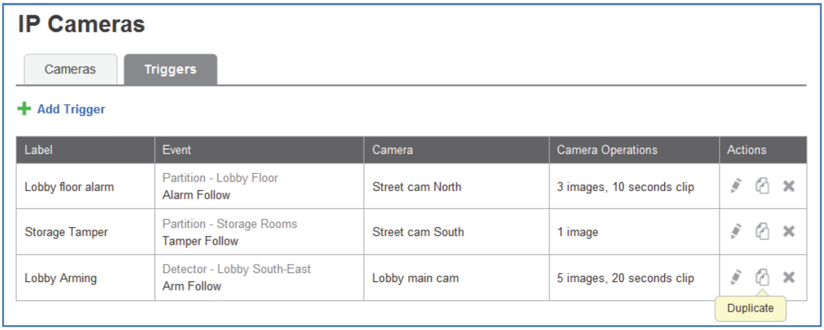
4. Define the following fields in the Add Trigger dialog box according to the event type that you selected.

Field	Description	Event Type
Partition(s)	Select the partition(s) from the list. **NOTE** – Only partitions associated with the camera are displayed.	Partition events only
Detectors	Select the detector from the list	Detector events only
Event	Select the event from the list	Partition and Detector events

5. Define the following image (still) and clip (video) definitions:

Field	Description
Images (still)	**Pre-event starting time (sec)** – time, before the actual event occurred, to start displaying still images. **Number of images** – number of still images to display. **Interval between images (sec)** – time required between each still image.
Clips (video)	**Pre-event starting time (sec)** – time, before the actual event occurred, to start displaying video clip (fixed parameter and cannot be adjusted). **Duration (sec)** – total duration of the video clip (fixed parameter and cannot be adjusted).

6. Once finished, click Done. The defined camera trigger is displayed in the Camera Triggers List page.



Label	Event	Camera	Camera Operations	Actions
Lobby floor alarm	Partition - Lobby Floor Alarm Follow	Street cam North	3 images, 10 seconds clip	✎ ⧉ ✕
Storage Tamper	Partition - Storage Rooms Tamper Follow	Street cam South	1 image	✎ ⧉ ✕
Lobby Arming	Detector - Lobby South-East Arm Follow	Lobby main cam	5 images, 20 seconds clip	✎ ⧉ ✕

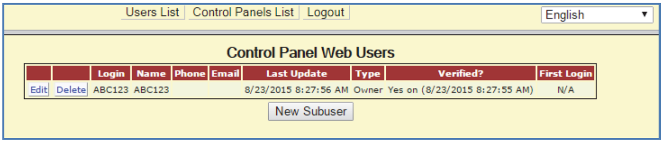
Figure 27 Camera Triggers List

NOTE – You also have the options to edit ✎, create a duplicate ⧉, or to delete ✕ the selected camera trigger.

IMPORTANT – No two camera triggers can be defined as identical. If a camera trigger is duplicated, the event, camera or both definitions must be changed.

WEB Users

On the WEB Users page, the RISCO Cloud administrator can create additional Sub users to work with the WUApp, receive Video Events and use a Look In option to view their premises. Sub users can also be created by the Master user of the security panel registered in the Control Panel Update page, and referred as Web Users in the WAApp.



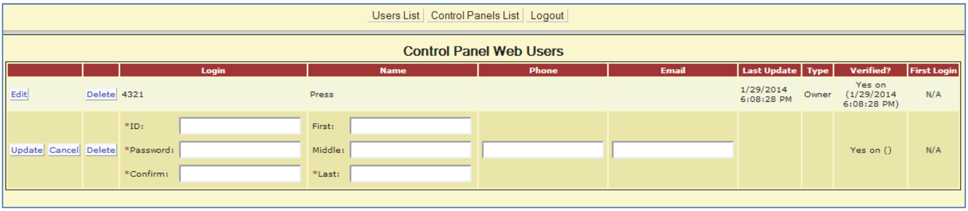
Control Panel Web Users

		Login	Name	Phone	Email	Last Update	Type	Verified?	First Login
Edit	Delete	ABC123	ABC123			8/23/2015 8:27:56 AM	Owner	Yes on (8/23/2015 8:27:55 AM)	N/A

Figure 28 New Web Page User

To create a WEB User (Sub User) to work with the control panel:

1. Open the Control Panel Update page.
2. Click the Web Users link in the left-hand column, the Control Panel Web Users page is displayed.
3. Click on New Sub user.
4. Control Panel Web Users page appears, as displayed below.



