grass valley
A BELDEN BRAND

ICONTROL

CUSTOMIZED, END-TO-END FACILITY MONITORING

User Guide

M226-9900-294

2017-02-24

www.grassvalley.com

Copyright and Trademark Notice

Warranty Policies

Warranty information is available from the Legal Terms and Conditions section of Grass Valley's website (www.grassvalley.com).

Title	iControl User Guide
Part Number	M226-9900-294
Revision Date	24 February 2017 3:57 pm

toc

Table of Contents

1 Introduction to iControl

iControl is a high-level Element and Network Management System for television service providers, content originators and broadcasters, used to perform wide-ranging video and audio signal, device and facility monitoring and control over a TCP/IP network.

Summary

Overview

Grass Valley's ƒ is a coordinated suite of software applications and hardware designed for the interactive control and monitoring of distributed broadcasting networks.

iControl allows operators to control and monitor the status of Grass Valley and third-party video and audio modules (converters, distribution amplifiers, probes, etc.), routing switchers, and other network equipment, all from any convenient point with IP access.

Features of the iControl system include:

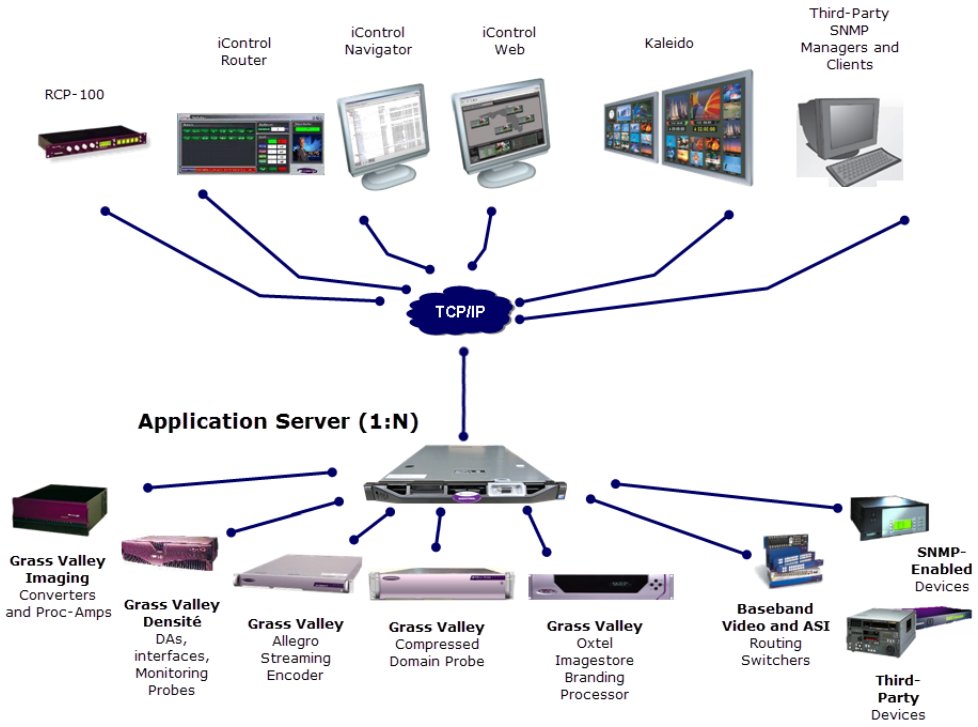
- **Fully integrated desktop:** iControl brings together equipment, signal and facility monitoring and control for highly efficient operations.
- **Visual customization:** Highly customized graphical representations of one or more facilities can be created to offer a highly intuitive control environment.
- **Third party application control:** Multiple third party applications can be hosted in the iControl interface, and these can be selected manually or presented automatically for effective device control.
- **SNMP support:** iControl combines IP monitoring with SNMP to allow the collection of third party equipment status and offer multi-vendor interoperability.
- **Media streaming:** High quality streaming provides effective visual monitoring feedback.
- **Modularity & scalability:** iControl is fully scalable and can be used to control just part of a television system or for complete management of multiple sites.
- **Automated responses:** A *scripted macros* feature can provide automated reactions to alarm conditions and guide operators through complex diagnostics.

iControl represents video networks with rich, interactive graphics that are immediately understandable and easy to operate. The system is geared towards simplifying operations so

that a single user can control more channels, or a broader range of monitoring and control tasks.

With iControl, customized views of a network can be created, complete with full motion, high quality streaming video and audio. The highly graphical nature of iControl allows operators to quickly identify and respond to alarm conditions, thereby reducing *Mean Time to Repair* (MTTR).

iControl leverages industry-standard SNMP protocols and integrates other third party control applications to provide a complete facility monitoring environment.



Multi-Channel Monitoring and Control

iControl is currently used by cable, satellite and IPTV channel distributors for the monitoring and control of hundreds of channels. iControl contributes to the reduction of MTTR, and gives operators the ability to monitor signal performance throughout even the most complex distribution and processing networks. iControl allows “monitoring by exception”, to help operators better handle large channel counts.

Multi-Site Monitoring and Control

iControl is currently used by broadcasters and networks with facilities and signals distributed in multiple cities and across multiple time zones.With its TCP/IP-based architecture, iControl provides flexibility in gathering data from remote signals and systems, and performing remote control of network devices.

Incoming Feed Quality Control

iControl is currently used by broadcasters and channel distributors for quality control of incoming feeds.SInce it supports streaming media, iControl provides the ability to provide image-based recognition of incoming video feeds, and the ability to control associated video processors and routing switcher assignments.

Router Control

iControl is currently used by broadcasters and multi-channel distributors to control local and remote routing switchers, from multiple manufacturers.

See also

For more information about:

- Setting up iControl Router, see the *iControl Router Quick Start Guide*.
- Operating iControl Router, see the *iControl Router User Guide*.

Video Element Management

iControl is currently used by broadcasters and television service providers for the monitoring and control of dozens of third-party devices. iControl can be used in NOCs (Network Operation Centers), master control rooms and playout centers to interface to a multitude of systems, performing a wide range of functions.With its ability to measure the health and performance of various devices in the signal chain or within the underlying infrastructure, iControl can be configured to perform failover management of signals and systems.

Monitoring and Control of Grass Valley Devices and Systems

iControl provides control and monitoring of:

- Densité-series and Imaging-series interface cards
- Imagestore channel branding processors
- EdgeVision streaming encoder/servers
- Kaleido-K2, Kaleido-Alto, Kaleido Quad, and Kaleido-X multi-image display processors

Features and Benefits

Rich monitoring, including streaming video

- iControl provides the essentials of television: images and sounds to provide operators quick and accurate access to all signals in the network.
- iControl provides visual and audible monitoring of signals via a standard TCP/IP network:
- displays high frame rate video as well as low frame rate video thumbnails
- accesses audio streams and displays audio levels
- Local signals can be incorporated directly into **iC Web** pages as high-resolution, high quality images

- Remote signals can be accessed via quality streams generated by the EdgeVision device, as either single images of multi-image mosaic from the outputs of the Kaleido multi-image display processors.

End-to-end facility monitoring

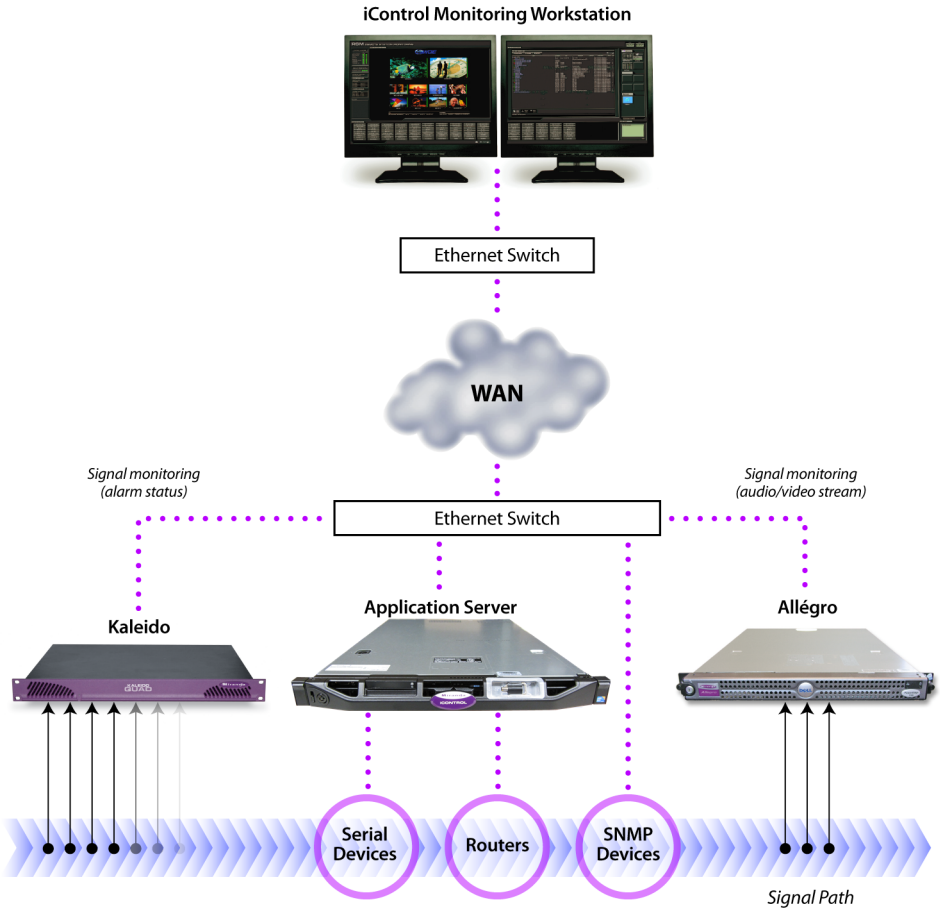
- iControl provides end-to-end facility monitoring by performing signal quality and device health monitoring across all essential formats: audio, video and ancillary data in RF, baseband, analog, SD, HD, ASI and IP.
- All the diverse elements involved in playout can be controlled from a single, integrated GUI and just one keyboard and mouse.
- The highly graphical views, with full motion and high quality streaming video, allow operators to quickly identify and respond to alarm conditions, and thereby reduce the Mean Time to Repair (MTTR).
- iControl helps correlate alarms and data from multiple sources and devices by dynamically displaying only the elements associated to a particular service or location, whether upstream or downstream. This can greatly help operators in assessing fault conditions and their consequences.

Extensive third-party device control and monitoring by SNMP and embedded applications

- A high level of device control and monitoring for a wide range of devices and manufacturers is available with iControl, covering all essential television distribution and broadcast applications
- Interfacing to third-party devices is achieved by combining industry standard SNMP control protocols with feedback from full motion and high quality streaming video.
- iControl can also control third party devices using embedded control applications, and these can be automatically presented to the operator by device alarms to speed response times.

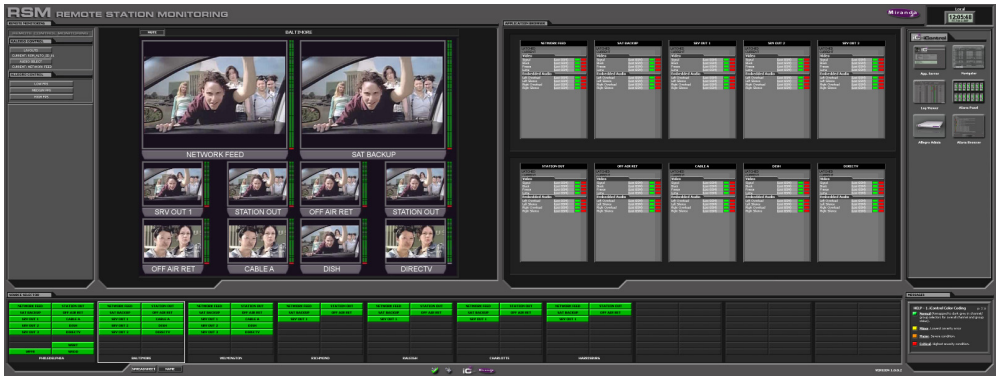
Operational Overview

The diagram below shows the relationship between the elements of an iControl system, and how they work together to provide real time monitoring of a signal path.



User Interface

Once the iControl system is up and running, monitoring data and live audio/video streams are automatically presented to operators via custom Web pages. Operators have access to current and historical information on every device and signal being monitored.



Example of a customized iControl User Interface

Example of a customized iControl User Interface

Example of a customized iControl User Interface

How iControl Works

The central element of any iControl system is the iControl Application Server. The Application Server is a compact, 1 RU server that interfaces to video, audio and other hardware through a variety of configurable ports (RS-232, RS-422, Ethernet), and connects to a local LAN over TCP/IP.

iControl runs in a distributed network environment. Devices to be monitored or controlled are either directly connected to the iControl Application Server, or accessible over a TCP/IP connection. Each iControl Application Server runs several device control services, as well as a lookup service.

Multiple Application Servers can coexist on a network, allowing large-scale distributed systems to be defined and controlled. Using a Web browser, multiple users can connect to any Application Server from any convenient desktop or portable computer.

On your client PC, you may launch any of the iControl components from a single user interface called the **iControl Launch Pad**. The iControl Launch Pad may be downloaded to your client PC from your Application Server.

iControl Launch Pad

Components of iControl

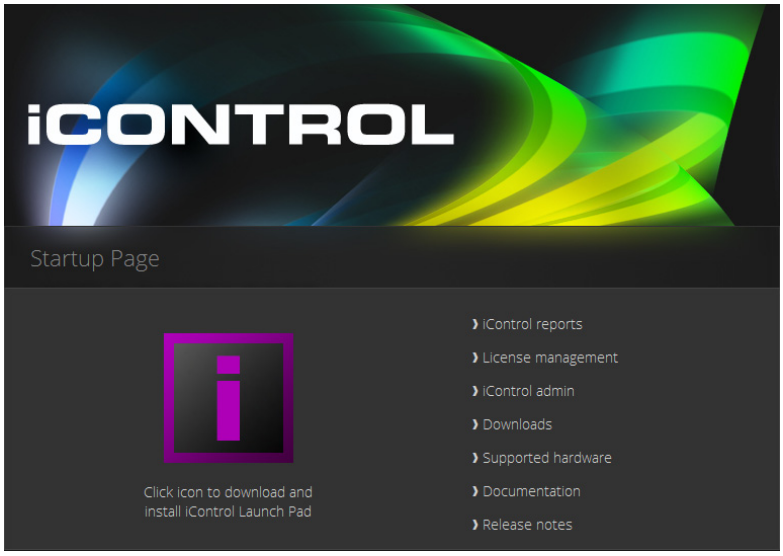
iControl consists of a set of software components, the principal ones being:

- **iC Navigator** (see iC Navigator, on page 8)
- **iC Router** (see iC Router, on page 10)
- **iC Creator** (see iC Creator, on page 11)
- **iC Web** (see iC Web, on page 12)

Each of these core components can be started from **iControl Launch Pad**, which is a client-side application downloadable from iControl's *Startup* page.

There are three other core iControl components, important for system administration, and the smooth, integrated operation of iControl as a whole. You can link to pages dedicated to their functions from the Startup page. These other components are:

- *iControl admin* (see iControl admin Page, on page 12)
- *License management* (see License Management, on page 81)
- *Reports* (see iControl Reports, on page 126)

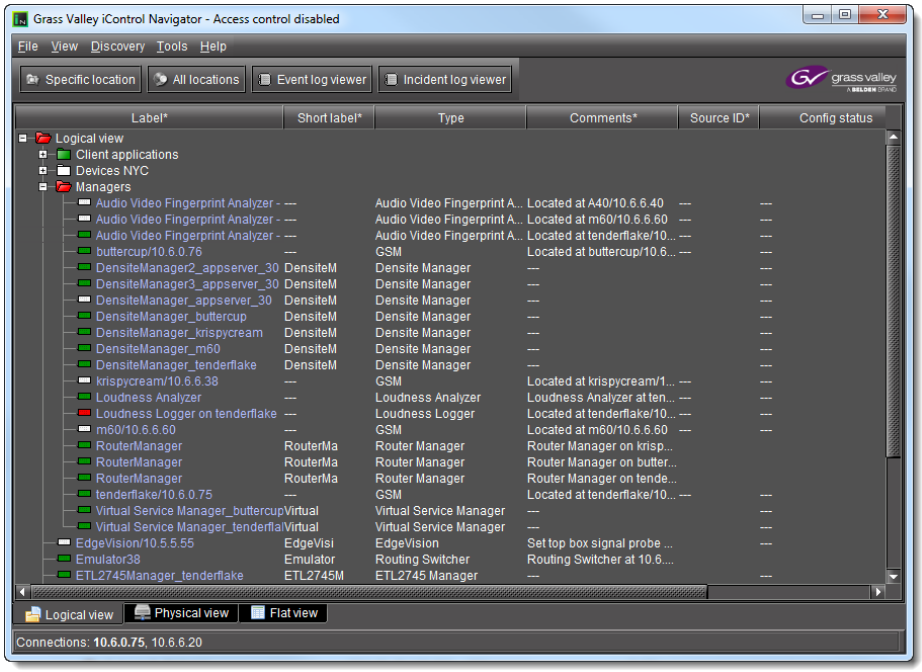


iControl's Startup Page

iC Navigator

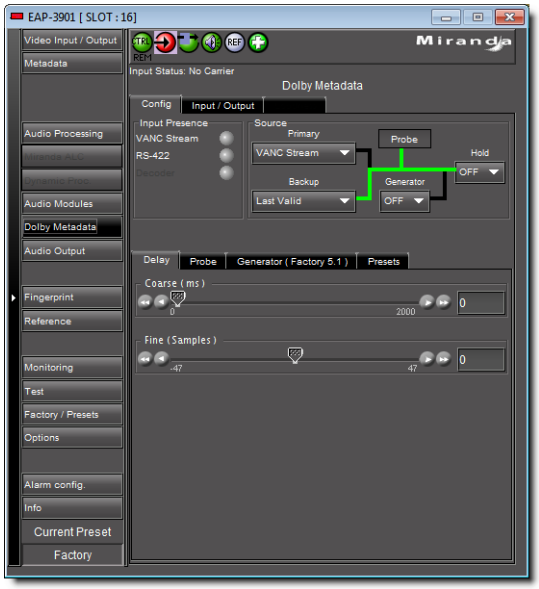
iC Navigator is used to view, control and monitor Grass Valley and associated third-party devices. This application provides users with direct access to the control windows of all devices on an iControl network. Users can easily configure parameters, monitor functionality, pinpoint problems, and track errors. It supports administrative tasks such as status reporting and event logging.

iC Navigator presents devices and services in a hierarchical view. The tree-like structure lists all recognized devices and services along with descriptions, including name, type, associated comments, configuration status, frame and slot number.



iC Navigator

iC Navigator lets users display device-specific control windows. Icons at the top of the control window provide a quick status indicator of key parameters. Color-coding enables operators working locally or remotely to quickly identify the operating status of a device or service. From iC Navigator, they can also display a configuration log panel for each device or service, which highlights error conditions.



iC Navigator also provides access to a Log Viewer (via the General Status Manager (GSM)—see below), which displays up to 100,000 of the most recent messages.

> **Note:** Displaying more than 10,000 messages in the Log Viewer may require system adjustments to maintain acceptable performance levels.

iC Navigator leverages industry standard SNMP protocols, and can fully integrate third party control applications to create a complete facility-monitoring environment. With automated reactions to failures, and guided operator responses, the system can deliver dramatically reduced down times.

iC Navigator Views

Sorting allows you to determine the way in which devices will be arranged for display in iC Navigator. Three views are available:

- **Logical View** arranges the devices in groups created by the user. Devices are sorted into groups, and within each group, arranged in alphabetical order. Ungrouped devices are displayed at the end of the list. Empty slots are not shown (unless they are in the Reference Config).

  > **Note:** The grouping is done on the Application Server, and therefore, changes apply for all users.

- **Physical View** arranges the devices relative to their physical connections and network location. All frame slots are shown, even if they are empty. This is done automatically by the system. Devices are sorted by:
  - the IP address of the iControl server,
  - then the serial communication port of the server where the (Imaging) frame is connected,

OR,

- the IP address of the Densité communicator,
- then the frame itself.

Once the frame folder is open, you can see the device by the slot when applicable.

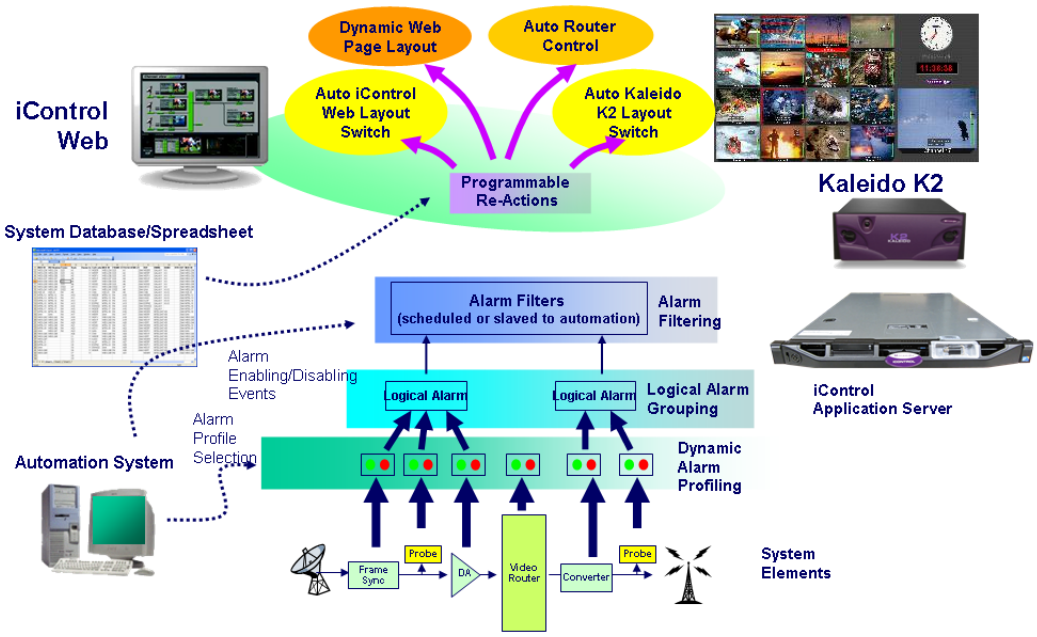
> **Note:** **Physical View** may only be applied to devices in frames.

- **Flat View** shows all devices in alphabetical order without any grouping.

With **Logical View** and **Physical View**, you can open and close folders in the list to display any level of the hierarchy.

General Status Manager (GSM)

iC Navigator is also the front end for—and depends largely upon—an iControl service called the *General Status Manager (GSM)*. At least one GSM is always running on an Application Server on a given network[1]. It acts as a central clearing station for device discovery and alarm status.

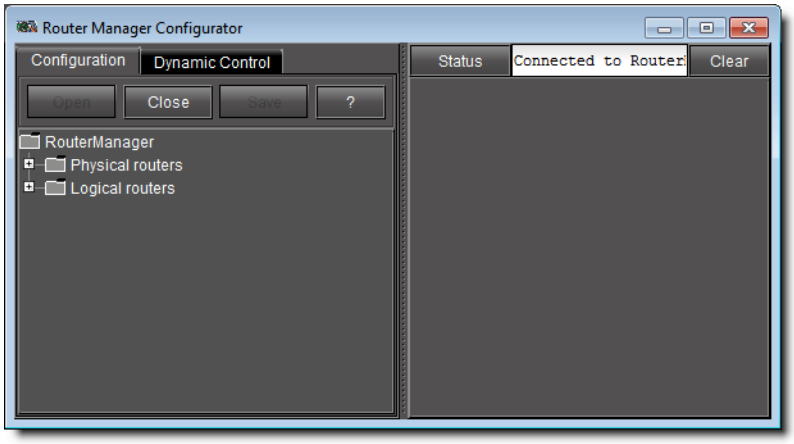


All iControl alarm notifications are managed through a central GSM. Alarm notifications from multiple distributed GSMs are managed by the multi-GSM Manager, which computes the virtual alarm, gets its status and dispatches the alarm status to the client.

iC Router

iC Router provides advanced router control and status monitoring via a flexible graphical user interface. With protocol and driver support for many router models, iC Router can be configured to manage multiple routers from multiple vendors from a single user interface.

1. To be more specific, on each subnet in a network being monitored by iControl there must be at least one Application Server with an active GSM.

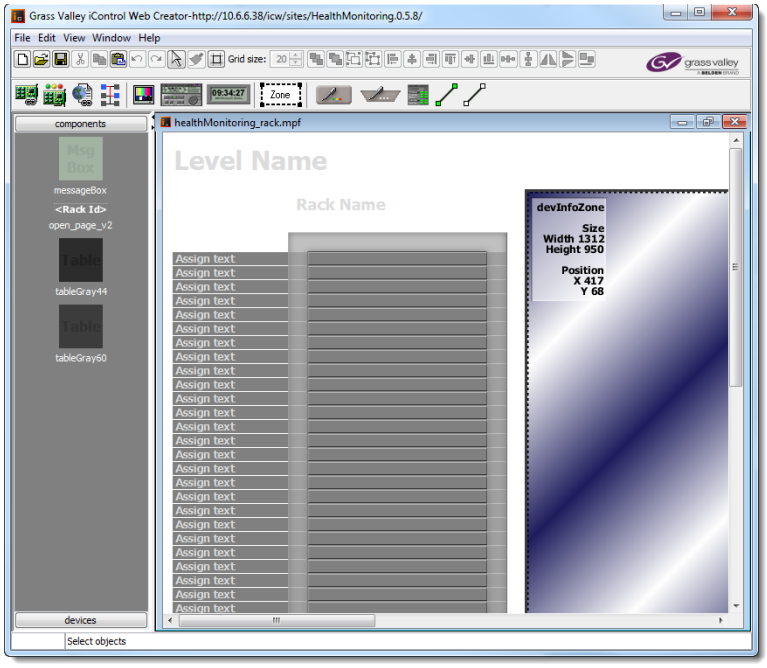


iControl Router Manager Configurator

iC Router works over regular IP networks, so that multiple users can monitor and control several routers, even from remote locations. Users can create virtual routing environments where physical router resources are deployed and controlled by software in customized configurations optimized for operational needs.

iC Creator

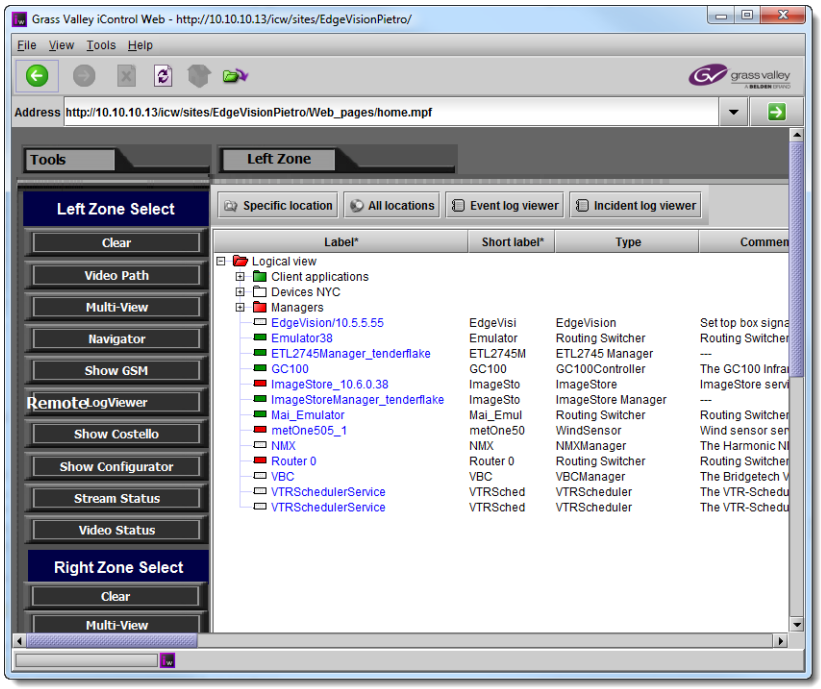
iC Creator is the application used to create **iC Web** sites. The pages of these Web sites provide a user-friendly interface for operators to control and monitor devices connected throughout the iControl environment. With iC Creator, users can build multiple representations of their networks and facilities using a simple drag-and-drop drawing editor. Objects that you create in iC Creator can be saved as *widgets*, and then re-used on other pages.



***iC Creator** is used to build monitoring and control Web sites*

iC Web

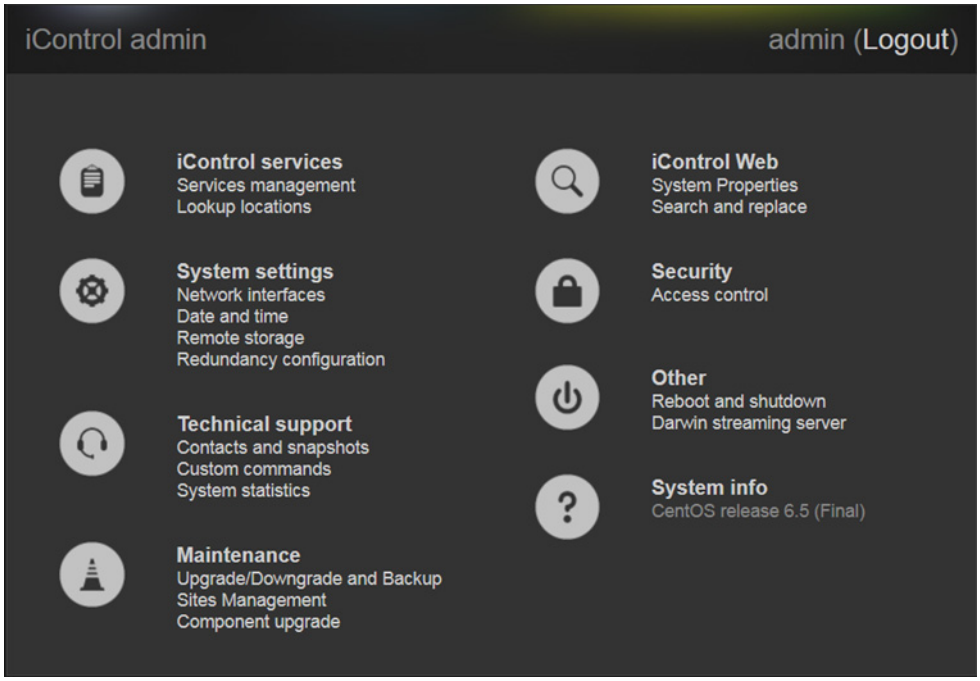
iC Web is a custom Web browser used to access iC Web sites hosted on an Application Server. It is sometimes referred to as the *runtime mode* of **iC Creator**.



iC Web site viewed using iC Web

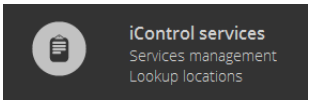
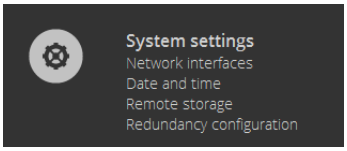
iControl admin Page

The *iControl admin* page is a sub-area of the iControl main site, and is devoted to administrative configuration. This page contains links to most of the functionality that you will use to administer iControl on a regular basis. Everything accessible within the *iControl admin* page is password-protected. The table below describes the tools available from this page.

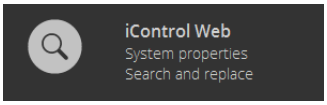
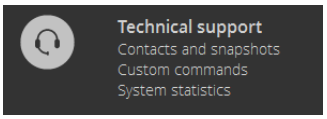
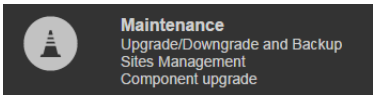
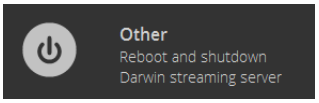
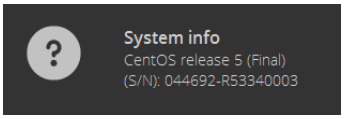


iControl admin page (see table, below, for descriptions)

iControl admin tools

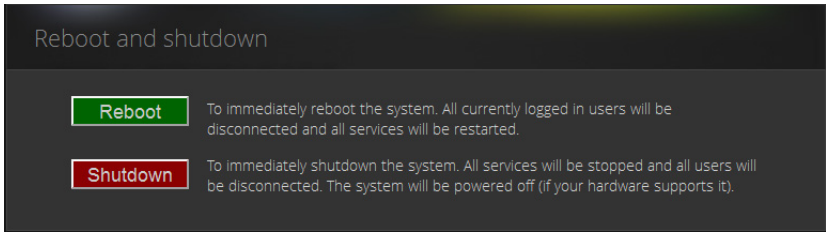
Category	Tool name	Tool description
iControl Services 	iControl Services Management	Used to start, stop and display the status of iControl services (e.g., GSM, Router Manager Service, RMI Daemon). Also used to load balance Densité Managers, configure serial ports, to start/stop lookup services, and to view a system profile of the Application Server.
	Lookup Locations	iControl uses a lookup service to get information about remote programs or machines, and uses that information to establish communications. In this way, cards, frames and other devices make their presence known on an iControl network, and participate in monitoring and control operations.
System Settings 	Network Interfaces	This page has links to other pages that allow you to configure an Application Server for network operations.
	Date and Time	Used to set the system's date and time, time zone, and either enable or disable NTP synchronization.
	Remote Storage	
	Redundancy Configuration	Used to set up N+1 redundancy configurations for Application Servers.

iControl admin tools*(Continued)*

Category	Tool name	Tool description
iControl Web 	System Properties	
	Search and Replace	Used to change (search and replace) a specific attribute in multiple iControlWeb (iC Web) pages on an Application Server.
Technical Support 	Contacts and Snapshot	Contact information (by region) for Grass Valley Technical Support and a utility application to create a system snapshot if one is required by Technical Support.
	Custom Commands	Behaves as front end to the execution of a collection of custom scripts, and is primarily used for troubleshooting problems on an Application Server.
	System Statistics	Provides links to statistics and graphs that can be used to monitor and troubleshoot the performance of an Application Server.
Maintenance 	iControl installation and backup	Used to install iControl software, back up data and configuration files, and restore iControl configuration data from a backup file.
	Sites Management	Used to upload and download channel spreadsheets to/from the Application Server.
	Component Upgrade	Used to upgrade iControl components, as well as to roll back iC Web sites and SNMP Drivers.
Security 	Access Control	Used to enable security, LDAP services, and Active Directory single sign-on. Also used to perform basic user management, to consult access-control related logs, and to allow or deny root user login over SSH.
Other 	Reboot and Shutdown	Used to reboot or shut down an Application Server.
	Darwin Streaming Server	Allows an Application Server to provide real-time streaming of video thumbnails. This page is primarily used to start or stop the Darwin Server.
System info 		Indicates the Application Server's current operating system.

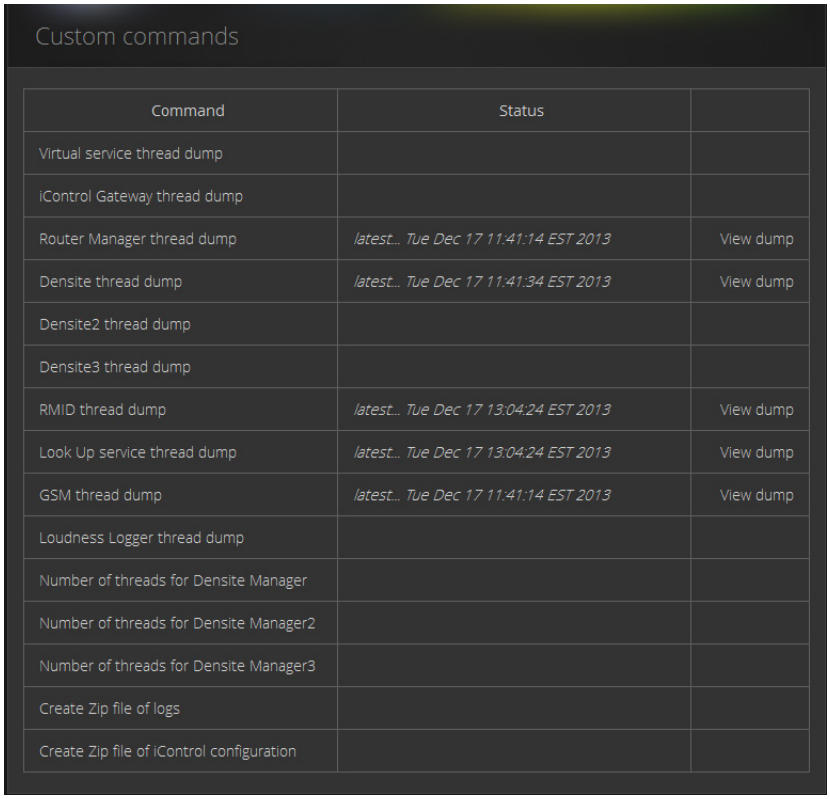
Reboot and Shutdown

This page is used to reboot or shut down an Application Server.



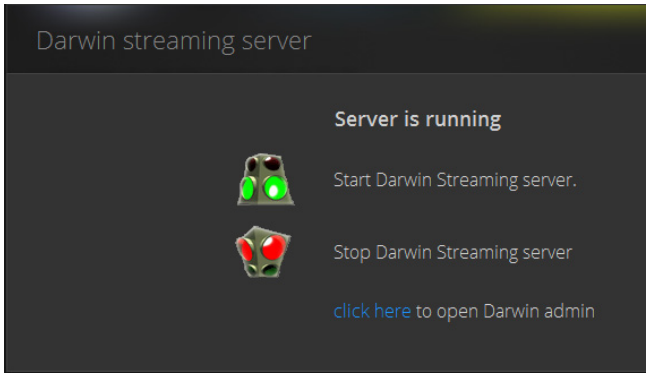
Custom Commands

This page acts as front end to the execution of a collection of custom scripts, and is primarily used for troubleshooting problems on an Application Server.



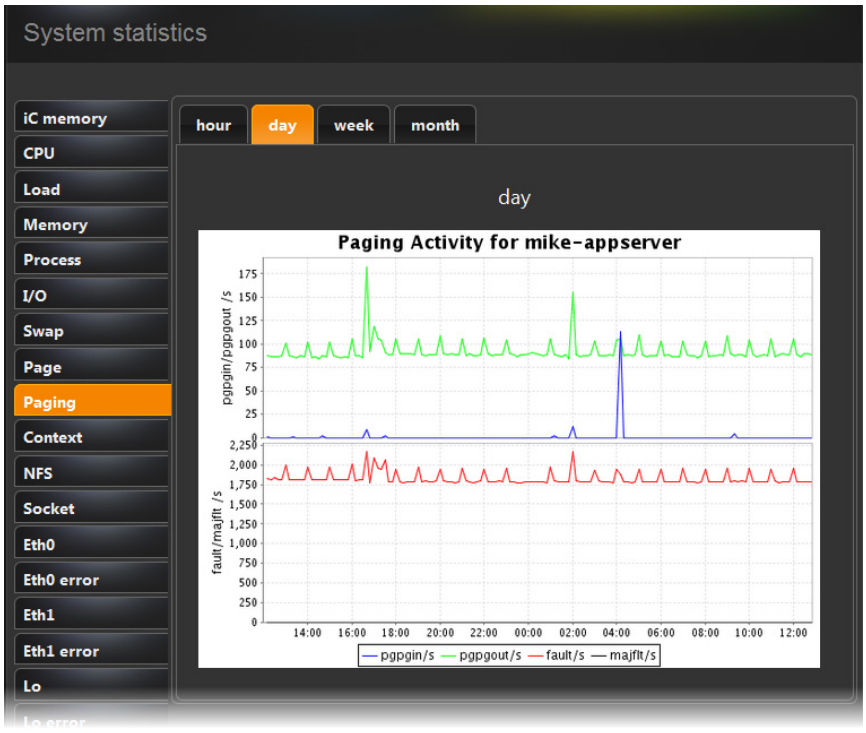
Darwin Streaming Server

The Darwin Streaming Server allows an Application Server to provide real-time streaming of video thumbnails. This page is primarily used to start or stop the Darwin Server.



