Ocularis Administrator User Manual

Version 5.8

October, 2019

PROPRIETARY AND CONFIDENTIAL INFORMATION

All information contained herein is confidential, proprietary and the exclusive property of Qognify Ltd and its affiliates (“Qognify”). This document and any parts thereof must not be reproduced, copied, disclosed or distributed without Qognify's written approval and any content or information hereof shall not be used for any unauthorized purpose. The software described herein and any other feature or tools are provided "AS IS" and without any warranty or guarantee of any kind.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, QOGNIFY HEREBY DISCLAIMS ALL OTHER WARRANTIES OF ANY KIND WITH RESPECT TO THE SOFTWARE DESCRIBED HEREIN EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE

All contents of this document are: Copyright © 2019 Qognify Ltd. All rights reserved.

Revision History

Revision	Purpose for Change	Author	Date
00	GA	D. Jecker	Oct 2019
01	Title	D. Jecker	Oct 2019

Contents

1 About This Guide 11
1.1 Related Documentation 11
2 Introduction 12
3 Overview 13
4 Prerequisites 1
5 Ocularis Administrator 2
5.1 Ocularis Administrator Login 2
5.2 Schedules for Logins 3
5.3 Change Password Upon First Time Login 3
5.4 Dual Authorization 4
5.5 Ocularis Administrator Log Off 4
6 The Ocularis Administrator Interface 6
6.1 Ocularis Administrator Tabs 6
6.2 Ocularis Administrator Process Flow 7
7 Server / Events Tab 8
7.1 Servers Pane 8
7.2 Servers Toolbar 8
7.3 Adding a Server 8
7.4 Slave Core Redundancy 11
7.5 Post Configuration Steps 11
7.6 Servers List 11
7.7 SMA Expiration Notice 19
7.8 Automatic Base Update 19
7.9 Camera Properties 21
7.10 Actions 31
7.11 Events Pane 43
7.12 Simple Event Rules 46
7.13 Event Properties 48
7.14 Composite Events 54
7.15 Generic Events 59
7.16 Device Filter / Event Filter 65
7.17 Filter Lock 67
7.18 Camera Migration Tool 68
8 Users / Privileges Tab 75
8.1 User / Privileges Toolbar 76
8.2 Working with User Groups 76
8.3 User Group Privileges 77
8.4 User Privileges 83
8.5 Device Privileges 88
8.6 Trigger Privileges 93

8.7 Video Wall Privileges 95
8.8 Weekly Schedule 98
8.9 Holiday Schedule 101
9 Views Tab 103
9.1 Resizing Panes 104
9.2 View Basics 104
9.3 View Configurations 106
9.4 Contents 107
9.5 Contents Navigation 108
9.6 View Organization 114
9.7 Creating Views 114
10 Assets Tab 142
10.2 Maps 143
10.3 Event Audio Clips 145
11 Maps Tab 148
11.1 Working with Maps 153
11.2 Linking Maps 158
12 System Status Tab 167
12.1 Event Management 168
12.2 Event Management 169
12.3 Event Configuration 169
12.4 Event Handling 171
13 Table Management Tab 172
13.1 Configure Classifications 172
13.2 Configure Tags 174
13.3 Configure Cases 174
14 Distribution Groups Tab 176
14.1 To Create a Distribution Group 176
14.2 Distribution Groups 177
15 Logs Tab 187
15.1 What Data is Audited? 187
15.2 Viewing the Audit Log 187
15.3 Exporting the Audit Log 192
16 Settings Tab 196
16.1 Audit Log Settings 196
16.2 Update Settings 197
17 About Tab 200
17.1 About Ocularis 200
17.2 Base Licenses 200
17.3 Recorder Licenses 202
17.4 Help 203
18 OpenSight 204
18.1 What is Ocularis OpenSight? 204
18.2 OpenSight Entities 205

18.3 Configuring OpenSight 207

List of Tables

Table 1-1: Related Documents 11

List of Figures

Figure 1 Ocularis Administrator Login Screen 2
Figure 2 Unauthorized Login Attempt by a Group Administrator 3
Figure 3 Login Approval Needed 4
Figure 4 Log Off or Shut Down 5
Figure 5 Ocularis Administrator Interface 6
Figure 6 Servers / Events Tab 8
Figure 7 Servers Pane Toolbar 8
Figure 8 Add Server 9
Figure 9 Added Recorders 12
Figure 10 Missing or Outdated Recorder Proxy 13
Figure 11 Recorder Proxy Offline 14
Figure 12 Right-click to Refresh the server 15
Figure 13 Edit Server Sample 16
Figure 14 Camera Licenses 17
Figure 15 Multi-Channel Devices 18
Figure 16 Recorder refresh is pending 20
Figure 17 Camera Properties 21
Figure 18 Calibrate a Sentry360 Camera 23
Figure 19 Sentry360 24
Figure 20 Right-click to draw privacy mask 27
Figure 21 Configuring Multiple Privacy Masks 27
Figure 22 Privacy Masks when viewed in Ocularis Client 28
Figure 23 Critical Camera Failover Editor 29
Figure 24 Drag and Drop to create failover cameras list 29
Figure 25 Drag and drop cameras to reorder the failover list 30
Figure 26 Alert Actions 31
Figure 27 Configure Camera Move to Preset 32
Figure 28 Preset Move Actions 33
Figure 29 Configure the Email Server 35
Figure 30 Configure a new email 36
Figure 31 Add New HTTP Request 38
Figure 32 Add New TCP/UDP Data Packet 41
Figure 33 Batch Handle Events 45
Figure 34 Drag & Drop to Associate Events 47
Figure 35 Associated Events 48
Figure 36 Event Rule Properties: Priority 50
Figure 37 Priorities Color Coding sample in Ocularis Administrator 50
Figure 38 Event Rule Properties: Audio Samples 52
Figure 39 Add Composite Event Folder 55
Figure 40 Rename Composite Event Folder 55
Figure 41 Configure a Composite Event: Rule Details Tab 56
Figure 42 Composite Rule Example 58
Figure 43 Add a Generic Event Connection 60

Figure 44 Click [add rule…] to configure the generic event connection 61
Figure 45 Creating a Generic Event Rule 61
Figure 46 Patters for Generic Events 63
Figure 47 Using Multiple Patterns 63
Figure 48 Testing Generic Events 64
Figure 49 Selecting a Pattern to Test 65
Figure 50 Generic event test data sent confirmation 65
Figure 51 Device and Event Filters 66
Figure 52 Filter for 'lab' 66
Figure 53 Event Filter for 'fire' 67
Figure 54 Filter for 'Lab' cameras and events 68
Figure 55 Sample Cameras from an RC-C Recorder 69
Figure 56 Added v5 recorder 70
Figure 57 Remap Cameras 71
Figure 58 Drag and drop individual cameras 72
Figure 59 Drag and drop server to server 72
Figure 60 Remove a single mapping 73
Figure 61 Remove All Mappings for a Server 73
Figure 62 Delete Server warning message 74
Figure 63 Users / Privileges Tab 75
Figure 64 Users / Privileges Toolbar 76
Figure 65 User Group Privileges 78
Figure 66 Modify a User Group Privilege 81
Figure 67 Configure Branches 82
Figure 68 Assign a Branch 82
Figure 69 Add New User 84
Figure 70 Duplicate Username 85
Figure 71 New User Account 86
Figure 72 Modify User Privilege 87
Figure 73 All Cameras Start as Unprivileged 89
Figure 74 Camera Privilege Group Settings 90
Figure 75 Drag and Drop to Assign Cameras 92
Figure 76 Right-click to Assign Cameras 93
Figure 77 Trigger Privileges 94
Figure 78 Check box for assigned video wall 95
Figure 79 Weekly Schedule 98
Figure 80 Click and Drag from left to right 100
Figure 81 Time Range Pop-Up 100
Figure 82 Holiday Schedule 101
Figure 83 Select Date 101
Figure 84 Add a Holiday 102
Figure 85 Adjust Access Hours on a Holiday 102
Figure 86 Views Tab 103
Figure 87 Resizing a Pane 104
Figure 88 Sample views via Ocularis Client 105
Figure 89 Available View Layouts 106
Figure 90 Built-in Tab of Contents List 109
Figure 91 Cameras Tab 109
Figure 92 All Cameras for the selected View Group 110
Figure 93 Expand Camera Preview Icon 111
Figure 94 Camera Preview Thumbnail 111
Figure 95 Camera Search box 112
Figure 96 Click store to Save Search Filter 113
Figure 97 Example of stored camera filter 'engin' 113
Figure 98 Creating a New View for a Single User Group 116

Figure 99 Shared Views 117
Figure 100 Example: Drag a Hotspot to a View Pane 118
Figure 101 Example: Drag a Camera to a View Pane 118
Figure 102 Select Multiple Cameras 119
Figure 103 Populate View in One Easy Step 120
Figure 104 Click Clear View to remove pane contents 121
Figure 105 Sharing Views 122
Figure 106 Sharing View Groups 123
Figure 107 Padlock indicates view may not be modified in this selection 124
Figure 108 Click on the pane to modify parameters 125
Figure 109 Set the default stream 128
Figure 110 Use the 'aux' button to select a live stream 128
Figure 111 Adding Camera Streams 129
Figure 112 Configuring a Camera Stream 130
Figure 113 Video Classifications 131
Figure 114 Carousel Edit icon 132
Figure 115 Carousel Editor 132
Figure 116 Creating a carousel list 133
Figure 117 Drag a Folder to create a carousel 134
Figure 118 Reorder a Camera in a Carousel 134
Figure 119 Change the Default Dwell Time 135
Figure 120 A configured carousel in the Views Tab 136
Figure 121 Configuring Hot Spot Output 138
Figure 122 Configuring a Push Video Pane 139
Figure 123 Configuring a Web Page Pane 140
Figure 124 Configuring a Blank Screen Pane 141
Figure 125 Assets Tab 142
Figure 126 Sample Coordinates for Pearl River, NY 144
Figure 127 Setting the default Audio Asset 146
Figure 128 Maps Tab 148
Figure 129 Selecting a Map for a single group (Private) 149
Figure 130 Expand the Available Maps folder to choose a map 149
Figure 131 Added Map to Operators Group 150
Figure 132 Used Maps in Assets Tab shown with Green Checkmark 151
Figure 133 Select Default Alert Map 152
Figure 134 Default Alert Map 152
Figure 135 Drag & Drop a camera onto the map 154
Figure 136 Remove a Camera 154
Figure 137 Expanded Views List 155
Figure 138 Change font size with slider 156
Figure 139 Resize a camera icon 156
Figure 140 Rotate a camera icon 157
Figure 141 Adjustable sliders 158
Figure 142 Draw Link Area 160
Figure 143 Link Area unnamed and unassigned 160
Figure 144 Pin Name Link 161
Figure 145 Link area inherits pin name 161
Figure 146 Drag & drop color to modify link area 162
Figure 147 Drag and drop Map Pin 163
Figure 148 Map with three floating map shortcuts 163
Figure 149 Add from Shared Maps folder to share a map 165
Figure 150 Padlock icon indicates a shared map 165
Figure 151 System Status Tab 167
Figure 152 Table Management Tab 172
Figure 153 Add a new Classification 173

Figure 154 Distribution Group Tab 177
Figure 155 Distribution Group parameters 178
Figure 156 Assigning Events to a Distribution Group 179
Figure 157 Setting a Weekly Schedule 182
Figure 158 Time Range Pop-Up 183
Figure 159 Clear a Weekly Schedule 183
Figure 160 Cleared Schedule for Monday 184
Figure 161 Reset a Weekly Schedule 184
Figure 162 Reset Schedule 184
Figure 163 Holiday Schedules 185
Figure 164 Setting a Time Range during a Holiday 186
Figure 165 Delete a Holiday icon 186
Figure 166 Logs Tab 188
Figure 167 Sample Results (unfiltered) 189
Figure 168 Sample Results Filtered by Action Type 189
Figure 169 Tool tip 191
Figure 170 Resize a column 191
Figure 171 Reorder Columns 191
Figure 172 Sort any column 191
Figure 173 Right-click Session ID 192
Figure 174 Audit Log Export pop-up 193
Figure 175 Cancel an Export 194
Figure 176Sample Exported Log as viewed in Excel 195
Figure 177 Configure the Audit Log 196
Figure 178 Version Check for Ocularis Client 198
Figure 179 Upgrade Downloaded Message 198
Figure 180 Allow Ocularis Clients to Self-Update 199
Figure 181 Version Information on the About Tab 200
Figure 182 About Tab License Information 201
Figure 183 About Tab Expanded Rows 201
Figure 184 Recorder Licenses 202
Figure 185 OpenSight Layout (Sample) 205
Figure 186 Ocularis Recorder Recorder Proxy 208
Figure 187 Configure Base Settings 208

1 About This Guide

This document describes how to administer and configure Ocularis.

1.1 Related Documentation

Related documents are listed below.

Table 1-1: Related Documents

Document Name	Version	File Type	Date
Ocularis 5.8 Release Notes	5.8	PDF	October 2019
Ocularis Installation & Licensing Guide	5.8	PDF	October 2019
Ocularis Client User Manual	5.8	PDF	October 2019
Ocularis Viewer User Manual	5.8	PDF	October 2019
Add-on Documentation			

2 Introduction

The **Ocularis Platform** consists of the following components:

- **Ocularis Base** – server software application which regulates and manages the flow of data between video client users, recording servers, video wall management, event management and alerting.
- **Ocularis Administrator** - The front end software application used to configure and manage Ocularis Base.
- **Ocularis Client** – The award winning video client application used to view and monitor surveillance video.
- **Ocularis Recording Component** – Camera management and recording software. Each model of Ocularis contains a corresponding recording component application.
- **Ocularis Recorder Proxy** – This component manages many aspects of Ocularis including: transmitting events from recorders to Ocularis Base, managing muliple live streams from cameras, handling PTZ presets, optimizing the best stream to use with Ocularis 5 Web or Mobile and much more. It is a very important component and should be installed on every Ocularis system.
- **Ocularis Media Server**– This component allows for the viewing of Ocularis video using a web browser (Ocularis 5 Web) or mobile device (Ocularis 5 Mobile)
- **Optional Add-On Applications** – these currently include:
  - Remote VideoWall
  - Ocularis OpenSight™
  - Various third party integrations

For all Ocularis models, including the RecOn5 NVR and RecOn5 Server, configuration of Ocularis is performed using the Ocularis Administrator application.

3 Overview

Ocularis is a distributed, video-centric, PSIM (Physical Security Information Management) software platform, which offers central event, user rights, video distribution and system management.

Ocularis supports:

- The ability for the user to view, manage and record video from an unlimited number of IP and non-IP video surveillance cameras at multiple sites.
- The management of short- and long-term video storage, and combine video with non-video alerts, resulting in automatic video delivery to subscribers of interest.
- The utilization of off-the-shelf hardware, and facilitates the integration of new technologies, thus combining the detection and distribution of video events with data and alerts received from a host of physical security and transaction systems.
- The use of separate or common networks, VLANS or switches for connecting cameras to the recording servers and video clients. This provides physical network separation between the camera and servers/clients.
- The use of VMware to run recording servers and client applications on virtual computers, servers, and networks.

Ocularis consists of the following software components:

- Ocularis Base – This component provides for:
    - system-wide management
    - user access
    - shared event management
    - alarm and event correlation
    - video access and distribution

  Ocularis Base regulates and manages the flow of data between video client users, connecting recording servers and integrated alerting application using an SQL database. This allows creating composite events from multiple detection systems; sharing resources between video client users; shared bookmarking and event handling among multiple users at multiple sites; and management of all user authorization data. The front end application used to manage Ocularis Base is the *Ocularis Administrator*.

- Ocularis Recorder Software – This component provides for video recording, camera management, and archiving configuration.

- Ocularis Client – This award winning component is the user interface for accessing video, managing alerts and shared event handling, and observing Video Wall environments.

- Ocularis Media Server – This component allows users to access Ocularis video with a web browser (via *Ocularis 5 Web*) or mobile device (via *Ocularis 5 Mobile*).
- Add-Ons and Integrated Applications – includes Remote Video Wall and Ocularis OpenSight.

4 Prerequisites

Prior to using the *Ocularis Administrator* application, the following steps should be completed:

1. *Ocularis Base* server software should be installed.
2. The *Ocularis Base* license should be activated.
3. *Ocularis Administrator* software application filesare automatically installed on the Base computer. You may also want to install this application on additional computers on the network.
4. Ocularis Recorder(s) should be installed and configured with cameras.

See the *Ocularis Installation & Licensing Guide* for instructions on all steps listed above.

5 Ocularis Administrator

The *Ocularis Administrator* is the software application used for configuring *Ocularis Base*. This includes the management of recorders and the configuration of users, groups, cameras, maps, events, and video walls.

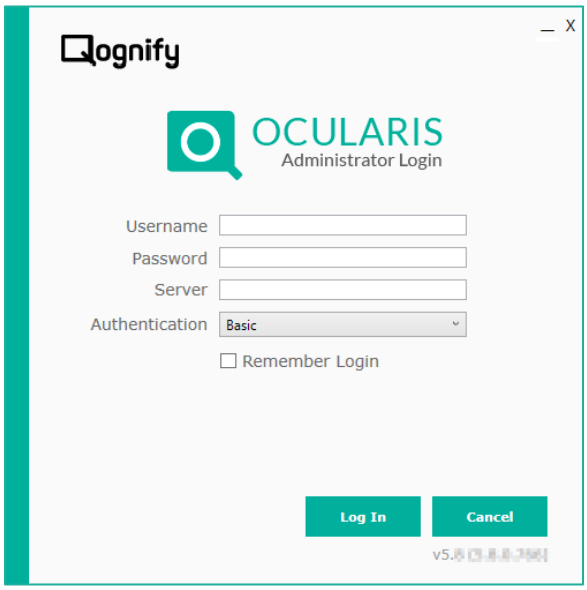
The *Ocularis Administrator* application is primarily used by system administrators. This application may be installed on any machine with connectivity to the Ocularis Base computer. It is also automatically installed on the Ocularis Base computer. It may be installed on more than one computer.

5.1 Ocularis Administrator Login

- Launch *Ocularis Administrator*:
  - from the desktop icon

  - or from the Windows menu ***Start*** ➔ ***All Programs*** ➔ ***OnSSI*** ➔ ***Ocularis Administrator***

Figure 1 Ocularis Administrator Login Screen



- Fill out the dialog based on the following:

Username	Enter the username for an account created with *Ocularis Administrator*. For first time access, enter the username: **admin**
Password	Enter the corresponding password for the user name entered. For first time access, enter the password: **admin** The first time you login after a fresh install, you will be asked to change this password. See *Change Password Upon First Time Login* below.

Server	Enter the IP address where the Ocularis Base server software is installed. Using 'localhost' is acceptable if Ocularis Base is on the current machine. If the IIS port is anything other than 80, add ":port#" to the IP address.
Authentication	Of the choices **[Current User]**, **Windows** or **Basic**, select **Basic** for first time use.
Remember Login	Click this checkbox to have the application remember your login credentials for subsequent logins.
Version Number	The *Ocularis Administrator* software version number is located in the lower right portion of the Login screen.

- When complete, click the **Log In** button.

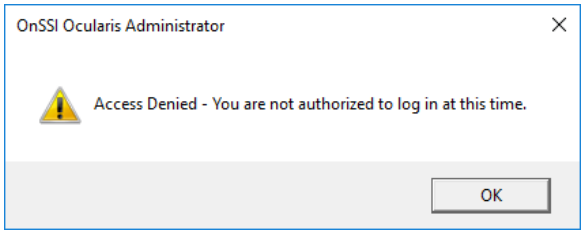
> ***Tip***: *We recommend that you change the password for the Admin account immediately for security purposes.*

Note: *If you receive the following error message when logging in: "*An unsecured or incorrectly secured fault was received from the other party. See the inner FaultException for the fault code and detail*", check that the date and time on the PC with Ocularis Administrator is synchronized with the date and time on the PC with Ocularis Base.*

5.2 Schedules for Logins

Administrators can control when users can login to Ocularis Client, Ocularis Web, Ocularis Mobile and even Ocularis Administrator. For Ocularis Administrator, all members of the 'Administrators' user group have unlimited access to the application. For Group Administrators, access to Ocularis Administrator follows the same schedule set for client applications. If a Group Administrator attempts to login to Ocularis Administrator during an unapproved time, they will see this message:

Figure 2 Unauthorized Login Attempt by a Group Administrator



5.3 Change Password Upon First Time Login

After you install Ocularis the first time, you will be prompted to change the **admin** password.

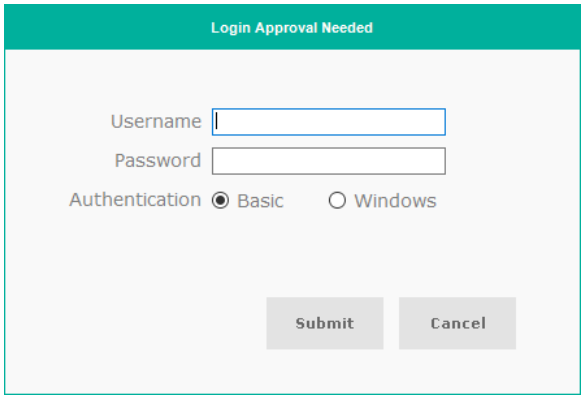
You may use any characters, numbers, symbols, upper or lowercase. You can click the 'Show Password' checkbox to see what you type. You will receive feedback on the strength of the password (weak, moderate or strong) and confirmation when both passwords match.

For upgrades, you will get this prompt if your **admin** account password is still set to 'admin'. If you've already changed it to something else, you will not be prompted.

5.4 Dual Authorization

In certain cases, system administrators may not want certain users to be able to have unfettered access to Ocularis video. They may, however, want to allow access on a case-by-case basis. In this instance, the system administrator can set the user's account to 'Deny' the privilege of 'Login to Ocularis Client' from the **Users / Privileges** Tab. When the user needs to access video, their login attempt will yield:

Figure 3 Login Approval Needed

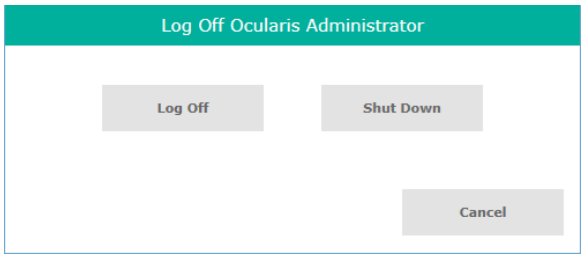


Another user with the privilege 'Login to Ocularis Client' set to 'Allow' must enter their own account credentials in order for the original user to gain access. This is called the "Four Eyes Principle". Record of the approval login will be registered in the Audit Log. The approving user must either be an administrator (i.e. a member of the Administrators group) or a member of the same user group as the original person logging in. Someone who is not an administrator or not from the same user group may not approve the login for a member of a different user group. For more information see ***Group Privileges Defined*** on page 79.

5.5 Ocularis Administrator Log Off

When you close the Ocularis Administrator application using the Windows Close button (the 'X' in the upper right corner), you have the option, similar to Ocularis Client, to Log Off or Shut Down.

Figure 4 Log Off or Shut Down

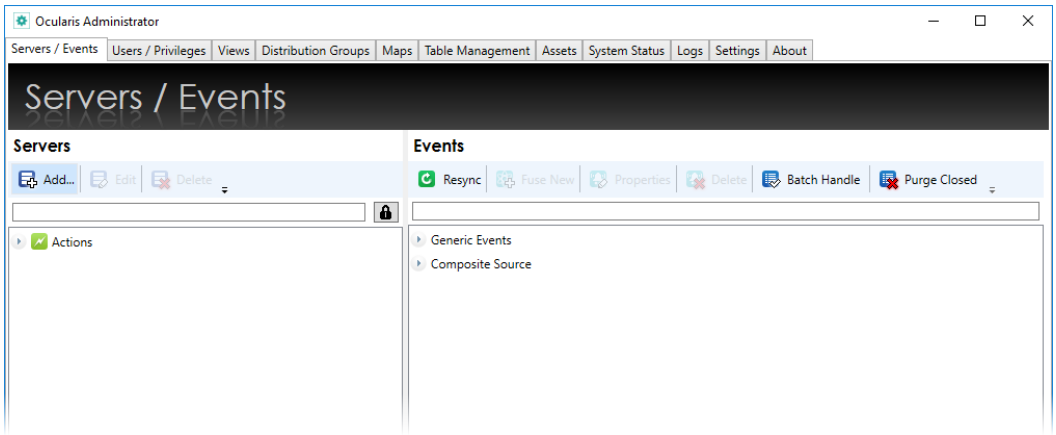


- **Log Off** - this option will log the current user out of the system and return you to the Ocularis Administrator Login screen. It allows you to either log into the same Base as a different user or to log into an entirely different Base.
- **Shut Down** – this option will log the current user off and close the application. You will need re re-launch in order to see the login page.
- **Cancel** – this option closes the dialog and returns you to the Ocularis Administrator application.

6 The Ocularis Administrator Interface

When you launch *Ocularis Administrator*, the resulting screen is a window comprised of a series of tabs.

Figure 5 Ocularis Administrator Interface



Each tab serves to provide the system administrator with the ability to configure the various aspects of the video management system.

6.1 Ocularis Administrator Tabs

- Server / Events Tab
- **Users / Privileges Tab**
- **Views Tab**
- **Distribution Groups Tab**
- **Maps Tab**
- **Table Management Tab**
- **Assets Tab**
- **System Status Tab**
- **Logs Tab**
- **Settings Tab**
- **About Tab**

6.2 Ocularis Administrator Process Flow

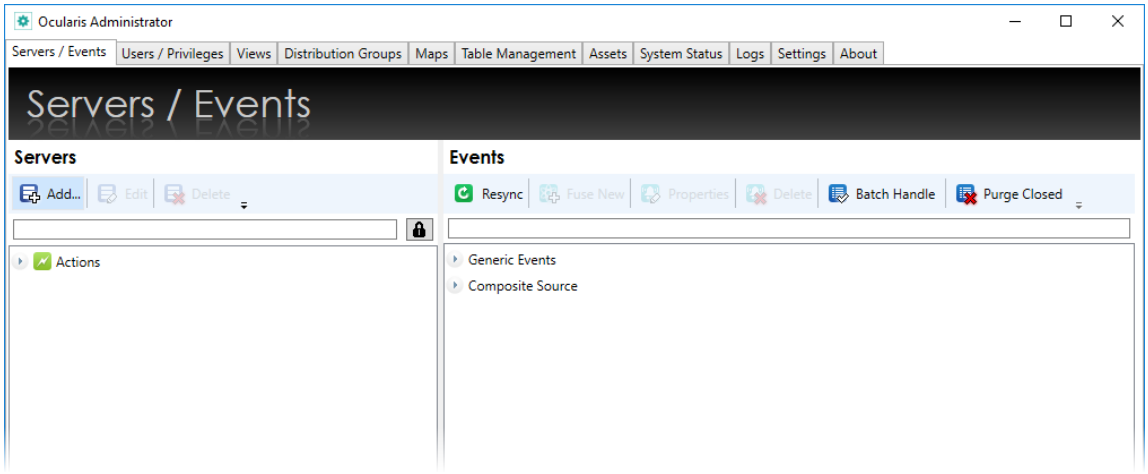
A typical process flow for administrators to use when first configuring the system with *Ocularis Administrator* is as follows:

1. Import system recorders using the Server / Events Tab.
2. Create users and groups and assign device privileges in the **Users / Privileges Tab**.
3. Create views for the user groups in the **Views Tab**.
4. Enable and configure the Audit Log in the **Settings Tab**.
5. Determine if you want Ocularis Client users to receive a version check in the **Settings Tab**.
6. Import maps, icons and sound files in the **Assets Tab**.
7. Configure maps with cameras and views for use in video walls in the **Maps Tab**.
8. Create video wall names and assign video wall privileges in the **Users / Privileges Tab**
9. Identify events and cameras you would like to monitor in the Server / Events Tab.
10. Identify the alert distribution and actions for system configured events in the **Distribution Groups Tab**.
11. Configure tags, classifications and cases in the **Table Management Tab**. Tags, classifications and cases are used when handling events and saving bookmarks.

7 Server / Events Tab

This tab is used to manage recorders, servers and events within the Ocularis environment.

Figure 6 Servers / Events Tab



The tab contains two panes: **Servers** and **Events**. Administrators identify various servers used in the system, including recording components (NVRs), in the left pane and configure events in the right pane.

7.1 Servers Pane

Configuration and information from existing recorders and servers to be used with Ocularis need to be imported into the *Ocularis Administrator*. This is done within the **Servers** pane of the **Servers / Events** Tab.

7.2 Servers Toolbar

The toolbar in the **Servers** pane of the **Servers / Events** Tab controls server related functions.

Figure 7 Servers Pane Toolbar

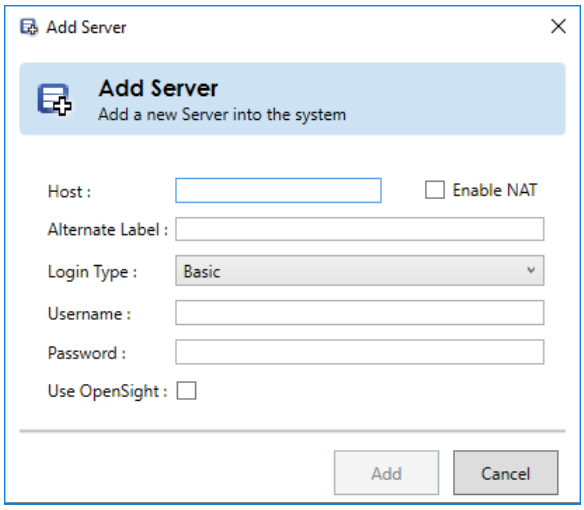
7.3 Adding a Server

To add a recording component to Ocularis Base, follow these instructions. The recorder that you may add is determined by the Ocularis SLC video channel licenses purchased. You may mix and

match new or legacy recorders in Ocularis Base for the same level recorder as the Base or lower when using PRO, ENT or ULT. For instance, if you have Ocularis Ultimate, you may add any supported NVR (provided you have purchased licenses for it). This includes any v5 recorder, v4 recorder or even NetDVMS and NetDVR. If you have Ocularis PRO Base, you may not add Enterprise or Ultimate recorders. With a RecOn5 Base, you also may not add any additional recorders.

1. In the **Servers / Events** Tab, click the **Add** button.

Figure 8 Add Server



2. In the **Host** field of the resulting pop-up window, enter the IP Address or hostname and in some cases, the port number of the server to be added to the Ocularis Base system.

    - If the port number for the recorder or camera is 80, there is no need to enter it.
    - If the port number for the Ocularis 5 recording component is set to the default value of 60000, there is no need to enter it.
    - Otherwise, use the following format:

      IP Address:Port Number

    For example on an Ocularis 5 Recorder:

    IP Address of Server: 192.168.10.111
    Port for recorder: 80
    Enter: **192.167.10.111**

Note: *For Ocularis Ultimate, Ocularis Enterprise and Ocularis Professional, enter the IP address or hostname of the Master Core Server*

For Ocularis Professional or any installation with multiple Master Cores, do this for each Master Core in the system

For a RecOn5 NVR, specify the IP address of the RecOn5 unit

For an ULT Base importing a RecOn5 recorder, specify the IP address of the RecOn5 unit AND select 'Use OpenSight'

You do NOT need to specify the default port of 60000

'localhost' is not supported

3. If NAT is used due to one or more components requiring access from outside the firewall, click the *Enable NAT* checkbox and refer to the document *How To Configure NAT with Ocularis*.
4. If you would like to change the label on the server you are adding, you may enter an **Alternate Label** next. This label appears only in the **Servers/Events** tab or in the *Remap Cameras Setup* screen. The default is to use the IP Address or Hostname followed by the recorder name. For example: 192.168.11.122 (Ocularis Enterprise Recorder).
5. Select the **Login type** from the drop-down. Choose from **Basic** or **Windows** based on an account located on the recording component that has full access rights.
6. Enter a **User name** for the corresponding user account with full administrative access rights.

Note:

For Ocularis 5, enter an account on the Master Core Server.

For legacy Ocularis LS/ES, enter an account on the Management Server.

For legacy Ocularis PS/IS/CS/NetDVMS, enter an account on the recorder.

The user name is case sensitive.

7. Enter the **Password** for the username entered. The password is case sensitive.
8. If importing an OpenSight recorder, check the *Use OpenSight* checkbox to apply OpenSight licenses. See page 204 for more information on OpenSight.
9. Click **Add**.

The recorder/server should now appear in the list.

Note: *if the server you are importing has more cameras than your Ocularis license allows, you will receive a warning message that the number of cameras exceeds the amount licensed.*

For *Editing a Server*, see page 15.

For *Deleting a Server* see page 16.

7.4 Slave Core Redundancy

This feature applies to Ocularis Ultimate and Ocularis Enterprise only.
When you add a recorder (Master Core) to Ocularis using Ocularis Administrator, the system will automatically look for a Slave Core at the root level. If found, the Slave Core will automatically be assigned as backup in the database. Then, in an instance where an Ocularis Client user logs in and the Master Core is unavailable, the user will still be able to access video via the Slave Core.
For upgrades or if you add a Slave Core to the recorder after you've already added the Master Core to the Base, manually refresh the Master Core on the **Servers / Events** tab (see *To Update a Server's Configuration* on page 14).

7.5 Post Configuration Steps

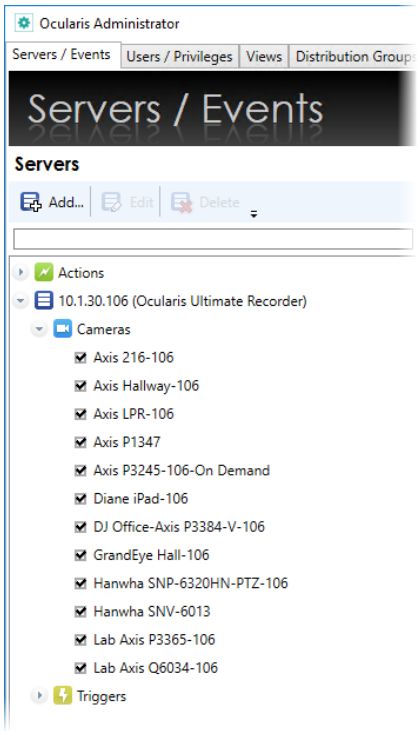
Once you've added a recorder to Ocularis Administrator, you're not quite done. There are a few minimum steps to take to use the system.

1. Assign the cameras from the recorder to applicable User Groups. Create these groups in the
   Users / Privileges Tab.
2. If your recorder has configured Triggers, privilege these to User Groups in the **Users / Privileges** Tab.
3. Create views for the User Groups in order to view the camera video in the **Views** Tab.

7.6 Servers List

As Master Cores/recording servers are added to Ocularis, the resulting **Servers** list presents these as collapsible and expandable by clicking the symbol in front of the list item. Cameras, Microphones, and sometimes Speakers, Relay, Alerts and Inputs are imported from recorders as shown in Figure 9 .

Figure 9 Added Recorders



Unless you've used an Alternate Label for the Server, the recording component is displayed by its IP address followed by the type of recording component (e.g. Ocularis Ultimate Recorder Expand the node to view the camera name and license checkbox.

> ***WARNING***:
> *The camera names listed here are those assigned in the recording component. Please note that certain special characters are not supported by Ocularis and if included in a device name, may cause erratic or non-functional behavior. We recommend you avoid all special characters in camera names and events including (but not limited to):*
> **< > & ' " \ / : * ? | [ ]**

7.6.1 Missing a Recorder Proxy

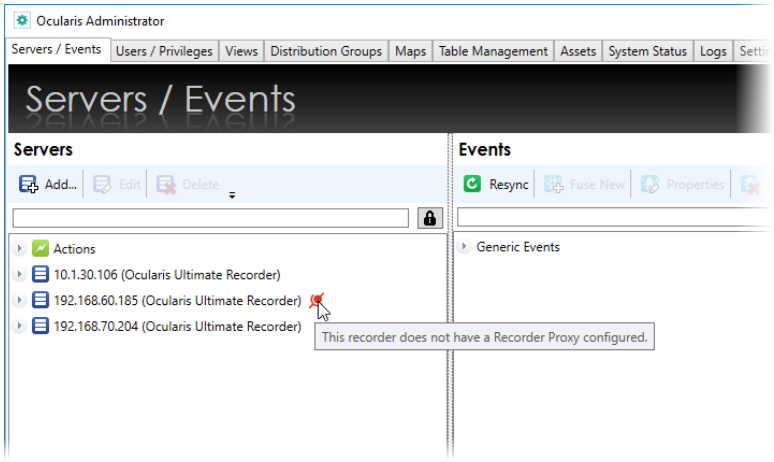
Recorder Proxy Icon

The Ocularis Recorder Proxy (formerly call the *Event Proxy*) is a required component for Ocularis to function properly. If you see an icon adjacent to a server in the list in the Servers pane of the Servers / Events Tab, and it is shown as a solid color image, it means that you have not installed and/or configured the most current version of the Recorder Proxy. You can position the mouse over the

icon to see the tool tip description: “This recorder does not have a Recorder Proxy configured.” as shown in Figure 10 below.

Once you install and configure the latest Recorder Proxy, the icon should disappear. Refer to the *Ocularis Installation & Licensing Guide* for instructions on installation.

Figure 10 Missing or Outdated Recorder Proxy



Note: *If Ocularis Administrator is open while the Recorder Proxy is installed, the indicator will not disappear until the Administrator is closed and then re-opened.*

7.6.2 Recorder Proxy Offline

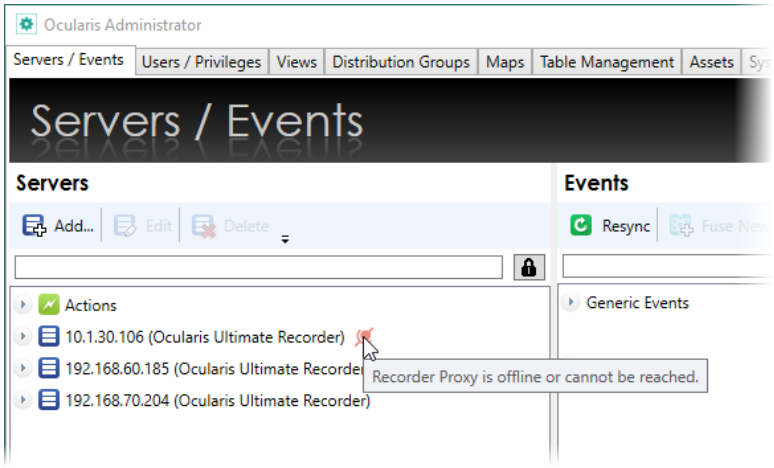
If the Ocularis Recorder Proxy is installed but the proxy service has stopped or is offline or, for some reason, the computer where the Recorder Proxy is located cannot be reached, you will see the Recorder Proxy icon adjacent to the server in the list in

Recorder Proxy Icon

the Servers pane of the Servers / Events Tab. In this case, the icon will pulse to indicate an offline status.

Position the mouse over the icon to see the tool tip description: “Recorder Proxy is offline or cannot be reached.” as shown in Figure 11 below.

Figure 11 Recorder Proxy Offline



Once the service is restarted or reconnection is established, the icon should disappear.

7.6.3 Updating Servers

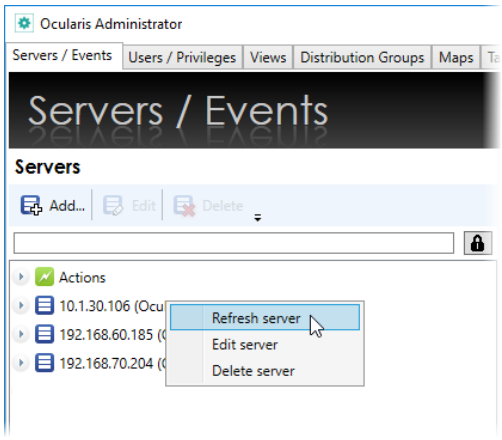
In the course of normal use, recording component properties change over time. New cameras are added, outdated cameras are removed, camera settings are changed, events are implemented, software is upgraded, etc. In order for Ocularis be aware of any new parameters configured on the recorder, the recording component (Master Core) server information should be updated periodically. When you upgrade recording component software, you should refresh the server in Ocularis Administrator.

7.6.3.1 To Update a Server’s Configuration

Follow these steps to update recording component configuration and camera list. Use this function when you add or remove cameras or modify camera settings. Also use this if you’ve changed any of the properties of the recorder’s Slave Core (ENT & ULT only). This procedure is not to be used to modify the recording component's IP Address. (See *Editing a Server* below.)

1. In the **Servers / Events** Tab, right-click the server you wish to update from the **Servers** pane.
2. In the resulting menu, select ‘Refresh server’.

Figure 12 Right-click to Refresh the server



An 'Updating' message appears as the configuration is refreshed from the selected server. Device licensing is updated.

> ***A Note About Licensing***
>
> *One Ocularis license is used for each IP address on the device. Therefore, for encoders or multi-lens cameras, if the device utilizes one IP address for multiple channels, you gain the benefit of accessing multiple streams at the cost of only one license (per IP address).*

3. Verify the license assignment by expanding the recording component. Licensed devices appear with a checkmark. Re-apply licenses if necessary.
4. Repeat these steps for each server you wish to update.

7.6.3.2 Editing a Server

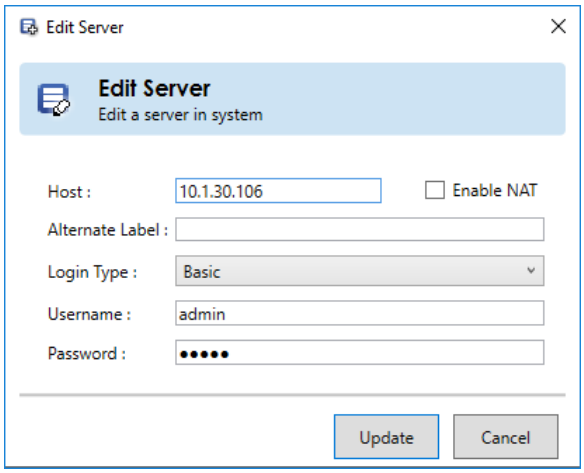
Follow these steps to modify a recorder's IP Address or changes to its corresponding username and password.

TO EDIT A RECORDER'S IP ADDRESS OR ACCOUNT INFO

1. In the **Servers / Events** Tab, select the server you wish to update from the **Servers** pane.
2. Either right-click the server and select 'Edit server' or click the **Edit** button in the Servers Toolbar.

   An *Edit Server* pop-up screen appears.

Figure 13 Edit Server Sample



3. Modify the settings as needed.
4. Click the **Update** button.

   An “Updating” message appears as the configuration is updated.

7.6.3.3 Deleting a Server

Use the procedure below to remove a recorder or other server from the Ocularis Base. This will not delete the recorder or its software; it will simply remove Ocularis’ access to the server. This function is only available members of the 'Administrators' user group of *Ocularis Administrator*. ‘Group Administrators’ do not have permission to delete servers.

TO REMOVE A RECORDER OR OTHER SERVER

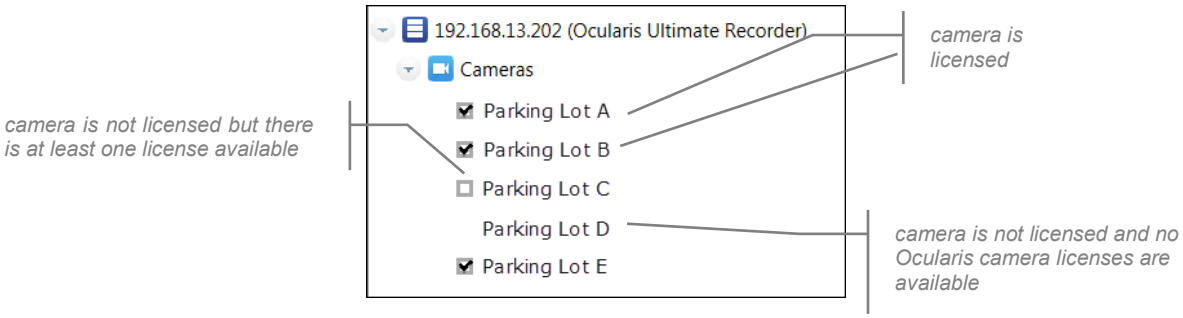
1. In the **Servers / Events** Tab, select the server you wish to remove from the **Servers** pane.
2. Either right-click the server and select ‘Delete server’ or click the **Delete** button in the Servers Toolbar.

   A message appears as the server is removed.

7.6.4 Selecting Licensed Cameras

In the Servers pane, you may expand the recorders in order to see the imported cameras associated with each one. A checkbox appears next to each camera, indicating if the camera is Ocularis licensed or not.

Figure 14 Camera Licenses



Ocularis camera licenses are purchased as part of the Ocularis model licensing. You may view the quantity of Ocularis camera licenses in the *License Information* section of the **About** Tab. Cameras which are 'unchecked' or show no checkbox are not licensed and will not be available for use with Ocularis. You must either purchase additional Ocularis camera licenses or reassign the camera selection.

A Note about License Counts:

Ocularis v5 includes categories where recorder licenses are assigned. These categories are labeled:

RL-1 Channels
RL-2 Channels
RL-3 Channels
RL-4 Channels

The categories simply represent a counter where similar recorder model counts are placed. Since Ocularis 5 supports Mix & Match of recorders, different recorder counts can be combined into the same category.

For example: camera licenses for RC-E and Ocularis Ultimate Recorder would both appear in the category RL-1 Channels. If you had 50 RC-E licenses and 50 Ocularis Ultimate licenses, the RL-1 count would be 100. This also gives you the flexibility to exchange licenses between the two models, allowing you the time and flexibility to migrate cameras from one recorder model to another at your own pace.

RL-4 licenses are reserved for RecOn5 NVRs. PRO, ENT and ULT Bases do not recognize RL-4 licenses.

You will see the Video Channel License counts in the Ocularis License Activation application and in the About Tab of the Ocularis Administrator application. Here you can get a detailed breakdown of each specific recorder camera license count.

TO REASSIGN CAMERA SELECTION

If you need to reassign camera selection for licensed cameras, follow these steps:

1. In the **Servers / Events** Tab, expand the recorder and Cameras node accordingly.
2. Then, deselect a camera which you want to unassign. Do this by unchecking the adjacent checkbox.
3. When a camera license is deselected, unassigned cameras become available for selection and empty checkboxes appear.
4. Click the checkbox for each camera you wish to be used with Ocularis. If the checkboxes disappear, you have used up all available Ocularis camera licenses.

7.6.5 Multi-Channel Device Licensing

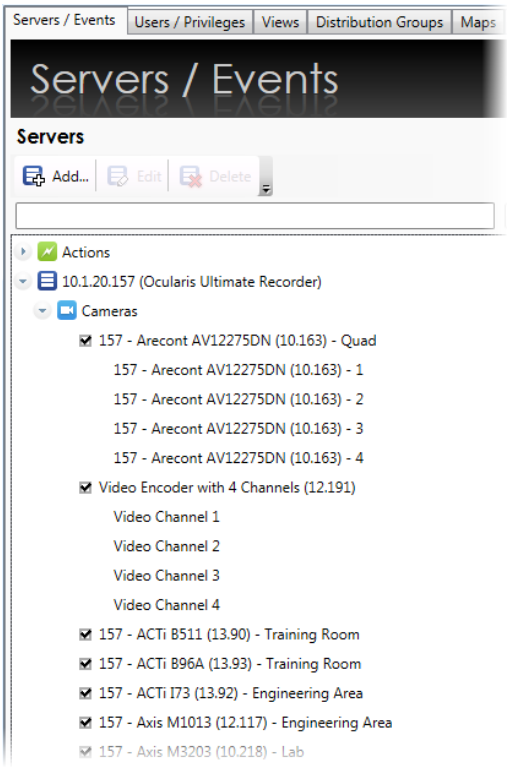
With Ocularis 5, one license is required for each IP Address on a device. This licensing model applies to video encoders and multi-lens cameras.

For instance, the example on the right shows a camera with four lenses (Arecont AV12275DN) and a video encoder with four channels. As you can see, only two Ocularis licenses are used for these eight channels. Verify your license counts in the **About** tab.

Update the camera license counts after the recording component upgrade is complete by right-clicking the server name in the **Servers / Events Tab** and clicking 'Refresh Server'.

You can, however, use each stream individually for blank screen events, assigning privileges, views and maps. With this licensing model, if you uncheck (unlicensed) the device, all channels/streams on that device become unlicensed.

Figure 15 Multi-Channel Devices



7.7 SMA Expiration Notice

SMA (Software Maintanence Agreement) is a program designed to keep your Ocularis software up-to-date. Under SMA, your organization has access to all upgrades of Ocularis and world class technical support.

The Ocularis Administrator application may display a pop-up 'Notice' box to inform all administrators about the status of their SMA. The following rules apply:

- If the expiration date for the SMA plan is further than 90 days out, no indication pop-up appears inside Ocularis Administrator. The expiration date can be found on the **About** tab.
- If the expiration date for the SMA plan is 90 days in the future (or sooner), a yellow 'Notice' pop-up appears identifying the expiration date.
- If the expiration date for the SMA plan passes, a red 'Notice' pop-up appears. This pop-up will continue to appear for 14 days and then disappear completely.

The message is informational only. The software will continue to function beyond the SMA expiration date. You will not, however, be able upgrade to a newer version of Ocularis or receive technical support until the SMA expiration date has been extended. Click the SMA link to open the corresponding webpage for information on SMA or contact Qognify Inside Sales to extend the expiration date.

The 'Notice' message will appear on each tab of the application. Click the 'Notice' bar to expand or collapse the message. Click the 'X' to clear the box for the current session. If still applicable, the message will appear again the next time you log in to Ocularis Administrator.

The SMA expiration date may also be found in the About Tab on page 200.

7.8 Automatic Base Update

Whenever a change is made on a recorder that requires a refresh in the Base, Ocularis Administrator will perform an automatic refresh of the affected server. This is actually controlled by the Ocularis Recorder Proxy (formerly called 'Ocularis Event Proxy') and is equivalent to a user right-clicking a server name and selecting 'Refresh Server'. Once a recorder change is made (e.g. a new camera is added, camera name changed, etc.), the Recorder Proxy is aware of this change. It will then instruct Ocularis Administrator to refresh the applicable server.

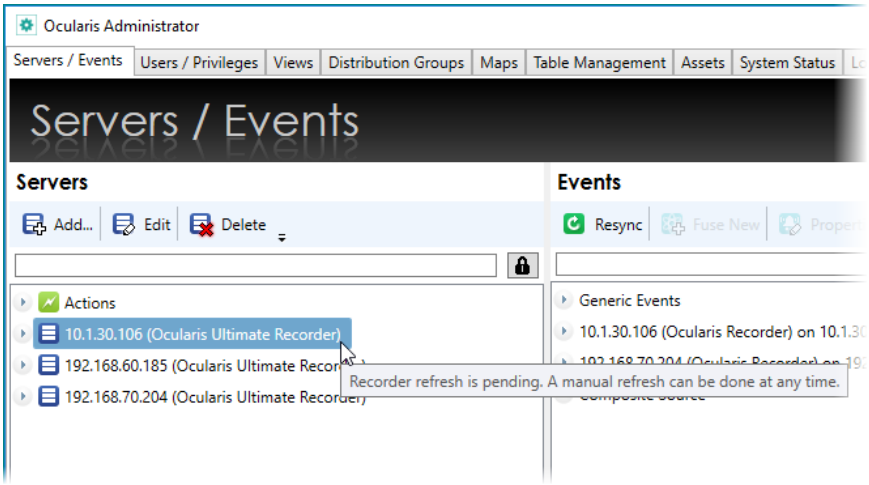
The recorder changes that will cause the Base to refresh include:

- Adding a device or adding an additional camera from a multi-channel device
- Renaming a device (at the top level name only; does not apply to renaming a camera name for a multi-channel device)
- Deleting a device

Adding, modifying or deleting a camera stream, however, will be silently updated by the Recorder Proxy. These do not require a recorder refresh on the Base.

When the first change is made, a refresh is immediate, however on larger systems this could take up to a minute. If the *Ocularis Administrator* application is open and you want to see the change either click the 'Resync' button in the **Events** pane or switch tabs. To prevent too many automatic refreshes, subsequent recorder changes will not immediately force a refresh if performed within five minutes of the first change. Once the second change is made on the recorder, a five minute timer starts and a blue highlight will pulse over the server name in the **Servers / Events** tab to indicate that a Recorder refresh is pending. If another change is made on the recorder, the timer is reset at five minutes from that point on and so on. You can wait until the system does the refresh automatically or you can perform a manual refresh by right-clicking the server name and selecting 'Refresh Server'. If a manual refresh is performed, the scheduled automatic refresh is cancelled.

Figure 16 Recorder refresh is pending



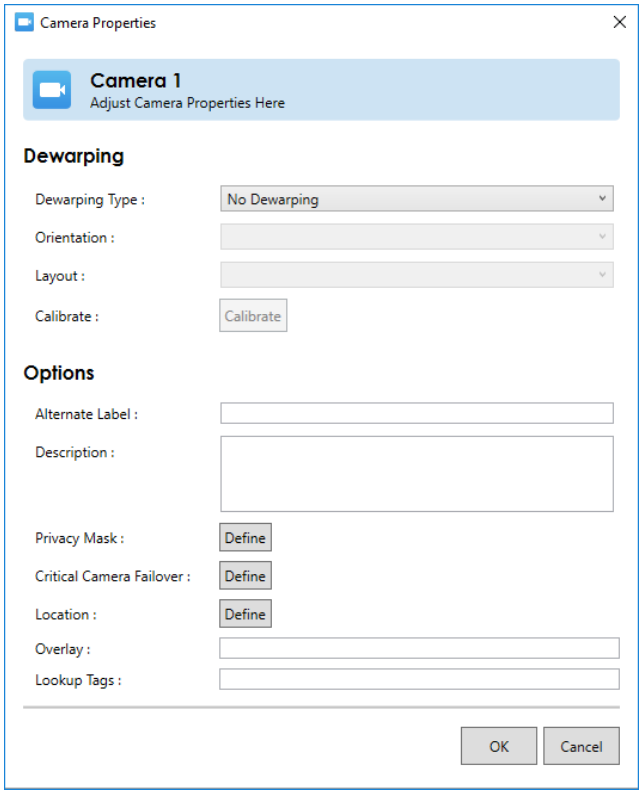
In order for this feature to work, the checkbox 'Auto Update Recorder on Ocularis Base' must be checked inside the Recorder Proxy, under **Base Settings** for each server. This feature is enabled by default.

***Note**: If a camera name is changed on the recorder, this feature will automatically update it in the Servers pane. However, the camera name change will not be reflected in the Events pane. The event will continue to work, however, even with the outdated name. To correct this, restart the Recorder Proxy.*

7.9 Camera Properties

Certain parameters can be set on a camera by camera basis by the administrator in the **Servers / Events** tab. This is done by right-clicking a camera name in the *Servers* pane and selecting *Properties* (or double-click the camera name).

Figure 17 Camera Properties



7.9.1 Dewarping

Cameras using 360° or *panomorph* lenses have a 360°x 180° field of view. When video from these cameras is displayed on a two dimensional computer screen, the original image appears as a dome or ellipse and is not very usable. Ocularis can *dewarp* or flatten video from these lenses and display them in ways that make them quite useful. One lens strategically positioned in the center of a room can cover the same area where multiple cameras were once required. Operators can operate the field of view from a 360° lens similar to that of a PTZ camera. Meanwhile behind the scenes, Ocularis records the full 360° image so that investigations can access the entire image regardless of the field of view that a particular operator happens to be displaying.

Each lens manufacturer approaches their panomorph algorithm differently and therefore, each require a unique *plug-in* (additional software component) in order to properly display video. If you

do not see your supported camera in the 'Dewarping Type' drop-down list, check the software downloads page on the website at www.onssi.com/software-downloads/. Plug-ins are no longer bundled with the software. All supported plug-ins are available from the Qognify website as stated above.

7.9.1.1 Plug-In Installation

Dewarping plugs-ins must be installed on the Ocularis Base server. If your Base does not have internet connectivity, download the software from a different computer and bring the installation file to the Base server.

1. Go to www.onssi.com/software-downloads/ and scroll the page until you see *Ocularis Client* Dewarping Plugins.
2. Click the plug-in you wish to install. It will be downloaded locally using the browser's normal file download steps.
3. If you are not already located on the Ocularis Base server, bring the downloaded file to that server.
4. Click the .exe file to launch the installation wizard.
5. Follow the on-screen prompts and click **Finish** when done.

The plug-in should now be visible in the 'Camera Properties' dialog in *Ocularis Administrator*.

When an *Ocularis Client* user logs into the Base, the necessary .dlls are downloaded from the Base to the client machine. At this time viewing dewarped images is supported only on *Ocularis Client* (not with *Ocularis Viewer*, *Ocularis Web* or *Ocularis Mobile*).