Control Panel Web Users

		Login	Name	Phone	Email	Last Update	Type	Verified?	First Login
Edit	Delete	4321	Press			1/29/2014 6:08:28 PM	Owner	Yes on (1/29/2014 6:08:28 PM)	N/A
Update Cancel	Delete	*ID: *Password: *Confirm:	First: Middle: *Last:					Yes on ()	N/A

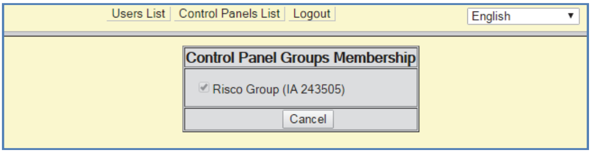
Figure 29 New Web (sub) User Creation

Field	Description
Login ID	The customer's login name that they must enter when they log in to the Web User Application (only applicable when the Self Registration option is disabled).
Login Password **Login Confirm**	The customer's password that must be entered when they log in to the Web User Application. The maximum number of characters you should enter for the Web Password is 16 and the password must begin with a letter (only applicable when the Self Registration option is disabled). Confirmation field for the Web Password (only applicable when the Self Registration option is disabled).
First/Middle/ Last Name	The customer's personal details for identification purposes (only applicable when the Self Registration option is disabled).
Cell Phone/E-mail	Additional customer information for reference purposes (only applicable when the Self Registration option is disabled).
Last Update	Last time the web user's information was updated.

Group Membership

On the Group Membership page, you can view the panel groups that the current user is assigned to.

1. Open the Control Panel Update page.
2. Click the Group Membership link in the left-hand column, the Control Panel Group Membership page is displayed.



Control Panel Groups Membership

☑ Risco Group (IA 243505)

Figure 30 View Group Membership page

3. Click Cancel to close.

User Video Events

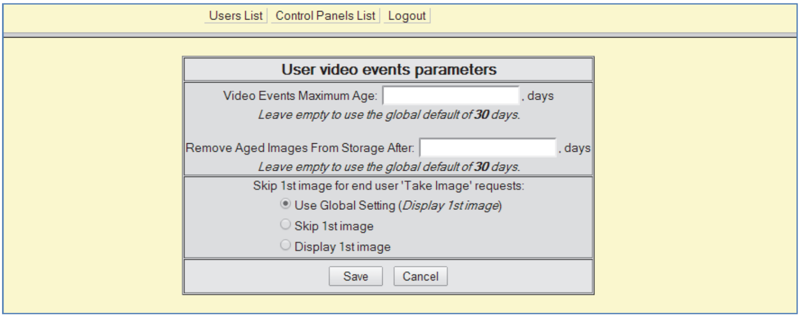
On the User Video Events page the user can define additional user video event parameters.

1. Open the Control Panel Update page.
2. Click the User Video Events link in the left-hand column, the Control Panel User Video Events page is displayed.

User Video Events

On the User Video Events page the user can define additional user video event parameters and view a log of the video events removed by the web user.

1. Open the Control Panel Update page.
2. Click the User Video Events link in the left-hand column, the Control Panel User Video Events page is displayed.