System Statistics

This page provides links to statistics and graphs that can be used to monitor and troubleshoot the performance of an Application Server.



iControl Services

iControl Services are software components that support (or make additional functionality available to) iControl. These services are described in the table below:

iControl services

Service	Description
Imaging Communicators	Software components used to configure and control Grass Valley Imaging-series frames
Densité Communicators	Software components used to configure and control Grass Valley Densité frames
Kaleido/Oxtel Communicators	Software components used to configure and control Grass Valley Kaleido and Oxtel devices
Gateway	Software component that enables third party applications to monitor and control Grass Valley devices. It is also used to connect an RCP-100 or RCP-200 Remote Control Panel to iControl and to provide line selection from the iC Web player Densité-series cards scope option
GSM (General Status Manager)	Software component used for central management of all alarm conditions and error logging
Virtual Service Managers	Software components used for configuring and controlling Grass Valley proc amp devices and composite panels
Router Manager	Software component used for configuring and controlling routing switchers

In addition, services providing interfaces to third party devices are available as options. These services include VTR and IRD (Integrated Receiver Decoder) devices.

SNMP

SNMP (Simple Network Management Protocol) has emerged as an important standard in the broadcast industry, allowing broadcasters to monitor the equipment from multiple vendors using a single, IP-based protocol. iControl provides SNMP support in two distinct and important ways.

iControl acts as an *SNMP manager* by reading the status of third party devices that support SNMP and have published their SNMP MIB (Management Information Base). It augments the status information using streaming video, audio and scope telemetry data gathered using Densité Series cards and the Allégro Streaming Encoder/Server.

In those cases where a third party SNMP management application is deployed, iControl acts as an *SNMP agent* reporting errors and status to the SNMP manager using the SNMP protocol and its own SNMP MIB.

For devices that do not provide IP connectivity, the iControl Application Server acts as an SNMP translator and provides SNMP Agent functionality. The Application Server receives status information from the devices using their existing protocols, and will issue SNMP TRAPS and respond to SNMP GET messages on behalf of the devices below it. The Application Server further enhances SNMP Agent capability by allowing users to create virtual alarms, which can be enabled or disabled according to a schedule, or slaved to an automation system.

Note: Grass Valley devices that provide IP connectivity at the frame—such as Densité and Kaleido—offer direct SNMP support, allowing third party SNMP Manager applications to get status information using an SNMP `GET` command.

iControl Integration with Other Grass Valley Products

Grass Valley products are, naturally, tightly integrated with iControl, and are often found in networks where iControl has been installed. Some of the more popular Grass Valley products are described below.

Control Windows and Device Parameters

To control device parameters, double-click the device in the navigation pane to display the control window for that device. Or right-click the device and select **Show Control** window from the pop-up menu.

The device name is listed along the top of each control window along with the "status icon" for the device. Icons in the upper left corner of the control window (again depending on the device type) provide a quick status indicator of key parameters such as the Operational or Test Mode, Input Status, or Reference Status. This is called the "status dashboard".

On each control window, there are different selector tabs that correspond to different groups of parameters for each device. When working with control windows, you begin by selecting the tab to display the parameters for a particular group (see Control window parameters, on page 19).

Note: If you try to display the control window for a device and you get the message Control window `Not Available`, this means that this device type has not been implemented as a controllable device by iControl. Therefore, you can only see the status of this device but cannot configure any control parameters.

When one or more Control windows are open, the **View** menu item **Close All** Control windows becomes available, and the menu lists the device names of open control windows for selection.

Each device in the system is controlled via a control window. The control window is an operational window for the selected device, which you display to control the device. Parameters vary according to the type of device, although the Info parameters are common to all devices.

To access the control window for a device, double-click the device in the **iC Navigator** display, or right click and select **Show Control window** from the pop-up menu.

Control window parameters

Control windows are specific to the device type. Following are examples of control window selector tabs and their associated parameters:

Selector tab	Sample parameters
Config	Audio destination, Audio source, Audio Delay, No signal delay, Signal standards detection, No signal delay, Scan, VBI, Video.
Info	Comments, Device Type, Label, Long ID, Manufacturer, Remote system administration, Service Version, Short Label, Source ID, Vendor.
Video	Player, Thumbnail streaming, Streaming priority control, Waveform monitor and vector scope.
Timing	Horizontal fine, Horizontal position, Horizontal Timing, Vertical Timing, Fine Timing Adjustments
Meta	Aspect ratio, Copy control information, Source.

With some devices, the control window includes the button Load Factory which resets the parameters on the window group to their original factory values.

Info Control Panels

Info control panels display parameters for individual devices, and is available for all device types. The *Info control panel* includes device identification information such as the label, short label, type, comments, source ID, config status, frame, and slot. You can display the Info control panel from the device control window, or you can right-click the device in **iC Navigator** and select **Show info control panel**.

From the info control panel, you can change the name of the selected device, as well as, type comments. By default, the device name takes the type identification; however, you will find it helpful to rename devices using user-specific names. Once you change the device name in the control window, the name of the item is also changed in the iC Navigator display, making it easier to locate.

From the info control panel, you can also register the service to a remote Application Server using Remote system administration.

Densité

Grass Valley's Densité-series products are rack-mountable frames that house a variety of compact cards used for infrastructure interfacing and distribution. Operators can see the signals they are controlling using advanced *visual monitoring over IP* features integrated in the processing modules. Feedback in the form of integrated streaming thumbnails and

waveform/vectorscopes provides much easier and highly cost effective control and monitoring of signals.

Remote control options for the Densité series include a traditional remote control panel (RCP-100, RCP-200), and a stand-alone PC-based control application called *iControl Solo*. More advanced control over IP is provided by **iC Web**.

The full range of video and audio signal parameters and alarms provided by Densité probes can be extracted and displayed using alarm panels in iC Web. With iControl's advanced alarm management, operators can choose to display specific device alarms. Alternatively, users can build their own alarms by choosing from an endless combination of signal and device conditions and external triggers. Users can choose to be alerted only on specific criteria.

Imaging Series (Symphonie & Quartet)

Grass Valley's Imaging-series products are rack-mountable frames that house a variety of full-size cards used for a wide range of interfacing and distribution functions. Two frames are available: the Symphonie, which can accommodate up to 16 cards, and the Quartet, which holds four cards.

Notable among the many Imaging cards available is the XVP family, which offers advanced processing and noise reduction for incoming SD and HD feeds. A single XVP card offers up, down, and cross conversion plus frame synchronization and 16 channel audio processing.

The Imaging Series combines rich processing functionality with high image quality, along with several remote control options.

Kaleido

Grass Valley's Kaleido product line provides multi-image processing and router functionality in a single, expandable chassis. Fully integrated with iControl, they are ideal for advanced monitoring applications, such as multi-channel playout centers.

- The Kaleido-X (7RU) is a multi-room, multi-image processor and router. Each chassis can display 96 HD, SD or analog inputs any number of times, in any size, across 8 displays of any resolution and orientation. As a router, it offers switching of 96 unprocessed inputs to 48 HD/SD outputs for feeding monitors, test equipment and master control or production switchers.

- The Kaleido-X (4RU) is a multi-room, multi-image processor. Each chassis can display 32 HD, SD or analog inputs any number of times, in any size, across 4 displays of any resolution and orientation.
- The Kaleido-X16 is a 1RU, multi-image display processor. Each chassis can display up to 16 auto-sensing HD, SD, or Analog inputs that can be displayed across two high resolution outputs at multiple sizes.
- The Kaleido-K2 is a 32-input advanced, modular multi-image display processor. Fully integrated with Grass Valley's master control switching and infrastructure monitoring systems, it is designed to simplify HD/SD broadcast monitoring requirements.
- The Kaleido-Alto-HD is a 10-input multi-image display processor. It features auto-sensing HD SDI, SDI, and analog composite video inputs, and a high-quality DVI output with up to 1920 × 1080 or 1600 × 1200 pixels.
- The Kaleido-Quad-HD is a high-quality quad-split multi-image display processor designed for monitoring applications demanding fewer inputs. It features 4 auto-sensing HD SDI, SDI, and analog composite video inputs, and a high-quality DVI output with up to 1920 × 1080 or 1600 × 1200 pixels.
- The Kaleido-Quad-Dual combines two independent, high-quality quad-split multi-image display processors in a single 1RU frame for optimal space efficiency. The processor has 2 x 4 auto-sensing HD-SDI/SDI/ Analog Composite video inputs, and 2 high-quality DVI outputs with up to 1920 × 1080 or 1600 × 1200 pixels.

Imagestore

Grass Valley's Imagestore devices deliver high performance, HD/SD master control switching with HD/SD branding graphics capabilities, along with 5.1 audio mixing and storage. They offer video and multi-channel audio mixing plus audio playout. High impact channel branding and promotional graphics can be inserted by multiple independent keying layers. Each Imagestore processor features independent HD/SD preview, clean-feed and auxiliary outputs. The Imagestore series supports serial or Ethernet automation via a single interface. Integration with iControl is achieved using the widely supported Oxtel protocol.

Allégro

Grass Valley's Allégro is a 1 RU streaming encoder/server that allows real-time confidence monitoring of remote signals. It combines encoder and server functions to enable low latency streaming of video, audio and data over a standard IP network. Fully adapted to the monitoring of critical broadcast signals, it integrates telemetry such as signal presence, VBI extraction and audio level metering.

Multiple Allégro encoders can be managed remotely from a central location. Up to 16 local and remote player clients can monitor the same signal. Streaming video for Allégro can be fully integrated into **iC Web**, **iC Router** or Kaleido series products to optimize operator effectiveness. With Allégro's practical Quick Start menu and Web-based graphical user interface, only a few clicks are required to get the unit ready for operation.

What's New in Version 7.30

Building on the success of previous versions, iControl version 7.30 is an important new release of Grass Valley's system for monitoring and control over IP. The main features and enhancements introduced in iControl version 7.30 are listed below. Refer to the Release Notes for more information.

- **iControl hardware:** iControl version 7.30 introduces support for the Dell PowerEdge R330 server in the role of Application Server.
- **Access control:** Support for the Active Directory single sign-on (SSO) infrastructure. See Enabling Active Directory Single Sign-on on page 317.

  Note: As of iControl version 7.30, if you wish to import user profiles from a CSV file, the passwords must be MD5-hashed.

- **Densité card comparison:** In iControl Navigator, **Device Profile Manager** now allows comparison of two or more cards, of the same type and firmware version, and identifies differences in configured parameters, between the selected cards. You can export the comparison results to a CSV file. See Comparing Configured Parameters Between Selected Devices on page 271.
- **Densité card configuration change logs:** Ability to enable logging of card configuration changes. Contact Grass Valley Technical Support for more information (see Contact Us, on page 739).
- **SNMP Manager:** Ability to publish a new SNMP driver to GSMs from the **SNMP Manager** window. See iControl as an SNMP Manager on page 451.
- **Router control:** NVISION router protocol names have been updated.

New protocol name	Old protocol name
NVEP Router (NP0016)	NVISION Ethernet Protocol - Compact Router
NVEP NV9000 - Device Takes (NP0017)	NVISION Ethernet Protocol - Enterprise Router (Device ID based)
NVEP NV9000 - Port Takes (NP0017)	NVISION Ethernet Protocol - Enterprise Router (Physical)
NVEP NV9000 - Deprecated (NP0017)	NVISION Ethernet Protocol - Enterprise Router (Logical)

- **Router control:** A system property file is available to prevent an iControl user from unlocking destinations that were previously locked from an NVISION control panel that uses the NVEP NV9000 – Device Takes (NP0017) protocol. In `java_router.properties`, you can set the release policy, as well as a user name. Refer to the *iControl Router User Guide,* for details.
- **Densité/GeckoFlex remote control:** Support for remote control of GeckoFlex, Densité and GV Node cards by external management systems via a RESTful API. Refer to the *Densité/GeckoFlex RESTful API Reference Guide* (available from the Documentation Library section of Grass Valley's website), for more information.

- **GSM remote control:** Support for accessing alarms managed by iControl's General Status Manager, via a RESTful API. Contact Grass Valley Technical Support for more information (see Contact Us, on page 739).

2 Getting Started with iControl

Summary

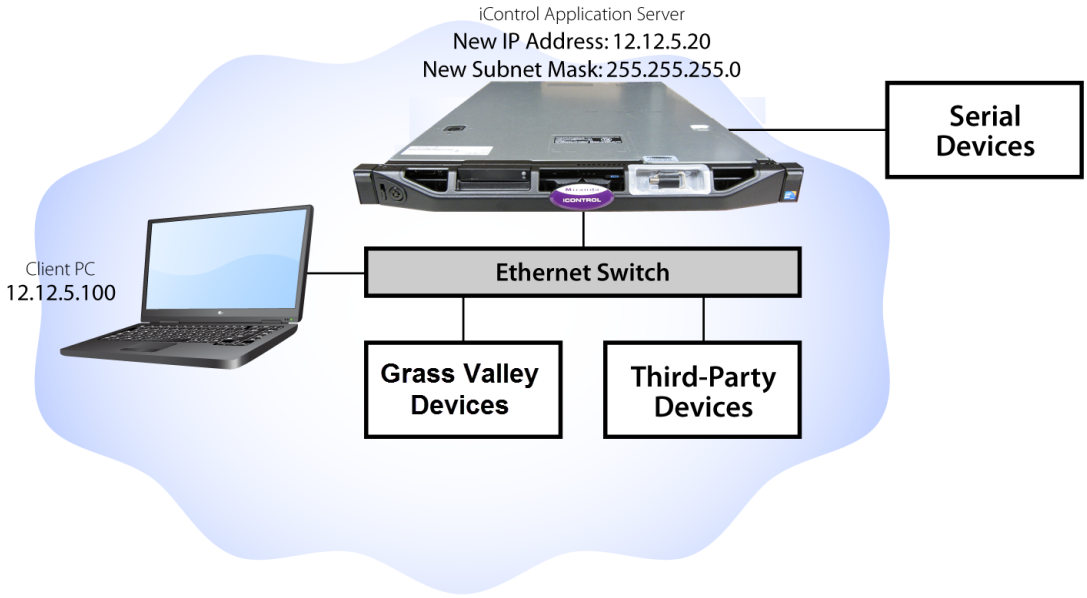
Overview

The iControl Application Server is shipped in a default configuration, with its **eth0** port turned on. In order for it to be able to join a network, it must have its network settings modified. For example, the default IP address and subnet mask must be changed to values that will work on your network.

> **IMPORTANT: Ethernet Port Label Considerations**
>
> Please read the section regarding Ethernet port labels (see Ethernet Port Labels on Dell PowerEdge Application Servers, on page 48).

This is done by connecting a client PC directly to the Application Server, using a crossover Ethernet cable. You will be able to connect to the Application Server from the client PC using a standard Web browser. A series of Web pages will permit you to make the necessary changes.

Once the network settings are configured, you will be able to connect the Application Server to the LAN containing the devices to be monitored and controlled.



You can access an iControl Application Server from a Windows workstation by using a Web browser, such as Microsoft Internet Explorer or Mozilla Firefox. Some tasks can be accomplished on the Application Server via a Web interface. For other functionality, you can download iControl client applications directly from the Application Server.

We recommend that you install the iControl Application Server on a dedicated LAN along with the equipment it is intended to monitor, using the existing security infrastructure. A qualified system administrator should verify that the setup follows your organization's security standards.

Release Notes

The Release Notes contain important information on iControl system requirements, the latest features, performance tips, and known issues. The Release Notes can be downloaded from your iControl system's *Startup* page (see Starting iControl, on page 677). The Release Notes for the latest versions of iControl (and for a number of earlier versions) are available from the *Documentation Library* section of Grass Valley's website (see Contact Us, on page 739).

Upgrading iControl

Instructions for performing an upgrade of an existing iControl system are provided in the Release Notes for the iControl version you wish to use. The iControl Release Notes are available from the *Documentation Library* section of Grass Valley's website (see Contact Us, on page 739).

Recommendations for System Optimization

Here are some guidelines for optimizing performance and balancing the load on an iControl system:

- Where a large number of devices are being monitored, consider setting up multiple GSMs (one per Application Server).
- Allocate a maximum of 150 streams per Densité Manager. A typical Densité frame containing 10 DEC cards and 10 UAP cards creates 30 streams, whereas a Densité frame with SCP cards generates 22 streams.
- Assign a maximum of five Densité frames to a Densité Manager.

Redundancy Planning

While iControl Application Server failures are not common, it is prudent to plan for such an eventuality. Fortunately, recovery from a hardware failure can be ensured by the use of one or more standby Application Server(s). A standby server takes over all the system monitoring and control processes that were running on a main Application Server prior to a failure.

Additionally, unexpected power disruptions, such as might occur during a power failure, can damage the file system on an iControl Application Server. It is strongly recommended that all Application Servers be connected to a standby power source, such as a UPS (Uninterruptible Power Supply), as a preventive measure.

Before putting your Application Server into operation, you should consider implementing a redundancy plan. A redundancy plan defines the use of standby Application Servers in case of hardware failure. This ensures that all the processes that run on the main server(s) will continue to operate uninterrupted.

Redundancy (or recovery) planning is best done at the same time as the system set-up. Full redundancy requires one standby server for each running Application Server. More typically, an iControl system includes one standby server for every five primary Application Servers, since it is unlikely that more than one will fail at the same time.

IMPORTANT: If you require assistance with your recovery planning, please contact Grass Valley Technical Support (see Contact Us, on page 739).

See also

For more information, see:

- Application Server Auto-failovers and Manual Takeovers on page 573.
- Configuring and Managing Application Server Redundancy on page 584.

Key Concepts

Lookup Services

iControl—and Grass Valley products in general—use a lookup service to get information on remote programs or machines, and use that information to establish communications. In this way, cards, frames and other devices can make their presence known on an iControl network, and thus can participate in monitoring and control operations.

By default, each Application Server runs a lookup service that registers and makes available information about the devices on its network. It will also register with all lookup services that are running on other Application Servers on the same LAN.

> **Note:** Displaying more than 10,000 messages in the Log Viewer may require system adjustments to maintain acceptable performance levels.

When client PCs are on different subnets, or when multiple Applications Servers are involved, the locations of lookup servers must be properly specified in order for operators to be able to (a) access iControl monitoring Web pages using **iC Web**, and (b) use **iC Navigator** to view iControl alarms and control panels.

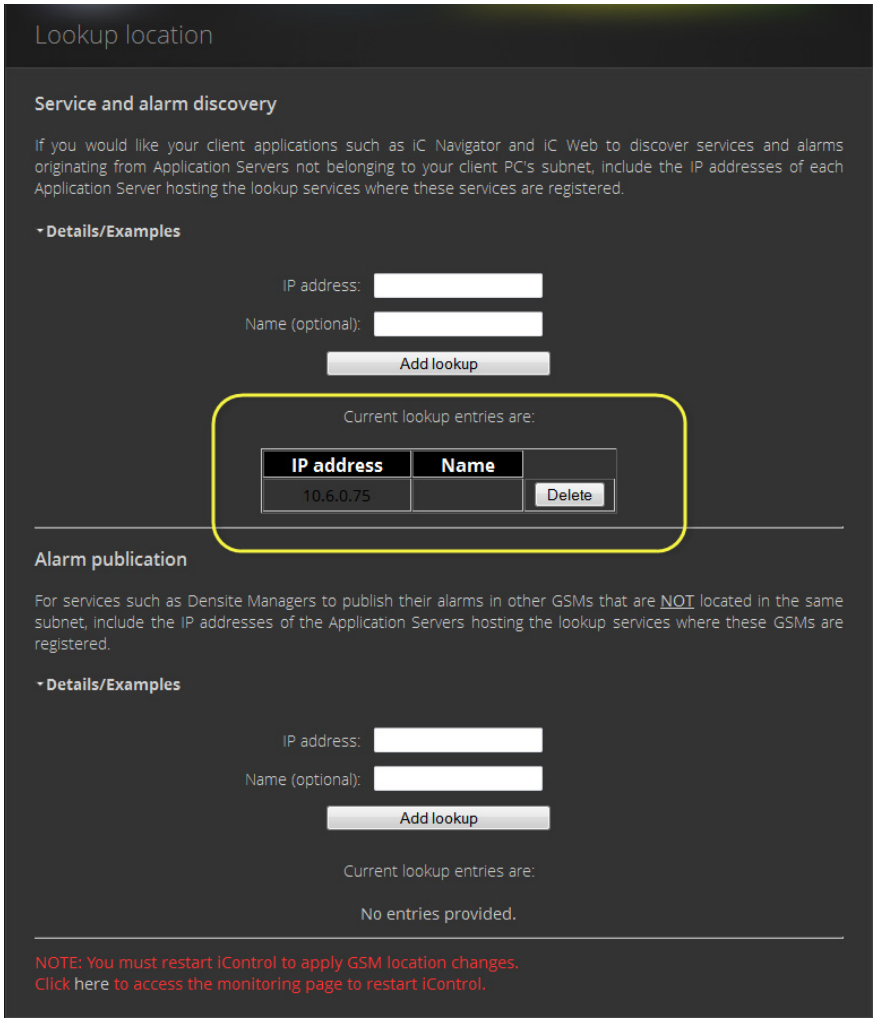
On the iControl Lookup locations page, there are two areas representing two distinct lookup tables.

Service and Alarm Discovery Lookup Table

As a default, an Application Server's client applications, such as **iC Navigator** and **iC Web**, discover services and alarms originating from Application Servers on the local subnet. Leaving the **Service and alarm discovery** table empty results precisely in this behavior with no need for further configuration.

> **IMPORTANT: System behavior**
>
> If the **Service and alarm discovery** table of Application Servers is empty, client applications on the local Application Server can see services and alarms coming from the local GSM and all active GSMs on Application Servers within the subnet.

If, however, you would like an Application Server's client applications to see services and alarms from Application Servers **OUTSIDE** the local subnet, you must include the IP addresses of these external servers in the **Service and alarm discovery** table.



Populated Service and alarm discovery table (circled)

IMPORTANT: System behavior

If there are Application Servers listed in your **Service and alarm discovery** table and you would like for client applications to see services and alarms hosted by the local Application Server as well, you must include the IP address of the local Application Server in this list.

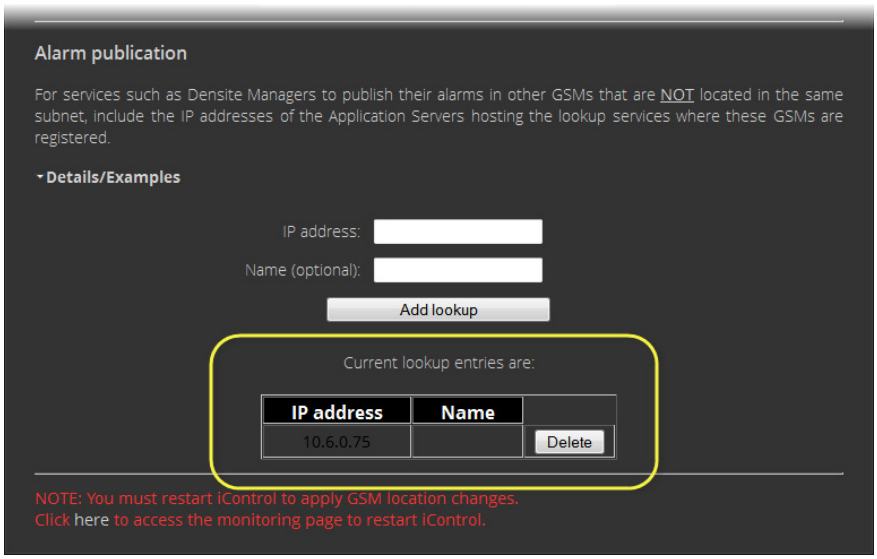
See also

For more information, see Examples: Service and Alarm Discovery Scenarios on page 30.

Alarm Publication Lookup Table

Services, such as Densité Manager, automatically publish their alarms on GSMs within the same subnet as the Application Server hosting the service. However, if you would like alarms to be visible to a GSM outside the local subnet, you must specify the IP address of the external

Application Server (the server hosting the lookup service where the target GSM is registered) in the **Alarm publication** table of the iControl Lookup locations page.



Populated Alarm publication table (circled)

IMPORTANT: System behavior

If the **Alarm publication** table of Application Servers is empty, the Densité Manager on the local Application Server publishes its alarms exclusively on the local GSM and active GSMs on Application Servers within the subnet.

If the **Alarm publication** table is populated with the IP address of a non-local Application Server, and you would like the local GSM to see alarms originating from the local Densité Manager, you must also include the IP address of the local Application Server.

See also

For more information, see:

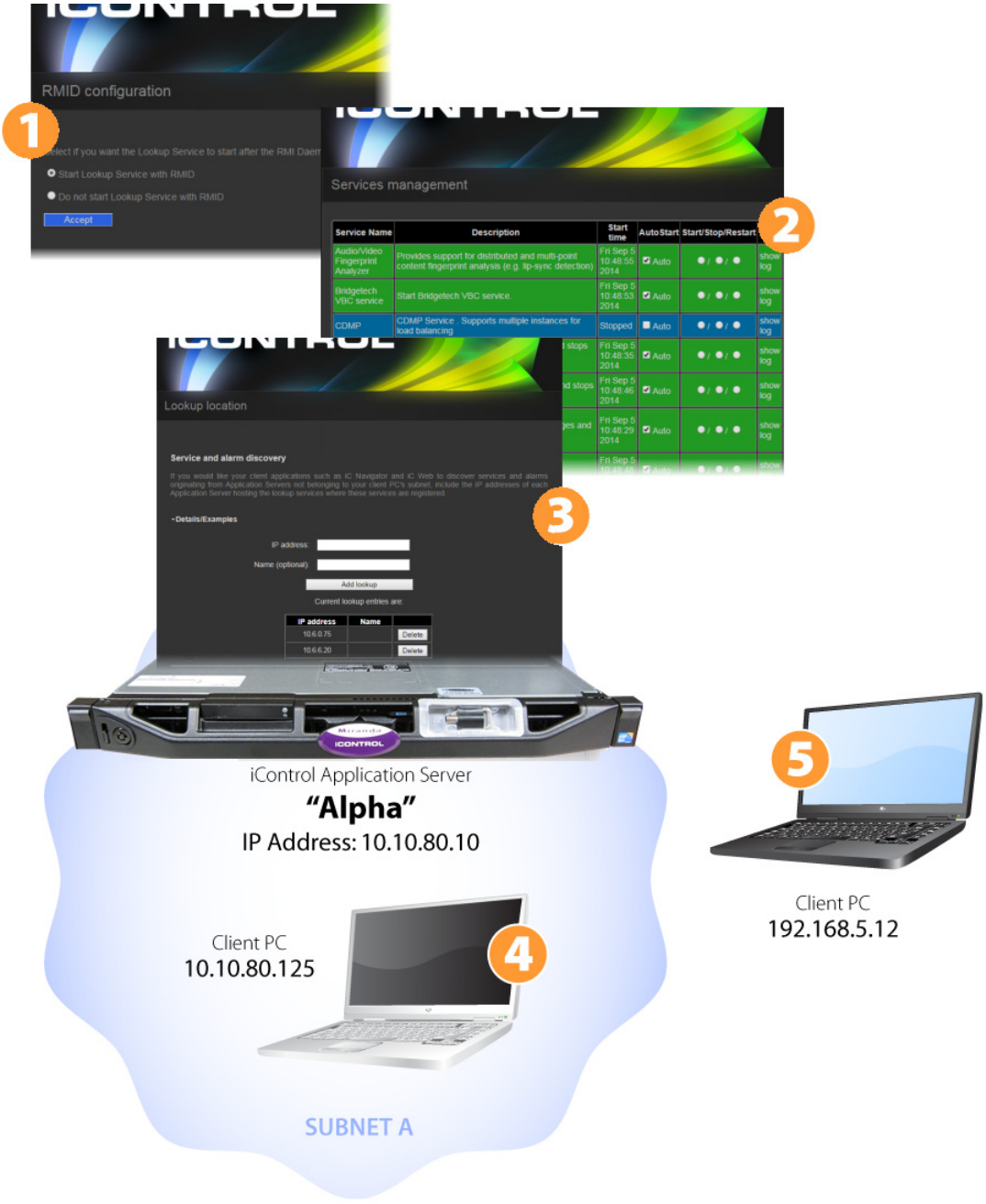
- Examples: Alarm Publication Lookup Scenarios on page 36.
- About the Alarm Publication Lookup Table on page 41.

Examples: Service and Alarm Discovery Scenarios

The way in which lookup services are configured varies from one installation to another. The examples on the following pages demonstrate the basic concepts, and can serve as a guide as you set up your own iControl network.

Example 1 — Single Application Server

In a typical, basic iControl configuration, only one Application Server is needed to handle all of the iControl functions. Any TCP/IP devices associated with the Application Server are on the same subnet.



1. Since Alpha is the only Application Server on Subnet A, its Lookup Service should be **ON**.
2. The GSM is active on Alpha.
3. Since Alpha is the only Application Server on Subnet A, it is not necessary to type anything in the **Service and alarm discovery** area.

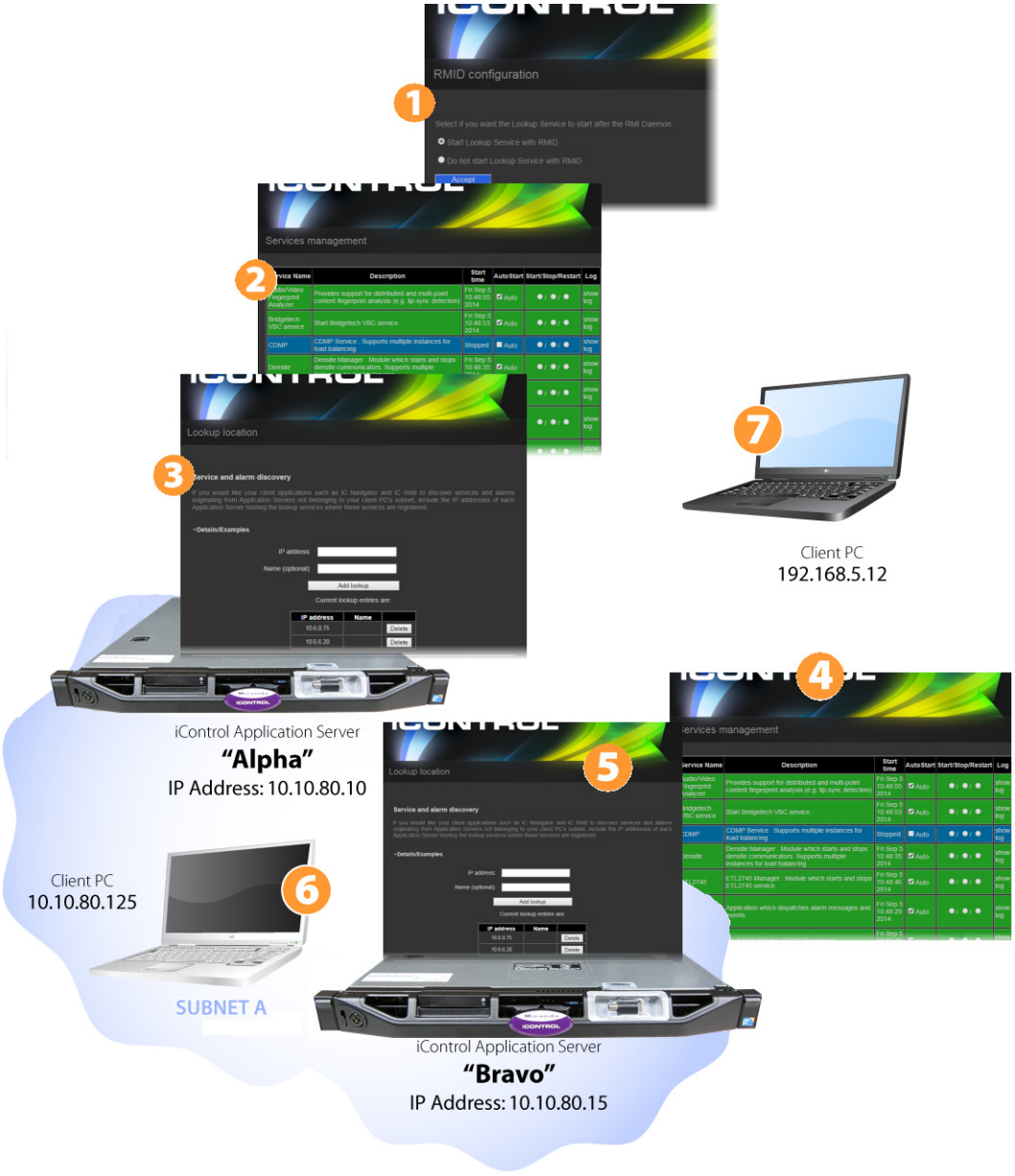
IMPORTANT: System behavior

If the **Service and alarm discovery** table of Application Servers is empty, client applications on the local Application Server can see services and alarms coming from the local GSM and all active GSMs on Application Servers within the subnet.

4. When **iC Navigator** (or any client application) is downloaded from Alpha by this PC, the application will perform a multicast discovery within Subnet A, find the Alpha Lookup Service, and then be able to see all devices and services registered on Alpha.
5. If this PC has access to Subnet A (e.g., via VPN), it can access Alpha's *Startup* page from a Web browser, and download **iC Navigator** (or any client applet). The application *knows* about the Lookup Service on Alpha, and so the client PC will be able to see all devices and services registered on Alpha.

Example 2 — Two Application Servers, Same Subnet

As an iControl configuration grows, additional Application Servers can be added to handle the increased workload. Any TCP/IP devices associated with either Application Server should be on the same subnet.



1. For the purpose of this example, Alpha is the only Application Server running the Lookup Service. Under actual conditions, you should have two Application Servers (per subnet) running the lookup service to provide redundancy.
2. The GSM is active on Alpha.
3. It is not necessary to type anything in Alpha's **Service and alarm discovery** area. The discovery process will automatically result in all devices and services on Subnet A registering with Alpha's Lookup Service.

IMPORTANT: System behavior

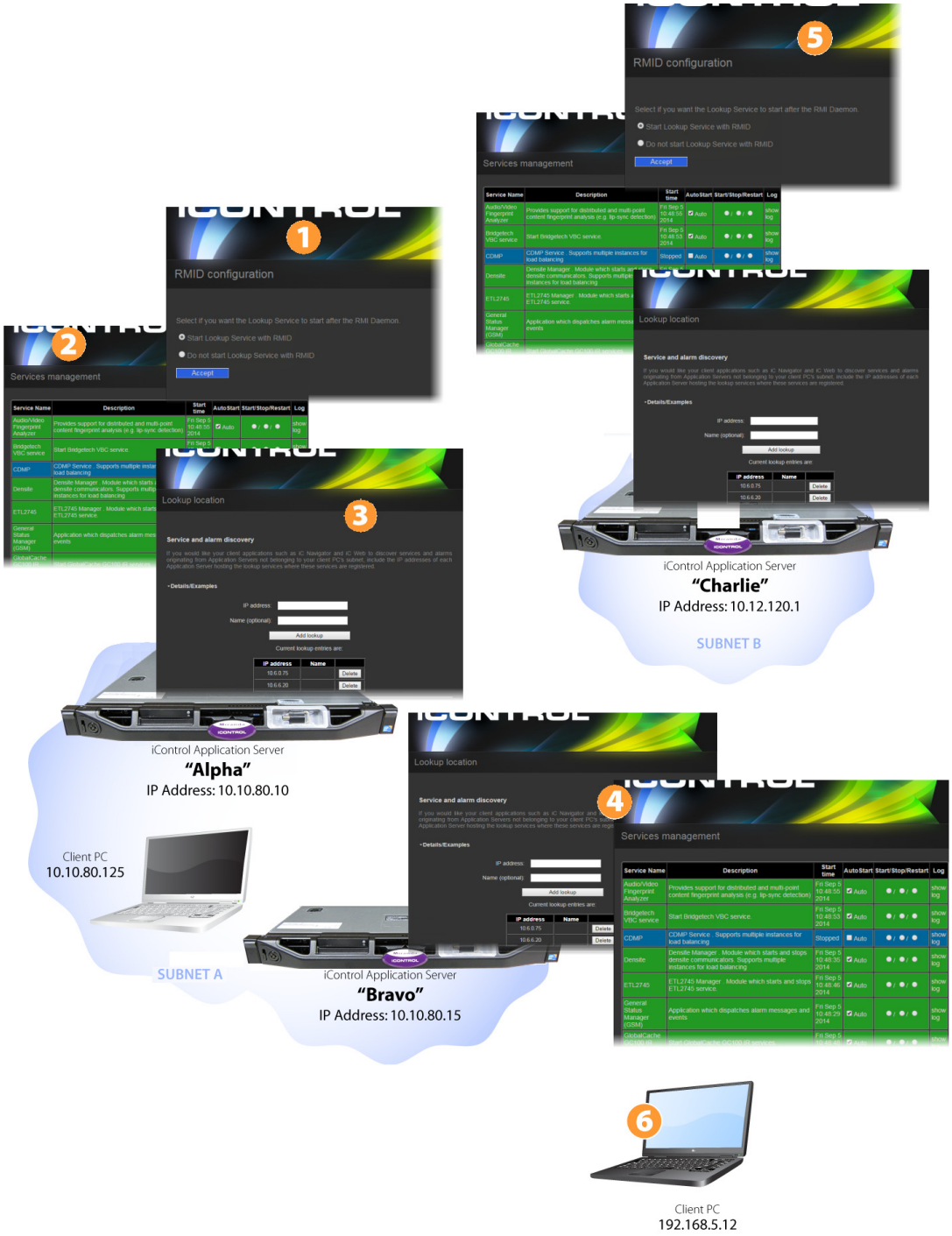
If the **Service and alarm discovery** table of Application Servers is empty, client applications on the local Application Server can see services and alarms coming from the local GSM and all active GSMs on Application Servers within the subnet.

4. In order to share the monitoring workload, the GSM is active on Bravo.
5. As mentioned above, the discovery process will result in all devices and services on Subnet A automatically registering with Alpha's Lookup Service. So it would not ordinarily be necessary to type anything in Bravo's **Service and alarm discovery** area. This is not true, however, when Bravo is accessed by a client PC from another subnet (see below).
6. When **iC Navigator** (or any client application) is downloaded from Alpha by this PC, the application will perform a multicast discovery (see Multicast vs. Unicast, on page 38) within Subnet A, find the enabled Alpha Lookup Service, and then be able to see all devices and services registered on both Alpha and Bravo.
7. If this PC has access to Subnet A (e.g., via VPN), it can access Alpha's *Startup* page from a Web browser, and download **iC Navigator** (or any client applet). The application *knows* about the enabled Lookup Service on Alpha, and so the client PC will be able to see all devices and services registered on both Alpha and Bravo.

   If, however, the PC's Web browser is pointed to Bravo's *Startup* page, and downloads a client application, the applet will not automatically detect the lookup service on Alpha, and so none of Bravo's services or devices will be visible on the client PC. In order to enable direct access, type Alpha's IP address in Bravo's **Service and alarm discovery** area—the application will be able to find the lookup service, and therefore *see* everything on Subnet A.

Example 3 — Multiple Application Servers on Different Subnets

It is common in larger iControl configurations to have multiple Application Servers on different subnets. Lookup services allow Application Servers from one subnet to share information with Application Servers on another subnet.



1. For the purpose of this example, Alpha is the only Application Server running the Lookup Service on Subnet A. Under actual conditions, you should have two Application Servers (per subnet) running the lookup service in order to provide redundancy.
2. A GSM is active on Alpha.

3. The discovery process will result in all devices and services on Subnet A automatically registering with Alpha's Lookup Service. If a client PC opens **iC Navigator** from Alpha, all Subnet A devices and services will be visible in **iC Navigator**.
4. As mentioned above, as a result of the discovery process, all devices and services on Subnet A will automatically register with Alpha's Lookup Service. So it would not ordinarily be necessary to type anything in Bravo's **Service and alarm discovery** area. However, if a client PC opens **iC Navigator** (or any client application) from Bravo, it will not see anything unless there is an IP address (either Alpha's or Charlie's) entered in Bravo's **Service and alarm discovery** area.

   IMPORTANT: System behavior

   If the **Service and alarm discovery** table of Application Servers is empty, client applications on the local Application Server can see services and alarms coming from the local GSM and all active GSMs on Application Servers within the subnet.

5. The discovery process will result in all devices and services on Subnet B automatically registering with Charlie's Lookup Service. If a client PC opens **iC Navigator** from Charlie, all Subnet B devices and services will be visible.
6. If this client PC has access to Subnet A (e.g., via VPN), it can access Alpha's *Startup* page from a Web browser, and download **iC Navigator** (or any client application). The application knows about the Lookup Service on Alpha, and so the client PC will be able to see all devices and services registered on both Alpha and Bravo. Similarly, downloading an application from Charlie would make all of the devices and services on Subnet B visible.

   However, in order for that same client PC to be able to see services and devices from both Subnet A and Subnet B, the IP addresses of both *Alpha* and *Charlie*, must be typed in each other's **Service and alarm discovery** areas.

   Note: The order in which the IP addresses are typed is not important.