As plug-ins for camera manufacturers are created they will be available for download on the Qognify website.

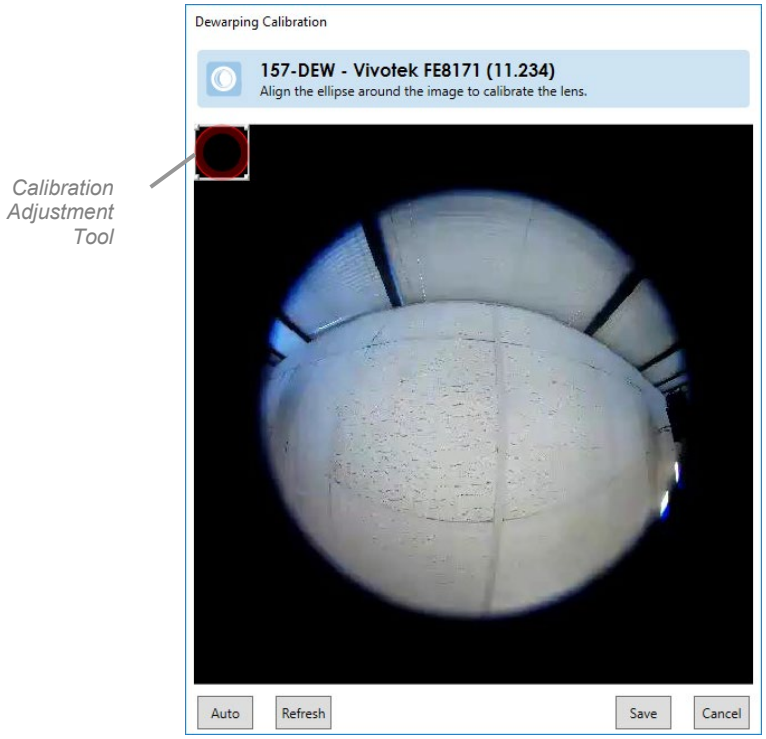
7.9.1.2 Plug-In Configuration

In order to take advantage of 360° lenses, the camera with the panomorph lens needs to be configured in the *Ocularis Administrator*. The lens' corresponding driver needs to be selected along with the camera's orientation and layout.

1. On the *Ocularis Administrator* **Servers / Events** tab, right-click the camera with the 360° lens and select 'Properties'.
2. In the *Dewarping Type* drop-down list, select the plug-in for the corresponding camera or lens.

3. Select the positioning of the camera mount under *Orientation*. Choices are: Ceiling, Wall, Floor
4. Select the default layout for the image under *Layout*. Choices will vary based on manufacturer. Examples include: Single, Quad, Panorama Narrow, Panorama Wide or VCam. This is what will be displayed in Ocularis Client when the camera initially appears or when a view is reloaded.
5. For Sentry360 and Vivotek cameras, calibration must be performed. Click the **Calibrate** button.
    a. A spherical snapshot should appear showing the native fisheye view from the camera. A calibration adjustment tool in the form of a red circle appears in the upper left corner.

Figure 18 Calibrate a Sentry360 Camera



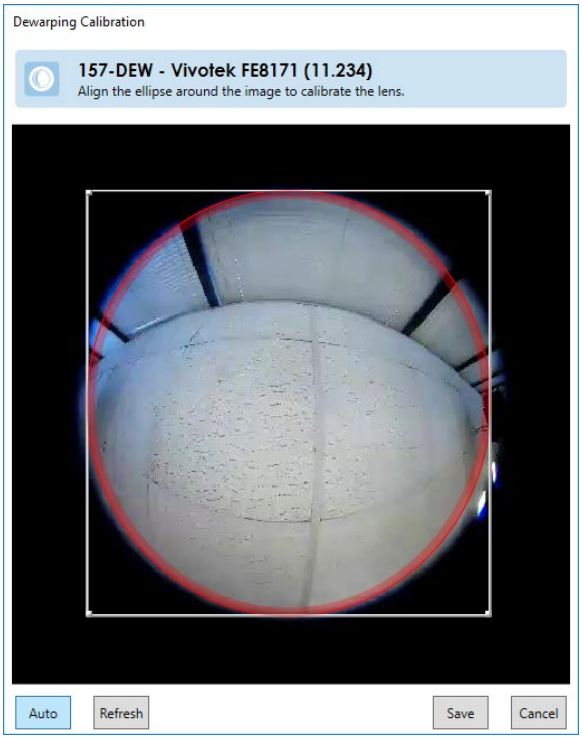
The goal is to use the Calibration Adjustment tool to outline the area of view. This may be done manually or automatically.

***Note**: The image that appears may not be the most recent. Click the Refresh button to take a current snapshot of the camera's image.*

b. For manual adjustment, use the mouse to drag the calibration adjustment tool across the screen. Use the mouse to stretch the edge of the calibration adjustment tool so that the outline matches that of the image.

c. For automatic adjustment, simply click the **Auto** button on the bottom left portion of the pop-up. You may further provide manual adjustments if you do not like the automatic selection.

Figure 19 Sentry360



d. When finished, click **Save**.

6. If you are finished configuring Camera Properties, click **OK**.

The user will now be able to take advantage of the 360° x 180° field of view when viewing via Ocularis Client.

7.9.2 Options

The following table describes additional parameters in the *Camera Properties* dialog box.

Item	***Description***
Alternate Label	The text entered here will be used to identify this camera in Ocularis Client. This gives the administrator the ability to change the display of a camera name without changing it permanently on the recorder. You may consider using this field in conjunction with Description (below) to clearly identify your cameras.
Description	You may add a description for the camera which provides more detail on its location, purpose, settings, etc. This field is available to administrators while viewing the camera thumbnail in preview modes within Ocularis Administrator as well as in tool tips within Ocularis Client. You may consider using this field in conjunction with Alternate Label (above) to clearly identify your cameras.
Privacy Mask	Click **Define** to identify areas on the video image to be masked for privacy. Only applicable to fixed cameras. See *Privacy Mask* below for more information.
Critical Camera Failover	Click **Define** to configure failover cameras for this camera. See below for more information.
Location	You may manually enter GPS coordinates for a camera. This can be used with third party integrations, on certain Ocularis Maps or with the Android version of Ocularis Mobile.
Overlay	This function is used with third party integrations. You can specify a .txt or .aspx file which will be used to supply an overlay of text, symbols or images within the camera stream. The data displayed can change dynamically if the content of the overlay file changes. The additional metadata will not be recorded along with the video. Enter a URL for the location full path and full name of the file.
Lookup Tags	Add keywords to be used in a quick lookup by operators in Ocularis Client. See *Keyword Quick View* below for more details.

7.9.2.1 Keyword Quick View

A *Keyword Quick View* is used in Ocularis Client to quickly create a view for which all cameras share the same keyword or tag. For instance, you may have a camera positioned at every doorway in the office. If the keyword 'door' is assigned to these cameras, operators can quickly show all cameras that meet the keyword criteria. While this may also be done in a preconfigured view, using keyword quick view can be significantly faster than paging through dozens or hundreds of views and selecting one from the menu.

TO ASSIGN KEYWORDS TO A CAMERA

1. In the **Servers / Events** tab, locate and right-click the desired camera.
2. Select **Properties**.
3. In the **Lookup Tags** field enter one or more keywords that will be used to invoke the camera in a quick view.
    - Each keyword tag is limited to no more than ten characters.
    - The following characters are not allowed: []*?@/=+|\:;!#$%^()_{}'.-~&”><,
    - Use the comma character to separate multiple tags in the field. Do NOT use a space after the comma.

    For instance:

    If you want to assign the keyword 'door' and the keyword 'lobby', enter as follows:

    door,lobby

    - While there is no limit to how many cameras you can assign a keyword to, only the first twenty-five cameras found will be displayed in Ocularis Client. The grid layout will vary depending on how many cameras are displayed:
        - ⇨ Results of between 1-4 cameras will display in a 2 x 2 view
        - ⇨ Results of between 5-9 cameras will display in a 3 x 3 view
        - ⇨ Results of between 10-16 cameras will display in a 4 x 4 view
        - ⇨ Results of between 17-25 cameras will display in a 5 x 5 view
    - The view displayed will use the highest resolution stream available for each camera found.
    - The view for the operator will be temporary and last only during the existing log in session. Refer to the *Ocularis Client User Manual* for more instructions on how to use this feature.

7.9.2.2 Privacy Mask

A *Privacy Mask* is an area of an image that is blocked out from view. For instance, in an office environment you may want to see the images of the general office area but want to block out someone’s private desk area to provide the employee with some privacy. In this example, you may select a section of the image to NOT appear in the video feed. This is called a privacy mask. Privacy masks may be used for legal or liability reasons as well.

Ocularis supports three levels of privacy masking: on the camera, on the recorder and within Ocularis. Setting a privacy mask in Ocularis has the following benefits:

- You may designate multiple but separate masks on the same image.
- The mask shapes can be any polygon. There are no shape restrictions.

Privacy Masks set in Ocularis are supported on fixed cameras only and will not appear in *Ocularis Mobile* or *Ocularis Web*. Also, if you use multiple live streams, the position of the privacy mask may move slightly when you change from one stream to another with a different resolution.

Figure 20 Right-click to draw privacy mask

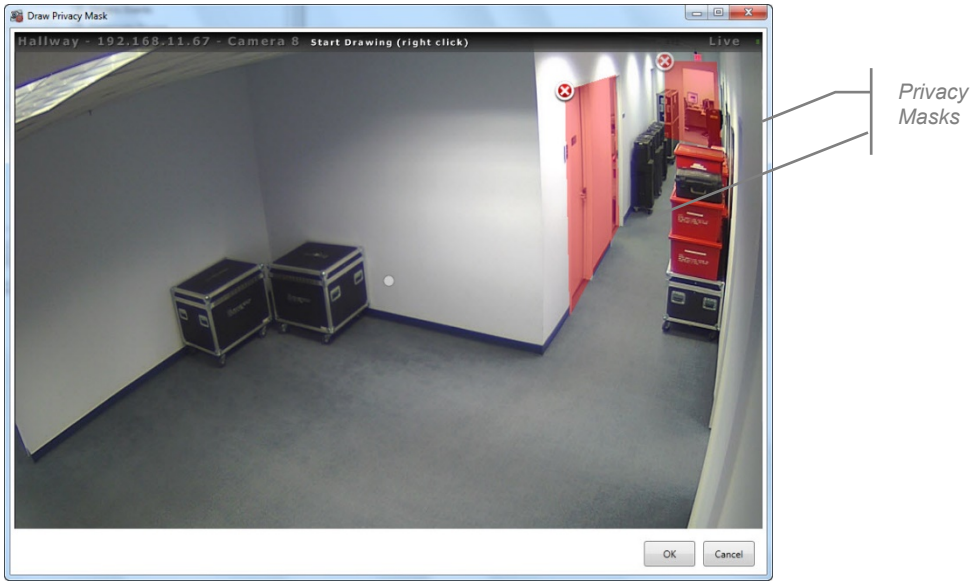
To Create A Privacy Mask

1. In the **Servers / Events** tab, locate and right-click the desired camera.
2. Select **Properties**.
3. Click **Define** in the *Options* section of the *Camera Properties* pop-up.
4. In the *Draw Privacy Mask* pop-up, the camera image appears.
5. Use your mouse to identify an area or areas of the image that you wish to block out.

   To draw the area, right-click the mouse, drag, right-click, drag, repeat until you have identified the blocked area. Be sure to right-click back on the original starting point to complete the shape.

   You may draw multiple, non-contiguous shapes.

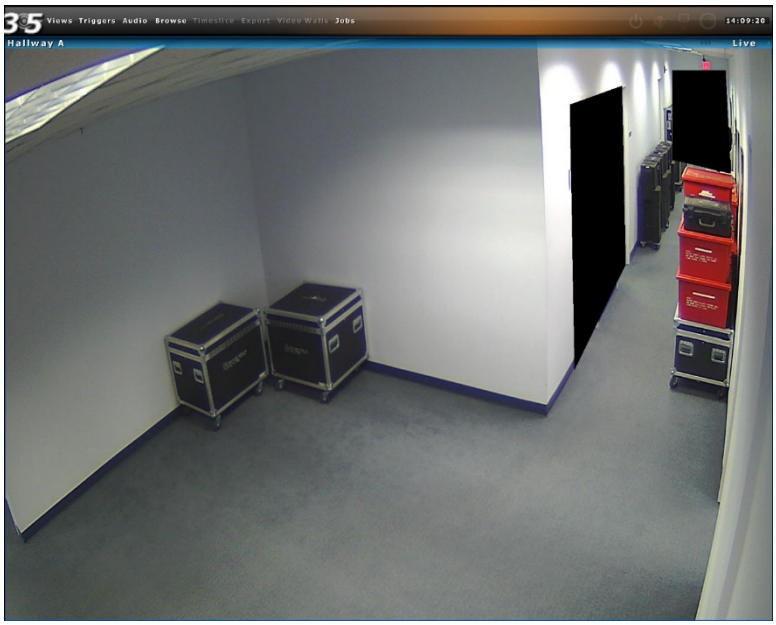
Figure 21 Configuring Multiple Privacy Masks



6. Click **OK** when finished setting the privacy mask(s).

   The mask shapes appear translucent on this screen to aid you in understanding what the mask is covering. When viewing video from this camera in a client, the shapes will be opaque.

Figure 22 Privacy Masks when viewed in Ocularis Client



7.9.2.3 Critical Camera Failover

Critical Camera Failover is used for mission critical applications where live video cannot be interrupted. Camera streams may become unavailable for multiple reasons such as network failure, device failure or even recorder failure. Critical Camera Failover automatically switches the camera pane to an alternate stream in a little as 2-3 seconds without operator intervention and works in all Camera Views, Map Views and Alerts. Critical Camera Failover will continue to function even if Ocularis Base is unavailable. Multiple cameras can be designated as failover cameras for the same primary camera.

Cameras selected as failover cameras include:

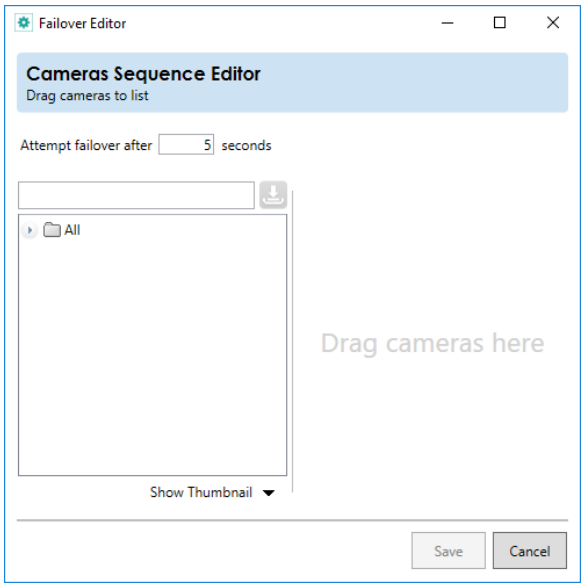
- Duplicate camera stream from a redundant recorder
- Different camera from the same recorder
- Different camera from a different recorder
- Any combination of the above

TO CONFIGURE CRITICAL CAMERA FAILOVER

1. From the *Servers* pane, right-click the critical camera you wish to configure and select **Properties**.
2. In the 'Camera Properties' pop-up, click the **Define** button next to 'Critical Camera Failover'. The *Critical Camera Failover Editor* appears.

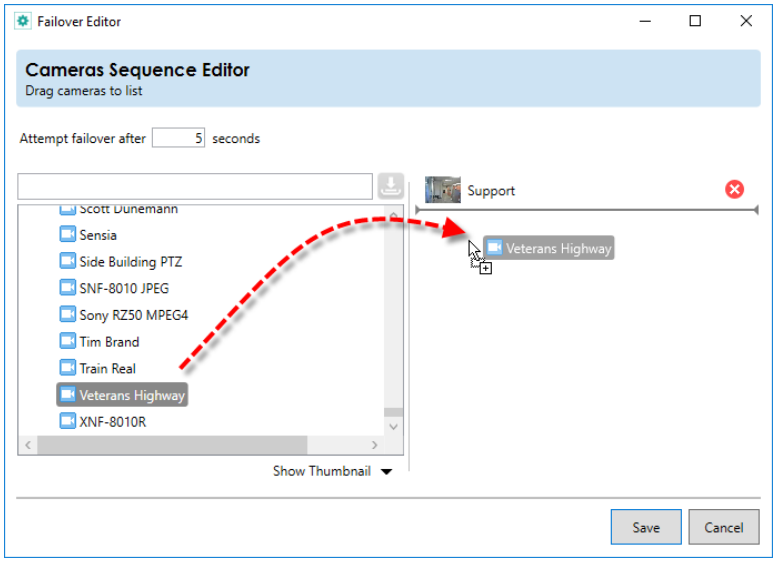
   The primary camera that you're setting up is listed at the top of the pop-up.

Figure 23 Critical Camera Failover Editor



3. Expand the camera folder(s) to expose the list of available failover cameras.

Figure 24 Drag and Drop to create failover cameras list



4. Drag and drop the desired failover camera(s) from the list on the left to the drop area on the right. There is no limit to the number of cameras that can be configured as a backup.

HOW DOES IT WORK?

If the primary camera stream fails for any reason, the next camera in the list will be displayed in its place in the Ocularis Client. This could be in a view pane or on a map or video wall. If that camera fails then the next camera (in order) will appear. In the example above, if Camera 1 fails, Camera 2 will be displayed. If Camera 2 fails, Camera 5 will display. Then if Camera 5 fails, Camera 3 is displayed.

Ocularis Client monitors the stream and if it determines that the stream is no longer there, it will switch to the next camera in the list. The amount of time to wait to determine if the stream is live is controlled by the 'Switch Time' field when you configure the failover cameras. The more critical the camera, the shorter duration to use in this field.

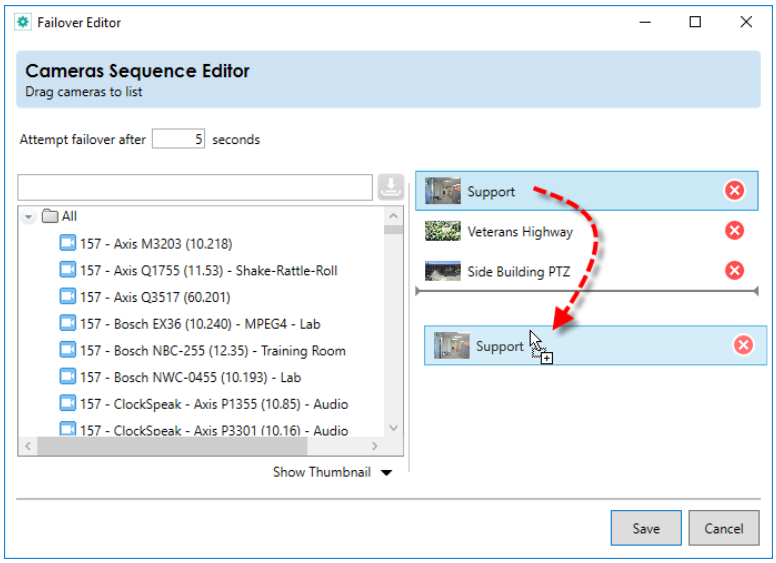
When a failover camera is displayed in a view, there is a 'Failover Camera' overlay that appears in the view pane to notify you that the stream has changed. By default, the overlay is displayed for 10 seconds and then disappears. This time may be modified in the Client Setup of the Ocularis Client. The failover camera name is shown in the image bar of the pane along with an orange status light.

Also, when you use the mouse to display the pane's streaming information, you'll see a message that the video is a failover for the primary camera.

Lastly, during the time that the failover camera is displayed, Ocularis Client continues to check the primary camera stream. If the primary camera stream is restored, the video from this camera will be returned to the display.

The order of the cameras listed will be the order to display each failover camera. If you need to recorder the list, simply drag and drop cameras from within the list.

Figure 25 Drag and drop cameras to reorder the failover list



5. If you need to remove a camera from the failover list, simple click the red icon to the right of the camera name.
6. When finished configuring this camera's failover list, click **Save**. Then click **OK**.

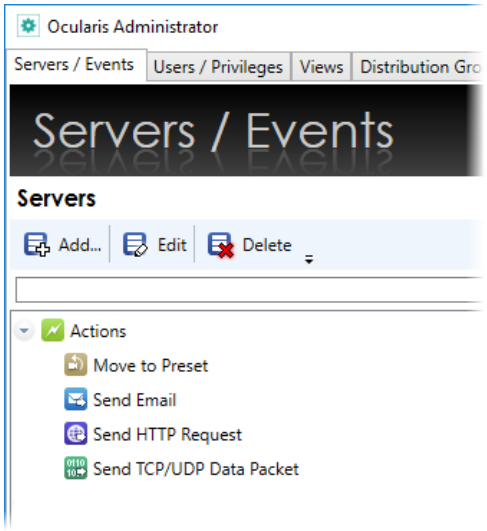
7.10 Actions

One of the primary features of Ocularis is its ability to alert the right person when some event occurs. The alert can take several forms:

- Video from one or more cameras can appear on a dedicated monitor or portion thereof
- A custom sound can be played to alert an operator to a specific event
- A PTZ camera can be moved to a configured preset position
- An email can be sent to one or more people
- An HTTP Get or Post Request can be issued
- An outgoing data packet (generic string) can be sent

The first two items in the list above are configured in the Events pane and covered in the next section. The latter four items are configured in the Servers pane and discussed below.

Figure 26 Alert Actions



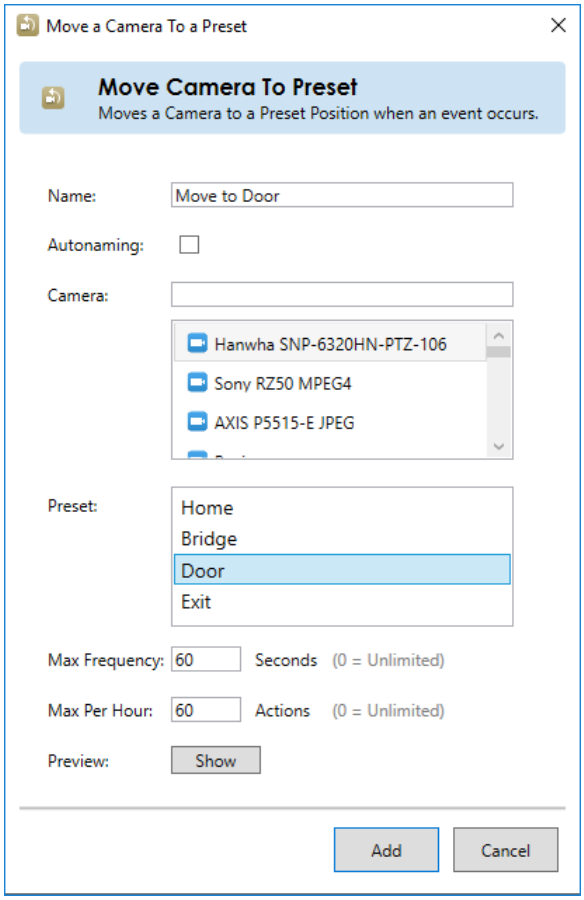
7.10.1 Move to Preset

When a particular event occurs, one of the actions that you may configure is to move a camera to a preconfigured preset position. For instance, if there is an ‘access denied’ event received from a key card entry system, you may want a local camera to move to the position that views the door to see the incident as it occurs. The preset configurations are made under the actions. Associating the action with an event is done in the **Distribution Groups** tab. As a reminder, presets are set on the recording component using the Ocularis Recorder Manager. The presets are imported into Ocularis when the server is imported or refreshed in the **Servers / Events** tab.

7.10.1.1 To Add a New Preset Move

1. Expand the Actions node in the **Servers / Events** tab.
2. Right-click the 'Move to Preset' list item and select *Add New Move to Preset…*

Figure 27 Configure Camera Move to Preset



3. In the **Name** field, enter a descriptive name to identify this action. Alternately, if you click the **Autonaming** checkbox, the **Name** will be filled in automatically using the format:

   Move **[camera name]** to **[Preset name]**

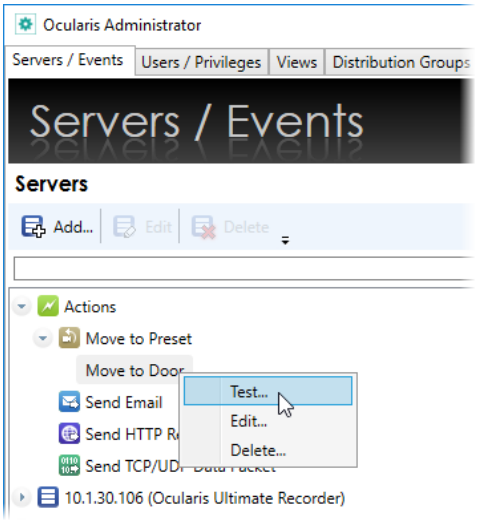
4. Select the camera with the preset you wish to use in the action. You may use the **Camera** text field to filter the list by entering all or a portion of a key word within the camera name.
5. Once the camera is selected, configured presets appear in the **Preset** text field. Select the preset you wish the camera to move to once the event is configured.

6. The **Max Frequency** field is set to 60 seconds as the default value. This field identifies the time interval in seconds in which you would like to monitor alerts. This feature will reduce the amount of repeated alerts within a specified timeframe. You may modify this value to any number between 1 and 3600. A zero value indicates an unlimited time period and may accumulate many unnecessary events.
7. The **Max Per Hour** field allows you to control the maximum number of times you want this action to be performed in an hour.
8. Click the **Show** button to launch a pop-up that shows the image of the preset to insure that you are selecting the correct one. Click OK to close the Preview pop-up.
9. When done, click the **Add** button.

The preset move has just been configured but has not been assigned to any particular alert. This association is done in the **Distribution Groups** tab. See ***Actions*** on page 180.

Once a preset move has been configured, you may test, edit or delete the configuration.

Figure 28 Preset Move Actions



7.10.1.2 To Test a New Preset Move

You can test the functionality of a configured preset move to be sure that it works properly.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Move to Preset** item.
3. Right-click the configured move to preset list item and select *Test…*
4. A pop-up appears indicating that a test move will be issued.

5. Click **Send** to execute the move.

7.10.1.3 To Edit a Preset Move

You can edit the configuration of a preset move if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Move to Preset** item.
3. Right-click the configured move to preset list item and select *Edit…*
4. Modify the changes as needed.
5. Click **Update** to save changes.

7.10.1.4 To Delete a Preset Move

You can delete a configured preset move if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Move to Preset** item.
3. Right-click the configured move to preset list item and select *Delete…*
4. An '*Are you sure you want to delete*…" pop-up is displayed. Click **Yes** to confirm the deletion.

7.10.2 Send Email

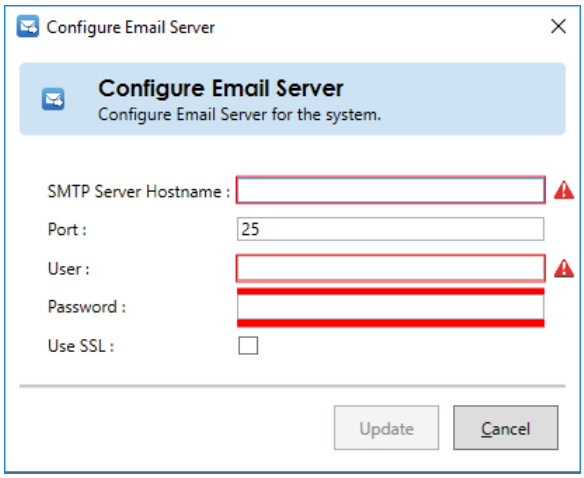
When an event occurs you may want to send an email to someone for notification purposes. Emails are configured in the **Servers / Events** tab and associated with an event in the **Distribution Groups** tab. An email SMTP server is required in order to send outgoing email.

7.10.2.1 To Configure an Email Server

Configuring your email server need only be done once.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Right-click the 'Send Email' list item and select *Configure Email Server…*

Figure 29 Configure the Email Server



3. Fill out the fields of the pop-up according to the following:

Item	***Description***
SMTP	Enter the host name for the SMTP email server.
Port	Identify the port number to be used to send email. Typically, port 25 is reserved for this but you can modify the port if necessary.
User	Enter the user account to be used as the sending email account.
Password	Enter the password for the user account.
Use SSL	Click this box if email server uses SSL (Secure Sockets Layer)

The red outlined warnings will disappear once data is entered in the correct format into each field.

4. When complete, click **Update**.

7.10.2.2 To Modify an Email Server Configuration

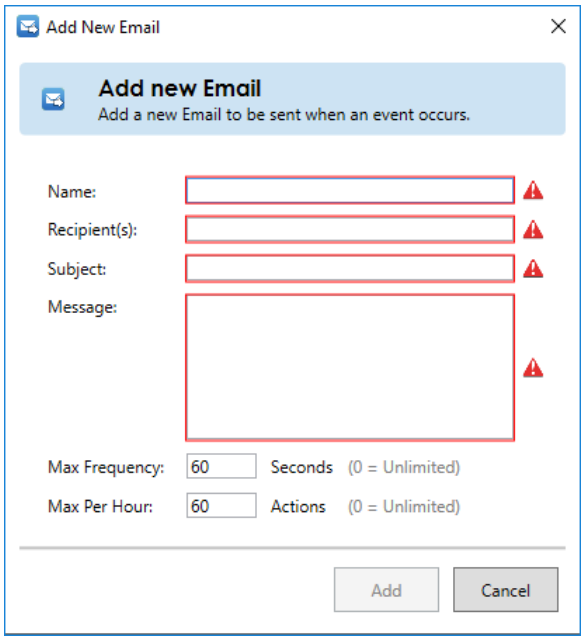
1. Expand the *Actions* node in the **Servers / Events** tab.
2. Right-click the 'Send Email' list item and select *Configure Email Server…*
3. Modify the fields of the pop-up as needed.
4. When complete, click **Update**.

7.10.2.3 To Configure an Email

One or more emails can be pre-configured so that when an event triggers, a custom email can be sent.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Right-click the 'Send Email' list item and select *Add New Email…*

Figure 30 Configure a new email



3. Fill out the fields of the pop-up according to the following:

Item	***Description***
Name	Enter a descriptive name for the email template so that you can easily identify it.
Recipient(s)	Enter the email distribution list using standard email format (e.g. john@domain.com). If you want to send to multiple recipients, separate each with a comma.
Subject	Enter text to be used as the subject of the email.
Message	Enter text for the message body of the email. You may also insert system variables here. See *Action Variables* on page 43 for more information.
Max Frequency	The **Max Frequency** field is set to 60 seconds as the default value. This field identifies the time interval in seconds in which you would like to monitor alerts. This feature will reduce the amount of repeated alerts within a specified timeframe. You may modify this value to any number between 1 and 3600. A

Item	*Description*
	zero value indicates an unlimited time period and may accumulate many unnecessary events.
Max Per Hour	The **Max Per Hour** field allows you to control the maximum number of times you want this action to be performed in an hour.

The red outlined warnings will disappear once data is entered in the correct format into each field.

4. When complete, click **Add**.

The email has been configured but has not been assigned to any particular alert. This association is done in the **Distribution Groups** tab. See ***Actions*** on page 180.

Once an email has been configured, you may test, edit or delete it.

7.10.2.4 To Test an Email

You can test the functionality of a configured email.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send Email** item.
3. Right-click the configured email list item and select *Test…*
4. A pop-up appears indicating that a test move will be issued.
5. Click **Send** to send a test email.
6. Click **OK** when the *Test Status* pop-up appears.

7.10.2.5 To Edit an Email

You can edit the configuration of an email if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send Email** item.
3. Right-click the configured email list item and select *Edit…*
4. Modify the changes as needed.
5. Click **Update** to save changes.

7.10.2.6 To Delete an Email

You can delete a configured email if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send Email** item.
3. Right-click the configured email list item and select *Delete…*
4. An '*Are you sure you want to delete…*" pop-up is displayed. Click **Yes** to confirm the deletion.

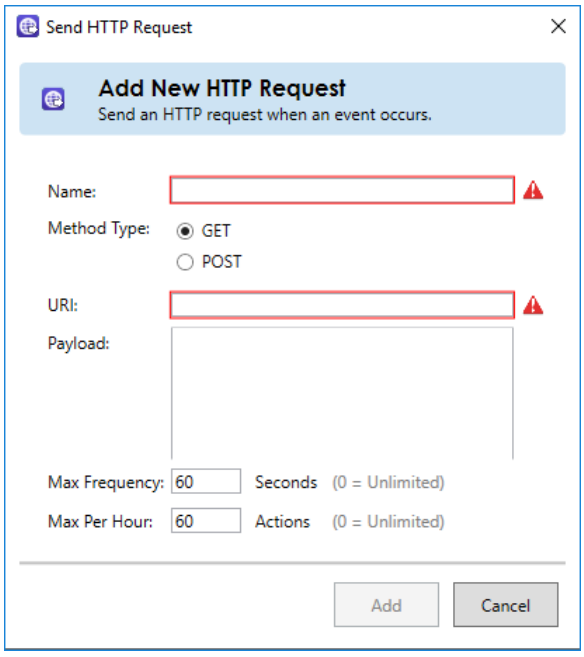
7.10.3 Send HTTP Request

Used when Ocularis is integrated with certain 3rd party systems, HTTP requests (GET and POST) can be sent when an event occurs. The requests are configured in the **Servers / Events** tab and associated with an event in the **Distribution Groups** tab.

7.10.3.1 To Configure an HTTP Request

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Right-click the 'Send HTTP Request' list item and select *Add New HTTP Request…*

Figure 31 Add New HTTP Request



3. Fill out the fields of the pop-up according to the following:

Item	*Description*
Name	Enter a descriptive name for the request so that you can easily identify it.
Method Type	Select 'GET' or 'POST' based on your integration.
URI	Enter the URI to send the request to.
Payload	Enter the payload information to be sent. You may also insert system variables here. See *Action Variables* on page 43 for more information.
Max Frequency	The **Max Frequency** field is set to 60 seconds as the default value. This field identifies the time interval in seconds in which you would like to monitor alerts. This feature will reduce the amount of repeated alerts within a specified timeframe. Valid values are any number between 1 and 3600. A zero value indicates an unlimited time period and may accumulate many unnecessary events.
Max Per Hour	The **Max Per Hour** field allows you to control the maximum number of times you want this action to be performed in an hour.

The red outlined warnings will disappear once data is entered in the correct format into each field.

4. When complete, click **Add**.

The HTTP Request has been configured but has not been assigned to any particular alert. This association is done in the **Distribution Groups** tab. See ***Actions*** on page 180.

Once an HTTP Request has been configured, you may test, edit or delete it.

7.10.3.2 To Test an HTTP Request

You can test the functionality of a configured HTTP Request.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send HTTP Request** item.
3. Right-click the configured HTTP Request list item and select *Test…*
4. A pop-up appears indicating that a test move will be issued.
5. Click **Send** to send a test HTTP Request.
6. Click **OK** when the *Test Status* pop-up appears.

7.10.3.3 To Edit an HTTP Request

You can edit the configuration of an HTTP Request if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send HTTP Request** item.
3. Right-click the configured HTTP Request list item and select *Edit…*
4. Modify the changes as needed.
5. Click **Update** to save changes.

7.10.3.4 To Delete an HTTP Request

You can delete a configured HTTP Request if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send HTTP Request** item.
3. Right-click the configured HTTP Request list item and select *Delete…*
4. An '*Are you sure you want to delete…*" pop-up is displayed. Click **Yes** to confirm the deletion.

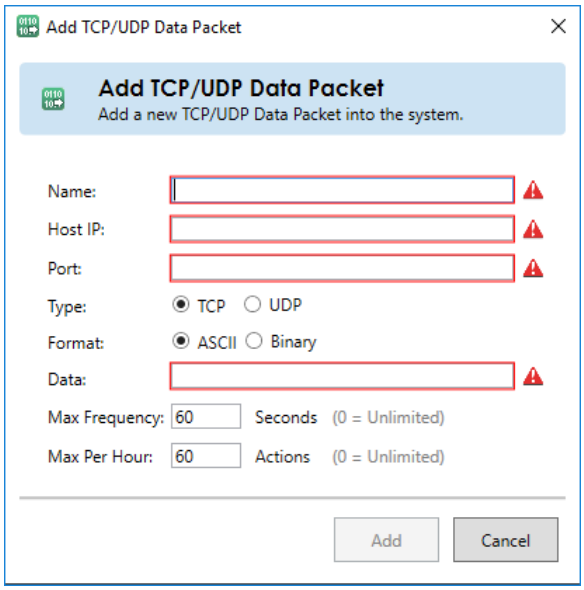
7.10.4 Send TCP/UDP Data Packet

Used when Ocularis is integrated with certain 3rd party systems, data packets can be sent from Ocularis when an event occurs. The packets are configured in the **Servers / Events** tab and associated with an event in the **Distribution Groups** tab.

7.10.4.1 To Configure a TCP/UDP Data Packet

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Right-click the 'Send TCP/UDP Data Packet' list item and select *Add New Data Packet…*

Figure 32 Add New TCP/UDP Data Packet



3. Fill out the fields of the pop-up according to the following:

Item	***Description***
Name	Enter a descriptive name for the data packet so that you can easily identify it.
Host IP	Enter the recipient host IP address.
Port	Enter the port number to use to send the data packet.
Type	Select either **TCP** or **UDP** depending on the transmission desired.
Format	Choose either **ASCII** or **Binary**.
Data	Enter the string to be sent. You may also insert system variables here. See *Action Variables* on page 43 for more information.
Max Frequency	The **Max Frequency** field identifies the time interval in seconds in which you would like to monitor alerts. This setting will reduce the amount of repeated alerts within a specified timeframe. Valid values are any number between 1 and 3600. A zero value indicates an unlimited time period and may accumulate many unnecessary events. Default value is 60 seconds.
Max Per Hour	The **Max Per Hour** field allows you to control the maximum number of times you want this action to be performed in an hour.

The red outlined warnings will disappear once data is entered in the correct format into each field.

4. When complete, click **Add**.

The Data Packet has been configured but has not been assigned to any particular alert. This association is done in the **Distribution Groups** tab. See ***Actions*** on page 180.

Once a Data Packet has been configured, you may test, edit or delete it.

7.10.4.2 To Test a TCP/UDP Data Packet

You can test the functionality of a configured TCP/UDP Data Packet.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send TCP/UDP Data Packet** item.
3. Right-click the configured TCP/UDP Data Packet list item and select *Test…*
4. A pop-up appears indicating that a test move will be issued.
5. Click **Send** to send a test TCP/UDP Data Packet.
6. Click **OK** when the *Test Status* pop-up appears.

7.10.4.3 To Edit a TCP/UDP Data Packet

You can edit the configuration of a TCP/UDP Data Packet if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send TCP/UDP Data Packet** item.
3. Right-click the configured TCP/UDP Data Packet list item and select *Edit…*
4. Modify the changes as needed.
5. Click **Update** to save changes.

7.10.4.4 To Delete a TCP/UDP Data Packet

You can delete a configured TCP/UDP Data Packet if necessary.

1. Expand the *Actions* node in the **Servers / Events** tab.
2. Expand the **Send TCP/UDP Data Packet** item.
3. Right-click the configured TCP/UDP Data Packet list item and select *Delete…*
4. An '*Are you sure you want to delete…*" pop-up is displayed. Click **Yes** to confirm the deletion.

7.10.5 Action Variables

For the *Email*, *Send HTTP Request* and *Send TCP/UDP Data Packet* alert actions, variables may be used to automatically insert system fields into the message/payload/data fields of the action. These action variables are defined here:

Tag	***Value***
<%=Event.ID%>	ID of entry in Events table
<%=Event.EventSource.Name%>	Event Source Name (Could be Generic Events, Composite Source, Recorder Proxy Name)
<%=Event.EventRule.Name%>	Name of Event Rule (Could be Motion, entry from under Generic Event when [add rule...] saved
<%=Event.EventRule.ID%>	ID of Event Rule (such as Motion) when added to the EventRules table
<%=Event.EventRule.EventPriority.Value%>	Priority assigned to an Event Rule such as Motion, Not Responding, etc.
<%=Event.Occurred%>	Time the event occurred which is stored in the Events table
<%=Event.EventRule.Sensor.Name%>	Name of Event Sensor (Could be Recorder Proxy Camera, entry under Generic Events when [add connection...] saved
<%=Camera.Altlabel%>	Name of the alternate label for the camera

7.11 Events Pane

The **Event** pane of the **Servers / Events** tab is where administrators configure Ocularis events. This includes:

- Camera events are identified and video alerting is mapped between cameras and events.
- Creating associations between events and cameras.
- Creating new events, such as Generic, Composite Events and Analytic Events.

Events configured in this tab identify system wide events. Filtering these events to individual users is configured in the **Distribution Groups Tab**.

***Note**: In order to use camera events with Ocularis Base, the Ocularis Recorder Proxy must first be installed and configured to forward events to the Ocularis Base server. See the Ocularis Installation & Licensing Guide for more details.*

The proxies configured to forward camera and system events to Ocularis Base are listed in the **Events** pane. If the desired proxy is not shown, you should:

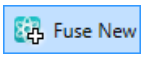
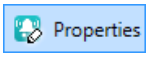
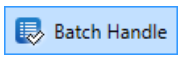
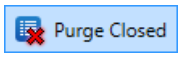
- Click the **Resync** button (*see Events Toolbar* on page 44).

- Double-check the recorder proxy installation and configuration. You may need to restart the recorder proxy and/or restart the *Ocularis Administrator* application in order for it to appear on this screen.

Administrators determine which events on which camera they would like included as part of the alert notification process. This is accomplished by associating camera video with these events to create what is called an **Event Rule**.

7.11.1 Events Toolbar

Buttons within the *Events* pane are defined as follows:

Resync		The *Ocularis Administrator* application polls the Ocularis Base SQL database at regular intervals. If, for whatever reason, you wish to manually synchronize event data from the database with *Ocularis Administrator*, click the **Resync** button in the Events Toolbar. SQL Server data updates should now be reflected on the screen.
Fuse New		Use this to create a new composite event. See *To Configure a Composite Event*.
Properties		Use this to modify the priority or audio file of a Composite Event or Simple Event Rules.
Delete		Use this to delete Composite or Generic Events. See Generic Events.
Batch Handle		Use the **Batch Handle Events** button to handle 'unhandled' alerts. See also: *To Batch Handle Events.*
Purge Closed		Use the **Purge Close** button to delete all closed events on the server. See also: *To Purge Closed (Handled) Events*.

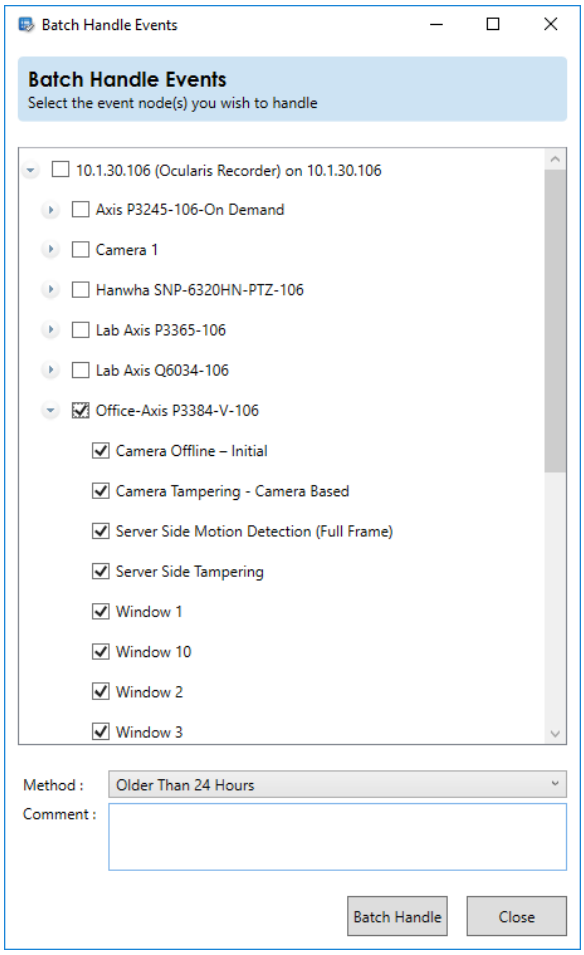
7.11.2 Batch Handle Events

As events occur and users are alerted in the *Ocularis Client*, operators "handle" the events. (See '*Handling Alerts*' in the *Ocularis Client User Manual*.) All 'unhandled' events eventually accumulate. Administrators may remove these events and place them in a 'Closed' status by using the **Batch Handle Events** button.

TO BATCH HANDLE EVENTS

1. In the **Servers / Events** tab, click the **Batch Handle Events** button.
   A *Batch Handle Events* pop-up appears.

Figure 33 Batch Handle Events



2. Expand the list of events as needed and select the events for whose unhandled alerts you wish to delete. You may get as granular as you like.
3. Choose the amount of events you wish to delete in the **Method** drop-down list. The selection choices are: **Older than 24 Hours**, **Keep only last 100 events**, **Clear everything!**
4. Enter optional comments. These comments will be visible when viewing the Handled Events in the *Ocularis Client Handled Events* list.
5. Click **Batch Handle** to handle these events.

You'll be able to see these in the Handled Alerts list in the *Ocularis Client*.

7.11.3 Purge Closed Events

When an event is handled in the *Ocularis Client*, it becomes a handled or "closed" event. The *Ocularis Administrator* application provides a means to delete all closed events. When administrators purge closed events they are deleted permanently.

TO PURGE CLOSED (HANDLED) EVENTS

1. In the **Servers / Events** tab, click the **Purge Closed Events** button.
   An "*Are you sure you wish to delete all handled events*" warning message appears.
2. Click **Yes** to purge these events.

7.12 Simple Event Rules

Simple Event Rules identify which events will be monitored on the system. An entry to the *Ocularis Client* Alert Manager will be recorded and, if configured, video may appear in a blank screen pane. Cameras are mapped to events that are system defined (such as motion on a camera) or user defined (such as a Generic or Composite Event).

Create a simple Event Rule by associating camera video with an event. Events which are mapped in the **Servers / Events** tab are system-wide. Administrators determine which users will get visibility to these events in the **Distribution Groups Tab**.

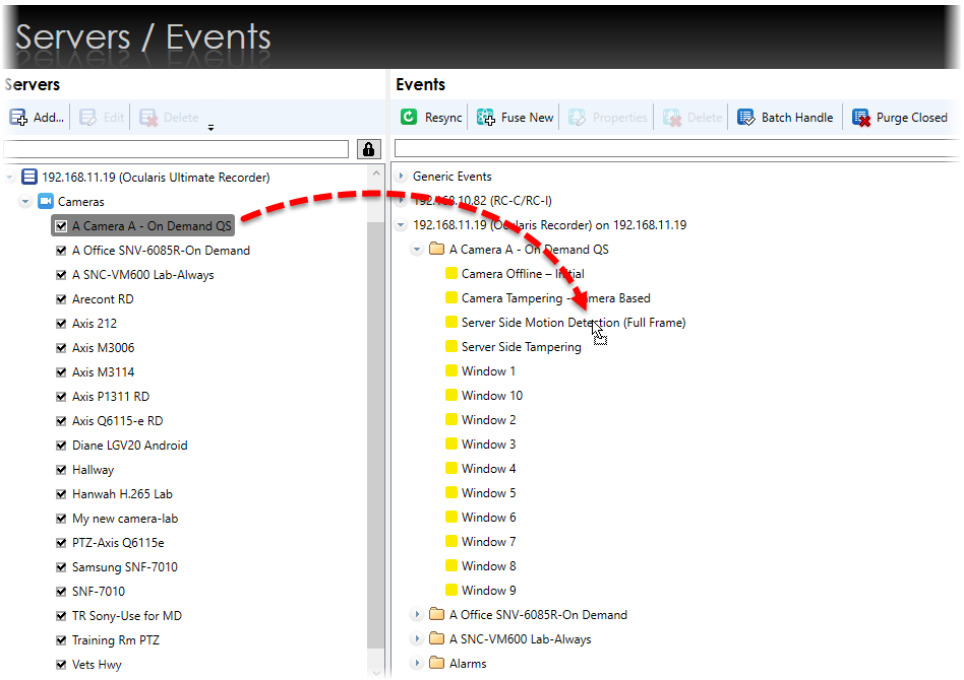
TO CREATE AN EVENT RULE (TO ASSOCIATE CAMERA VIDEO WITH EVENTS)

1. In the **Servers / Events** Tab, expand the **Cameras** list in the **Servers** pane for cameras you wish to associate with automated events.
2. Expand the list in the **Events** pane until you locate the event you would like to monitor.
3. For the desired event, drag & drop a camera name from the **Servers** pane to the event listed in the **Events** pane. (See Figure 34).

> ***Tip***: *If you want to associate the camera video to all events affiliated with that camera, drag & drop the camera name from the left Servers pane directly onto the camera name in the Events pane.*

When the camera video is successfully associated and an ***Event Rule*** is created, it appears in the collapsible list.

Figure 34 Drag & Drop to Associate Events



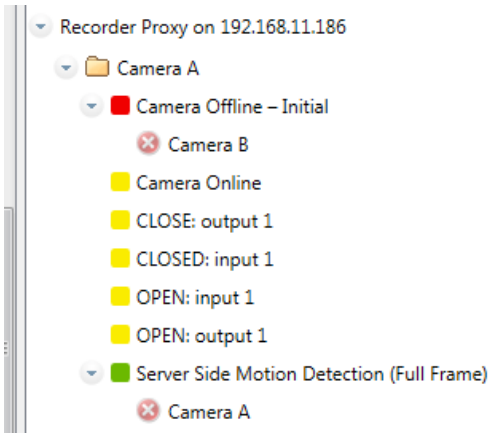
4. You may drag additional cameras to the same event for the event to have multiple camera associations.

Video generated by automated events will appear in a ***Blank Screen*** pane on the operator's *Ocularis Client* view. If multiple cameras are associated the an event, the cameras will appear in the blank screen as a carousel.

For the example shown in Figure 35, the events shown here are:

- If there is motion on Camera A, associate the camera feed from this same camera with the event.
- If Camera A is not responding, register an event and associate the feed Camera B with this event.

Figure 35 Associated Events



TO REMOVE A CAMERA FROM AN EVENT RULE (DISASSOCIATE A CAMERA)

1. In the **Servers / Events** Tab, expand the nodes in the **Events** pane until you see the Event Rule you wish to remove.

You can:

a. Click the ⊗ next to the camera name to disassociate it from the event.

b. Right-click on the associated camera name and select 'Delete'.

c. Right-click on the event source camera name and select 'Remove Camera Associations'. This will remove all event mapping on this camera.

d. Right-click on the event source label itself and select 'Remove Camera Associations'. This will remove all event mapping for all cameras on this recorder.

The camera mapping is removed.

7.13 Event Properties

For the events that you wish to monitor, you may define certain parameters related to the behavior of the alert. These properties apply to simple event rules, generic events or composite events. The properties are grouped into two sections:

- Alert
  - Priority
  - Audio
  - Handle In Client

- Retention
    - Max Events
    - Max Age
    - Max Frequency

7.13.1 Alert

In the Alert section, specific properties on the behavior and appears of the alert is set.

7.13.1.1 Priority

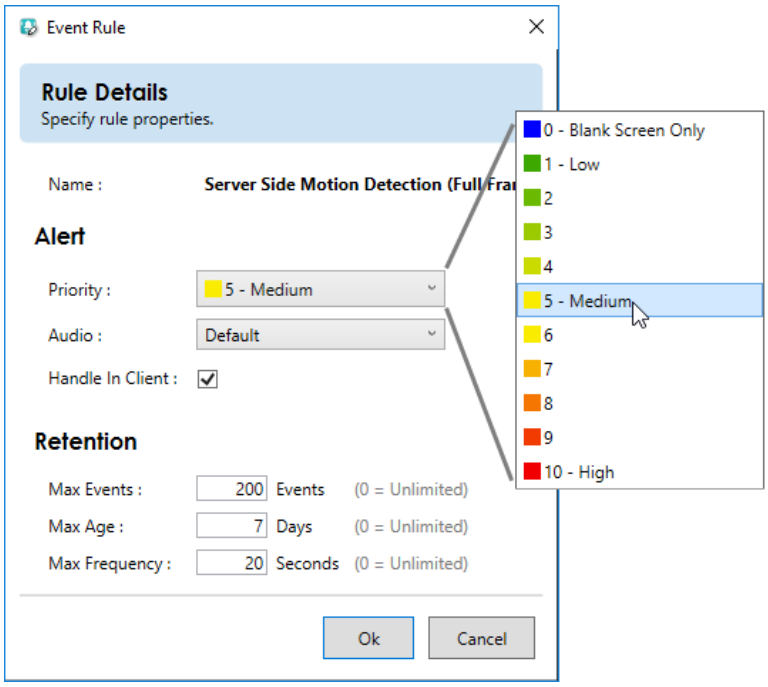
Events can be prioritized. For example: an organization may deem that the loss of video from camera 1 is critical but the loss of video of camera 7 is not. These priorities may be set by the system administrator. The priority of the event will dictate how it appears within the *Ocularis Client*.

By default, when an Event Rule is created, it is assigned a priority of 5 or *Medium*. Priority levels range from 0 – 10 where 10 is the highest priority

TO MODIFY THE PRIORITY OF AN EVENT

1. In the **Servers / Events** tab, expand the **Event Rule** in the **Events** pane whose priority you wish to change.
2. Select (highlight) the **Event** for the event rule (not the camera name).
3. Click the **Properties** button or double-click the event.
4. In the resulting **Event Rule** pop-up, select the desired priority level and click **Ok**.

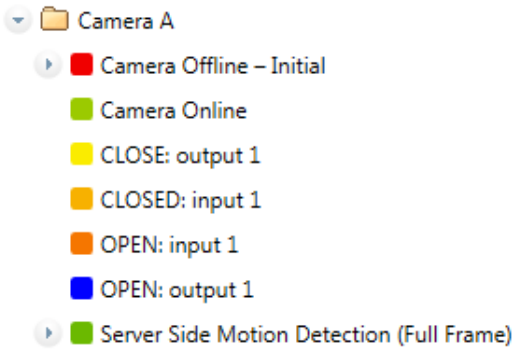
Figure 36 Event Rule Properties: Priority



Event priorities are identified in *Ocularis Administrator* and in *Ocularis Client* by color.

Priority Level	***Color Shade***	***Priority Level***
0	Blue	None
1-3	varying shades of green	Low
4-6	varying shades of yellow	Medium
7-10	varying shades of red	High

Figure 37 Priorities Color Coding sample in Ocularis Administrator



Event priorities work hand-in-hand with the *Blank Screen Only/Handle In Client* option. Priority levels determine different behavior of the alert.

7.13.1.2 Audio

When an event occurs, the subsequent alert can play a sound file through the Ocularis Client as an added attention getting mechanism. The sound played can be configured by the system administrator. The same sound can be played for all alerts or configured on an alert by alert basis. A default audio setting is available. Sounds are not required and a 'no sound' option is also supported.

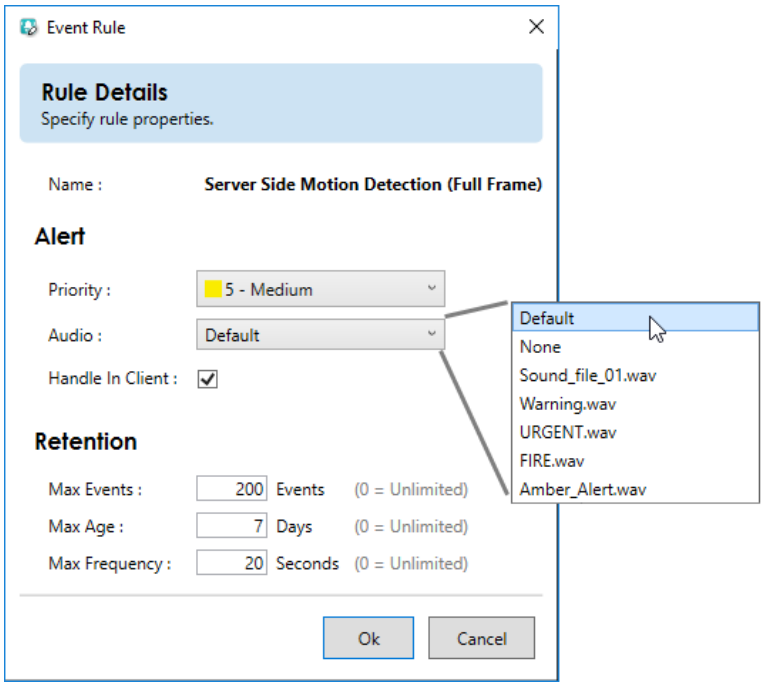
Audio files are imported in the **Assets** Tab where the default audio file is set. See ***Event Audio Clips*** on page 145 for more information on sound file configuration.