User video events parameters

Video Events Maximum Age: ____ , days

*Leave empty to use the global default of **30** days.*

Remove Aged Images From Storage After: ____ , days

*Leave empty to use the global default of **30** days.*

Skip 1st image for end user 'Take Image' requests:

● Use Global Setting (*Display 1st image*)

○ Skip 1st image

○ Display 1st image

Figure 31 Control Panel User Video Events

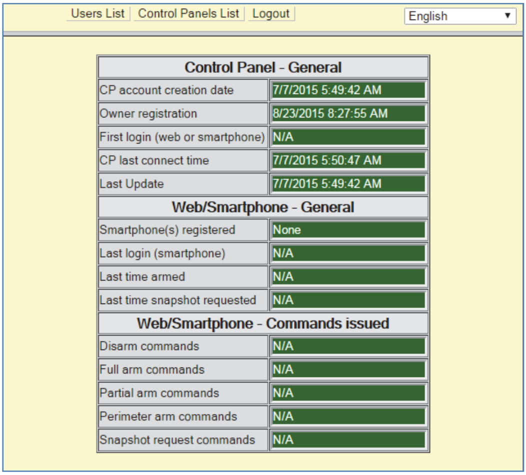
3. Define the relevant parameters.
4. Click Save to update the changes.

CP Statistics

The CP Statistics page allows the user to view general statistical information about the selected control panel and associated Web and Smartphone user.

To display the CP Statistics page:

1. Open the Control Panel Update page.
2. Click the CP Statistics link in the left-hand column; the CP Statistics page is displayed.



Control Panel - General	
CP account creation date	7/7/2015 5:49:42 AM
Owner registration	8/23/2015 8:27:55 AM
First login (web or smartphone)	N/A
CP last connect time	7/7/2015 5:50:47 AM
Last Update	7/7/2015 5:49:42 AM
Web/Smartphone - General	
Smartphone(s) registered	None
Last login (smartphone)	N/A
Last time armed	N/A
Last time snapshot requested	N/A
Web/Smartphone - Commands issued	
Disarm commands	N/A
Full arm commands	N/A
Partial arm commands	N/A
Perimeter arm commands	N/A
Snapshot request commands	N/A

Figure 32 Control Panel User Video Events

Field	Description
CP account creation date	The time the control panel account was created
Owner registration	The first time the owner of the control panel registered to the RISCO Cloud system
First login (Web or Smartphone)	The first time the user logged into the RISCO Cloud system using the web or Smartphone application was recorded
CP last connect time	The last time that the control panel connected to the RISCO Cloud system
Last update	Last time the Web or Smartphone application user's information was updated.
Smartphone(s) registered	The number of Smartphone registered to the control panel

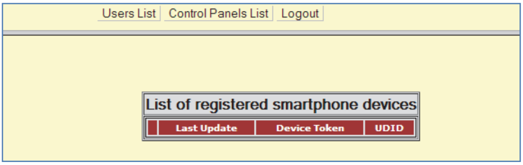
Field	Description
Last login (Smartphone)	The last time that a Web or Smartphone application user logged into the RISCO Cloud system
Last time armed	The last time Web or Smartphone application user armed the control panel
Last time snapshot requested	The last time Web or Smartphone application user requested a snapshot
Disarm commands	The number of times a Web or Smartphone application user activated a disarm command
Full arm commands	The number of times a Web or Smartphone application user activated a full arm command
Partial arm commands	The number of times a Web or Smartphone application user activated a partial arm command
Perimeter arm commands	The number of times a Web or Smartphone application user activated a perimeter arm command
Snapshot request commands	The number of times a Web or Smartphone application user activated a snapshot request command

Smartphone List

The Smartphone List page allows the user to view the list of registered Smartphone's associated to the selected control panel.

To display the Smartphone List page:

1. Open the Control Panel Update page.
2. Click the Smartphone List link in the left-hand column; the Smartphone List page is displayed.



List of registered smartphone devices

	Last Update	Device Token	UDID

Figure 33 CP Statistics

The Unregister option allows the administrator user to unregister any Smartphone user from the system.

Appendix A: Event Table

The following table explains the events that are included in the event table, their SIA and Contact ID equivalents and each event's associated event data (address field).

For each defined Service Provider, any event that appears in the event table may be enabled or disabled (i.e. an enabled event shall be forwarded to the service provider when the event is received by RISCO Cloud).