Examples: Alarm Publication Lookup Scenarios

Example 1 — Publishing Densité Alarms to all GSMs within the Local Subnet

If you want your local Application Server's Densité alarms to be visible only to the GSMs within the local subnet, you can leave the **Alarm publication** table of the local Application Server unpopulated except for the local Application Server's own IP address.

1. Alpha's Lookup Service should be **ON**.
2. The GSM is active on Alpha.
3. Since, in this example, we only want Alpha's Densité alarms to be visible within the subnet, it is not necessary to type anything in the **Alarm publication** table.

Example 2 — Publishing Densité Alarms outside the Local Subnet

If you want your local Application Server's Densité alarms to be visible to the GSM on an Application Server outside the local subnet, you need to include the IP address of the external (to the local subnet) server in the **Alarm publication** table of the local Application Server.

1. Alpha's Lookup Service should be **ON**.
2. The GSM is active on Alpha, Bravo, and Charlie.
3. Since, in this example, you do not want Charlie to publish its Densité alarms outside its own subnet, there is no need to populate its (Charlie's) **Alarm publication** table.
4. Since, in this example, you do want Bravo to publish its Densité alarms to Alpha but not to Charlie, there is no need to populate its (Bravo's) **Alarm publication** table.

> **Note:** Since Bravo is already in the subnet of Alpha, Bravo's Densité alarms will be visible to Alpha's GSM.

5. Charlie's Lookup Service should be **ON**.

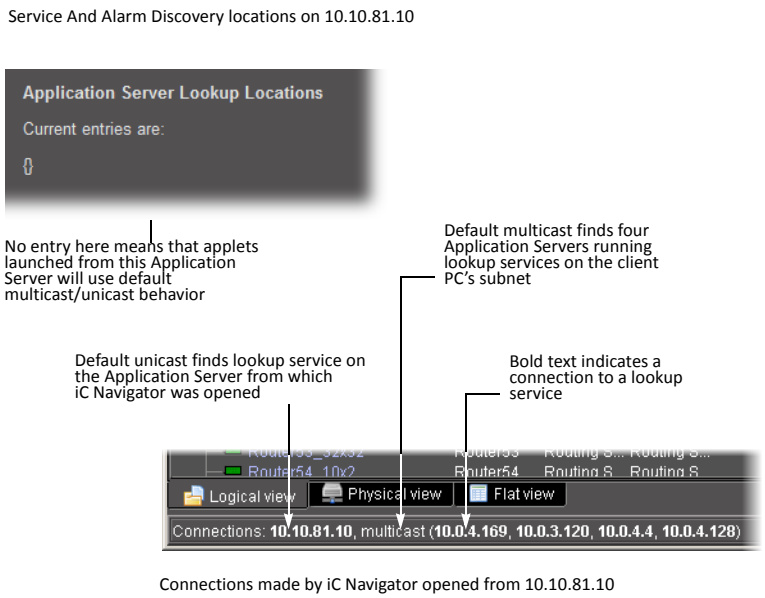
Multicast vs. Unicast

When a client application (e.g., **iC Navigator**) is opened, one of the first things it does is to search for a lookup service that has a registry of devices and services available for monitoring and/or control. There are two ways it can perform this search: *multicast* and *unicast*.

A *multicast* search is a general broadcast on a TCP/IP subnet—the applet is basically saying, *Are there any lookup servers out there?* Lookup servers on the same subnet will reply to the multicast, making their registries available to the applet.

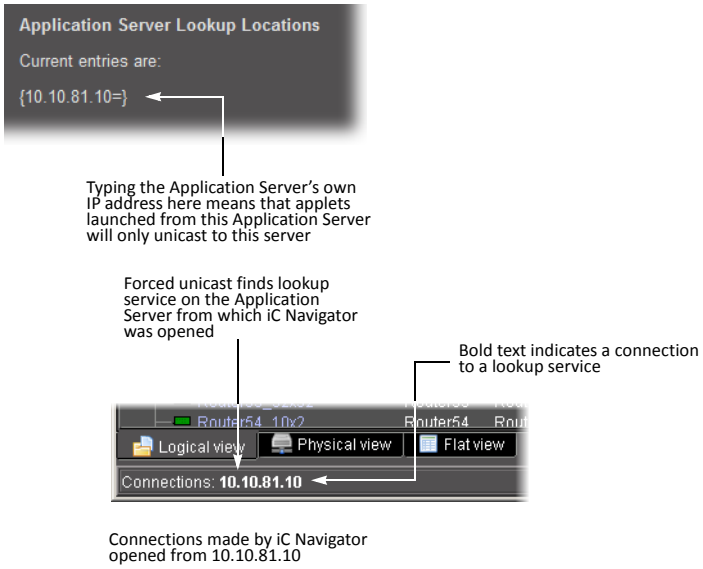
A *unicast* search is a request directed to a specific IP address. In this case, the applet is saying, *Attention server X, are you running a lookup service?* If the answer is *yes*, the server will make its registry available to the applet.

By default, an iControl applet starts by performing a multicast search on its own subnet (i.e., the subnet to which the client PC is connected), followed by a unicast search on the Application Server from which it is launched. This behavior can be modified by editing the lookup locations list on the Application Server.



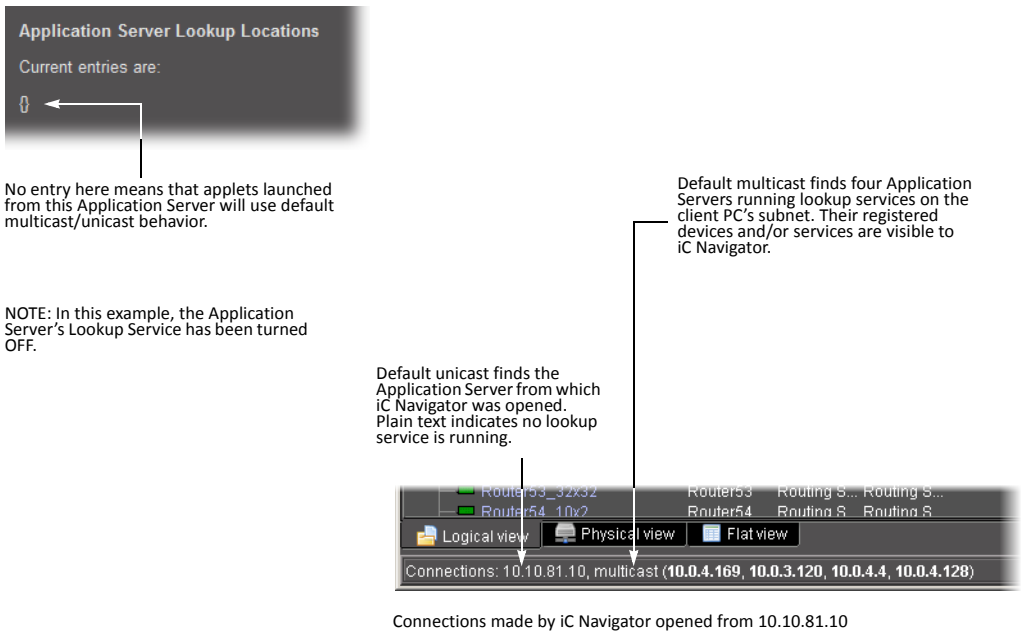
Example — Default Multicast/Unicast

Service And Alarm Discovery locations on 10.10.81.10

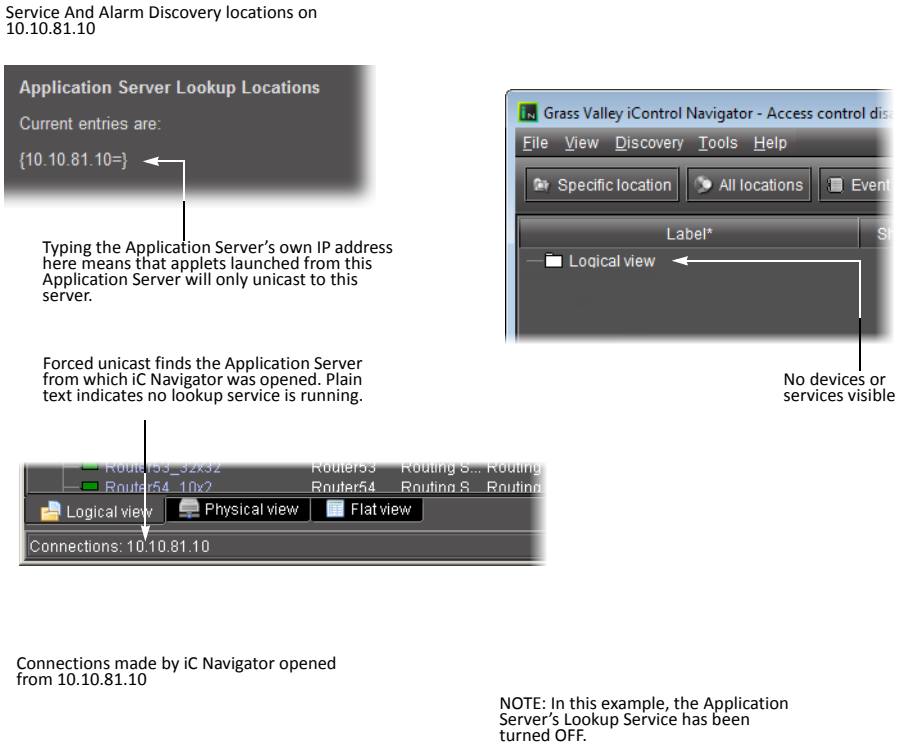


Example — Forced Unicast

Service and alarm discovery locations on 10.10.81.10



Example — Default Multicast/Unicast with Lookup Service OFF



Example — Forced Unicast with Lookup Service OFF

About the Alarm Publication Lookup Table

> **Note:** The current version of iControl has a built-in feature called *multi-GSM* that eliminates the need for specifying alarm publication lookup locations. The description and procedures below are being kept in this User Guide in support of legacy iControl installations. Please consult with *Grass Valley Technical Support* before making any modifications to your **Alarm publication** lookup table (see Contact Us, on page 739).

In a basic iControl configuration, services such as the Densité Manager or the Imagestore Manager will automatically detect—and begin publishing alarm status information to—the GSM(s) on their own subnet.

If, however, you wish to have these services connect to GSMs running on Application Servers on other subnets, you must explicitly specify the GSM locations. You do this by typing the IP address of the target Application Server (on the remote subnet) in the **Alarm publication** lookup table of the Application Server running the Densité, Imagestore, or other service on the local subnet.

If the remote GSM is registered in a lookup service on another Application Server in its subnet, you can use the IP address of that server instead.

For example, let's say you want a Densité frame to publish its alarms and status information to GSMs on two different subnets. The table below describes a possible configuration:

Device	Services	Subnet	IP Address
Densité Frame	--	10.10.03	10.10.03.99
Application Server 1 (AS1)	Densité Manager	10.10.03	10.10.03.11
Application Server 2 (AS2)	Lookup Service, GSM	10.10.03	10.10.03.22
Application Server 3 (AS3)	Lookup Service	10.10.04	10.10.04.33
Application Server 4 (AS4)	GSM	10.10.04	10.10.04.44

When Application Server 1 (AS1) starts up, its Densité Manager service will discover the enabled **Alarm publication** lookup table on AS2 automatically, and begin publishing to the GSM on AS2, because they are on the same subnet. In order to have the Densité Manager publish to the GSM on AS4, you must include one of the following in the **Alarm publication** lookup table of AS1:

- the IP address of AS4, in which case the Densité Manager will publish to GSMs on AS2 and AS4
- the IP address of AS3, in which case the Densité Manager will publish to the GSM on AS2 and any other GSM on subnet `10.10.04` that is registered in the lookup service on AS3

GPI-1501 I/O Module (Densité Card)

The GPI-1501 is a 2RU Densité card that provides 20 dedicated GPI (General Purpose Interface) inputs plus eight terminals that can be individually configured as either a GPI input or GPI output. When paired with an iControl Application Server, the GPI-1501 provides alarm aggregation from older devices that do not offer Ethernet port connectivity. The Application Server can report alarm status information to operators via iControl or SNMP. It can also trigger external events, such as selecting an alternate source.

In iControl, you can configure GPI outputs to respond to alarms triggered on another card on the network.

See also

For more information about:

- the GPI-1501 I/O module, see the *GPI-1501 General Purpose Interface I/O Module Guide to Installation and Operation*.
- Configuring GPI outputs to respond to alarms triggered on another card on the iControl network, see page 58.

Getting Started Workflow

Note: You are currently reading the *iControl User Guide*. This manual and all other documents that apply to iControl, iControl Router, and iControl Solo are available from the *Documentation Library* section of Grass Valley's website (see Contact Us, on page 739). Alternatively, you can perform the following workflow to set up iControl, and then gain access to the iControl online help system.

Workflow: Getting Started

1.	Installing the iControl Application Server on page 43
2.	Preparing a PC for Configuring the Application Server on page 45
3.	Configuring the iControl Application Server on page 46
4.	Configuring Client Workstations on page 52
5.	Configuring the Application Server on the Network on page 53
6.	Configuring GPI Outputs on a GPI-1501 on page 58
7.	Connecting & Configuring Devices on page 63
8.	Configuring an Application Server's Date and Time on page 66
9.	[OPTIONAL] Gaining Access to Documentation on page 69

Task 1: Installing the iControl Application Server

Grass Valley's Application Server is the hardware at the heart of the iControl system, providing control, monitoring, logging and interface services. The Application Server is a compact 1 RU server that interfaces to other iControl devices over TCP/IP. A user can connect to the Application Server via TCP/IP from any desktop or portable computer.

Note: Install the faceplate after the server is placed in a rack. If your Application Server is an older Supermicro model, install the faceplate before the server is placed in a rack.

To install the iControl Application Server

1. Place the iControl Application Server in a standard 19-inch rack, using the rails, screws and washers provided. Make sure that the unit has adequate ventilation.
2. Connect power cords, and then turn the server on. The power switch is located on the front panel.
3. **[OPTIONAL]** Install the Grass Valley faceplate onto the front of the Application Server by sliding it onto the guide blocks on the side handles, then pushing it in until it clicks into place.

Notes

- An unexpected power disruption, such as might occur during a power failure, can damage the file system on an iControl Application Server. It is strongly recommended that all Application Servers be connected to a standby power source, such as a UPS (Uninterruptible Power Supply), as a preventive measure.
- Hardware documentation for the Dell PowerEdge R200, R210, R310, R320, and R330 is available from `dell.com/poweredgemanuals`.

Connecting the 8-port Break-Out Box (optional)

You can optionally purchase an 8-port Comtrol RocketPort card (with breakout box) if required.

REQUIREMENT

Before beginning this procedure, make sure you have installed the RocketPort PCI card into the Application Server according to the appropriate hardware manual. Follow the procedure for installing an expansion card. The manuals are available from `dell.com/poweredgemanuals`.

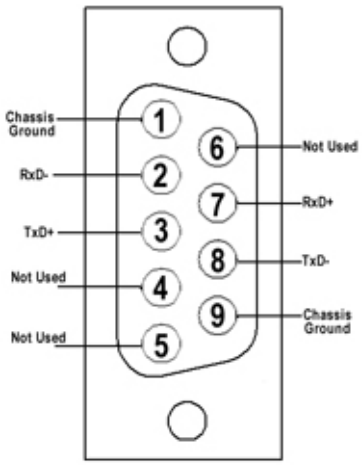
To connect the 8-port breakout box

1. Plug the breakout box connector into the large port (PCI expansion slot) at the back of the Application Server.
2. Connect cables from the devices to be controlled to the serial ports on the breakout box.

Note: It is important to assign serial ports on both the iControl Application Server and any routers that will be participating in the iControl system to avoid conflicts that might negatively affect system performance (see Connecting & Configuring Devices, on page 63).

RS-422 Pinout Assignments

When connecting an iControl Application Server to other serial devices, such as Symphonie or Quartet frames, use a straight-through RS-422 cable. If the need arises to create a custom cable, refer to the pinout assignment diagram below.



RS-422 connector pinout

Task 2: Preparing a PC for Configuring the Application Server

You will use a client PC to configure the new Application Server. The client PC must have network settings that will allow it to communicate with an iControl Application Server in its default state.

To configure TCP/IP settings of a client PC

1. Press the Windows key on your keyboard, type "control panel" and then press Enter.
2. In the search box, type "adapter" and then, under **Network and Sharing Center**, click **View network connections**.
3. In **Network Connections**, right-click the network adapter you wish to configure (e.g., *Local Area Connection,* or *Ethernet*), and then click **Properties**. If the system prompts you for an administrator password or confirmation, type the password or provide confirmation.

   The Properties window for the selected network adapter opens.
4. On the **Networking** tab, under **This connection uses the following items**, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.

   The **Internet Protocol Version 4 (TCP/IPv4) Properties** window appears.
5. Take note of the PC's current settings.
6. On the **General** tab, click **Use the following IP address**.

   The default IP address of a new iControl Application Server is 10.0.3.6.
7. Type an IP address in the same range (e.g., `10.0.3.10`) in the **IP address** box.

   The default subnet mask of each new iControl Application Server is 255.255.0.0.
8. Type `255.255.0.0` in the **Subnet mask** box.
9. Click **OK**.
10. In **Local Area Connection Properties**, click **Close**.

Notes

- The factory-default IP address and subnet mask settings for an Application Server appear on a sticker, on the top cover of the chassis.
- Remember to return the PC to its original network settings once you have finished configuring the Application Server.

Task 3: Configuring the iControl Application Server

Before you can begin operations, you must configure the Application Server and make it available on your local network. Specifically, you will have to:

- Connect to the Application Server from a client PC
- Log in to the Application Server's *iControl admin* page and configure the Application Server's:
  - Ethernet interface
  - Network gateway
  - Domain Name Service settings
  - Host name and IP address
- Apply your changes and perform a readiness check

Connecting to a New iControl Application Server

Before you can begin operations, you must configure the Application Server and make it available on your local network. The iControl Application Server is shipped with its **eth0** port configured to a standard setting. As you perform the configuration procedures in this manual, you will reconfigure the port to integrate the Application Server into your network.

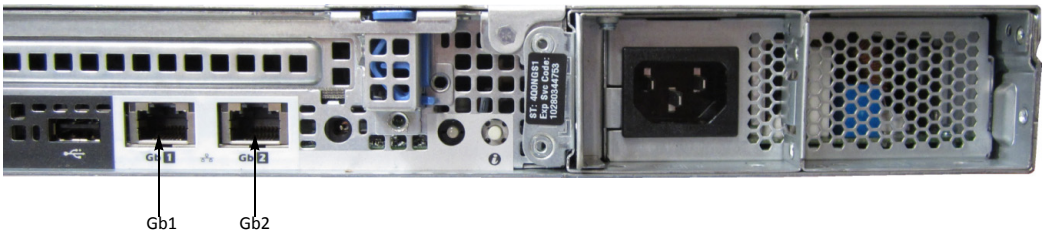
IMPORTANT: Ethernet Port Labels on Dell PowerEdge Application Servers

Please read the section regarding Ethernet port labels (see page 48).

To connect to a new Application Server

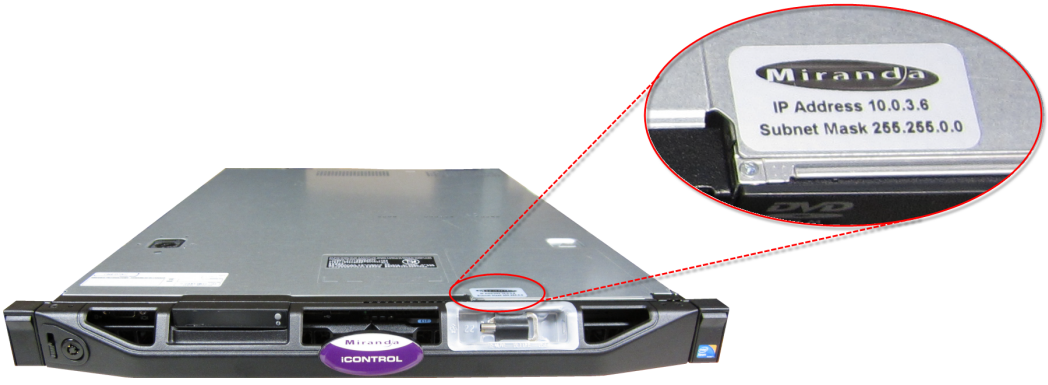
1. Using a crossover Ethernet cable, connect the client PC to the **eth0** port on the new Application Server.

Connection between client PC and Application Server



Rear view of R310 Application Server, showing logical ports eth0 and eth1 (physical ports Gb1 and Gb2, respectively)

Note: The default IP address and subnet mask settings for the Application Server when shipped from the factory are shown on a sticker on the top cover of the chassis above the front-panel power switch. The factory default is `10.0.3.6`.



2. Open a browser window on the client PC.
3. In the address field, type `10.0.3.6` (this is the default IP address of the iControl Application Server).

   The *Startup* page appears.

Note: If your Web browser cannot find the Application Server, make sure the PC's network settings are correct (see Preparing a PC for Configuring the Application Server, on page 45).

Ethernet Port Labels on Dell PowerEdge Application Servers

The physical Ethernet ports on the back of the Dell PowerEdge R200, R210, R310, R320, and R330 are labeled **1** and **2**, or **Gb1** and **Gb2**, depending on the actual model. The physical (cabling) port called **Gb1** (or **1**) corresponds to logical port **eth0**. Likewise, the physical port called **Gb2** (or **2**) corresponds to logical port **eth1**. In all iControl-related documentation, when speaking of cabling and physical ports, we use the logical port names. For example, if a procedure instructs you to connect a cable to **eth0**, you must connect the cable to the Application Server's physical port labeled **Gb1** (or **1**).

Configuring the Network

When configuring your network you must configure host addresses, DNS client, and network interfaces in the proper sequence.

Configuring the network

1.	Open the *Network interfaces* page of your Application Server (see page 688).
2.	Configure network interface settings (see page 49).
3.	Restart the Application Server (see page 50).

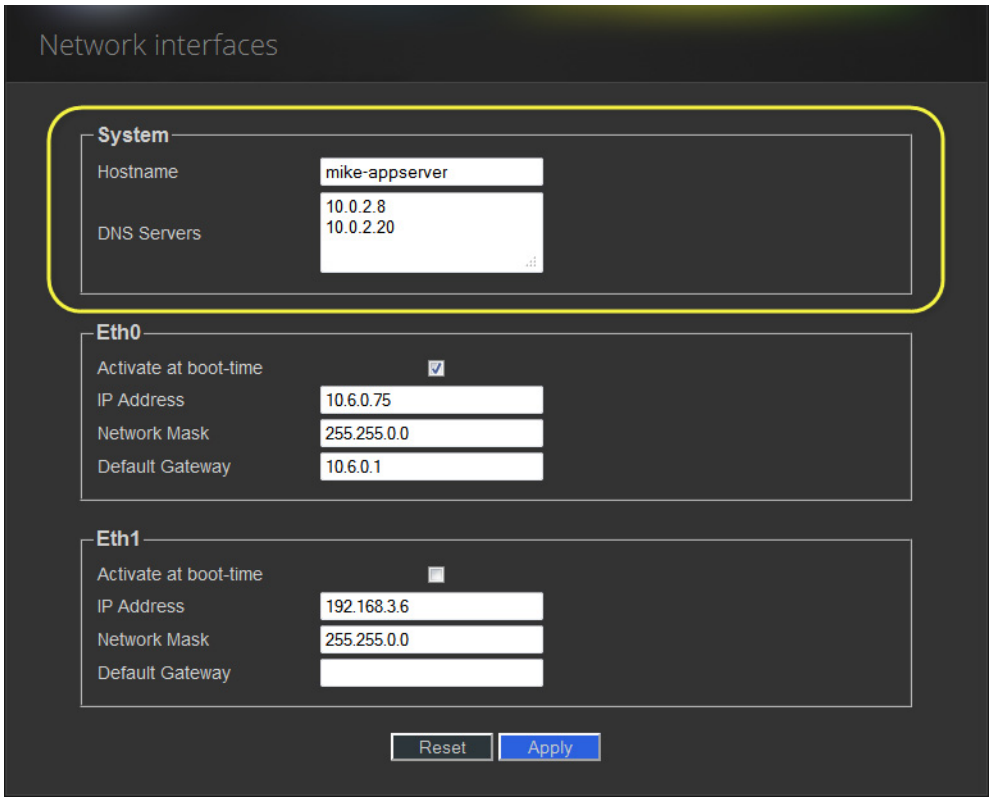
Configuring Network Interface Settings

REQUIREMENT

Before beginning this procedure, make sure you have navigated to the *Network interfaces* page (see page 688).

To configure network interface settings

1. On the *Network interfaces* page, under **System**, perform the following sub-steps:
   a) In the **Hostname** field, type the host name by which you would like this Application Server to be known on your network.
   b) If required, add DNS servers to the list of IP addresses in the **DNS Servers** list.



2. Under **eth0**, configure Ethernet interface settings by performing the following sub-steps:

Notes

- The Application Server is shipped with the **eth0** port turned on, in a default configuration that permits an initial connection. The default IP address setting for the Application Server is `10.0.3.6`, with subnet mask `255.255.0.0`. This sub-procedure describes how to reconfigure **eth0** to meet your local network requirements.
- You must use **eth0** as your main network interface. The other Ethernet port (**eth1**) is also configurable, but is intended for specialized use, such as connecting Grass Valley Densité frames and some third-party devices (e.g., SNMP devices) as long as they are on the same local subnet as **eth1**. The **eth1** network interface is disabled by default.

IMPORTANT: Ethernet Port Labels on Dell PowerEdge Application Servers

Please read the section regarding Ethernet port labels (see page 48).

a) Select the **Activate at boot** option.

If you do not select the **Activate at boot** check box, the **eth0** interface resets to its previous values the next time the system restarts.

b) In the **IP Address** field, type the IP address you would like to use for this iControl Application Server.

Typically the IP addresses for all devices on a LAN will begin with the same two data groups, and the remaining two will be assigned by the system administrator.

c) Type an IP address in the **Network mask** field that corresponds to your desired network configuration.

d) In the **Default Gateway** field, type the desired gateway address.

Ask your system administrator for the IP address of the network gateway that this Application Server will use. If a gateway is *not* being used, then leave the **Default Gateway** field empty.

3. Click **Apply**.
4. Proceed to the procedure Restarting the Application Server on page 50.

Restarting the Application Server

Once you have specified all the settings your Application Server needs to be able to operate on your local network, you must restart the system to apply the new configuration.

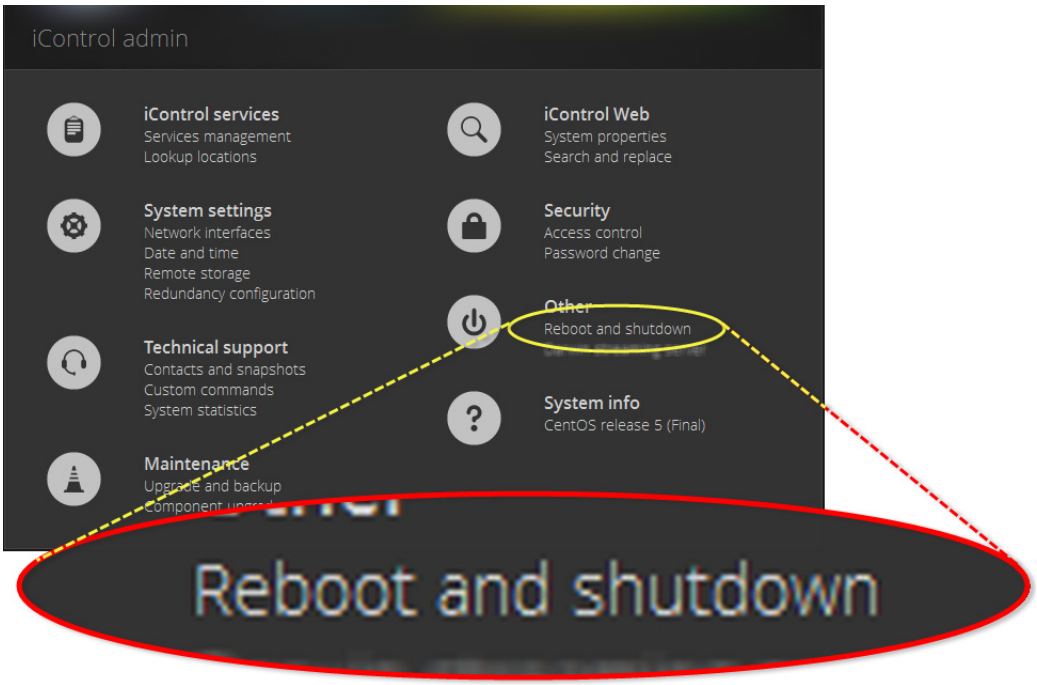
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

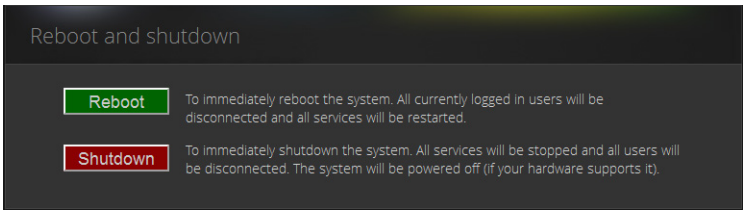
- You have configured your network interface settings (see page 49).
- You have opened the *iControl admin* page (see page 681).

To restart the Application Server

1. On the *iControl admin* page, click **Reboot and shutdown**, under **Other**.



The *Reboot and shutdown* page appears.



2. Click **Reboot**.

IMPORTANT:	**You may lose communication to the Application Server** If your PC is on a different subnet than the Application Server's new address, you will lose communication with the Application Server once you reboot.

The Application Server restarts with the network parameters you have established.

3. Disconnect the client PC that was used to configure the Application Server. Remember to restore the previous network settings on the PC (see Preparing a PC for Configuring the Application Server, on page 45).
4. Connect the Application Server to its designated network. Use a standard Ethernet cable plugged into the Application Server's **eth0** port (see Installing the iControl Application Server, on page 43).

IMPORTANT: Ethernet Port Labels on Dell PowerEdge Application Servers

Please read the section regarding ethernet port labels (see page 48).

Task 4: Configuring Client Workstations

Any Windows 10, Windows 8, or Windows 7 workstation with access to an Application Server can be used to operate iControl, without the need for special client-side software. There is, however, one consideration in preparing them to work with iControl: the workstation's local DNS settings.

Configuring DNS Settings

Application Servers use the Darwin Streaming Server to stream video thumbnails from some network devices to iControl applets running on client PCs. For example, when you open a video card's control panel from **iC Navigator**, the control panel displays a thumbnail representation of the current video signal.

In order for such streaming to work properly, a client PC's internal Domain Name Service (DNS) must be able to resolve the host name (and reverse resolve the IP address) of the Application Server from which the applet was launched.

In order to avoid slower streaming performance, you should make sure that each client PC has all available Application Servers and Allégro-1 systems listed in its DNS configuration file.

To configure DNS settings

1. On the client PC, open the `hosts` file (no extension) in a text editor. In Windows, the `hosts` file is located in `C:\Windows\System32\drivers\etc`.
2. For each Application Server and Allégro-1 that the PC will be accessing, add a line of the form:

   ```
   AAA.BB.CC.DD      HostName.yourDomain.com
   ```

   where `AAA.BBB.CC.DD` is the IP address of the Application Server or Allégro-1.
3. Save and close the `hosts` file.

Connecting to the Application Server

At this point, you should verify that the iControl Application Server is available on your network.

To connect to the Application Server

1. From a workstation on the same subnet, open a Web browser window and type the IP address of the newly-configured iControl Application Server. You should see the *Startup* page.
2. Alternatively, you can use the `ping` command by performing the following sub-steps:
   a) On the **Start** menu of the client PC, point to **All Programs**, and then to **Accessories**, and click **Command Prompt**.
   b) Type the following:

      ```
      ping AAA.BBB.CCC.DDD
      ```

      where `AAA.BBB.CCC.DDD` is the Application Server's new IP address.

A small window should briefly appear with a message similar to the following:

```
Reply from AAA.BBB.CCC.DDD: bytes=32 time<1ms TTL=62
```

Task 5: Configuring the Application Server on the Network

Once the Application Server is plugged into and available on your network, you will need to configure additional settings to permit it to operate in that environment. Specifically, you will need to configure lookup services to make sure that all devices on the network are visible to iControl.

> **Note:** Services in iControl are generally administered via the *Services management* page. You may find it useful to refer to Starting & Stopping iControl Services on page 678.

Configuring Lookup Services

iControl uses a lookup service for discovery over a network (see Lookup Services, on page 27). By default, each iControl Application Server runs a lookup service that registers and makes available information about the devices on its network. It will also register with all lookup services that are running on other Application Servers on the same subnet.

If you have multiple Applications Servers and/or multiple subnets in your iControl network, you will need to configure these lookup services.

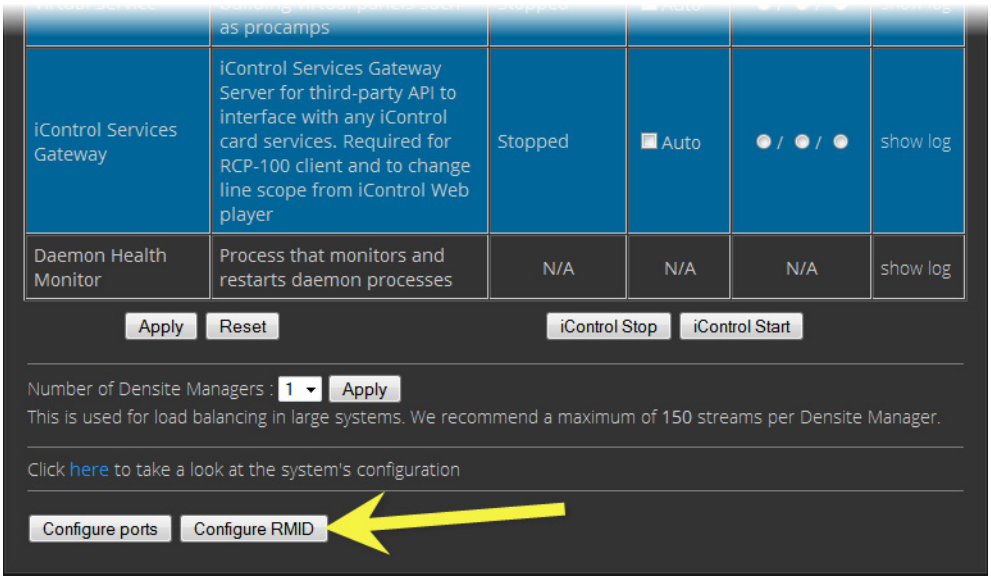
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

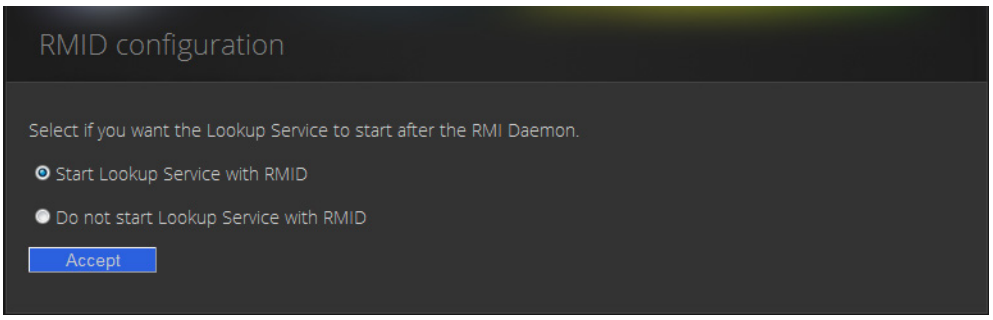
- You have opened the *Services management* page (see page 678).
- You have familiarized yourself with the behavior of the *Lookup location* page (see Lookup Services, on page 27).

To turn a lookup service on or off

1. On the *Services management* page, click **Configure RMID**, near the bottom of the page.



The *RMID configuration* page appears.



2. Click **Start Lookup Service with RMID** if you want this Application Server to run the Lookup Service.

IMPORTANT:	The lookup service should only be activated on a maximum of two Application Servers per subnet.

3. Click **Do not start Lookup Service with RMID** if you do not want this Application Server to run the Lookup Service.
4. Click **Accept**.

Note: The Kaleido-K2 has its own built-in lookup service which must be turned off before it is added to an iControl network.

Specifying Service and Alarm Discovery Locations

In order to operate **iC Web** on client PCs on a subnet other than the one used by the iControl Application Server, you must add the IP address of an Application Server running a lookup service.

To do this...	...do this...
Add locations for service and alarm discovery	1. Type the IP address and (optionally) the name of an Application Server that **is** running a lookup service. 2. Click **Add lookup**. The new lookup location appears in the **Service and alarm discovery** table**.**
Delete a service and alarm lookup entry	1. In the **Service and alarm discovery** table, find the IP address corresponding to the Application Server you would like to remove. 2. In this row, click **Delete**. The specified IP address is removed from the table.

Specifying Alarm Publication Lookup Locations

In a basic iControl configuration, services such as the Densité Manager or the Imagestore Manager will automatically detect—and begin publishing alarm status information to—the GSM(s) on their own subnet.

> **Note:** The current version of iControl has a built-in feature called *multi-GSM* that eliminates the need for specifying alarm publication lookup locations (see About the Alarm Publication Lookup Table, on page 41). The procedures below are being kept in this User Guide to support legacy iControl installations. Please consult with Grass Valley Technical Support before making any modifications to your Lookup Locations (see Contact Us, on page 739).

If, however, you wish to have these services connect to GSMs running on Application Servers on other subnets, you must explicitly specify the GSM locations. You do this by typing the IP address of the target Application Server (on the remote subnet) in the iControl Lookup locations page of the Application Server running the Densité, Imagestore, or other service on the local subnet.

On the Application Servers in the different subnet, you need to specify the IP address of the lookup service where a GSM is registered in the other subnet.

Adding an Alarm Publication Lookup Location

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Lookup location* page for the Application Server that is running the Densité, Imagestore, or other service you wish to publish to remote GSMs (see page 686).

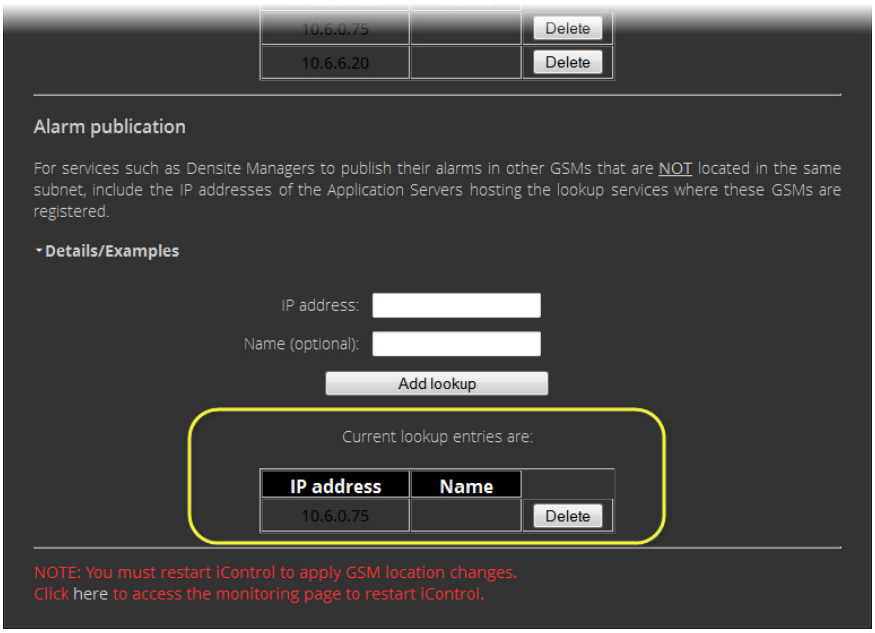
To add an Alarm publication lookup location

1. On the *Lookup location* page, under **Alarm publication**, type one of the following:
   - the IP address of an Application Server on a remote subnet that is running a GSM
   - the IP address of an Application Server on a remote subnet that is running a lookup service

   Note: Use of the **Name** field to indicate the Application Server's host name is optional.

2. Click **Add lookup**.

   The address appears in the **Alarm publication** lookup table.



3. Restart the specific service (e.g., Densité Manager) that you wish to publish to the remote GSM, or restart iControl to publish all services to the remote GSM (see Starting & Stopping iControl Services, on page 678).