***Note**: If you are using audio alerts with Ocularis Web, the redalert.wav file will be played regardless of which sound file is selected here. This sound file will be played in Ocularis Client.*

TO MODIFY THE AUDIO OF AN EVENT

1. In the **Servers / Events** tab, expand the **Event Rule** in the **Events** pane whose sound you wish to change.
2. Select (highlight) the **Event** for the event rule (not the camera name).
3. Click the **Properties** button or right-click the event and select **Properties**.
4. In the resulting **Event Rule** pop-up, from the Audio drop-down, select the desired sound file, **None** or **Default**.
    - If you click 'None', no sound file will be played when the event occurs. If there is no option available labeled 'None', then 'None' must already be set as the default option. Select 'Default'.
    - If you select a .wav file, that sound will play through the Ocularis Client when the event occurs.
    - If you select 'Default', you may get a sound file or no sound, depending on the default setting in the **Assets** tab. In the event where 'None' is configured as the default audio in the **Assets** Tab, the option 'None' will not be visible in the drop-down list. In this case, selecting 'Default' is equivalent to selecting 'None'. You should be aware of the default audio setting in the **Assets** Tab when configuring events.
5. Click **Ok**.

Figure 38 Event Rule Properties: Audio Samples



7.13.1.3 Handle In Client

The 'Handle In Client' checkbox allows administrators to control which alerts they want their operators to acknowledge in Ocularis Client and which need not. In other words, if the Handle In Client checkbox is checked (or on), the alert will appear in the Alert Manager (i.e. list of unhandled alerts) when the event occurs until such time that the alert is handled (or login session has ended). The alert counter will increment for each alert. If the checkbox is not checked (or off), the alert will be shown on a Blank Screen pane (if one is displayed) and then disappear when cleared or when the dwell time is reached.

Priority 0 An alert with a Priority 0 is one where video from associated cameras will be displayed on a blank screen only. No additional data is kept or logged for these alerts. Priority 0 is used when you only want to see an event posted to a blank screen but then no longer need to monitor it. Therefore, if there is no blank screen displayed, you won't see a priority 0 event. The alert counter will not increment for alerts with this priority. By default, when you select Priority 0, the 'Handle in Client' checkbox is unchecked. This means that the event will not be logged into the database.

Priority 1-6 Alerts with Priority 1-6 are categorized low or medium. By default, these alerts will be shown on a blank screen (if one is visible) and be shown in the Alert Manager

list of unhandled events until the event is handled (or the session ends). The video in the blank screen will clear after the configured dwell time for the pane in the view has been reached. If the 'Handle In Client' checkbox is unchecked, the alert will NOT appear in the Alert Manager.

Priority 7-10 Alerts with Priority 7-10 are considered high priority alerts. These alerts behave like the priority 1-6 alerts in that by default, they are to be acknowledged by operators using Ocularis Client. What can makes these priority alerts different (other than their color representation), is that if configured properly they remain on-screen in blank panes until acknowledged by an operator or until another alert with the same or higher priority appears. For this behavior, the 'Handle in Client' checkbox must be checked.

7.13.2 Event Retention

Depending on the environment, the types and number of events monitored, the amount of events can quickly build up in the system. The database can be overcome with too many events. The operator's blank screen panes may also be cluttered by repetitive or too many events. Therefore, system administrators have the ability to limit the events that are stored and retained in the database and shown on a blank screen. These parameters are found when configuring an event rule (basic, generic or composite).

7.13.2.1 Max Events

This field holds the total count of event instances to save to the database for the event rule. For instance: if this value is set to 10 for a motion event on Camera A, then only 10 motion events for Camera A will be in the database at any given time. Once 10 events have accumulated and new events occur, the oldest event will be deleted and the newer event will be stored. Valid values are between 0 (the default which means unlimited) and 2,147,483,647. The default setting is 200. Keep in mind that this field works in conjunction with 'Max Age' and 'Max Frequency'.

7.13.2.2 Max Age

The 'Max Age' for an event rule is the number of days (in 24 hour multiples) in which to store events generated by the event rule. The time is calculated from when the event took place. For instance: if this value is set to 7 for a motion event on Camera A, then each of Camera A's motion events will be deleted ('expire') 7 days or 168 hours after they take place. The value is measured in days between 0 (unlimited and the default value) and 2,000. The default setting is 7 days. Keep in mind that this field works in conjunction with 'Max Age and Max Events'.

7.13.2.3 Max Frequency

This field identifies the time interval in seconds in which you would like to monitor alerts. This feature will reduce the amount of repeated alerts within a specified timeframe.

For instance, if the Max Frequency is set to 10 (seconds) for a motion event on Camera A and then motion occurs:

1. the timer is theoretically set to zero and the clocks starts. The event is registered in the Alert Manager and sent to the Operator's blank screen pane.
2. If the same motion event on camera A occurs again in the next second, nothing will happen.
3. If the same motion event on camera A occurs again in the second after that, nothing will happen.
4. If the same motion event on camera A occurs again for the next 8 seconds, nothing will happen.
5. At the 11th second, if the motion event on Camera A occurs, register the event in the Alert Manager, display it on the Operator's blank screen pane and reset the timer to zero.

The value is measured in seconds between 0 (unlimited and the default) and 3600 (one hour). The default setting is 20 seconds. Keep in mind that this field works in conjunction with 'Max Events' and 'Max Age'.

7.13.2.3.1 Event Properties Combined

Keep in mind that three event properties work in combination with each other. The 'Max Events', 'Max Age' and 'Max Frequency' all affect the amount of events that are stored and the duration of their storage.

***Note**: The default values for retention properties were modified in version 5.6 to promote system performance. These values will take effect for new events. Existing events will retain their current settings.*

7.14 Composite Events

A *Composite Event* (also called 'Event Fusion") is combination of two other events defined with a specific relationship and timeframe. The following are examples of a composite event:

If there is motion on Camera 1 and within the next 5 seconds
there is motion on Camera 2, register an event

or

If there is a card swipe detected from an access control panel AND there is an analytic event that determines two people entered ("tail-gating"), trigger an alert

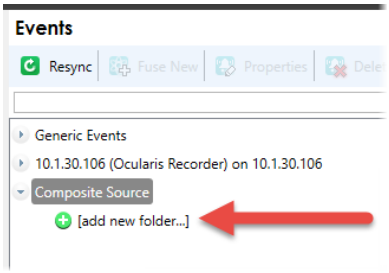
Composite Events are supported by all models of Ocularis.

TO CONFIGURE A COMPOSITE EVENT

1. In the **Servers / Events** tab, create a Composite Sensor folder by clicking '[add new folder…]

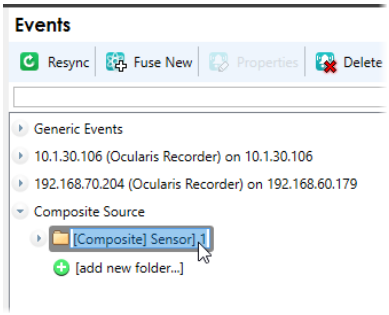
   You may add as may folders as desired to organize your composite events.

Figure 39 Add Composite Event Folder



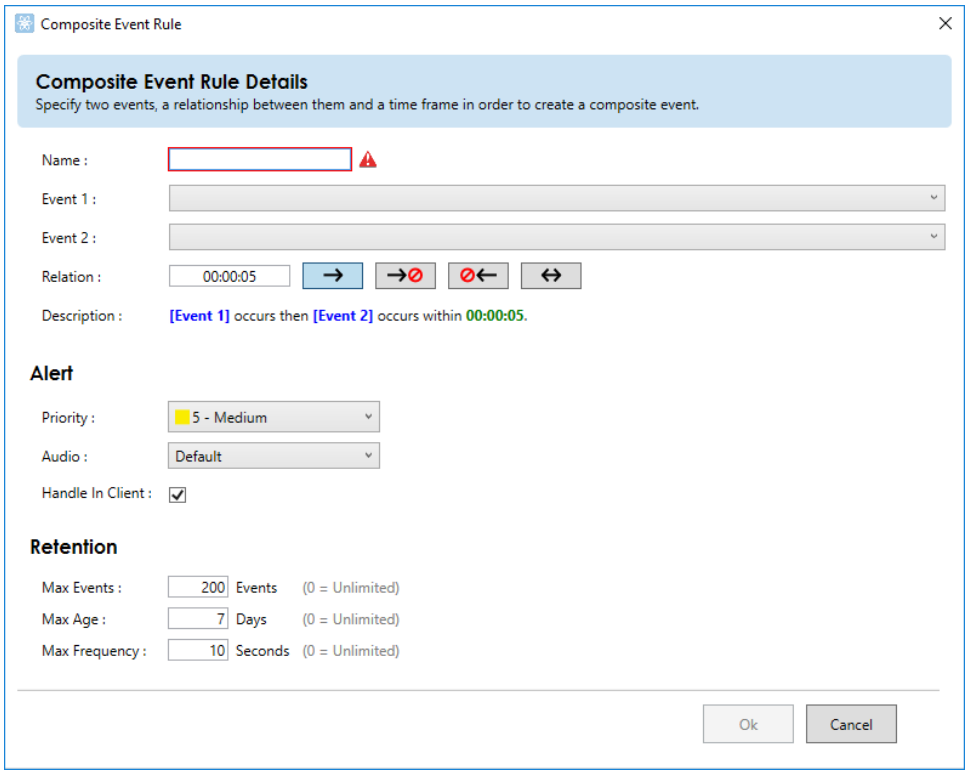
2. If you want to rename the folder now or at a later time, double-click it and replace the text. Then press [ENTER].

Figure 40 Rename Composite Event Folder



3. To create the event either click the **Fuse New Event** button on the toolbar, or expand the folder you just created and click '[add new..]'.
4. Fill out the **Composite Event Rule** pop-up.

Figure 41 Configure a Composite Event: Rule Details Tab



Fields are defined as follows:

Item	Description
Name	Enter a descriptive name for the composite event. Avoid using special characters for the event name.
Event 1	Select an event to begin to define the condition for which the rule alert should be met. This event may be an Event Rule, Generic Event, another composite event or any event listed.
Event 2	Select a second event to finalize the condition for the composite formula. This event may be an Event Rule, Generic Event or another Composite Event.
Relationship	You must indicate how event 1 is related to event 2. The directional arrows define the relationship between two Event Rules and are defined below. In addition, a time period must be specified. This works in conjunction with the relationship icons in identify a time limit that may apply to the relationship. Valid times are: HH = 0 through 23 MM = 0 through 59 SS = 0 through 59
Description	As you build your composite event, a description appears in this section helping you understand rule's meaning.

Item	Description
Priority	Select a Priority for the composite event. See *Alert* In the Alert section, specific properties on the behavior and appears of the alert is set. Priority on page 49 for more information about priorities.
Audio	Select the sound file to be played when the composite event occurs. See *Audio* on page 51 for more information about audio.
Handle In Client	If this checkbox is checked (on), Ocularis Client will receive a registry entry for the event and (depending on priority) may require the operator to manually acknowledge the alert. See *Handle In Client* on page 52 for more information.
Max Events	Set the maximum number of event registries to retain for this composite event. See *Event Properties* on page 48 for more information.
Max Age	Set the maximum age to save event registries for this event. See *Event Properties* on page 48 for more information.
Max Frequency	Set the frequency for this event. See *Event Properties* on page 48 for more information.

Relationship Icons

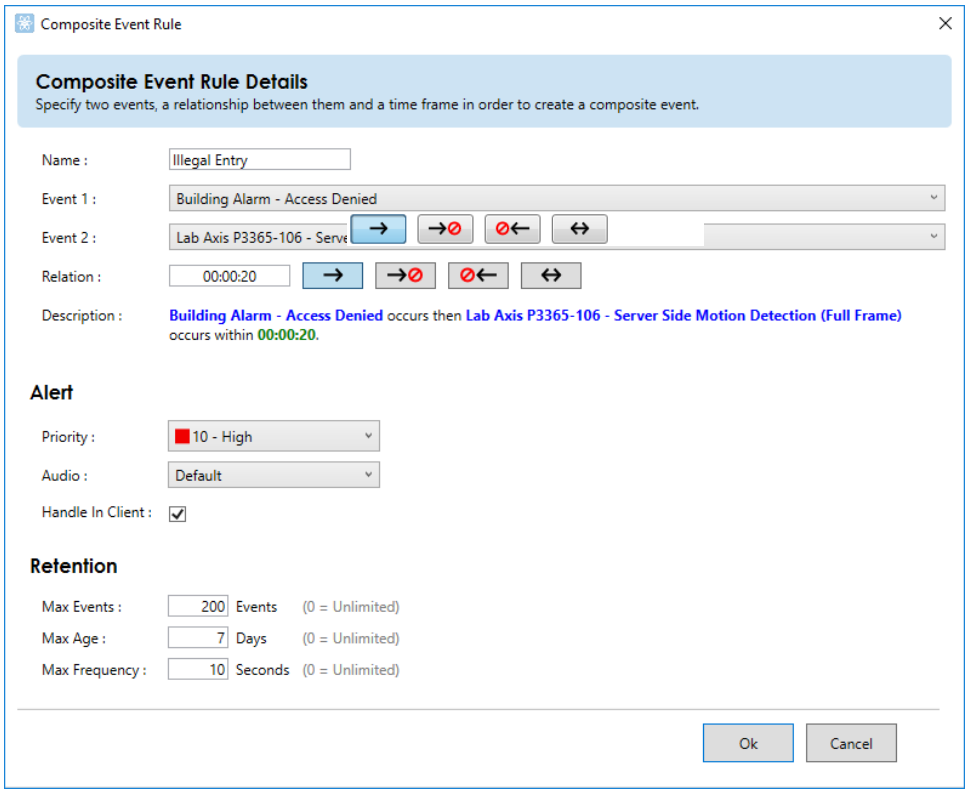
	If Event 1 occurs **before** Event 2 occurs
	If Event 1 occurs but Event 2 does not occur within the specified time period
	If Event 1 does not occur in the time period defined, prior to Event 2 occurring.
	If Event 1 and Event 2 occur within the time period specified.

Please note:

- You may effectively nest composite events with other composite events resulting in a highly complex fusion of events. Consider, however, that the more complex an event, the more difficult troubleshoot may become.
- If you do not see a recently created generic event in the list of available events in the Event1 or Event2 drop-down list, click the **Resync** button to refresh the Events pane.

Refer to the example shown in Figure 42: This composite event will trigger an alert if there is an Access Denied code registered from the building alarm system and 20 seconds later there is motion on the lab camera (indicating that someone has gained illegal access).

Figure 42 Composite Rule Example



TO MODIFY A COMPOSITE EVENT

1. In the **Servers / Events** tab, locate the Composite Event in the **Events** pane under the Composite Source node.
2. Highlight the Composite Event.
3. Click the **Properties** button.
4. In the resulting *Edit Composite Event* pop-up, modify desired settings.
5. Click **Apply** to save changes.

TO DELETE A COMPOSITE EVENT

1. In the **Servers / Events** tab, locate the Composite Event in the **Events** pane under the Composite Source node.
2. Highlight the Composite Event.
3. Click the **Delete** button.
4. You will be prompted with the message: *"Are you sure that you want to delete this composite event rule?"*
5. Click **Yes** to delete the Composite Event.

7.15 Generic Events

Ocularis Base has the ability to analyze TCP or UDP data packets and automatically trigger an alert when specified criteria are met. This expands event coverage to external devices such as access controls systems. These events are called *Generic* events. Generic events may be used in Blank Screen monitoring and they are supported by all models of Ocularis.

7.15.1 Components of a Generic Event

Generic Events are made up of *Connections* and *Rules*. Connections define the protocol and port which Ocularis should monitor and a

nalyze for the event. This is considered the *event source*. Rules allow you to define the actual string that should be used in the analysis of the event source. You may have multiple rules defined for the same connection and these rules may also be used in Composite Events.

TO CREATE A GENERIC EVENT

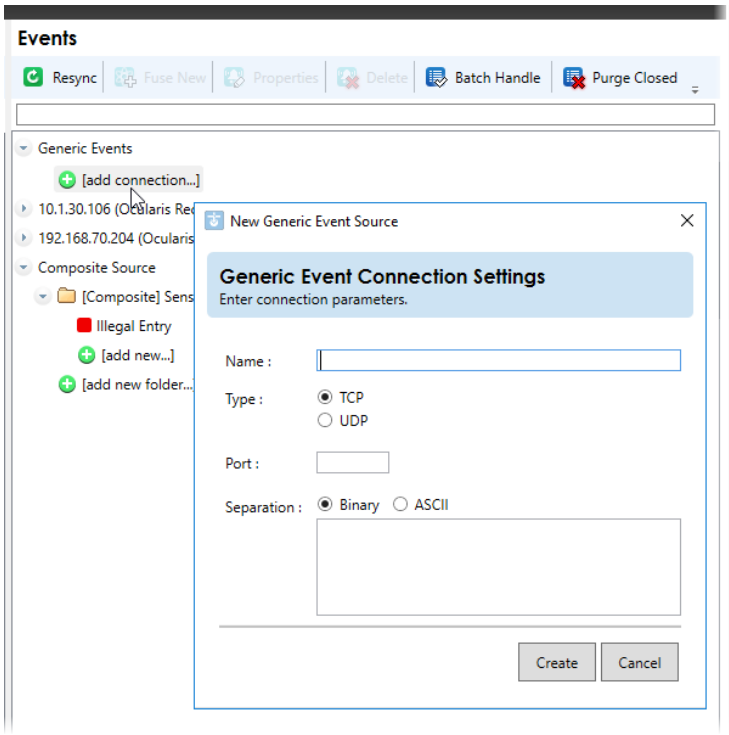
Creating a Generic Event involves these steps:

- Create a Connection to define the event source.
- Define at least one rule for the Connection.
- Test the Rule
- Map camera video to the rule to enable it and allow for Blank Screen monitoring.

TO CREATE A CONNECTION FOR A GENERIC EVENT

1. In the **Servers / Events** tab, expand the *Generic Events* node in the **Events** pane.
2. Click **[add connection..]**

Figure 43 Add a Generic Event Connection



3. Fill out the fields in the resulting *New Generic Event Source* pop-up window as defined below. You may need to contact or review the manufacturer specifications of the device for which you are configuring the event.

Item	*Description*
Name	Enter a descriptive name for the Event Source. This is what will appear in the alert so be as descriptive yet concise as possible. Avoid using special characters in this name. For example: *Front Entrance* might be used to describe alerts transmitted access control systems on the main door to the facility.
Type	Select the protocol (**TCP** or **UDP**) based on the device you are monitoring.
Port	Enter the port on which Ocularis Base should listen for the data sent by the event source.
Separation	Select the format for data transmission. (**Binary** or **ASCII**) You may also enter a Separation character to identify to Ocularis Base, when an end of string as been received. Enter this character in the Separation field.

4. When pop-up is complete, click the **Create** button.

The Connection for the event source should be listed under *Generic Events* in the **Events** pane.

To Define a Rule for a Generic Event Connection

Be sure to first define an event source prior to defining a rule. See *To Create a Connection for a Generic Event* on page 59.

1. In the **Servers / Events** tab, expand the Generic Events node in the **Events** pane and select the desired generic event.
2. Expand the generic event connection source.

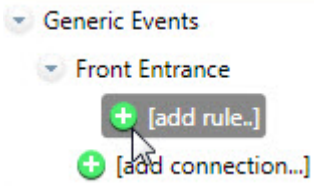
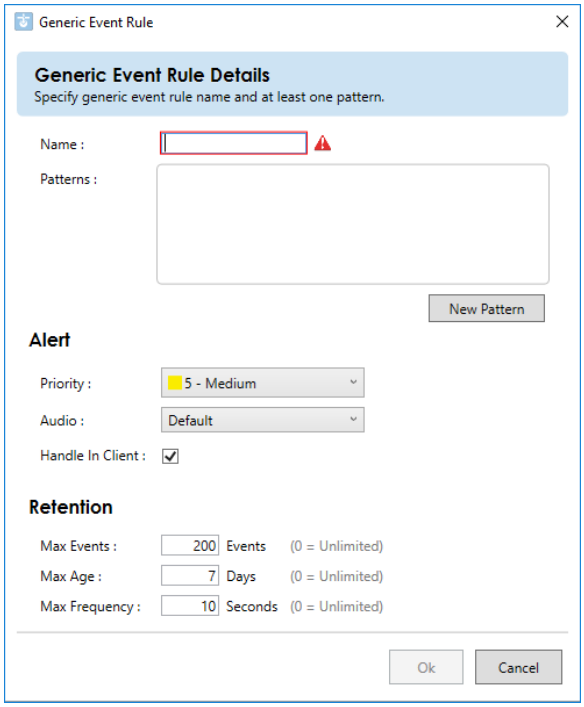


Figure 44 Click [add rule…] to configure the generic event connection

3. Click **[add rule..]** beneath the event.

Figure 45 Creating a Generic Event Rule



4. In the resulting pop-up window, fill out the fields as follows:

Item	Description
Name	Enter a descriptive name for the rule. Avoid using special characters in the name field. Following our earlier example, the name could potentially be something like: *Access Denied* or *Access Granted*.
Patterns	Click the **New Pattern** button to open up a row for pattern definition. See Patterns for Rules below for more information.
Priority	Assign a priority for the rule. See *Event Properties* on page 48 for more information on event priorities.
Audio	Select an sound file to play when the event occurs. This selection is optional. See *Event Properties* on page 48 for more information on event audio.
Handle In Client	If this checkbox is checked (on), Ocularis Client will receive a registry entry for the event and (depending on priority) may require the operator to manually acknowledge the alert. See *Handle In Client* on page 52 for more information.
Max Events ***Max Age*** ***Max Frequency***	Set the retention parameters for this event. See *Event Properties* on page 48 for more information on event retention.

5. Click **OK** when done.

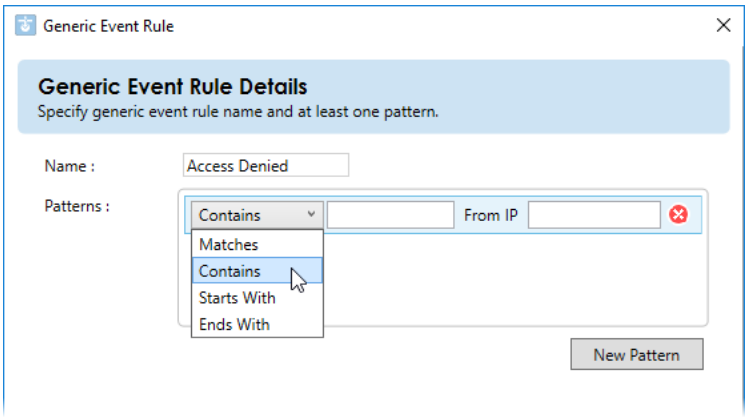
You may define multiple rules for the same generic event connection.

7.15.2 Patterns for Rules

When specifying the logic for Ocularis Base to use when analyzing data packets you have several options. You must know the string or a portion thereof that you wish to look for in order to trigger the event. The options for searching for the string are as follows:

Item	Description
Matches	The string you specify must be detected in its entirety with exactly the characters you specify.
Contains	The string you specify can be located anywhere within the string of the data packet.
Starts With	The data packet must begin with the string you specify.
Ends With	The data packet must end with the string specified.

Figure 46 Patters for Generic Events

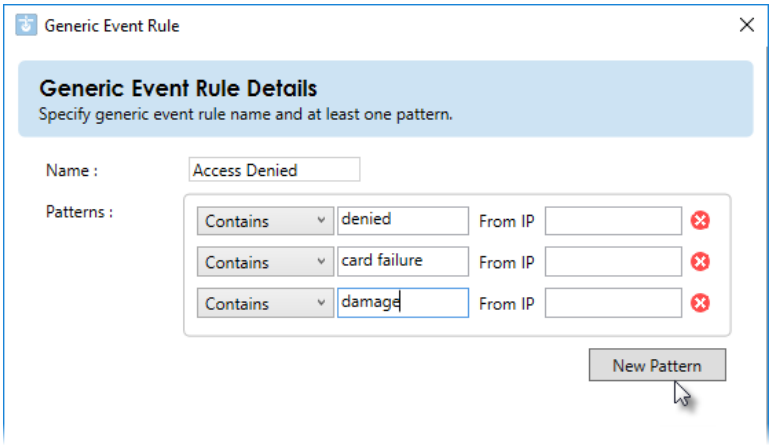


Sources for Patterns

For each string to be analyzed on a specified port, you can also limit the analysis to be from a specific IP address. For TCP based connections, enter the IP address for the pattern for which you wish to restrict analysis in the **From IP** field. This is an optional field. If left blank, the pattern will be evaluated on any IP address.

You may include multiple patterns for the same rule. The Boolean logical operator “OR” will be applied for each.

Figure 47 Using Multiple Patterns



Click the **New Pattern** button to add a row to configure each pattern.

In the example shown in Figure 47, the following generic event is configured: “if the text string ‘access denied’ or ‘card failure’ or ‘damaged’ appears within the specific port of the connection, trigger the *Access Denied* Rule. (the port is configured with the connection).

TO MAP THE RULE

Once the rule has been created, you may associate video from a camera to this event. Do this by dragging and dropping the camera from the *Servers* pane to the Generic Event on the *Events* pane. Follow the same steps as discussed in *To Create an Event Rule (To Associate Camera Video with Events)* on page 46.

7.15.3 Determine Alert Distribution

Configuring alerts for events does not automatically activate them. Additional steps are needed to assign who should receive notification for which alert and when. Administrators determine which users will get notification of associated events in the **Distribution Groups Tab**. This step needs to occur in order to see alert video, to transfer alerts from Ocularis Base to Ocularis Client operators or to test a Generic event.

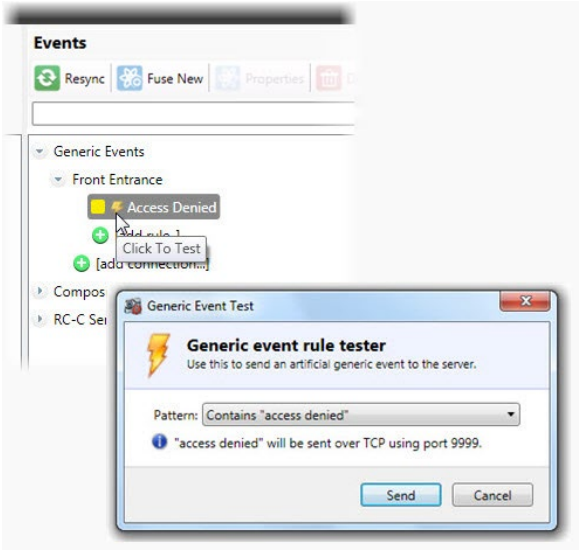
TO TEST THE GENERIC EVENT

You can perform a manual test of the Generic event to determine if it is properly configured.

1. In the **Servers / Events** tab, expand the Generic Events node in the **Events** pane to expand it and select the Generic Event.
2. Expand the Connection by clicking the expand symbol next to it.
3. Click the lightning bolt symbol adjacent to the rule name.

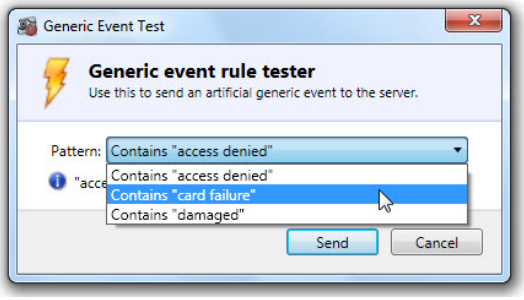
   A *Generic event rule tester* pop-up appears.

Figure 48 Testing Generic Events



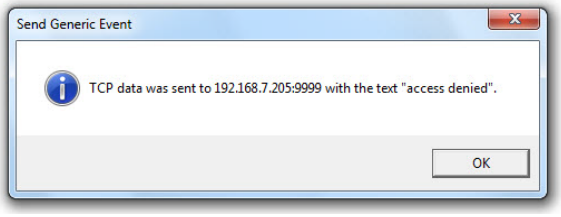
4. You can select any pattern associated with the event from the drop-down list to test.

Figure 49 Selecting a Pattern to Test



5. Click **Send**.

Figure 50 Generic event test data sent confirmation

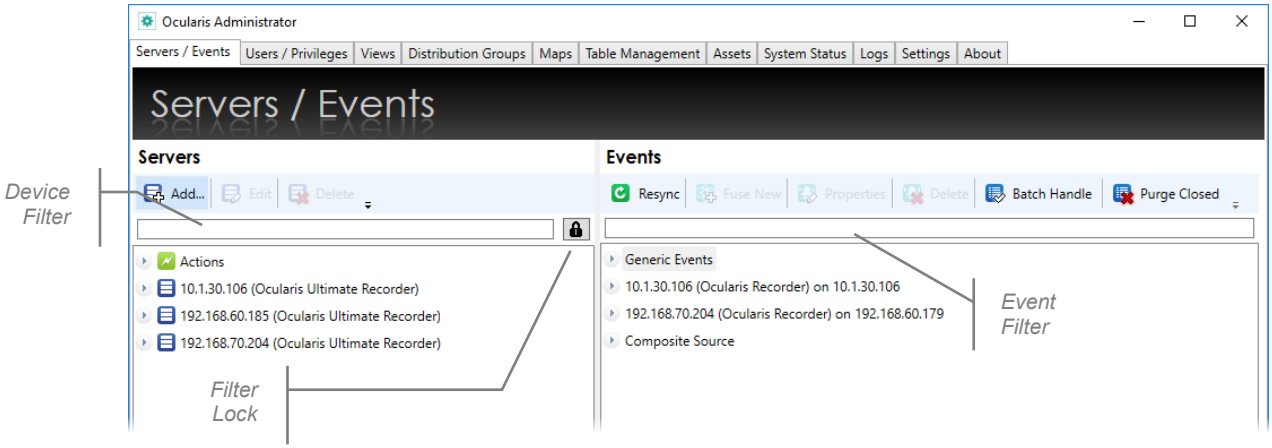


A test event will be generated and sent based on configured rules.

7.16 Device Filter / Event Filter

As the system grows and more and more cameras and devices are added, it can take some time to locate the desired device amongst the list of hundreds or even thousands of devices. The same applies to events. If there are dozens or hundreds of events, it can be cumbersome to try to locate a specific event. To alleviate this, a 'Device Filter' and 'Event Filter' are available from the **Servers / Events** Tab.

Figure 51 Device and Event Filters

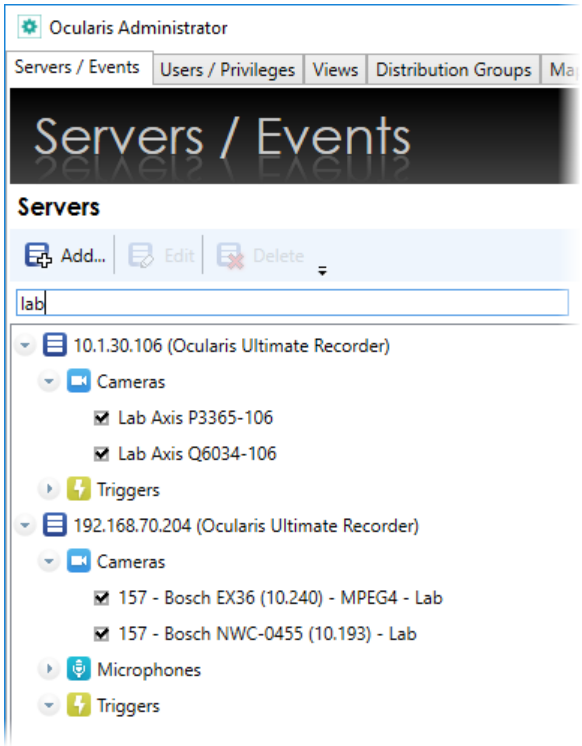


7.16.1 To Use the Device Filter

1. From the **Servers / Events** tab, type a portion of a string to filter the device list in the 'Device Filter' text box. The string can contain letters, numbers or special characters. The filter is not case sensitive. The resulting list will be an exact match of the content typed into the Device Filter text box.

   For instance, in Figure 52, the filter is for all 'lab' devices.

Figure 52 Filter for 'lab'



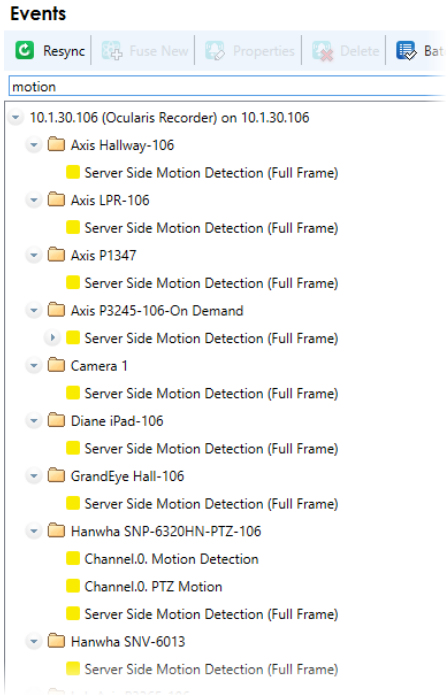
You may clear the filter by deleting the text in the Device Filter text box.

7.16.2 To Use the Event Filter

1. From the **Servers / Events** tab, type a portion of a string (or keyword) to filter the event list in the 'Event Filter' text box. The filter is not case sensitive.

   The list will display only those events whose name includes the text typed. For instance, in Figure 53, the filter is for all events related to 'motion'.

Figure 53 Event Filter for 'fire'



7.17 Filter Lock

You may use the 'Filter Lock' icon to lock the filter. This will disable the 'Event Filter' text box from accepting entries and allow the 'Device Filter' to filter both devices and events. This makes locating events related to a particular device quick and easy.

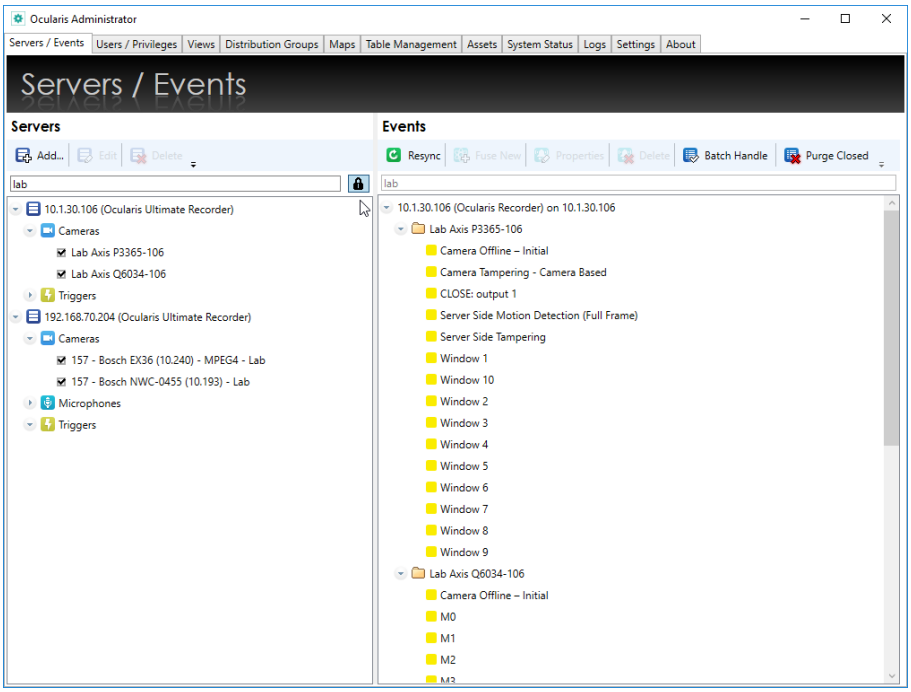
7.17.1 To Use the Filter Lock

1. From the **Servers / Events** tab, first type a portion of a string to filter the device list in the 'Device Filter' text box. The filter is not case sensitive.
2. Click the 'Filter Lock' icon.

The filter text from the ‘Servers’ list is now applied to the filter of the ‘Events’ list. The filter will apply to both panes.

For instance, the sample shown in Figure 54 shows the Device Filter and Event Filter for all ‘Lab’ cameras and associated events.

Figure 54 Filter for 'Lab' cameras and events



7.18 Camera Migration Tool

As you know, when you add a recorder to Ocularis Base, additional configuration is required. This includes (but is not limited to):

1. Assigning privileges to the cameras to the applicable user groups
2. Creating views using the newly added cameras and
3. Adding the newly added cameras to maps.

These steps are required whether you install a new recorder or if the new recorder is replacing an existing recorder such as the case when you migrate cameras from version 4 Ocularis to version 5.

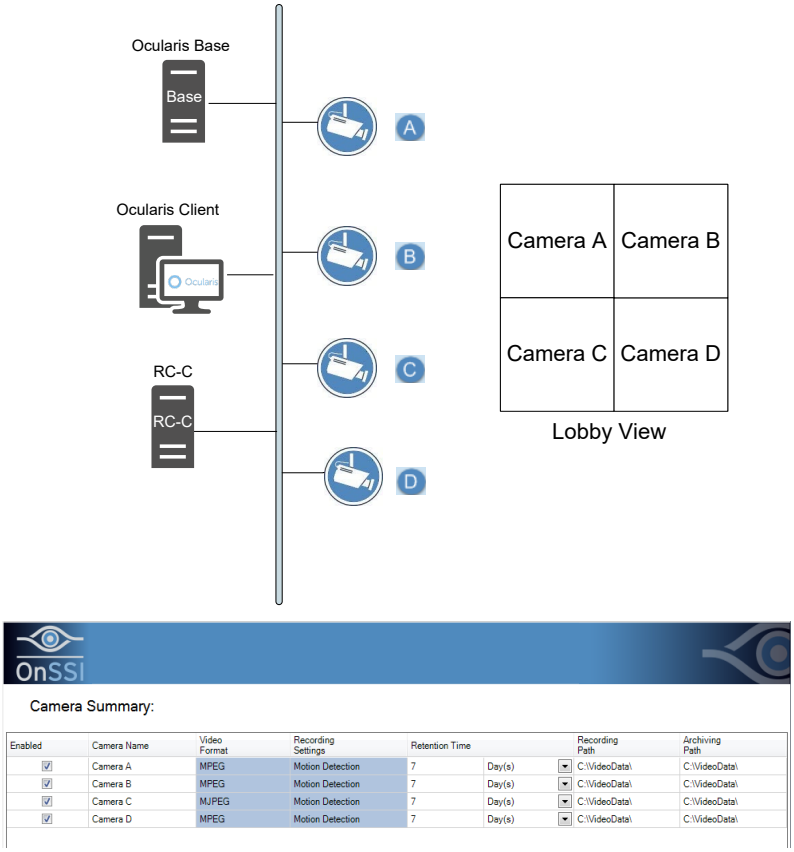
Keep in mind that with Ocularis Mix and Match you may still incorporate older version recorders with a version 5 Base. In fact, Ocularis 5 is compatible with all current and prior recorders.

However, in the event that you do want to migrate cameras from a prior version to an Ocularis 5 recorder, we have implemented a tool to help in this process.

The **Camera Migration Tool** in *Ocularis Administrator* allows you to easily replace one camera with another in all instances where the camera is used in Ocularis Views and Maps, saving the time and effort to reconfigure the system. You can even replace an entire recorder!

Note: this feature is available only to the **admin** user. Group Administrators do not have access.

Figure 55 Sample Cameras from an RC-C Recorder



7.18.1 How It Works

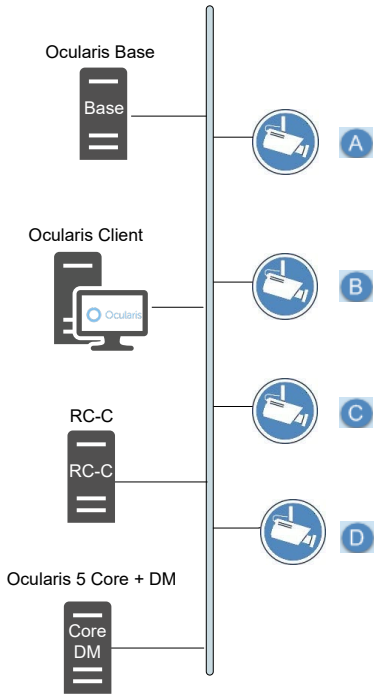
In the example shown in Figure 55, four cameras are located on an RC-C recorder labeled 'Camera A', 'Camera B', etc. They are used in a view called 'Lobby View' as shown.

If you want to migrate these cameras to a v5 recorder, install the same four cameras on a version 5 recorder. You can name the cameras with the same name or different names. Temporarily, both cameras will stream to two recorders.

Figure 51 shows an added Enterprise recorder. The camera names were assigned 'ENT Camera 1', etc.

After adding the v5 recorder to Ocularis Administrator, you can map the Enterprise cameras to their RC-C counterparts.

Figure 56 Added v5 recorder



ENT Camera 1 is mapped to Camera A

ENT Camera 2 is mapped to Camera B

ENT Camera 3 is mapped to Camera C

ENT Camera 4 is mapped to Camera D

When the mapping is complete, the 'Lobby View' will automatically be updated[1].

ENT Camera 1	ENT Camera 2
ENT Camera 3	ENT Camera 4

Lobby View

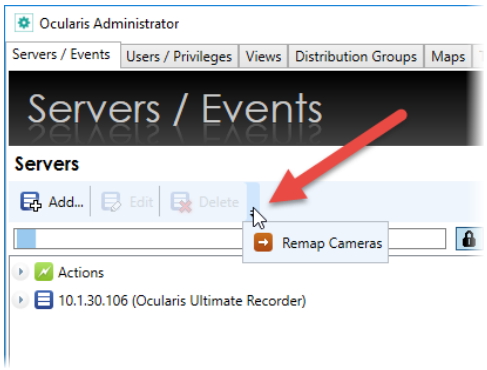
If the names of the cameras are identical from one server to another, you can save time by mapping one server to another server. The system will map all matching camera names to their corresponding counterpart.

[1]Mapping changes are not reflected in *Ocularis Client* until the next time the operator logs off and then back on.

To Use the Camera Migration Tool

1. After logging in to *Ocularis Administrator* using the **admin** account, from the **Servers / Events** tab, click the arrow adjacent to the **Delete** button in the Servers pane.

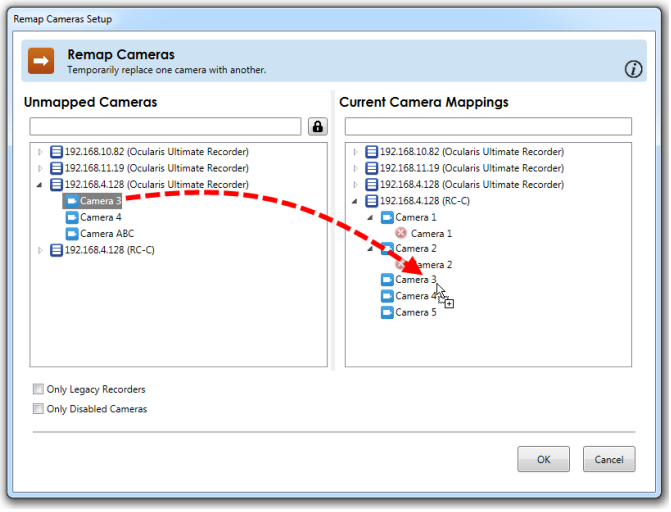
Figure 57 Remap Cameras



Then click **Remap Cameras**.

2. In the resulting pop-up, expand the new recorder on the left side of the screen and then expand the recorder that is being replaced on the right side of the screen.
    - You can use the filter entry box to filter the list by camera or server name
    - Check the 'Only Legacy Recorders' if you want to filter the list on the right by Ocularis v4.x and prior servers
    - Check the 'Only Disabled Cameras' to filter the list by disabled cameras
3. Then you can identify which camera on the right is being replaced with its corresponding camera on the left. You can:
    a. Drag and drop cameras one at a time

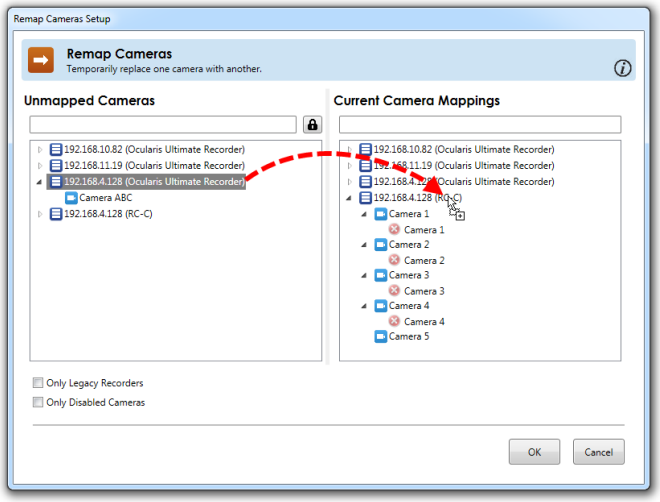
Figure 58 Drag and drop individual cameras



As cameras are mapped, they are removed from the 'Unmapped Cameras' list to prevent duplicate mappings. Also, you may not map a camera to itself.

b. Drag and drop from one server to another.

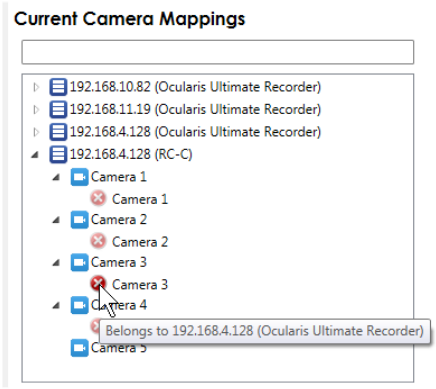
Figure 59 Drag and drop server to server



Notice that in Figure 54, the system was unable to find a match for 'Camera ABC'. In this case, the camera can be mapped individually to its corresponding camera.

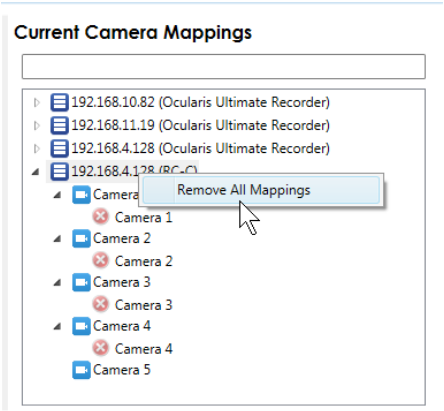
4. If you need to remove a mapping, click the red X as shown below. Also notice that the tool tip identifies the server to which camera the camera belongs.

Figure 60 Remove a single mapping



5. To remove all mappings on a server, right-click on the server name itself and select **Remove All Mappings**.

Figure 61 Remove All Mappings for a Server



6. When finished, click **OK**.

Now, everywhere the mapped camera is used in a View or on a Map, Ocularis will now display the newly mapped camera. This saves you from having to reconfigure the newly added recorder's cameras from scratch.

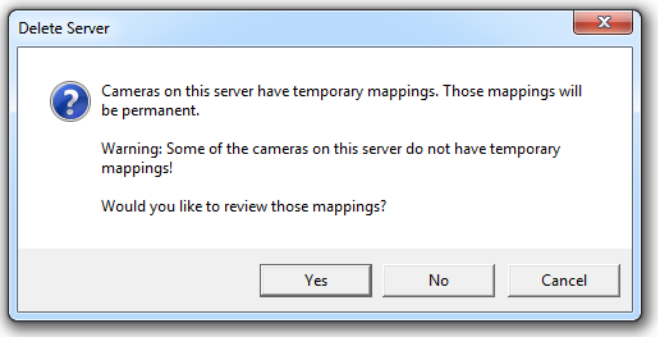
Keep in mind that the mapping is temporary until you remove the old server from *Ocularis Administrator*. Then the mappings will become permanent.

TO MAKE TEMPORARY MAPPINGS PERMANENT

To make temporary mappings permanent, delete the server from the **Server / Events** tab.

1. From the **Servers / Events** tab, right-click the server name you wish to remove.
2. Select **Delete Server**.
3. You will see an 'Are you sure you want to delete...' pop-up message. Click **Yes**.
4. You will then see the following warning:

Figure 62 Delete Server warning message



If all cameras are mapped, the second line will not display.

5. Click:
    a. **Yes** to review the mappings in the *Remap Cameras* pop-up. When you are done reviewing, click **OK** to continue with the deletion operation. Then, you will get a second warning message. Click **Yes** to remove the recorder and make the mappings permanent.
    b. **No** to skip the review , remove the server and make the mappings permanent.
    c. **Cancel** to abort the operation.

***Note**: Keep in mind that you must have an adequate supply of camera licenses for the level of recorder you map to when you make mappings permanent. For example: if you map 50 Enterprise cameras to 50 RC-I cameras, once you make the mappings permanent, you'll need to be sure that you have 50 valid ENT licenses (RL-2).*

8 Users / Privileges Tab

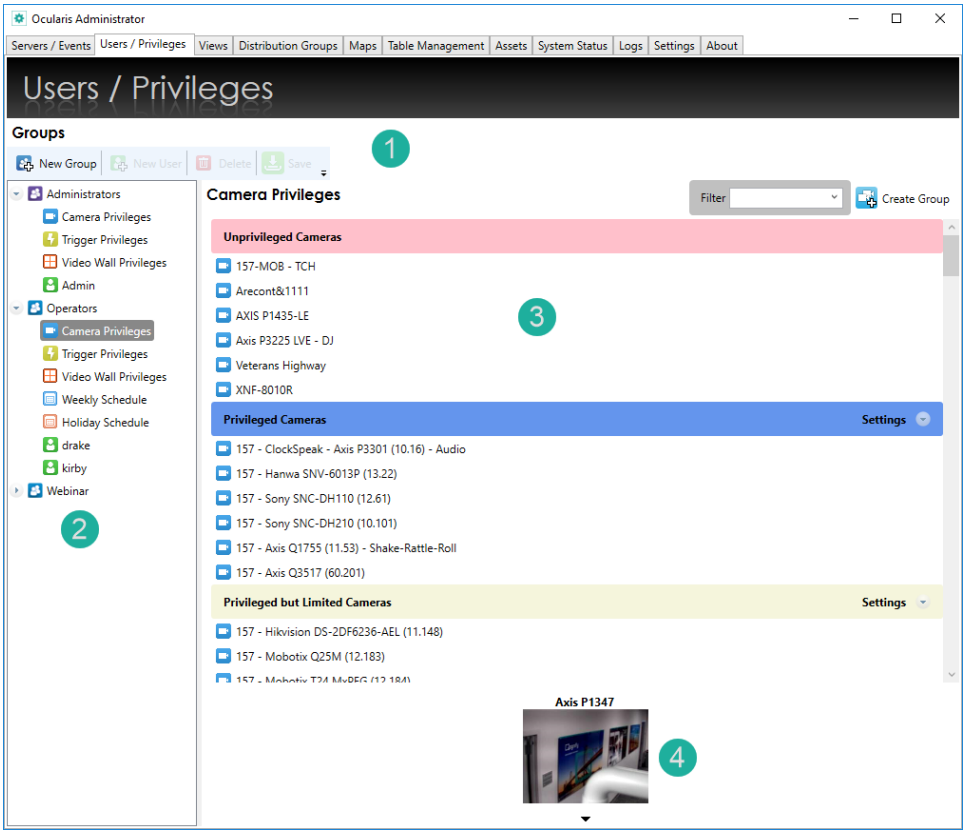
This tab is used to define users, user groups and camera privileges within an Ocularis system.

The Ocularis User Group/User Hierarchy

Access to the Ocularis surveillance environment is controlled through the use of **User Groups** and **User Accounts**. User Groups are assigned access and privileges to various components of the system. An example would be to assign a specific set of cameras or video wall to a user group. Once a group's operating parameters are established, user accounts can simply be assigned to the group and inherit the privileges of the group. Furthermore, each user account within a group (except 'Administrators' group) may have alternative privileges set beyond those of the group.

Privileges to cameras may be controlled through *camera privilege groups*. These groups allow you to organize a set of cameras *per user group* and apply specific parameter restrictions to the camera group as a whole.

Figure 63 Users / Privileges Tab

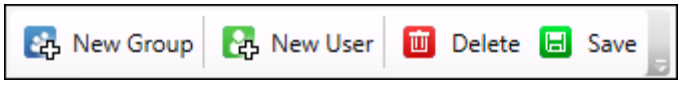


The **Users / Privileges** Tab is divided into several sections:

1. Near the top, there is a toolbar containing several function buttons that apply to items on the tab.
2. On the left, there is a **Groups** pane that displays existing groups and users and their hierarchy.
3. On the right, the pane will display details for the item selected in the Groups pane.
4. For cameras only, a preview pane is available displaying the camera's thumbnail image.

8.1 User / Privileges Toolbar

Figure 64 Users / Privileges Toolbar



8.2 Working with User Groups

The installation process creates one user group titled **Administrators**. This user group has one user account: **Admin**.

The 'Admin' user account is an administrative user account. The Admin user can view and change anything in *Ocularis Administrator*. We recommend changing the password of this account immediately. This account is referred to as a *super user* account. This account may not be deleted.

We recommend creating additional user groups for operators of the system.

FOUR TYPES OF USERS

There are four types of users in Ocularis:

1. Super administrator - this is the default account (admin/admin). This user can do anything in the system.
2. Standard administrator - this user account can do everything that **admin** can do except create other admins. This user is created by the **admin** user. Any user account placed in the user group 'Administrators' will be an admin. There is no limit to the amount of administrators for the system.
3. Group administrator - this user has limited access to *Ocularis Administrator* and may only work with data that corresponds to their own user group.
4. Standard - this user has no access to *Ocularis Administrator*.

***Note**: for upgrades from v5.2 or earlier, the 'Administrators' group is created and the user account admin is tranferred to this user group. The 'Default' group remains intact.*

ADMINISTRATORS USER GROUP

Any user account created in the **Administrators** user group will become an administrator. He/she can do anything in the system that the 'admin' user can do except create other administrators. Cameras added to the system will automatically be assigned to this group as privileged.

TO CREATE A USER GROUP

1. In the **Users / Privileges** toolbar, click the **New Group** button.
2. An entry in the list called **New Group** appears. Edit the text to the group label you wish to create.
3. Press **[ENTER]**.

The new group appears in the list. Repeat this process for each group you wish to add.

TO MODIFY A USER GROUP NAME

1. In the **Users / Privileges** Tab, double-click group name in the **Groups** list.
2. Edit the text to the group label as needed.
3. Press **[ENTER]**.

The updated group name appears in the list.

TO DELETE A USER GROUP

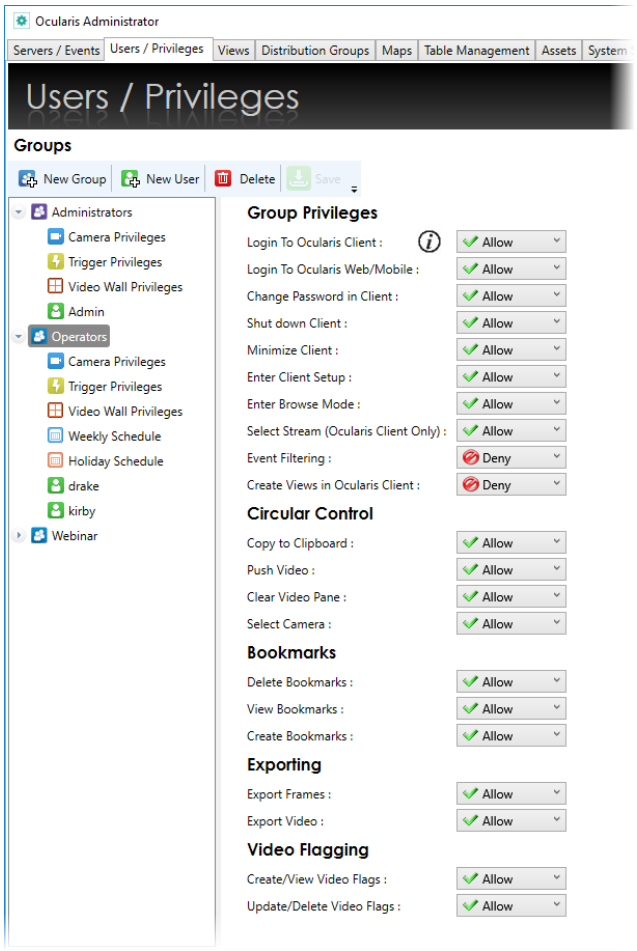
1. In the **Users / Privileges** Tab, select the group you wish to delete.
2. Click the **Delete** button on the toolbar.

   An "*Are you sure you want to delete this group*…?" warning message appears.
3. Click **Yes** to delete the group.

8.3 User Group Privileges

Privileges to specific functions of Ocularis may be set on a user group basis. Then, any user that is added to the user group may inherit the privileges set at the user group level. Default settings for most privileges is: *Allow*.

Figure 65 User Group Privileges



Users within a user group may further have alternate privileges set on a user level. The privileges for the user group 'Administrators' are all set to *Allow* and may not be modified.