ID	Event Name	SIA	CID Code	Event Group	Address Field
0	Fire Alarm	FA	1110	Fire	Device Number
1	Panic Alarm	PA	1120	Burglary	Device Number
2	Emergency Alarm	MA	1150	Emergency	Device Number
3	Alarm	BA	1130	Burglary	Device Number
4	Fire Restore	FR	3110	Fire	Device Number
5	Panic Restore	PR	3120	Burglary	Device Number
6	Medical Restore	MR	3150	Medical – SOS	Device Number
7	Alarm Restore	BR	3130	Burglary	Device Number
8	Trouble	BT	1380	Peripherals	Device Number
9	Zone Bypassed	UB	1570	Burglary	Device Number
10	Zone Unbypassed	UU	3570	Burglary	Device Number
11	Zone Tamper	TA	1137	Burglary	Device Number
12	Tamper Restore	TR	3137	Burglary	Device Number
13	Full Arm	CL	3401	Arm/Disarm	User Number
14	Part Arm	CG	3456	Arm/Disarm	User Number
15	Perimeter Arm	CG	3441	Arm/Disarm	User Number
16	Disarmed	OP	1401	Arm/Disarm	User Number
17	Medical Alarm	MA	1100	Medical – SOS	Device Number
18	Panic Alarm	PA	1120	Burglary	Device Number
19	Fire Alarm	FA	1110	Fire	Device Number
20	Edit User Code	JV	1462	Service – Maintenance	User Number
21	Delete User Code	JX	3462	Service – Maintenance	User Number
22	Duress	HA	1121	Burglary	N.A.

ID	Event Name	SIA	CID Code	Event Group	Address Field
23	Bell Cancel	BC	1521	Burglary	User Number
24	Battery Low	YT	1302	Power Outage	Device Number
25	Battery Restore	YR	3302	Power Outage	Device Number
26	Battery Low	XT	1384	Power Outage	Device Number
27	Battery Restore	XR	3384	Power Outage	Device Number
28	AC Loss	AT	1301	Power Outage	Device Number
29	AC Restore	AR	3301	Power Outage	Device Number
30	Tamper	TA	1137	Burglary	Device Number
31	Tamper Restore	TR	3137	Burglary	Device Number
32	Communication Trouble	YC	1350	Peripherals Notification	Device Number
33	Communication Restore	YK	3350	Peripherals Notification	Device Number
34	Media Loss	LT	1351	Peripherals Notification	Device Number
35	Media Restore	LR	3351	Peripherals Notification	Device Number
36	Device Trouble	ET	1330	Peripherals Notification	Device Number
37	Device Trouble Restore	ER	3330	Peripherals Notification	Device Number
38	FM Jamming	XQ	1344	RF Jamming	Device Number
39	FM Jamming Restore	XH	3344	RF Jamming	NA
40	Programming Start	LB	1627	Service – Maintenance	N.A.
41	Programming End	LX	1628	Service – Maintenance	N.A.
42	Remote Programming Start	RB	1412	Service – Maintenance	N.A.
43	Remote Programming End	RS	3412	Service – Maintenance	N.A.
44	Periodic Test	RP	1602	Always Report	N.A.
45	Walk Test	TS	1607	Service – Maintenance	User Number