Deleting an Alarm Publication Lookup Location Entry

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Lookup location* page on the Application Server hosting the Densité or Imagestore services you no longer wish to be visible outside the subnet (see page 686).

To delete an Alarm publication lookup location entry

1. On the *Lookup location* page, in the **Alarm publication** lookup table, find the IP address corresponding to the Application Server whose entry you would like to delete.
2. In this row, click **Delete**.

   The specified IP address is removed from the **Alarm publication** lookup table.

Configuring the iControl Services Gateway

The iControl Services Gateway is software that enables external devices to access resources (via XML) on an iControl network. You should activate the iControl Services Gateway on an Application Server if any of the following situations apply:

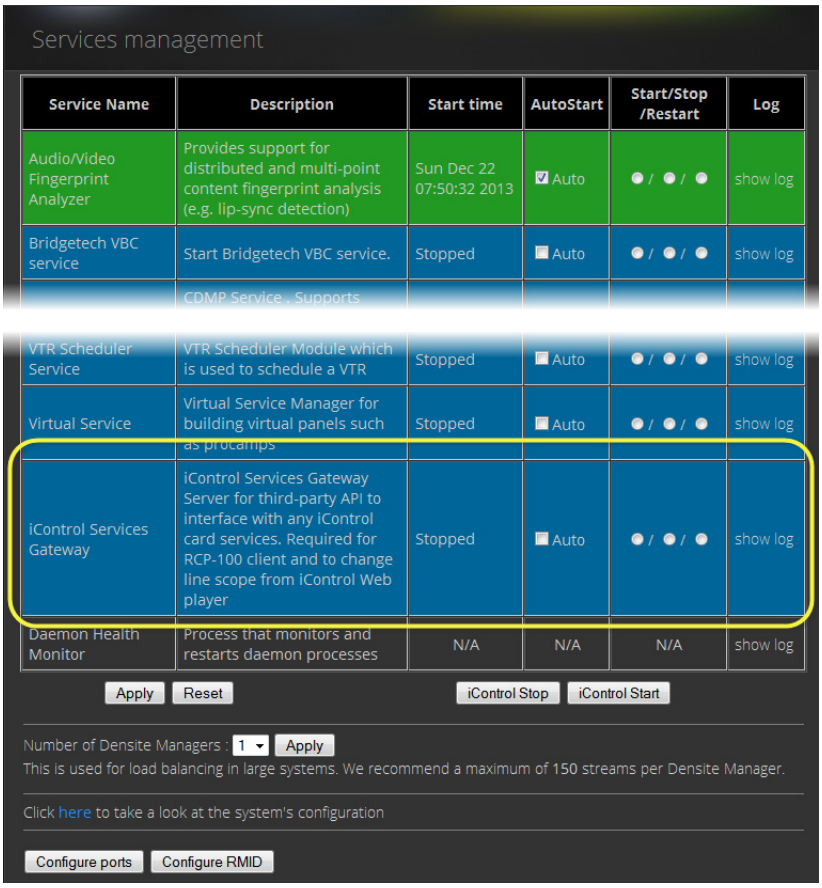
- an RCP-100 or RCP-200 remote control unit is being used as a client on the Application Server
- the **Line Selection** function of the **Line Scope** option for the VCP and SCP series of video probes is being used in **iC Web**
- decoded VBI or CC from VCP or SCP probes is to be displayed in **iC Web**
- third-party applications are being used to control Densité or Imaging cards via iControl

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Services management* page (see page 678).

To activate the iControl Services Gateway

1. On the *Services management* page, locate the **iControl Services Gateway** row in the list of services.



2. In the **Auto Start** column, select the **Auto** check box.

   This is to ensure that the iControl Services Gateway will restart automatically if the Application Server is rebooted.

3. In the **Start/Stop/Restart** column, click the left-most button (corresponding to **Start**).

4. Click **Apply**.

   After a few seconds, the Web page reloads, and the row corresponding to iControl Services Gateway is green (indicating that the service is active).

Task 6: Configuring GPI Outputs on a GPI-1501

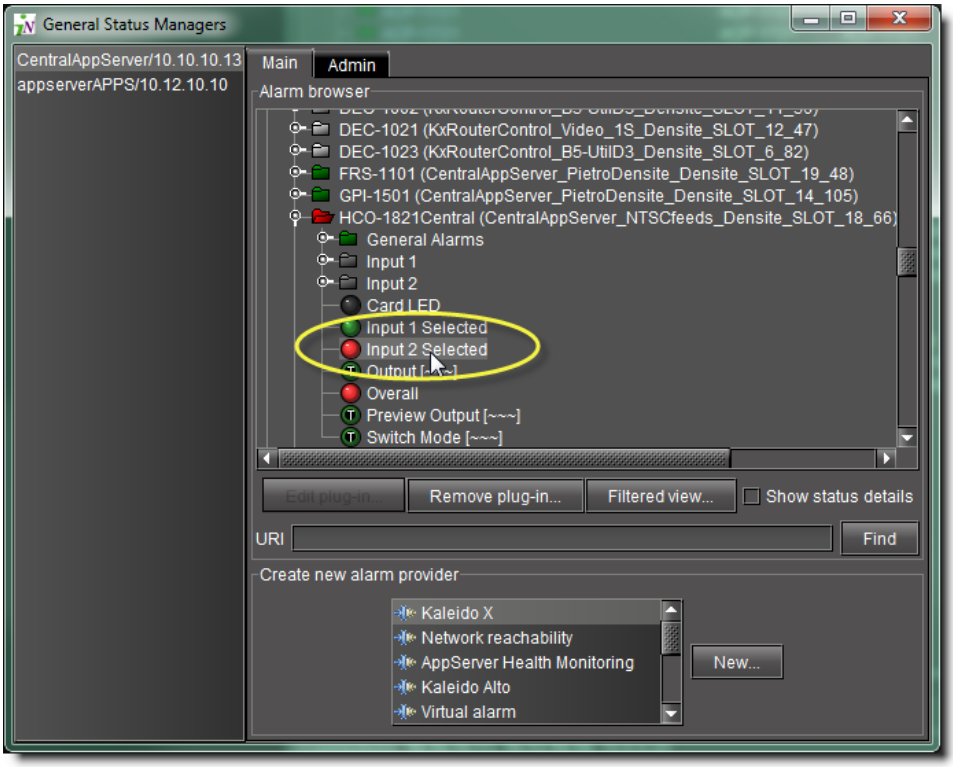
This procedure allows you to configure the GPI outputs on a GPI-1501 to respond to alarms triggered on another card on the iControl network.

REQUIREMENT

Before beginning this procedure, make sure you have opened the GSM Alarm Browser (see Opening the GSM Alarm Browser, on page 710).

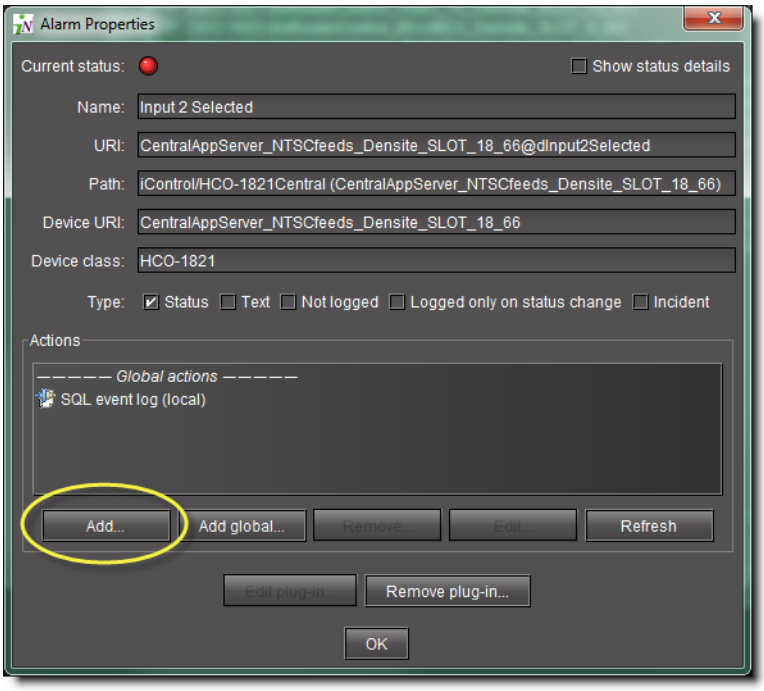
To configure GPI outputs on a GPI-1501

1. In the GSM Alarm Browser, use the vertical scroll bar to find the alarm for which you would like to trigger a GPI output on a GPI-1501 card.

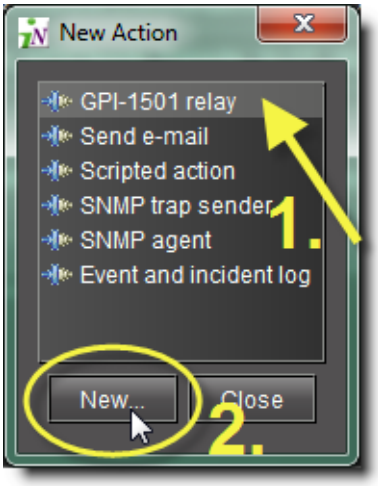


2. Double-click the alarm.

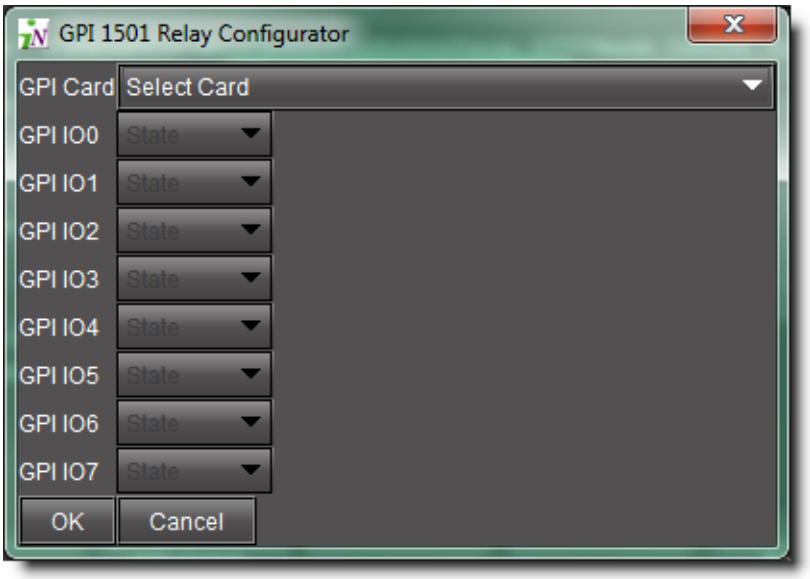
   The **Alarm Properties** window appears.



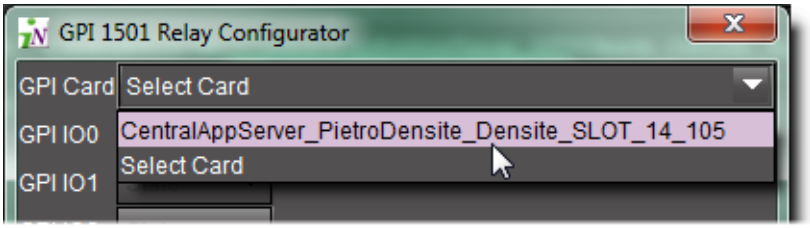
3. Click **Add**.
   The **New Action** window appears.
4. Click **GPI-1501 relay** to select it.
5. Click **New**.



The **GPI-1501 Relay Configurator** window appears.



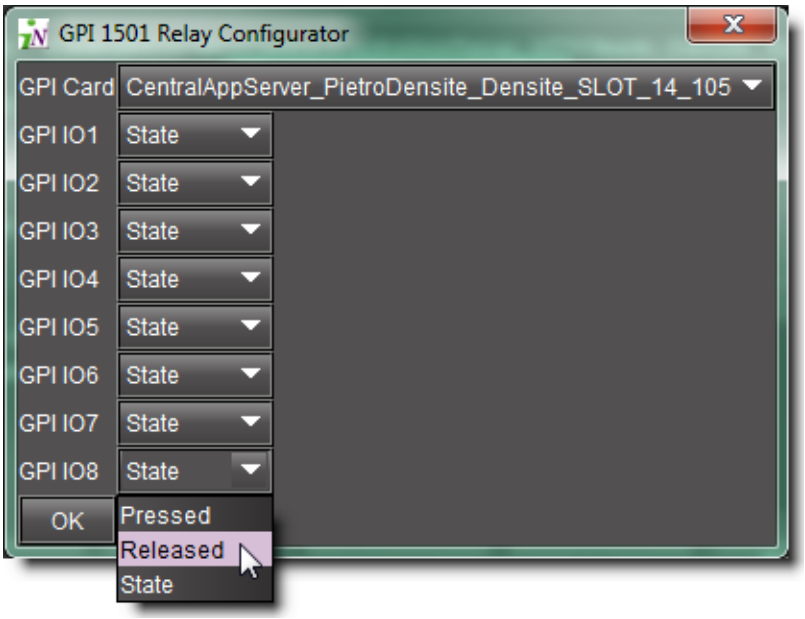
6. In the **GPI Card** list, select the GPI-1501 card whose GPI outputs you would like to control from this alarm.



> **Note:** Only configurable GPIs that are configured as OUT on the GPI-1501 card itself can be operated in this manner.

The eight output relays on the selected card are shown. The names of the GPIs are set in the GPI I/O Config panel of the GPI card itself.

7. You may program one or more GPI outputs on this card or on other cards to respond to this alarm.



Each GPI out on this GPI-1501 card can be programmed to respond to a different alarm from a different card. The eight output relays on the selected card are shown. The names of the GPIs are set in the GPI I/O Config panel of the GPI card itself.

- **Pressed** = high
- **Released** = low

Notes

- If you leave it at State, the GPI is not programmed to respond to this alarm, and can be assigned to a different alarm.
- You can use the labels to identify the alarm source once it is set.

8. Click **OK** when done, or **Cancel** to leave the status unchanged

   This new event appears in the **Actions** window in the **Alarm Properties** panel.

Note: You can edit or delete the event by selecting the GPI-1501 action and clicking **Edit** or **Remove**, respectively.

See also

For more information, see:

- GPI-1501 I/O Module (Densité Card) on page 42.
- the *Densité Series GPI-1501 General Purpose Interface I/O Module Guide to Installation and Operation* (**M906-9900-100**).

Task 7: Connecting & Configuring Devices

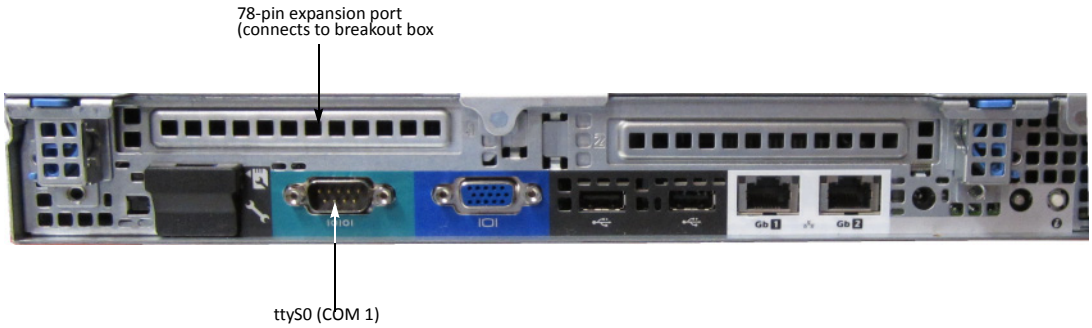
The iControl Application Server communicates with devices in your network over both serial and TCP/IP connections. Once these connections are made physically (using the appropriate cabling), the corresponding ports must be configured.

Configuring Serial Ports

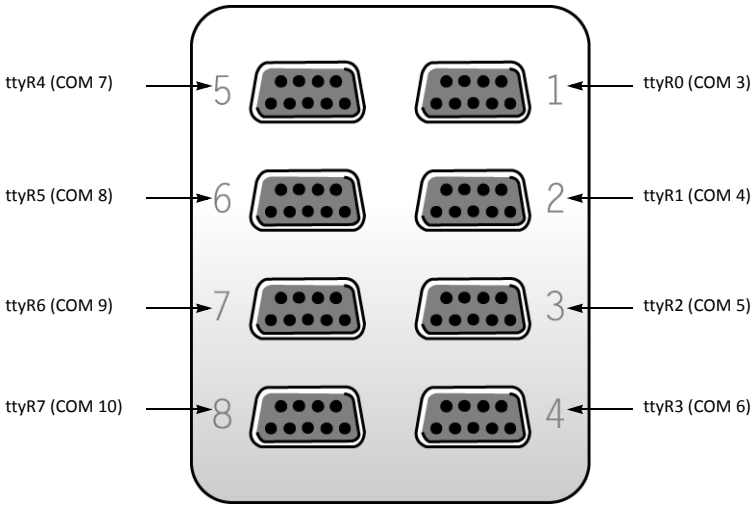
In its standard configuration, the iControl Application Server has two built-in RS-232 ports (one internal, one external). An 8-port expansion card with breakout box optionally can be purchased to accommodate eight RS-422 serial ports.

Port Designation		Protocol
TTY	COM	
R0	3	RS-422
R1	4	
R2	5	
R3	6	
R4	7	
R5	8	
R6	9	
R7	10	

Port Designation		Protocol	Connector Location
S0	COM 1	RS-232	rear panel
S1	COM 2	RS-232	internal



Dell PowerEdge R310 with optional 8-port serial expansion card



RocketPort 8-port serial breakout box

Note: The numbers stamped into the breakout box case (if any) do **not** correspond to the port number.

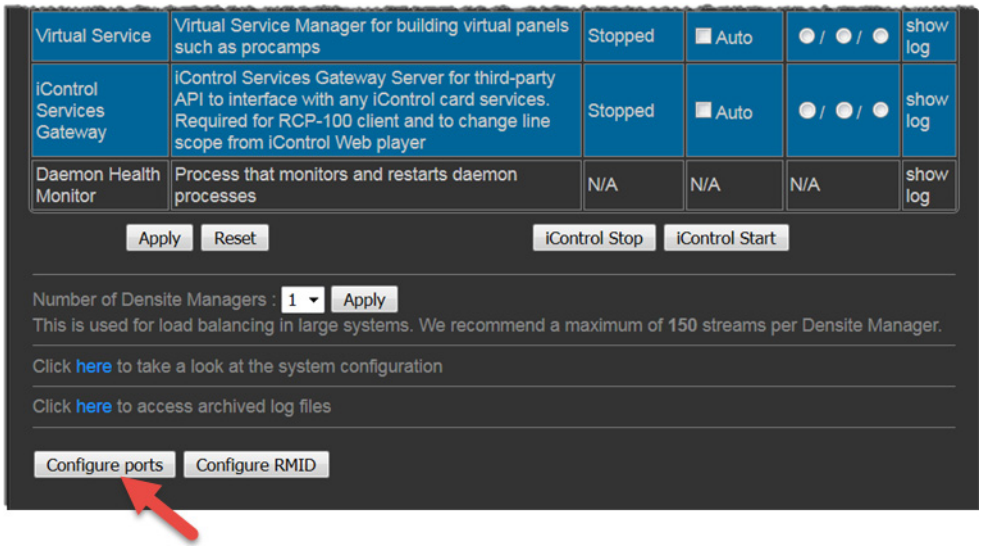
Configuring Serial Ports for a Specific Application Server

REQUIREMENT

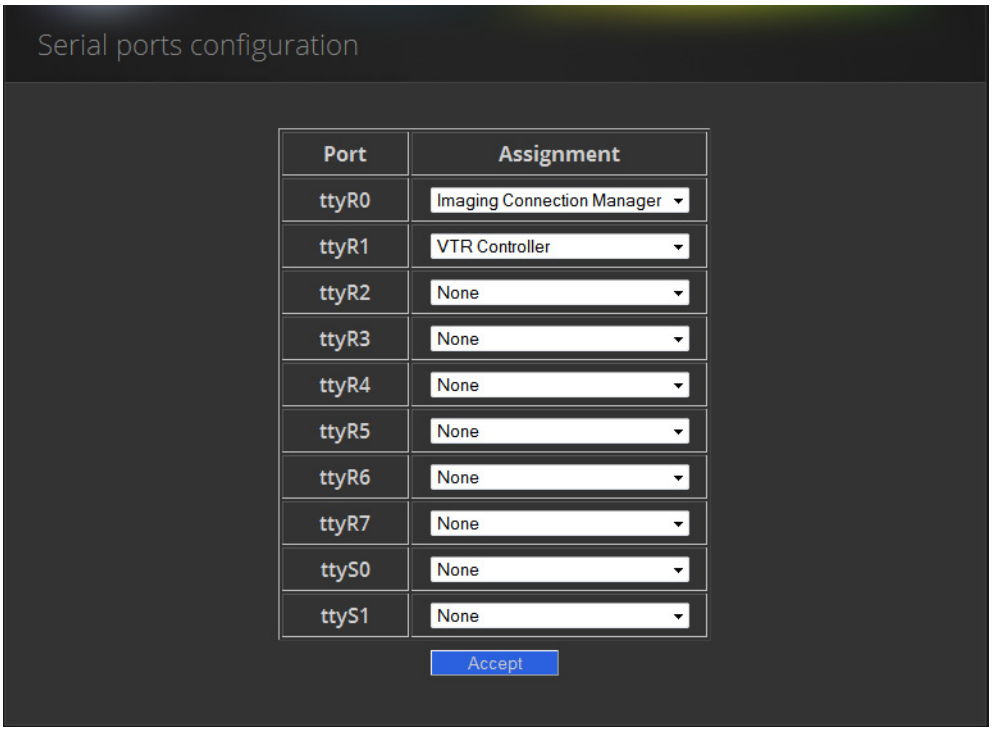
Before beginning this procedure, make sure you have opened the *Services management* page (see page 678).

To configure serial ports for an Application Server

1. On the *Services management* page, near the bottom, click **Configure Ports**.



The *Serial ports configuration* page appears, showing all available ports and their current assignments. Some ports may be assigned, even if this is the first time the Application Server has been configured.



2. Choose an assignment for each active port from its drop down menu.

Port Assignment	Description
None	Configures the port to communicate with standard RS-422 devices (e.g., routers)
Imaging Connection Manager	Configures the port to communicate with Grass Valley's Symphonie or Quartet frames and their Imaging series cards
VTR Controller	Configures the port to communicate with a VTR
Tandberg Alteia	Configures the port to communicate with a device using the Alteia Remote Control Protocol

Note: It is good practice to activate only the required ports, since the Application Server will unnecessarily monitor active ports that are not in use.

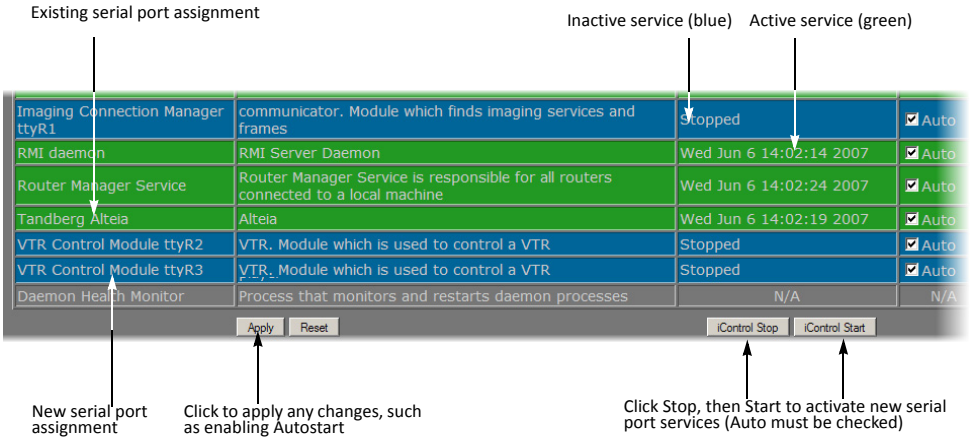
3. When you have finished assigning ports, click **Accept**.

   The *Services management* page reappears, with new rows in the list of services for each of the newly assigned ports.

   If more than one port has been assigned to an Imaging Connection Manager or VTR Connection service, there will be a new row for each, identified by the port number.

Only one row for the Tandberg Alteia service will be created, even if more than one port has been assigned to that service.

A green background indicates a service that is running. Blue indicates a service that is stopped.



New rows in list on Services management page

4. In the **AutoStart** column, select the **Auto** check box for each of the services corresponding to the newly assigned serial ports.

   This will cause the services to start automatically if the Application Server is rebooted.

5. In the **Start/Stop/Restart** column, select Start for each of the services corresponding to the newly assigned serial ports.

6. Click **Apply**.

   The page reloads with the ports you have activated showing a green background.

Task 8: Configuring an Application Server's Date and Time

An Application Server's *Date* and *Time* reflects the time set in the operating system.

You may choose to peg the server's time to the time of another server. The other server must either be running an NTP (Network Time Protocol) server, or have the time protocol enabled in the *inetd* super-server daemon.

> **Note:** For your system to use NTP for synchronization you must have the `ntpdate` NTP client program installed.

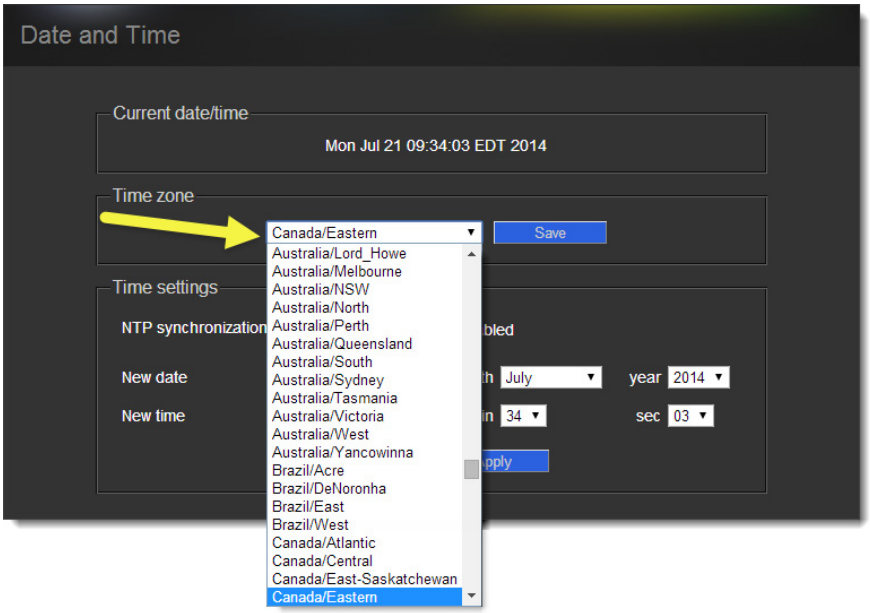
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- The remote Application Server whose time you would like to synchronize to, is online and functioning.
- On the Application Server whose time you would like to configure, you have navigated to the *Date and Time* page (see page 687).

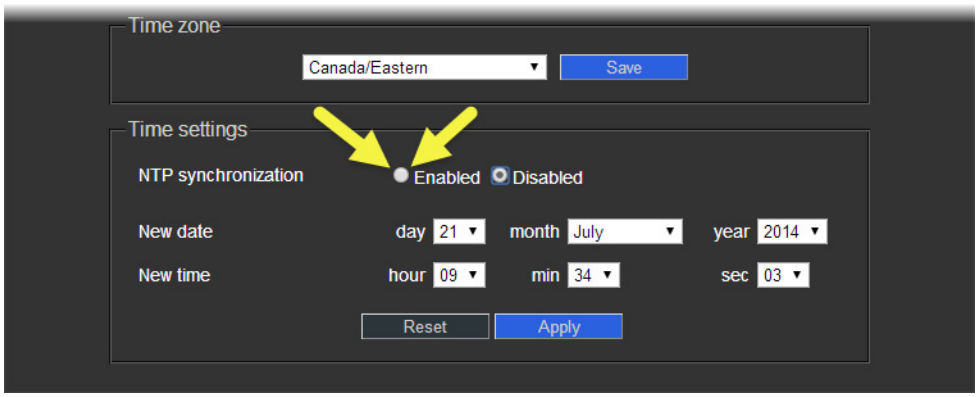
To synchronize an Application Server's time to an NTP server

1. On the *Date and Time* page, in the **Time zone** area, select the desired time zone from the list, and then click **Save**.

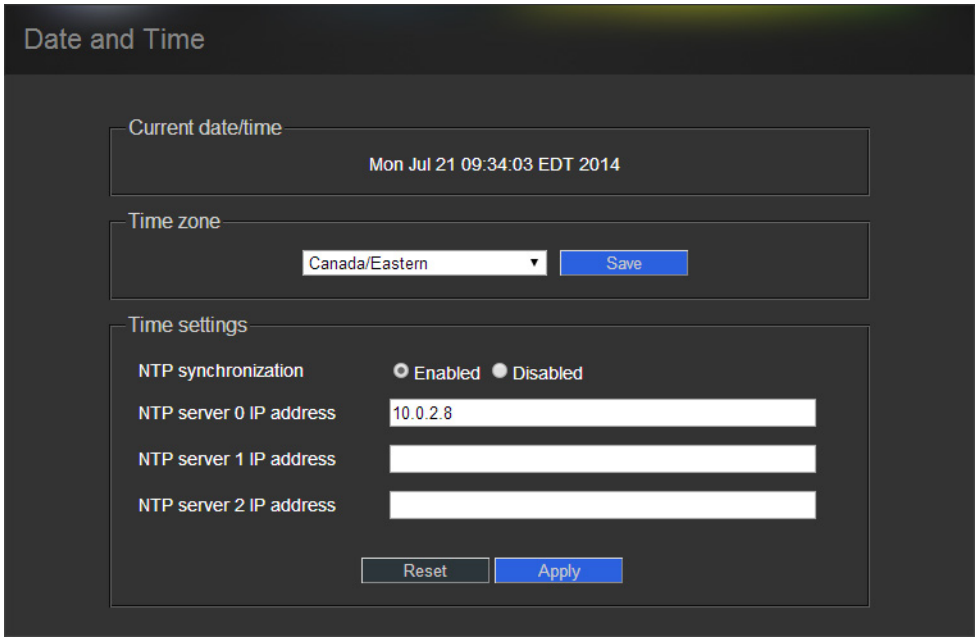


2. If you would like to synchronize your Application Server's time to a remote NTP server, perform the following sub-steps:

   a) In the **Time settings** area, enable **NTP synchronization**.



The **NTP server IP address** field appears.



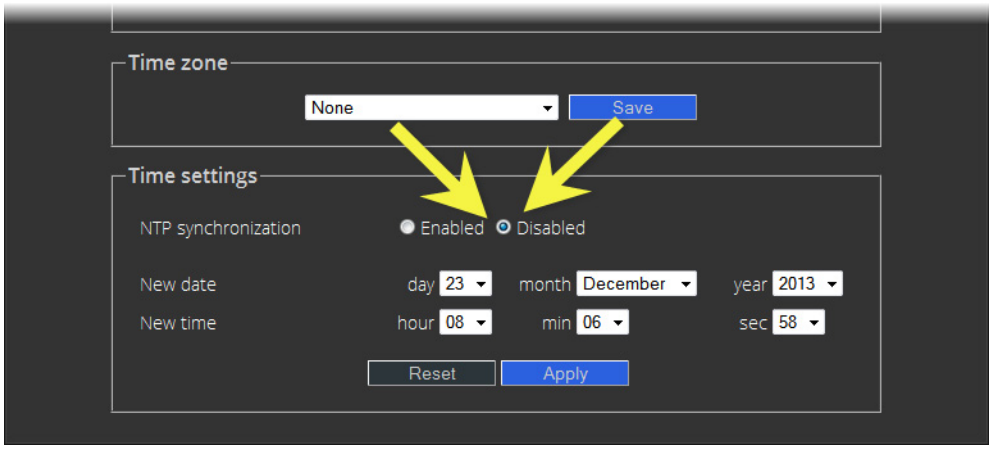
b) Type the IP address of the highest-priority NTP server in the **NTP server 0 IP address** box, and then click **Apply**.

Note: The highest-priority NTP server is the NTP server you would like to be considered as the preferred timing source. All other NTP timing sources (i.e., *NTP server 1*, *NTP server 2*) are to be considered as the next-in-line preferred timing source in order of ascending server number and upon the Application Server's inability to resolve the highest priority source.

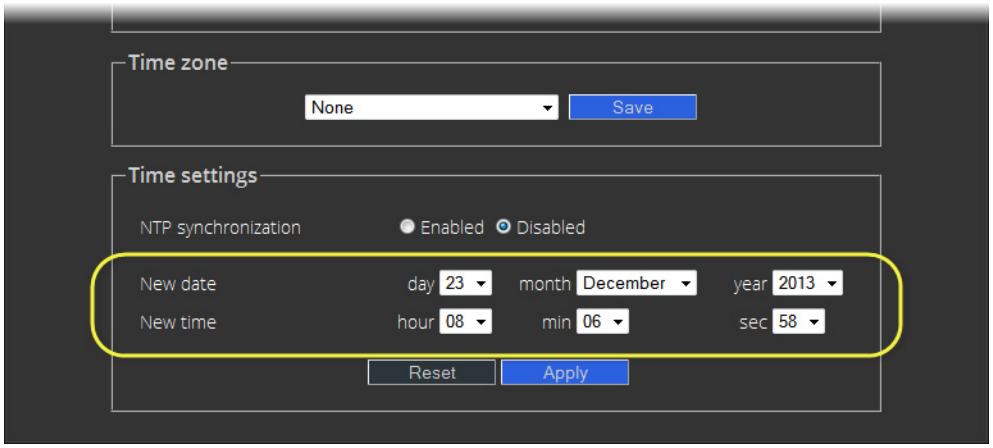
c) If there are alternate NTP servers available to act as NTP timing backup to the highest priority NTP server, type their IP addresses into the remaining fields in order of priority (lowest number is highest priority).

3. If you would **NOT** like to synchronize to a remote NTP server, perform the following sub-steps:

   a) In the **Time settings** area, disable **NTP synchronization**.



   b) Configure the desired date and time for this Application Server.



   c) Click **Apply**.

Task 9: **[OPTIONAL]** Gaining Access to Documentation

About Our Documentation Deployment Methods

Grass Valley makes its iControl documentation suite available to clients in two different formats, PDF and online help (HTML), depending on the document in question. All documents are available in PDF format from the iControl Documentation page. Additionally, you may access the latest version of any document, from the *Documentation Library* section of Grass Valley's website (see Contact Us, on page 739).

A subset of the documentation suite is also available as online help (HTML). The following documents are available in HTML format:

- iControl User Guide

- iControl Router User Guide
- iControl Solo User Guide

All online help is hosted on the Grass Valley website. The **HTML** links visible on the iControl Documentation page and the **Help** (or **?**) buttons/menus available from the Navigator, iControl Router, and iControl Solo client-side applications all link to the online help on the website. When clicking these links, you may need to authenticate yourself using your Grass Valley Support account profile.

See also

For more information about documentation and the Grass Valley Documentation Library, see Accessing Documentation from iControl's Documentation Page on page 70, Accessing Online Help from iC Navigator on page 71, and Accessing Online Help from Router Manager Configurator on page 72.

Accessing Documentation from iControl's Documentation Page

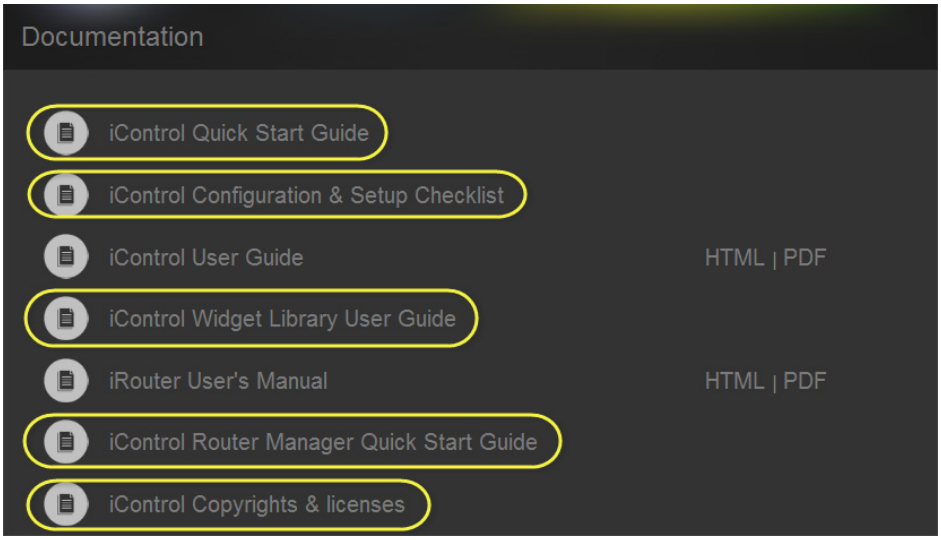
REQUIREMENT

Before beginning this procedure, make sure you have opened iControl (see page 677).

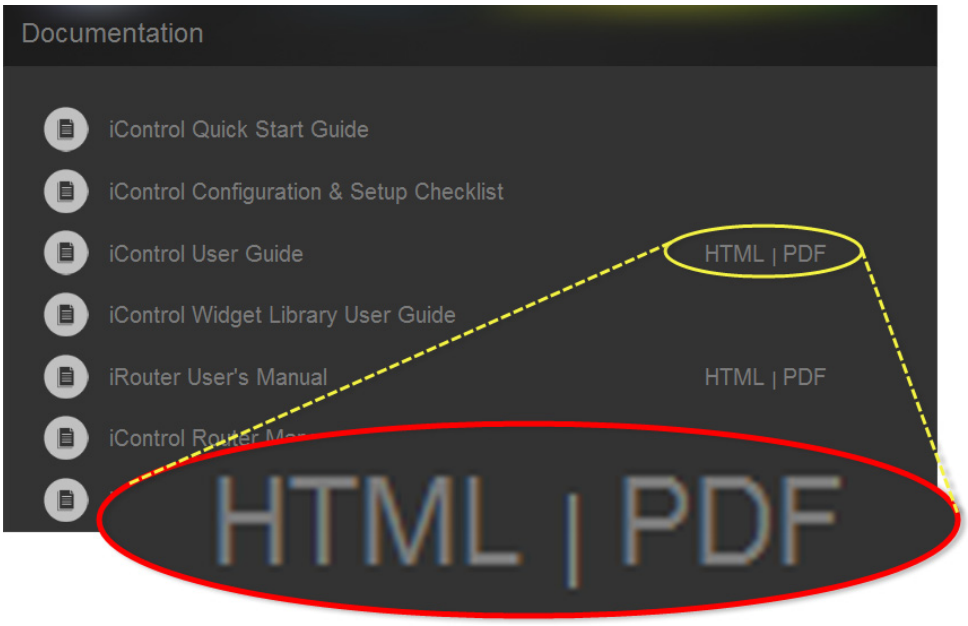
To access documentation from iControl's Documentation page

- On the *Startup* page, click **Release Notes** if desired, or click **Documentation** if you would like any other iControl documentation.

  Alternatively, you can access iControl documentation (PDF and HTML), from the *Documentation Library* section of Grass Valley's website.



Click any of the links (circled, here, in yellow) to open a PDF version



Where available, click either HTML or PDF to open those formats

Accessing Online Help from iC Navigator

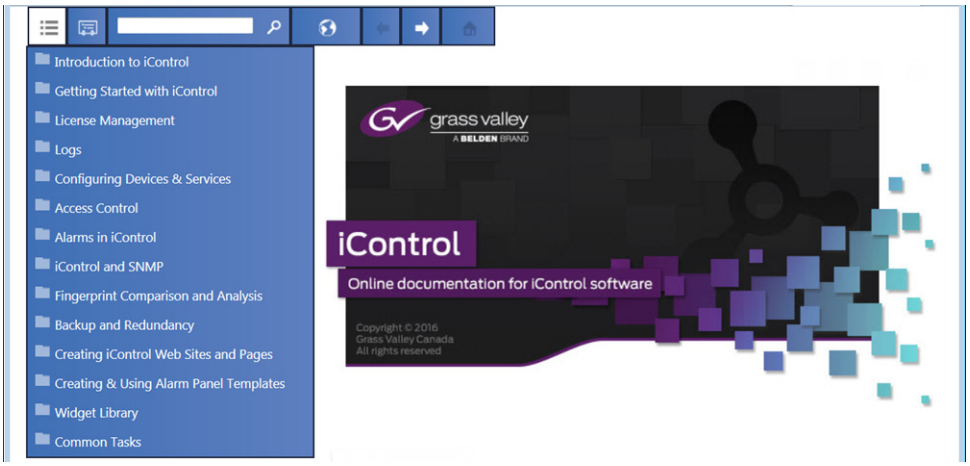
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **iC Navigator** (see page 697).
- The client PC you are using is connected to the Internet.