8.3.1 Group Privileges Defined

Item	*Privilege*
Group Privileges	
Login to Ocularis Client	By default, users of all groups will be granted access to log in to Ocularis Client. However, the system administrator can control which Ocularis user or group can perform a successful login. This setting can be used to control the user's access to specific features in Ocularis Client. If this setting is set to 'Deny', when the user tries to login, they will be presented with a different login dialog. Another user with login privileges must provide their credentials as approval for the original person to log in. Keep in mind this transaction is recorded in the system's Audit log. See *Dual Authorization* on page 4 for more details. This option controls access to only Ocularis Client.
Login to Ocularis Web/Mobile	By default, users of all groups will be granted access to log in with Ocularis Web and Ocularis Mobile. However, in some cases, system administrators may want their users to access video while at the office using Ocularis Client but deny them the access while outside the office. The privilege 'Login to Ocularis Web/Mobile' can be set to 'Deny' and the user will not be able to login with either Ocularis Web or Ocularis Mobile. They will receive the message "User is not allowed to login to Ocularis Web/Mobile" if attempting do to so. **Note:** if the privilege 'Login to Ocularis Client' is set to 'Deny' and the privilege 'Login to Ocularis Web/Mobile' is set to 'Allow', the user will have direct access to Ocularis Web or Mobile (no approval login needed).
Shut down Client	The user may exit Ocularis Client. When this option is set to 'Deny', the user must enter account credentials for an account who may log off or shut down the client application.
Minimize Client	The user may minimize the Ocularis Client application.
Enter Client Setup	The user may launch and make personal changes to Ocularis Client settings.
Enter Browse Mode	The user may leave Live mode and view recorded video.
Select Stream (Ocularis Client Only)	The user may select between multiple live streams for a supported camera in Ocularis Client. This privilege does not apply to Ocularis Web or Ocularis Mobile.
Event Filtering	The user may configure schedules for the automatic handling of events. This privilege is set to 'Deny' by default as it should only be allowed for limited users.
Create Views in Ocularis Client	Users of Ocularis Client may be allowed to create their own views from within the Ocularis Client application. By default, the privilege is set to 'Deny' so the administrator must manually enable it for the user or the group. For users who do not have this privilege, the 'Auto Views' feature in

Item	*Privilege*
	Ocularis Client is also disabled. For more details refer to the *Ocularis Client User Manual*.
Circular Control For each item in this section, the 'Allow' privilege will display the corresponding function on the Circular Control menu in the *Ocularis Client*.	
Copy to Clipboard	The user may copy the displayed image to the Window's clipboard. The clipboard image may be pasted into any compatible application.
Push Video	The user may send video to another user logged in to Ocularis Base.
Clear Video Pane	The user may remove the video stream from the current pane.
Select Camera	The user may select another privileges camera from the current pane.
Bookmarks*	
Delete Bookmarks	The user may delete any bookmark to which they have access.
View Bookmarks	The user may view bookmarks that they or other members of their group create.
Create Bookmarks	The user may export bookmarks from Browse mode of the *Ocularis Client*. This will only be applicable if the value in *Browsing Limit* on the camera is not equal to 0.
Exporting	
Export Frames	The user may export still images in .jpg format from Browse mode of the *Ocularis Client*. This will only be applicable if the value in *Browsing Limit* on the camera is not equal to 0. This privilege also controls whether the user may take a snapshot of video in Ocularis Client (live or browse mode).
Export Video	The user may export video in both .AVI and Database Format from Browse mode of the *Ocularis Client*. This will only be applicable if the value in *Browsing Limit* on the camera is not equal to 0.
Video Flagging	
Create/View Video Flags	This permission will allow the users of this group to create and view flags in Ocularis Client.
Update/Delete Video Flags	This permission will allow the users of this group to update and delete video flags.

**If a user is deleted, any bookmark they created will still be available to other members of the User Group or Administrator members.*

8.3.1.1 Video Flagging

Video flagging is where a user can reference a point in time in a camera's video (i.e. create a timestamp). Flags are created and viewed in Ocularis Client and the ability to create, view, update and delete are controlled by the Video Flagging permissions set at the user group level.

For more information, see the *Ocularis Client User Manual*.

8.3.1.2 To Modify a Group Privileges

1. In the **Users / Privileges** tab, select the User Group that you wish to modify.
2. From the drop-down menu next to the corresponding privileges, select the privilege to assign to the user group.

Figure 66 Modify a User Group Privilege

3. Click **Save**.

8.3.2 Manually Assign a Slave Core to a User Group

For a specific system layouts, it may be advantageous to assign a particular Slave Core to a specific user group. When an Ocularis user logs in, they initially connect to the recorder's Master Core. If there is a Slave Core configured (ENT & ULT only), the Master Core hands off the connection the Slave Core. By default, it will use the Slave Core at the root or company level. In cases where systems are geographically dispersed or very distributed, this can be problematic and impact bandwidth. You can manually assign a local Slave Core to a user group so that the system will use the most efficient core possible. The Master Core would be used if there was a problem with the assigned Slave Core. Only members of the Administrators group may configure branches.

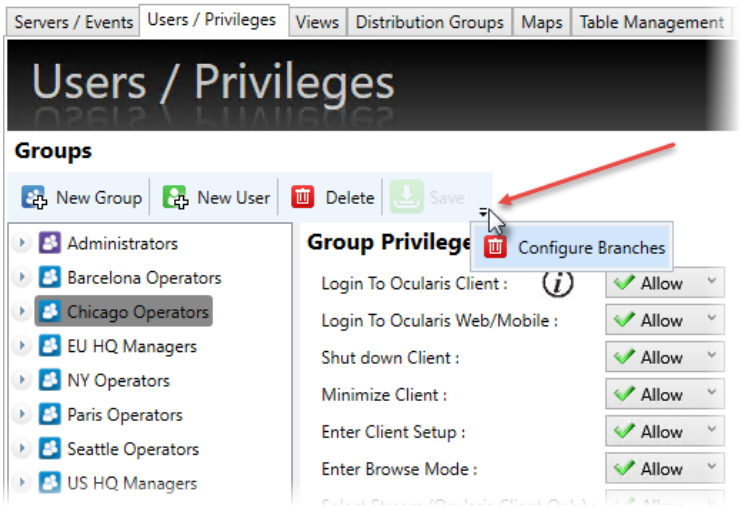
For this to work properly:

- Branches must be configured using Ocularis Recorder Manager
- Slave Cores must be installed within each branch
- The system must be Ocularis Enterprise or Ocularis Ultimate

TO ASSIGN A SPECIFIC SLAVE CORE TO A USER GROUP

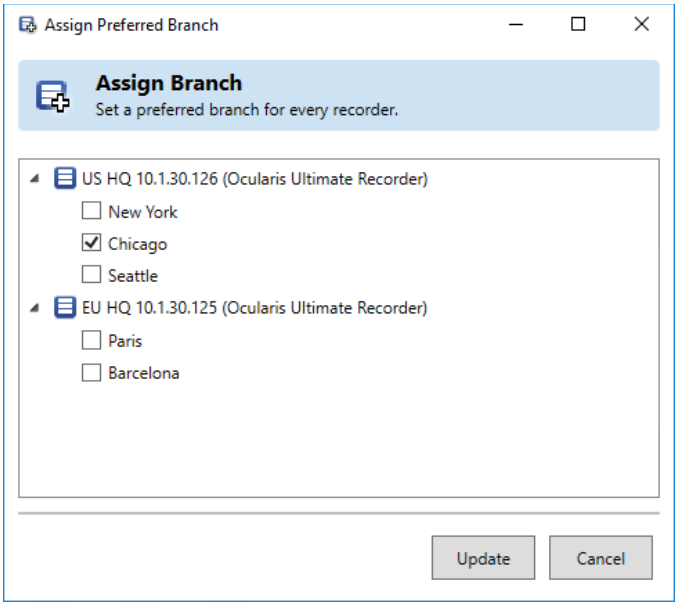
1. From the **Users / Privileges** tab, select the user group you wish to configure.
2. Click the down arrow on the far right of the toolbar and select **Configure Branches**.

Figure 67 Configure Branches



3. For each Master Core, you'll see its corresponding branches.

Figure 68 Assign a Branch



4. Select the branch for which you would like the user group to use. You may only assign one branch per user group.
5. When done, click **Update**.
6. Repeat for all user groups you wish to assign to a branch.

***Note**: If you do not see branches listed in the Assign Branch dialog, be sure to refresh the server(s) in the Servers/Events tab.*

8.4 User Privileges

Once privileges have been established for user groups, Ocularis users need to be created and assigned to the groups.

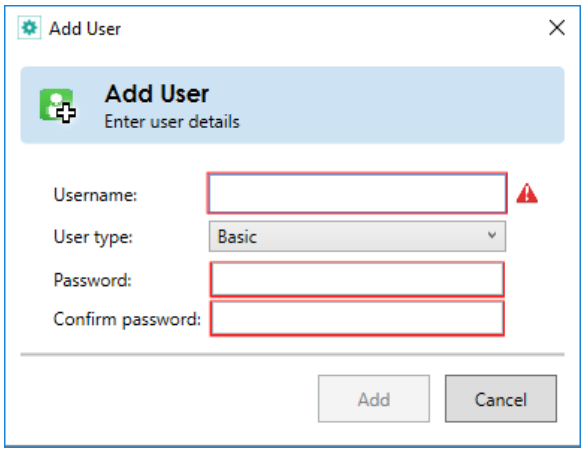
There are four user roles in Ocularis Base: **Super Administrator, Administrator**, **Group Administrator** and **Standard**.

User Role	*Description*
Standard	This user can access video from recorders using the *Ocularis Client* by logging into Ocularis Base. This user has no access to *Ocularis Administrator*.
Group Administrator	This user has limited access to *Ocularis Administrator*. He or she can log into *Ocularis Administrator* but may only manage their own user group or its settings. This user can add, modify or delete users in their own user group as well as modify other aspects of *Ocularis Administrator* as it applies to this user group. This user may not add, edit or delete servers. Additionally, there are some restrictions placed on Distribution Groups which will be discussed in **Distribution Groups Tab** on page 176.
Administrator	This user has the same privileges as the **admin** account except that they cannot create other administrators.
Super Administrator	This is the super user for Ocularis Base. It is the user account **admin**. This user may view, change or edit any part of the system. We recommend changing the password for this account.

8.4.1 To Create A User Account

1. In the **Users / Privileges** Tab, select the user group to wish you would like to add users.
2. Click the **New User** button.
3. In the **Add User** pop-up window, enter a unique **User name** to be created.
   - User names are not case sensitive
   - User names must begin with a letter (a through z)
   - User names may not contain the following characters: **[ ] * ? @ < > / = + | \ " : , ;**
   - The \ character is allowed only when specifying the domain along with the user name such as: **qognify\jsmith**

Figure 69 Add New User



As valid values are entered into each field, the red warning box will disappear.

***Note**: Users created in the 'Administrators' group will have admin privileges. These users may be **Basic** or **Windows** users.*

4. Select the **User type**:

Type	*Description*
Basic	Select **Basic** if not using Windows Active Directory
Windows User	Select **Windows User** if logging in with the local Window's user account
Windows Group	Select **Windows Group** if user is to log in via Windows Active Directory Group

***Note**: If the Windows User you are creating is part of a domain, you must include the domain when you enter the User Name. Use the format: **domain\username** in the User Name field*

***Note**: When adding a Windows Active Directory user to Ocularis Base, the system administrator can bypass the validation check for this user account if the username cannot be found by the system. This provides configuration flexibility for environments where the Ocularis Administrator is unable to check the validity of a user.*

5. Enter a **Password** for this user.

   A password:

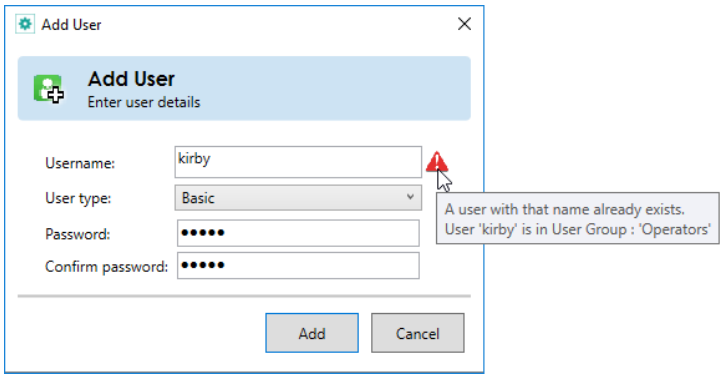
   - Is required
   - Must contain at least 4 characters
   - May contain letters, numbers, special characters and spaces
   - Is case sensitive
   - Does not expire

6. Re-enter the password to ensure accuracy.

7. Click **Add**.

   If the username already exists, the system will not let you add a duplicate. You will see a red informational triangle. Hover the mouse over the triangle to see to which User Group the username already belongs.

Figure 70 Duplicate Username



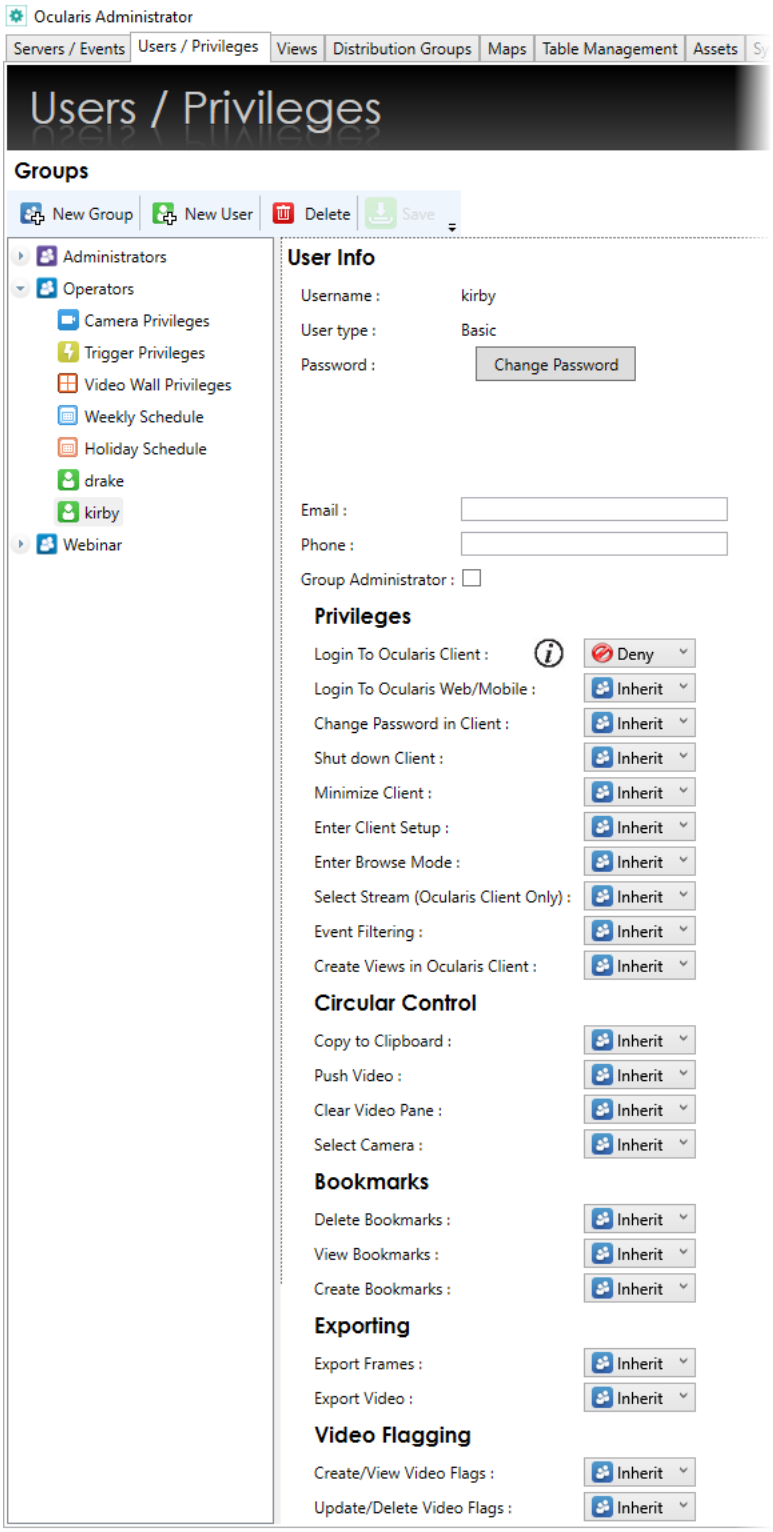
8. Repeat for all users.

The user account will inherit all privileges of the group in which it is placed.

8.4.2 Password Change Upon First Login

The user permission ‘Change Password in Client’ is set to ‘Inherit’ by default. The group level permission is set to ‘Allow’. This means that the first time the user logs in to Ocularis Client, they will be prompted to change their initial password. Users will need to enter their old password and then the new password. Ocularis Client also provides the option for users to change their own passwords at any time. This applies to ‘Basic’ users only.

Figure 71 New User Account



TO MODIFY USER ACCOUNT SETTINGS

Administrators may reset the password or modify privileges for a user account. Only the user 'admin' can create other administrators. Group Administrators may perform these actions only for those users in his/her own group. User accounts may have differing privileges (additional or fewer) than the group to which it belongs.

1. In the **Users / Privileges** Tab, select the user account you wish to modify.
2. In the details pane you can:
    a. Change the user account password
    b. Add or edit the user's contact information (email address or phone number).
    c. Set or remove Group Administrator privilege on the user account.
    d. Modify the specific user account privilege as needed. By default, new users are set to 'Inherit' privileges from the user group's setting.
    ***To modify a specific user account setting*:**
        i. Select the drop-down list next to the corresponding privilege.

Figure 72 Modify User Privilege

        ii. Change the setting: **Allow** or **Deny**
        iii. Repeat for other privileges
3. When finished modifying user account settings, click the **Save** button.

TO MOVE A USER ACCOUNT TO A DIFFERENT GROUP

1. In the **Users / Privileges** Tab, expand the user group containing the user you wish to move.
2. Drag-and-drop the user from the existing group to the new group name.

All user level permissions will follow the user. Private views will also be moved. The user now inherits the group privileges from the new group. You may not move a group administrator to

another group (until you remove their group administrator status) nor can you move users into the Adminstrators group.

TO DELETE A USER ACCOUNT

The account 'admin' may not be deleted.

3. In the **Users / Privileges** Tab, select the user account you wish to delete.
4. Click the **Delete** button.

   An "*Are you sure you want to delete this user…*?" warning message appears.

5. Click **Yes** to delete the user account.

***Note**: Any Bookmarks created by the deleted user will still exist and be available to other members of the User Group or by an Administrator.*

8.5 Device Privileges

Ocularis provides administrators centralized control for assigning privileges to users for all cameras on the system regardless of the recorder on which it resides. Users will not be able to view camera video unless they are given access privileges in the **Users / Privileges** tab of the *Ocularis Administrator* application. Access to a device is granted at the group level and individual functions for that device may also be granted or denied.

***Note**: All devices will be assigned to the 'Administrators' group by default. As new cameras are added, these will automatically be assigned. This group will have only one camera privilege group titled 'Privileged Cameras'.*

8.5.1 Assign Devices To A User Group

There are three general steps in providing user groups access to devices:

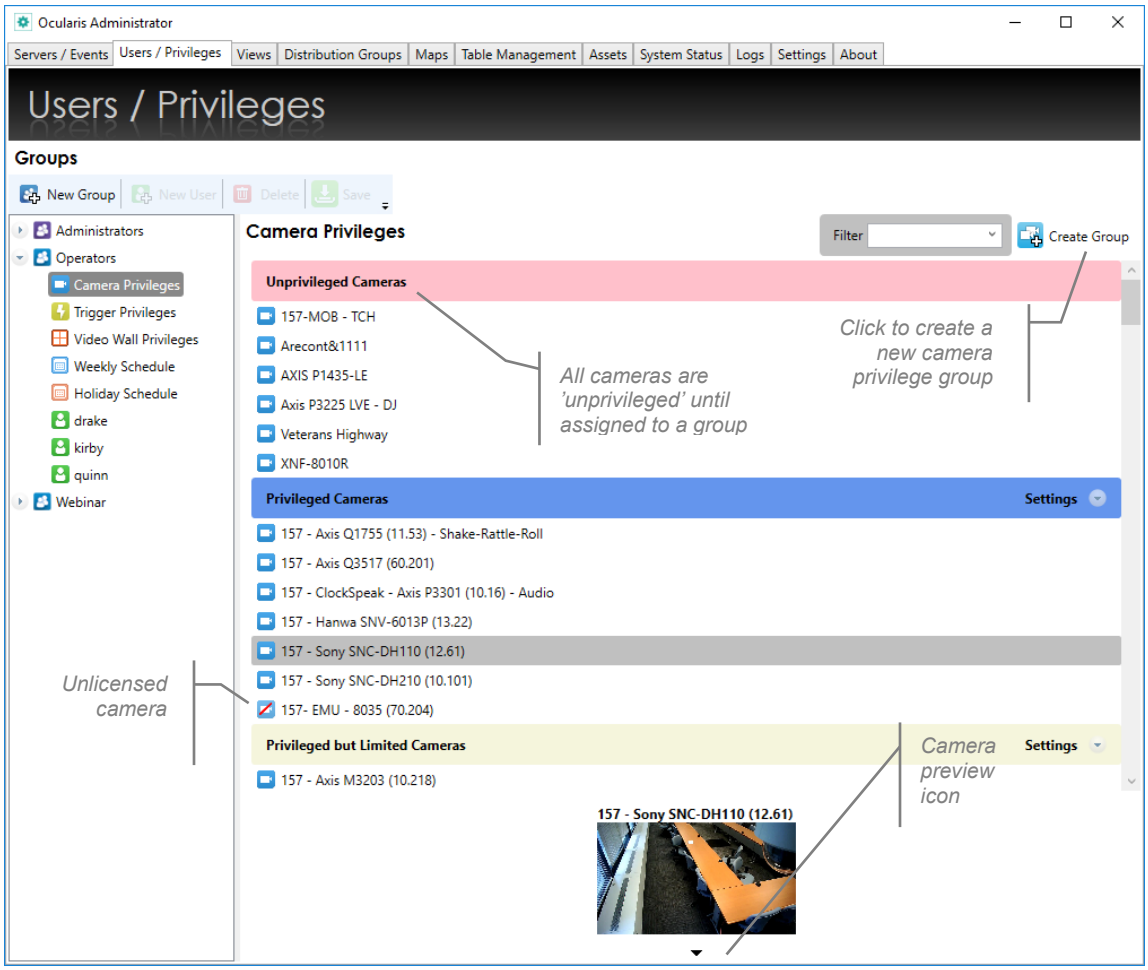
- Create a Camera Privilege Group
- Modify Camera Privilege Group Settings
- Assign Camera to the Permission Group

When a new user group is created, its members do not have privileges to any camera or device. All cameras are listed under 'Unprivileged Cameras'. Licensed cameras will have a different icon representation than unlicensed cameras. Administrators (i.e. the user *admin* or any user within the 'Administrators' user group) assign cameras to camera privilege groups based on the selected user group.

8.5.1.1 To Create a Camera Privilege Group

1. In the **Users / Privileges** Tab, under the user group you wish to assign devices, select the **Camera Privileges** node.
   All cameras appear under the group 'Unprivileged Cameras'.
   - To see a preview of the camera image, click the camera thumbnail icon.
   - To filter the camera list displayed, enter a keyword or phrase in the *Filter* text box.

Figure 73 All Cameras Start as Unprivileged



2. In order to give members of a user group access to a camera, the camera must be assigned to a camera privilege group.

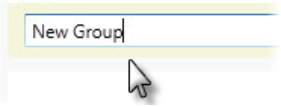
***Note**: Camera privilege groups set in this tab should be organized by intended functionality (vs. camera location or name) as the administrator applies camera privileges to the entire group of cameras.*

3. Click the **Create Group** button and a *New Group* entry appears.

You may now add cameras to this permission group.

8.5.1.2 To Modify a Camera Privilege Group Name

1. In the **Users / Privileges** Tab, under the user group you wish to assign devices double-click the camera privilege group name you wish to modify.

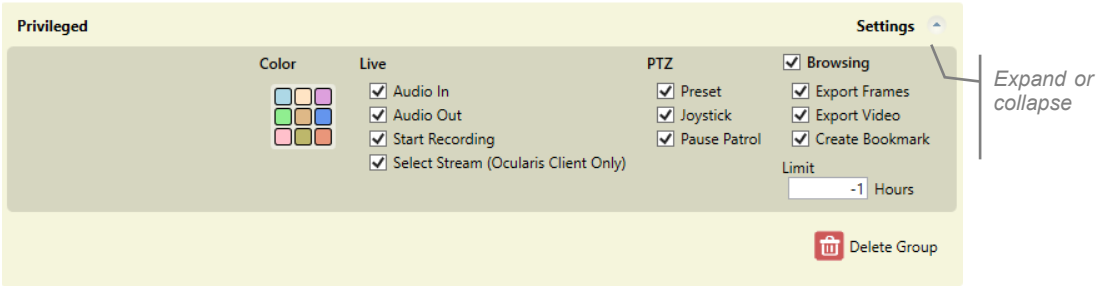
   The existing name appears in an editable text box. Modify the name or replace as needed.

2. Press **[ENTER]** to save changes.

8.5.1.3 To Modify Camera Privilege Group Settings

1. In the **Users / Privileges** Tab, under the user group you wish to modify device settings, click the expand icon to the right of the permission group name to expand the settings parameter area.

Figure 74 Camera Privilege Group Settings



2. Modify settings based on the following:

   Color

   Click a color swatch on the color palette to change the color of the permission group bar displayed in this tab.

   Camera Permission

   For any camera placed in this group, you may apply or remove privileges as follows:

Item	*When checked, for these cameras:*
Live	
Audio In	If the device supports it, the users of this group will have the ability to listen to audio from the device.
Audio Out	If the device supports it, the users of this group will have the ability to speak to the device through its speakers.

Item	*When checked, for these cameras:*
Start Recording	This privilege allows the user to initiate manual recording while viewing live video feed from the corresponding device. Video will be recorded to the location and for the duration as defined in the NVR for that camera.
Select Stream (Ocularis Client Only)	If a camera has multiple live streams, this privilege allows the members of this group to change streams using Ocularis Client or Ocularis Mobile. This privilege does not apply to Ocularis Web. If unchecked, users of both Ocularis Client and Ocularis Mobile will NOT be able to change live streams.
PTZ	
Presets	The users of this group will be able to direct a PTZ camera to configured preset positions.
PTZ	The users of this group will have the ability to operate pan, tilt & zoom functions on applicable cameras.
Toggle Patrol	If the camera is a PTZ camera with presets configured to patrol, this privilege allows users of this group to pause the camera at any given preset.
Browsing The checkbox under 'Browsing' will allow the camera's recorded video to be viewed by any user with Ocularis Client, Web or Mobile.	
Export Frames	The users of this group will have the ability to export still images in .jpg format from Browse mode of the *Ocularis Client* for these cameras. This will only be applicable if the value in *Browsing Limit* is not equal to 0. This parameter also controls the operator's ability to perform a snapshot of the video from Ocularis Client.
Export Video	The users of this group will have the ability to export video in both .AVI and Database Format from Browse mode of the *Ocularis Client*. This will only be applicable if the value in *Browsing Limit* is not equal to 0.
Create Bookmark	The users of this group will have the ability to export bookmarks from Browse mode of the *Ocularis Client*. This will only be applicable if the value in *Browsing Limit* is not equal to 0.
Limit	The value entered here identifies if and for how long into the past the camera's video may be viewed by this user group in Browse mode of the Ocularis Client. Valid Values include: 0 = No Browse Privilege -1 = Unlimited Browse Privilege (any available video from past recordings may be viewed) 1 through 168 = The number of hours that the users in this group may browse recorded video for the device. If the user does not have Browse privileges to a device or the user attempts to view video prior to valid browse hour times, the video will appear darkened within the *Ocularis Client*.

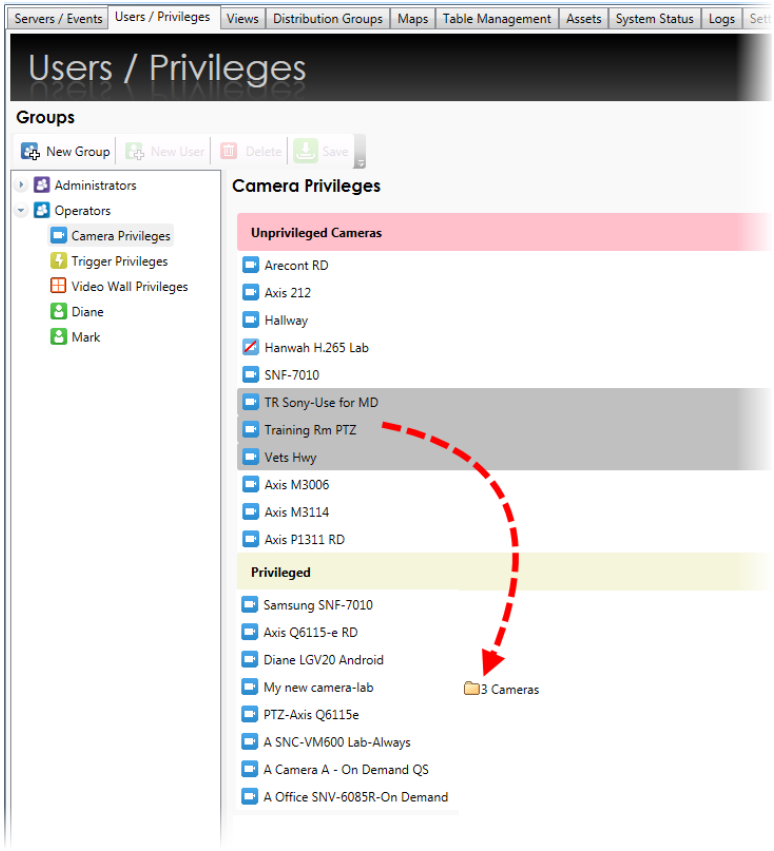
***Note**: If the 'Browsing' privilege is unchecked in the Camera Privileges group, you will not be able to view recorded video but you will still be able to hear recorded audio.*

8.5.1.4 To Assign Cameras to a Permission Group

When a user group is first created, all cameras are grouped in an 'Unprivileged Cameras' group. This means that the cameras listed here are not accessible to the user group members at all. In order for the user group to obtain any access to a camera, a camera privilege group must be created and cameras added it to it. The camera must also be licensed in the **Servers / Events** tab. Unlicensed cameras may still be assigned to a user group in the event that, at some future date, those cameras do become licensed.

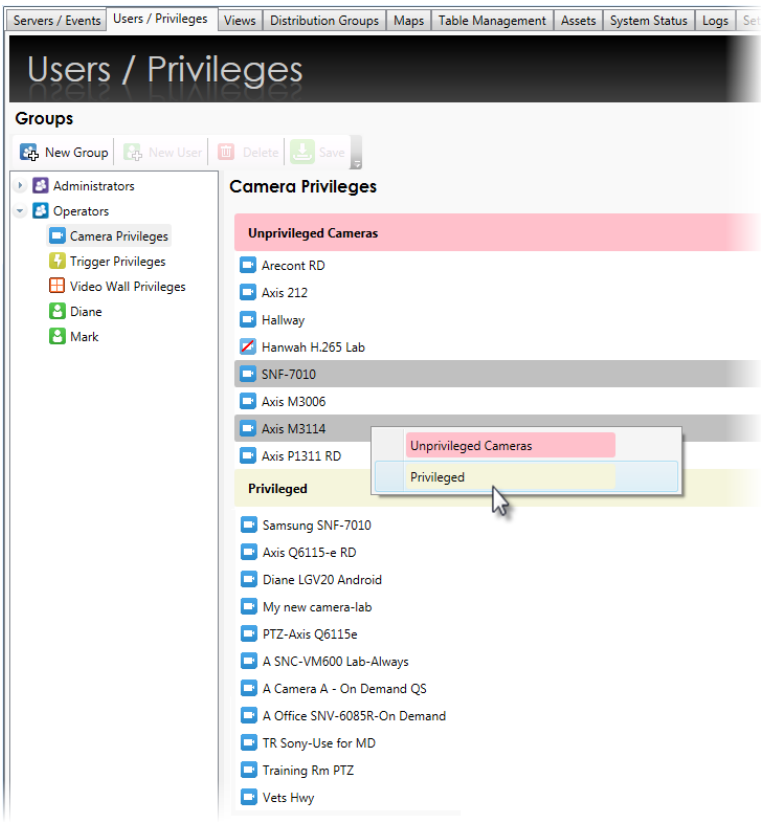
1. In the **Users / Privileges** Tab, under the user group you wish to assign devices, select the **Camera Privileges** node.
2. Select the device or devices you wish to assign to the group in the **Devices** list. Use the **SHIFT** or **CTRL** keys to select multiple items.
3. Assign cameras using either of these methods:
    a. Drag and drop the camera(s) from the **Unprivileged Cameras** group to the destination group. Cameras may also be moved between groups.

Figure 75 Drag and Drop to Assign Cameras



b. Right-click the highlighted camera(s) and select the destination camera privilege group.

Figure 76 Right-click to Assign Cameras



TO REMOVE A CAMERA FROM A PRIVILEGE GROUP

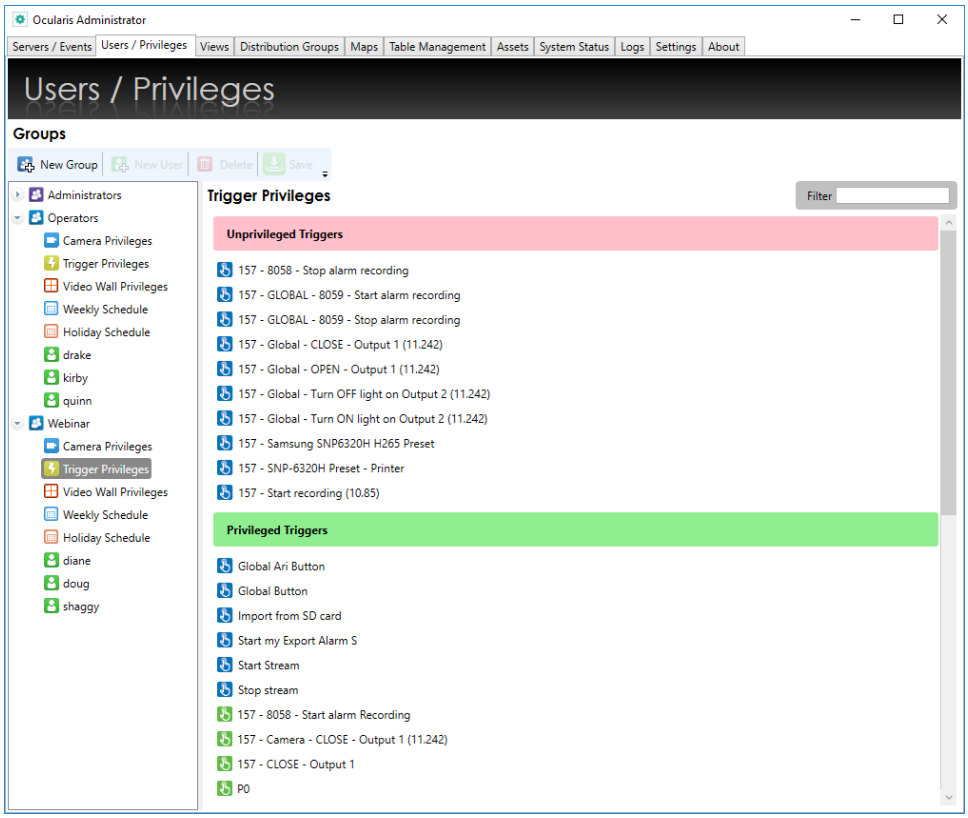
1. In the **Users / Privileges** Tab, select the group containing the device you wish to remove.
2. You can either:
   a. Drag and drop the camera to the **Unprivileged Cameras** group.
   b. Right-click the camera and select **Unprivileged Cameras**.

8.6 Trigger Privileges

Triggers are a privileged function as of Ocularis v5.4. A 'Trigger' (also called 'Button') is a manual action that an Operator can take from the Ocularis Client interface that does something. For example: you can configure a trigger to stop the camera from streaming, start the camera stream, start or stop an alarm scenario, open or close an output and more! Triggers are configured using *Ocularis Recorder Manager* under the 'Buttons' section. They are privileged in the *Ocularis Administrator* **Users / Privileges** Tab. Triggers can be camera specific or global. Global triggers

are executed from the *Ocularis Client* 'Triggers' menu and camera specific triggers are located in the camera pane's 'aux' menu.

Figure 77 Trigger Privileges



Upon new installation or upgrade, all triggers are located in the 'Unprivileged Triggers' group for each User Group except for the 'Administrators' group. The 'Administrators' group is automatically assigned all triggers.

1. Select the user group for which you want to assign triggers.
2. Assign triggers to the 'Privileged Triggers' group by either dragging and dropping the trigger between groups or by right-clicking the trigger(s) and selecting 'Privileged Triggers'. You may use the [CTRL] or [SHIFT] keys to multi select items. Use the same procedure as you would when you assign camera privileges.

There is a 'Filter' field that acts as a keyword search of the triggers list if you want to narrow your selection. Notice that Global Triggers display a blue icon and camera level triggers display a green icon.

8.7 Video Wall Privileges

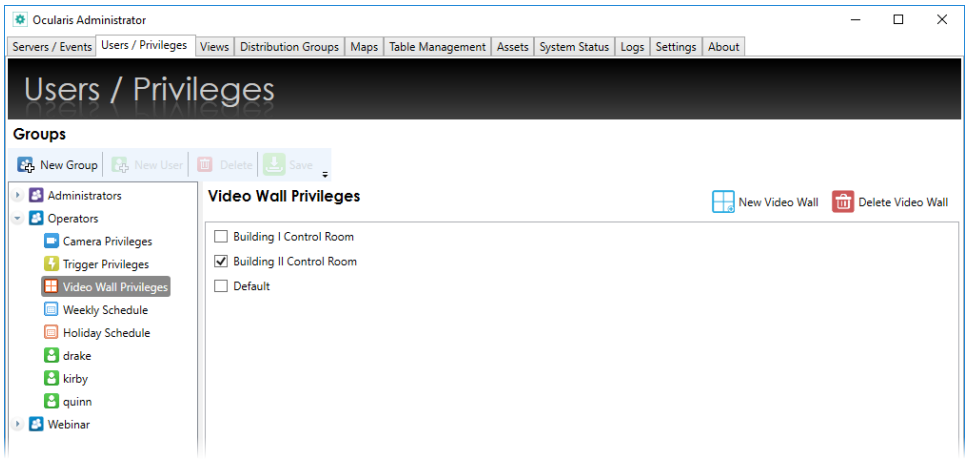
Similar to devices, users need privileges in order to view a video wall. These privileges are set in the **Users / Privileges** tab. The user group 'Administrators' will be granted access to all video walls.

To Assign Access to a Video Wall To A Group

Use these steps for user accounts that will be pushing video to video walls as well as video wall user accounts that will be used on a video wall.

1. In the **Users / Privileges** Tab, select the group you wish to assign the video wall(s).
2. Select the **Video Wall Privileges** node.
3. Existing video walls are displayed. Check the checkbox for the videowall(s) to assign to this user group.

Figure 78 Check box for assigned video wall



To Remove A Video Wall From A Group

1. In the **Users / Privileges** Tab, select the group you whose video wall(s) assignment you wish to modify.
2. Select the **Video Wall Privileges** node.
3. Uncheck the video wall(s) you wish to unassign.

8.7.1 Video Walls

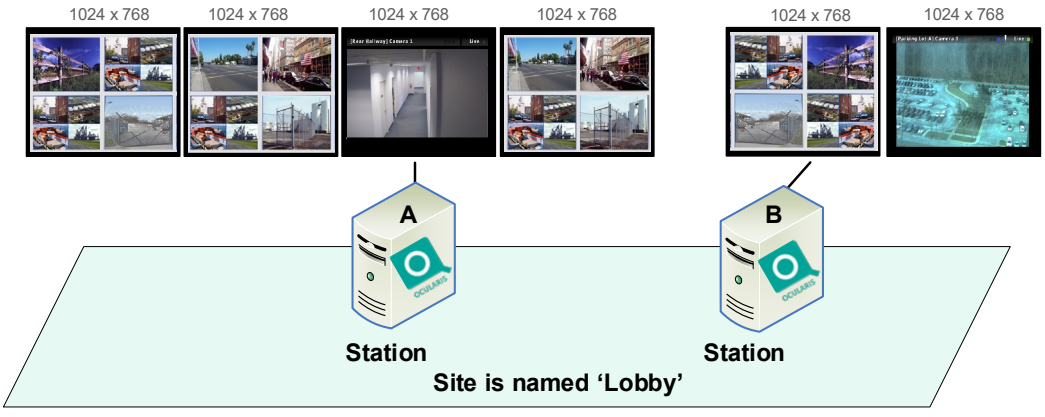
Video walls are simply a collection of monitors typically posted in a public or other observation area, with no visible keyboard attached. They are used to display video from preset cameras as well as receive video on demand, pushed there by operators or configured events. Video Walls in Ocularis are defined in the Base using the *Ocularis Administrator*. *Ocularis Client* is used to display the video wall. Remote Video Wall is an optional add-on component for Ocularis Enterprise and some legacy models. It is included as a standard option with Ocularis Ultimate.

8.7.1.1 Local vs. Remote

Local video walls are those on the same station (PC) as the operator. For instance, an operator's pc may have 4 monitors attached to it with an appropriate video card. The operator can use one of the monitors to observe views and maps and the other three monitors as the video wall on which he can post video. Local video walls are available in all Ocularis models.

Remote video walls are those where the video wall display monitors are not attached to the same pc as the operator. These monitors may be located in the same room or in another remote location from the operator.

The system administrator determines which video wall a user may push video to as well as which video wall a user account may be associated with. A *site* is synonymous with video wall. The video wall in the example shown in the graphic below has six monitors and two *stations*. Each station is a separate PC with a unique IP address. Both stations combined make up the video wall named 'Lobby'. Video wall site names are created by the administrator on the Ocularis Base. Video wall names can be any short label or description about the video wall.



Sample Video Wall

There is no technical limit to the number of screens/monitors which can encompass a video wall. There is, however, a limit to the number of screens that each Ocularis Client installation can

support. Currently, each instance of Ocularis Client can support up to eight (8) monitors on a single station (or IP address). Therefore, if you wanted a video wall comprised of sixteen (16) monitors for instance, you would need at least two PCs, each with its own instance of Ocularis Client installed.

8.7.1.2 Configuring a Video Wall

Defining a video wall involves these steps:

- Creating a video wall name in the *Ocularis Administrator* **Users / Privileges** Tab.
- Assign user privileges to the video wall within the *Ocularis Administrator* **Users / Privileges** Tab.
- For automated alerts to appear on video walls in blank screen panes in sequence, include the video wall as part of the distribution group for the event in the **Distribution Groups** Tab.
- On the station(s) which includes video wall monitors, select the video wall from the 'Client Setup' function in *Ocularis Client*. See the *Ocularis Client User Manual* for more information.
- Video Walls are used in conjunction with Ocularis Maps and at least one map should be configured in order for the operator to push video to a video wall. See ***Working with Maps*** on page 153.

TO DEFINE A VIDEO WALL

1. In the **Users / Privileges** tab, select any user group.
2. Select the **Video Wall Privileges** node.
3. Click the **New Video Wall** button.

A new video wall site is added and available for all user groups. Modify the text (double-click the name and press ENTER) to change the site name.

TO DELETE A VIDEO WALL

1. In the **Users / Privileges** tab, select any user group.
2. Select the **Video Wall Privileges** node.
3. Select the video wall to be removed.
4. Click the **Delete Video Wall** button.

TO ASSIGN VIDEO WALL PRIVILEGES

Once a video wall site has been created, it must be assigned to a user group in order for it to be visible in the *Ocularis Client*. It should also be assigned to the user group which contains

the user account(s) of the video wall station(s). This is assigned in the **Users / Privileges** Tab. For more information, see To Assign Access to a Video Wall To A Group on page 95.

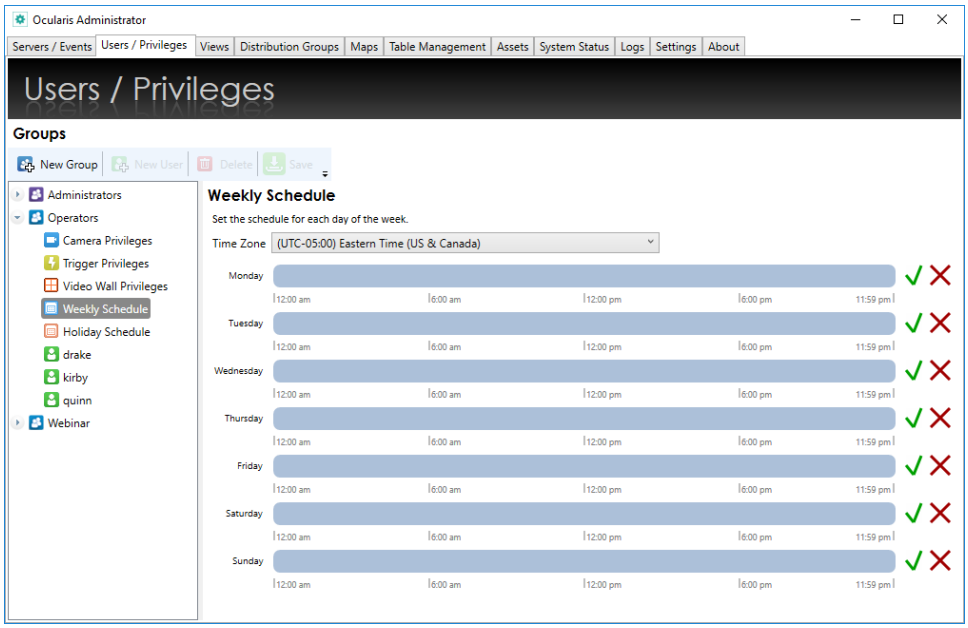
OFFSETS

When multiple stations (PCs) are used in the same video call, offsets must be defined in order to prevent overlap on the operator's station. The configuration of the offsets is performed in the *Ocularis Client* 'Client Setup' screen. See the *Ocularis Client User Manual* for instructions on how to configure offsets.

8.8 Weekly Schedule

For added security, administrators can control when members of a user group can access Ocularis video. This is configured in the **Weekly Schedule** module.

Figure 79 Weekly Schedule



By default, a user group's access is all the time (24 x 7 x 365). Administrators can establish approved login hours for each group based on their work schedule. Then, if a user attempts to log in with Ocularis Client, Ocularis Web, Ocularis Mobile or the Ocularis SDK, the system will deny access. Also, for Group Administrators, the schedule also controls their access to Ocularis Administrator.

8.8.1 Automatic Log Off

As the period for when a user's shift is over (i.e. when their end time is approaching), a pop-up warning will appear in Ocularis Client notifying the user that the approved login period is reaching its limit. This pop-up first appears when it is five minutes until the end time. When it is 50 seconds to the scheduled end time, the pop-up appears again with a countdown. Once the time limit has been reached, the user will automatically be logged off Ocularis Client and returned to the login screen with the message: 'Automatic Log Off – You were logged off by the system since it is outside of your scheduled hours'.

TO MODIFY THE LOGIN SCHEDULE FOR A USER GROUP

Use these steps to restrict the acceptable login times for a user group. Members of the 'Administrators' user group may modify schedules for any group and Group Administrators may modify the schedules for their own user group.

1. In the **Users / Privileges** Tab, select the group whose schedule you wish to configure.
2. Select the **Weekly Schedule** node.
3. Each day of the week is shown. Blue indicates approved access time.

> ***Tip***: *If you position the mouse over the timescale, a balloon appears displaying the Start and End time on the timescale.*

4. At the top of the schedule, a time zone drop-down is available. Select the time zone applicable to the users of the selected group. This restricts the access time based on the local time of the selected time zone.

   For example:

   The time zone selected is Paris time (UTC +01:00) and the schedule for Mondays is 9:00 a.m. to 4:00 p.m.

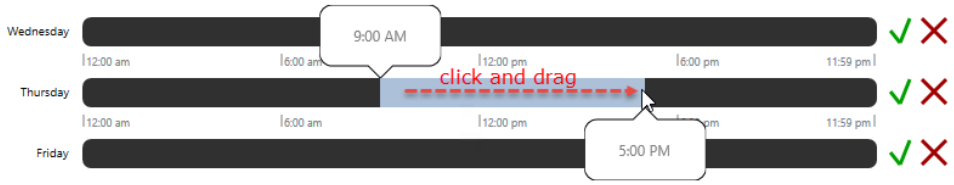
   A user from this group travels to the NYC office which is in Eastern Time (UTC -05:00). This user will only have access on Mondays from 3:00 a.m. to 10:00 a.m. local NY time.

   > ***Note***: *The time zone set for the group's Weekly Schedule is shared with the time zone for its Holiday Schedule.*

5. For each day of the week:
   - Click the 'X' to remove all privileges for that day.
   - Click the checkmark to apply privileges for the entire day.

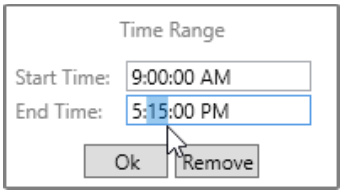
- To limit the time period, clear the daily schedule with the 'X' icon and then drag and release the mouse across the time period.

Figure 80 Click and Drag from left to right



5. When you release the mouse, the Time Range pop-up appears.

Figure 81 Time Range Pop-Up



You can manually fine tune the time period. Click **Ok** to save the settings.

6. Repeat for each day of the week.

If a user attempts to login to Ocularis Client during their off hours, the message: ' Access Denied – You are not authorized to lon in at this time.' will appear.

A similar message is displayed in Ocularis Administrator for Group Administrator logins.

8.8.2 More Information on Schedules

- Schedules apply to the entire user group. If a user requires a different schedule, he or she must be placed in a different user group.
- There may be more than one valid, non-contiguous access time periods set with the same day.
- All login attempts, valid or after hours, are registered in the audit log.
- Access restrictions apply to Ocularis Client, Ocularis Web, Ocularis Mobile, Ocularis Administrator and any 3rd party application using the Ocularis SDK
- The 'Administrators' user group has no time or date restrictions.
- Use a Holiday Schedule to further refine access times for each user group (see below).

8.9 Holiday Schedule

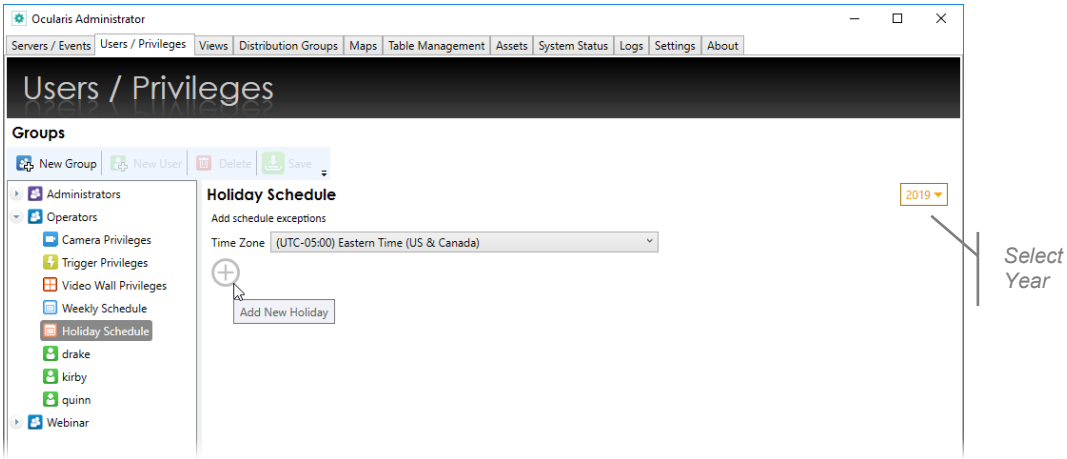
In conjunction with the Weekly Schedule, administrators can also configure a holiday schedule for the calendar year. This is done on a per group basis.

TO MODIFY THE HOLIDAY SCHEDULE FOR A USER GROUP

Use these steps restrict the acceptable login times for a user group during company holidays.

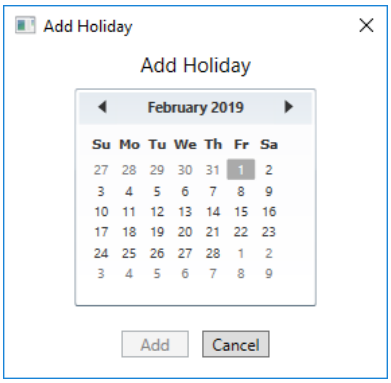
1. In the **Users / Privileges** Tab, select the group whose schedule you wish to configure.
2. Select the **Holiday Schedule** node. The time zone will be the same as the one set for weekly schedules. If you change the time zone here, it will be changed in the **Weekly Schedules** node.
3. You may select the calendar year from the drop-down on the right.

Figure 82 Holiday Schedule



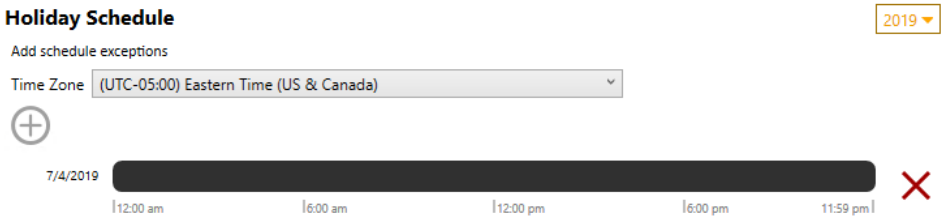
4. Click the ⊕ to add a new holiday. A month calendar appears.

Figure 83 Select Date



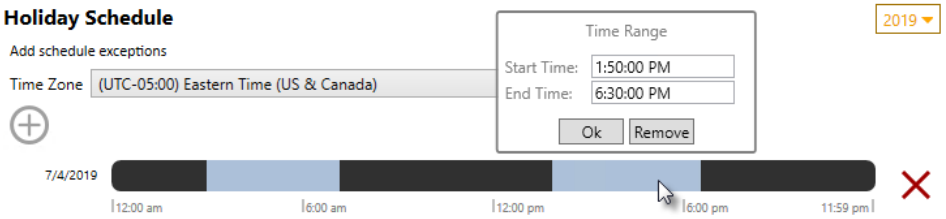
5. Navigate to the month for the holiday and select the date. Click **Add**. A day time bar appears with no time selected. This means the group will have no access to the system for the entire day.

Figure 84 Add a Holiday



6. If you want to grant this user group access for a portion of the day, simply drag and release the mouse on the timeline to identify the time period as you would with the weekly schedule. Fine tune with the Time Range pop-up.

Figure 85 Adjust Access Hours on a Holiday



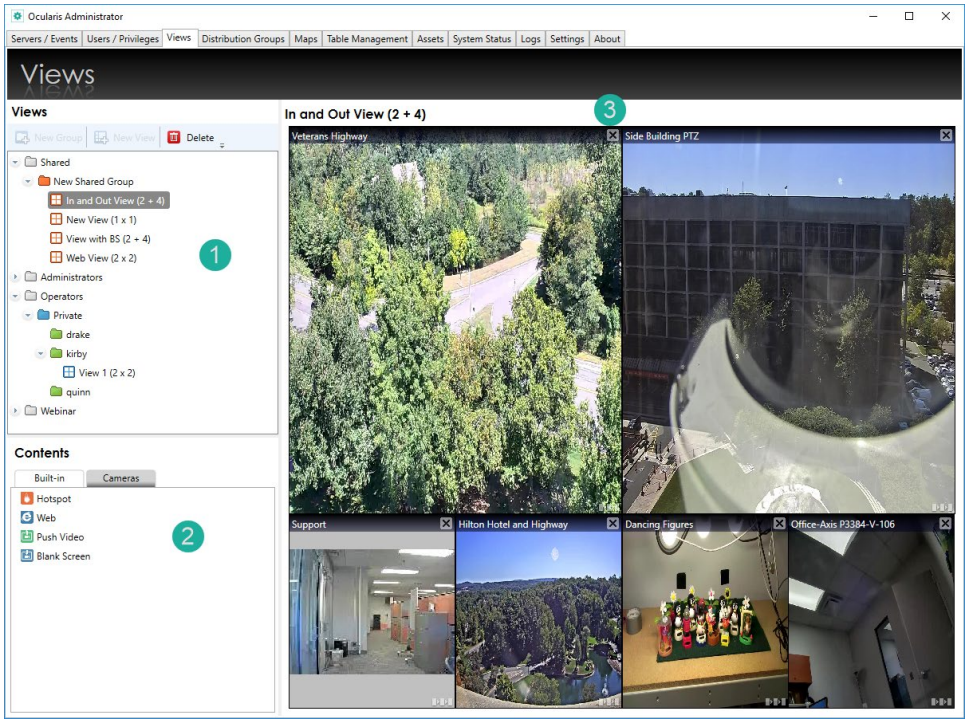
7. Repeat this process for each holiday, for each user group.