ID	Event Name	SIA	CID Code	Event Group	Address Field
46	End Walk Test	TE	3607	Service – Maintenance	NA
47	Set Time	JT	1625	Service – Maintenance	User Number
48	Set Date	JD	1625	Service – Maintenance	User Number
49	Out of synchronization	UT	1341	Do Not Report	Device Number
50	Resynchronization	UR	3341	Do Not Report	Device Number
51	CP out of synchronization	UT	1341	Peripherals Notification	Device Number
52	CP resynchronization	UR	3341	Peripherals Notification	Device Number
53	Supervision Loss	US	1381	Peripherals Notification	Device Number
54	Supervision Restore	UR	3381	Peripherals Notification	Device Number
56	Clear Log	LB	1621	Service – Maintenance	User Number
57	Stop Communication	OC	1350	Do Not Report	User Number
58	Listen In Start	LF	1606	Service – Maintenance	N.A.
59	Listen In End	LE	3606	Service – Maintenance	N.A.
60	WDT Reset	RR	1305	Service – Maintenance	Task
61	Power Up Reset	RR	3301	Power Outage	Device Number
62	Net Disconnect	RA	1350	Service – Maintenance	Device Number
63	Init Start	YD	1551	Service – Maintenance	Device Number
64	Init End	YE	3551	Service – Maintenance	Device Number
65	Message Queue Full	JO	1624	Service – Maintenance	Device Number
66	Message Queue Restore	JL	3621	Service – Maintenance	Device Number

ID	Event Name	SIA	CID Code	Event Group	Address Field
67	Message Queue Disc.	YO	1102	Service – Maintenance	Device Number
68	24 HR-X Alarm	TT	1370	Burglary	Device Number
69	24 HR-X Restore	TR	3370	Burglary	Device Number
70	Open After Alarm	OR	1458	Burglary	User Number
71	GSM Signal Level	YY	1605	Peripherals Notification	Signal Level (0-9)
72	No Arm Period Expire	CD	1654	Service – Maintenance	N.A.
73	Trouble Restore	BJ	3380	Peripherals Notification	Device Number
74	Water Alarm	WA	1154	Burglary	Device Number
75	Water Restore	WH	3154	Burglary	Device Number
76	Gas Alarm	GA	1151	Fire	Device Number
77	Gas Restore	GH	3151	Fire	Device Number
78	Environmental Alarm	UA	1150	Burglary	Device Number
79	Environmental Restore	UH	3150	Burglary	User Number
80	No Motion Alarm	NA	1102	Medical – SOS	Device Number
81	Manual Test	RX	3601	Burglary	User Number
82	Recent Closing	CR	1459	Burglary	User Number
83	Exit Alarm	EA	1454	Burglary	User Number
84	Exit Error	EE	1457	Burglary	User Number
85	Alarm Canceled	OC	1406	Burglary	User Number
86	Report Aborted	YO	1466	Do Not Report	User Number
87	Swinger Trouble	BD	1377	Service – Maintenance	Device Number
88	Cross Zoning Verification	BG	1378	Service – Maintenance	Device Number
89	Daylight Change	YO	0000	Do Not Report	NA
90	RF Comm Trouble	XQ	1353	Service – Maintenance	Device Number
91	RF Comm Restore	XH	3353	Service – Maintenance	Device Number
92	System Bell Fault	YA	1321	Service – Maintenance	Device Number

ID	Event Name	SIA	CID Code	Event Group	Address Field
93	System Bell Restore	YH	3321	Service – Maintenance	Device Number
94	Web User Access Start	RB	1412	Service – Maintenance	User Number
95	Web User Access End	RS	3412	Service – Maintenance	User Number
96	No XML Proxy Connection	NC	1350	Do Not Report	NA
97	No XML Proxy Connection Restore	NR	3350	Do Not Report	NA
98	System Radio Jamming	XQ	1344	RF Jamming	Device Number
99	External Battery Low	YT	1302	Service – Maintenance	Device Number
100	External Battery Restore	YR	3302	Service – Maintenance	Device Number
101	DHCP Fail	LT	1351	Peripherals Notification	NA
102	DHCP Restore	LR	3351	Peripherals Notification	NA
103	High Temperature	KA	1158	Burglary	Device Number
104	High Temperature Restore	KH	3158	Burglary	Device Number
105	Low Temperature	ZA	1159	Burglary	Device Number
106	Low Temperature Restore	ZH	3159	Burglary	Device Number
107	Partition 1 Armed	CG	3400	Arm/Disarm	User Number, Address Number
108	Partition 2 Armed	OG	3400	Arm/Disarm	User Number, Address Number
109	Partition 1 Disarmed	CG	1400	Arm/Disarm	User Number, Address Number
110	Partition 2 Disarmed	OG	1400	Arm/Disarm	User Number, Address Number