To access online help from iC Navigator

1. In **iC Navigator**, on the **Help** menu, click **Online Help**.
2. If the Gate Keeper page appears, then follow the login or sign up instructions, as required. The requested online help appears.



Accessing Online Help from Router Manager Configurator

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **Router Manager Configurator** (see the "Open Router Manager Configurator" section in the *iControl Router Quick Start Guide*).
- The client PC you are using is connected to the Internet.

To access online help from Router Manager Configurator

1. In **Router Manager Configurator**, click the *Help* button (?).
2. If the Gate Keeper page appears, then follow the login or sign up instructions, as required. The online help appears in your browser.

Network Considerations & Port Usage

Network Considerations

In general, large iControl systems (with multiple Application Servers, and a moderate amount of streaming) have the following client-to-server communication requirements:

- less than 100 ms of latency
- an available bandwidth of 1 Mbit/s (sustained)
- an available bandwidth of 5 Mbit/s (peak)

The sustained bandwidth requirement may be higher, depending on the number of streams (see Allégro-1 Bandwidth Requirements and see Densité Probe Bandwidth Requirements, on page 73).

Note: iControl does not support NAT (Network Address Translation). Reverse NAT or double-NAT techniques can be used as an alternative.

Allégro-1 Bandwidth Requirements

The table below provides an Allégro-1's typical bandwidth (bit rate) requirements, based on using the MVC-3 codec:

Image Size	Frame rate	Hi Quality (Medium bandwidth, Audio)	Low Quality (Low bandwidth, Audio)
1024 × 768	15 fps 30 fps	1500 kbps 2200 kbps	800 kbps 1300 kbps
800 × 600	15 fps 30 fps	1000 kbps 1600 kbps	600 kbps 800 kbps
640 × 480 Full 601 Resolution	15 fps 30 fps	500 kbps 625 kbps	225 kbps 285 kbps
320 × 240 1/2 601 Resolution	15 fps 30 fps	200 kbps 250 kbps	60 kbps 90 kbps
176 × 144 1/4 601 Resolution	15 fps 30 fps	100 kbps 125 kbps	30 kbps 40 kbps
88 × 60	15 fps 30 fps	80 kbps 100 kbps	10 kbps 15 kbps

Densité Probe Bandwidth Requirements

The tables below provide typical bandwidth (bit rate) requirements (per card) for Densité cards capable of audio/video streaming (SCP-, ACP-, VCP- and DCP-series).

Thumbnails

Size		Poor Quality	Medium Quality	High Quality
--- ***Refresh Mode: Fast*** ---				
Small	80 × 60 pixels	8.9 kb/s	11 kb/s	14.5 kb/s
Medium	160 × 120 pixels	19 kb/s	23 kb/s	35 kb/s
Large	320 × 240 pixels	55 kb/s	68 kb/s	85 kb/s
--- ***Refresh Mode: 1 second*** ---				
Small*	80 × 60 pixels	1.9 kb/s	2.2 kb/s	2.9 kb/s
Medium*	160 × 120 pixels	3.8 kb/s	4.6 kb/s	7 kb/s
Large	320 × 240 pixels	11 kb/s	13.6 kb/s	17 kb/s
* Very low bit rate optimized for transmitter site and cell.				
--- ***Refresh Mode: 10 seconds*** ---				

(*Continued*)

Size		Poor Quality	Medium Quality	High Quality
Small	80 × 60 pixels	0.9 kb/s	1.1 kb/s	1.4 kb/s
Medium	160 × 120 pixels	1.8 kb/s	2.4 kb/s	3.5 kb/s
Large	320 × 240 pixels	5.5 kb/s	6.8 kb/s	8.6 kb/s
Compression type VBR; variation of ± 20%				

IP (Waveform + Vector) Scope

Refresh Speed	Fast	1 second	10 seconds
Bit Rate	5 kb/s	1 kb/s	0.1 kb/s

Remote Audio Level Meter (RALM)

Refresh Speed	Typically 40 – 60 ms
Bit Rate	0.33 – 0.8 kb/s

VB

Refresh Speed	Typically 40 – 60 ms
Bit Rate	0.33 – 0.8 kb/s

Note: Maximum transmission speed per channel for any combination of data is 90 kb/s.

TCP/IP Port Usage

The various iControl services require access to specific ports. The tables below describe the ports used in a multi-site configuration. In networks where a firewall is present between device A and device B, the ports used to communicate from device A to device B must be open on the incoming (external) side of the firewall.

From Client to Application Server

Service	Port	Transport	Notes
DMT	5432	TCP	Communication between Data Management tool and Postgres database
DSS Admin	1220	TCP	Darwin Streaming Server Admin

(*Continued*)

Service	Port	Transport	Notes
FTP	20, 21	TCP	Used for maintenance purposes (file transfer). SSH can be used instead. Not necessarily required (can be turned off). iControl upgrade page uses HTTP transfer.
HTTP	80	TCP	
iControl Gateway	10001, 13000	TCP	Optional, only if IP scope probe option is enabled or RCP-100/RCP-200 client required to communicate with Application Server.
Location services	4160, 8000-8010	TCP, UDP	Responsible for discovery and communications between devices/services on iControl network.
Java RMI	32768-65535	TCP	Remote Method Invocation (client/server communication). Dynamic Allocation of ports. Required for communication between client and Application Server. This range can be restricted to match specific security requirements. A minimum of 4000 ports should be allocated. Please contact Grass Valley Technical Support, for more information (see Contact Us, on page 739).
Java RMID	1098–1099	TCP, UDP	Remote Method Invocation Daemon to support client/server connections. Required for communication between client and Application Server.
LDAP	389	TCP	Required for the iControl Access Control/Authentication feature (user login).
RTSP	554 6970–6999	TCP, UDP UDP	Real Time Streaming Protocol required for thumbnail streaming. Streams from probes sent to clients from Application Server.
SSH, SCP	22	TCP	Used for maintenance purposes. Secure Shell Login and Secure Remote Copy are required to log on to an Application Server for maintenance. You can use an SSH client like PuTTY.
Streaming Sync	1555	TCP, UDP	Required for thumbnail streaming
TELNET	23	TCP	Used for maintenance purposes (remote login). SSH can be used instead. Less secure than SSH, but useful when a SSH client is not available. Can be turned off.

From Application Server to Client

Service	Port	Transport	Notes
Java Jini	4160, 8000-8010	TCP, UDP	Responsible for discovery and communications between devices/services on iControl network.
Java RMI	49152-65535	TCP	Remote Method Invocation (client/server communication). Dynamic Allocation of ports. Required for communication between client and Application Server.
Java RMID	1098–1099	TCP, UDP	Remote Method Invocation Daemon to support client/server connections. Required for communication between client and Application Server.

(*Continued*)

Service	Port	Transport	Notes
RTSP	554 6970–6999 20000–65535	TCP, UDP UDP UDP	Real Time Streaming Protocol. Streams from probes sent to clients from Application Servers. The 20000–65535 range can be restricted to match specific security requirements. A minimum of 10,000 ports should be allocated.
SMTP	25	TCP	Simple Mail Transfer Protocol, for email alerts

Between Application Server and External Management System

Service	Port	Transport	Notes
HTTP	5955	TCP	Used to monitor and control cards housed in Densité or GV Node frames registered with *Densité Manager 1,* via a REST API.
	5953		Used to monitor and control cards housed in Densité or GV Node frames registered with *Densité Manager 2,* via a REST API.
	5951		Used to monitor and control cards housed in Densité or GV Node frames registered with *Densité Manager 3,* via a REST API.
	5949		Used to monitor and control cards housed in GeckoFlex frames registered with *GeckoFlex Manager,* via a REST API.
	5957		Used to monitor and control alarm status information in a GSM, via a REST API.

From Application Server to Allégro-1

Service	Port	Transport	Notes
Java Jini	4160, 8000-8010	TCP, UDP	Responsible for discovery and communications between devices/services on iControl network. Uses multicast in remote regions only, unicast and multi-unicast elsewhere.
Java RMI	49152-65535	TCP	Remote Method Invocation (client/server communication). Dynamic Allocation of ports. Required for communication between Application Server and Allégro-1.
Java RMID	1098-1099	TCP, UDP	Remote Method Invocation Daemon to support client/server connections. Required for communication between Application Server and Allégro-1.

Note: If an Application Server is used as an Allégro-1 Streaming Relay, additional ports are required.

From Client to Allégro-1

Service	Port	Transport	Notes
Java RMI	49152-65535	TCP	Remote Method Invocation (client/server communication). Dynamic Allocation of ports. Required for communication between client and Allégro-1 applications.
Tomcat	8080	TCP	Required to access Allégro-1 Web pages

From Allégro-1 to Client

Service	Port	Transport	Notes
Java RMI	49152-65535	TCP	Remote Method Invocation (client/server communication). Dynamic allocation of ports. Required for communication between client and Allégro-1 applications.
RTSP	554 6970–6999 20000–65535	TCP, UDP UDP UDP	Real Time Streaming Protocol. Streams from probes and Allégro-1 sent to clients from Allégro-1 servers. The 20000–65535 range can be restricted to match specific security requirements. A minimum of 10,000 ports should be allocated.

From Allégro-1 to Application Server

Service	Port	Transport	Notes
Java Jini	4160, 8000-8010	TCP, UDP	Responsible for discovery and communications between devices/services on iControl network. Uses multicast in remote regions only, unicast and multi-unicast elsewhere.
Java RMI	32768–65535	TCP	Remote Method Invocation (client/server communication). Dynamic Allocation of ports. Required for communication between Allégro-1 and Application Server. This range can be restricted to match specific security requirements. A minimum of 4000 ports should be allocated.
Java RMID	1098–1099	TCP, UDP	Remote Method Invocation Daemon to support client/server connections. Required for communication between Allégro-1 and Application Server.

From Local Application Server to Remote Application Server

Service	Port	Transport	Notes
Event log	5432	TCP	Communication between SQL event log plug-in and Postgres database
Java Jini	4160, 8000-8010	TCP, UDP	Responsible for discovery and communications between devices/services on iControl network. Uses multicast in remote regions only, unicast and multi-unicast elsewhere.
Java RMI	32768–65535	TCP	Remote Method Invocation (client/server communication). Dynamic Allocation of ports. Required for communication between Allégro-1 and Application Server. This range can be restricted to match specific security requirements. A minimum of 4000 ports should be allocated.
Java RMID	1098–1099	TCP, UDP	Remote Method Invocation Daemon to support client/server connections. Required for communication between Allégro-1 and Application Server.

From Remote Application Server to Local Application Server

Service	Port	Transport	Notes
Event log	5432	TCP	Communication between SQL event log plug-in and Postgres database
Java Jini	4160, 8000-8010	TCP, UDP	Responsible for discovery and communications between devices/services on iControl network. Uses multicast in remote regions only, unicast and multi-unicast elsewhere.
Java RMI	32768–65535	TCP	Remote Method Invocation (client/server communication). Dynamic Allocation of ports. Required for communication between client and Application Server/Allégro-1 applications. This range can be restricted to match specific security requirements. A minimum of 4000 ports should be allocated.
LDAP	389	TCP	Required for the iControl Access Control/Authentication feature (user login).
rsync	873	TCP, UDP	Mirrors file systems for redundancy
SNMP Health Monitoring Agent	1161	UDP	Required for centralized Application Server Health Monitoring

From Application Server to Densité

Service	Port	Transport	Notes
Densité	5100, 5110	TCP	Required if Densité controller is installed. Recommendation is to isolate Densité on ETH1 for optimal performance. Can also be installed remotely to communicate with Application Server over WAN.

From Densité to Application Server

Service	Port	Transport	Notes
	None		Response is sent through the connection initiated by the Application Server.

Between Application Server and SNMP Devices

Service	Port	Transport	Notes
SNMP	161, 162	UDP	Simple Network Management Protocol, used for communications between iControl and third party devices. Required for Application Server acting as an agent or a manager.
SNMP Health Monitoring Agent	1161	UDP	Required for centralized Application Server Health Monitoring

From Application Servers to IR Controller

Service	Port	Transport	Notes
IR Controller	4998	TCP, UDP	Used for set-top box control via infrared signal

Between Application Server and NTP Server

Service	Port	Transport	Notes
NTP	123	UDP	Used for Network Time Protocol synchronization, which is strongly recommended in a multiple Application Server configuration. Port needs to be open in both directions.

From Application Server to SMTP Server

Service	Port	Transport	Notes
SMTP	25	TCP	Simple Mail Transfer Protocol, for email alerts

3 License Management

Summary

Key Concepts

License management is the method by which iControl administrators can request, activate, and distribute licenses for options and drivers among their user base. The majority of tasks related to license management have as a starting point iControl's *License Management* page.

Concept	Description
License	An agreement to use a specific software module or collection of modules under specific terms
License Management page	Web-based license management for end-users.
Software Feature	A licensable portion of software.
License request file	A file iControl generates that you send to Grass Valley by e-mail in order to request licenses for one or more optional features.
Activation file	A file Grass Valley sends to you that, when uploaded to an Application Server, unlocks and activates one or more optional features.

Sample Workflows

Depending on your needs, you may wish to activate licenses for a single Application Server or for several Application Servers at once.

IMPORTANT: Considerations in choosing a licensing strategy

Licensing several Application Servers at once carries with it the advantage of not having to perform a licensing workflow on each of potentially many servers. In such a networked licensing topology, one server requests and activates licenses for itself, and these newly unlocked features will subsequently become unlocked on the remaining Application Servers (on the same site).

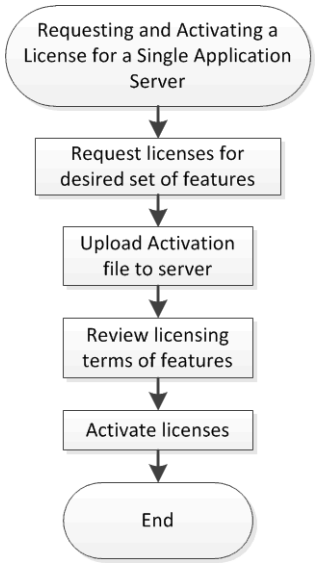
There is, however, a reduction in robustness in the networked model: If the Application Server originally used to request and activate licenses goes offline, the network-licensed features on the remaining servers may become locked again should these servers, in their own right, need to reboot or have their iControl Services restart. If resilience and robustness in feature licensing is critical to your network of Application Servers, you may want to consider individually licensing each Application Server.

[Workflow]: Requesting and Activating a License for a Single Application Server

If you would like to activate one or more licenses on a single Application Server, perform this workflow.

IMPORTANT: System behavior

If you would like to activate licenses on a single Application Server (to the exclusion of all others) but have a Redundancy Group configured for this server, you will not be able to remove the other servers that belong to this Redundancy Group from the license activation list.



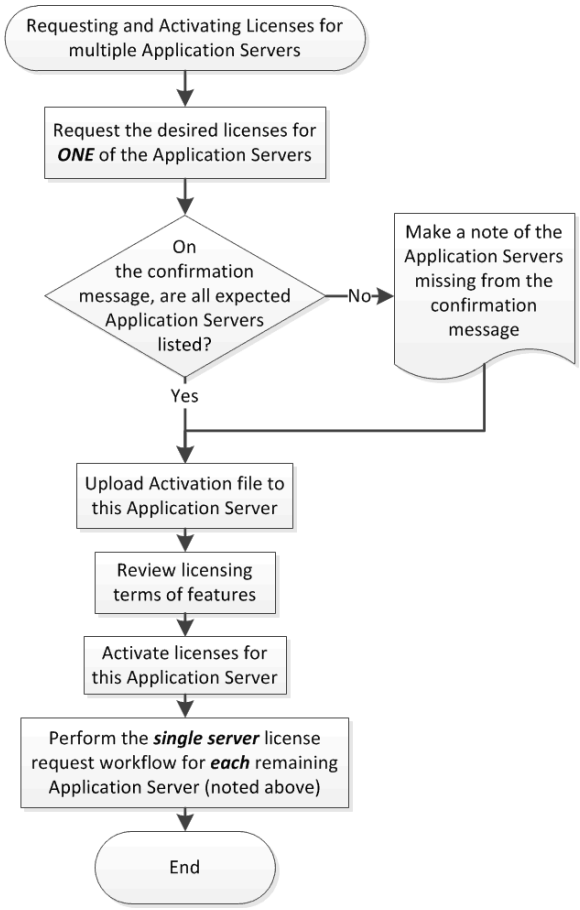
Flowchart depicting licensing workflow (single Application Server)

Workflow: Requesting and activating a license for a single Application Server

1.	On the Application Server, open the *License Management* page (see page 684).
2.	Request the desired set of iControl licenses (see page 84).
3.	Wait for Grass Valley to return an activation file.
4.	Upload the activation file to the Application Server (see Activating a License, on page 88).
5.	Review the licensing terms of the requested features.
6.	Preview the requested features.
7.	Activate the license (see page 88).

[Workflow]: Requesting and Activating Licenses for Several Application Servers

If you would like to activate one or more licenses on multiple Application Servers, perform this workflow.



Flowchart depicting licensing workflow (several Application Servers)

Workflow: Requesting and activating licenses for several Application Servers

1.	Ensure all Application Servers for which you would like to license features is currently running iControl version 4.30 or later.
2.	Choose one of the Application Servers for which you would like to license features. (hereafter called *AS 1*).
3.	Ensure *AS 1* is connected to the network through its **eth0** Ethernet port (see page 48).
4.	Request the desired set of iControl licenses for *AS 1* (see page 84). If, on the license request file confirmation message one or more of the expected Application Servers are missing, make a note of each of the missing Application Servers by IP address.
5.	Wait for Grass Valley to return an activation file.
6.	Upload the activation file to *AS 1* (see Activating a License, on page 88).
7.	Review the licensing terms of the requested features.
8.	Preview the requested features.
9.	Activate the licenses for *AS 1* (see page 88).
10.	For **each Application Server** you made note of in Task 4, perform the workflow for requesting and activating licenses on a single Application server (see page 83).

Detailed Directions

IMPORTANT: Grass Valley strongly recommends performing procedures only in the context of how they are called from the workflows (see Sample Workflows, on page 81).

Requesting a License

IMPORTANT: Features listed as *Pending* were active on this Application Server before it was upgraded to the current version of iControl. The first time you request a license, iControl also requests activation files for these already licensed features at no additional charge.

Until you upload activation files to the Application Server for these already-paid-for features, you will be using these features on a trial basis which will expire 30 days after first use.

It is important to request these features' activation files as soon as possible after upgrading to this version of iControl

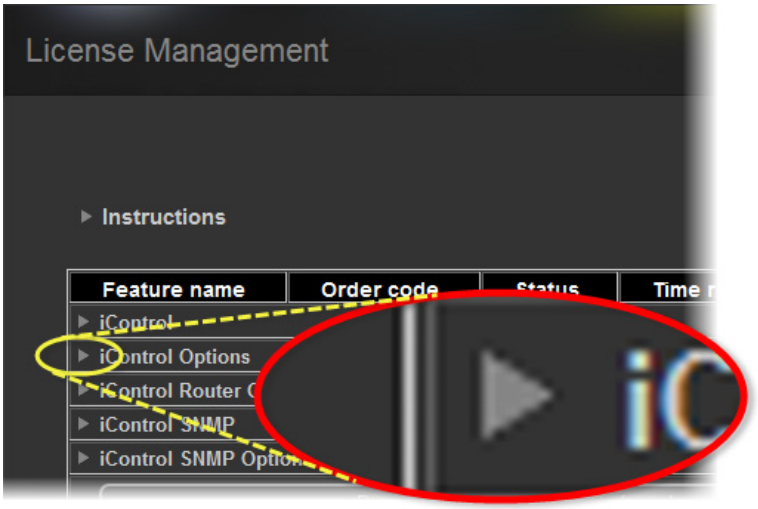
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

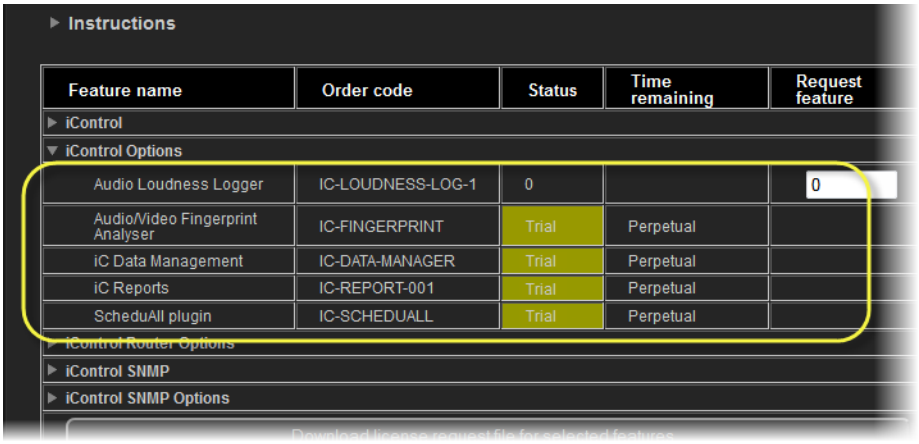
- You have opened the *License Management* page (see Opening the License Management Page, on page 684).
- You are able to send and receive e-mail on your client PC.
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see Sample Workflows, on page 81).

To request a license

1. On the *License Management* page, in the **Feature name** column, use the expansion triangles to locate the feature for which you would like to request a license.



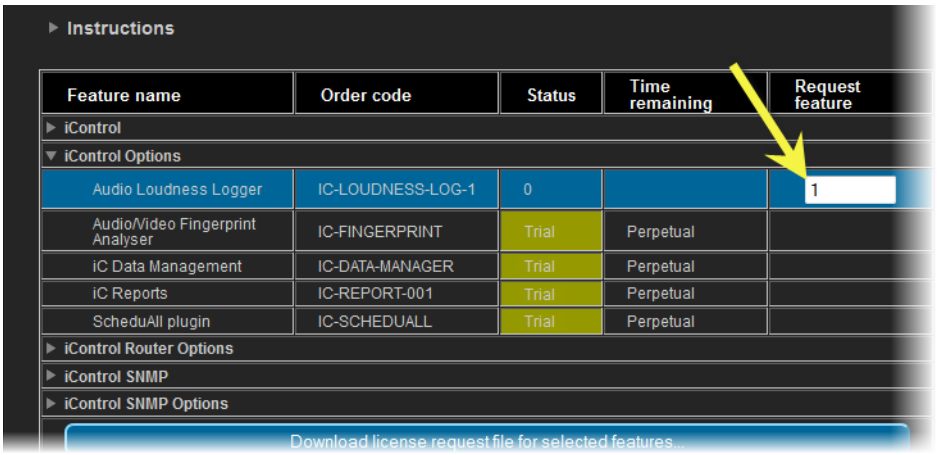
Click the right-pointing expansion triangle to display a category's features



View of the expanded iControl Options category (circled)

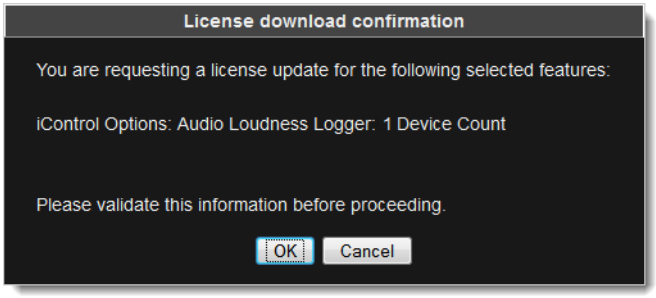
Note: The *Pending* status of several features (visible in the graphic, above), will change to *Active* immediately following the first license activation. Features initially showing *Pending* are those features you have already paid for but whose licensing has not yet been synchronised with Grass Valley's new licensing structure. It should also be noted that features for whom licenses are *Pending* have pre-selected check boxes.

2. In the **Request Feature** column, select the check boxes corresponding to the features whose licenses you would like to request, or, if applicable, specify the number of licenses you would like to request.



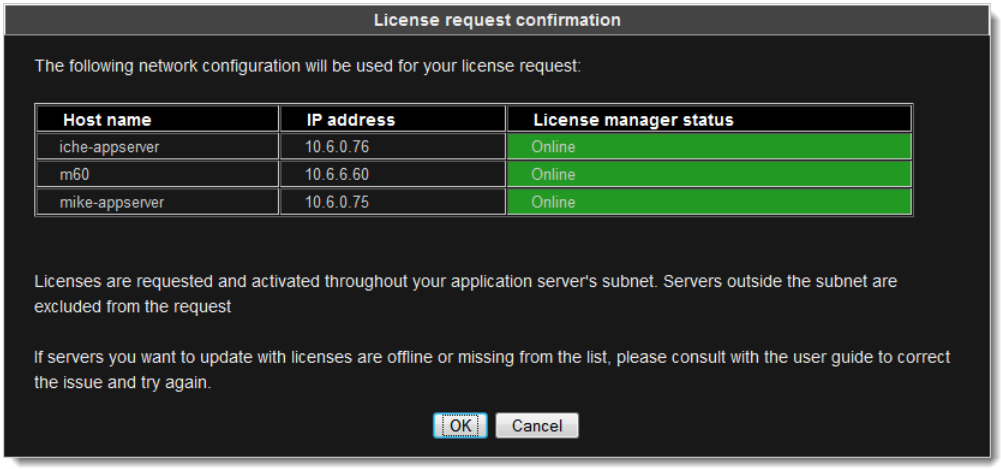
3. Click **Download license request file for selected features**.

   A confirmation message appears.



4. Validate the information listed in the confirmation, and if satisfactory, click **OK**. If not satisfactory, click **Cancel**.

   If you clicked **OK**, a confirmation message appears. A confirmation message lists the Application Servers used for the license request.



Request confirmation message

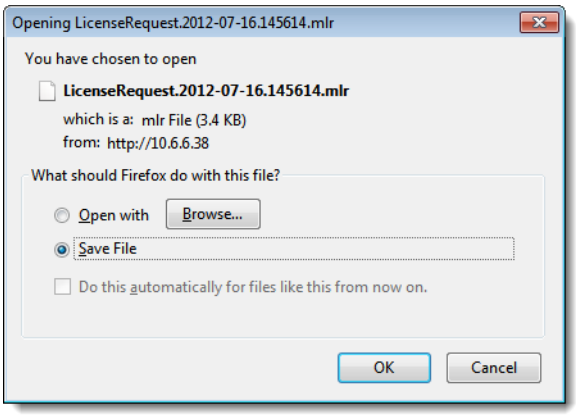
IMPORTANT: System behavior

Network licensing covers those Application Servers that have at least one active license key (not a trial or demo) but that also belong to the original licensing Application Server's subnet.

You may find, however, that there are more servers listed in the License Request confirmation message than you expect. This may be because you have an Auto-failover Redundancy Group configured. If you have activated licenses on at least one Application Server in a configured Redundancy Group, the other servers belonging to the Redundancy Group will be discovered by the Application Server currently making the license request.

For more information about Redundancy Groups, see page 573.

5. If the listed network configuration is satisfactory, click **OK**. If not satisfactory, click **Cancel**. If you clicked **OK**, you are prompted to save the downloaded license request file.



6. Save the MLR file to a convenient location on your hard drive.

7. In your e-mail client application, create a new e-mail with the following recipient:

   `ordering@grassvalley.com`

8. Attach to this e-mail the MLR file you saved to your local hard drive in step 6, and then send the e-mail.

   The request for an activation file is sent to Grass Valley. Wait until Grass Valley provides you with the activation file before proceeding to the next task in the workflow (see [Workflow]: Requesting and Activating Licenses for Several Application Servers, on page 83).

Activating a License

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened the *License Management* page (see page 684).
- You have received an activation file from Grass Valley and it is stored on your client PC's hard drive (either a `V2C` file or a `ZIP` file).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see Sample Workflows, on page 81).

To activate a license

1. On the *License Management* page, in the **Licensed feature activation form** area, click **Browse**.

   A browse window appears.

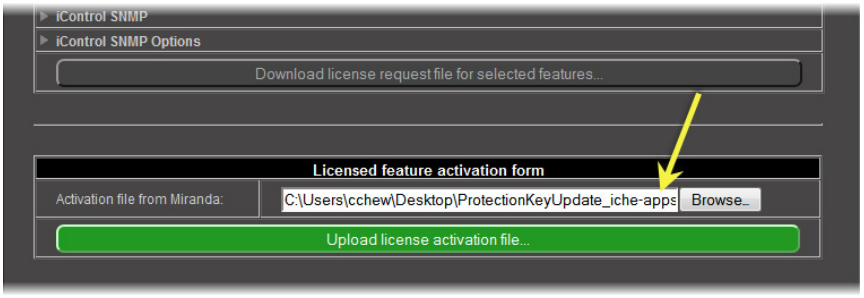
2. Navigate to the directory containing the appropriate activation file.

IMPORTANT: Activation files may be V2C or ZIP files

The file Grass Valley sends back to you may have a `v2c` suffix or a `zip` suffix. In either case, the steps to follow are the same.

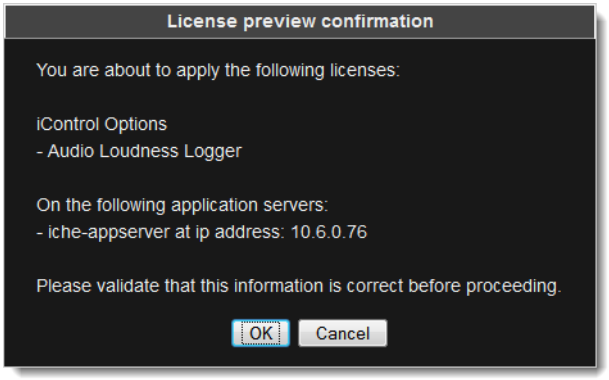
3. Select and then open the file.

   On the *License Management* page, the path and file name of the desired activation file appear next to the **Browse** button.



4. Click **Upload license activation file**.

   A confirmation window appears.

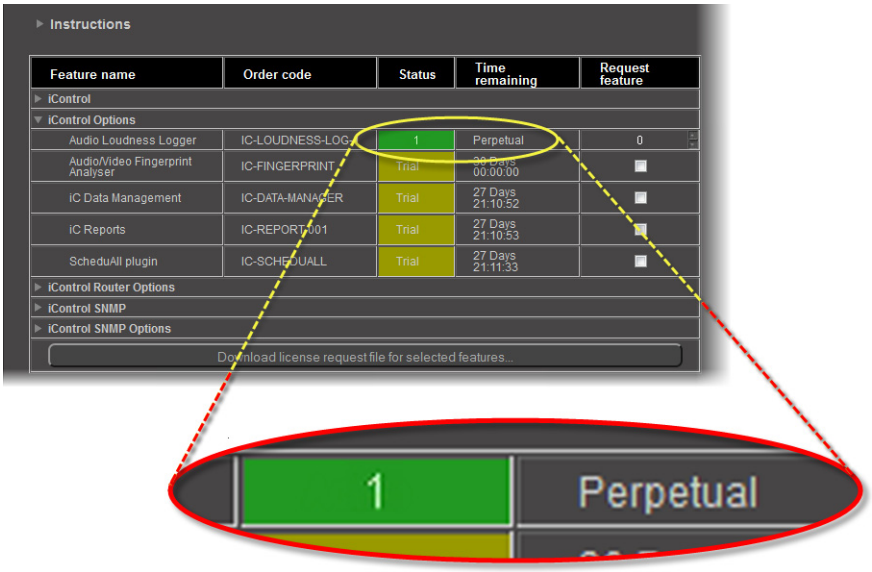


Confirmation showing target server (updating existing key with new features)

5. Verify the list of licenses you are about to apply.
6. If the list of licenses is not **BOTH** correct and complete, click **Cancel** and generate the license request file again (`*.mlr`), being careful to review your choices of features in the checklist (see Requesting a License, on page 84).
7. Once you are satisfied with the list of features, click **OK**.

   A message appears indicating the license activation is complete.
8. Click **OK**.

   On the *License Management* page, the statuses of the features update to reflect the newly-activated licenses.



4 Logs

Summary

Key Concepts

Event

An event in iControl is any occurrence that changes the condition of a monitored element, for example:

- a change in alarm status, including updates to status text
- an acknowledgement
- a change in an alarm's latch status
- a change in an alarm's mode (offline, in maintenance, or online)
- the creation or deletion of a virtual alarm
- the addition or removal of a device
- execution of a script (if the script supports logging)
- a router crosspoint change

> **Note:** Not all events are associated with alarms. For example, if a device driver triggers a reboot, this event might be recorded in the log database with a timestamp, device name, text message, etc., but with no associated alarm information.

Incident

An incident is a grouping of related iControl events. Incidents make it much easier to extract useful information from iControl. Instead of looking for answers in a large list of alarm events, you can have events automatically correlated and grouped into manageable incidents, making it easier to explore the current status of a problem, its root cause, its duration, or its resolution.

Loudness Logging and Analyzing

Certain devices like the Kaleido-Solo are capable of monitoring the loudness of audio streams. The data generated from monitoring may be sent to an Application Server where iControl's *Loudness Logger* can record and archive this stream of loudness data to a dedicated, external drive.

> **Note:** Logging loudness data necessarily involves an external drive in a NAS (network attached storage) environment because loudness log files can grow rapidly in size and number. The storage capacity of an Application Server is inadequate for this purpose.

After (or even during) the logging of loudness data, iControl's **Audio Loudness Analyzer** can plot a log file's data, making it visible in units of LUFS (EBU) or LKFS (A85) over the time period covered by the file. **Audio Loudness Analyzer** allows you to zoom into the data plot as well, effectively taking a subset of the time frame analyzed while increasing data granularity in the chart.

With **Audio Loudness Analyzer**, you may edit analysis parameters as well as showing or hiding certain data plots (e.g., choosing to show or hide the *DIALNORM* and *Short-term Momentary 1* data plots on the chart).

Analysis of Multi-Segment Loudness Logs

Depending on the type of device used to log loudness data (upstream of your Application Server), you may or may not have segment-specific information multiplexed with the loudness data. If the loudness data in your log file consists of many segments (perhaps hundreds), you may wish to generate a multi-segment report over a span of time of your choosing. iControl allows you to do this.

If your loudness log file consists of segments, you may wish to view analysis data with clear demarcations between segments, along with the display of other segment-specific meta-data. This is possible if segment information is included with the loudness data by the source logging device. Alternatively, it is also possible if segment information is available as an external `As-Run` log file.

An `As-Run` log file is a text-based file. There are variations in `As-Run` file types, but these differ from one another only in format and organization of information. Regardless of the file type chosen, all `As-Run` log files are equivalent in function, that being to allow **Audio Loudness Analyzer** to map the `As-Run` file's segment times (and other meta-data) to discrete chunks of loudness data. This effectively allows **Audio Loudness Analyzer** to analyze, display, and report loudness data with segment-level granularity.

See also

For more information about:

- **Loudness Logger**, see page 115.
- **Audio Loudness Analyzer**, see page 116.
- A sample workflow for loudness logging and analyzing, see [Workflow]: Logging and Analyzing Loudness, on page 131.

See also (*Continued*)

For more information about:

- **Audio Loudness Analyzer** [*more detail*] and loudness analysis [*more detail*], see the *Audio Loudness Analyzer User Manual*, available by clicking **Help** in **Audio Loudness Analyzer**.
- The use of `As-Run` log files for parsing discrete segments out of loudness data, see the *Audio Loudness Analyzer User Manual*.

Log Database

Events and incidents in iControl can be recorded in a *log database*. If logging is enabled on an Application Server, the GSM records detailed information, including timestamp, for (potentially) every event in the system. The historical information in the database can help track and identify problems. There is a unique log database for each GSM.

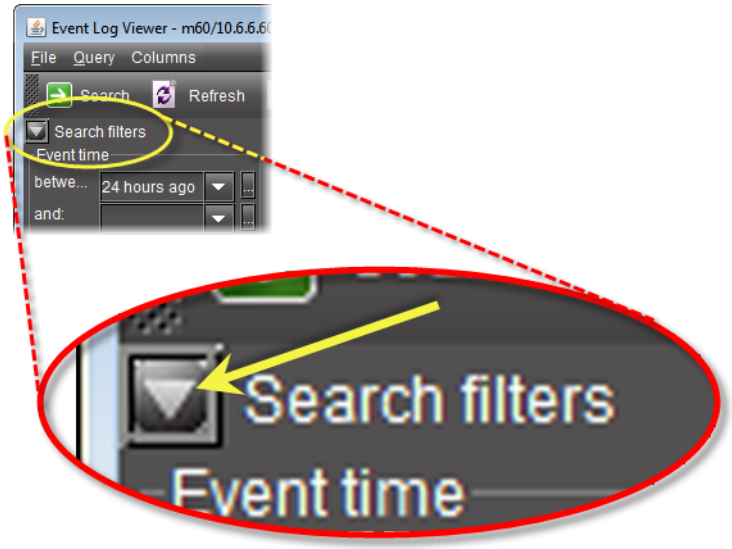
Note: By default, every iControl alarm is configured to be *logged*. It is possible, however, to turn off logging for individual alarms (see Alarm Configuration for Event Logging, on page 125).

Loggers and Log Viewers

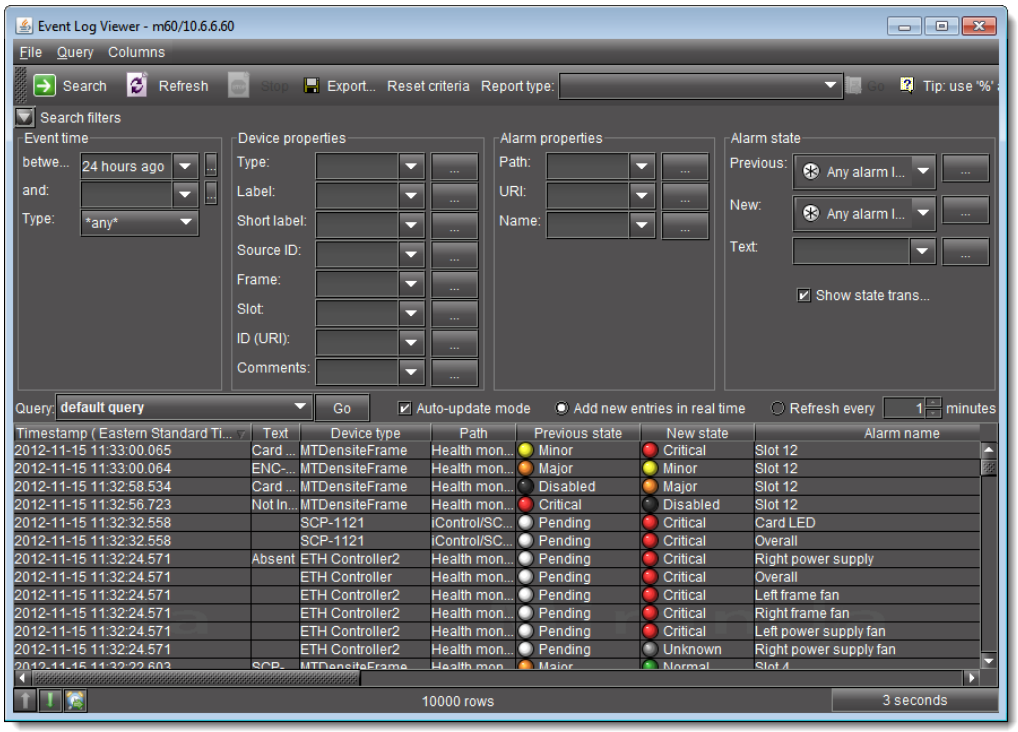
Event Log Viewer

Event Log Viewer is a tool used to search for, sort, and manage records in an iControl log database. **Event Log Viewer** allows you to build queries based on the type of event, the device(s) and alarms involved, the time period, and a variety of other criteria. Query criteria can be saved for reuse. The results of a query, referred to as *records* or *rows* contain detailed information about the events that match the search criteria. Records can be sorted in the log viewer, or exported to a text file.