***Note**: The Holiday Schedule can grant greater access than the Weekly Schedule. For instance: if a user group has no login access on Mondays and a Holiday that falls on a Monday has a valid login period from 9:00 a.m. to 5:00 p.m., the user group members will be allowed to login even though this is not allowed in their Weekly Schedule.*

9 Views Tab

A *View* is the fundamental display when observing video from a client application such as *Ocularis Client*. When using Ocularis Base, views are configured within *Ocularis Administrator*, in the **Views** Tab.

Figure 86 Views Tab



The **Views Tab** is divided into three (3) areas:

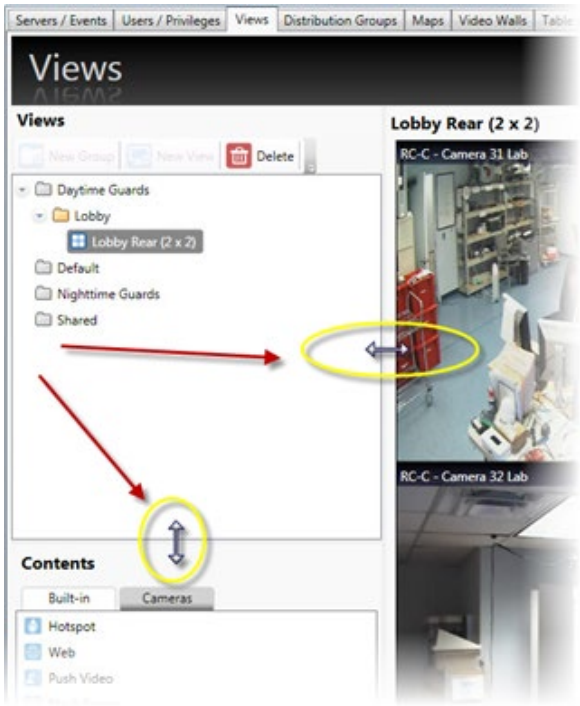
1. The **Views** list (1) in the upper left portion of the tab contains a list of configured views organized by user group and view folders.
2. The **Contents** list (2) in the lower left contains two tabs used to populate the various tiles of the displayed view pane.
3. The View working area (3) can be found in the upper right area of the tab and is labeled with the view name or with **Select a View** if no view is currently selected.

> ***Tip***: *You must have privileges to a device in order to create a view using that device. If you do not see any or a specific camera video in this pane, make sure the group you belong to contains privileges to view that camera's video.*

9.1 Resizing Panes

In the event you need to manually resize a pane in the Views tab, position the mouse on the divider between two panes until you see the mouse cursor change to a double arrow. Then you may click and drag to resize the pane.

Figure 87 Resizing a Pane



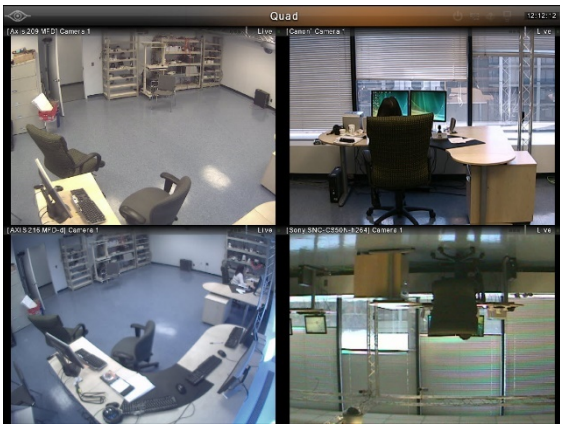
9.2 View Basics

A *View* is a collection of panes or windows that display video output. There are many layout options for views.

Ocularis Base views are configured from the **Views** Tab in *Ocularis Administrator*. Administrators configure the views on a group by group basis and control which view layouts and cameras are available to users when they use *Ocularis Client*.

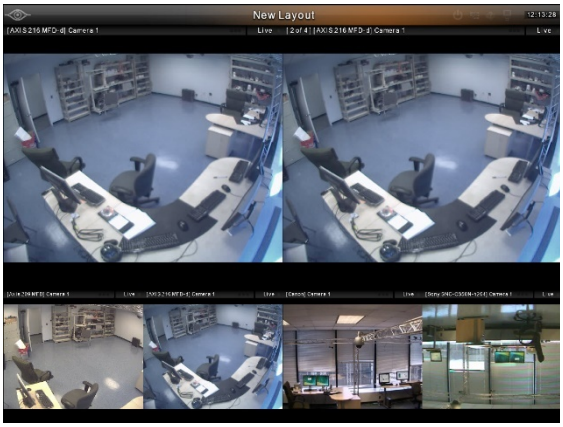
If a new employee joins the organization, for instance, once they are made a member of a group they inherit all Ocularis Base views for that group.

Figure 88 Sample views via Ocularis Client

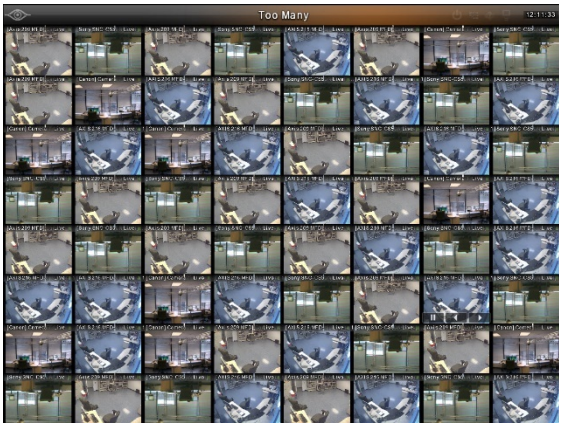


2 x 2 View

1 + 5 View



2 + 4 View

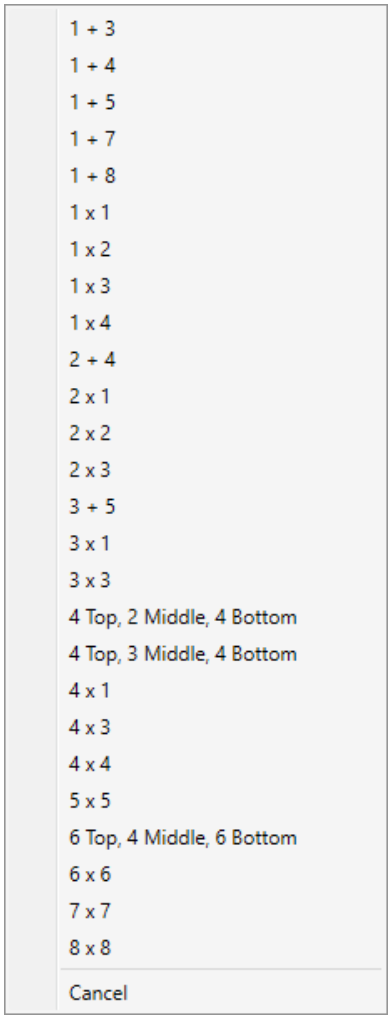


8 x 8 View

9.3 View Configurations

The following view configurations are available in Ocularis:

Figure 89 Available View Layouts



A View consists of a varying number of *panes*. A *pane* will most often contain video output from a camera.

9.4 Contents

In addition to streaming camera video, a pane may contain other content such as a:

- Carousel
- Hot Spot
- Push Video
- Web Page
- Blank Screen

9.4.1 Ocularis 5 Web Users

- If you are using Ocularis 5 Web there is a maximum limit to the number of panes in a view of sixteen. Any views with more than sixteen panes will not be available in Ocularis 5 Web so keep this in mind when creating views.
- Ocularis 5 Web can only display camera video in views. Non-camera video content in view panes (e.g. Carousel, Hot Spot, Push Video, Web page and Blank Screen) will not display in Ocularis 5 Web. The view will show these panes as empty.
- Also, when configuring cameras using *Ocularis Recorder Manager*, be sure to configure multiple live streams and include at least one low resolution H.264 stream (under 600 pixels high). This will allow Ocularis 5 Web to display the camera in a view with a large number of panes.
- Ocularis 5 Web can only display H.264 streams in Live mode. In Browse mode, streams of any codec are visible.

9.4.2 Carousel

A Carousel within a view pane will alternate video from camera to camera. The cameras included in the alternating output as well as the transition time between images are configured in the *Ocularis Administrator*. See *To Configure A Carousel* on page 132.

9.4.3 Hot Spot

A Hot Spot is a view pane dedicated to displaying images from another view pane when manually selected by the user in *Ocularis Client*. For practical purposes, hot spots are typically placed in one of the larger size view panes. See *To Configure A Hot Spot* on page 138.

9.4.4 Push Video

A Push Video window pane is one that is configured to accept video from another computer. Video may be “pushed” manually from one user to another user on the Ocularis Base environment. This action is performed in the *Ocularis Client*. See *To Configure Push Video* on page 139.

9.4.5 Web Page

A pane may contain an HTML webpage including (but not limited to): corporate websites, online maps, link collections, IP video camera configuration, flash presentation and images of a suspect, logo, map or event. See *To Configure a Web Pane* on page 140.

9.4.6 Blank Screen

When a pane contains a *Blank Screen* configuration, the pane will remain “blank” in the view until event driven video is triggered. The video will then be displayed in the Blank Screen pane. A benefit to using a Blank Screen is that it is attention getting. A Blank screen that suddenly displays video is easily noticed by a security guard or operator. Blank screen monitoring is supported by all Ocularis models. See *To Configure a Blank Screen* on page 141 to configure a blank screen.

9.5 Contents Navigation

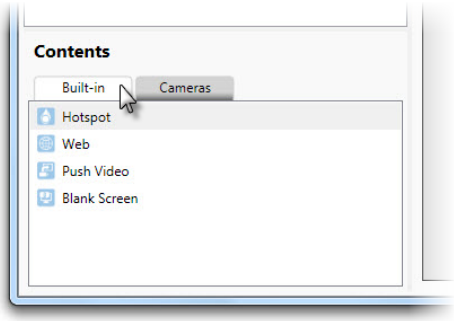
The **Contents** list within the Views tab (see item #2 in Figure 86) contains two tabs:

- Built-in
- Cameras

9.5.1 Built-in

The tab labeled ‘Built-in’ displays various content available for view panes. These include: Hotspot, Web, Push Video and Blank Screen. To use any of these, simply drag and drop the item from this list to a displayed view pane.

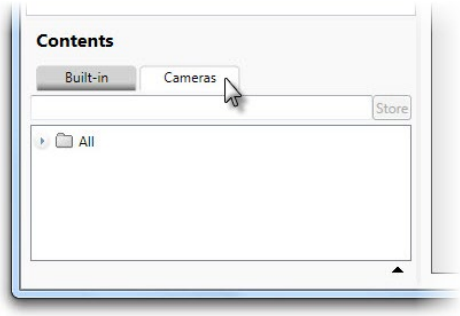
Figure 90 Built-in Tab of Contents List



9.5.2 Cameras

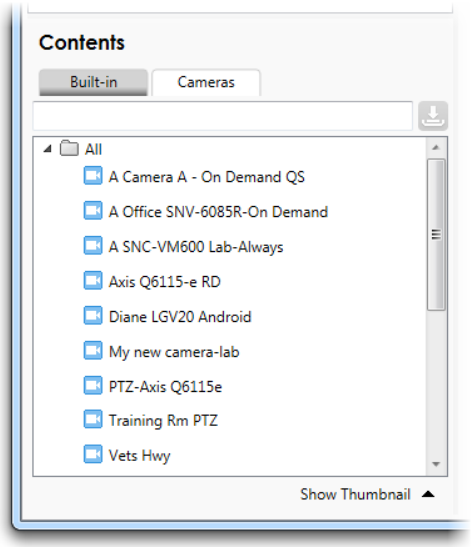
The tab labeled ‘Cameras’ displays the cameras assigned to the selected view group from the Views list above. By default, a folder labeled ‘All’ appears, listing all available cameras for the selected group in alphanumeric order.

Figure 91 Cameras Tab



Expand the folder to see its contents.

Figure 92 All Cameras for the selected View Group



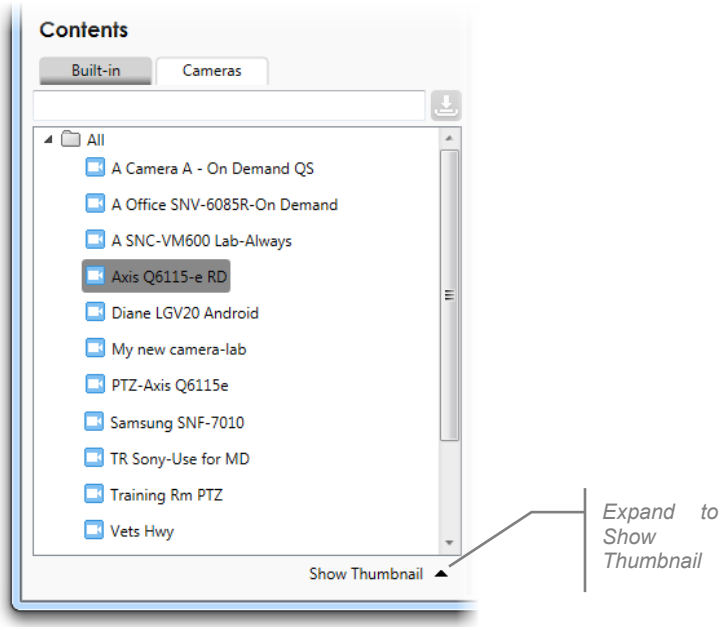
9.5.2.1 Camera Preview

In many cases, you may not know the image of a camera simply by looking at its name. In these cases, you may invoke a *Camera Preview* for a selected camera.

TO PREVIEW A CAMERA IN THE VIEWS TAB

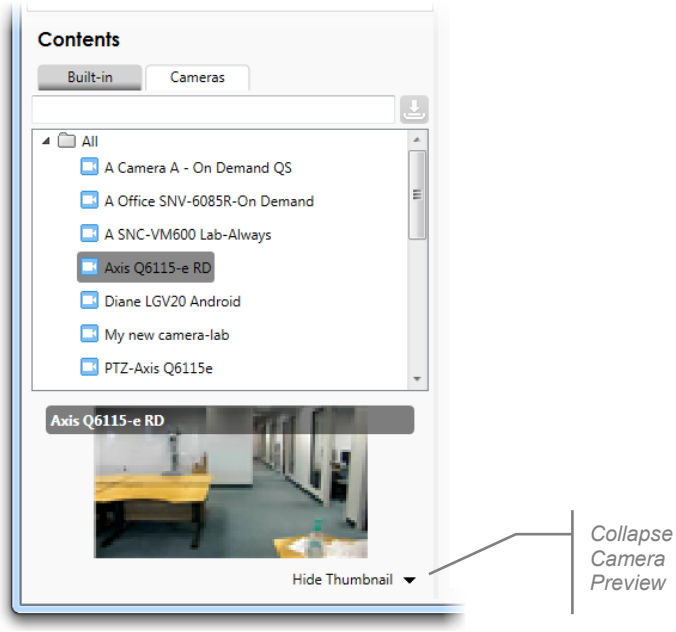
1. In the Views tab, select the View Group for cameras you wish to preview.
2. Click the **Cameras** tab in the Contents list.
3. Expand a camera folder and select a camera.
4. Click the *Expand Camera Preview* icon.

Figure 93 Expand Camera Preview Icon



A camera preview thumbnail appears below the camera list. The camera list will remain in preview mode until you collapse the preview. Select another camera and the preview thumbnail will update.

Figure 94 Camera Preview Thumbnail



5. Collapse the camera preview by clicking the *Hide Thumbnail* icon.

9.5.2.2 Camera Filter

The camera list in the Views Tab (and Maps Tab) may be quite lengthy depending on the installation. The list can contain hundreds or thousands of cameras making locating just the one you want a time consuming process. Luckily, you have the ability to filter the list of cameras based on a keyword and also to store this search for later use.

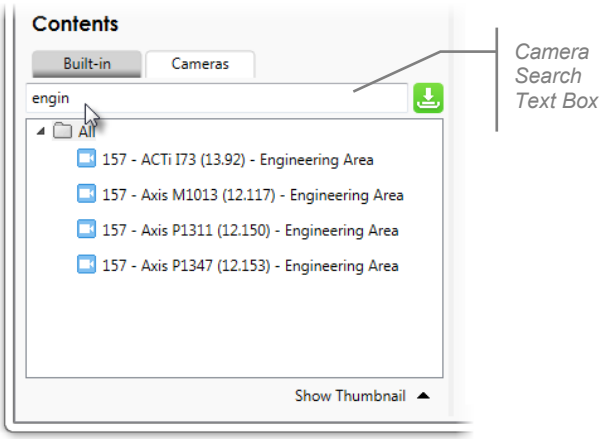
TO USE THE CAMERA SEARCH FILTER

1. In the Views tab, select the View Group you wish to work with.
2. Click the **Cameras** tab in the Contents list.
3. In the *Camera Search* text box, type in a keyword to be used as the camera filter.

   Keywords are not case sensitive and filter based upon the camera name as inherited by the recorder. (Therefore, it is important to know and understand the naming structure of the recorder cameras). If, for instance, you named your cameras using the manufacturer name, you may use this as the keyword. Or perhaps the cameras were named based on their location (Parking Lot A, Parking Lot B, etc.). Use any portion of the camera name to filter the list.

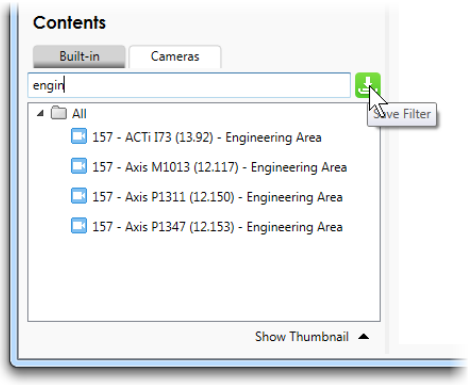
4. As you begin to type the keyword, the list will update.

Figure 95 Camera Search box



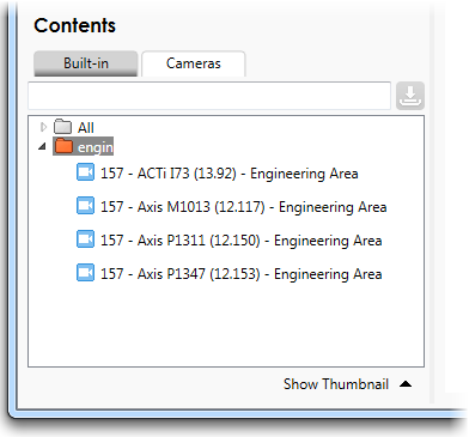
5. You can use the list as is (i.e. drag and drop displayed cameras).
6. If you would like to store the list for later use or in the Maps tab, click the **Save Filter** button.

Figure 96 Click store to Save Search Filter



7. A new folder is created containing the subset of cameras as filtered in step 3. This filter can now be shared:
    - With other view groups
    - In the Maps Tab

Figure 97 Example of stored camera filter 'engin'



8. Repeat these steps to add additional camera search filters.

Now you may use these stored folders to easily locate cameras as defined by the keyword filter.

***Note**: The cameras displayed in stored camera folders will be filtered further based upon the user group privileges assigned. If, for instance, the keyword search is on the word 'lab' and the Daytime Guards have access to 10 cameras which include the keyword 'lab' but the Nighttime Guards only have access to 5 of these cameras, only the 5 cameras will be available to the Nighttime Guards.*

9.6 View Organization

Views are organized first by user group (as defined in the **Users / Privileges** Tab) and then by *view group* or *folder*. A view group may contain multiple folders and a folder may contain multiple views. A folder may also contain multiple folders (or nested folders). A folder called 'Shared' appears in all Ocularis installations. This folder contains views that may be shared across multiple user groups.

9.7 Creating Views

Consider the users and their user groups as they are intended to use the system. Some users will require certain views to certain cameras. Other users may require access to different cameras in different locations. The system administrator should take into account the user role and job function when creating views in the *Ocularis Administrator*.

As discussed previously, views are assigned to user groups but are organized by folders. Therefore, you must first create a folder or view group and then you may create a view. Group Administrators may only create, edit or delete views within their own user group.

9.7.1 Shared, Group and Private Views

There are three levels of views in Ocularis: Private, Group and Shared Views.

Private views are limited to a single user. They may be created using Ocularis Administrator by an administrator user (i.e. member of the Administrators group) or Group Administrator for members of their own group. Private views may also be created by the individual user from within Ocularis Client. These views may be edited from within Ocularis Client by the user (owner), an Administrator or Group Administrator. They may also be edited from within Ocularis Administrator by an Administrator or Group Administrator. View creation or editing from within Ocularis Client is a privilege. By default, the privilege is denied to non-administrators. An administrator use can enable the privilege for a short time to allow the end user to create their own views in Ocularis Client and then later disable the feature so that the end user does not endlessly add views to the system.

For every user group, a 'Private' view group/folder is created and within that, a folder for each user account.

Group views are those available to a specific user group. They are unique ("private") to that group in that once created, they may not be shared with other groups or users outside of the user group.

These views may be created or edited by administrator users or Group Administrators from within either Ocularis Administrator or Ocularis Client.

Shared views may only be created by administrator users from within Ocularis Administrator. Shared views are used when more than one user group needs access to the view. These views are stored under the 'Shared' folder or group. Other than administrator users, no one can access Shared views unless an administrator user explicitly shares the view with a user group or user.

TO CREATE A FOLDER FOR A VIEW GROUP

1. In the **Views** Tab, select either:
   - the user group for which you would like to create a folder
   - the Shared folder
   - an existing folder beneath a user group or Shared group and create a nested folder beneath it.

2. Click the **New Group** button.
3. A folder is created labeled "New Group".

TO MODIFY THE NAME OF A VIEW GROUP

1. In the **Views** Tab, double-click the group folder you wish to rename.

   The folder name becomes highlighted.

2. Type the new name for the folder.
3. Press [**ENTER**] to accept changes.

TO DELETE A FOLDER WITHIN A GROUP

In the **Views** Tab, select the folder which you would like to delete.

Click the **Delete** button.

An "*Are you sure you want to delete this view group?*" prompt appears.

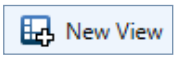
Click **Yes** to delete.

TO CREATE A VIEW WITHIN A FOLDER/VIEW GROUP

Once view folders / view groups are created, views may be added to them.

1. In the **Views** Tab, select the folder for which you would like to create the view.

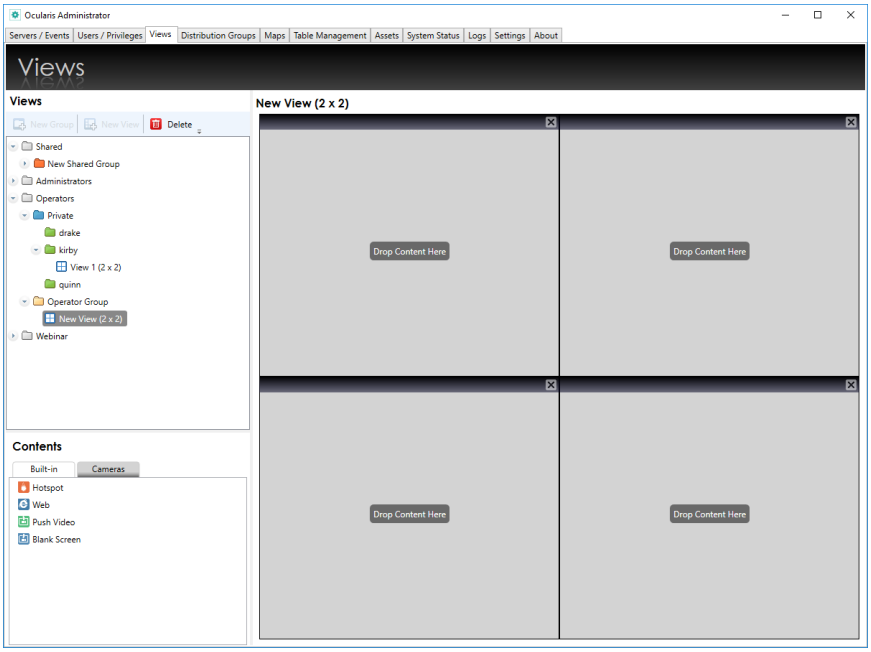
- If you intend on sharing this view with multiple groups, create the view under the ‘Shared’ folder hierarchy.
- For views for a specific user, select the user account under the ‘Private’ folder.
- For view for a specific user group, select a folder under the group’s folder.

2. Click the **New View** button. 

   The view layout pop-up appears. (see Figure 89 on page 106)

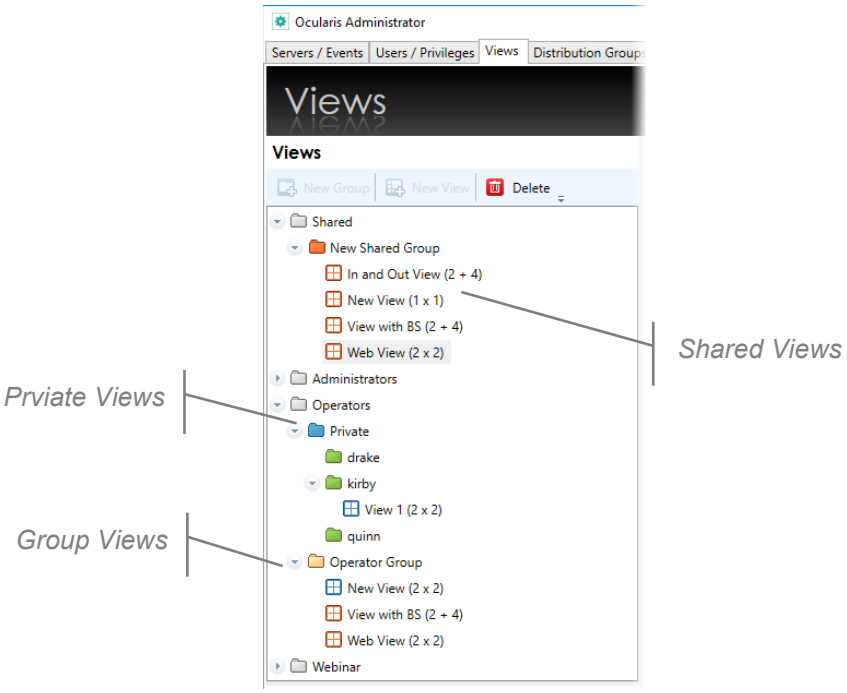
3. Select a layout from the list of View Configurations.
   A blank template for the layout appears in the View working area and a view called “New View(*layout*)” is created.

Figure 98 Creating a New View for a Single User Group



In the event that the view is to be shared between multiple user groups, be sure to create the view underneath the ‘Shared’ view group hierarchy. For example:

Figure 99 Shared Views



Notice in Figure 99, Shared items (folders and views) are shown in the color orange. Private or Group views are shown in blue and are private to either the user or group to which they are associated.

***Note**: If using Windows Active Directory, an AD group created in Ocularis will have a Private folder for all AD users of the group. Each user will have visibility to all views in the Private folder of the group.*

With the desired new view selected, populate each view pane by dragging and dropping a camera or other pane content from the

Contents list onto a pane.

Figure 100 Example: Drag a Hotspot to a View Pane

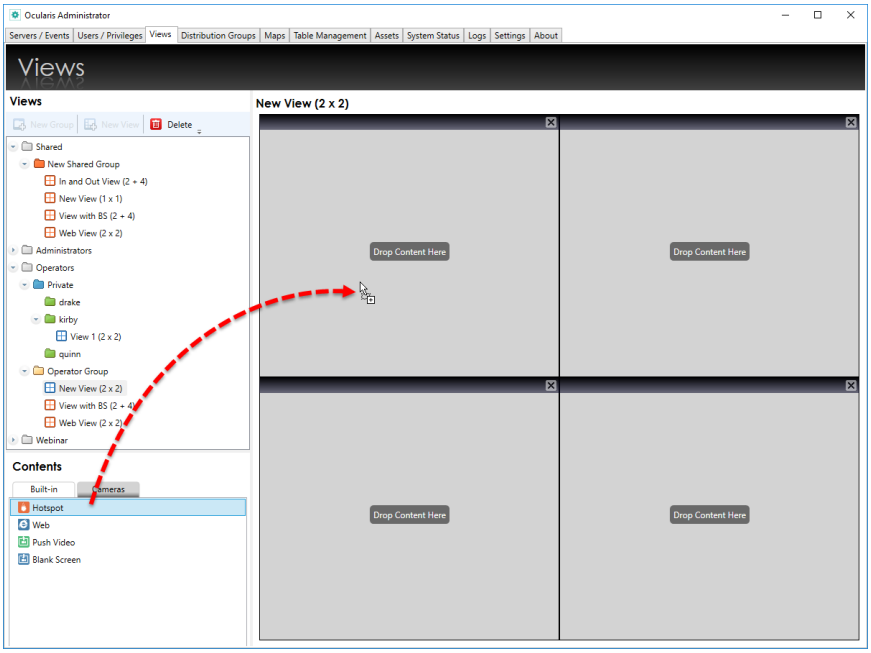
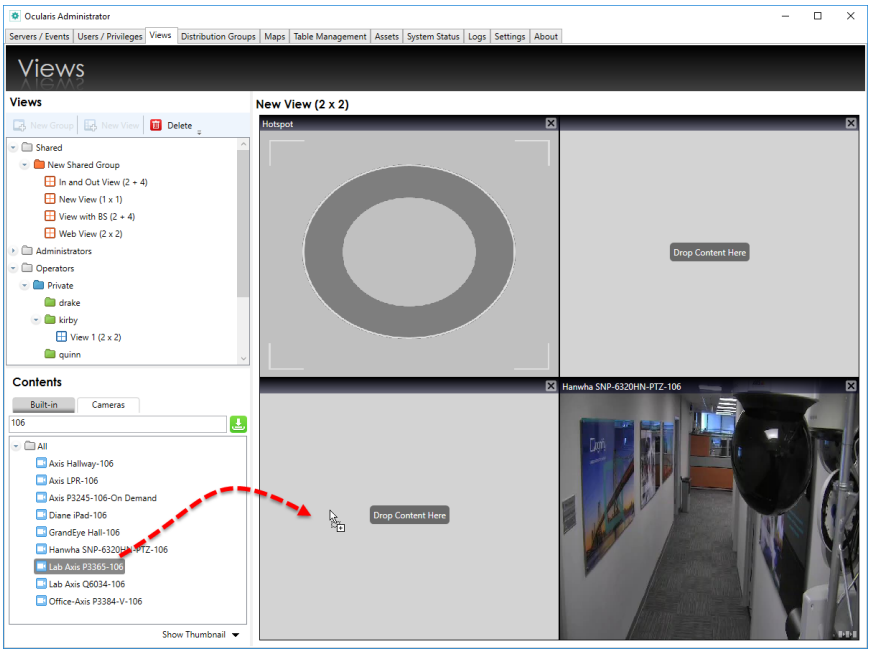


Figure 101 Example: Drag a Camera to a View Pane



Changes to views are automatically saved.

***Note**: If you have a view or view folder open and switch tabs, you will be returned to the same place upon reentering the Views Tab.*

9.7.1.1 Populating Views with Multiple Cameras

You can select multiple cameras and populate views quickly and easily.

- Use the [CTRL] key to select more than one camera
- Use the [SHIFT] key to select multiple contiguous cameras within the list
- Use the [CTRL] key to deselect cameras

1. Open or create a view to be populated.
2. Select cameras from the Cameras list. Use [SHIFT] and click the mouse for multiple selections.
3. Either drag and drop or right-click and select 'Move selected camera(s) to the view'.

Figure 102 Select Multiple Cameras

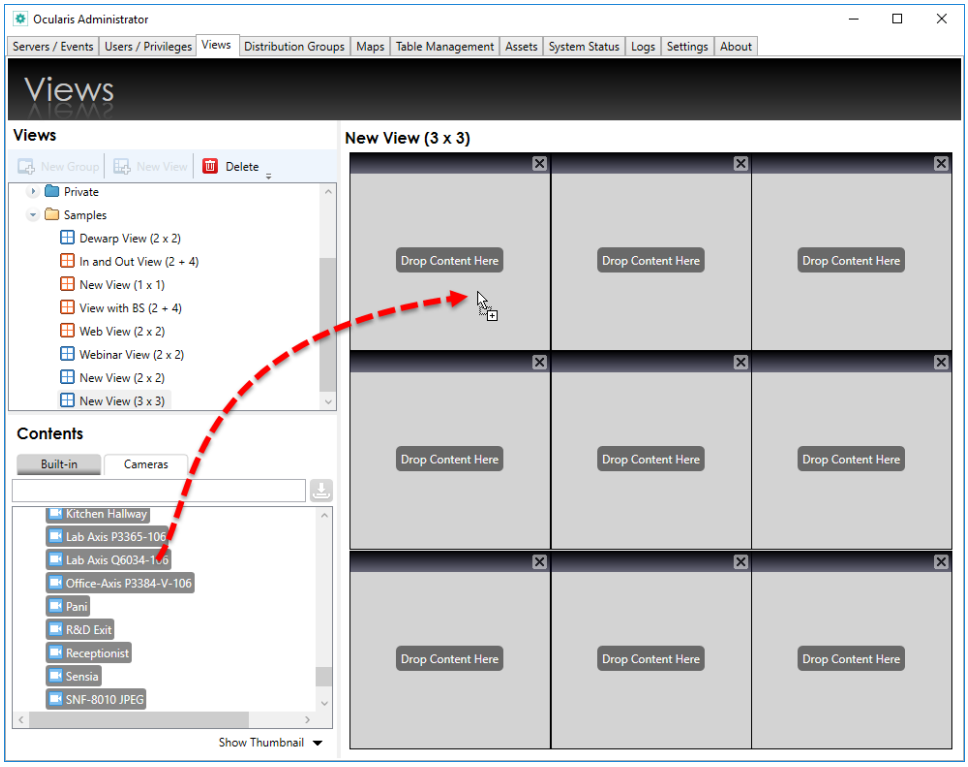
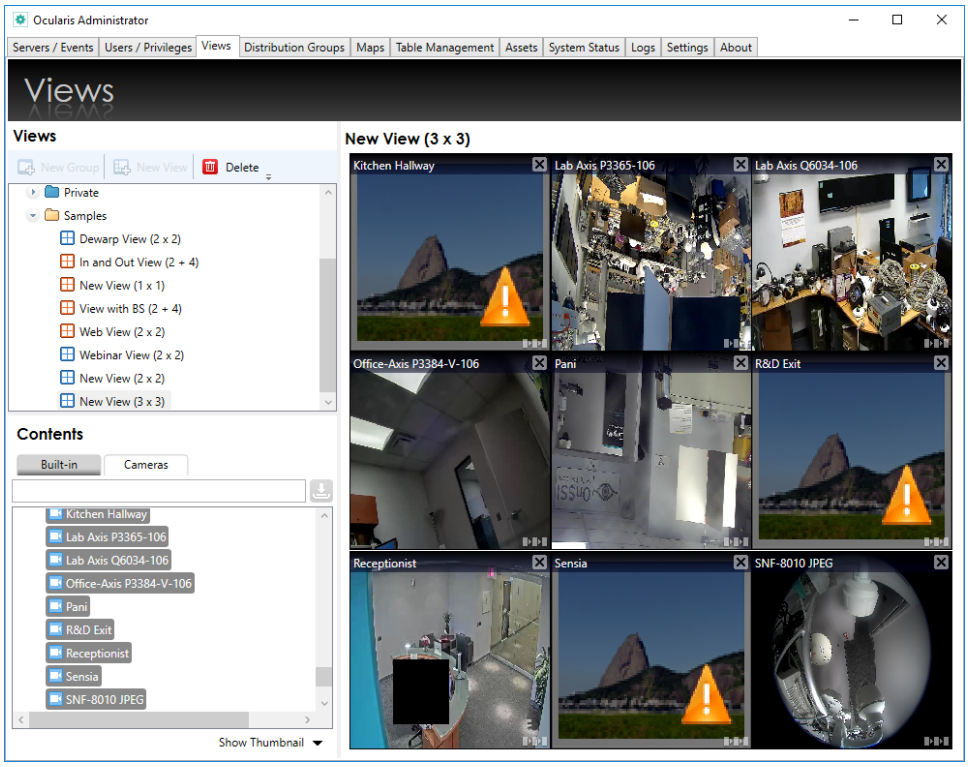


Figure 103 Populate View in One Easy Step



If you select more cameras than panes in the view, you'll see a message that there is not enough room. You can proceed by populating the first x cameras in the available panes.

If you use the drag-and-drop method, the system will begin populating cameras in the pane you dropped off to. Therefore, to populate the entire view, make sure you drag-and-drop to the first (upper left) pane.

If there is already a pane populated in the view, the system ask if you want to skip over the already populated view pane. If you select 'Yes', it will populate the panes but leave the existing camera in place and skip over that tile and continue populating cameras. Selecting 'No' will overwrite the existing camera.

9.7.2 View Modification

View modification is limited to renaming the view or changing the contents of a pane within the view. Reconfiguring the view layout is not available. Therefore if, for instance, you need to change the view layout from a 2 x 2 to a 3 x 3, you should delete the 2 x 2 view and create the 3 x 3 view from scratch.

To Rename a View

1. In the Views Tab, double-click the view you would like to rename.

Type the new name for the view.

Press [**ENTER**].

To Delete a View

1. In the **Views** Tab, select the view which you would like to delete.

   Click the **Delete** icon.

   An "*Are you sure that you want to delete this view?*" prompt appears.

Click **Yes** to delete the view.

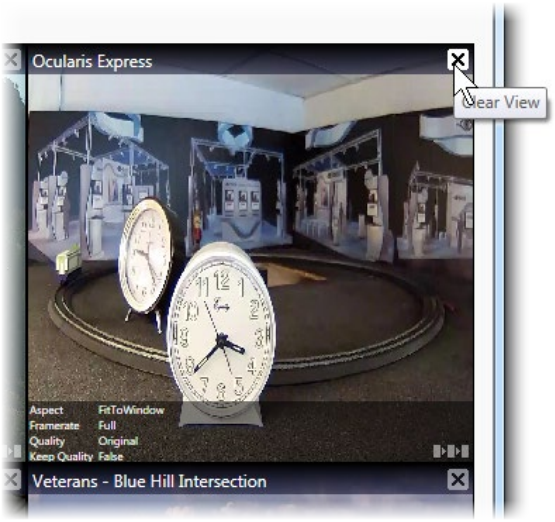
To Modify Contents of a View Pane

1. In the **Views** Tab, select the view which you would like to modify.

4. To change the configuration of an existing pane, click the pane to view the pane configuration settings. Make changes as required.

5. To replace a pane with a different component (camera, carousel, hot spot, etc.) you may:
   - Remove the pane content by clicking the **Clear View** icon in the pane.

Figure 104 Click Clear View to remove pane contents



   - Replace the pane contents by dragging & dropping a camera thumbnail or built-in type onto the pane.

Note: *Views may also be modified from within Ocularis Client.*

9.7.3 Shared Views

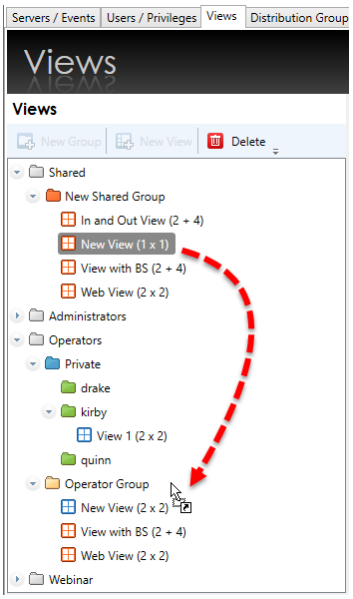
Once a shared view is created underneath the Shared folder, additional steps must be taken in order to share it. It must be assigned to the desired user group(s).

Note: *Shared Views may also be created, modified, or shared from within Ocularis Client by administrator users.*

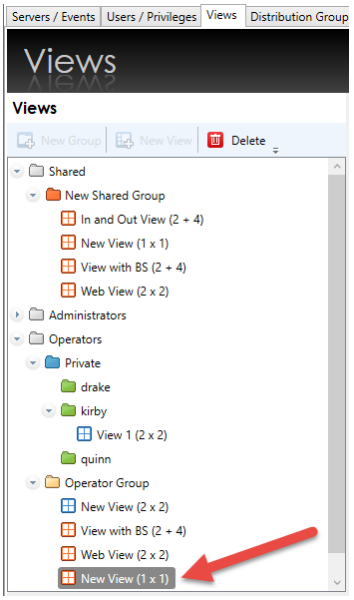
9.7.3.1 To Share a View with a User Group

1. In the **Views** Tab, expand both the view you would like to share under the Shared folder as well as the User Group (and its corresponding view group) or user that you wish to share the view with.
6. Drag and drop the view from the Shared view group to the view folder for the desired user or user group. Notice how the mouse cursor changes when it is positioned correctly over the destination folder.

Figure 105 Sharing Views



Drag and drop to share a view



Shared views displayed in orange

7. Repeat this procedure to share this view with other users or user groups or to share other shared views with any user group.

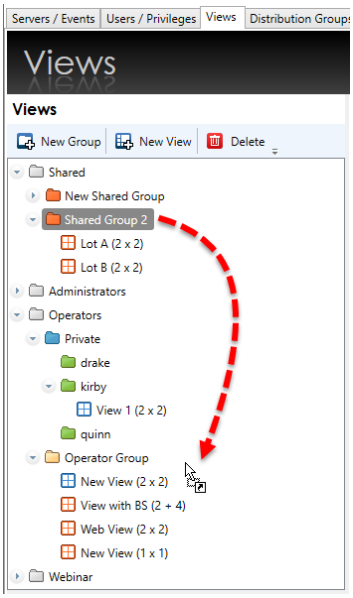
Additionally, entire groups of shared views may also be shared, making it easy to share multiple views in one step.

9.7.3.2 To Share a View Group with a User Group

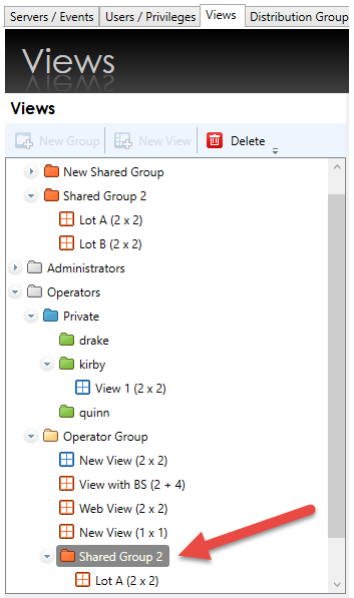
1. In the **Views** Tab, expand both the view group/folder you would like to share under the Shared folder as well as the User Group (and its corresponding view group) that you wish to share the view group with. Shared groups may not be shared with individual users, only groups.

2. Drag and drop the view group (folder) from the Shared view group to the view folder for the desired user group. Notice how the mouse cursor changes when it is positioned correctly over the destination folder.

Figure 106 Sharing View Groups



Drag and drop to share a view group



Shared Groups displayed in orange

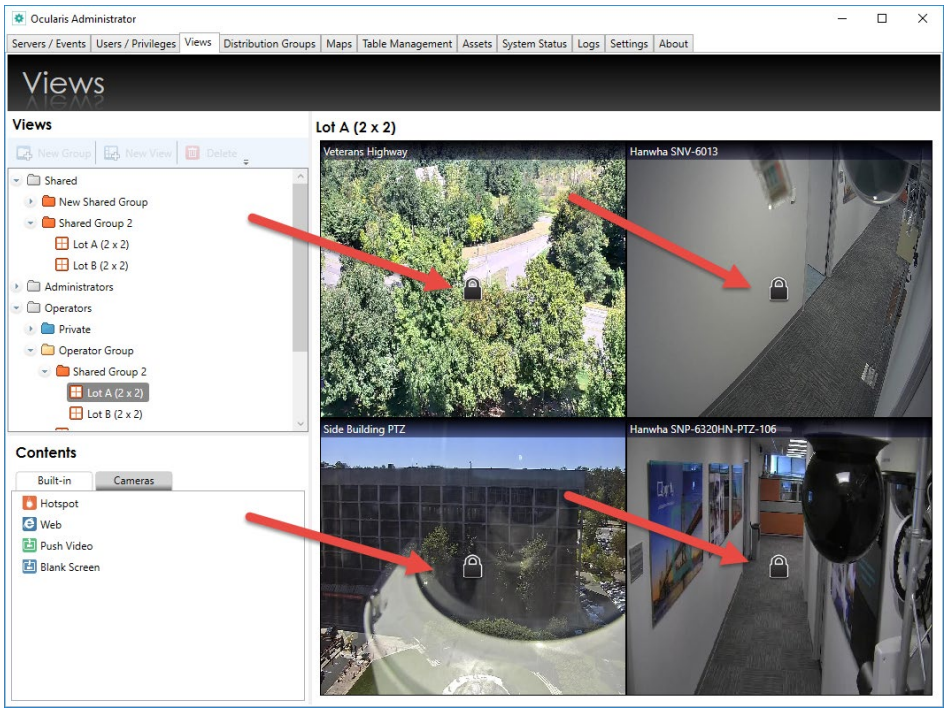
3. Repeat this procedure to share this view group with other user groups or to share other shared views with any user group.

9.7.3.3 Modifying Shared Views

Shared views may be modified the same way as other views (see *To Modify Contents of a View Pane* on page 121). However, only the *admin* user or member of the Administrators group can modify a shared view and it can only be modified when selected under the Shared view group. When a shared view is selected under a user group, a 'padlock' icon appears over the pane to indicate that the view may not be modified.

Note: *Shared Views may also be modified from within Ocularis Client by administrator users.*

Figure 107 Padlock indicates view may not be modified in this selection



Changes made to a shared view will be reflected for everyone with permission to access the view.

***Note**: If you have a view or view folder open and switch tabs, you will be returned to the same place upon reentering the Views Tab.*

9.7.4 Configuring View Content Types

Once view panes are populated with content, specific parameters may be set for each content type. The following section will discuss:

- Camera Configuration
- Carousel Configuration
- Hot Spot Configuration
- Push Video Configuration
- Web Page Configuration
- Blank Screen Configuration

9.7.4.1 Camera Output Configuration

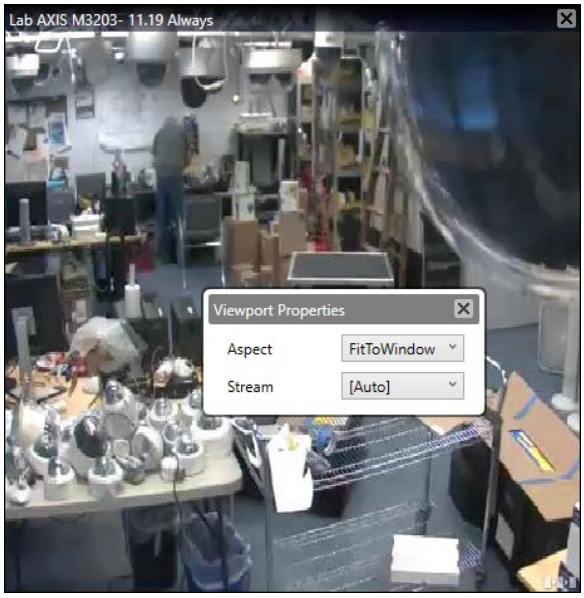
Actual video configuration for camera resolution and recording is done on the recorder. Configuration for camera output here refers to how the camera's video appears in the *Ocularis Client*.

9.7.4.2 To Configure Camera Output

1. In the **Views** Tab, select the view which contains the pane with the camera video you wish to configure. (For information on creating a view see *To Create A View within a Folder* on page 115.)
2. Click on the pane with the video you wish to configure.

   A *Viewport Properties* pop-up appears corresponding to the type of pane content selected (in this case, a camera). View pane contents with a single camera is considered a one camera carousel. (More details on carousels in the next section).

Figure 108 Click on the pane to modify parameters



You have the option to modify the following *Camera Overlay Parameters*:

Aspect	Useful for wide screen video output, the default option, **Fit to Window** will cause the video to be stretched to fit the window pane and may cause the video to appear slightly distorted. The option **Keep Original** may result in black vertical or horizontal bars surrounding the video when viewed in *Ocularis Client*.
Framerate	**Version 4.x and prior recorders only.** This setting is the framerate for the camera while viewing Live video in *Ocularis Client*. Available options are: **Full** (default), **Medium** or **Low**. Save bandwidth by selecting Medium or Low.
Quality	**Version 4.x and prior recorders only.** Options are: **Original**, **Super High**, **High**, **Medium**, and **Low**. This setting applies to Live video. To save on bandwidth, lower the image quality. The video from the camera is re-encoded to a JPEG format on the server before being sent to *Ocularis Client*. The default quality setting, **Original**, provides full quality of the original video. **Low** quality re-encodes the image to an output width of 160 pixels and a JPEG quality level of 20%.
Keep when maximized	**Version 4.x and prior recorders only.** When an individual pane is maximized in *Ocularis Client*, the default is to display the video in its Original quality. Check this box to maintain the quality parameters set here when the pane is maximized to full screen.

Stream	Version 5.2.1 or later recorders. Select a camera stream to display as the default stream from the camera for this view. If you do not see this option on a v5.2.1 or later camera, Stream 1 needs to be assigned a video classification on the recorder. The default selection is [Auto]. See Alternate Default Live Stream below for more information.

To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up.

9.7.4.3 Alternate Default Live Stream

In Ocularis 5 recorders, multiple live streams may be configured to display within Ocularis Client. The number of streams varies from camera to camera.

Administrators can select a default live stream for the camera to use when it initially displays in the view in *Ocularis Client*. The system will automatically set '[Auto]' as the default stream. This allows Ocularis to initially display the best stream in a view based on the size of the pane.

This feature benefits those installations where bandwidth may be a consideration and/or views with many high resolution cameras are used. Selecting a lower resolution as the default stream, will allow the view to be drawn more quickly and aid in general performance. The operator, given the appropriate permissions, may manually select a higher resolution stream where needed.

Additionally, administrators can override the '[Auto]' selection and identify any stream as the default live stream.

When the pane is viewed with Ocularis Web or Mobile, it will always default to [Auto], even if another stream is selected as the default.

9.7.4.4 Prerequisites

The following must be done in order for this feature to function properly:

- In the Ocularis 5 Recorder, multiple streams for the camera must be configured.
- Each stream, including Stream 1, must be assigned a unique video classification. See Adding Camera Streams and Configuring Camera Streams for more information.
- The Ocularis 5 Recorder Proxy must be installed and configured. Only one instance is needed per Master Core Server. This component is required even if the system does not utilize event alerting.
- All Ocularis components (Base, Administrator, Client and Recorder Proxy) must be using the latest version of Ocularis.

9.7.4.5 To Set An Alternate Default Live Stream

Ensure that all prerequisites listed above are met.

1. In *Ocularis Administrator* **Views** tab, create a new view (it can be a Shared or dedicated view).
2. Drag and drop a camera from an Ocularis 5 recorder to an available pane.
3. Click the pane to display its *Viewport Properties*.
4. Click the *Stream* drop-down menu. All available streams are listed using the Video Classifications as identified in the Ocularis 5 recorder. Reminder, video classifications are labels that may be modified by the system administrator. Classifications on your system may be different than the example shown below in Figure 112.

   Note: *if you do not see the Stream option for a camera on a v5.3 or later recorder, it could mean the following:*
   - *The camera has only one stream.*
   - *The camera's Stream 1 does not have an assigned video classification in the recorder.*
   - *The Ocularis Administrator application was still open when the Ocularis Recorder Proxy service was restarted. Simply close and restart Ocularis Administrator.*

5. You can leave the default option at '[Auto]' or select the stream you would like to use as the default live stream for this particular view. Note that if you use this camera in another view, a different default stream may be identified in that view.

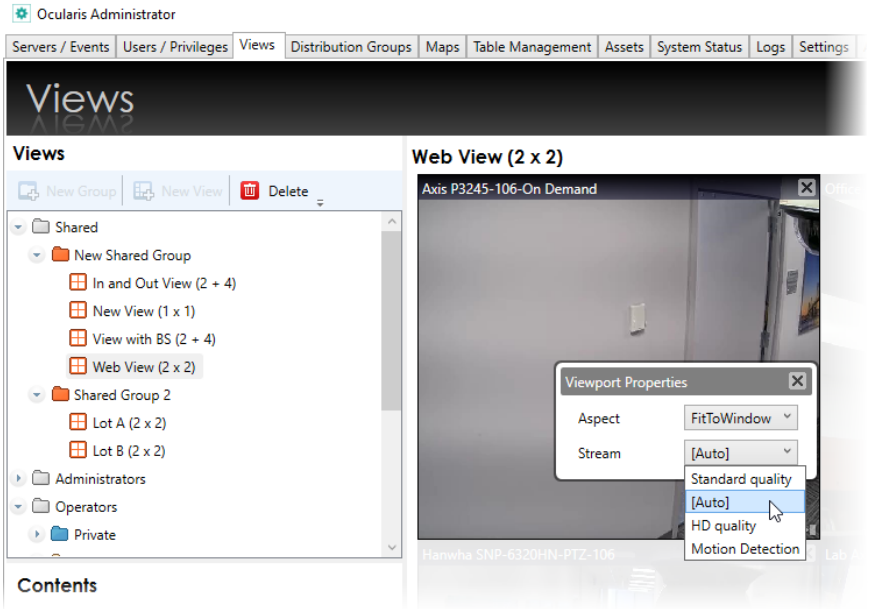
9.7.4.6 Auto

The default stream selection, '[Auto]', instructs *Ocularis Client* to display the most efficient stream in the pane based on system resources. Therefore, if the pane in one operator's *Ocularis Client* display monitor can support, for example, a resolution of 800x600, it will display the stream that is closest to this resolution. Another operator with a different quality monitor may be shown a different stream based on his/her screen resolution.

9.7.4.7 Carousels

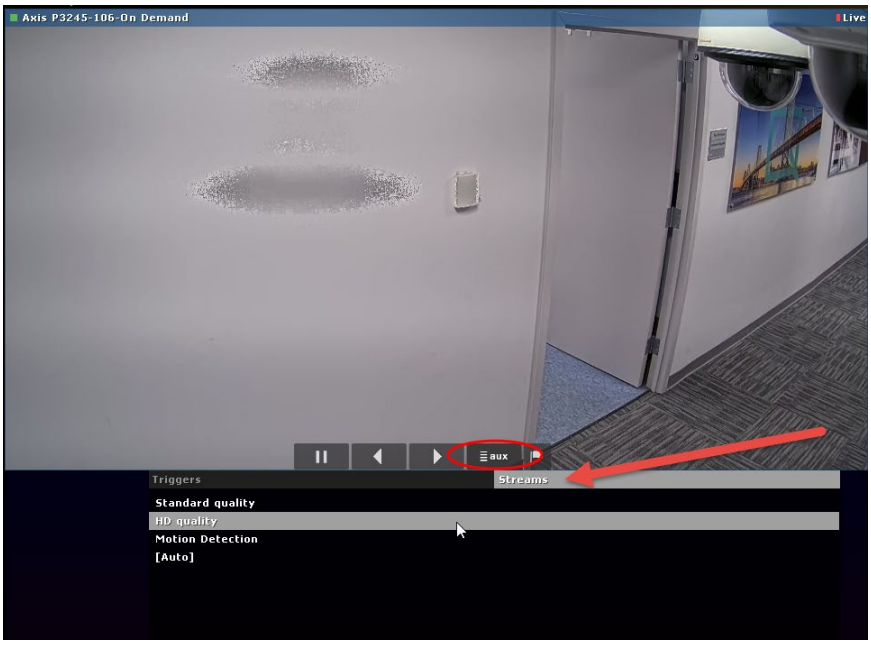
When you create a Carousel and select a specific stream (as opposed to '[Auto]'), *Ocularis Client* will attempt to display the same stream for all cameras in the carousel. If a particular camera does not have the stream identified in the *Viewport Properties*, it will display Stream 1.

Figure 109 Set the default stream



Operators (with appropriate permission) can select any stream from Ocularis Client's 'aux' button in the camera's view pane.