ID	Event Name	SIA	CID Code	Event Group	Address Field
111	Local Snapshot	XX	1400	Do Not Report	User Number, Address Number
112	SMS Snapshot	XX	1400	Do Not Report	User Number, Address Number
113	WEB Snapshot	XX	1400	Do Not Report	User Number, Address Number
114	RP User Snapshot	XX	1400	Do Not Report	User Number, Address Number
115	Sensor Snapshot	TW	1139	Burglary	Device Number
116	RF Device WDT Reset	RR	1305	Do Not Report	User Number, Address Number
117	Crash and Smash	UZ	1777	Burglary	Device Number
118	Group A Arm	CG	3456	Arm/Disarm	User Number, Address Number
119	Group B Arm	CG	3456	Arm/Disarm	User Number, Address Number
120	Group C Arm	CG	3456	Arm/Disarm	User Number, Address Number
121	Group D Arm	CG	3456	Arm/Disarm	User Number, Address Number
122	No Activity Alarm	NA	1102	Medical - SOS	Device Number
123	No Activity Restore	NS	3102	Medical – SOS	Device Number
124	SIM Card Will Expire	YO	0000	Do Not Report	Device Number
125	Auto Arm Fail	CI	1455	Arm/Disarm	User Number, Address Number
126	Burglary Verified	BV	1139	Burglary	Device Number

RTTE Compliance Statement:

Hereby, RISCO Group declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. For the CE Declaration of Conformity please refer to our website: www.riscogroup.com.

Standard Limited Product Warranty

RISCO Ltd., its subsidiaries and affiliates ("**Risco**") guarantee Risco's hardware products to be free from defects in materials and workmanship when used and stored under normal conditions and in accordance with the instructions for use supplied by Risco, for a period of (i) 24 months from the date of connection to the Risco Cloud (for cloud connected products) or (ii) 24 months from production (for other products which are non-cloud connected), as the case may be (each, the "**Product Warranty Period**" respectively).

Contact with customers only. This Product Warranty is solely for the benefit of the customer who purchased the product directly from Risco, or from any authorized distributor of Risco. Nothing in this Warranty obligates Risco to accept product returns directly from end users that purchased the products for their own use from Risco's customer or from any installer of Risco, or otherwise provide warranty or other services to any such end user. Risco customer shall handle all interactions with its end users in connection with the Warranty, inter alia regarding the Warranty. Risco's customer shall make no warranties, representations, guarantees or statements to its customers or other third parties that suggest that Risco has any warranty or service obligation to, or any contractual privy with, any recipient of a product.

Return Material Authorization. In the event that a material defect in a product shall be discovered and reported during the Product Warranty Period, Risco shall, at its option, and at customer's expense, either: (i) accept return of the defective Product and repair or have repaired the defective Product, or (ii) accept return of the defective Product and provide a replacement product to the customer. The customer must obtain a Return Material Authorization ("**RMA**") number from Risco prior to returning any Product to Risco. The returned product must be accompanied with a detailed description of the defect discovered ("**Defect Description**") and must otherwise follow Risco's then-current RMA procedure in connection with any such return. If Risco determines in its reasonable discretion that any Product returned by customer conforms to the applicable warranty ("**Non-Defective Products**"), Risco will notify the customer of such determination and will return the applicable Product to customer at customer's expense. In addition, Risco may propose and assess customer a charge for testing and examination of Non-Defective Products.

Entire Liability. The repair or replacement of products in accordance with this warranty shall be Risco's entire liability and customer's sole and exclusive remedy in case a material defect in a product shall be discovered and reported as required herein. Risco's obligation and the Warranty are contingent upon the full payment by customer for such Product and upon a proven weekly testing and examination of the product functionality.