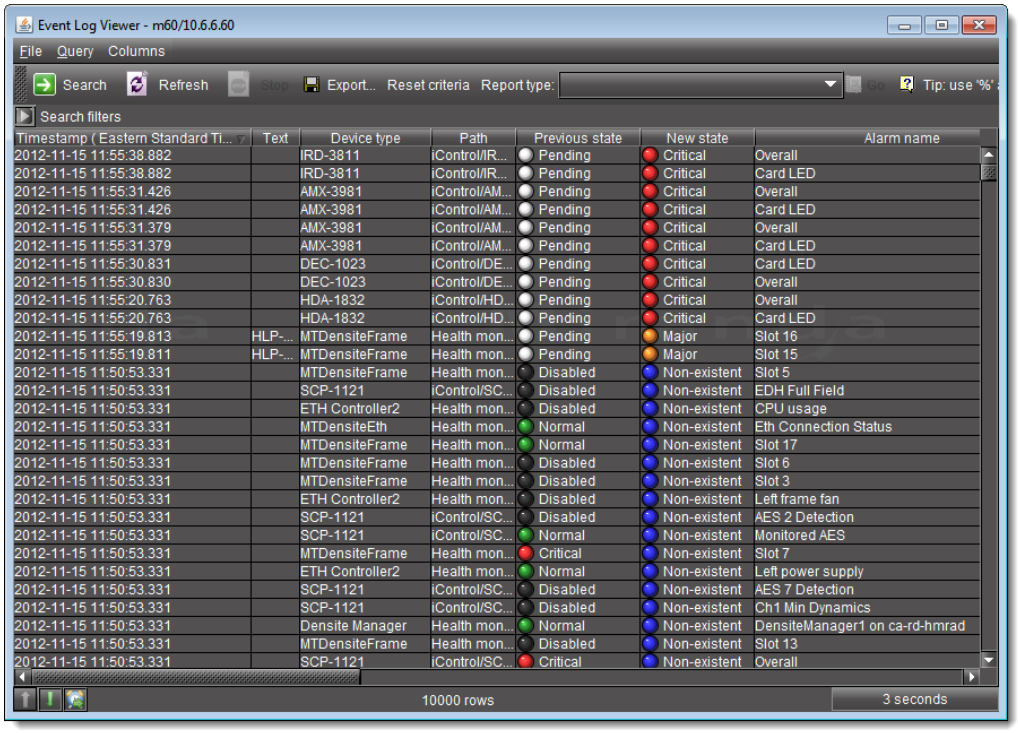
Event Log Viewer allows you to toggle between showing and hiding search filter criteria. By hiding the **Search filters** area, you can significantly increase the number of visible rows in the **Results table**.



Expand/Collapse button for the "Search filters" area



Event Log Viewer with expanded "Search filters" area



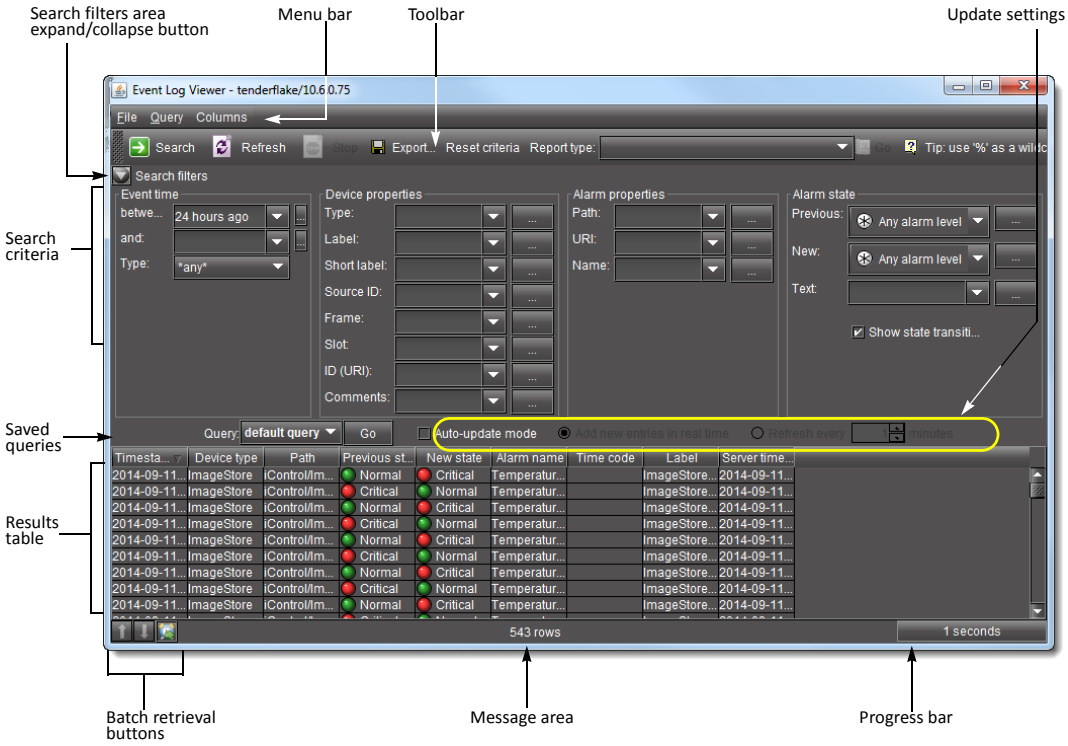
Event Log Viewer with collapsed "Search filters" area

Event Log Viewer also displays device metadata from **iC Navigator**. When you edit any of the device metadata in **iC Navigator**, the system updates the corresponding metadata in the log databases for each discovered GSM. The following is a list of device metadata columns in **Event Log Viewer**:

- Device type
- Label
- Short label
- Source ID
- Comments
- Frame
- Slot
- Path

In addition, you can filter your search using the **Device properties** criteria which correspond to the **iC Navigator** metadata.

The figures and table below describe **Event Log Viewer**.



Timestamp (Eastern Standar...	Device Type	Device ID (URI)
2009-01-05 13:47:04.666 EST	Virtual alarm	virtualAlarm://Cheyenne%2Fgroup26%2Fchannel1831%40V...
2009-01-05 13:47:04.594 EST	DEC-1002	CHEapps3_D16_Densite_SLOT_5_56
2009-01-05 13:47:04.394 EST	Virtual alarm	virtualAlarm://Cheyenne%2Fgroup28%2Fchannel1872%40V...
2009-01-05 13:47:04.385 EST	DEC-1002	CHEapps3_D16_Densite_SLOT_7_56
2009-01-05 13:43:13.840 EST	Virtual alarm	virtualAlarm://Cheyenne%2Fgroup30%2Fchannel1896%40V...
2009-01-05 13:43:13.839 EST	Virtual alarm	virtualAlarm://Cheyenne%2Fgroup8%2Fchannel1546%40Vi...
2009-01-05 13:43:13.839 EST	Virtual alarm	virtualAlarm://Cheyenne%2Fgroup7%2Fchannel1526%40V...

	Path	Previous state	New state	Alarm name	Time co...	Label
hannel1831%40V...	Cheyenne/virtual/overall/video/Gr...	Normal	Critical	Cheyenne/group2...		
	iControl/Logical view/DECs/DEC...	Normal	Critical	White Max		DEC-1002
hannel1872%40V...	Cheyenne/virtual/overall/video/Gr...	Normal	Critical	Cheyenne/group2...		
	iControl/Logical view/DECs/DEC...	Normal	Critical	White Max		DEC-100...

	User	Event type	Previous latch	New latch	Previous ack.	New ack.	Alarm URI	Text	Gsm timestamp
		status	Critical	Critical	Critical	Critical	virtualAlarm...		2009-01-05 13:47:04.679 EST
02		status	Critical	Critical	Critical	Critical	CHEapps3...		2009-01-05 13:47:04.605 EST
		status	Critical	Critical	Critical	Critical	virtualAlarm...		2009-01-05 13:47:04.395 EST
		status	Critical	Critical	Critical	Critical	CHEapps3...		2009-01-05 13:47:04.394 EST

Gsm timestamp	Short label	Source ID	Comments	Frame	Slot
2009-01-05 13:47:04.679 EST					
2009-01-05 13:47:04.605 EST	DEC-1002		10 Bits Composit...	D16	5
2009-01-05 13:47:04.395 EST					
2009-01-05 13:47:04.394 EST	DEC-1002M...	M7m	10 Bits Composit...	D16	7

Additional columns

Main Event Log Viewer

Interface Element	Description
--- ***Toolbar*** ---	
Search	Click to begin a search of the log database using the criteria in the **Event time**, **Device properties**, **Alarm properties** and/or **Alarm state** sections
Refresh	Updates the contents of the log viewer results table (re-executes the previous search using a cached version of the query criteria)
Stop	Stops a search
Export	Saves the results of the current query as a text (CSV) file, which can be opened in a spreadsheet application. The exported file contains data from the currently displayed columns in **Event Log Viewer**, and preserves the sort order.
Reset criteria	Clears the current criteria in the Event time, Device properties, Alarm properties and/or Alarm state sections
--- ***Event time*** --- ***The fields and menus in this section allow you to enter search criteria based on the type of events you are looking for, as well as the period in which they occurred.***	
between	Enter a START date/time for your search, or choose a preset or previously entered date/time from the drop-down menu.
and	Enter an END date/time for your search, or choose a a preset or previously entered date/time from the drop-down menu. Leave this field blank if you wish to search from the START date/time up to the CURRENT date/time.
…	Click the ellipsis […] button to display a calendar, from which you can choose a date and time for the START and/or END of the period in which you wish to search
Type	Choose the type of log entry to search for (status, text, event or any). An event can be anything that has occurred that is not an alarm, like device metadata updates and schedule changes (e.g., ack and unlatch can be events).[1]
--- ***Device properties*** --- ***The fields and menus in this section allow you to enter search criteria based on the properties of the device(s) you are looking for.***	
Type	Choose a device type to search for event logs matching only this criterion.
Label	Choose a device label to search for event logs matching only this criterion.
Short label	Choose a device short label to search for event logs matching only this criterion.
Source ID	Choose a source ID to search for event logs matching only this criterion.
Frame	Choose a frame to search for event logs matching only this criterion.
Slot	Choose a slot to search for event logs matching only this criterion.
ID (URI)	Enter a device's Uniform Resource Identifier (URI)
Comments	Choose a comment to search for event logs matching only this criterion.

Main Event Log Viewer (*Continued*)

Interface Element	Description
--- ***Alarm properties*** --- ***The fields and menus in this section allow you to enter search criteria based on the properties of the alarm(s) you are looking for.***	
Path	Enter an alarm's path (i.e. where it appears in the GSM Alarm Browser hierarchy)
URI	Enter an alarm's URI
Name	Enter an alarm's name
--- ***Alarm state*** --- ***The fields and menus in this section allow you to enter search criteria based on the state (status) of the alarm(s) you are looking for.***	
Previous	Enter the previous status of the alarm(s) you are looking for
New	Enter the new status of the alarm(s) you are looking for
Text	Enter all or part of the text status of the alarm(s) you are looking for
Show state transition only	Select to display only those logged events with changed alarm states **(enabled by default)**
--- ***Query / Update*** ---	
Query	Enter the preset query name whose search criteria you would like to use in a new search.
Go	Click to begin a search of the event log database using the criteria of the query selected in the **Query** box.
Auto-update mode	Select to configure **Event Log Viewer** to automatically refresh the log list.
Update entries in real time	When the **Auto-update mode** check box is selected, the **Update entries in real time** option is no longer grayed out. The real-time refresh option auto-updates the event log list on a real-time basis.[2]
Refresh every 	When the **Auto-update mode** check box is selected, the **Refresh every** option is no longer grayed out. This manual refresh option auto-updates the event log list at the frequency specified in the **Refresh frequency**.[3]
Refresh frequency 	Use the up and down arrows or enter the number of minutes between automatic refreshes of **Event Log Viewer**.
--- ***Columns*** ---	
Timestamp (<Time Zone>)	The date and time at which the event occurred (e.g., `2008-11-04 16:57:54.437`)
Device type	The type of device associated with the event (e.g., `DCP-1721`)
Device ID (URI)	The URI of the device associated with the event (e.g., `App13_d14_Densité_SLOT_6_35`)
Path	The path of the alarm associated with the event (e.g., `iControl/Logical View/UAP_Cards/DCP-1721 (App13_d14_Densité_SLOT_6_35)`)
Previous state	The state of the alarm prior to the event (e.g., `Normal`)

Main Event Log Viewer (*Continued*)

Interface Element	Description
New state	The state of the alarm at the time of the event (e.g., `Critical`)
Alarm name	The user-defined name of the alarm (e.g., `ServiceOverall`)
Time code	The time code associated with the event (if applicable)
Label	The long label of the device associated with the event
User	The IP address of the workstation from which the event was triggered. Available only for certain events, such as the acknowledgement of an alarm.[4]
Event type	The event type (text, status, or event)
Previous latch	The state of an alarm's latch component prior to the event (e.g., `Normal`)
New latch	The state of an alarm's latch component at the time of the event (e.g., `Critical`)
Previous ack.	The state of an alarm's acknowledgement component prior to the event (e.g., `Normal`)
New ack.	The state of an alarm's acknowledgement component at the time of the event (e.g., `Critical`)
Alarm URI	The URI of the alarm associated with the event (e.g., `virtualAlarm://NL-AD-TS_14-80-MAGICFM%40ServiceOverall`)
Text	The text message, if any, associated with the event (e.g., `Card not ready.`)
GSM timestamp	The date and time at which the event was received by the GSM(e.g., `2008-11-05 16:11:54.667 EST`)
Short label	A more compact version of the **Label** column.
Source ID	Descriptive text used to describe the source that goes into the device. Not applicable for some device types.
Comments	Descriptive text used to provide device-specific comments regarding this event.
Frame	A system-assigned value that denotes the frame on which the device is located.
Slot	A system-assigned value that denotes the slot on which the device is located.
<User-defined custom timestamp>	The date and time at which the event occurred in a custom, user-defined time zone.
--- ***Batch retrieval buttons*** ---	
Previous result set 	If the results for the current search exceeds 10000 rows and you have already advanced beyond the first screen, click this button to retrieve the previous screen of results for this search.
Next 10000 results 	If the results for the current search exceeds 10000 rows, click this button to display the next screen (the next 10000 results) for this search.
Results for the next time interval 	Returns a new search result using the time interval for the previous search but starting the time interval at the end of the time interval for the previous search.[5]

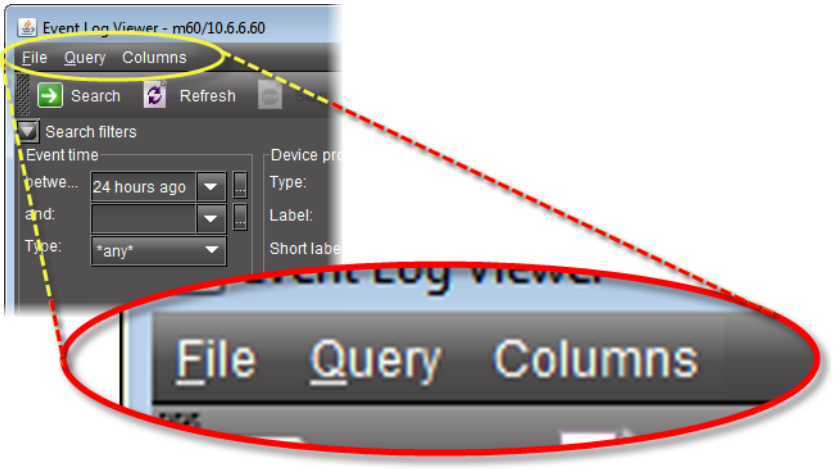
Main Event Log Viewer (*Continued*)

Interface Element	Description
--- ***Bottom Bar*** ---	
Message area	Displays system messages (e.g., `40255 rows found`)
Progress bar	Displays progress of search (% completion)

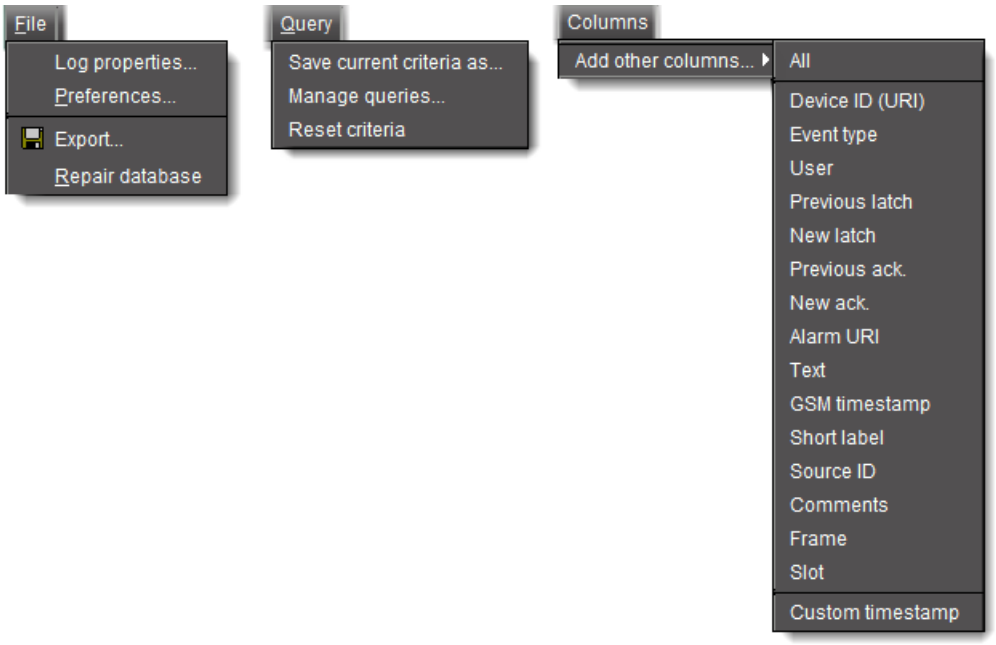
1. An event of type *event* refers to the acknowledgement of an alarm, the setting of an alarm latch, or a driver-specific log entry.
2. The Update entries in real time and Refresh every option buttons are mutually exclusive toggle options (i.e.: when one is selected, the other is not).
3. The Update entries in real time and Refresh every option buttons are mutually exclusive toggle options (i.e.: when one is selected, the other is not).
4. The iControl security module (i.e. user authentication) is not integrated with the log database at this time.
5. An example is if the previous time interval was a 24-hour span from 00:00:00.000 on Sunday to 23:59:59.999 on Sunday, clicking the Next time interval retrieve button returns a new search for a 24-hour time interval starting at 00:00:00.000 on Monday.

Event Log Viewer Menus

Event Log Viewer has three menus: **File**, **Query**, and **Columns**. The menu options are described in the table below.



Event Log Viewer *menu bar*



***Event Log Viewer** menus (expanded)*

Interface Element	Description
--- ***File Menu*** ---	
Log properties	Opens the **Log Properties**
Preferences	Opens the **Preferences**
Export	Opens a file browser, allowing you to name and save the results of the current query as a text (CSV) file, which can be opened in a spreadsheet application. The exported file contains data from the currently displayed columns in **Event Log Viewer**, and preserves the sort order.
Repair database	Repairs the database
--- ***Query Menu*** ---	
Save current criteria as	Allows you to name and save the current criteria in the **Event time**, Device properties, Alarm properties and/or Alarm state sections; the named query appears in the Query menu
Manage queries	Allows you to modify or remove saved queries
Reset criteria	Clears the current criteria in the Event time, Device properties, Alarm properties and/or Alarm state sections
--- ***Columns Menu*** ---	
Add other columns	Allows you to display additional columns in the results table; as you add columns, they are removed from this menu (and vice versa)[1]

1. To add a custom, user-defined timestamp column, click **Custom Timestamp**.

Event Log Viewer Shortcut Menu

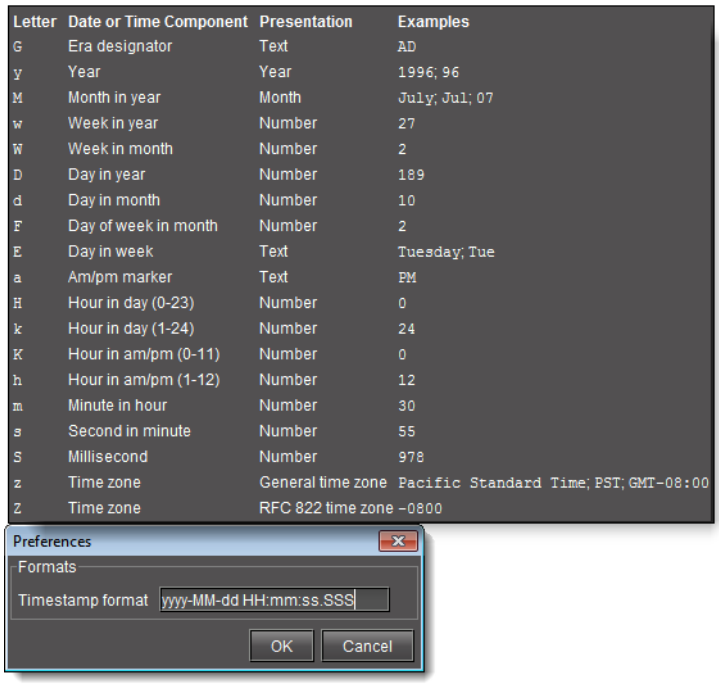
A shortcut menu is displayed when you right-click on a row in the results table of **Event Log Viewer**. The menu options are described in the table below.

Menu Item	Description
Remove [name] column from view	Allows you to remove columns from the results table; as you remove columns, they are added to the **Add other columns** menu
Add to search criteria	Adds the value you right-clicked to the current search criteria and retrieves items matching the updated criteria (that is, the current search criteria are further constrained by the addition of this new filter).[1]
Search with this value only	Replaces the current search criteria with only the value you right-clicked and retrieves items matching the updated criteria.[2]
Add other columns	Allows you to display additional columns in the results table; as you add columns, they are removed from this menu (and vice versa).[3]
Create incident template	Opens **New Incident Template**, allowing you to create an incident template based on the currently selected event(s).

1. When you right-click to get your shortcut menu, make sure you right-click directly over the value (the intersection of the event row with the desired column) you wish to use in your search criteria.
2. When you right-click to get your shortcut menu, make sure you right-click directly over the value (the intersection of the event row with the desired column) you wish to use in your search criteria.
3. To add a custom, user-defined timestamp column, click **Custom Timestamp**.

Event Log Viewer Preferences

Event Log Viewer preferences allow you to specify a display format for the time stamp associated with each log entry. When this window appears, a popup legend also appears listing possible values for the Timestamp format field.



Letter	Date or Time Component	Presentation	Examples
G	Era designator	Text	AD
y	Year	Year	1996; 96
M	Month in year	Month	July; Jul; 07
w	Week in year	Number	27
W	Week in month	Number	2
D	Day in year	Number	189
d	Day in month	Number	10
F	Day of week in month	Number	2
E	Day in week	Text	Tuesday; Tue
a	Am/pm marker	Text	PM
H	Hour in day (0-23)	Number	0
k	Hour in day (1-24)	Number	24
K	Hour in am/pm (0-11)	Number	0
h	Hour in am/pm (1-12)	Number	12
m	Minute in hour	Number	30
s	Second in minute	Number	55
S	Millisecond	Number	978
z	Time zone	General time zone	Pacific Standard Time; PST; GMT-08:00
Z	Time zone	RFC 822 time zone	-0800

The default time stamp format is `yyyy-MM-dd HH:mm:ss.SSS`, where each letter represents a character of a specific time stamp component. Dashes, periods, spaces and other characters are used to separate the elements of the time stamp.

So, as an example, for an event logged at one millisecond before 6:00 p.m. on August 21st, 2007, the default syntax would result in the following time stamp:

`2007-08-21 17:59:59.999`

The table below lists the elements that can be used to build a time stamp format:

Letter	Date or Time Component	Presentation	Examples
G	Era designator	Text	AD
Y	Year	Year	2007 (YYYY), 07 (YY)
M	Month in year	Month	August (MMMM), Aug (MMM), 08 (MM)
w	Week in year	Number	27
W	Week in month	Number	2
D	Day in year	Number	189
d	Day in month	Number	10
F	Day of week in month	Number	2
E	Day in week	Text	Tuesday (EEEE), Tue (EEE)
a	Am/pm marker	Text	PM
H	Hour in day (0-23)	Number	0

(*Continued*)

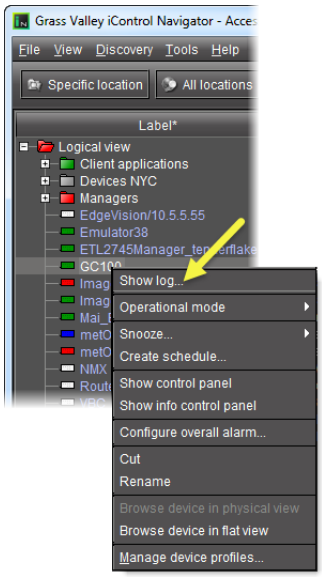
Letter	Date or Time Component	Presentation	Examples
k	Hour in day (1-24)	Number	`24`
K	Hour in am/pm (0-11)	Number	`0`
h	Hour in am/pm (1-12)	Number	`12`
m	Minute in hour	Number	`30`
s	Second in minute	Number	`55`
S	Millisecond	Number	`978`
z	Time zone	General time zone	`Pacific Standard Time (zzzz), PST (z)`
Z	Time zone	RFC 822 time zone	`-0800`

Device-Specific Event Log Viewer

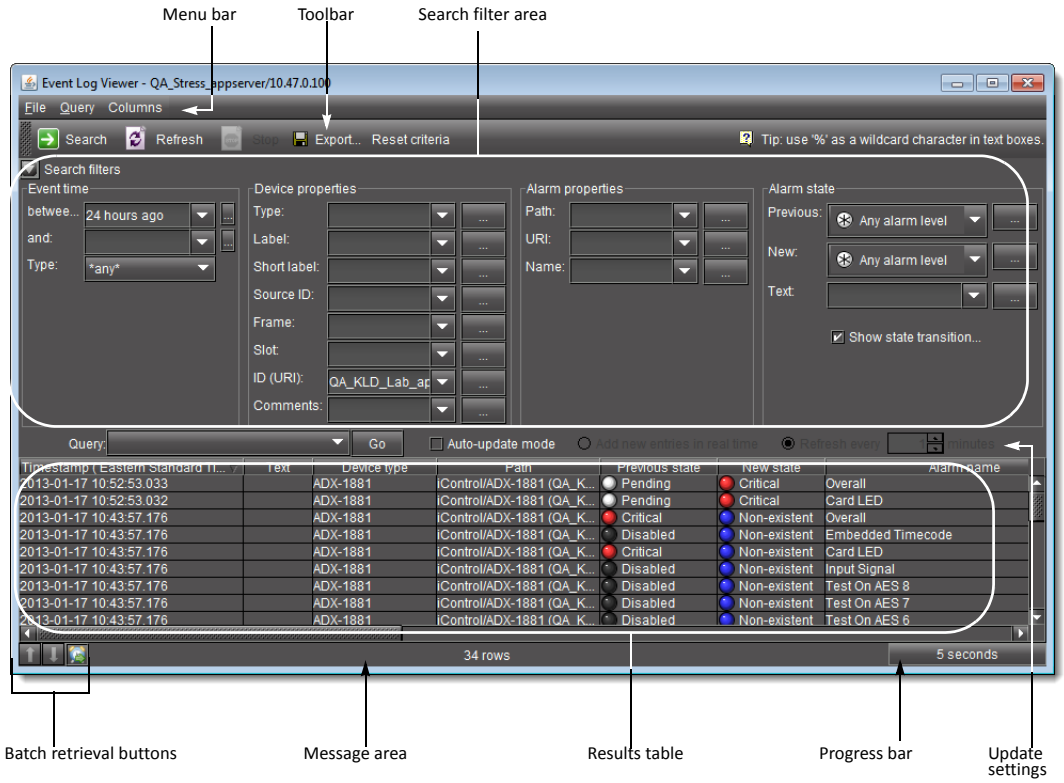
In **iC Navigator** and **iC Web**, you can access **Event Log Viewer** in the context of a particular device. When you open **Event Log Viewer** in a device-specific context, only events particular to that device are visible.

The device-specific **Event Log Viewer** uses the same interface as the main event log viewer (see Event Log Viewer, on page 93).

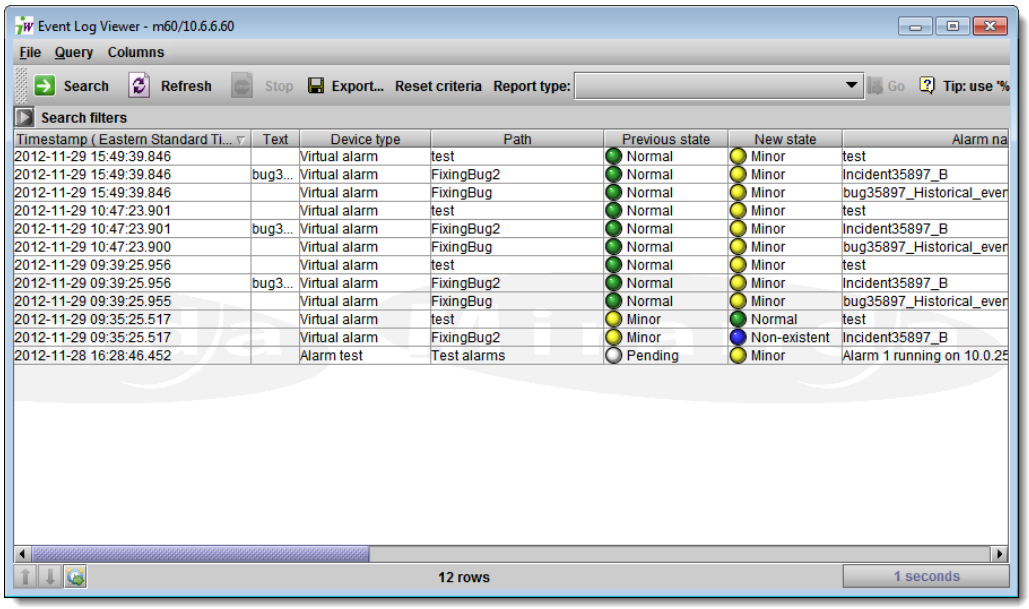
The device-specific **Event Log Viewer** can be displayed by right-clicking on a device (in **iC Navigator** or on a Web page) and clicking **Show Log** (in **iC Navigator**) or **Show status log** (in **iC Web**).



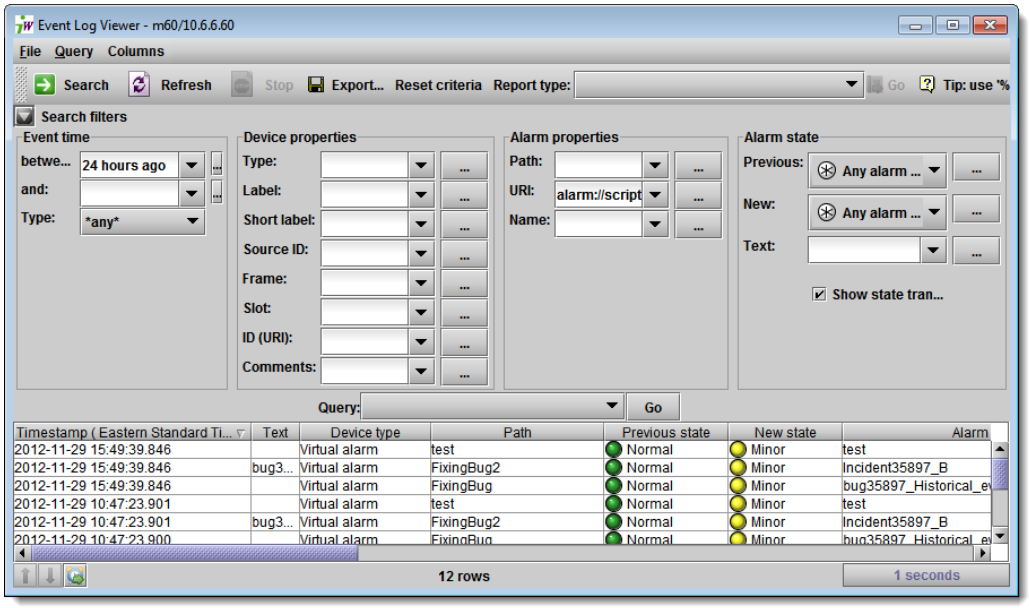
*Navigating to the device-specific **Event Log Viewer** in **iC Navigator***



*Device-specific **Event Log Viewer** as seen from **iC Navigator***

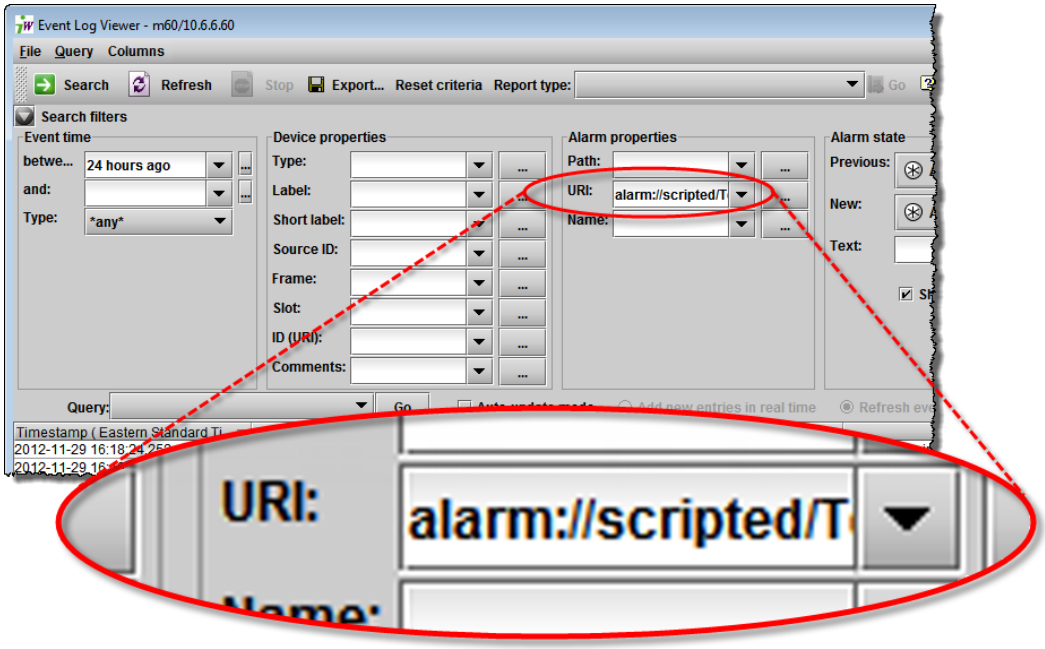


*Device-specific **Event Log Viewer** in **iC Web** (Search filters area collapsed)*



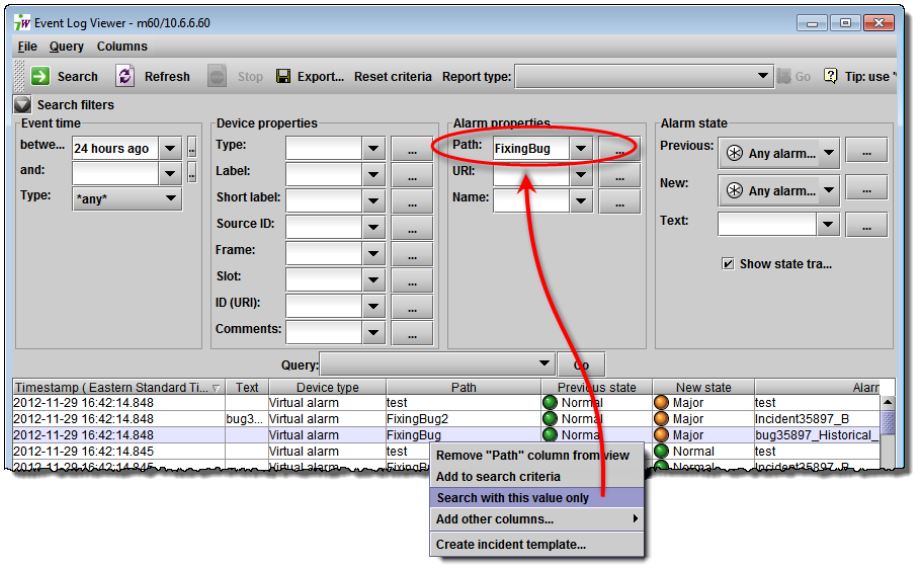
*Device-specific **Event Log Viewer** in **iC Web** (Search filters area expanded)*

If the context is a *virtual* alarm, the **URI** field — under **Alarm properties** in the **Search filters** area — is automatically populated with the URI of that virtual alarm.

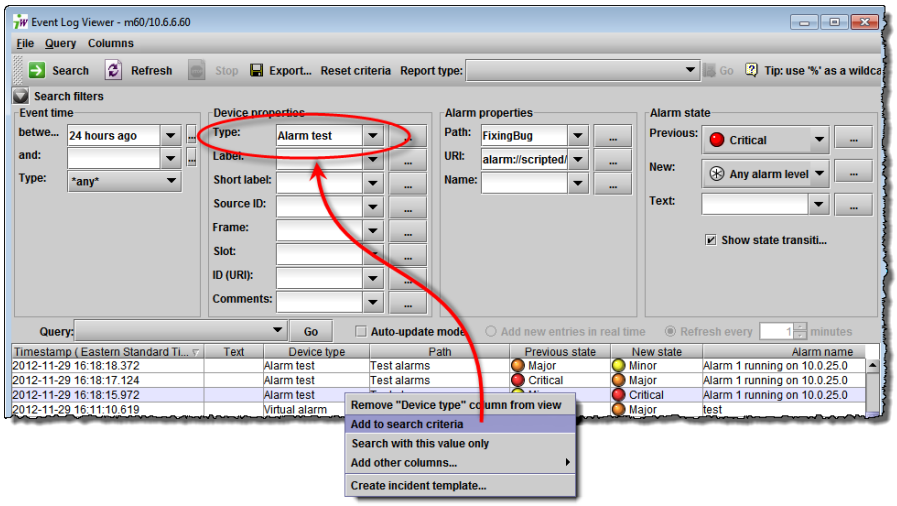


*Pre-populated URI search field for virtual alarm (context-sensitive **Event Log Viewer**)*

Additionally, in the device-specific **Event Log Viewer**, by taking advantage of the search filter features of the standard Log Viewer window, you can use any parameter of any listed log entry as either a solitary search criterion or else to be added to the existing search criteria of the current filter simply by right-clicking any cell of any log listing.



*Using the **Search with this value only** feature in the context-sensitive Log Viewer*



*Using the **Add to search criterion** feature in the context-sensitive Log Viewer*

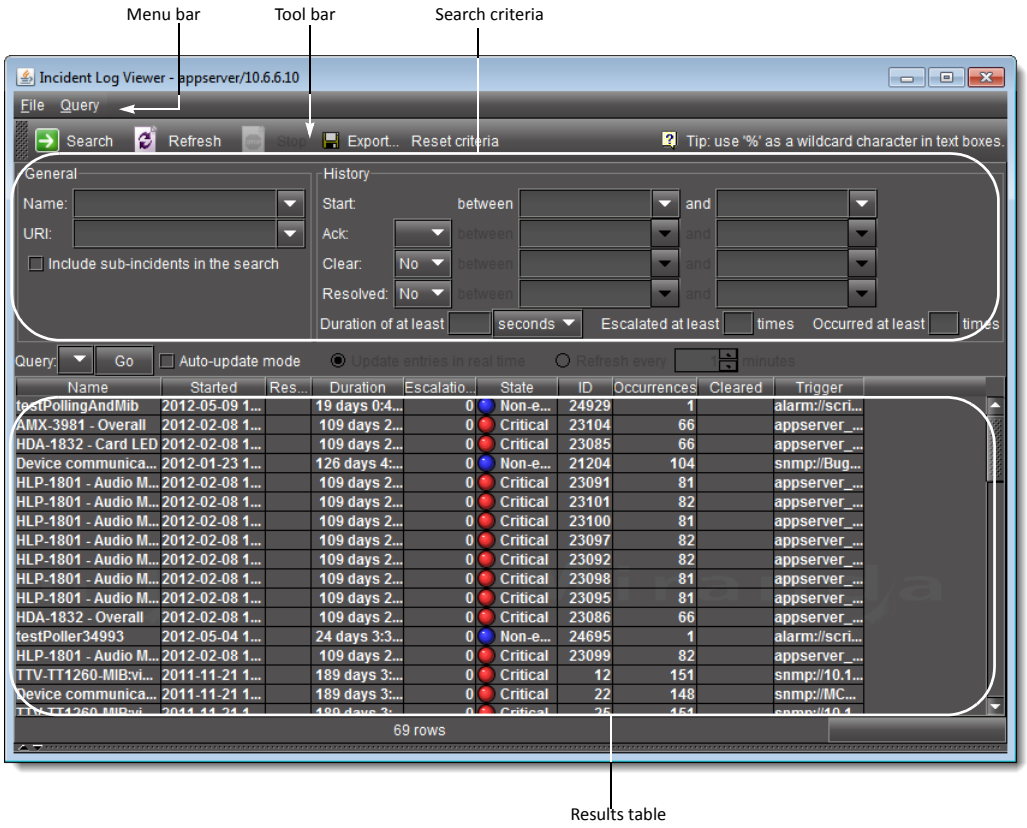
> **Note:** If the context of a context-sensitive **Event Log Viewer** is a *virtual* alarm, the **URI** field — under **Alarm properties** in the **Search filters** area — is automatically populated with the URI of that virtual alarm.