Figure 110 Use the 'aux' button to select a live stream



9.7.4.8 Streams used in Digital Zoom and Maximizing

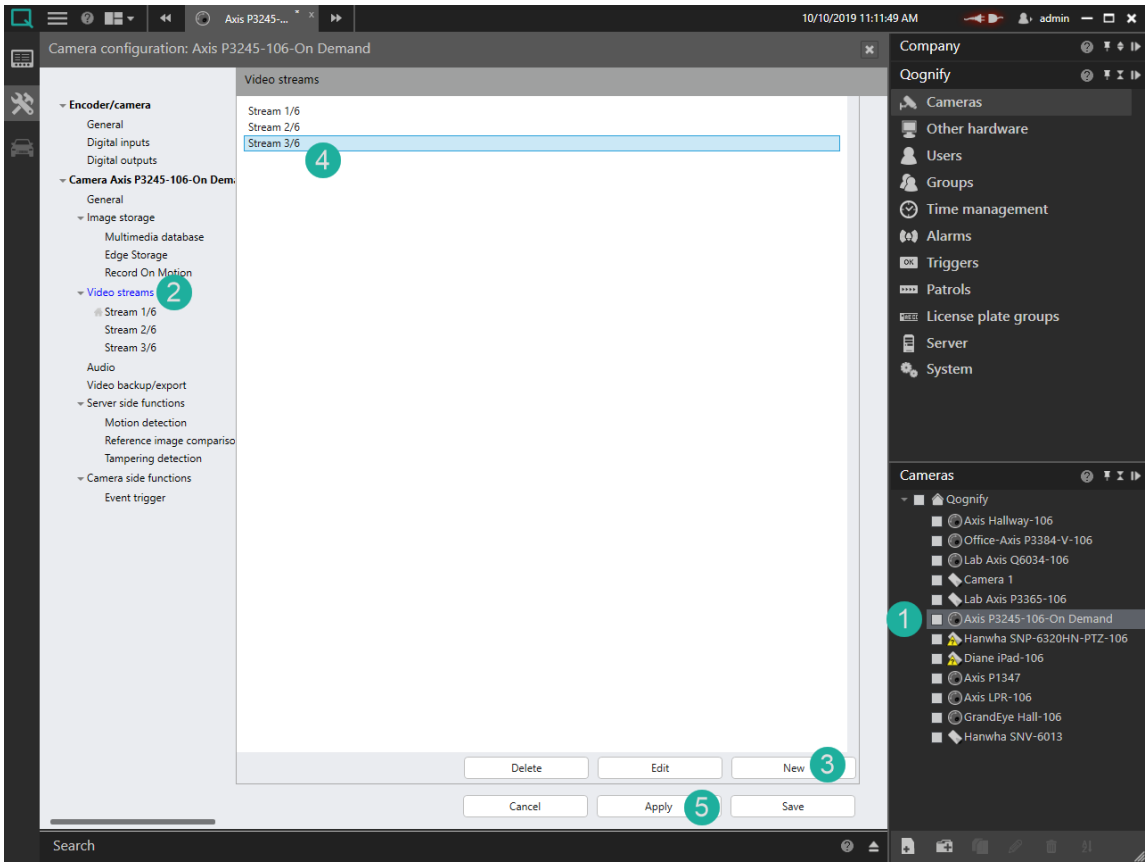
If the pane is set to '[Auto]', and the pane is maximized or the operator uses digital zoom, the highest resolution stream will be used and displayed. If a specific stream is set, this streams resolution will be used when maximized or with digital zoom.

9.7.4.9 Adding Camera Streams

Most cameras provide multiple streams that Ocularis 5 can tap into. The number of streams varies from manufacturer to manufacturer. Adding camera streams manuallyis easy to do. Refer to Figure 111 for the following instructions.

1. In the *Ocularis Recorder Manager*, select the camera that will have additional streams added **[1]**.
2. Select 'Video streams' **[2]**
3. Click 'New' **[3]**. A new stream will be listed **[4]**.
4. Repeat as needed. Click 'Apply' **[5]** when done.

Figure 111 Adding Camera Streams



9.7.4.10 Configuring Camera Streams

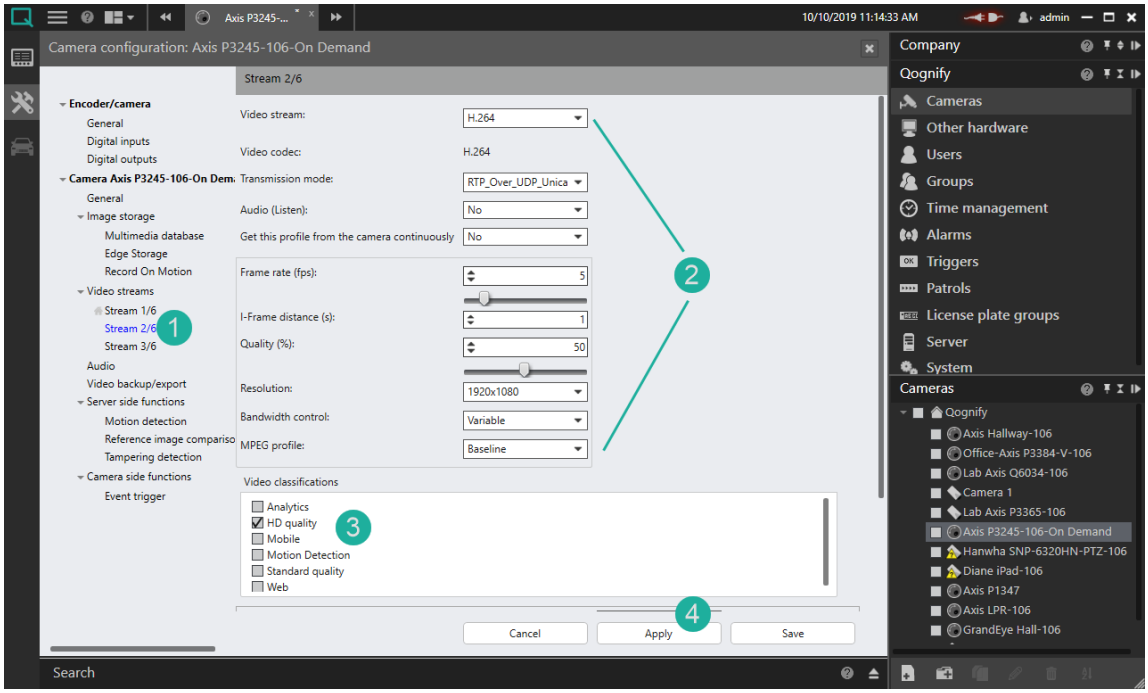
Each stream from a camera can have different settings. You may want one that is high resolution and another that is low resolution. You may want one that is H.264 and another that is MJPEG (This is camera dependent of course!). You may want one that is dedicated solely for motion detection analysis. Ocularis 5 gives you the flexibility to configure a camera's streams differently. You may also modify the text labels for video classifications to those which are more applicable to your installation. Refer to Figure 112 for the following instructions.

1. In the *Ocularis Recorder Manager* application, select the stream you wish to configure **[1]**.
2. Modify settings for this stream as desired **[2]**.
3. Select a 'Video classification' for this stream **[3]**. While more than one classification may be selected, it is not recommended. You may not select a classification for this stream that was already assigned to another stream for this camera.

> ***Note:*** *Video classifications for Stream 1/x will not appear until a second stream is added. Remember to go back and assign a video classification for Stream 1/x. This is required in order to set a default live video stream to a stream other than Streams 1/x.*

4. Click 'Apply' to save changes **[4]**.

Figure 112 Configuring a Camera Stream



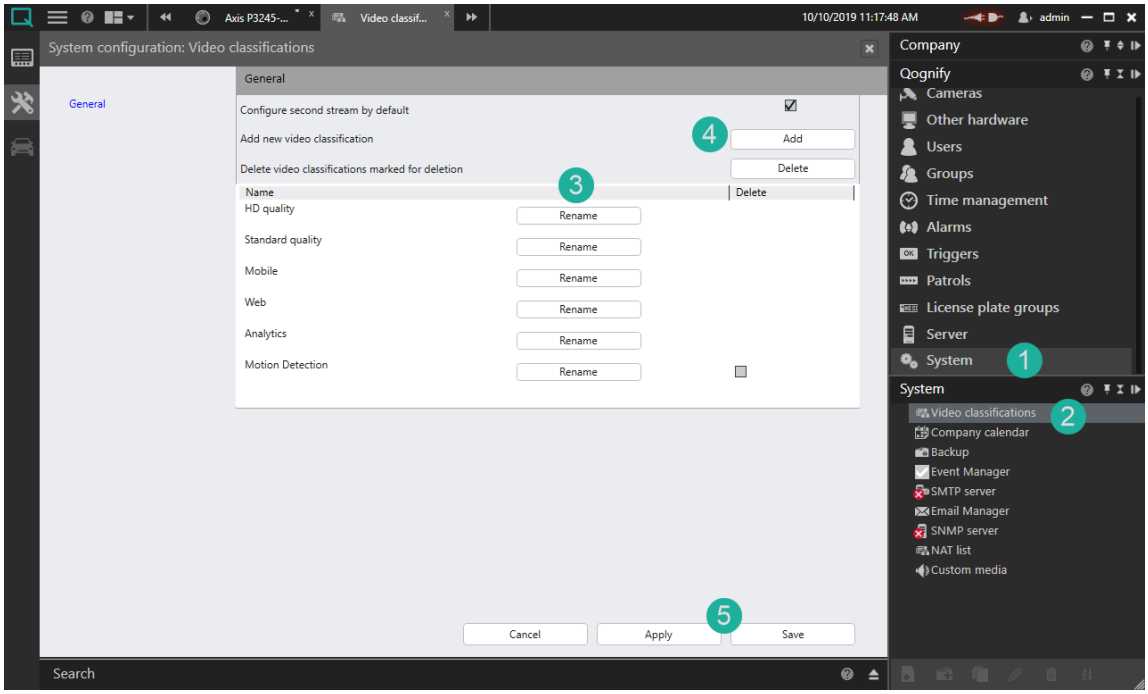
Note: *If using Ocularis 5 Web, be sure to configure at least one low resolution H.264 stream (i.e. under 600 pixels high). This will allow the stream to display in a view with numerous panes.*

9.7.4.11 Video Classifications in Ocularis 5

Video classifications are labels that can be associated with each stream from a camera. In order to use multiple live streams in *Ocularis Client*, each stream must be assigned a video classification. We recommend only one video classification per stream. You may not assign the same video classification to multiple streams within the same camera.

In the *Ocularis Recorder Manager* application, (see Figure 113 below) select 'System' **[1]** and then 'Video classifications' **[2]**. The five default video classifications appear. You may 'Rename' any existing video classification **[3]** or Add new ones **[4]**. You may only delete video classifications you have added. You may not delete any of the five streams that ship with the product (even though you can rename them). Make the video classification labels something easy to understand as this is how the stream will be identified in *Ocularis Client* and *Ocularis Administrator*. Remember to click 'Save' or 'Apply' **[5]** after making any changes.

Figure 113 Video Classifications



9.7.5 Carousel Configuration

Carousel configuration includes: identifying which cameras are to be used in the Carousel, the video parameters as displayed in Ocularis Client and the image's dwell time.

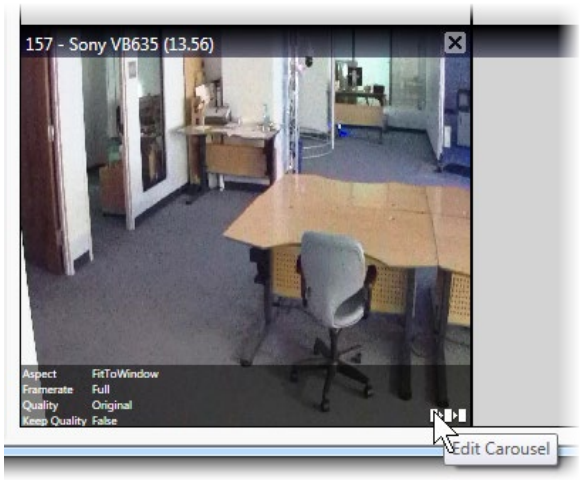
9.7.5.1 To Configure A Carousel

1. In the **Views** Tab, select the view (or create a new view) which contains the pane with the carousel you wish to configure. (For information on creating a view see *To Create A View within a Folder* on page 115.)

   Assign one camera to the pane (drag and drop) which will display the carousel.

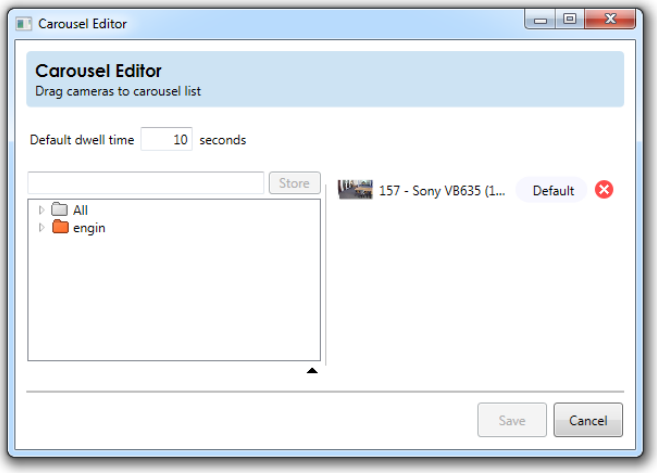
2. Click the **Carousel Edit** icon found in the overlay section of the pane (lower right).

Figure 114 Carousel Edit icon



A *Carousel Editor* pop-up appears.

Figure 115 Carousel Editor

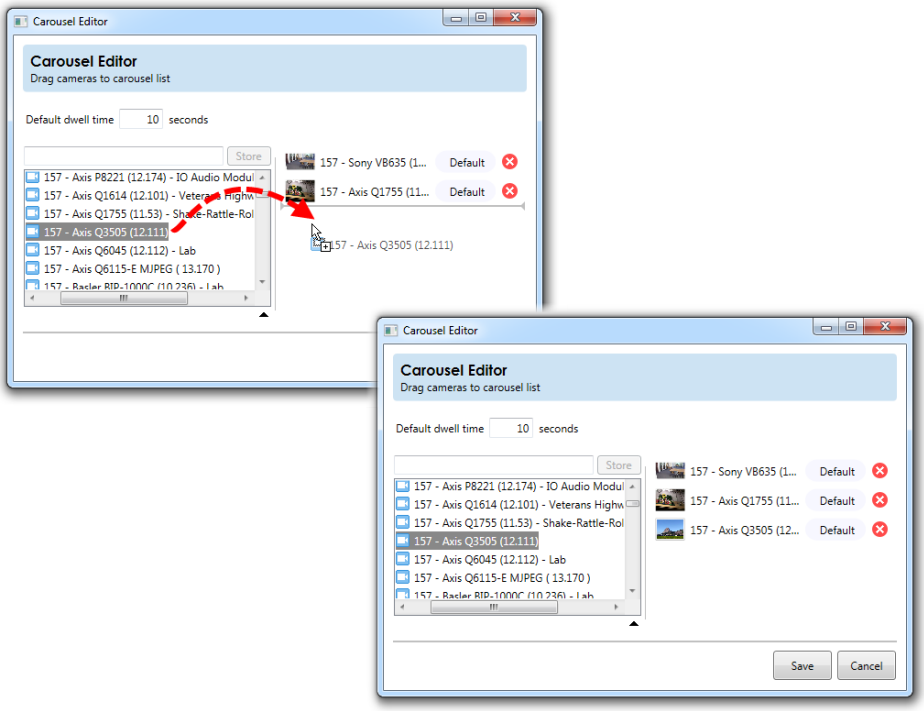


The goal is to create a list of the cameras you wish to display in the carousel in the camera list on the right of the pop-up. You have the same tools in this dialog to locate cameras as you do when building a view. (See *Camera Preview* on page 110 and *Camera Filter* on page 112).

> ***Tip***: *You may widen the dialog box to be able to read lengthy camera names more easily.*

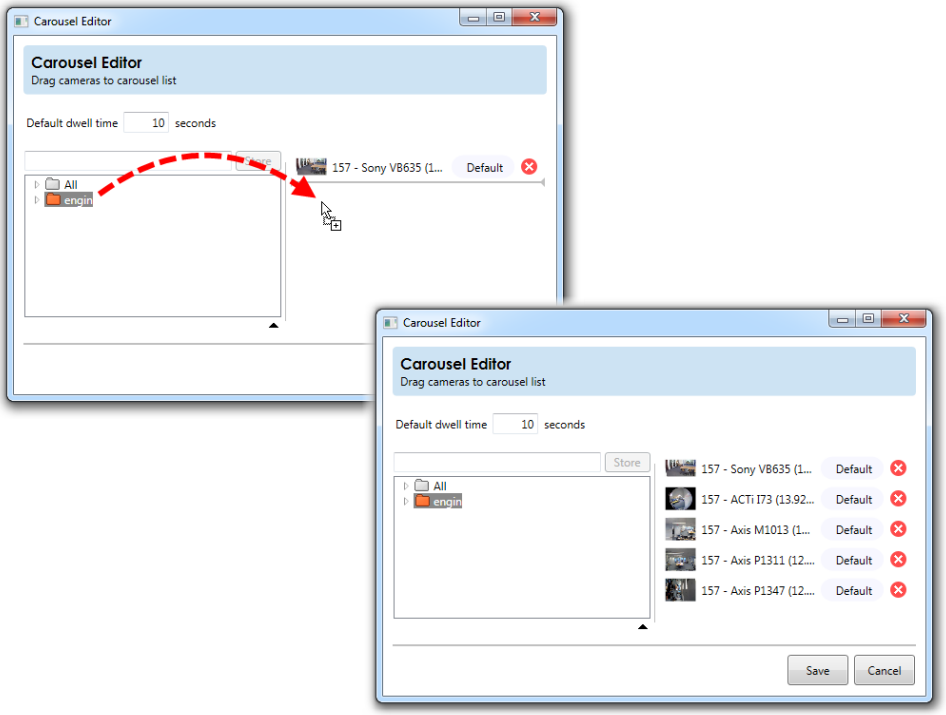
Once you locate the desired camera in the camera list on the left, drag and drop the camera to the camera list on the right.

Figure 116 Creating a carousel list



Alternatively, if you've saved a camera filter in a folder, you can drag the entire folder to the camera list.

Figure 117 Drag a Folder to create a carousel

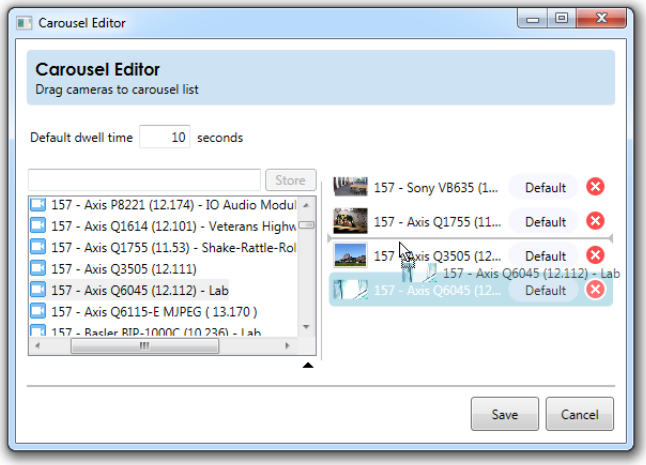


***Note**: At least one camera must be selected before you are able to drag an entire folder.*

Carousel Order

The progression of video will go from each camera in the order listed here. If you wish to reorder, simply drag and drop the camera to the correct order.

Figure 118 Reorder a Camera in a Carousel



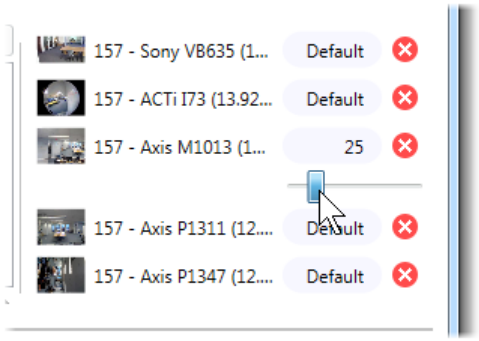
Dwell Time

Dwell Time is the amount of time, in seconds, that camera video is displayed in the *Ocularis Client* before switching to the next camera in the list. The default Dwell Time is 10 seconds.

You may modify the default dwell time for all cameras shown by simply changing the number in the **Default dwell time** field. (see Figure 115).

If you want a single camera to have a different dwell time than the default, click the **Default** button next to the camera name. A slider becomes visible.

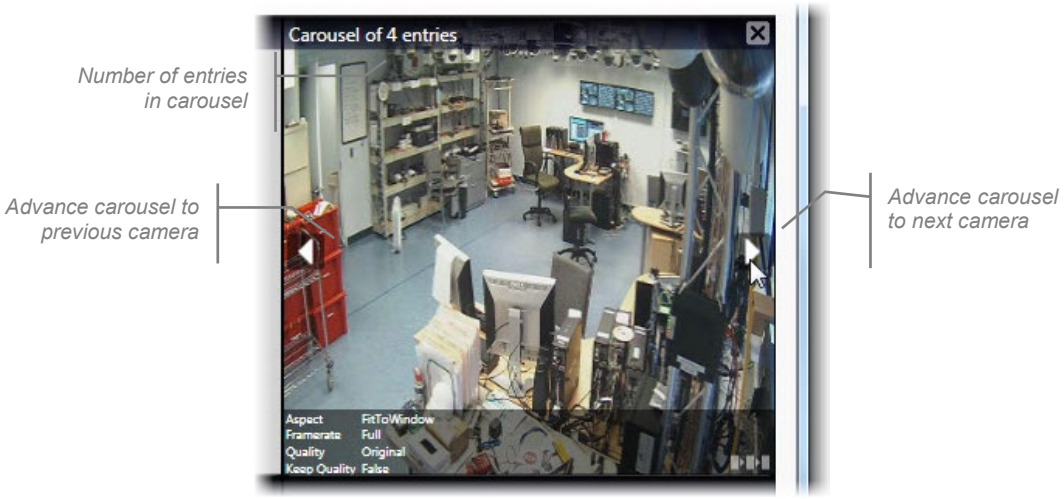
Figure 119 Change the Default Dwell Time



Drag the slider left or right to see the amount of seconds change. Stop when you arrive at the desired amount.

3. You may do this for each and every camera listed.
4. To remove a camera from the carousel list, click the Delete icon to the right of the camera name.
5. When the carousel configuration is complete, click **Save**.

Figure 120 A configured carousel in the Views Tab



The **Views** tab shows the carousel with left and right arrows. The top of the pane indicated the number of cameras in the carousel (e.g. “Carousel of 4 entries”). Click the left or right arrow to scroll through the display of the cameras you selected for the carousel

TO REORDER CAMERAS IN A CAROUSEL

1. In the **Views** Tab, select the view with the carousel you wish to configure.
2. Click the **Carousel Edit** icon found in the overlay section of the carousel pane (lower right).
3. In the *Carousel Editor* pop-up, drag and drop the cameras listed to the desired order. (see Figure 118*).*
4. Repeat for all cameras you wish to reorder.
5. Click **Save** when done.

TO REMOVE CAMERAS FROM A CAROUSEL

1. In the **Views** Tab, select the view with the carousel you wish to configure.
2. Click the **Carousel Edit** icon found in the overlay section of the carousel pane (lower right).

   Locate the camera you wish to remove.
3. Click the **Remove Camera** icon.
4. Repeat for all cameras you wish to remove.
5. Click **Save** when done.

9.7.5.2 To Change or View the Dwell Time for an Individual Camera

1. In the **Views** Tab, select the view with the carousel you wish to configure.
2. Click the **Carousel Edit** icon found in the overlay section of the carousel pane (lower right).

   Locate the camera whose dwell time you wish to modify.
3. Click the **Dwell Time** button (see Figure 119).
4. When the dwell time slider appears, drag it left or right to modify the dwell time.
5. Repeat for each camera whose dwell time you wish to modify.
6. Click **Save** when done.

9.7.5.3 To Configure Video Displayed in a Carousel

Video parameters displayed while viewing the carousel in Ocularis Client may be adjusted, similar to adjusting video for a single camera.

1. In the **Views** Tab, select the view which contains the pane with the carousel.
2. Click on the pane video.
3. In the resulting *Viewport Properties* dialog, modify the parameters as defined in the following table. The settings will apply to all camera video displayed in the carousel.

Aspect	Useful for wide screen video output, the default option, **Fit to Window** will cause the video to be stretched to fit the window pane and may cause the video to appear slightly distorted. The option **Keep Original** may result in black vertical or horizontal bars surrounding the video when viewed in *Ocularis Client*.
Stream	Version 5.2.1 or later recorders. Select a camera stream to display as the default stream from the camera for this view. If you do not see this option on a v5.2.1 or later camera, Stream 1 needs to be assigned a video classification on the recorder. See Alternate Default Live Stream below for more information.

To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up.

***Note**: The properties: Framerate, Quality and Keep when maximized have been removed for all current and legacy recorders for Carousels, Hotspots, Blank Screens and Push video panes.*

9.7.6 Hot Spot Configuration

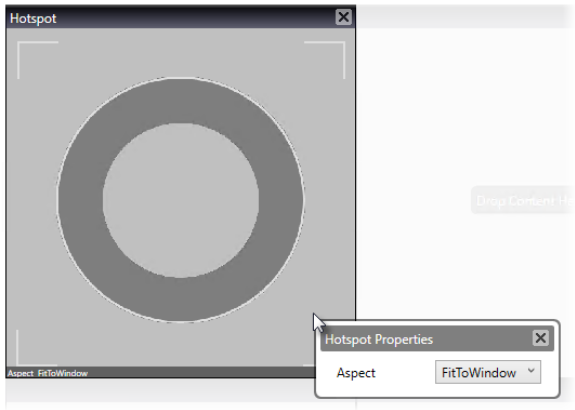
Administrators can configure the quality of the camera video displayed in a Hot Spot pane.

9.7.6.1 To Configure A Hot Spot

1. In the **Views** Tab, select the view which contains the Hot Spot. (For information on creating a view with a hot spot, see *To Create A View within a Folder* on page 115.)
2. Click on the pane with the hot spot.

   A *Hotspot Properties* pop-up appears.

Figure 121 Configuring Hot Spot Output



You have the option to modify the following:

Aspect	Useful for wide screen video output, the default option, **Fit to Window** will cause the video to be stretched to fit the window pane and may cause the video to appear slightly distorted. The option **Keep Original** may result in black vertical or horizontal bars surrounding the video when viewed in *Ocularis Client*.

To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up.

***Note**: The properties: Framerate, Quality and Keep when maximized have been removed for all current and legacy recorders for Carousels, Hotspots, Blank Screens and Push video panes.*

9.7.7 Push Video Configuration

Push Video panes are used in *Ocularis Client* to manually push video from one logged in Ocularis Base user to another logged in user. The Push Video function uses port 7008. Push video with Ocularis is supported with all Ocularis models.

9.7.7.1 To Configure Push Video

1. In the **Views** Tab, select the view which contains the Push Video Port pane. (For information on creating a view see *To Create A View within a Folder* on page 115.)
2. Click the Push Video pane.

Figure 122 Configuring a Push Video Pane

You have the option to modify the following:

Window Index	If there are multiple panes configured for Push Video this index determines the order in which pushed video will appear in the view.
Aspect	Useful for wide screen video output, the default option, **Fit to Window** will cause the video to be stretched to fit the window pane and may cause the video to appear slightly distorted. The option **Keep Original** may result in black vertical or horizontal bars surrounding the video when viewed in *Ocularis Client*.

To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up.

***Note**: The properties: Framerate, Quality and Keep when maximized have been removed for all current and legacy recorders for Carousels, Hotspots, Blank Screens and Push video panes.*

9.7.8 Web Configuration

In addition to camera video, panes may be populated by an HTML page accessible via URL or IP Address. Typical examples of these include:

- Company websites or logos
- Online or static maps

- Link collections
- IP Camera configuration page

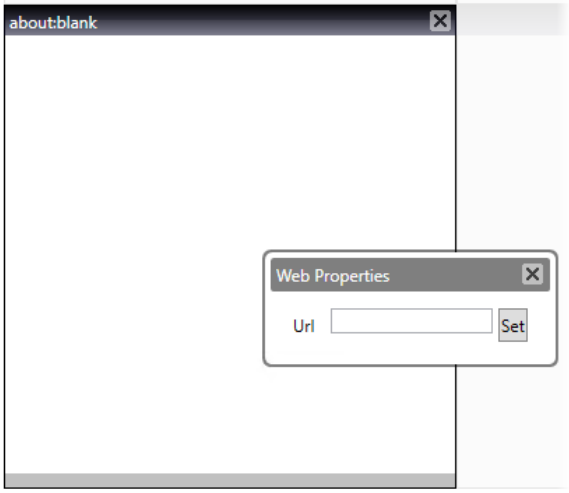
***Note**: Panes with web pages or images may not be maximized in Ocularis Client. For web pages, we recommend using a large size pane or even a 1 x 1 pane.*

TO CONFIGURE A WEB PANE

1. In the **Views** Tab, select the view which contains the Web Page. (For information on creating a view see *To Create A View within a Folder* on page 115.)
2. Click on the pane with the Web Page.

   A *Web Properties* pop-up appears.

Figure 123 Configuring a Web Page Pane



Type in the URL or IP Address for the content to be displayed. You will see a preview of the page.

To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up. The web page will now appear in the *Ocularis Client* and the user will be able to navigate the page using embedded links.

You may also link to an image located on the network or internet by inserting the file's full path and filename in the Url field.

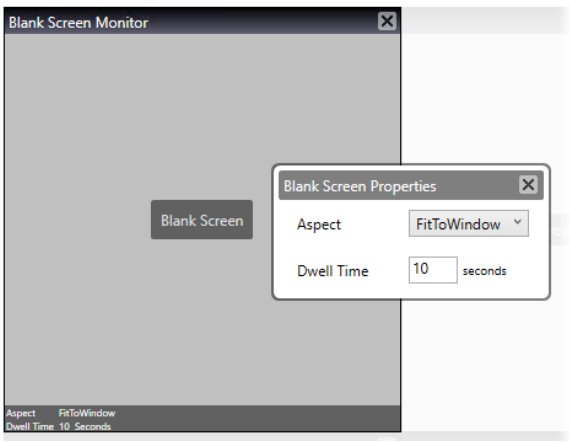
9.7.9 Blank Screen Configuration

As the name indicates, the view pane configured with a Blank Screen remains 'blank' until populated by video triggered by an event. The event trigger is configured in *Ocularis Administrator* and is discussed in Simple Event Rules on page 46.

9.7.9.1 To Configure a Blank Screen

1. In the **Views** Tab, select the view which contains the Blank Screen. (For information on creating a view see *To Create A View within a Folder* on page 115.)
2. Click on the pane with the Blank Screen. A *Blank Screen Properties* pop-up appears.

Figure 124 Configuring a Blank Screen Pane



You have the option to modify the following:

Aspect	Useful for wide screen video output, the default option, **Fit to Window** will cause the video to be stretched to fit the window pane and may cause the video to appear slightly distorted. The option **Keep Original** may result in black vertical or horizontal bars surrounding the video when viewed in *Ocularis Client*.
Dwell Time	This is the amount of time in seconds that video will be displayed in a Blank Screen pane; applies to low and medium priority only.

To save settings, click on another part of the view pane or click the Close icon ('X') on the pop-up.

***Note**: The properties: Framerate, Quality and Keep when maximized have been removed for all current and legacy recorders for Carousels, Hotspots, Blank Screens and Push video panes.*

10 Assets Tab

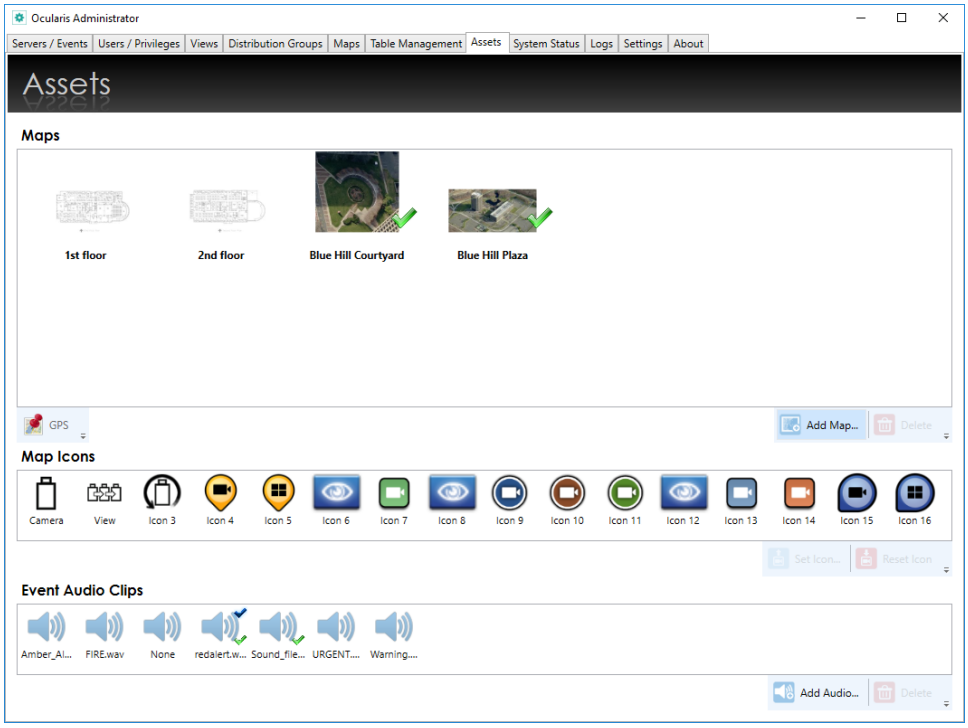
The **Assets** Tab displays the centralized repository of all graphic images and audio files used in Ocularis Base. Administrators import graphic files and icon assets in this tab that may be used to configure Ocularis Maps.

Each organization will have a unique set of images and there is no limit to the amount of images that may be imported. An unlimited amount of audio files for use in alert notifications are also imported here.

Graphic images are imported through the Assets Tab and configured in the Maps Tab.

Audio files are imported through the Assets Tab and configured in the Server / Events Tab.

Figure 125 Assets Tab



The Assets Tab is divided into three sections:

1. The upper section displays imported map images.
2. The middle section displays default and imported map icons used for cameras and other items on maps.
3. The lower section displays imported sound files.

10.1.1 Maps

This area houses the navigation maps available for use within the Ocularis Maps feature. Navigation maps can be any descriptive image of the surveillance installation – geographical maps, CAD drawings, aerial photographs, architectural plans, etc. Image file types supported are: .jpg, .png, .gif and .bmp. The system supports an unlimited number of maps.

10.1.2 Map Icons

Icons identify items placed on Ocularis Maps. Icons can be any imported .png image file. Typically, icon images are of IP cameras. The first icon on the left is reserved for the default display when a camera is placed on a map. There is also a default icon for when a view is placed on a map.

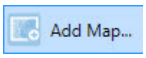
Administrators import maps and icons here in the **Assets** tab first and then continue with map configuration in the **Maps** tab.

10.1.3 Event Audio Clips

Audio files placed here may be used by the administrator to configure the sound played when an event occurs. The default sound is set on the Ocularis Base and is identified by the green checkmark. The default “sound” may be **None,** which therefore indicates no sound during alert notification. The audio file type supported is: .wav.

10.2 Maps

TO ADD A MAP TO THE ASSETS TAB

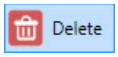
1. In the **Assets** Tab, click the **Add Map** button. 

2. Browse for the image file and select it.
3. Click **Open**.

A thumbnail image of the map appears in the *Maps* area of the Assets Tab. Images are displayed in alphabetical order of the filename.

10.2.1 To Delete A Map from the Assets Tab

Use the following procedure to remove a map image from the Ocularis database. This will not delete the image file from the source location.

1. In the **Assets** Tab, select the map to be removed. You may use the [**SHIFT**] or [**CTRL**] function keys to select multiple files.
2. Click the **Delete** button. 

   An "*Are you sure you want to delete…*?" pop-up window appears.

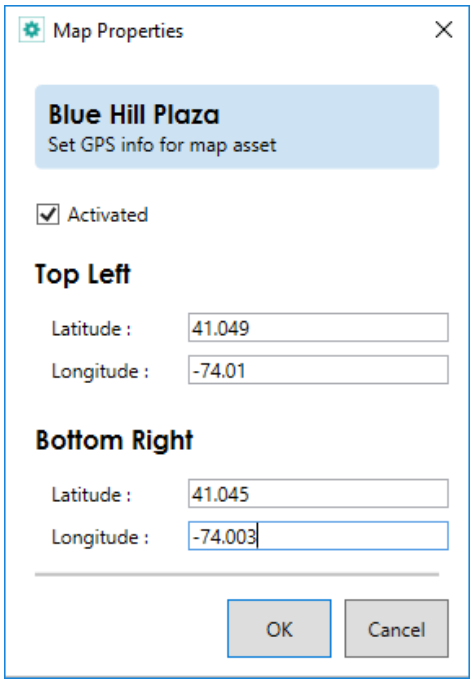
3. Click **Yes** to remove the map(s).

10.2.2 Map Coordinates

For certain integrations, you can manually configure the GPS coordinates of an Ocularis Map. This can later be used to see a camera in its proper on a map. This assumes the map is using a 'North UP' orientation.

1. Select the map that you want to configure.
2. Click the GPS pushpin button.
3. Make sure the 'Activated 'checkbox is selected.
4. Enter the Latitude and Longitude coordinates for the upper left corner of the map. If necessary, use the '-' character to indicate west of the prime meridian in Greenwich England or south of the equator.

Figure 126 Sample Coordinates for Pearl River, NY

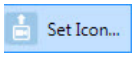


5. Enter the Latitude and Longitude coordinates for the lower right corner of the map.
6. Click **OK**.

10.2.3 Map Icons

To Import or Modify a Map Icon

Use the following procedure to set or replace an icon. Icon 1 is the default icon used when creating new items on a map so you may want to leave this icon as the default. Icon 2 is the default icon used for views.

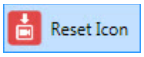
1. In the **Assets** Tab, select the icon to be set.
2. Click the **Set Icon** button. 

3. Browse to the image file and select it.
4. Click **Open**.

The icon is displayed in the *Icons* section of the Assets Tab.

To Remove a Map Icon

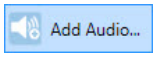
Use the following procedure to remove an imported icon image and reset it to the default.

1. In the **Assets** Tab, select the icon to be changed. You may use the [**SHIFT**] or [**CTRL**] function keys to select multiple icons.
2. Click the **Reset icon** button. 

The icon(s) should be reset.

10.3 Event Audio Clips

To Add an Audio File to the Assets Tab

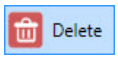
1. In the **Assets** Tab, click the **Add Audio** button. 

2. Browse for the sound file and select it. The maximum size of the .wav file is 4 MB.
3. Click **Open**.

An image with the name of the sound file appears in the *Audios* area of the Assets Tab. Sound files are displayed in alphabetical order of the filename.

10.3.1 To Delete An Audio File from the Assets Tab

Use the following procedure to remove a sound file from *Ocularis Administrator*. This will not delete the file from the source location.

1. In the **Assets** Tab, select the sound file to be removed.
2. Click the **Delete** button. 

   An "*Are you sure you want to delete…*?" pop-up window appears.

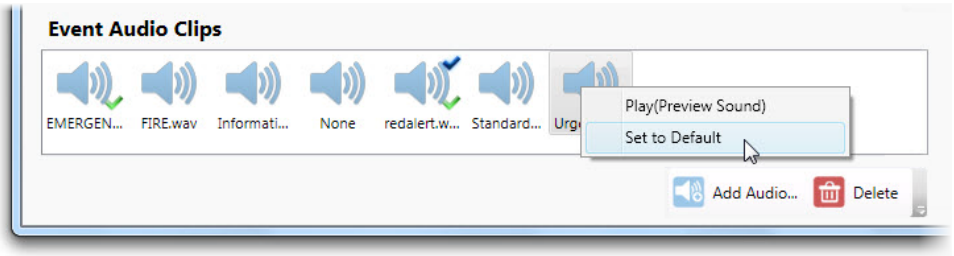
3. Click **Yes** to remove the audio file.

10.3.2 To Set or Modify the Default Audio Clip

Ocularis Base is shipped with one default sound file: *redalert.wav*. A blue checkmark symbol indicates the default sound in the **Assets** tab. When an alert notification is configured in the **Servers / Events** Tab, the default sound is assigned to the alert. If the default *Event Audio Clip* is a .wav file, that sound will play when the alert occurs. If the default *Event Audio Clip* is set to 'None', no sound will play when the alert takes place. Administrators can configure sound on an alert by alert basis. A green checkmark indicates that the sound file is already assigned for use to an alert.

1. In the **Assets** Tab, right-click the sound file to be set as the default. Or select 'None' to have no sound as the default
2. Select **Set to Default** in the resulting right-click menu.

Figure 127 Setting the default Audio Asset



The .wav file now is displayed with the green checkmark to indicate it as the default audio asset.

10.3.3 To Preview An Audio Clip

To preview the sound that a particular .wav file will make when the alert occurs:

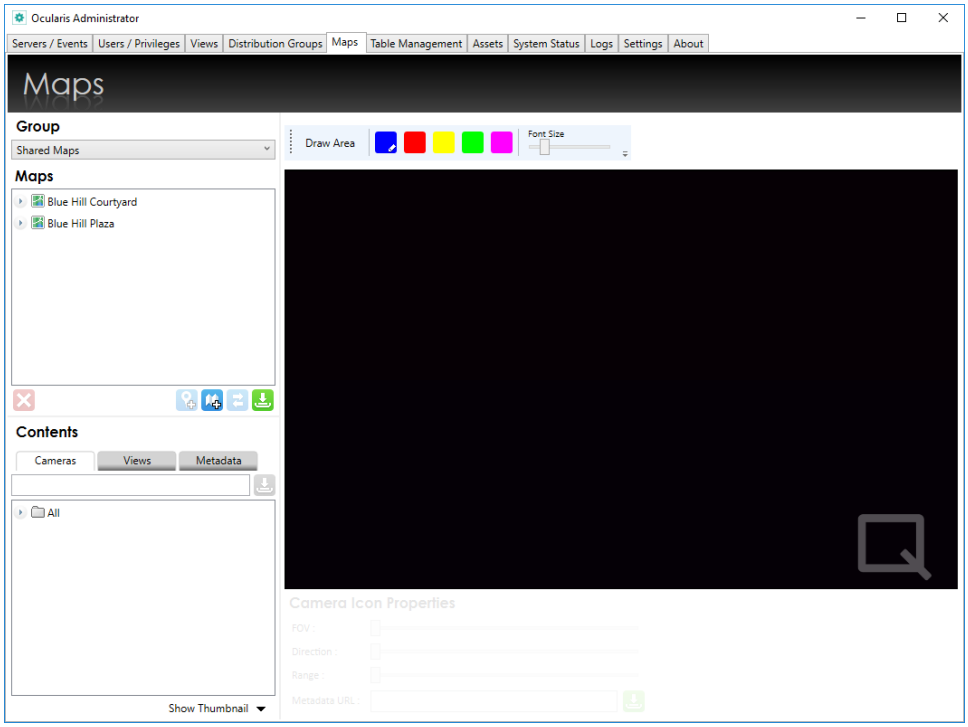
1. In the **Assets** Tab, right-click the audio clip to be previewed.
2. Select Play (Preview Sound) in the resulting right-click menu.

The .wav file now is played through the local pc speakers.

11 Maps Tab

Once maps and icons have been imported in the Assets Tab, they can be configured in the **Maps** Tab.

Figure 128 Maps Tab



The left side of the Maps Tab contains elements available for configuring a map and is segmented into a section for **Group** selection, **Maps**, and **Contents** (Cameras, Views and Metadata). The right side of the Maps Tab is the working area used to display and configure a map.

Maps are configured and organized by user group. Administrators should select the group for which the map should be configured. Maps may be configured for a single user group (“private”) or shared across multiple user groups (“shared”).

> ***Note**: If you know in advance that a map is to be shared among multiple groups, be sure to configure the map under the Shared Maps group from the beginning. See Sharing Maps on page 164.*

To Add a Map

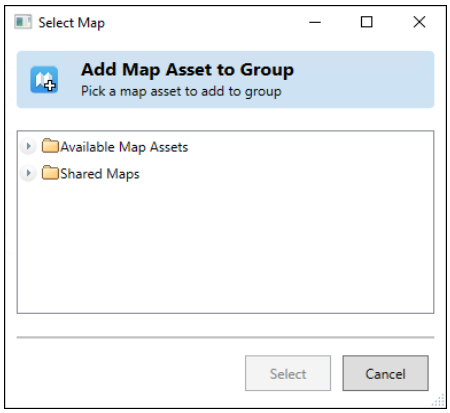
This procedure assumes that navigation maps have already been imported into the **Assets** Tab and may be used to add a Private or a Shared map. (See *To Add A Map to the Assets Tab* on page 143.)

1. In the **Maps** Tab, select the group from the *Group* drop-down menu for which the map should be available. If you would like the map to be shared between more than one user group, select *Shared Maps* in the drop-down **Group** list. *Shared Maps* is the default selection.

2. Click the **Add new map** icon.

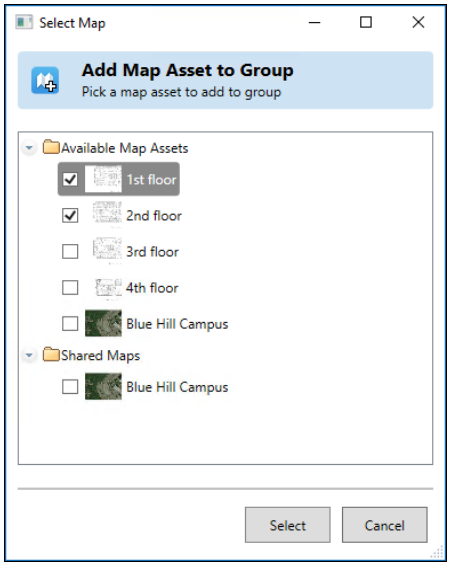
   The *Select Map* dialog box appears

Figure 129 Selecting a Map for a single group (Private)



This pop-up displays the list for *Available Maps* and *Shared Maps*. Available Maps are those which have been imported in the Assets Tab, but not yet assigned to this group or to the Shared Group. Expand Available Maps to see available map images.

Figure 130 Expand the Available Maps folder to choose a map

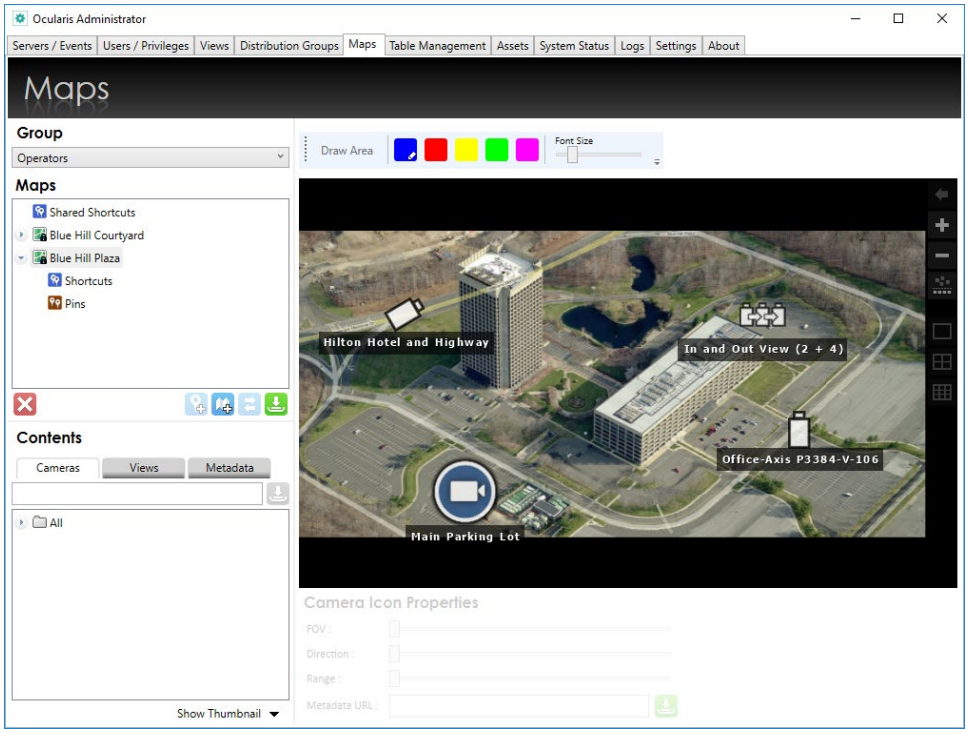


When creating a map to be shared by others, the maps displayed here, populated by maps that exist in the **Assets** Tab, are available for selection.

3. Select the map you wish to add. You may select multiple maps as well.
4. Click **Select**.

The selected map now appears in the Maps list. Expand the node to see its associated Shortcuts and Pins.

Figure 131 Added Map to Operators Group



To Change a Map Name

If desired, you may change the name of a map.

1. Under the desired group, double-click the map name in the Maps list. The name becomes editable.
2. Modify the map name and press **[ENTER]**.

A map name changed on a Shared Map will change the name for all groups that use the map. A map name changed for a single map in a user group will only be changed for that group. The map names in the Assets Tab will not be changed.

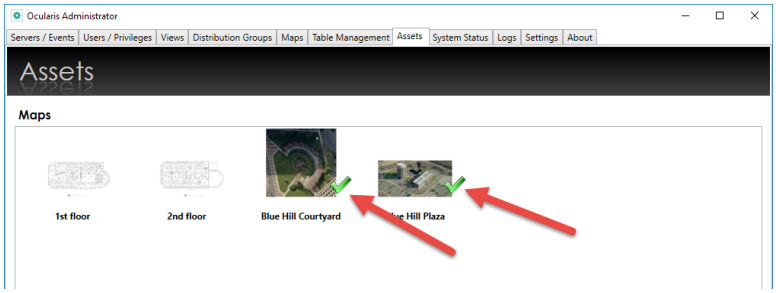
To Display a Map

You need to display a map in order to configure it. This procedure assumes that navigation maps have already been added for the User Group or Shared Maps group in the Maps Tab.

1. Under the desired group, double-click the map name in the Maps list.
2. Reposition the image in the working area by clicking and dragging the map to the desired location.

Once a map is added to a group, a green checkmark icon appears next to the map image in the **Assets** Tab. This helps administrators manage system assets.

Figure 132 Used Maps in Assets Tab shown with Green Checkmark



In the example shown in Figure 132, the *Blue Hill Courtyard* and *Blue Hill Plaza* maps have been assigned to a group. The other maps have not been assigned to any group.

To Remove a Map

1. In the **Maps** Tab, select the map you wish to remove.
2. Click the **Delete Selected Map** icon.

   An "*Are you sure you want to delete this map*?" dialog box appears.
3. Click **Yes** to remove the map.

The map is removed from the group but it is still available to other groups from within Ocularis Administrator.

To Switch a Map Image

Use this feature when you have a map configured with cameras and views but need to change the background image.

1. In the **Maps** Tab, display the map you wish to be switched.
2. Click the **Switch Map** icon.

   A *Select Map* pop-up appears.
3. Choose the map you want to switch to and click **Select**.
4. Re-select the map group from the Group drop-down menu to see the updated map.

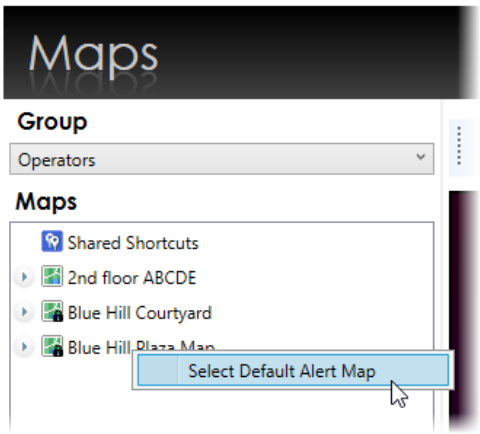
Be aware that if the resolution of the new image is different from the old image, the position of the map elements may change.

TO SET A DEFAULT ALERT MAP

If you use alerts with Ocularis, you can set a map to be the default map displayed when you enter the Alert Manager of Ocularis Client. You can set a unique map for each user group.

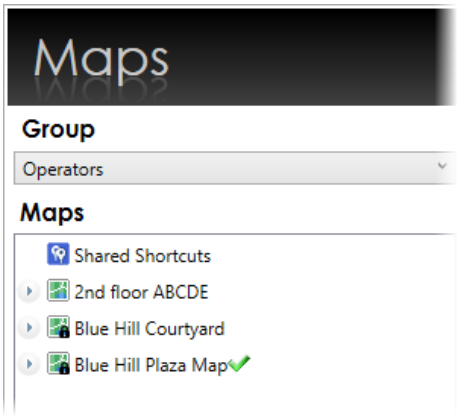
1. Under the desired group, right-click the map name in the Maps list and click 'Select Default Alert Map'. The name becomes editable.

Figure 133 Select Default Alert Map



A green checkmark appears next to the default map.

Figure 134 Default Alert Map



11.1 Working with Maps

Once maps are selected for use in the Maps tab, you can configure it by:

- Add Cameras to A Map
- Add Views to A Map
- Link one map to another Map

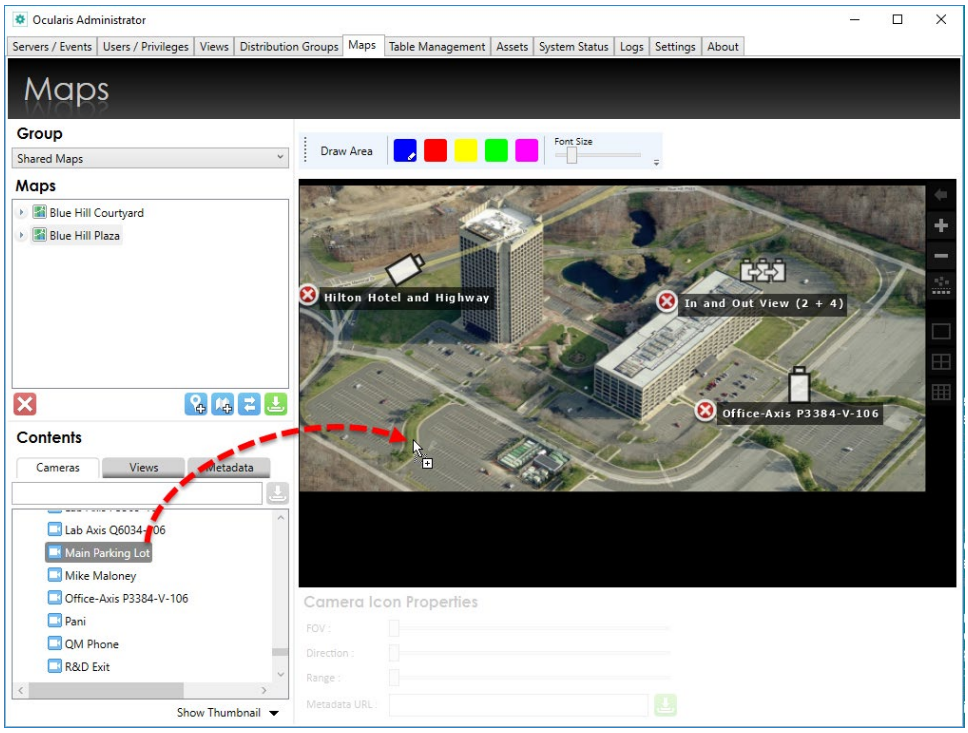
11.1.1 Adding Cameras to Maps

Cameras may be added to a map to visually depict its location and field of view. This aids the operator in being able to better understand where it is that the camera is positioned. The accuracy of the location of the camera on the map is subjected to wherever the administrator/map creator decides to place it. On the map, the camera is represented by an icon (which can be modified) and camera name (which is inherited from the recorder). Operators are able to preview the camera feed when viewing the map with Ocularis Client.

TO ADD A CAMERA TO A MAP

1. In the **Maps** tab, display the map to add a camera(s). (see *To Display a Map* on page 150.)
2. Locate the desired camera in the **Contents** area. Click the *Cameras* tab, expand the cameras folder and take advantage of other methods of locating camera such as *Camera Filter* and *Camera Preview*.

Figure 135 Drag & Drop a camera onto the map



3. Click, drag and drop the camera from the Cameras list to the location on the map.

To Relocate a Camera on a Map

1. Locate the camera on the map and simply drag and drop the camera to the desired location.

To Remove a Camera From a Map

1. Locate the camera on the map.
2. Click the delete icon next to the camera to delete.

Figure 136 Remove a Camera

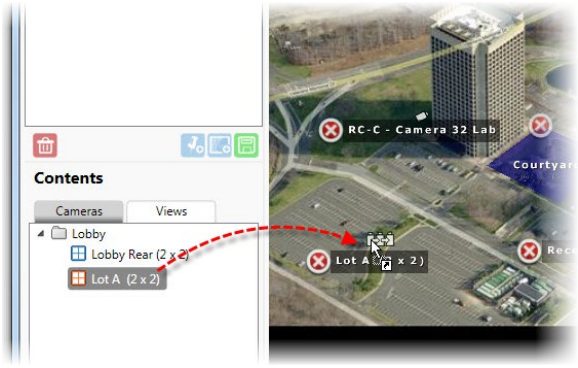
11.1.2 Adding Views to Maps

Similar to cameras, views may be added to a map to visually depict multiple cameras. On the map, the view is represented by an icon (which can be modified) and view name. Operators are able to preview the view when viewing the map with Ocularis Client.