Limitations. The Product Warranty is the only warranty made by Risco with respect to the Products. The warranty is not transferable to any third party. To the maximum extent permitted by applicable law, the Product Warranty does not apply and will be void if: (i) the conditions set forth above are not met (including, but not limited to, full payment by customer for the product and a proven weekly testing and examination of the product functionality); (ii) if the Products or any part or component thereof: (a) have been subjected to improper operation or installation; (b) have been subject to neglect, abuse, willful damage, abnormal working conditions, failure to follow Risco's instructions (whether oral or in writing); (c) have been misused, altered, modified or repaired without Risco's written approval or combined with, or installed on products, or equipment of the customer or of any third party; (d) have been damaged by any factor beyond Risco's reasonable control such as, but not limited to, power failure, electric power surges, or unsuitable third party components and the interaction of software therewith or (e) any delay or other failure in performance of the product

attributable to any means of communications, provided by any third party service provider (including, but not limited to) GSM interruptions, lack of or internet outage and/or telephony failure.
BATTERIES ARE EXPLICITLY EXCLUDED FROM THE WARRANTY AND RISCO SHALL NOT BE HELD RESPONSIBLE OR LIABLE IN RELATION THERETO, AND THE ONLY WARRANTY APPLICABLE THERETO, IF ANY, IS THE BATTERY MANUFACTURER'S WARRANTY.
Risco makes no other warranty, expressed or implied, and makes no warranty of merchantability or of fitness for any particular purpose. For the sake of good order and avoidance of any doubt:
DISCLAIMER. EXCEPT FOR THE WARRANTIES SET FORTH HEREIN, RISCO AND ITS LICENSORS HEREBY DISCLAIM ALL EXPRESS, IMPLIED OR STATUTORY, REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS WITH REGARD TO THE PRODUCTS, INCLUDING BUT NOT LIMITED TO ANY REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND LOSS OF DATA. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, RISCO AND ITS LICENSORS DO NOT REPRESENT OR WARRANT THAT: (I) THE OPERATION OR USE OF THE PRODUCT WILL BE TIMELY, SECURE, UNINTERRUPTED OR ERROR-FREE; (ii) THAT ANY FILES, CONTENT OR INFORMATION OF ANY KIND THAT MAY BE ACCESSED THROUGH THE PRODUCT BY CUSTOMER OR END USER SHALL REMAIN SECURED OR NON DAMAGED. CUSTOMER ACKNOWLEDGES THAT NEITHER RISCO NOR ITS LICENSORS CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, GSM OR OTHER MEANS OF COMMUNICATIONS AND THAT RISCO'S PRODUCTS, MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH MEANS OF COMMUNICATIONS.
RISCO IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS. RISCO WARRANTS THAT ITS PRODUCTS DO NOT, TO THE BEST OF ITS KNOWLEDGE, INFRINGE UPON ANY PATENT, COPYRIGHT, TRADEMARK, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHT
IN ANY EVENT RISCO SHALL NOT BE LIABLE FOR ANY AMOUNTS REPRESENTING LOST REVENUES OR PROFITS, PUNITIVE DAMAGES, OR FOR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, EVEN IF THEY WERE FORESEEABLE OR RISCO HAS BEEN INFORMED OF THEIR POTENTIAL.
Risco does not install or integrate the product in the end user security system and is therefore not responsible for and cannot guarantee the performance of the end user security system which uses the product.
Risco does not guarantee 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.
Customer understands that a correctly installed and maintained alarm may only reduce the risk of burglary, robbery or fire without warning, but is not an assurance or a guarantee that such an event will not occur or that there will be no personal injury or property loss as a result thereof.
Consequently Risco shall have no liability for any personal injury, property damage or loss based on a claim that the product fails to give warning.
No employee or representative of Risco is authorized to change this warranty in any way or grant any other warranty.

Contacting RISCO Group

RISCO Group is committed to customer service and product support. You can contact us through our website (www.riscogroup.com) or at the following telephone and fax numbers:

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

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

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

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

Belgium (Benelux)
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
support-cn@riscogroup.com

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

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

Australia
Tel: +1800-991-542
support-au@riscogroup.com