Incident Log Viewer

Incident Log Viewer is used to browse and manage *incidents*, which are groupings of multiple events. With **Incident Log Viewer**, you can view details of an incident, add comments to qualify it, acknowledge the incident and its associated alarms (so that your colleagues know someone is working on the problem), escalate the incident to a higher-level user, and more.

Entries listed in the results table of **Incident Log Viewer** are color-coded, based on their respective status, to help discriminate among them:

- New (or unacknowledged) incident entries appear in **bold** text.
- Acknowledged Incident entries appear in regular text.
- Cleared incident entries appear in gray text.
- Child (consolidated/linked) incidents appear in smaller text.



Note: If you right-click on any one of the **State**, **Occurrences**, or **Status** columns, the resulting Shortcut menu does not include the items **Add to search criteria** nor **Search with this value only**.

Interface Element	Description
--- ***Toolbar*** ---	
Search	Click to begin a search of the incident log database using the criteria in the **General** and/or **History** sections
Refresh	Updates the contents of the **Incident Log Viewer** results table (re-executes the previous search using a cached version of the query criteria)

(*Continued*)

Interface Element	Description
Stop	Stops the active search
Delete all	Deletes the results of the current search (all found rows) from the database
Export	Saves the results of the current query as a text (CSV) file, which can be opened in a spreadsheet application. The exported file contains data from the currently displayed columns in **Incident Log Viewer**, and preserves the sort order.
Reset criteria	Clears the current search criteria.
--- ***General*** --- ***The fields and menus in this section allow you to enter search criteria based on the general characteristics of the incidents you are looking for.***	
Name	Enter the name of the incident you are searching for.
URI	Enter the Uniform Resource Identifier (URI) of the incident you are searching for.
Include sub-incidents	Select this check box to include sub-incidents in the search.
--- ***History*** --- ***The fields and menus in this section allow you to enter search criteria based on the history of incidents you are looking for, as well as their escalation level.***	
Start	Specify a date/time interval to be searched for incidents. Enter a starting point in the **between** field, or choose a preset value from the menu (**30 hrs**, **24 hrs**, **1 week**, or**1 month ago**). Enter an ending point in the **and** field, or choose a value from the menu (**now**, **30 minutes**, **24 hours**, **1 week**, or **1 month ago**).[1]
Ack	Specify how the *acknowledgement* status of an incident is to be considered in the search. From the menu, choose **Yes** to find only acknowledged incidents, **No** to find only unacknowledged incidents, or leave blank to find both. Enter a starting point in the **between** field, or choose a preset value from the menu (**30 hrs**, **24 hrs**, **1 week**, or**1 month ago**). Enter an ending point in the **and** field, or choose a preset value from the menu (**now**, **30 minutes**, **24 hours**, **1 week**, or **1 month ago**).
Clear	Specify how the **cleared** status of an incident is to be considered in the search. From the menu, choose **Yes** to find only cleared incidents, **No** to find only incidents not yet cleared, or leave blank to find both. Enter a starting point in the **between** field, or choose a preset value from the menu (**30 hrs**, **24 hrs**, **1 week**, or**1 month ago**). Enter an ending point in the **and** field, or choose a preset value from the menu (**now**, **30 minutes**, **24 hours**, **1 week**, or **1 month ago**).
Resolved	Specify how the **resolved** status of an incident is to be considered in the search. From the menu, choose **Yes** to find only cleared incidents, **No** to find only incidents not yet cleared, or leave blank to find both. Enter a starting point in the **between** field, or choose a preset value from the menu (**30 hrs**, **24 hrs**, **1 week**, or**1 month ago**). Enter an ending point in the **and** field, or choose a preset value from the menu (**now**, **30 minutes**, **24 hours**, **1 week**, or **1 month ago**).
Duration of at least	Specify a minimum incident duration for the search.
Escalated at least [..] times	Specify a minimum number of incident escalations for the search.

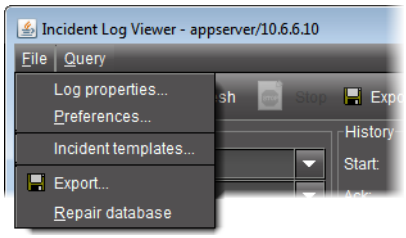
(*Continued*)

Interface Element	Description
Occurred at least [..] times	Specify a minimum number of times an open incident's trigger has changed state from *normal* to *fault* for the search.
--- ***Query / Update*** ---	
Query	Enter the preset query name whose search criteria you would like to use in a new search.
Go	Click to begin a search of the incident log database using the criteria of the query selected in the **Query** box.
Auto-update mode	Select to configure the **Incident Log Viewer** to automatically refresh the log list.
Update entries in real time	When the `Auto-update mode` check box is selected, the **Update entries in real time** option is no longer grayed out. The real-time refresh option auto-updates the incident log list on a real-time basis.[2]
Refresh every 	When the **Auto-update mode** check box is selected, the **Refresh every** option is no longer grayed out. This manual refresh option auto-updates the incident log list at the frequency specified in the **Refresh frequency**.[3]
Refresh frequency 	Use the up and down arrows or enter the number of minutes between automatic refreshes of **Incident Log Viewer**.
--- ***Columns*** ---	
Name	The user-defined name of the incident
Started	The creation date and time of the incident
Acknowledged	The date and time when the incident was last acknowledged – empty if not acknowledged
Resolved	The date and time when the incident was resolved (based on the virtual alarm linked to the incident template) – empty if not resolved
Cleared	The date and time when the incident was cleared – empty if not cleared
Duration	The interval between the date and time of creation and of resolution for an incident, or the elapsed time since its creation.
Escalations	The number of times an incident has been escalated
State	The state of the virtual alarm associated with the incident template
ID	The unique ID of the incident
Occurrences	The number of times an open incident's trigger has changed state from *normal* to *fault*
Status	The status of the incident (**New**, **Acknowledged**, **Cleared** or **Acknowledged+Cleared**)
Trigger	The URI of the incident template that triggered an incident

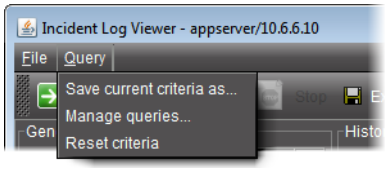
1. The **between** and **and** menus for **Ack**, **Clear**, and **Resolved** (see below) are used in a similar way.
2. The Update entries in real time and Refresh every option buttons are mutually exclusive toggle options (i.e.: when one is selected, the other is not).
3. The **Update entries in real time** and **Refresh every option** buttons are mutually exclusive toggle options (i.e.: when one is selected, the other is not).

Incident Log Viewer Menus

Incident Log Viewer has two menus.



*File menu on **Incident Log Viewer***

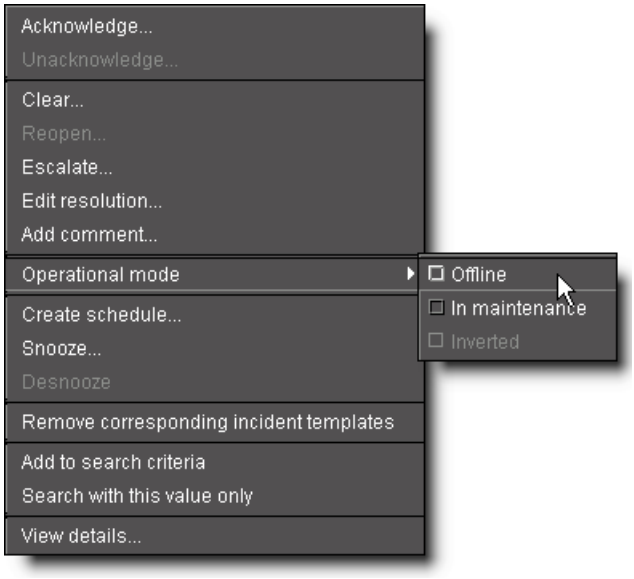


*Query menu on **Incident Log Viewer***

Interface Element	Description
--- ***File Menu*** ---	
Log properties	Opens the **Event and incident log configuration** window
Preferences	Opens the **Preferences** window
Incident templates	Opens the **Incident Templates** window
Export	Opens a file browser, allowing you to name and save the results of the current query as a text (*.CSV) file, which can be opened in a spreadsheet application. The exported file contains data from the currently displayed columns in **Event Log Viewer**, and preserves the sort order.
Repair database	Repairs the database
--- ***Query Menu*** ---	
Save current criteria as	Saves the current criteria as a stored query under a user-definable name
Manage queries	Opens the **Manage queries** window
Reset criteria	Resets the default query so that no query executes when the viewer is opened

Incident Log Viewer Shortcut Menu

A shortcut menu is displayed when you right-click on an incident entry in **Incident Log Viewer**. The menu options are described in the table below.



Menu Item	Description
Acknowledge	Opens a window allowing you to acknowledge the currently selected incident and enter a comment.
Unacknowledge	Opens a window allowing you to unacknowledge the currently selected incident and enter a comment.
Clear	Opens a window allowing you to clear the currently selected incident and enter a comment. The color of the text in the row corresponding to the cleared incident changes to gray. Only resolved incidents can be cleared.
Reopen	Opens a window allowing you to reopen the currently selected (cleared) incident and enter a comment.
Escalate	Opens a window allowing you to escalate the currently selected incident and enter a comment.
Edit Resolution	Opens a window allowing you to enter comments associated with the resolution of the currently selected incident.
Add Comment	Opens a window allowing you to enter a comment about the currently selected incident, without an associated action.
Operational mode	Point to **Operational mode**, and then click **Offline**, **In maintenance**, or **Inverted** to change the operational state of the incident.
Create schedule	Create a schedule for alarm suppression
Snooze	Temporarily suppresses alarms associated with the selected incident (see Alarm Operational Modes, on page 358)
Desnooze	Removes alarms associated with the selected incident from *snooze* mode
Remove corresponding incident templates	Allows you to remove incident templates from **Incident Log Viewer**.

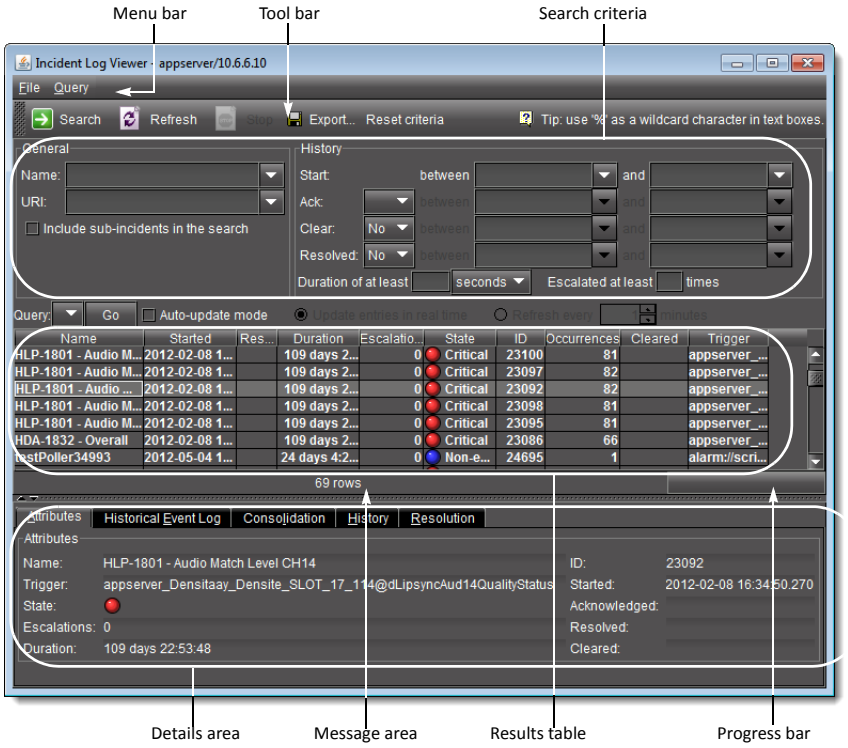
(*Continued*)

Menu Item	Description
Add to search criteria	Adds the value you right-clicked to the current search criteria and retrieves items matching the updated criteria (that is, the current search criteria are further constrained by the addition of this new filter).[1]
Search with this value only	Replaces the current search criteria with only the value you right-clicked and retrieves items matching the updated criteria.[2]
View details	Displays detailed information about the currently selected incident

1. When you right-click to get your shortcut menu, make sure you right-click directly over the value (the intersection of the event row with the desired column) you wish to use in your search criteria.
2. When you right-click to get your shortcut menu, make sure you right-click directly over the value (the intersection of the event row with the desired column) you wish to use in your search criteria.

Incident Log Viewer — Details

When you first open **Incident Log Viewer**, only the **Search criteria** and **Results table** areas are visible, There is another area that is used to display detailed information about an individual incident. The **Incident details** area can be made visible either by double-clicking an incident in the **Results table**, or by right-clicking on it and clicking **View details**.



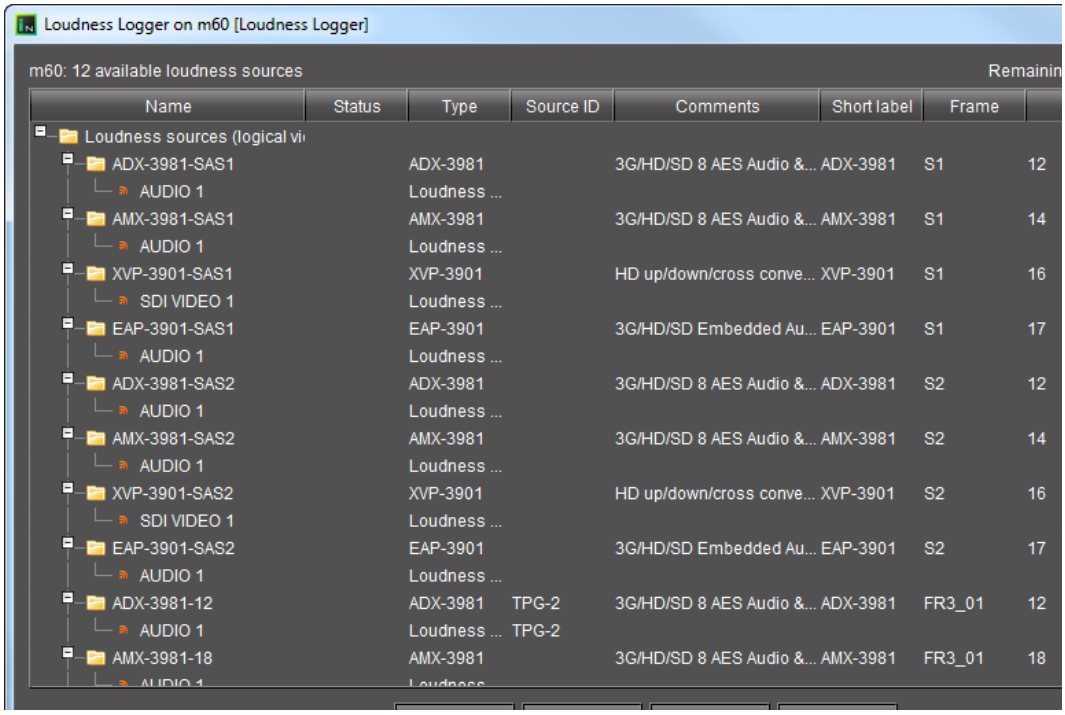
Interface Element	Description
--- ***Attributes*** --- ***Shows the attributes of the currently selected incident***	
Name	The name of the currently selected incident
Trigger	The URI of the incident template that triggered the currently selected incident
State	The overall alarm for the currently selected incident. This is a virtual alarm, created automatically, that summarizes the statuses of the alarms for all of events contributing to this incident
Escalations	The number of times the currently selected incident has been escalated
Duration	The time elapsed since the currently selected incident was first created. For cleared incidents, this parameter represents the elapsed time between the incident's creation and the moment it was cleared.
ID	The unique ID of the currently selected incident
Started	The creation date and time of the currently selected incident
Acknowledged	The date and time at which the currently selected incident was last acknowledged
Resolved	The date and time at which the currently selected incident was resolved
Cleared	The date and time at which the currently selected incident was cleared
--- ***Historical Event Log*** --- ***Shows the alarm events associated with the currently selected incident.***[1]	
Primitive alarms only	Select to filter the events so that only primitive alarms are displayed.
Last occurrences only	Select to display only the last occurrence of each alarm.
Refresh	Click to refresh the contents of the **Events** tab if you made changes to the search criteria (see above), or to scan the log database, again, for updates.
Current Status Decomposition Shows the composition of the incident templates thereby allowing users to find the root causes of individual incidents.	
Consolidation Shows the incidents that have been consolidated under the currently selected incident. You can drag-and-drop incidents from the **Results** table into the **Sub-incidents** area to consolidate them.[2]	
History Shows the history of the actions and comments associated with the currently selected incident.	
Resolution Shows the actions and comments associated with the resolution of the currently selected incident.	

1. For a description of the columns in this section, see Event Log Viewer, on page 93.
2. For a description of the columns in this section, see Incident Log Viewer, on page 107.

Loudness Logger

Loudness Logger allows you to start and stop the logging of loudness data streams coming from external audio sources, such as Kaleido-Solo. When you initiate logging of a loudness data stream, you are streaming the data to a log file on a remote drive.

> **Note:** Prior to the logging operation, you must mount the remote drive to the designated loudness directory on the Application Server.



Loudness Logger

UI Element	Description
Main window	Displays available loudness data streams
Refresh	Refreshes the main window
Start all	Starts logging all available loudness data streams
Stop all	Stops logging all available loudness data streams
Settings	Allows you to: • mount the remote drive to the loudness directory on the Application Server • configure loudness alarm settings

IMPORTANT: Make sure you have sufficient storage space for loudness data

When specifying a location for storing loudness data, make sure you have enough storage space available. If, when logging loudness data, the logger runs out of space, it will stop logging (

Differential bit rate of loudness raw data from various devices

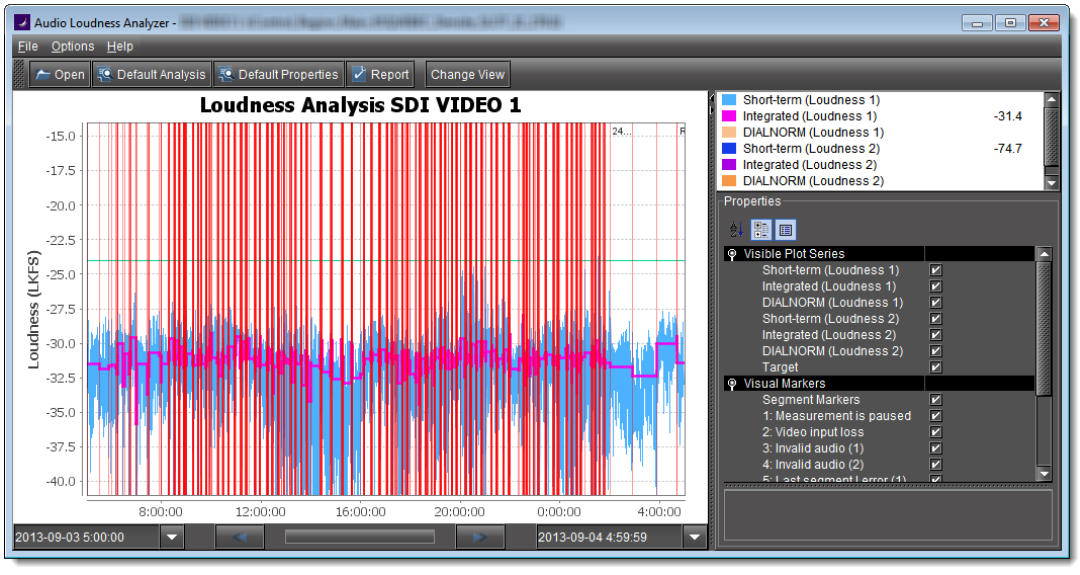
Device	Number of audio programs	Bitrate (Bytes/second)	Bitrate (MB/day)
KS-910	1-2	170-210	14.7-18.2
XVP-3901	1-8	170-450	14.7-39
EAP-3901	1-8	170-450	14.7-39
AMX-3981	1-8	170-450	14.7-39
ADX-3981	1-8	170-450	14.7-39

See also

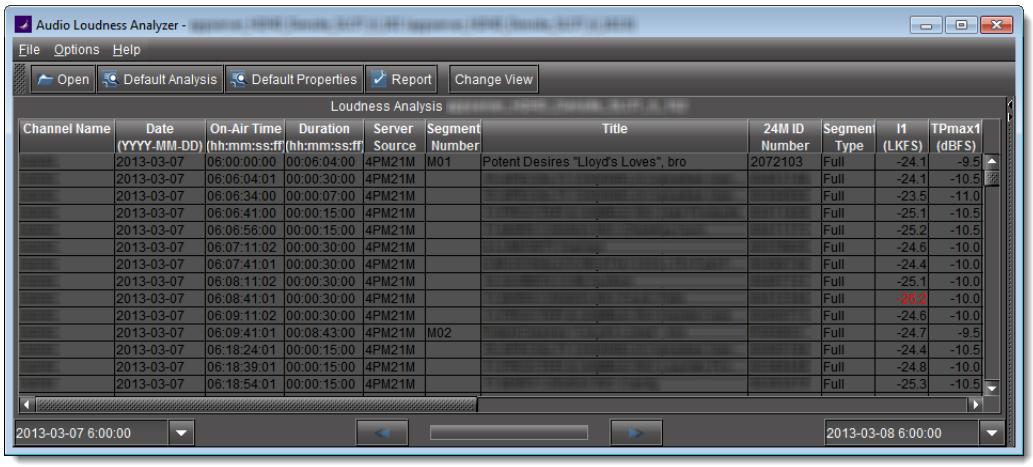
For more information about:

- Loudness logging and analyzing, see page 92.
- A sample workflow for loudness logging and analyzing, see [Workflow]: Logging and Analyzing Loudness, on page 131.

Audio Loudness Analyzer



***Plot** view of Audio Loudness Analyzer*



***Tabular** view of Audio Loudness Analyzer*

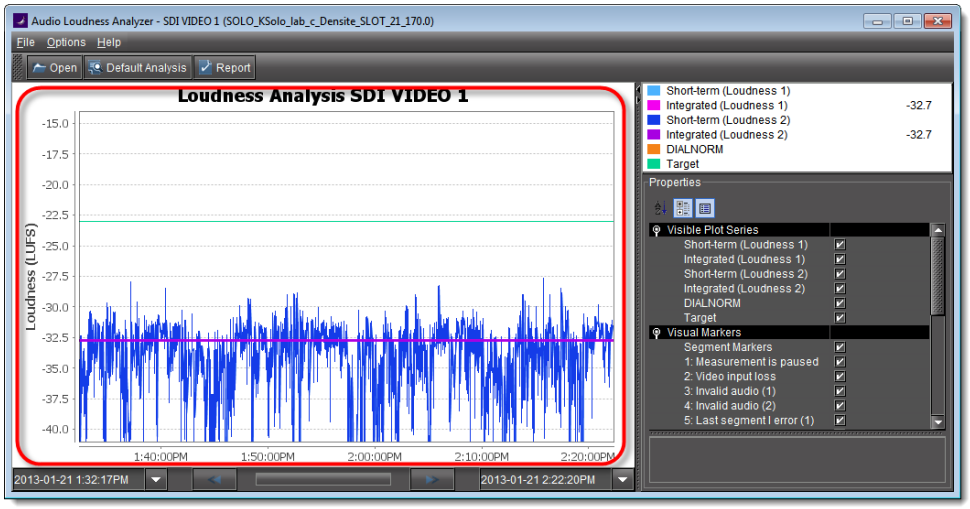
Audio Loudness Analyzer is a powerful tool for graphically depicting an audio source's loudness data over a period of time. The power of this tool lies primarily in its configurability of analysis parameters, including the applicable loudness standard, relative gating, and short-term window. As well, **Audio Loudness Analyzer** allows you to *zoom into* a data plot. Each zooming action triggers a new analysis of loudness data from source, for the requested time period (configurable start and stop times) and given the configured analysis parameters.

Additionally, one can choose to incrementally display or hide plot series. For example, you may decide to display only *Short-term Momentary 1*, *Integrated Momentary 1*, and *DIALNORM* data while hiding the remaining series in order to unencumber the visual chart. See the following figures for detailed views of **Audio Loudness Analyzer**:

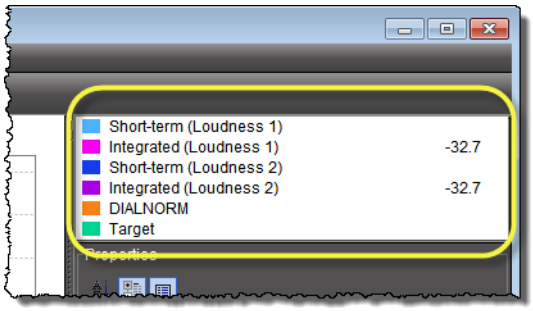
See also

For more information about:

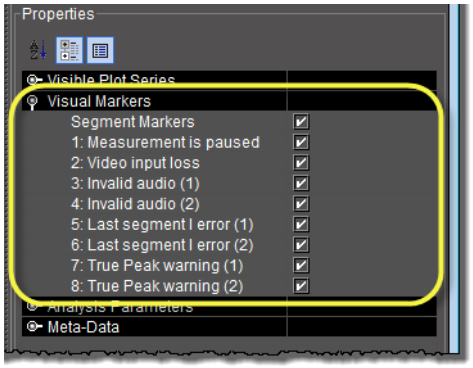
- Loudness logging and analyzing [*descriptive information*], see page 92.
- A sample workflow for loudness logging and analyzing, see [Workflow]: Logging and Analyzing Loudness, on page 131.
- **Audio Loudness Analyzer** [*more detail*] and loudness analysis [*more detail*], see the *Audio Loudness Analyzer User Manual*, available by clicking **Help** in **Audio Loudness Analyzer**.
- The use of `As-Run` log files for parsing discrete segments out of loudness data, see the *Audio Loudness Analyzer User Manual*.



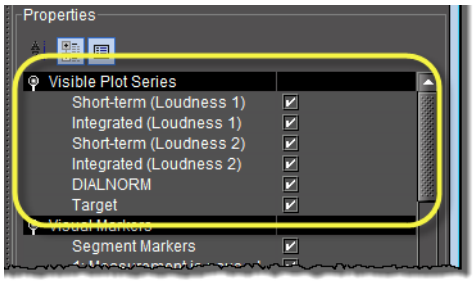
Data plot chart (circled in red)



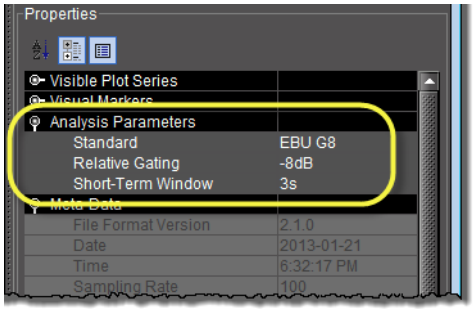
Visible plot series: Color-coded legend and values



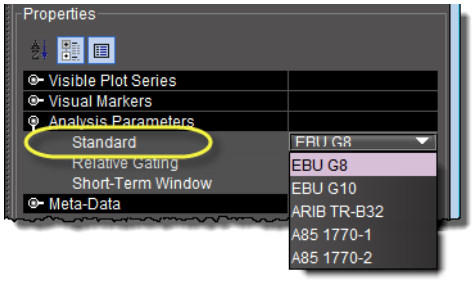
Visual Markers: Display options



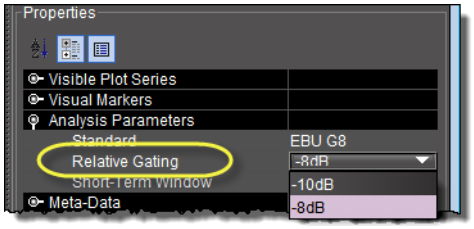
Visible plot series: Display options



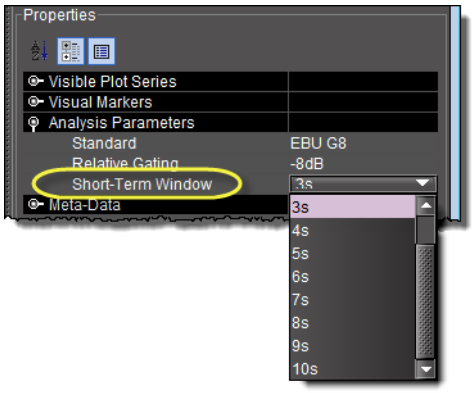
Properties: Analysis parameters



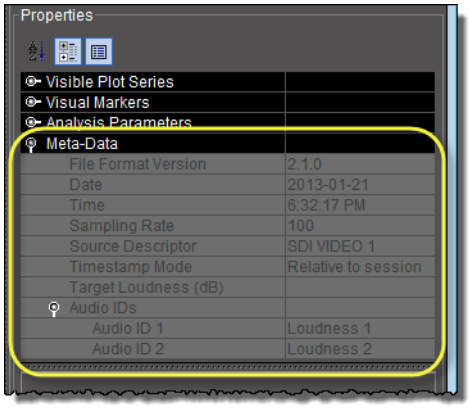
Properties: Analysis parameters (available standards)



Properties: Analysis parameters (relative gating)



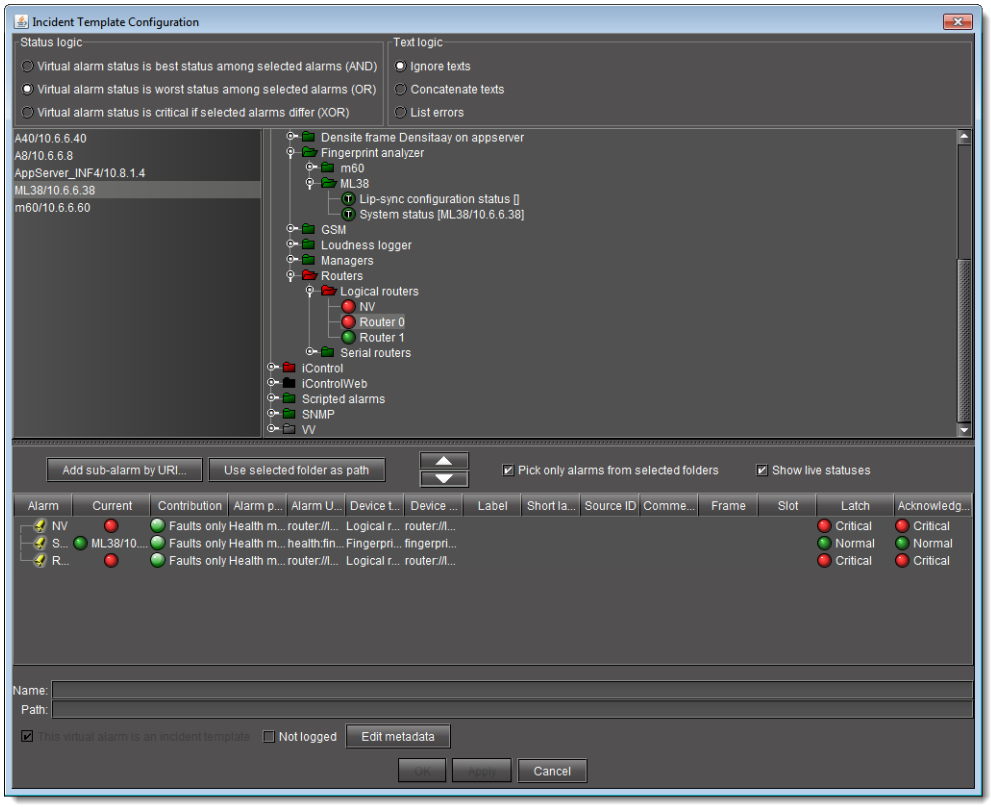
Properties: Analysis parameters (short-term window)



Meta-data (not editable)

Incident Template Configuration

The **Incident template configuration** window is similar to **Build Virtual Alarm** (see Working with Virtual Alarms, on page 399), but is customized for creating or editing an incident.



Interface Element	Description
--- ***Status Logic***[1] ---	
--- ***Text Logic***[2] ---	
--- ***GSM Alarm Browser*** --- ***This section allows you to choose a GSM and specific alarm to use when building or modifying an incident template.***	
--- ***Incident template elements*** --- ***This section is used to assemble, view and/or modify incident template elements.***	
Add sub-alarm by URI	Allows you to add an alarm to the table of incident template components by specifying its URI.
Use selected folder as path	Copies the path of the currently selected item in the GSM Alarm Browser to the **Path** field (see below).
Edit metadata	Allows you to edit a virtual alarm's metadata.
Up arrow 	Click this arrow to remove currently selected rows from the table of incident template components.

(*Continued*)

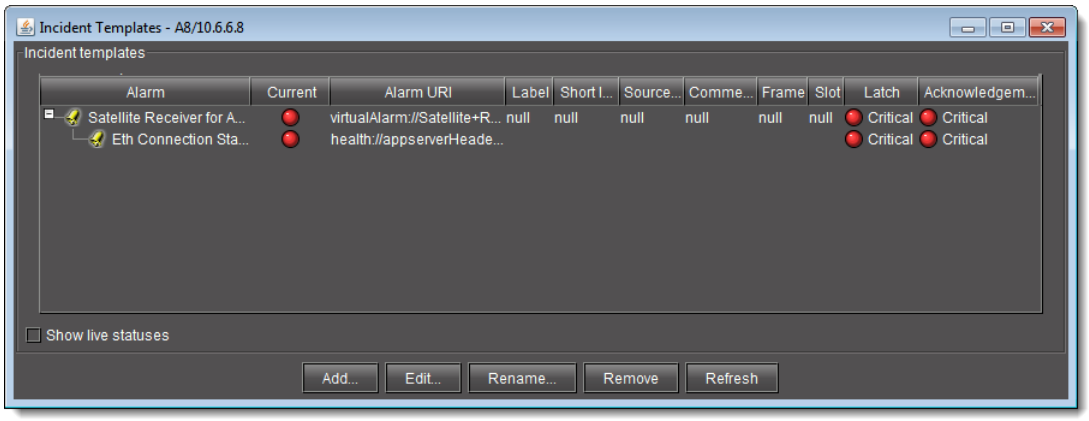
Interface Element	Description
Down arrow 	Click this arrow to add alarms currently selected in the GSM Alarm Browser to the table of incident template components.
Pick only alarms from selected folders	Select this check box to select only alarms that are descendants of a selected folder when pressing the down arrow button. If this check box is cleared, each selected folder is added to the bottom pane.
Show live statuses	Select this check box to see real-time alarm status updating
--- ***Columns*** --- ***The columns in the table containing the incident template components are described below:***	
Alarm	The name of the alarm mapped to the incident template.
Current	The current status of the alarm mapped to the incident template.
Contribution	The contribution of the alarm mapped to the incident template.[3]
Alarm path	The path of the alarm in the GSM Alarm Browser.
Alarm URI	The URI of the alarm mapped to the incident template.
Device type	The type of device with which the alarm is associated.
Device URI	The URI of the device with which the alarm is associated.
Label	An operator-friendly name for a device.
Short label	A more compact version of the **Label** column.
Source ID	A name used to describe the source that goes into the device (not applicable for some device types).
Comments	Device-specific comments.
Frame	A system-assigned value that denotes the frame on which the device is located.
Slot	A system-assigned value that denotes the slot on which the device is located.
--- ***Other*** ---	
Name	Enter a name for the incident template.
Path	Enter a path for the incident template. This is where the template's overall alarm will appear in the GSM Alarm Browser hierarchy. If you leave this field blank, the overall alarm will appear in the **Virtual alarms** folder.
This virtual alarm is an incident template	Select this check box to make the new virtual alarm into an incident template. If this check box is cleared, the new virtual alarm will be a regular virtual alarm.
OK	Click to create a new incident template using the current settings.
Apply	Click to create a new incident template using the current settings without closing the window.
Cancel	Click to close the window without applying the current settings.

1. This section is disabled. By default, Incident Templates employ *optimistic* (AND) logic (see Alarm Logic Tables, on page 354)
2. This section is disabled.

3. The contribution cannot be changed.

Incident Template Management

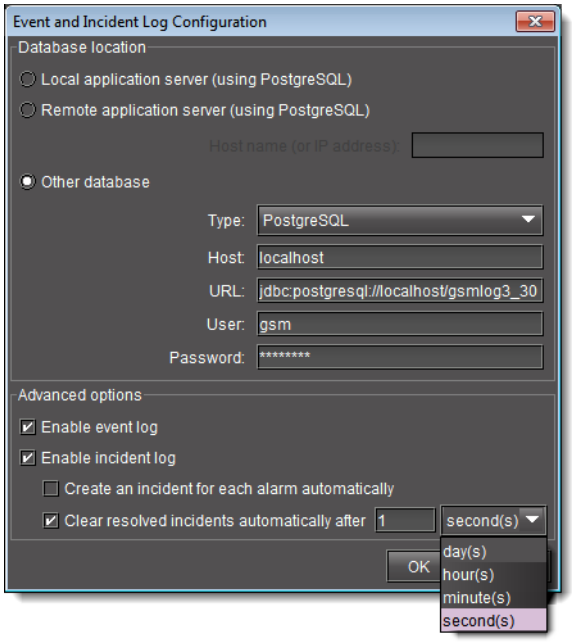
The **Incident templates** window is used to create, modify, and manage incident templates.



Interface Element	Description
--- ***Incident templates*** --- ***This section displays the currently active incident templates along with their overall alarm statuses. Click the [+] and [–] symbols beside each incident name to show or hide its subalarms.***	
Show live statuses	Select this check box to see real-time alarm status updating
Add	Click to display the **Incident template configuration** window (see Incident Template Configuration, on page 120)
Edit	Click to display the **Incident template configuration** window with the currently selected template settings (see Incident Template Configuration, on page 120)
Rename	Click to display a window allowing you to rename the currently selected incident template. **Warning:** Changing the incident template's name will also update all incidents that use the template. Archived incidents will not be updated.
Remove	Click to delete the currently selected incident template.
Refresh	Click to refresh the display.

Event & Incident Log Configuration

The **Event and Incident log configuration** window is used to set up the log database, as well as to enable the logging of events and incidents.



Note: When **Create an incident for each alarm automatically** is selected, new faults trigger incidents only if their attributes are accepted by the filters. The filters are specified by a configurable file and take effect only after GSM restarts.

Interface Element	Description
--- ***Database location*** ---	
Local application server	Click here to specify the use of the log database on the local Application Server (the one from which you opened **Event Log Viewer**). This is the most commonly used setting, where you intend to explore the log database on the same Application Server from which you open **Event Log Viewer** or **Incident Log Viewer**:
Remote application server	Click here to specify the use of the log database on a remote Application Server. This setting should be used when you intend to explore the log database on an Application Server other than the one from which you open **Event Log Viewer** or **Incident Log Viewer**:
Host name (or IP address)	Enter the host name or IP address of the remote Application Server
Other database	Click here to use a log database on a remote Application Server. This setting serves essentially the same purpose as Remote Application Server, except that it allows you to identify the remote database in greater detail. It is intended for advanced users only:
Type	Choose a database type (MySQL or PostgreSQL).[1]
Host	Enter the host name or IP address of the Application Server where the database is located (changing this field will automatically change the address field).