11.1.2.1 To Add a View to a Map

1. In the **Maps** tab, display the map to add the view. (See *To Display a Map* on page 150.)
2. Click the Views tab in the **Contents** list and expand each folder until you locate the desired one.

Figure 137 Expanded Views List



3. Click, drag and drop the view from the Views list to the location on the map.

The view will use Icon 2 located in the Assets Tab. You may want to develop your own icon for use specifically for views.

> ***Note**: Views that contain a Hotspot, Blank Screen, Push Video or Web page may be added to a map but the pane with these content types will not display any preview images and remain blank.*

To Change the Appearance of a Map Icon

The first image shown in the Icons section in the Assets tab is the default icon used when adding cameras to maps. The second icon is the default used for views. You may customize the icons for each camera to signify a camera model or type or any designation you so choose. (See *To Import or Modify* an Icon on page 145).

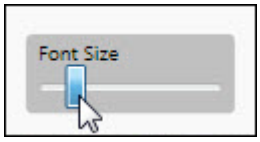
1. Locate the camera icon or view icon on the map you wish to change.
2. Right-click the icon.
3. The icons from the **Assets** tab appear. Click the desired icon.

TO MODIFY THE FONT SIZE OF MAP ICONS

The descriptions associated with icons on a map come from either the camera name on the recorder or the view name in the Views tab. The size of the fonts used may be made larger or smaller.

1. Open the desired map in the **Maps** tab.
2. Drag the Font Size slider button left or right to make the font size smaller or larger.

Figure 138 Change font size with slider



TO RESIZE A MAP ICON

1. Locate the camera or view icon on the map you wish to change.
2. Hold the [**SHIFT**] key and position the mouse over the icon until you see a set of 4 arrows.
3. Click and drag the mouse in a vertical direction up and down to make the icon larger or smaller.
4. Release the mouse when done.

Figure 139 Resize a camera icon

TO ROTATE A MAP ICON

1. Locate the camera or view icon on the map you wish to change.
2. Hold the [**CTRL**] key and position the mouse over the icon until you see a curved arrow.
3. Click and drag the mouse in a vertical direction up and down to rotate the icon.
4. Release the mouse when done.

Figure 140 Rotate a camera icon

TO ZOOM A MAP

1. Display the map in the working area of the **Maps** tab.
2. Zoom in and out using either the:
   - Scroll wheel of the mouse
   - Zoom In or Zoom Out icon

11.1.3 Camera Field of View

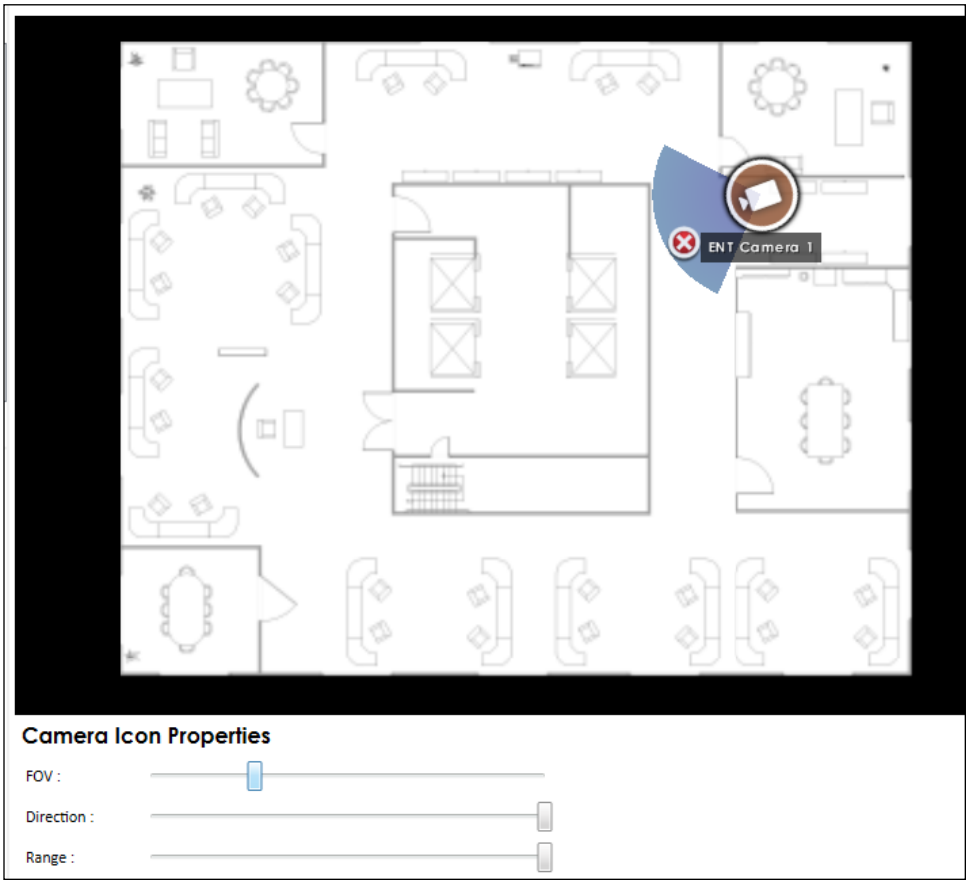
If you want to show a graphical depiction of the camera's range and field of view, you can add this shape adjacent to cameras on a map.

TO ADD FIELD OF VIEW TO A CAMERA ON A MAP

1. Display the map in the working area of the **Maps** tab.
2. If you haven't already done so, add the camera to the map. Position and size it accordingly.
3. There are three settings to maneuver:
   - **FOV**: This changes the angle for the field of view of the camera
   - **Direction**: This changes the direction for which the camera points
   - **Range**: This is the depth for coverage of the camera

   It is easiest to increase the **Range** first and then adjust the **FOV** and **Direction**. Move the sliders left and right to adjust the graphic.

Figure 141 Adjustable sliders



4. Repeat for each camera on the map.

11.1.4 Map Metadata

Map Metadata allows you to place non-camera icons on a map. This is typically used in third party integrations. A Metadata URL may be used to update the metadata shown on the map. Review the document Using Overlays with Ocularis 5 on the documentation page of the website for more information.

11.2 Linking Maps

Linking maps allows you to easily navigate from map to map and back again. Links to maps can be embedded within a map or displayed as floating links within the map display.

- To Embed a Link in a Map
- To Display A Floating Map Link

11.2.1 Shortcuts and Pins

A *Shortcut* is a link that appears on one map that, when clicked, will navigate the screen to another map. The shortcut inherits its name from the *pin* used. A *Pin*, is a shortcut name given to a location on a particular map and is created by the administrator. The pin sets the destination map as well as its horizontal position, vertical position and zoom level.

Prior to creating an embedded or floating link, you must first set the pin(s) on the map(s).

TO SET A MAP PIN

1. In the **Maps** Tab, with the desired group selected, open the *destination* map or the map to which you would like be linked. This is the map that must include the pin(s).
2. Position the map on the screen and zoom in or out so that the map is positioned in the location you wish it to be displayed when it is brought up by the link.
3. Click the **Add New Pin** icon.
4. A pin with the same name as the map is created. Double-click the pin name if you wish to rename it. Additional pins will follow the naming convention of ‘map name (1)’, ‘map name (2)’, etc.

11.2.2 To Embed a Link in a Map

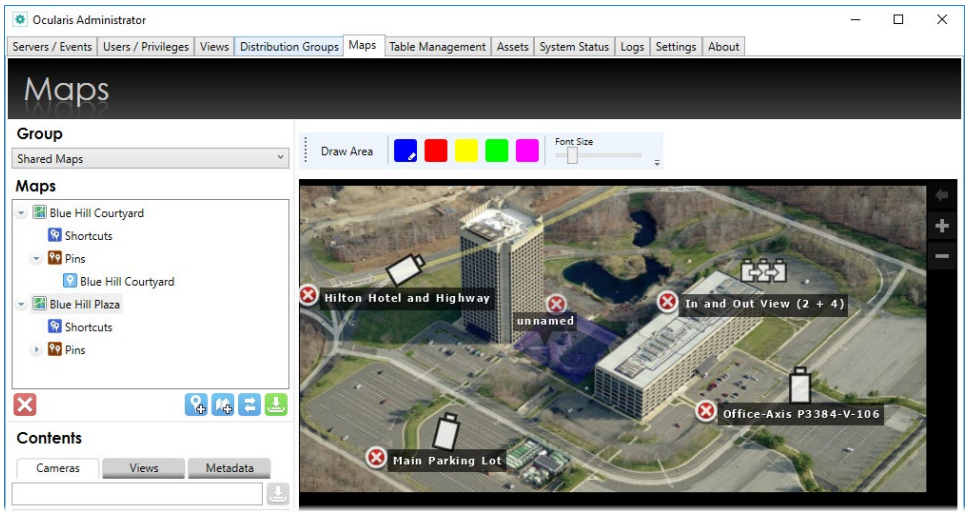
1. In the **Maps** Tab, with the desired group selected, be sure to have already set the pins on the destination map. See *To Set a Map Pin* on page 159.
2. Display the map on which you would like to place the embedded link.
3. You need to draw an area or zone where when clicked, will open up the linked map. Click the **Draw Area** button.

Figure 142 Draw Link Area

4. Use the mouse to draw a polygonal shape on the map which will link to the previous map. Click, release and drag with the right-button and when you get to a corner, click the right-button. Repeat this process for each leg of the shape. When you return to the starting point (“pencil”), the shape outline turns white. Click the right mouse button and releasing the mouse establishes the shape.

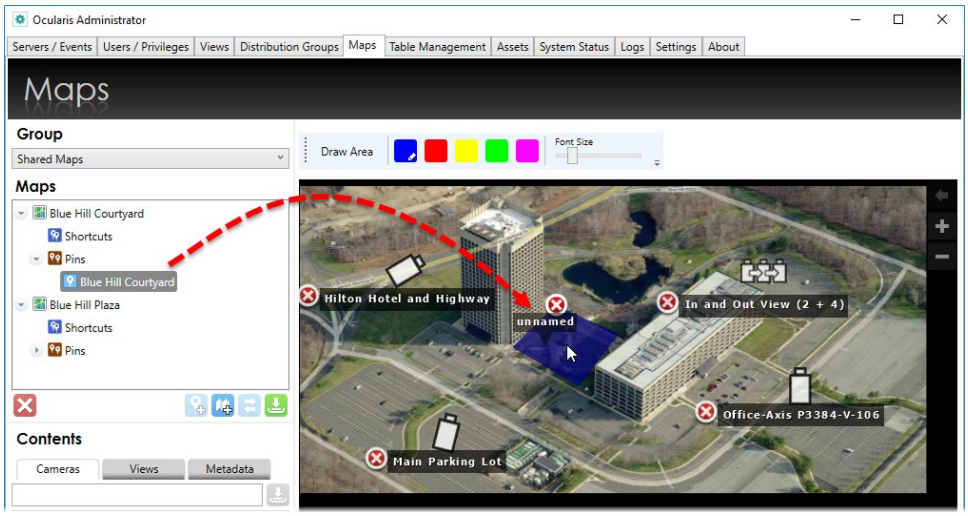
   The shape will appear shaded in color and be labeled “unnamed”.

Figure 143 Link Area unnamed and unassigned



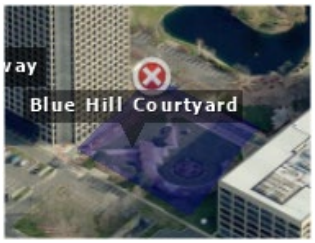
5. Click and drag a pin created earlier onto the unnamed shaded area.

Figure 144 Pin Name Link



The area name will change to display the pin name.

Figure 145 Link area inherits pin name



6. Click the pin area to be brought to the linked map.

TO RETURN TO ORIGINAL MAP FROM A LINKED MAP

Once you have navigated to a map via a link, you may return to the original map by either:

- Creating another pin to the original map using steps 1- 5 in the above section.
- Click the **Go Back** icon.

TO MODIFY THE COLOR OF THE LINK AREA

The default color for a map link is blue. If you want, you may change the color for each area from the available palette of colors.

1. Display the map with the link area.
2. Drag and drop the desired color from the color palette to the link area.

Figure 146 Drag & drop color to modify link area

TO DISPLAY A FLOATING MAP LINK (SHORTCUT)

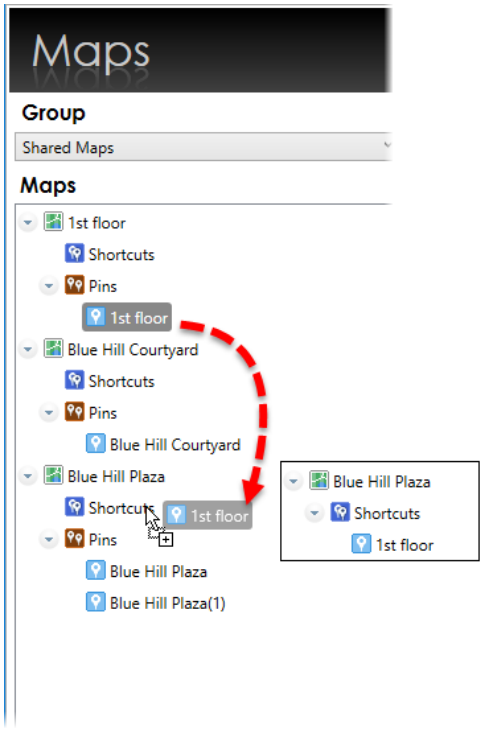
Floating map links or Shortcuts are easy to assign to multiple maps and appear on the Ocularis map when it is displayed in *Ocularis Client*. They are particularly useful in navigating very large maps. These links may appear on a single map or all maps for the selected group.

In the Maps list, beneath each map, is a node for Shortcuts. These shortcuts are similar to link areas in that, when click in *Ocularis Client*, they will navigate the screen to the map with the associated pin.

Floating Map links/shortcuts can be assigned to a map on an individual basis or to all maps of the group. The map on which the floating link appears can be considered the 'source' map and the map which is navigated to when the link is clicked can be considered the 'destination' map.

1. In the **Maps** Tab, with the desired group selected, be sure to have already set the pins on the destination map(s). See *To Set a Map Pin* on page 159. In the Maps list, expand the destination map node displaying the pin name.
2. Determine the source map on which you would like the floating links to appear. Expand the source map node to expose **Shortcuts** and **Pins**.
3. Drag and drop the pin from the destination map to the corresponding pin node of the source map.

Figure 147 Drag and drop Map Pin



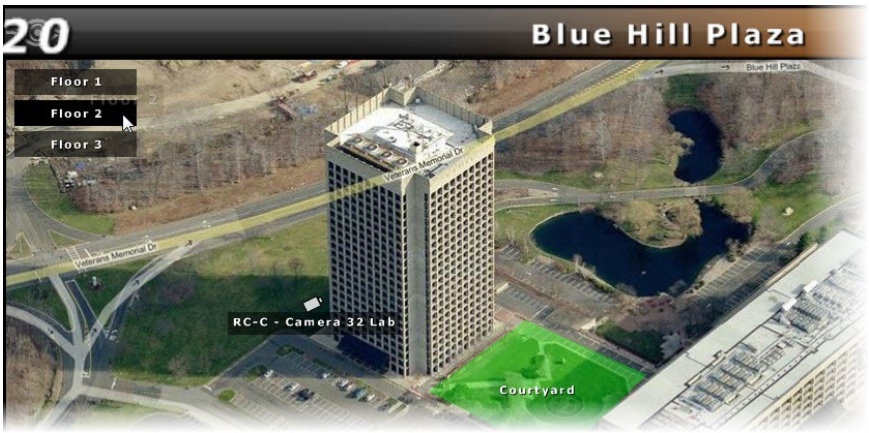
The map appears in the map's **Shortcuts** list.

4. Repeat for each map pin you wish to add.
5. Click the **Save** icon to save the map configuration.

If you wish to assign the pin as a shortcut for all maps of the selected group in one step, drag the pin to the **Shared Shortcuts** node. This shortcut will appear on all of the group's maps.

In *Ocularis Client*, the shortcuts appear as shown in Figure 148.

Figure 148 Map with three floating map shortcuts



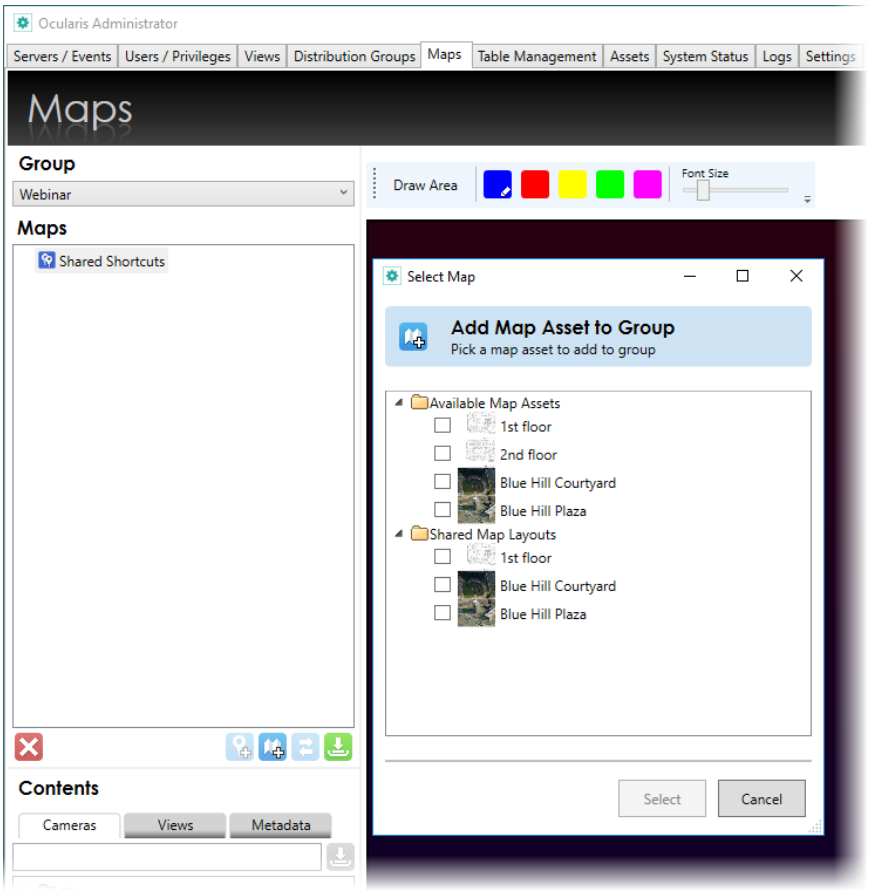
11.2.3 Sharing Maps

Creating a map that is to be shared among multiple user groups is the same process as creating one for a single user group. See *To Add a Map* on page 148 as well as the preceding pages for configuring maps. The difference with shared maps is where the map is created. The **Shared Maps** group is now the default selection when the Maps tab is first accessed.

11.2.3.1 To Share a Map

1. In the **Maps** tab, if not already shown, select *Shared Maps* from the **Groups** drop-down list.
2. Add a map(s) to the Shared Maps group.
3. Add cameras and views to the map as needed.
4. Add navigation links to the maps as needed.
5. Once the shared map is configured as desired, click the **Save Layout** icon.
6. Select the user group from the **Groups** drop-down list that you would like to have access to this map.
7. Click the **Add New Map** icon.
8. Expand the Shared Maps folder from the Select Map pop-up to see the list of available Shared Maps.

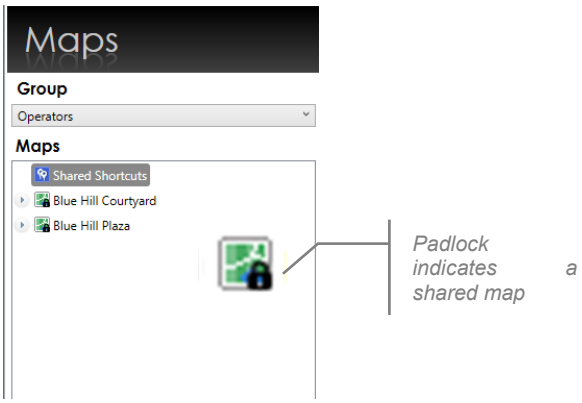
Figure 149 Add from Shared Maps folder to share a map



9. Select the desired map from the list shown and click **Select**.
10. Repeat for each shared map you would like to be assigned to this group.

When you view a shared map from the user group's perspective, a padlock icon appears on the map name in the maps list, indicating that the map is a shared map and may not be edited from the user group location.

Figure 150 Padlock icon indicates a shared map



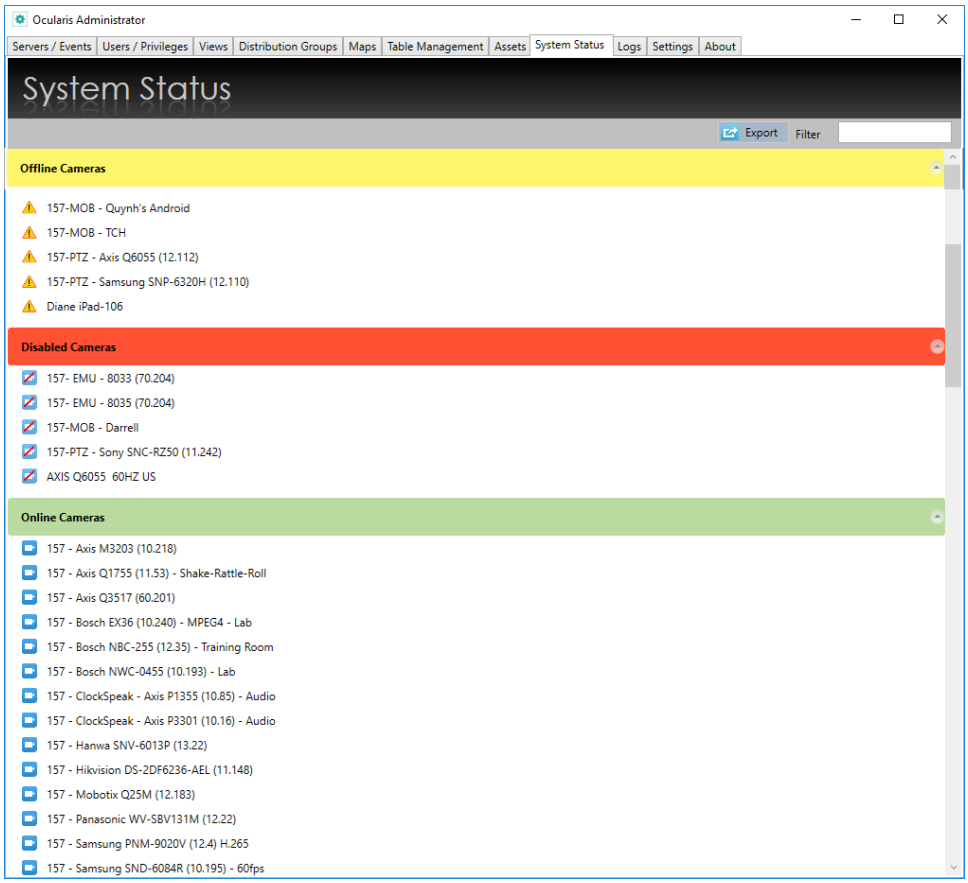
Like shared views, shared maps may only be modified from the Shared Maps group. Likewise, new changes to the shared map will be reflected in each groups' view of the map.

***Note**: Cameras displayed on a shared map are controlled via the user group's privileges to that camera in the Users/Privileges tab. If a user group does not have permission to view a camera or view, it will not appear on their view of the shared map.*

12 System Status Tab

As you know, cameras can sometimes go offline without you realizing it. Administrators now have a way to obtain a real-time update of the health of the cameras on their system via the **System Status** Tab.

Figure 151 System Status Tab



Here, you'll see groupings of three statuses: Offline, Disabled and Online. This screen is updated in real-time. You can expand or collapse a group by clicking the arrow icon on the right of the group name or on the heading itself.

There is a filter field in the upper right that allows you to use a keyword to help you locate a particular camera by its name.

Lastly, you can export the list of cameras and their status by clicking the 'Export' button. A pop-up allows you to select which cameras you'd like included in the report. You can specify a location for the resulting .csv (comma separated values) file and then click **Export**. Open the file with any text editor or Microsoft Excel to view the contents.

This feature is only available to the **admin** user or other users in the 'Administrators' user group. It is not available to Group Administrators.

12.1 Event Management

Ocularis facilitates displaying, investigating and shared handling of events received from:

- A recorder's native video motion detection (VMD) component
- Attached Devices
- Integrated Video Content Analytics
- Third party access control and security systems

Administrators determine which events to which a user should be alerted. Ocularis events maintain the following features:

- ⇨ Incoming events appear in the *Alerts Manager* in the *Ocularis Client*.
- ⇨ Video walls and Views containing a Blank Screen will display video from configured events.
- ⇨ Alert notifications may be designated with low, medium or high priority. Events with high priority will display on an *Ocularis Client* blank screen pane until a user "handles" the event. Medium or low priority alerts display for a designated time period.
- ⇨ Alerts appear in the order of occurrence

Each alert is accompanied by relevant metadata. Typically this includes the camera name that captured the event, time, date and type of event. The type of event is specified in generic terms (e.g. 'VMD Event') or, in the case of video content analytics or access control-generated events, by the analytics rule that triggered the event (e.g. "Stalled Vehicle on Shoulder').

Multiple authorized operators can share the investigation and handling of events through the dynamically-updated *Alerts Manager* in *Ocularis Client*. Once an event is 'handled', it is removed from the *Alerts Manager*. In this case, subsequent investigation is possible only through *Handled Alerts* in the *Ocularis Client*.

***Note**: In order to use camera events with Ocularis Base, the Ocularis Recorder Proxy must first be installed. See the Ocularis Installation & Licensing Guide for instructions on installation and configuration of supported event proxies.*

12.2 Event Management

Ocularis facilitates displaying, investigating and shared handling of events received from:

- A recorder's native video motion detection (VMD) component
- Attached Devices
- Integrated Video Content Analytics
- Third party access control and security systems

Administrators determine which events to which a user should be alerted. Ocularis events maintain the following features:

- ⇨ Incoming events appear in the *Alerts Manager* in the *Ocularis Client*.
- ⇨ Video walls and Views containing a Blank Screen will display video from configured events.
- ⇨ Alert notifications may be designated with low, medium or high priority. Events with high priority will display on an *Ocularis Client* blank screen pane until a user "handles" the event. Medium or low priority alerts display for a designated time period.
- ⇨ Alerts appear in the order of occurrence

Each alert is accompanied by relevant metadata. Typically this includes the camera name that captured the event, time, date and type of event. The type of event is specified in generic terms (e.g. 'VMD Event') or, in the case of video content analytics or access control-generated events, by the analytics rule that triggered the event (e.g. "Stalled Vehicle on Shoulder').

Multiple authorized operators can share the investigation and handling of events through the dynamically-updated *Alerts Manager* in *Ocularis Client*. Once an event is 'handled', it is removed from the *Alerts Manager*. In this case, subsequent investigation is possible only through *Handled Alerts* in the *Ocularis Client*.

***Note**: In order to use camera events with Ocularis Base, the Ocularis Recorder Proxy must first be installed. See the Ocularis Installation & Licensing Guide for instructions on installation and configuration of supported event proxies.*

12.3 Event Configuration

Camera related events which may be monitored include (but are not limited to):

- Motion in the camera field of view
- Camera is enabled
- Camera is disabled
- Camera is not responding
- Video Signal change (rise or fall)

- Audio Signal change (rise or fall)
- Tampering

Software specific events include:

- VMD Event

Third party events include:

- Analytic Event
- Generic Event

To instruct Ocularis which events you wish you monitor and create event associations, see Events Pane on page 43.

12.3.1 Quick Reference – EVENTS

The following steps are necessary in order for events to work properly with Ocularis.

1. In the *Ocularis Administrator* **Server / Events** tab, if applicable, add the recorder which contains the events you wish to monitor.
2. Locate the associated recorder proxy in the *Events* pane.
3. In the *Ocularis Administrator* **Server / Events** tab, drag cameras listed in the *Servers* pane to the events you want to enable in the *Events* pane. (see To Create an Event Rule (To Associate Camera Video with Events) on page 46).
4. If desired, change the priority of the alert by highlighting the event and clicking the **Properties** button. (see To Modify the Priority of an Event on page 49).
5. If desired, modify the sound played when the event occurs. (see To Modify the Audio of an Event on page 51).
6. In the *Ocularis Administrator* **Users / Privileges** tab, make sure the appropriate user has privileges to the device. (see Assign Devices To A User Group on page 88).
7. In the *Ocularis Administrator* **Distribution Groups** tab, be sure that the user is assigned to a distribution group which has corresponding events assigned in the group's events and that the weekly and holiday schedules are set appropriately. (see Distribution Groups on page 177).
8. The Event Coordinator service must be running on the Ocularis Base machine.
9. When a configured event occurs, it will be listed in the *Alert Manager* of the *Ocularis Client* and in a blank screen pane (if one is visible).

12.4 Event Handling

As events are triggered and alerts are displayed in the *Ocularis Client*, the operator has the opportunity to handle or ignore the alert.

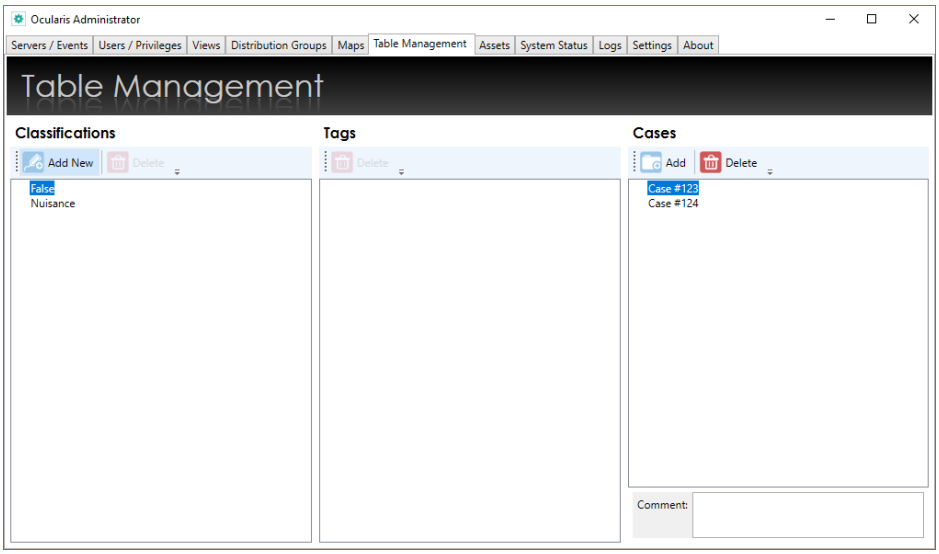
When a user handles an event through the *Ocularis Client*, it can be assigned a *Classification*, a *Tag* or *Case File*. These provide the operator with a means of organizing the alert. These organizational parameters are configured in the **Table Management** tab of the *Ocularis Administrator*. For information on handling events in Ocularis Client, see the *Ocularis Client User Manual*.

13 Table Management Tab

The following tasks are available on the **Table Management** Tab:

- Configure Classifications
- Configure Tags
- Configure Cases

Figure 152 Table Management Tab



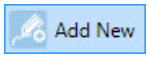
The **Table Management** tab is divided into 3 vertical panes: *Classifications*, *Tags*, and *Cases*.

13.1 Configure Classifications

When operators handle events or create a bookmark in the *Ocularis Client*, the event or bookmark may be categorized into predefined classes as defined by the system administrator. The default classifications are:

- False
- Nuisance

To Create A New Classification

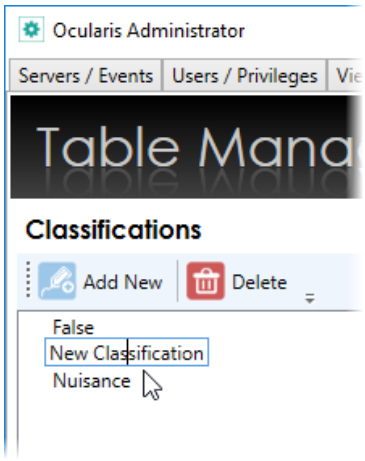
1. In the **Table Management** tab, click the **Add New** button in the **Classifications** 

   A 'New Classification' field is inserted into the Classifications list.

2. Double-click this entry to modify the label.

3. Press **[ENTER]**.

Figure 153 Add a new Classification



TO MODIFY A CLASSIFICATION

1. In the **Table Management** tab, double-click the classification you wish to modify.

   The field should become editable.

2. Type in text changes as desired.

3. Press **[ENTER]**.

***Note**: Modifying the name of a classification is global. Therefore, If you modify the name of a classification that has already been used in a bookmark or handled event, it will also change in that bookmark or handled event.*

TO DELETE A CLASSIFICATION

1. In the **Table Management** tab, select the classification you wish to delete.
2. Click the **Delete** button in the **Classifications** pane.

3. An "*Are you sure that you want to delete this classification…*" pop-up appears. Click **Yes** to delete the classification.

***Note**: Classifications which have been used in a bookmark or handled event may not be deleted.*

***Note**: Classifications may also be created on the fly from the Ocularis Client as an operator is handling the event. Classifications, however, may only be modified or deleted through the Ocularis Administrator.*

13.2 Configure Tags

When operators handle events or create bookmarks in the *Ocularis Client*, he or she may assign a tag or keyword to the event. Administrators may modify or delete tags entered by operators in the *Ocularis Administrator* **Table Management** tab.

13.2.1 To Modify A Tag

1. In the **Table Management** tab, double-click the tag you wish to modify.

   The field should become editable.

2. Type in text changes as desired.

3. Press **[ENTER]**.

***Note**: Modifying the name of a tag is global. Therefore, If you modify the name of a tag that has already been used in a bookmark or handled event, it will also change in that bookmark or handled event.*

13.2.2 To Delete a Tag

1. In the **Table Management** tab, select the tag you wish to delete.
2. Click the **Delete** button in the **Tags** pan

3. An "*Are you sure that you want to delete this tag…*" pop-up appears. Click **Yes** to delete the tag.

***Note**: Tags which have been used in a bookmark or handled event may not be deleted.*

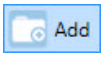
***Note**: Tags are created on the fly from the Ocularis Client, Ocularis Web or Ocularis Mobile as an operator is handling an event or creating a bookmark. Tags, however, may only be modified or deleted through the Ocularis Administrator.*

13.3 Configure Cases

When operators handle events or create bookmarks in the *Ocularis Client*, the event or bookmark may be assigned to an incident case. The use of an incidence case file is optional. Case names

can be created in *Ocularis Administrator* by the system administrator or on the fly as an operator is handling a case.

13.3.1 To Create A New Case

1. In the **Table Management** tab, click the **Add** button in the **Cases** pane. 

   A 'New Case' entry is inserted into the Cases list.

2. Double-click this entry and type in a descriptive name for the Case.
3. Press **[ENTER]**.

13.3.2 To Modify a Case

1. In the **Table Management** tab, double-click the case you wish to modify.

   The field should become editable.

2. Type in text changes as desired.
3. Press **[ENTER]**.

***Note**: Modifying the name of a case is global. Therefore, If you modify the name of a case that has already been used in a bookmark or handled event, it will also change in that bookmark or handled event.*

13.3.3 To Delete a Case

1. In the **Table Management** tab, select the case you wish to delete.
2. Click the **Delete** button in the **Cases** pane.

3. An "*Are you sure that you want to delete this case…*" pop-up appears. Click **Yes** to delete the case.

***Note**: Cases which have been used in a bookmark or handled event may not be deleted.*

***Note**: Cases may also be created on the fly from the Ocularis Client as an operator is handling an event. Cases, however, may only be modified or deleted through the Ocularis Administrator.*

14 Distribution Groups Tab

In the **Servers / Events** Tab, system administrators configure the events which should be monitored on the entire system. The **Distribution Groups** Tab provides system administrators with the ability to configure the distribution of alert notifications for system events. The system administrator determines which alerts to group together, to whom alert notifications should be distributed, if any actions should occur upon event trigger and when alerts should be received. A user must be assigned to a distribution group in order for that user to receive alerts. Additionally, for alerts to be visible on a video wall blank screen s

Distribution Groups are also designed to filter the myriad of alerts and “distribute” them to only those users who really need to see them. As an example, you may want to alert the weekend lobby security guard of only the alerts generated in or near the lobby during weekend hours. There may be many distribution groups configured depending on the number and complexity of events being monitored.

The **Distribution Group** tab is divided into two panes: on the left is the list of existing Distribution Groups and on the right is the detail for a selected group or item. Before a user can view events in the Alerts Manager in *Ocularis Client*, the user must be assigned appropriate permissions in this tab.

14.1 To Create a Distribution Group

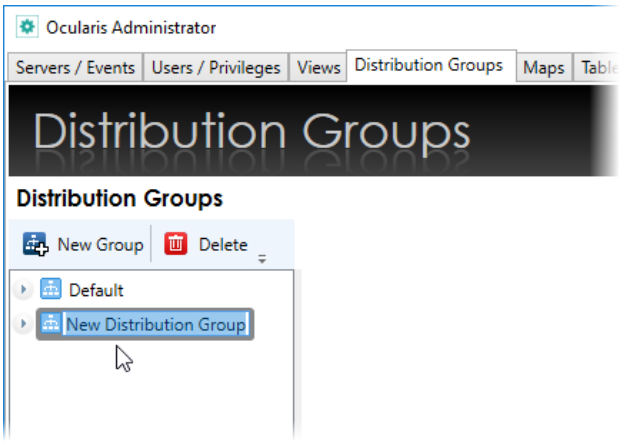
1. In the **Distribution Groups** Tab, click the **New Group** button.

   A ‘New Distribution Group’ entry is inserted into the Distribution Groups list.

2. Double-click the entry and type in a descriptive name for the Distribution Group.
3. Press **[ENTER]**.

The new group appears in the **Distribution Groups** list.

Figure 154 Distribution Group Tab



***Note**: Group Administrators may not create Distribution Groups but can view existing Distribution Groups.*

TO MODIFY A DISTRIBUTION GROUP

1. In the **Distribution Groups** Tab, double-click the Distribution Group you wish to rename.
2. The text becomes highlighted. Make the required change and press **[ENTER]**.

***Note:** Group Administrators may not modify Distribution Groups names.*

TO DELETE A DISTRIBUTION GROUP

1. In the **Distribution Groups** Tab, select the Distribution Group you wish to delete.
2. Click the **Delete** button.
3. In the "*Are you sure you want to delete the distribution group…*" pop-up, click **Yes** to delete the group.

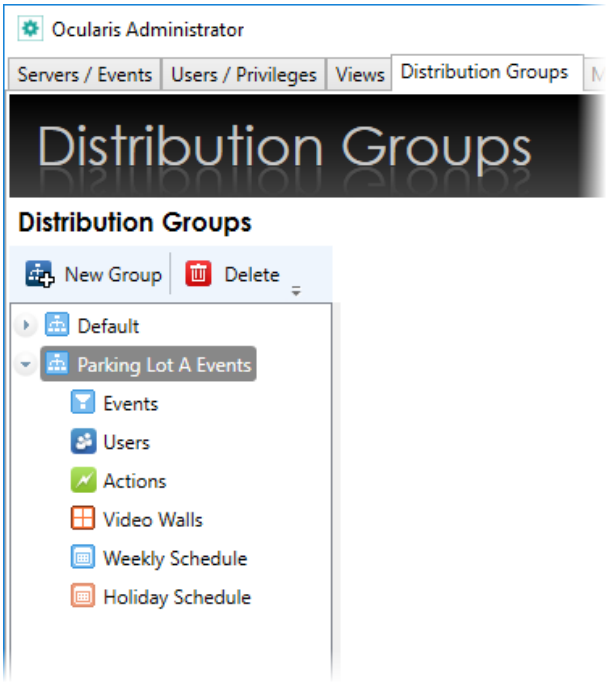
***Note:** Group Administrators may not delete Distribution Groups.*

14.2 Distribution Groups

There are six (6) parameters to configure for each Distribution Group:

- Events
- Users
- Actions
- Video Walls
- Weekly Schedule
- Holiday Schedule

Figure 155 Distribution Group parameters



14.2.1 Events

Formerly labeled 'Filter', the Events item is used to identify the events to be configured in this group.

14.2.1.1 To Assign Events to a Distribution Group

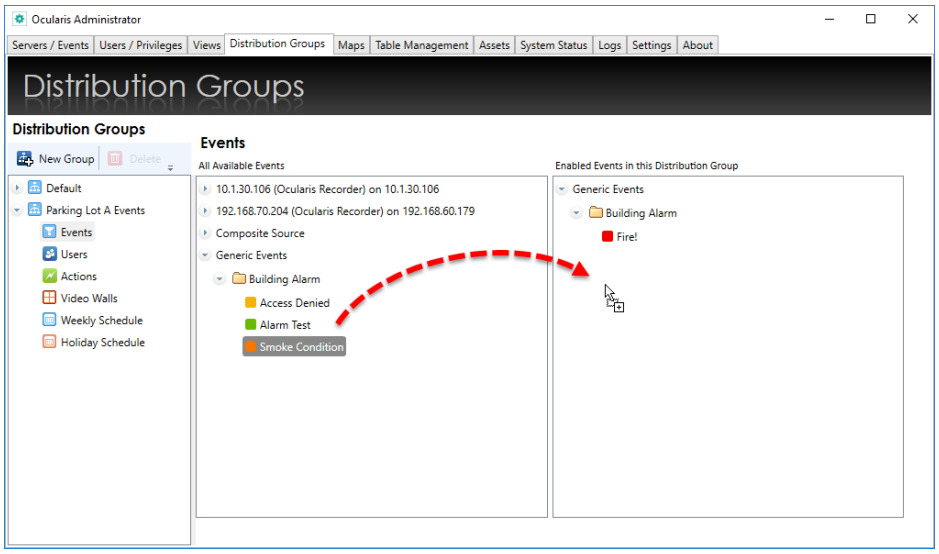
1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Events** item for the group you wish to configure.

   The tab updates and displays two panes: **All Available Events** and **Enabled Events in this Distribution Group**.

2. Drag & drop an event from the **All Events** list on the left to the **Users in Distribution Group** pane on the right.

   - You may move one event at a time or the entire hierarchical group of events.
   - You may move composite events, generic events or any event listed in the All Events pane.

Figure 156 Assigning Events to a Distribution Group



Note: *When new events are added/configured in the Servers / Events tab, you must return to the Distribution Groups tab and assign the events to a group in order for users to be alerted to the event(s).*

14.2.1.2 To Modify Event Assignments within a Distribution Group

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Events** parameter for the group you wish to modify.
2. Modify event assignments by dragging & dropping an event from the **Enabled Events** list on the right to the **All Available Events** pane on the left to remove an event assignment.
3. Drag a new event from the **All Available Events** pane to the **Enabled Events** list.

You may move one event at a time or the entire hierarchical group of events.

14.2.1.3 To Delete Events from a Distribution Group

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Events** item for the group you wish to modify.
2. Remove event assignments by dragging & dropping an event from the **Enabled Events** list to the **All Available Events** pane to remove an event assignment.

Note: *Group Administrators can view but may not modify or delete Events in Distribution Groups.*

14.2.2 Users

Once the events for the group have been determined, the user account for distribution may be assigned next.

14.2.2.1 To Assign a User to a Distribution Group

1. In the **Distribution Groups** Tab, expand a group and highlight the **Users** parameter for the group you wish to configure.

   The tab updates and displays two panes: **All Users** and **Users in Distribution Group**.

2. In the **All Users** pane, expand the user group which contains the user you want to assign.
3. Drag & drop the user name from the **All Users** list on the left to the **Users in Distribution Group** pane on the right.
   - You may only move one user at a time
   - Users from different user groups may be assigned to the same distribution group
   - The same user may be assigned to multiple distribution groups

14.2.2.2 To UnAssign a User From a Distribution Group

1. In the **Distribution Groups** Tab, expand the group and highlight the **Users** parameter for the user you wish to remove.
2. Drag & drop the user name from the **Users in Distribution Group** list on the right to the **All Users** pane on the left.

***Note**: Group Administrators can view Users in Distribution Groups. They can remove members of their own group only.*

14.2.3 Actions

A resulting action may be assigned to take place should an event occur. These actions, (Move to Preset, Send Email, Send HTTP Request, and Send TCP/UDP Data Packet) are configured in the **Servers / Event**s tab but assigned to events in the **Distribution Groups** tab.

14.2.3.1 To Assign an Action to a Distribution Group

1. In the **Distribution Groups** Tab, expand a group and highlight the **Actions** item for the group you wish to configure.
2. In the **All Actions** pane, expand the Action which contains the item you want to assign.

3. Drag & drop the Action item from the **All Actions** list on the left to the **Actions in Distribution Group** pane on the right. You can drag & drop all action items by dragging the Action top level item. ***In most cases, you probably do not want to do this!***

14.2.3.2 To UnAssign an Action From a Distribution Group

1. In the **Distribution Groups** Tab, expand the group and highlight the **Actions** parameter.
2. Drag & drop the Action item from the **Actions in Distribution Group** list on the right to the **All Actions** pane on the left.

14.2.4 Video Walls

For events to be posted to a video wall in a blank screen and in sequence, the video wall must be included in the alert distribution group. Remote video walls are supported with Ocularis ES, Ocularis LS, Ocularis CS and Ocularis IS.

14.2.4.1 To Assign a Video Wall to a Distribution Group

1. In the **Distribution Groups** Tab, expand a group and highlight the **Video Walls** parameter for the group you wish to configure.

   The tab updates and displays two panes: **All Video Walls** and **Video Walls in Distribution Group**.

2. In the **All Video Walls** pane, drag & drop the video wall from the **All Video Walls** list on the left to the **Video Walls in Distribution Group** pane on the right. Video walls are created in the **Users / Privileges** tab so if you need to create a new one, do so in that tab.

You may assign multiple video walls to a distribution group.

14.2.5 Weekly Schedule

Schedules for Distributions Groups can be set up to allow alert notification only during specific dates and times. This decreases the amount of alerts shown to a given user, making managing alerts an easier task.

By default, the Weekly Schedule is set to be on 24/7, seven days a week.

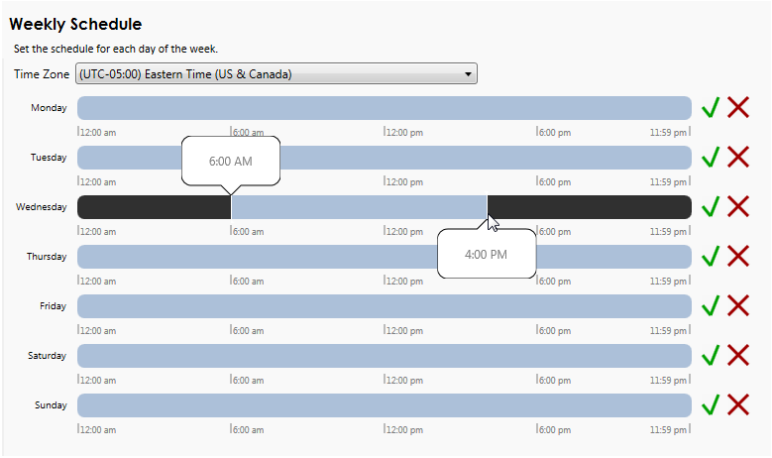
Note: *These schedules can be overridden in the Ocularis Client if the user account has been given the Event Filtering privilege in the Users/Privileges tab.*

14.2.5.1 To Set A Weekly Schedule

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Weekly Schedule** parameter for the group whose weekly schedule you wish to set.

   A **Weekly Schedule** appears in the details pane.

Figure 157 Setting a Weekly Schedule



Tip*: If you position the mouse over the timescale, a balloon appears displaying the Start and End time on the timescale.*

2. At the top of the calendar, a time zone drop-down list is available. Select the time zone for the Distribution Group. Alerts will be active for the members of this group during the time period of the time zone selected.

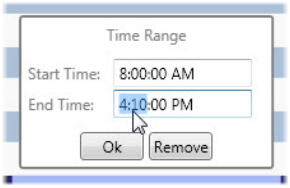
   Note: *Time zones selected here apply to the distribution group, regardless of the users in it. For instance: if the Distribution Group has a time zone assignment for Pacific Time and an alert window is set for 9:00 a.m. to 5:00 p.m., the alert would be distributed to the designated members of the group during this time. A member of this group who happens to be located in the Eastern Time zone, would therefore, receive alerts locally between 12:00 p.m. – 8:00 p.m.*

   The time zone set for the group's Weekly Schedule is shared with the time zone for its Holiday Schedule.

3. For each day of the week, click and drag to set the time schedule. Click the icon to clear the daily schedule.

4. When you release the mouse, after clicking and dragging to designate a time period, the *Time Range* pop-up appears with the **Start Time** and **End Time** displayed.

Figure 158 Time Range Pop-Up



5. Make changes manually as necessary. Click **Ok** to save the *Time Range* settings.
6. Repeat for each day of the week.

You may set multiple time ranges within a given day.

TO MODIFY A WEEKLY SCHEDULE

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Weekly Schedule** parameter for the group whose weekly schedule you wish to modify.

   The **Weekly Schedule** appears in the details pane.

2. Click on a Time Range you wish to modify.

   The **Time Range** pop-up appears as shown in Figure 158.

3. Modify the **Start Time** and / or **End Time** as needed.
4. Click **Ok** to save the *Time Range* settings.
5. Repeat steps 1-4 for each day of the week you wish to modify.

TO CLEAR A WEEKLY SCHEDULE

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Weekly Schedule** parameter for the group whose weekly schedule you wish to delete.

   The **Weekly Schedule** appears in the details pane.

2. Click on the **Clear Schedule** icon next to the day of the week you wish to clear.

Figure 159 Clear a Weekly Schedule

The schedule for that day has been removed.

Figure 160 Cleared Schedule for Monday

3. Repeat for each day of the week whose schedule you wish to clear.

TO RESET A WEEKLY SCHEDULE

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Weekly Schedule** parameter for the group whose weekly schedule you wish to reset.

   The **Weekly Schedule** appears in the details pane.

2. Click on the **Reset Schedule** icon next to the day of the week you wish to reset.

Figure 161 Reset a Weekly Schedule

The schedule for that day has been reset to the default of 24 hours.

3. Repeat for each day of the week whose schedule you wish to reset.

Figure 162 Reset Schedule

14.2.6 Holiday Schedule

Weekly schedules are for general use throughout the year. However, during days when an organization works a limited number of hours or with a limited number of employees, a Holiday Schedule can be followed.

Holiday Schedules are set on a distribution group basis and override any time range set in a Weekly Schedule.

By default, no Holiday Schedule is set and therefore, this task must be done for each Distribution Group. The time zone selected for the Holiday Schedule applies to the Distribution

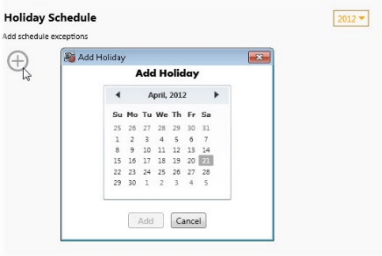
Group as a whole and must be the same time zone used as the Distribution Group's Weekly Schedule.

TO SET A HOLIDAY SCHEDULE

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Holiday Schedule** parameter for the group whose Holiday Schedule you wish to set.

   The details pane displays a Holiday Schedule with a pull-down menu for the year and an **Add New Holiday** icon.

Figure 163 Holiday Schedules



2. Select the year for the holiday from the year drop-down menu.
3. Click the **Add New Holiday** icon.

   An **Add Holiday** pop-up appears displaying a calendar.

4. Navigate to the month and day for the holiday and click the date to select it.
5. Click the **Add** button to add the date to the Holiday Schedule.
6. Once the date is added, the Time Range for the Holiday should be specified. Click and drag along the timescale to select the Start and End times.
7. Repeat steps 1-6 for each Holiday for this Distribution Group.

14.2.6.1 To Modify A Holiday Schedule

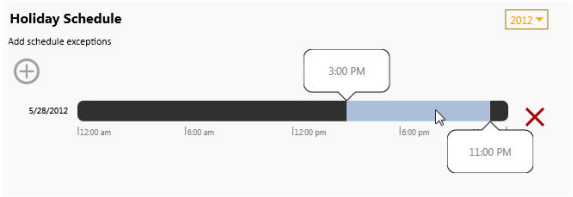
1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Holiday Schedule** parameter for the group whose Holiday Schedule you wish to modify.

   The details pane displays the group's Holiday Schedule.

2. To modify a Time Range, click on the range and change the Start Time and / or End Time directly and then click Ok.
3. To Add an additional holiday, click the **Add New Holiday** icon.

4. Navigate to the month and day for the holiday and click the date to select it.
5. Click the **Add** button to add the date to the Holiday Schedule.
6. Once the date is added, the Time Range for the Holiday should be specified. Click and drag along the timescale to select the Start and End times.

Figure 164 Setting a Time Range during a Holiday

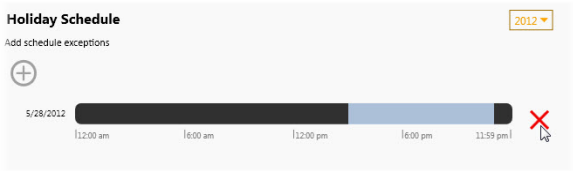


7. Repeat steps 1-6 for each Holiday for this Distribution Group.

14.2.6.2 To Delete A Holiday Schedule

1. In the **Distribution Groups** Tab, expand the Distribution Group and highlight the **Holiday Schedule** parameter for the group whose Holiday Schedule you wish to remove.
2. To delete a Time Range for a particular holiday, click on the range itself and click the **Remove** button in the resulting Time Range pop-up.
3. To delete an entire holiday day, click the Delete Holiday icon.

Figure 165 Delete a Holiday icon



The Holiday is removed from the schedule.

15 Logs Tab

The Logs Tab provides visibility into the activity Operators perform with Ocularis. Manual actions that someone performs are logged in a separate database ('VSAudits'). Currently, the log tracks Ocularis Client usage and many of the activities performed by a user in Ocularis Administrator. The 'admin' (super) user, Standard Administrators as well as Group Administrators have visibility into this data. (Group Administrators may only view data related to their own group). By default, the audit log is disabled and administrators must enable it for activity to be logged. Configuring the audit log has been moved to the Settings Tab which is documented on page 196.

15.1 What Data is Audited?

The data that is captured in the audit log is any action that a user performs manually in Ocularis Client. Automated actions, such as blank screen alerting, critical camera failover, etc. are not tracked in the audit log at this time. Anything that a user can 'click' is typically tracked. (See **Note*** below). Additionally, many of the actions Ocularis Administrator are also tracked.

***Note**:* *The following user actions are NOT captured in the audit log for Ocularis Client activities:*

Maximizing a View Pane

Using controls on a video wall

Using controls on a map

Tools and functions within the Alert Manager

15.2 Viewing the Audit Log

Administrators can view entries of the audit log via the **Logs** tab in Ocularis Administrator. Group Administrators can view data from users within their own group and the user 'admin' or any user in the 'Administrator' group can view all entries in the log. Search criteria are available to filter the log and an export function allows for the data to be exported and saved.

15.2.1 To Query the Audit Log

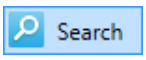
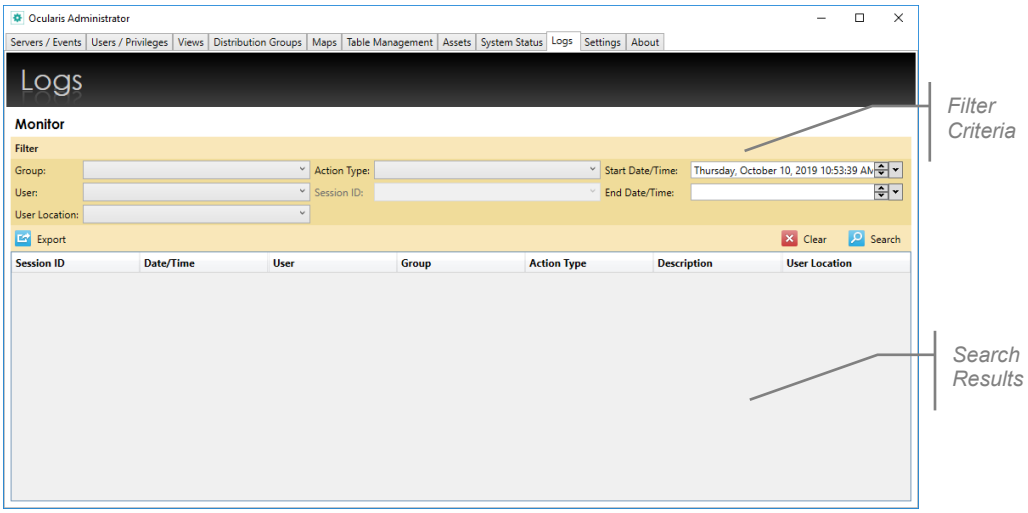
1. Select any desired **Filter** criteria.
2. Click the **Search** button. 

Figure 166 Logs Tab

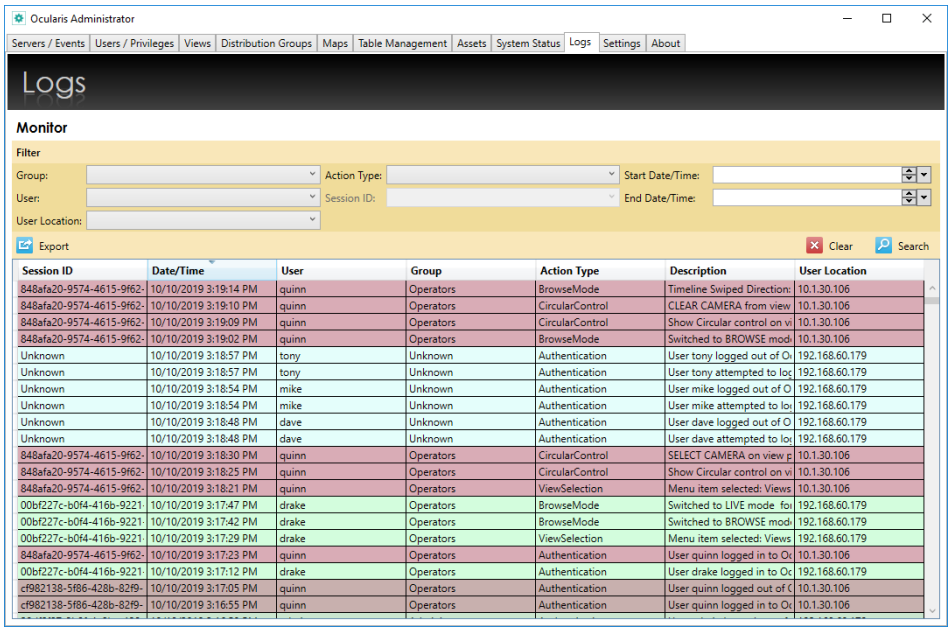


The following fields are available for filtering the search results:

Group	This is the Ocularis user group.
User	This is the Ocularis User account.
User Location	This is the IP address of the Ocularis Client computer.
Action Type	This is the category related to the audited item. E.g. Authentication For more information, see Action Types below.
Session ID	Each time a user logs in to Ocularis Client, they are assigned a unique Session ID. This field can be used as filter criteria.
Start Date/Time	You can filter by the start date or start time of the records. The default value when you first enter the Logs tab is one hour prior to the current time.
End Date/Time	The end time by which you want to filter log data.

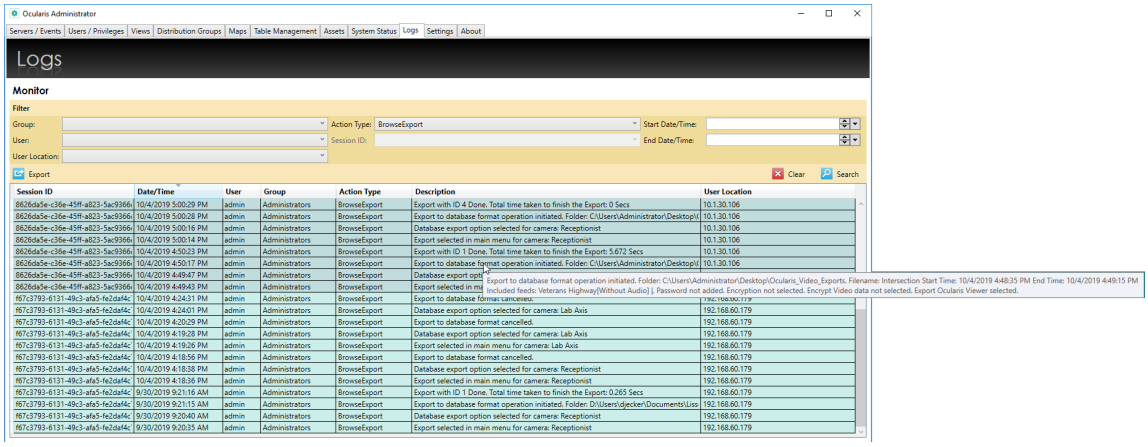
The drop-down lists for the above fields are dynamic based on the displayed results. For instance, if there are 5 users logged into the system but only 3 users have records for performing a Digital PTZ action, only those 3 user accounts will appear in the drop-down list as a filter option.

Figure 167 Sample Results (unfiltered)



Notice in the example below, the results are filtered by Action Type. If you position the mouse over a field with more data in it than is displayed, a tool tip appears with full details.

Figure 168 Sample Results Filtered by Action Type



15.2.1.1 Action Types

Entries into the audit log are categorized into the following Action Types:

```
AuxButton
Authentication
BackwardButton
BrowseExport
BrowseMode
BrowseMotionDetection
BrowseTimeSlice
CameraSelection
CarouselNavigation
CircularControl
ClientSetup
DigitalPTZ
ForwardButton
Hotspot
MicrophoneButton
OC Administrator
OpticalPTZ
PanamorphMode
PauseLiveVideo
PTZButton
SnapshotButton
SpeakerButton
StreamingInfo
ViewSelection
```

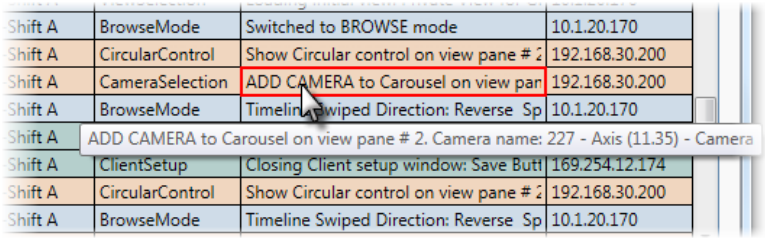
15.2.1.2 Search Results

Audit records are displayed in tabular format as shown in Figure 167. Results are displayed by default in order of *Date/Time*, most recent to oldest. Each Session ID has its own unique color to aid in reading the log.

15.2.1.3 Tool tip

If the column is not wide enough to display the associated data within the cell, position the mouse over the item to see an expanded tool tip of the cell contents.

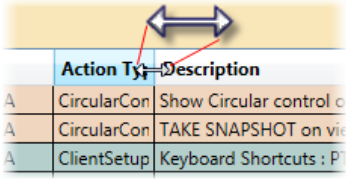
Figure 169 Tool tip



15.2.1.4 Resize a Column

If you want to change the size of a column in order to better organize its contents, click and drag the column heading divider to resize that column.

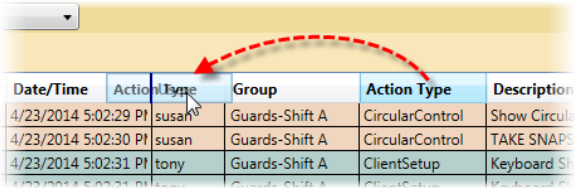
Figure 170 Resize a column



15.2.1.5 Reorder a Column

Click and drag a column heading along the row to reorder the table.

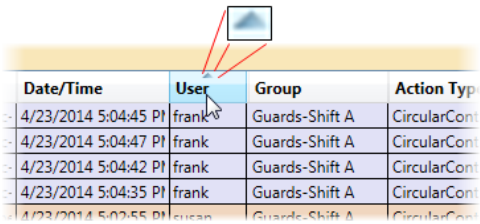
Figure 171 Reorder Columns



15.2.1.6 Re-sort a Column

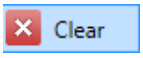
By default, the records are listed in order of date/time where the oldest date/time record is at the top of the list. To sort the search results by any column, click on the column heading.

Figure 172 Sort any column



Click the same column again to reverse the sort order. The triangular sort icon will appear and indicate whether the sort is ascending or descending.

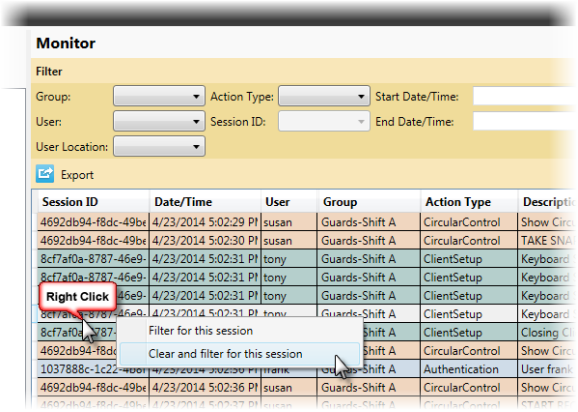
15.2.1.7 Clear Results

At any time, if you want to start over or simply clear the screen, click **Clear**. 

15.2.1.8 Session ID Search

Since Session ID is a large, complex identifier for each unique login session, a right-click option has been added. Right-click a Session ID on the results to see the following menu:

Figure 173 Right-click Session ID



- **Filter for this session** – this option will retain any filter criteria and add the selected Session ID as an additional filter. The new filters are immediately applied to the data.
- **Clear and filter for this session** – this option clears any filters already selected and queries the log with just the selected Session ID. The new filter is immediately applied to the data. This is equivalent to selecting the Session ID from the drop-down list.

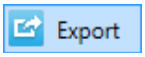
15.2.1.9 About Displayed Search Results

- Search results on the screen are by default sorted in descending order by *Date/Time* and limited to the newest (most recent) 5,000 records. If you want to access all records from the results of a search, you should **Export** the search results. (see *Exporting the Audit Log* on page 192)
- Changes made to the screen interface (resizing, re-sorting or reordering a column) are only temporary. The screen will revert back to default settings the next time the administrator logs in to Ocularis Administrator. These formatting changes will not be reflected in an exported .csv file.

15.3 Exporting the Audit Log

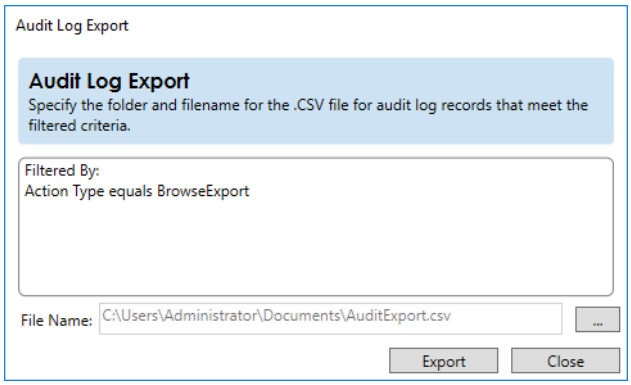
Audit Log search results may be exported to a .csv (comma separate value) file. This provides the administrator with the ability to use external tools (such as Microsoft Excel) to work with the log data. When search results are exported, all records of the query, regardless of size, are included.

15.3.1 To Export Audit Log Results

1. Query the log with the desired filters.
2. Click the **Export** button. 

The *Audit Log Export* screen appears.

Figure 174 Audit Log Export pop-up



The pop-up identifies any criteria used as a filter. The default path and filename is presented: `c:\Users\<PC Name>\Documents\AuditExport.csv`

3. To change the name or location of the exported file, click the ellipsis button.
4. Use standard Windows methods for choosing an alternate path and file name.
5. Click the **Save** button.
6. When the export is complete, a message '**Export Successful**' appears at the bottom of the pop-up.
7. Click **Close**.

Note: *The data exported is based on the filter criteria and will be inclusive of all records that meet the criteria.*

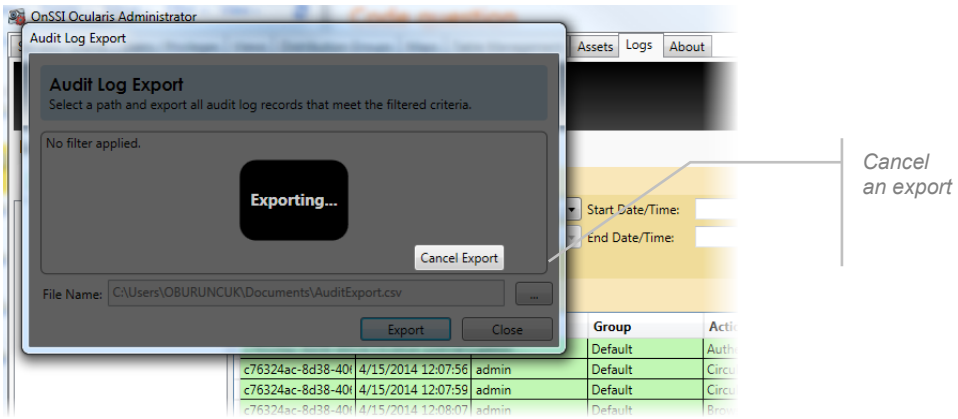
15.3.2 About Exported Search Results

- Search results on the screen are limited to the newest 5,000 records but if there are more records, these will all be included in an exported search.
- The order of the data in the .csv export is static. If you changed the order of columns in your audit log display, this order will not be reflected in the exported file. Use a third party application that supports .csv files to modify the column order.
- When you click the **Export** button, the query to the database is made again based on the criteria listed under 'Filtered By'. It does not simply export results you might have on the screen. The search results in an export include the most up-to-date results from the database at the time the user clicks the **Export** button. Therefore, these results may differ from those which may have been displayed on the screen due to the fact that the **Export** query was made after the initial **Search** query.

15.3.3 To Cancel an Export

Most exports occur within seconds. However, when you export data of a significant size it may take some time to complete the export. You are able to cancel an export while it is still in progress if necessary.

Figure 175 Cancel an Export

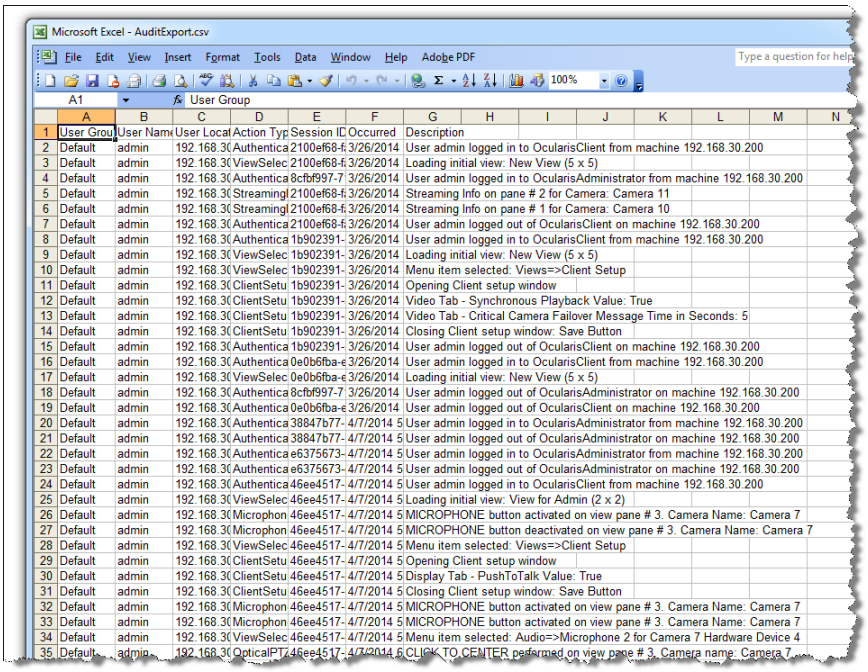


Click the **Cancel Export** button during the export process to cancel.

15.3.4 To View Exported Audit Log Results

1. Use any third party application that supports .csv files to open the exported file that was created in step 5 above. The most common application to use is a spreadsheet application.

Figure 176Sample Exported Log as viewed in Excel



	A	B	C	D	E	F	G
1	User Grou	User Nam	User Locat	Action Typ	Session ID	Occurred	Description
2	Default	admin	192.168.30	Authentica	2100ef68-f	3/26/2014	User admin logged in to OcularisClient from machine 192.168.30.200
3	Default	admin	192.168.30	ViewSelec	2100ef68-f	3/26/2014	Loading initial view: New View (5 x 5)
4	Default	admin	192.168.30	Authentica	8cfbf997-7	3/26/2014	User admin logged in to OcularisAdministrator from machine 192.168.30.200
5	Default	admin	192.168.30	Streaming	2100ef68-f	3/26/2014	Streaming Info on pane # 2 for Camera: Camera 11
6	Default	admin	192.168.30	Streaming	2100ef68-f	3/26/2014	Streaming Info on pane # 1 for Camera: Camera 10
7	Default	admin	192.168.30	Authentica	2100ef68-f	3/26/2014	User admin logged out of OcularisClient on machine 192.168.30.200
8	Default	admin	192.168.30	Authentica	1b902391-	3/26/2014	User admin logged in to OcularisClient from machine 192.168.30.200
9	Default	admin	192.168.30	ViewSelec	1b902391-	3/26/2014	Loading initial view: New View (5 x 5)
10	Default	admin	192.168.30	ViewSelec	1b902391-	3/26/2014	Menu item selected: Views=>Client Setup
11	Default	admin	192.168.30	ClientSetu	1b902391-	3/26/2014	Opening Client setup window
12	Default	admin	192.168.30	ClientSetu	1b902391-	3/26/2014	Video Tab - Synchronous Playback Value: True
13	Default	admin	192.168.30	ClientSetu	1b902391-	3/26/2014	Video Tab - Critical Camera Failover Message Time in Seconds: 5
14	Default	admin	192.168.30	ClientSetu	1b902391-	3/26/2014	Closing Client setup window: Save Button
15	Default	admin	192.168.30	Authentica	1b902391-	3/26/2014	User admin logged out of OcularisClient on machine 192.168.30.200
16	Default	admin	192.168.30	Authentica	0e0b6fba-e	3/26/2014	User admin logged in to OcularisClient from machine 192.168.30.200
17	Default	admin	192.168.30	ViewSelec	0e0b6fba-e	3/26/2014	Loading initial view: New View (5 x 5)
18	Default	admin	192.168.30	Authentica	8cfbf997-7	3/26/2014	User admin logged out of OcularisAdministrator on machine 192.168.30.200
19	Default	admin	192.168.30	Authentica	0e0b6fba-e	3/26/2014	User admin logged out of OcularisClient on machine 192.168.30.200
20	Default	admin	192.168.30	Authentica	38847b77-	4/7/2014 5	User admin logged in to OcularisAdministrator from machine 192.168.30.200
21	Default	admin	192.168.30	Authentica	38847b77-	4/7/2014 5	User admin logged out of OcularisAdministrator on machine 192.168.30.200
22	Default	admin	192.168.30	Authentica	e6375673-	4/7/2014 5	User admin logged in to OcularisAdministrator from machine 192.168.30.200
23	Default	admin	192.168.30	Authentica	e6375673-	4/7/2014 5	User admin logged out of OcularisAdministrator on machine 192.168.30.200
24	Default	admin	192.168.30	Authentica	46ee4517-	4/7/2014 5	User admin logged in to OcularisClient from machine 192.168.30.200
25	Default	admin	192.168.30	ViewSelec	46ee4517-	4/7/2014 5	Loading initial view: View for Admin (2 x 2)
26	Default	admin	192.168.30	Microphon	46ee4517-	4/7/2014 5	MICROPHONE button activated on view pane # 3. Camera Name: Camera 7
27	Default	admin	192.168.30	Microphon	46ee4517-	4/7/2014 5	MICROPHONE button deactivated on view pane # 3. Camera Name: Camera 7
28	Default	admin	192.168.30	ViewSelec	46ee4517-	4/7/2014 5	Menu item selected: Views=>Client Setup
29	Default	admin	192.168.30	ClientSetu	46ee4517-	4/7/2014 5	Opening Client setup window
30	Default	admin	192.168.30	ClientSetu	46ee4517-	4/7/2014 5	Display Tab - PushToTalk Value: True
31	Default	admin	192.168.30	ClientSetu	46ee4517-	4/7/2014 5	Closing Client setup window: Save Button
32	Default	admin	192.168.30	Microphon	46ee4517-	4/7/2014 5	MICROPHONE button activated on view pane # 3. Camera Name: Camera 7
33	Default	admin	192.168.30	Microphon	46ee4517-	4/7/2014 5	MICROPHONE button activated on view pane # 3. Camera Name: Camera 7
34	Default	admin	192.168.30	ViewSelec	46ee4517-	4/7/2014 5	Menu item selected: Audio=>Microphone 2 for Camera 7 Hardware Device 4
35	Default	admin	192.168.30	OpticalPT	46ee4517-	4/7/2014 5	CLICK TO CENTER performed on view pane # 3. Camera name: Camera 7

2. Use the third party application's tools to view, sort and print the data.

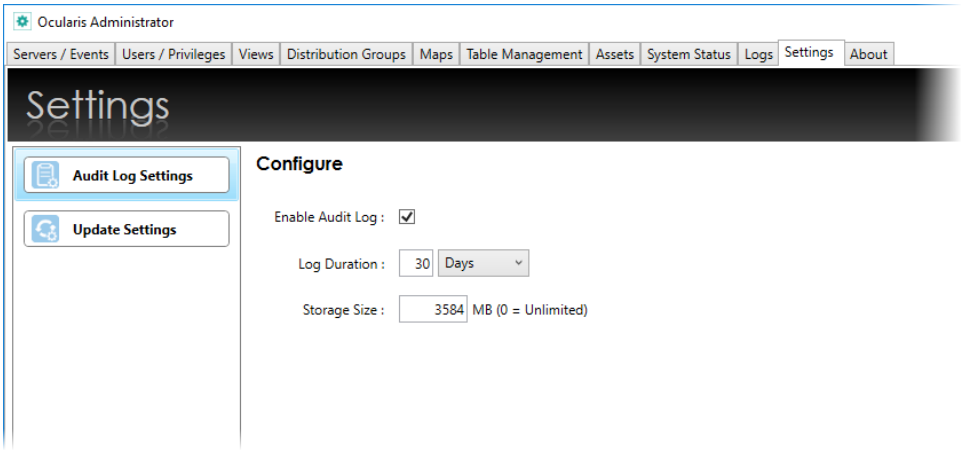
16 Settings Tab

The Settings Tab has been added to Ocularis Administrator to provide a central location for Ocularis Administrator settings. Here you can configure the Audit Log and the Client Update Settings

16.1 Audit Log Settings

Auditing is done system-wide and includes all users of Ocularis. Only the user 'admin' (super user) or a Standard Administrator can configure the settings for the audit log. By default, the audit log is not enabled and only the user 'admin' or any Standard Administrator can enable it.

Figure 177 Configure the Audit Log



TO CONFIGURE AUDIT LOG SETTINGS

1. In the **Settings** Tab, select the **Audit Log Settings** node.
2. Make changes to the **Configure** settings shown.

Field in the **Configure** pane include:

Enable Audit Log	This checkbox enables or disables system auditing. If the box is checked while Ocularis Client users are currently logged into Ocularis Base, actions performed by those logged in users will NOT be logged until their next session (the next time they log in to Ocularis). The default value is off/disabled.
Log Duration	Available units are: Hours, Days and Months. Log data will be retained for this period and purged once the duration has been reached.

Storage Size	This is the maximum size of the log database you want to dedicate for audit logging. The default value 3584 MB (or 3.5 GB) is well within the 4GB max limit for SQL Express. However, you can make the maximum database size any value you want, including 0 for unlimited size.

16.1.1 Storage of Log Data

As the system is used, each action is entered as one record into the log database, a separate SQL database within Ocularis. As you can imagine, this database can rapidly grow in size and fill up quickly. Data is written to the database in FIFO format ('first in, first out') so if the database is full, the oldest data is purged. Administrators have an option to control the size and/or the duration of maintaining data using the **Storage Size** and **Log Duration** settings respectively.

The log database is examined every hour. The **Storage Size** is checked first and the oldest data over the limit will be purged. Additionally, data that is older than the **Log Duration** setting will automatically be purged

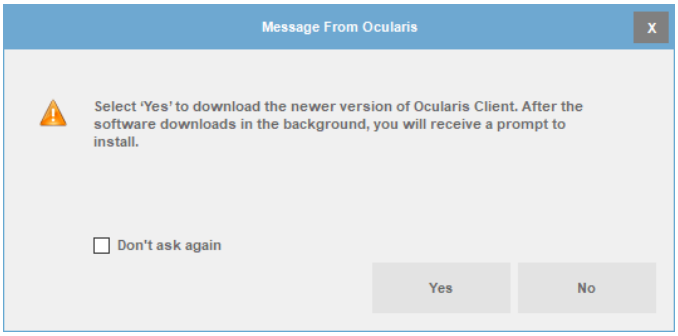
16.2 Update Settings

Introduced in Ocularis v5.4, we have provided a way for adminstrators to allow Ocularis Client users to update their own systems via an Auto Update option. This applies to upgrades from 5.3 SP1 or later. Whenever Ocularis Client's login process is performed, the software can check Ocularis Base for the most current version. If the version of Ocularis Client on the Base is newer than the one being used by the Operator, a prompt appears asking if the operator would like to download and install the new version.

Note: *The logged in Windows user must have administrator rights to the PC in order for this method to work. If the Operator does not have administrator rights, the prompt will not appear. Try right-clicking the Ocularis Client icon and select 'Run as administrator'.*

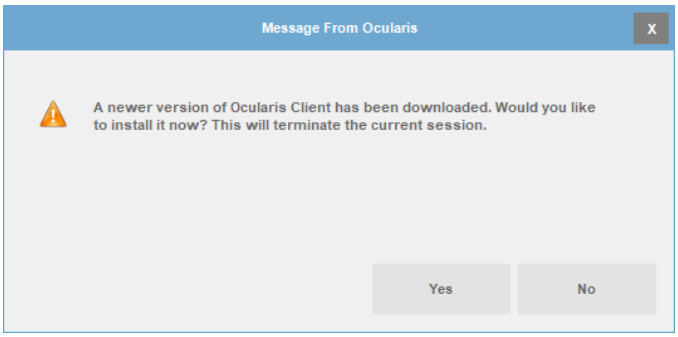
When an Ocularis Client login attempt is made after upgrading Ocularis Base, the following message appears:

Figure 178 Version Check for Ocularis Client



- Click **No** will delay the upgrade at the present time. The next time the user logs in to Ocularis Client, they will receive this message again. It will keep appearing until the software is upgraded or the 'Don't ask again' checkbox is clicked.
- Click **Yes** will download the installation files from Ocularis Base. Ocularis Client will launch and the files are downloaded in the background. This may take several minutes based on the network bandwidth. When the download is complete, the following message appears:

Figure 179 Upgrade Downloaded Message

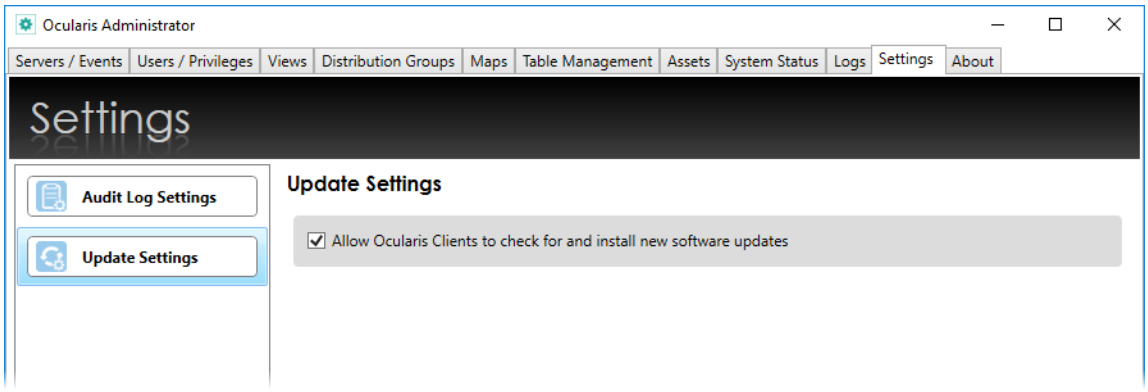


- Click **No** will avoid software installation at the present time. The software may be manually installed at a later time by launching Ocularis Client x64.exe from `c:\Program Data\OnSSI\OcularisClient`.
- Click Yes will close Ocularis Client and start the upgrade process.

16.2.1 To Allow Ocularis Client Users to Self-Update

1. First, make sure to update Ocularis Base and *Ocularis Administrator*.
2. In *Ocularis Administrator's* Settings Tab, make sure the checkbox to 'Allow Ocularis Client to check for and install new software updates' is checked. It is checked by default.

Figure 180 Allow Ocularis Clients to Self-Update



Reminder: the above process will work only if the Ocularis Client user has administrator privileges on their local PC. You can also right-click the Ocularis Client desktop icon and select 'Run as administrator'. If administrator privileges are unavailable, the standard method of re-installing the new Ocularis Client over the old Ocularis Client will then need to be performed.

17 About Tab

The About Tab displays system information regarding the Ocularis installation. The display is divided into four sub-tabs:

- About Ocularis
- Base Licenses
- Recorder Licenses
- Help

17.1 About Ocularis

The **About Ocularis** sub-tab displays version and build information for the Ocularis Administrator / Base installation.

Figure 181 Version Information on the About Tab

17.2 Base Licenses

The **Base Licenses** sub-tab provides a unified display of Ocularis Base license information as well as the number of cameras used and their corresponding recording components.

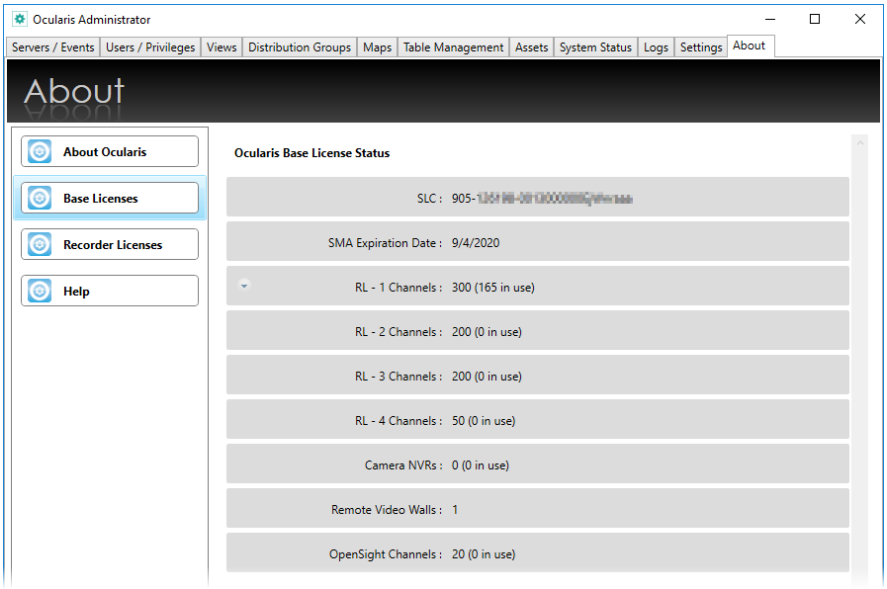
Ocularis v5.x includes categories where recorder licenses are assigned. These categories are labeled:

- *RL-1 Channels*
- *RL-2 Channels*
- *RL-3 Channels*
- *RL-4 Channels*

The categories simply represent a counter where similar recorder camera license counts are placed. Since Ocularis v5.x supports Mix & Match of recorders, different recorder counts can be combined into the same category.

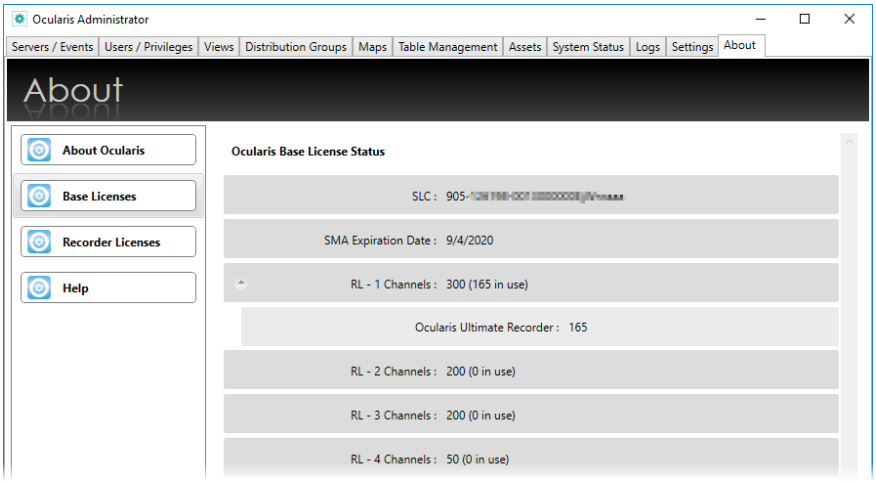
For example: camera licenses for Ocularis Ultimate Recorder, RC-E and RC-L would all appear in the category *RL-1 Channels*. The example shown in *Figure 182* shows that the license contains 300 RL-1 licenses, 165 of which are in use.

Figure 182 About Tab License Information



If you expand any row, you will see the detailed breakdown of how the licenses are distributed. (See Figure 183). In this example, the customer is using only Ocularis Ultimate.

Figure 183 About Tab Expanded Rows

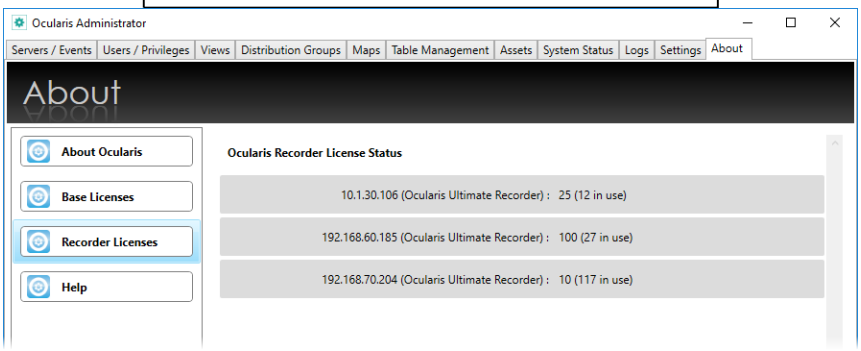


This feature gives you the flexibility to exchange licenses between recorders within the same RL level, allowing you the time and flexibility to migrate cameras from one recorder to another at your own pace. Video Channel licenses are assigned by the administrator in the **Servers / Events** tab. (See *Selecting Licensed Cameras* on page 16). RL-4 Channels are reserved for RecOn5 NVRs.

17.3 Recorder Licenses

The **Recorder Licenses** sub-tab provides a unified display of Ocularis recorder license information as well as the number of cameras used. This saves you the effort of logging into each Master Core individually to locate this information.

Figure 184 Recorder Licenses



17.4 Help

Click the **Help** sub-tab to launch the Ocularis Administrator User Manual using the corresponding PDF reader.

18 OpenSight

Ocularis OpenSight™ enables disparate Ocularis systems to be monitored within a single interface.

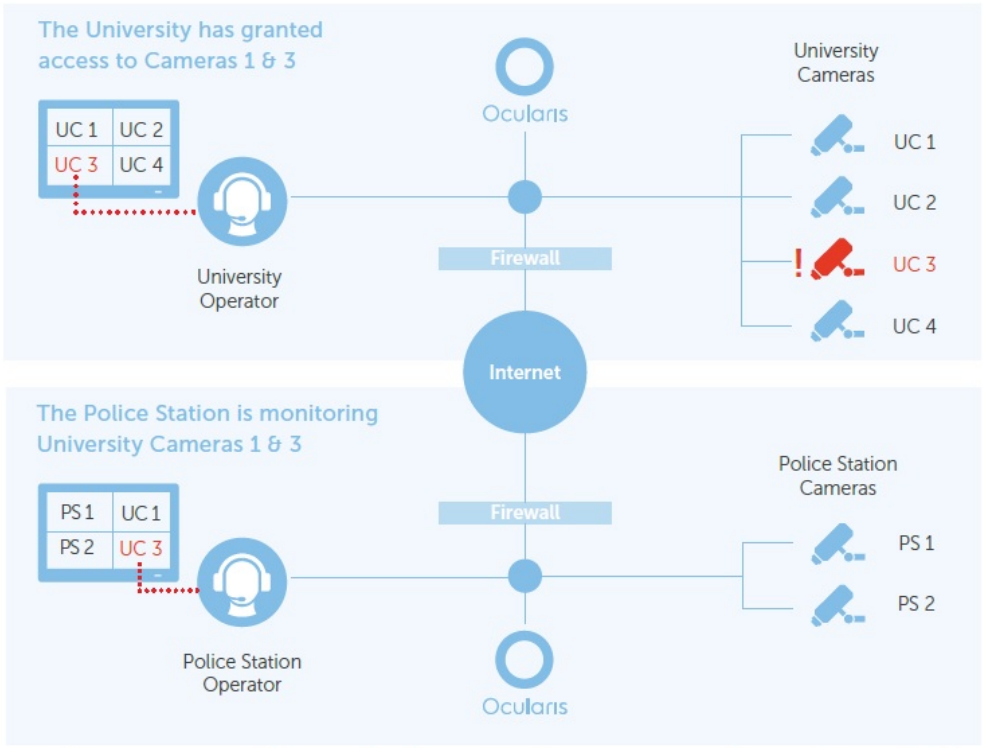
18.1 What is Ocularis OpenSight?

Ocularis OpenSight is designed to let users consolidate and share information from video surveillance and other security systems that are not within a single entity. For example, a school may wish to allow the local police department to monitor selected cameras of the school's security system. With OpenSight, the police can now view the school's designated cameras within the police department's own Ocularis configuration without the need for a separate login into the school's system. What's more, many other schools can be added to the same view at the police department. Ocularis OpenSight is an Add-On that is supported on the Base for Ocularis Ultimate.

When implementing OpenSight in this example, the university, or host, would grant the police department the user privileges and access rights the school feels is necessary for proper monitoring by the police. These rights and privileges can be different from the school's own internal personal use. If this university has multiple locations it may wish to share information between each in one integrated map.

Figure 185 OpenSight Layout (Sample)

Share as many or as few cameras and events from your Ocularis system with other security stations running Ocularis for added coverage.



Should an emergency situation develop, authorities can assess and respond immediately. Police stations can monitor multiple disparate systems simultaneously.

18.1.1 OpenSight & RecOn5 NVR

The RecOn5 NVR is a complete Ocularis system installed on specific hardware. This is an all-in-one implementation of Ocularis where all components are installed on the same computer. In the event where an organization would like to include cameras from a RecOn5 NVR into their corporate Ocularis installation, they may do using OpenSight. The organization must have Ocularis ULT as their Base and they must purchase OpenSight licenses to import RecOn5 cameras.

18.2 OpenSight Entities

As depicted in Figure 185 above, there are typically two parties or entities involved when using OpenSight. These are: the *Host* (who 'hosts' the video) and the *Remote Monitor* (who 'monitors' someone else's video).

18.2.1 Host

The *Host* entity in an OpenSight environment, is the party who wishes to share their cameras with someone else. Cameras may be shared across the same organization or with different companies. To use OpenSight, the Host may possess any of the following recorders:

Supported Recorders	
Ocularis Ultimate Recorder	RC-C
Ocularis Enterprise Recorder	RC-I
Ocularis Professional Recorder	RC-P
RC-E	NetDVMS
RC-L	…and other 3rd party recorders (check with Tech Support to see if your recorder is supported with OpenSight)
RecOn5 NVR	

In the example above, the host is the University.

See Host Configuration below for further instructions.

18.2.2 Remote Monitor

The *Remote Monitor* entity in an OpenSight environment, is the party who wishes to view the cameras of someone else. It can be across the same organization or with different companies. To use OpenSight, the Remote Monitor must possess a valid installation of Ocularis Base with corresponding OpenSight licenses. Supported models include Ocularis Ultimate as well as legacy models Ocularis ES, Ocularis LS and Ocularis CS. (Note: legacy models can only support legacy recorders). In the earlier example, the Remote Monitor is the Police Department.

Note: the Host recorders brought into a Base with OpenSight licenses must be the same model as the Remote Monitor's Base or lower. For instance, if the Police Department had Ocularis LS, they could only monitor a Host with RC-L, RC-C, RC-P or NetDVMS. They could not monitor RC-E, Ocularis Ultimate Recorders, Ocularis Enterprise Recorders or Ocularis Professional Recorders. If the PD used the Ocularis Ultimate model, they could monitor any supported recorder in the list shown on page 206.

See Remote Monitor Configuration below for further instructions.

18.3 Configuring OpenSight

This section reviews the steps necessary for OpenSight configuration.

- Host Configuration
- Remote Monitor Configuration

18.3.1 Host Configuration

The following steps should be performed by the Host when preparing their system for OpenSight use.

1. Determine which cameras you wish to be monitored by the Remote Monitor organization.
2. Create a user account on the recorder (Master Core) with the privileges you wish to provide to the Remote entity.
3. Provide the Remote Monitoring entity with the user account ID, password, public IP address and port number for the recorder (i.e. Image Server or Master Core).
4. The IT department should configure the firewall to port forward 1801 outbound to the remote monitor's public IP address.

Proceed with the following instructions based on the recorder used:

- For Ocularis Ultimate, Ocularis Enterprise, Ocularis Professional Recorders & RecOn5 NVRs see page 209.
- Host Configuration For NetDVMS 6.5x Recorders see page 209.
- Host Configuration For RC-C 7.0x/8.0x and Later Recorders see page 211.
- Host Configuration For NetEVS 3.1x, RC-L 6.0x, and RC-E 4.0x/5.0x/6.0x Recorders see page 212.

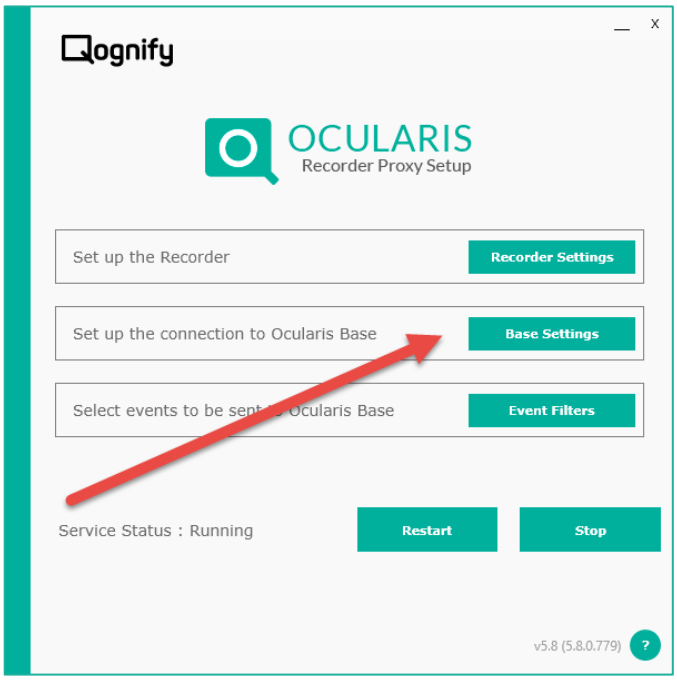
5. If you would like your Ocularis events forwarded to the Remote Monitor, add the Remote Monitor's public Ocularis Base IP Address to your recorder proxy.

   How To….

   Ocularis 5 Recorder proxy

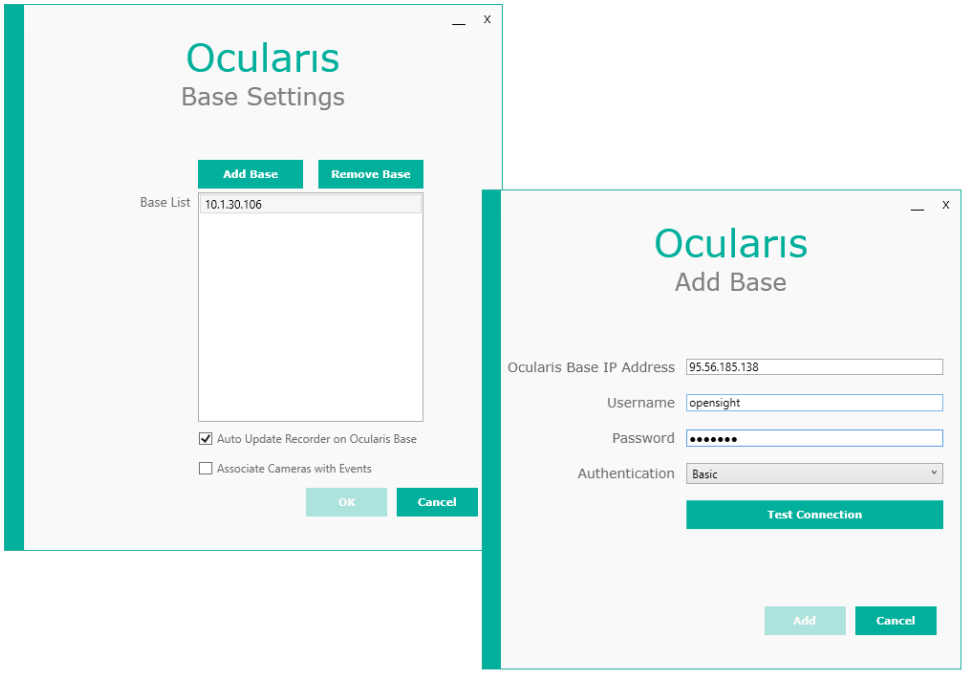
   In the Ocularis Recorder proxy, click **Base Settings**.

Figure 186 Ocularis Recorder Recorder Proxy



In the Base Settings screen, click **Add Base** and enter the Base IP address of the Remote Monitor's Ocularis Base (external address) as well as user account credentials they provide.

Figure 187 Configure Base Settings



Click **Test Connection** to verify credentials and then click **Add**.

Click **OK** on the Ocularis Base Settings screen.

Start the service if it is not running.

RC-C Event Proxy

In the RC-C / RC-I Event Proxy, enter the IP address for your own Ocularis Base computer as well as the Remote Monitor's Ocularis Base (external address) computer in the Server IPs field. Separate each IP address by a comma.

RC-L/RC-E Event Proxy

In the RC-L/RC-E Event Proxy, enter IP address for your own Ocularis Base computer as well as the Remote Monitor's Ocularis Base (external address) computer in the Base Server IP field. Separate each IP address by a comma.

18.3.1.1 Host Configuration for Ocularis Professional, Ocularis Enterprise and Ocularis Ultimate Recorders

How To….

1. Using the *Ocularis Recorder Manager*, log in to the Core.
2. Create a new user account.
3. In the 'Manage user rights' section of the user configuration, select the cameras that you would like to grant access to the remote monitor.
4. You may further select the rights of the selected cameras to include:
    a. Surveillance camera – allows access to live video
    b. Camera archive – allows access to recorded video
    c. Camera PTZ – allows the ability to use PTZ controls
    d. Use camera position – allow the ability to use PTZ presets that you have defined on the recorder
5. Click **Save**.
6. Close the *Ocularis Recorder Manager.*

18.3.1.2 Host Configuration For NetDVMS 6.5x Recorders

1. On the NVR responsible for those cameras you wish to share, create a new basic user account in the *NetDVMS Image Server Administrator* to be used by the Remote Monitoring entity. If the cameras are located on more than one NVR, this process must be repeated for each NVR. In the case of a master-slave, create the user account on the master NVR.

    How To….

    a. In the User Administration section of the *NetDVMS Image Server Administrator*, click the **User Setup** button.

b. Click the **Add a Basic User** button.

c. Enter a **Username** to be given to the Remote Monitoring entity.

d. Enter a **Password** for this account.

e. Click **OK** and then click **Close**.

2. Restrict the access for this new user account for only those cameras you wish to be monitored.

   How To….

   a. In the User Administration section of the Image Server Administrator, select the **Restrict user access** radio button.

   b. Click the **User Access** button.

   c. Select the new user account from the User drop-down list.

   d. Select the Global User Rights you wish to provide to the Remote Entity.

   e. Select the cameras you wish to enable for the Remote Entity.

   f. Select or remove additional privileges for the cameras (Browse rights, Export, etc.)

      Restrict the account privileges to only those which you want the Remote Monitoring entity to have. You may be as broad or as granular as you like. Consider, however, that you may not want to provide privileges to a feature that may interfere with your own operators (such as controlling PTZ).

   g. When finished, click **Close**.

3. If it is not already configured, outside access must be enabled in order to allow the Remote Monitoring entity to gain access to the NVR video.

   How To….

   a. In the Server Configuration section of the Image Server Administrator, check the **Enable Outside Access** checkbox.

   b. In the **Outside Address** field, enter the public IP address assigned to your firewall.

   c. In the **Outside Port** field, enter the port used by the public IP address to gain access via the firewall.

   d. Click the **Local IP Ranges** button to identify local address ranges used internally. This will enable the Image server to recognize login requests originating from these IP addresses as coming from a local network and provide access locally.

      ***Note**: when using outside access, the router or firewall used must be configured so that requests sent to the outside (public) IP address and port are forwarded to the inside (local) IP address and port of the server running the Image Server service.*

   e. When done adding local IP ranges, click **Close**.

   f. Click **OK** to save settings and close the NetDVMS Image Server Administrator.

18.3.1.3 Host Configuration For RC-C 7.0x/8.0x and Later Recorders

1. On the NVR responsible for those cameras you wish to share, create a new basic user account in the *Management Application* to be used by the Remote Monitoring entity. If the cameras are located on more than one NVR, this process must be repeated for each NVR. In the case of a master-slave, create the user account on the master NVR.

   How To….

   a. In the *Management Application*, expand the *Advanced Configuration* node of the Navigation Pane.
   b. Right-click the **Users** node.
   c. Select **Add New Basic User**.
   d. Enter a **Username** to be given to the Remote Monitoring entity.
   e. Enter a **Password** for this account.
   f. Click **OK**.

2. Restrict the access for this new user account for only those cameras you wish to be monitored.

   How To….

   a. In the *User Properties* screen, accessed by double-clicking the username if not already open.
   b. Click the **General Access Properties** tab.
   c. Select which general settings you would like to grant to this user account.
   d. Select the **Camera Access** tab
   e. Select the cameras you wish to enable for the Remote Entity.
   f. Select or remove additional privileges for the cameras (Browse rights, Export, etc.)

      Restrict the account privileges to only those which you want the Remote Monitoring entity to have. You may be as broad or as granular as you like. Consider, however, that you may not want to provide privileges to a feature that may interfere with your own operators (such as controlling PTZ).

   g. When finished, click **OK**.

3. If it is not already configured, outside access must be enabled in order to allow the Remote Monitoring entity to gain access to the recorder video.

   How To….

   a. In the Navigation Pane, right-click the *Server Access* node.
   b. Select **Properties**.
   c. In the Server Access tab, check the **Enable Internet Access** checkbox.

d. In the **Internet Address** field, enter the public IP address assigned to your firewall.

e. In the **Internet Port** field, enter the port used by the public IP address to gain access via the firewall.

f. Click the **Local IP Ranges** tab to identify local address ranges used internally. This will enable the Image server to recognize login requests originating from these IP addresses as coming from a local network and provide access locally.

***Note**: when using outside access, the router or firewall used must be configured so that requests sent to the outside (public) IP address and port are forwarded to the inside (local) IP address and port of the server running the Image Server service.*

g. Click **Add** to enter the *Start* and *End* Address for the Local IP Range

h. When done adding local IP ranges, click **OK**.

i. Click **Apply** to save settings.

18.3.1.4 Host Configuration For NetEVS 3.1x, RC-L 6.0x, and RC-E 4.0x/5.0x/6.0x Recorders

1. On the Management Server machine, create a new Windows account to be used by the Remote Monitoring entity. This account is created through the operating system user account utility. Be sure to create a password for this user account.

2. Using the Management Client (or NetEVS Manager), create a Role specifically for use by the Remote Monitor.

   How To….

   a. In the Management Client, right-click on *Security* > *Roles* in the navigation tree.

   b. Select **Add New Role…**

   c. Enter a name to assign to remote monitoring users.

   d. Enter an optional description for this role.

   e. Click **OK**.

3. Add the Windows account created in step 1 to this new role.

   How To….

   a. Select the Role created in step 2 above.

   b. In the **Users & Groups** tab, click the **Add** button.

   c. Verify that the required domain is specified in the *From this location* field. If not, click the **Locations** button to browse for the required domain.

   d. In the *Enter the object names to select* text box, type the user name created in step 1.

   e. Click the **Check Names** button to verify the entry.

f. If you are prompted for the username and password, enter it and click **OK**. The name should be listed n the *Enter the object names to select* text box.

g. Click **OK**. The account should be added as a member of this Role.

4. Configure the rights for this Role. Restrict or grant access to devices and functions as needed.

   How To….

   a. Select the Role created in step 2 above.

   b. For each tab, (Device, PTZ, Speech, Application, etc.) grant or restrict access to cameras and privileges for the remote monitor.

5. Save changes.

18.3.2 Remote Monitor Configuration

The following steps should be performed by the Remote Monitor entity when preparing their system for OpenSight use.

1. Purchase OpenSight licenses from your Qognify certified dealer.
2. Your Ocularis Base SLC will need to be refreshed to be updated with the new OpenSight camera licenses.
3. Open the *Ocularis License Activation* application located on the Ocularis Base computer.
4. For:
   a. Existing installations:
      i. Click the **Refresh** button.
   b. New Installations:
      i. Enter your Ocularis SLC and click **Activate SLC**.
5. If the Ocularis Base computer has internet connectivity, licensing is done online and you are done! If there is no internet connectivity, a few additional steps are required:
   a. Click the link in *Step 2: Click here to retrieve offline html file*.

      An html file is created named `OcularisActivationRequest.html` and stored in:

      ```
      c:\Program Files (x86)\OnSSI\Ocularis Licensing
      Activation\OfflineActivation
      ```

   b. Copy this file to portable media and bring to a computer that has internet connectivity.

   c. Launch the `OcularisActivationRequest.html` file (double-click it).

   d. The default web browser should launch and load a page with a Download button. Click the **Download** button.

   e. The browser may ask you if you want to save a file called `response.xml` from `licensing.onssi.com`. Choose **Save As** and save it to portable media.

   f. Bring the `response.xml` file back to the Ocularis Base computer.

   g. On the Ocularis License Activation screen, click the link in *Step 3: Click here and browse to the response file*.

h. In the resulting Windows' Open dialog, browse to the `response.xml` file you just brought from the internet connected machine. Select the file and click **Open**.

6. You should see a 'License Activation Successful' pop-up. Click **OK**.
7. Close the *Ocularis License Activation* application.
8. Obtain the access credentials from the Host.

   You will need:

   a. The public IP address of their recorder.

      i. For Ocularis Ultimate Recorder, Ocularis Enterprise Recorder, Ocularis Professional Recorder & RecOn5 NVR: You need the IP address of the Master Core Server.

      ii. For NetDVMS, RC-C, RC-I and RC-P: You need the IP address of the Recording Server machine(s).

      iii. For NetEVS, RC-L and RC-E: You need the IP address of the Management Server machine.

   b. The port number for the corresponding NVR Server(s) (a.k.a Image Server port #).

   c. The user account created for you by the Host.

   d. The password for this account.

9. In Ocularis, add the Host's NVR(s) using the credentials provided.

   How To….

   a. Open the *Ocularis Administrator* application.

   a. In the **Servers/Events** tab, click the **Add** button in the Servers pane. (See *Figure 8* on page 9).

   b. Type the IP address of the Host's NVR followed by a ":" and (for legacy recorders) the port number.

      For example:

      204.55.174.192:8080

   c. Select **Basic** or **Windows** as the login type as instructed by the Host.

   d. Enter the **User nam**e provided to you by the Host.

   e. Enter the **Password** provided to you by the Host.

   f. Click the *Use OpenSight* checkbox.

   g. Click the **Add** button.

   The server should appear in the Servers pane and the authorized cameras are displayed when the NVR is expanded. Only OpenSight licenses will be applied to cameras on this server. Check the **About Tab** to verify.

   Repeat these steps for each recorder to be used with OpenSight licenses.

10. Provide access to the new cameras to those Ocularis users as needed.

How To….

a. In the **Users/Privileges** tab, select the group for which you would like to provide access to the new cameras.

b. Drag and drop the camera from the **Devices** list to the **Privileges** pane.

11. Restrict further privileges if necessary.

How To….

a. In the **Users/Privileges** tab, uncheck privileges to the newly acquired cameras (PTZ, Presets, etc.)

Note: *Despite appearances, you may have fewer privileges than displayed on the Users/Privileges pane. You may further restrict privileges but you may not grant additional privileges to OpenSight licensed cameras.*

12. Assign the newly acquired cameras to new or existing views in the **Views** tab.
13. Save your changes.
14. The IT department should forward the following ports:

a. 1801 inbound to Ocularis Base

b. If receiving events from the Host using an RC-E, RC-L, RC-C, RC-I, RC-P or NetDVMS recorder, the NetCentral port #1237 should be forwarded inbound to Ocularis Base.

When viewed in the Ocularis Client, these cameras will appear as any other cameras and the fact that they may belong to another organization is entirely transparent to the operator.