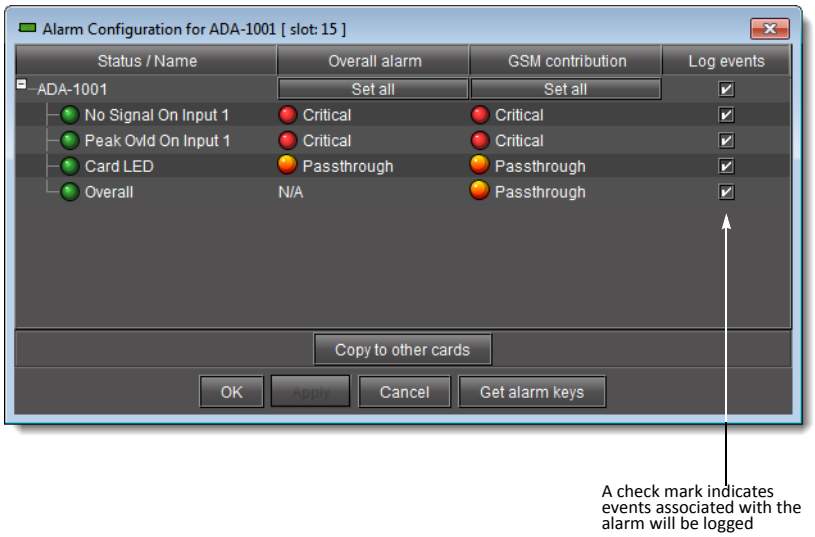
(*Continued*)

Interface Element	Description
URL	The location of the remote database—this value is automatically filled in based on the values in the **Type** and **Host** fields, but can be edited.
User	Enter a valid user name for access to the remote database.
Password	Enter a valid password for access to the remote database.
--- ***Advanced Options*** ---	
Enable event log	Select to have the GSM begin recording events in the log database.
Enable incident log	Select to have the GSM begin recording incidents in the log database.[2]
Create an incident for each alarm automatically	Select to generate a new incident for each alarm whenever its status changes to *minor*, *major*, or *critical*. When this option is checked, the Incident Viewer becomes a global viewer for all current faults in the current GSM.[3]
Clear resolved incidents automatically after	Select to automatically clear an incident if it has been resolved for the specified amount of time.[4]

1. Support for MySQL has not yet been implemented.
2. The incident log depends on the event log, so both options must be enabled.
3. This option is selected by default.
4. When an incident is cleared automatically, the corresponding alarm latch is also reset, which is not desirable in most situations. As of iControl version 3.31, this option is not selected by default. This does not affect existing configurations.

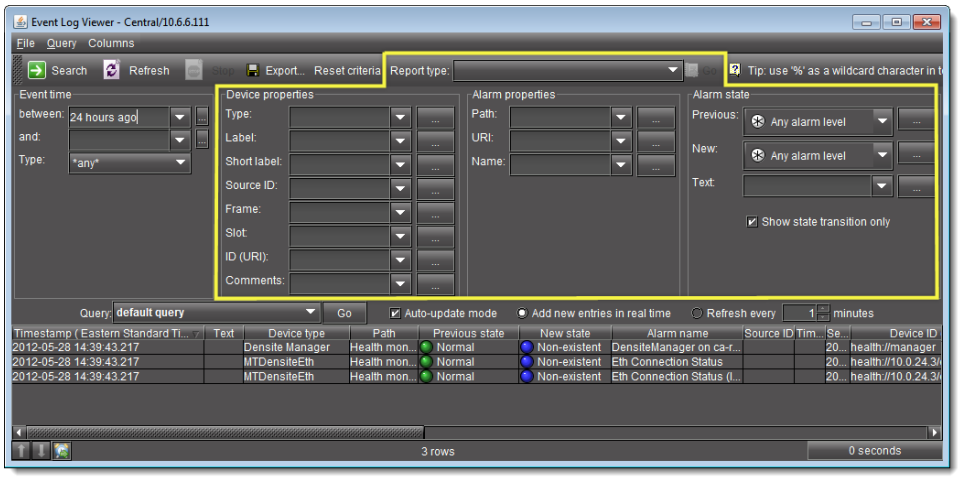
Alarm Configuration for Event Logging

By default, all alarm events in iControl are recorded in the log database (when logging is enabled). You can, however, change the default settings. For individual cards, this is done by opening the card's control panel (see Control Panels and Device Parameters, on page 225).

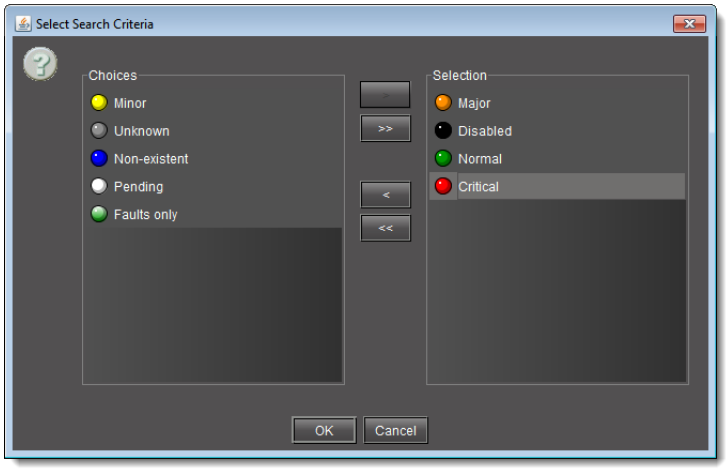


iControl Reports

iC Reports is a database reporter that allows you to connect to an Application Server's *postgreSQL* database and generate graphical reports of channel performance statistics. By using **Event Log Viewer**'s new multiple selection mechanism, you can define the parameters and scope of your report templates. In addition, iC Reports includes several default report templates you may want to use as is, or as a starting point to create your own user-defined version.



*iControl Reports area of **iC Navigator**'s **Event Log Viewer***



***Event Log Viewer**'s multiple selection mechanism*

If you don't need to create a report template, you can view a list of existing report templates and delete them, as well as generate, view, download, and delete reports, all from the *Reports* page.

Notes

- All report templates and reports listed on the *Reports* page are stored on the Application Server you are logged in to.

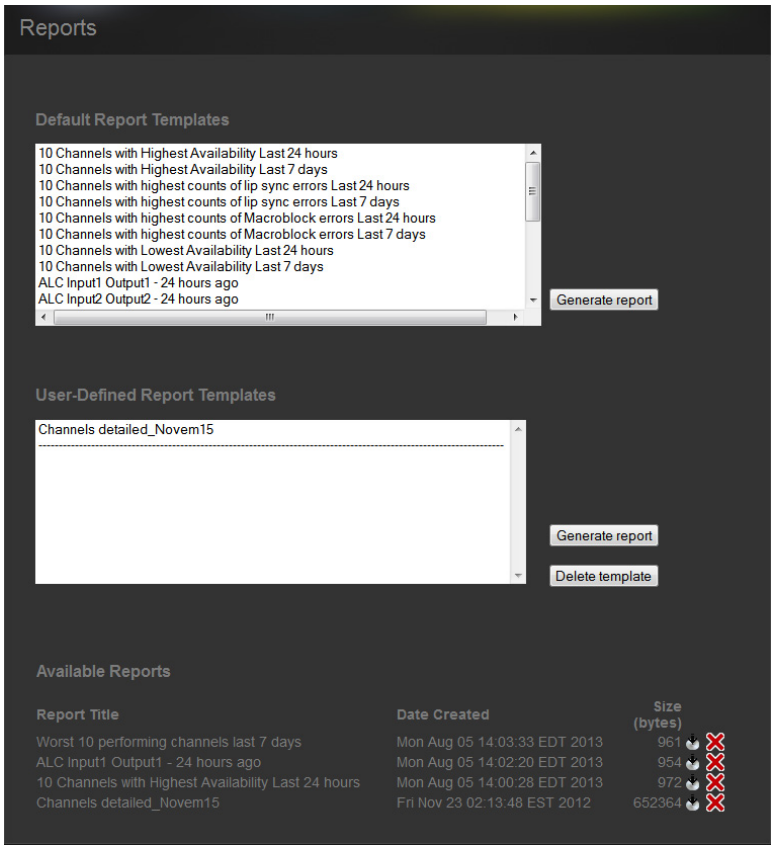
Notes (*Continued*)

- Downloaded reports are PDF files.

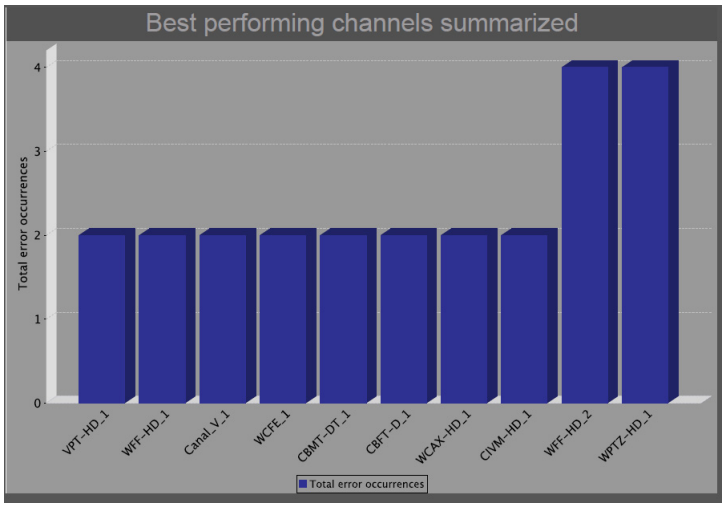
See also

For more information about:

- **Event Log Viewer**'s new multiple selection mechanism, see Filtering a Log Search Using Multiple Criteria, on page 143.
- Performing iC Reports user tasks, see Creating, Viewing, and Deleting Channel Performance Reports, on page 207.



Reports page of iControl



Generated report - HTML

GSM Log Files

You can download and view the latest and historic GSM log files stored on an Application Server. These log files are in the comma-separated-values (CSV) format. Consequently, you may use Microsoft Excel—among other programs—to view the contents of these files.

In terms of how the data within a GSM log file is organized, please refer to the following table for proper interpretation.

Legend of GSM log files

Column position	Column name	Type	Description
a	*Timestamp*	Integer	Timestamp as logged by device Integer represents the timestamp in milliseconds starting at midnight GMT, January 1st, 1970
b	*GSM timestamp*	Integer	Timestamp as logged by GSM upon reception of alarm from device Integer represents the timestamp in milliseconds starting at midnight GMT, January 1st, 1970
c	*Alarm URI*	Text	Alarm identifier For example: `10.0.24.81_dept_Densite_SLOT_19_102`
d	*Alarm name*	Text	Alarm friendly name For example: `Overall`
e	*Device URI*	Text	The identifier of the device that generated the alarm For example: `10.0.44.14_HH_Densite_SLOT_5_102`
f	*Device Type*	Text	The type of device to which the alarm is associated For example: `XVP-3901`

Legend of GSM log files (*Continued*)

Column position	Column name	Type	Description
g	*Alarm type*	Integer	For internal use only
h	*Username*	Text	Host name of client PC if alarm transition is caused by a user action (ex. alarm acknowledged, alarm unlatched) If Access control is activated, then this will contain a user name instead of a host name.
i	*Path*	Text	The path of the alarm in the GSM For example: `iControl/XVP-3901 (10.0.44.14_HH_Densite_SLOT_17_102)/User Defaults/Audio Processing/Fixed Delays`
j	*Previous state*	Integer	Previous state of the alarm[1]
k	*New state*	Integer	Current alarm state[1]
l	*Previous latch*	Integer	Previous state of the latched alarm[1]
m	*New latch*	Integer	Current state of the latched alarm[1]
n	*Previous ack.*	Integer	Previous state of the acknowledged alarm[1]
o	*New ack.*	Integer	Current state of the acknowledged alarm[1]
p	*Previous mode*	Integer	Previous alarm operating mode[1]
q	*New Operating mode*	Integer	Current alarm operating mode[1]
r	*Timecode*	Integer	Timecode as generated by device -1 = no timecode value provided
s	*Text*	Text	Text alarm current textual value For example: `[A8/10.6.6.8, iche-appserver/10.6.0.76,m60/10.6.6.60, mike-appserver/10.6.0.75,ML38/10.6.6.38]`

1. Please see Possible column values for a GSM log file, on page 129.

Possible column values for a GSM log file

Value	Description
--- ***Columns J, K, L, M, N, and O*** ---	
10	NORMAL
20	MINOR
25	MAJOR
30	CRITICAL
40	UNKNOWN

Possible column values for a GSM log file (*Continued*)

Value	Description
-1	DISABLED
-4	PENDING
-3	NON-EXISTENT
--- ***Columns P and Q*** ---	
0	No operating mode specified
1	Offline
2	Maintenance
4	Snooze
8	Inverted

See also

For more information about retrieving GSM log files, see page 216.

Sample Workflows

[Workflow]: Channel Performance Reporting

The Application Server database reporter allows you to connect to the Application Server database and generate reports and accompanying graphs of channel performance statistics.

A sample workflow, starting with designing a report template and finishing with viewing a report, is as follows:

Workflow: Channel Performance Reporting

1.	If you plan to use any of the four *Availability* default report templates[1] in this workflow, configure the Application Server's SQL Event Log plug-in to clear resolved incidents automatically after 1 second (see Enabling and Disabling the Automatic Incident Resolution Function for iC Reports, on page 207).
2.	Distinguish the alarms associated with the desired channels from other alarms by building a virtual alarm (see Creating a Virtual Alarm to Filter Out Non-Channel Alarms (iC Reports), on page 404).
3.	Open **Event Log Viewer** on the Application Server whose database you would like a report of (see page 697).
4.	Configure filtering criteria in the Log Viewer's report fields to fine-tune the report parameters. See: • Filtering a Log Search Using Multiple Criteria on page 143 • Filtering a Log Search using a Log's Textual Elements as Criteria on page 148

Workflow: Channel Performance Reporting (*Continued*)

5.	Perform one of the following two tasks: • Create a new report template to customize the filtering parameters of your reports, then generate a report (see Creating a Report Template, on page 208). • Select an existing report template to generate a report (see page 210).
6.	If desired, display the report in a Web browser (see page 211).
7.	If desired, download the report as a PDF file (see page 212).
8.	If space is an issue on your Application Server database, and you no longer require the use of any of the *Availability* default report templates, disable the SQL Event Log Plug-in's automatic incident clearing functionality (see Enabling and Disabling the Automatic Incident Resolution Function for iC Reports, on page 207).

1. The *Availability* default report templates are as follows: 10 Channels with Highest Availability Last 24 hours, 10 Channels with Highest Availability Last 7 days, 10 Channels with Lowest Availability Last 24 hours, 10 Channels with Lowest Availability Last 7 days

See also

For more information about iC Reports, see page 126.

[Workflow]: Logging and Analyzing Loudness

There are several tasks you can perform related to both logging and analyzing loudness data in iControl. Certainly, before you do anything else, you must make sure your system is properly configured. You must also make sure you log before you analyze. While the sequence of these tasks may seem obvious, the sequence of other required tasks may not be. The following is an approved workflow for configuring, logging, and analyzing loudness data in iControl.

Sample workflow: Logging and analyzing loudness

1.	Mount an external NAS drive to your Application Server (see page 184).
2.	**[OPTIONAL]** Map the external NAS drive onto your client PC (see your Windows® documentation).
3.	Start the *Loudness Logger* and *Loudness Analyzer* services (see page 183).
4.	Open **Loudness Logger** (see page 704).
5.	Configure desired event-logging settings for loudness alarms (see page 201).
6.	Log loudness data for the desired audio stream (see Logging an Audio Stream's Loudness Data, on page 188).
7.	Stop the loudness log recording (see page 189).
8.	Open **Audio Loudness Analyzer** (see page 705).
9.	Configure general **Audio Loudness Analyzer** settings (see page 190).
10.	Open a loudness log file (see page 196).

Sample workflow: Logging and analyzing loudness (*Continued*)

11.	**[OPTIONAL]** Zoom into **Audio Loudness Analyzer**'s data plot (see page 203).
12.	**[OPTIONAL]** Configure loudness analysis parameters for this data plot (see page 200).
13.	**[OPTIONAL]** Generate a loudness analysis report (see page 205).

See also

For more information about:

- Logging and analyzing loudness data [*descriptive information*], see page 92.
- **Loudness Logger**, see page 115.
- **Audio Loudness Analyzer**, see page 116.
- **Audio Loudness Analyzer** [*more detail*] and loudness analysis [*more detail*], see the *Audio Loudness Analyzer User Manual*, available by clicking **Help** in **Audio Loudness Analyzer**.
- The use of `As-Run` log files for parsing discrete segments out of loudness data, see the *Audio Loudness Analyzer User Manual*.

[Workflow]: Working with Incidents

The following example illustrates the life cycle of an incident. Let's say you have noticed an intermittent input signal loss on a particular card (an alarm keeps going from green to red and back in **iC Navigator** or on a Web page). There could be a number of reasons for this: a problem with the card itself, a faulty cable, or a problem further upstream in the signal path. Because the error comes and goes, it may be difficult to diagnose. By treating the problem as an incident, you can use iControl to track the series of associated events, and better manage the process of diagnosing and resolving the root cause.

Sample workflow: Incident lifecycle

1.	Create an incident template using Event Log Viewer (see Creating an incident template using Event Log Viewer, on page 173).
2.	View the incident details (see Viewing incident details, on page 175).
3.	Attach a comment to the incident (see Attaching a comment to an incident, on page 176).
4.	Escalate the incident (see Escalating an incident, on page 176).
5.	Acknowledge the incident (see Acknowledging an incident, on page 177).
6.	Explore the incident's details (see Exploring an incident's details, on page 178).
7.	Resolve the incident (see Resolving an incident, on page 181).
8.	Clear the incident (see Clearing an incident, on page 182).

Detailed Directions

Working with Event Log Viewer and Incident Log Viewer

Configuring Event Log Viewer to Display Kaleido Alarms

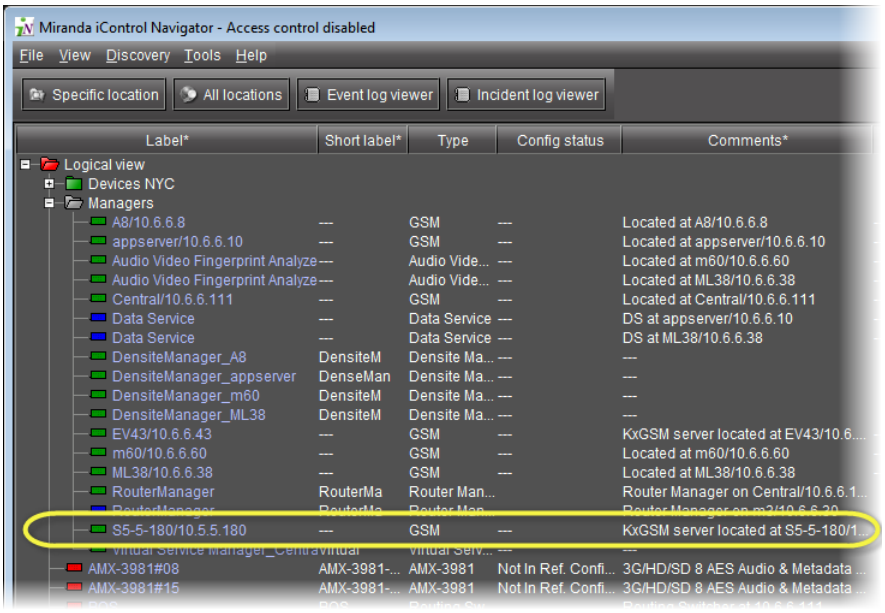
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

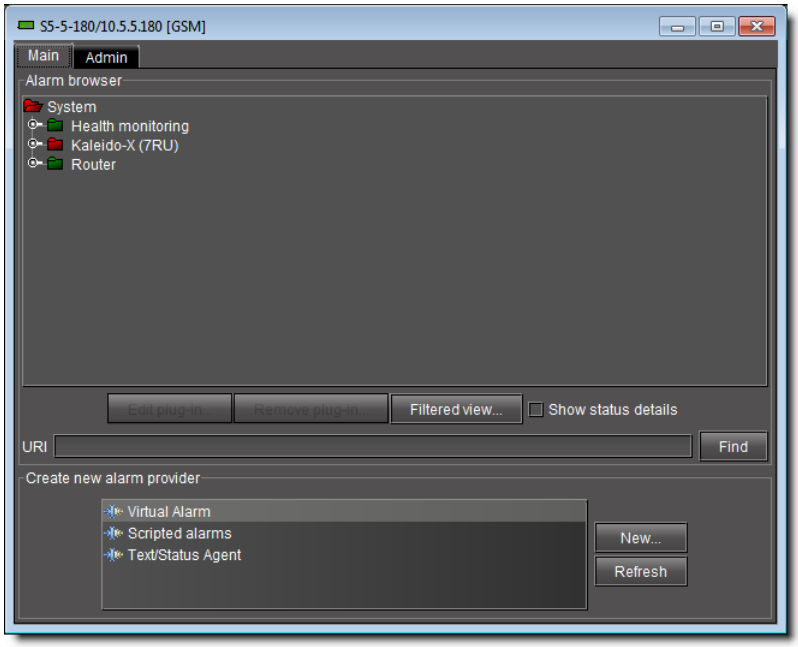
- You have opened the *Lookup location* page of your Application Server (see page 686).
- Your Kaleido GSMs are operational.
- You have defined your channel databases in XEdit with *feature-friendly* channel names. Doing this enables the system to automatically create entries in the *Global Alarms* portion of the Kaleido GSM.

1. On the *Lookup location* page, for each Kaleido device you would like to make visible to your system, perform the following sub-steps:
   a) Type the IP address and name of the Kaleido multiviewer to which you would like iControl to connect in the **Service and alarm discovery** area.

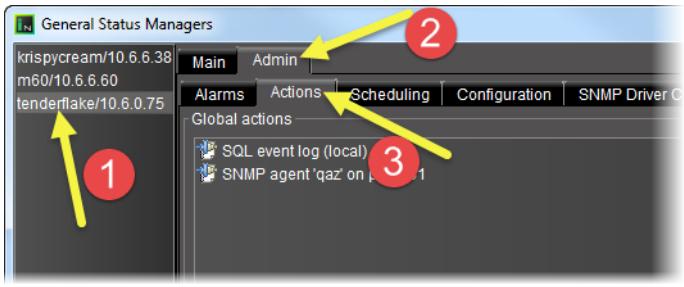
   b) Click **Add lookup**.
2. Open **iC Navigator** (see page 697).
3. In **iC Navigator**, in the **Logical View**, click the **Managers** folder.
   The Kaleido multiviewers you added should be visible in the **Managers** folder.



4. Perform the following sub-procedure for each Kaleido GSM you made visible to iControl.
   a) Double-click the Kaleido GSM.
   The GSM Control Panel appears.



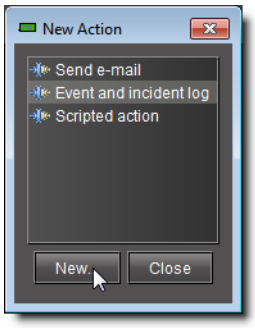
   b) Click the **Admin** tab and then click the **Actions** tab.



c) Click **Add global**.

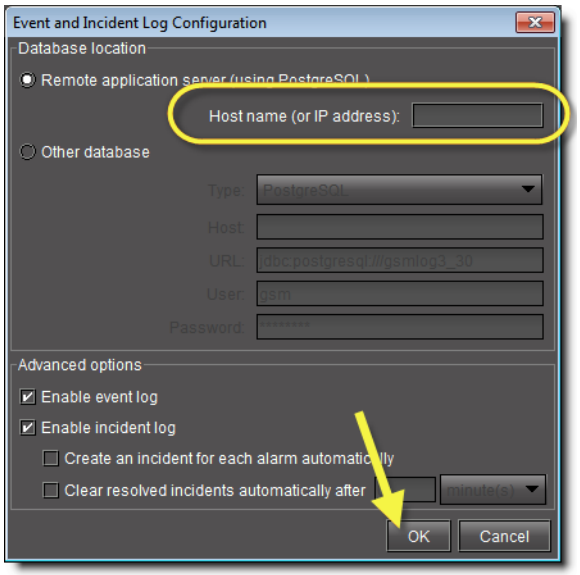
The **New Action** window appears.

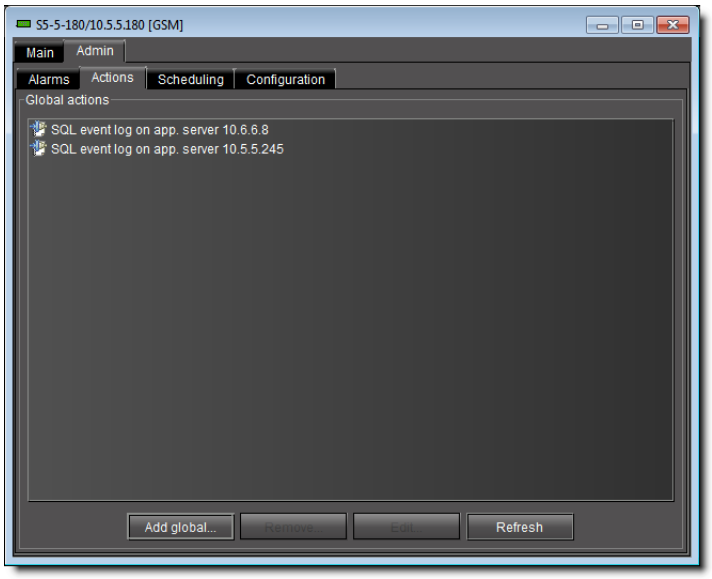
d) Click **Event and incident log**, and then click **New**.



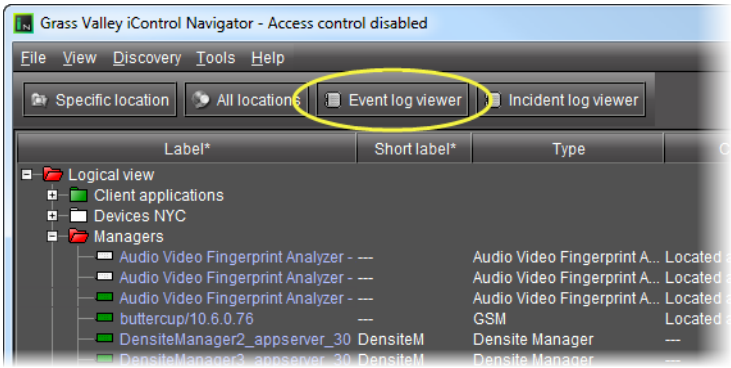
The **Event and Incident Log Configuration** window appears.

e) In the **Host name (or IP address)** field, type the IP address of your Application Server, and then click **OK**.

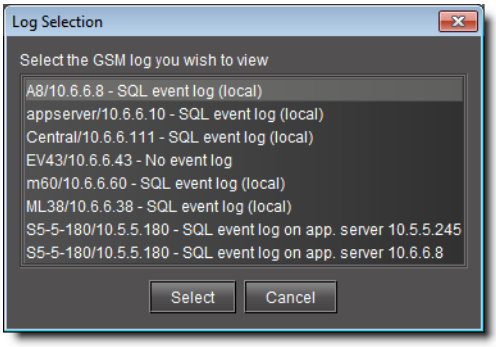




5. In **iC Navigator**, click **Event log viewer**.

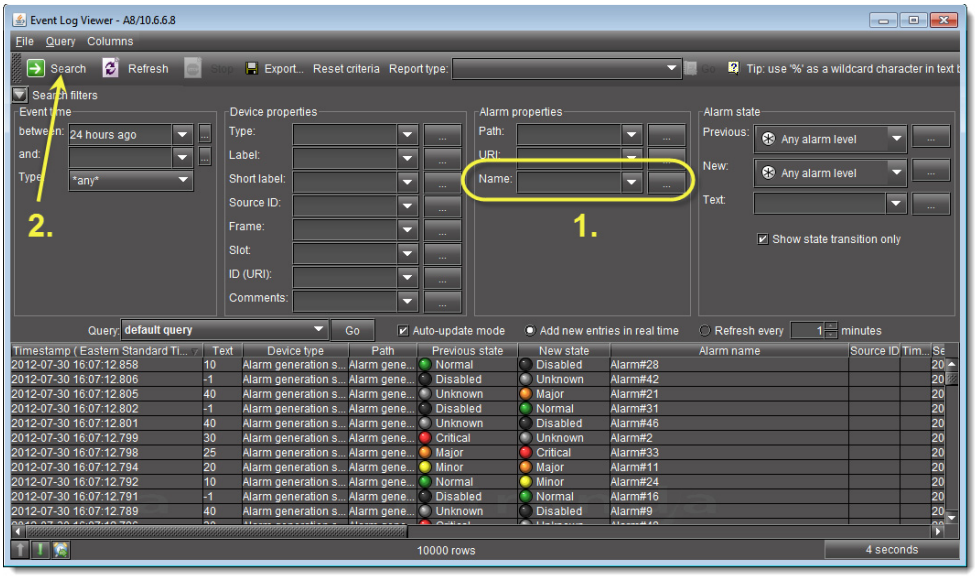


A **Log Selection** window appears.



6. Select your Application Server, and then click **Select**.
   Event Log Viewer appears.

7. In **Event Log Viewer**, type the channel name in the **Name** box of the **Alarm properties** area, and then click **Search**.



> **Note:** You can use the multi-criteria query tools of **Event Log Viewer** to refine your search. For more information, see Filtering a Log Search Using Multiple Criteria, on page 143.

Configuring Event & Incident Logging

Use this procedure if you just want to get started with event logging, on your Application Server using the default settings.

Automatically Configuring Event Logging

REQUIREMENT

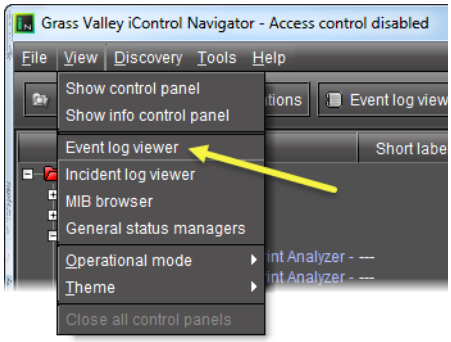
Before beginning this procedure, make sure you have opened **iC Navigator** (see page 697).

To automatically configure event logging

1. In **iC Navigator**, do only **ONE** of the following two actions:
   - Click **Event log viewer**,

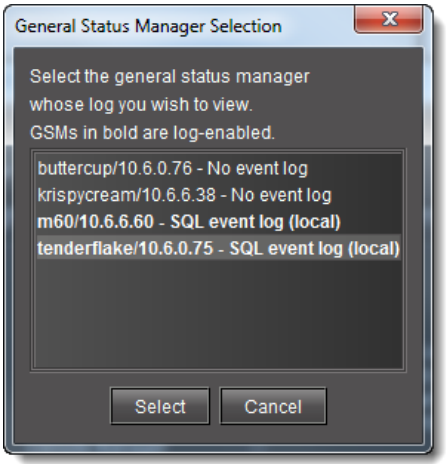
OR,

- On the **View** menu, click **Event log viewer**.



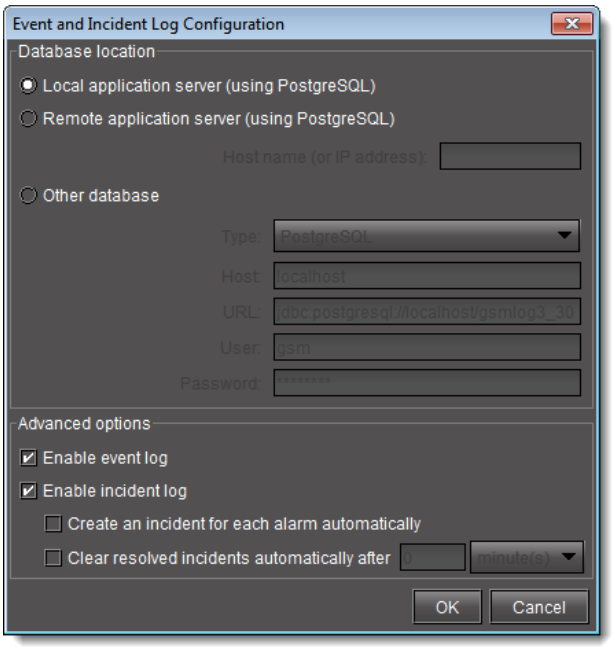
If there are more than one GSM event log, the **General Status Manager Selection** window appears.

2. Select a log event to view, and then click **Select**.



3. In the Log Viewer, on the **File** menu, click **Log properties**.

   The **Event and incident log configuration** window appears.



4. Configure settings as required.

> **Note:** The default configuration settings are suitable for most iControl users. For more information on configuration options, see Event & Incident Log Configuration, on page 123.

5. Click **OK**.

   A progress window briefly appears, followed by **Event Log Viewer**.

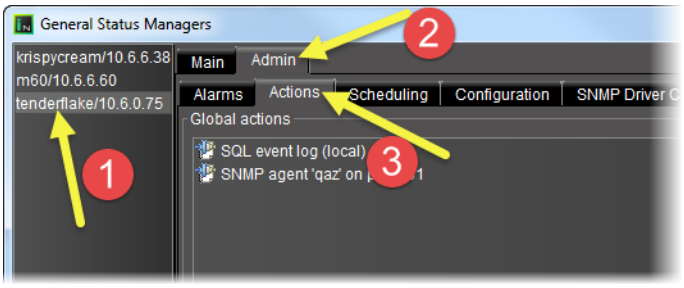
Manually Configuring Event and Incident Logging

REQUIREMENT

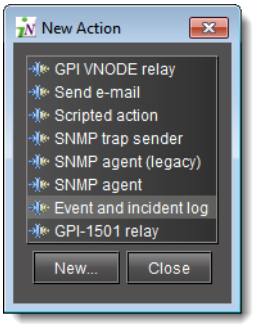
Before beginning this procedure, make sure you have opened GSM Alarm Browser (see Opening the GSM Alarm Browser, on page 710).

To manually configure event and incident logging

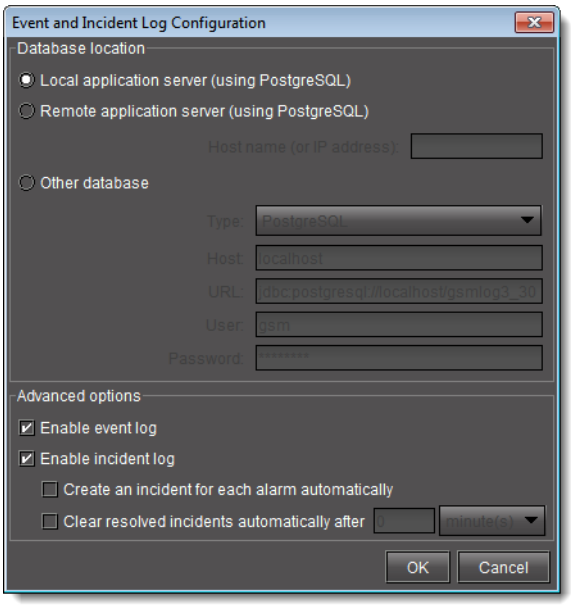
1. In the GSM Alarm Browser, in the list of GSMs in the left pane, select the GSM for which you would like to configure event and incident logging, click the **Admin** tab, and then click the **Actions** secondary tab.



2. Click **Add global**.
   The **New action** window appears.



3. Select **Event and incident log**, and then click **New**.
   The **Event and incident log configuration** window appears.



4. The default configuration settings, suitable for most iControl users, are:

Field	Default Value
--- ***Database location*** ---	
Local application server (using PostgreSQL)	enabled
Remote application server (using PostgreSQL)	disabled
Other database	disabled
--- ***Advanced Options*** ---	
Enable event log	enabled
Enable incident log (the incident log depends on the event log, so both must be enabled)	enabled
Create an incident for each alarm automatically	disabled
Clear resolved incidents automatically after	5 minutes

5. Click **OK**.

   The **General Status Managers** window reappears. The list under *Global actions* now contains an entry of the form `SQL event log (<database location>)`:

6. Click **Save**.

   The GSM starts to log events and incidents.

See also

For more information about configuration options, see Event & Incident Log Configuration, on page 123.

Stopping Event & Incident Logging

Use the following procedure to stop the logging of events and incidents.

IMPORTANT: Risk of data loss

Make sure that you have exported or archived any critical data before proceeding.

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Navigator** (see page 697).

To stop event and incident logging

1. In **iC Navigator**, locate the GSM running the SQL plug-in.
2. Double-click this GSM to open the Alarm Browser.
3. Click the **Admin** tab.
4. Select the **SQL Event Log** plug-in in the list of **Global Actions**.

5. Click **Remove**.

   A confirmation window appears.

6. In the confirmation window, click **Yes**.

Searching the Event or Incident Log Database

IMPORTANT: System behavior

In **Incident Log Viewer**, alarms that are **Offline** or **In maintenance** are not visible unless you have configured iControl to display *Offline* and *In maintenance* alarms. For more information, see Configuring iC Navigator to View Alarms with Specific Operational Modes, on page 367.

Searching the Log Database by Manually Entering Criteria

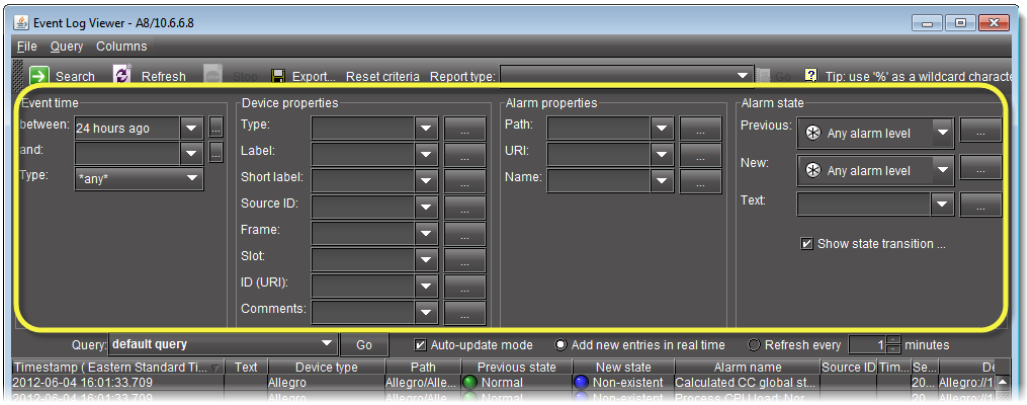
Note: In this procedure, the term *log viewer* refers to either *Event Log Viewer* or *Incident Log Viewer*, depending on which one you are using.

REQUIREMENT

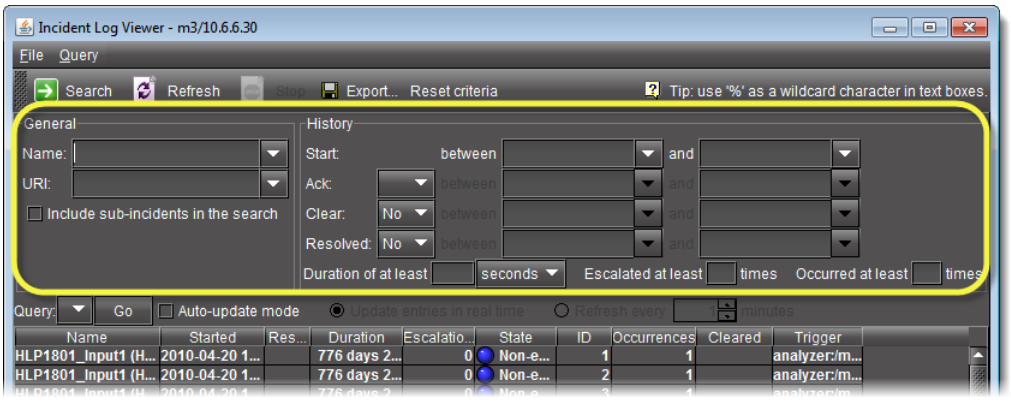
Before beginning this procedure, make sure you have opened either **Event Log Viewer** or **Incident Log Viewer**, as required (see Opening Event Log Viewer and see Opening Incident Log Viewer, on page 701).

To search the log database by manually entering criteria

1. In the log viewer, enter your search criteria in the fields provided (see Event Log Viewer or see Incident Log Viewer, on page 107).



Event Log Search Criteria



Incident Log Search Criteria

2. Click **Search**.

IMPORTANT: Keep in mind the following

- By default, a search will find only exact matches for all criteria, with the exception of what is entered in the **Text** field.
- The **Text** field lets you match text from the **Text** column, and always searches in substring mode (e.g., enter `comp` to find both *component* and *composite*).
- You can perform searches using the percentage sign (%) character as a wildcard. Any % character in a field will be interpreted as a string of zero or more arbitrary characters.To search for a literal % character, use two in a row (%%).
- An empty field is equivalent to having a single % character in the field (only faster).
- A maximum of 10,000 entries can be displayed at a time. If your search results in more than 10,000 results, use the *Batch retrieval* buttons (see Event Log Viewer, on page 93) to navigate through the search result screens.
- If a search takes longer than 5 minutes, the system resets the database connection and returns an error message asking the user to retry the search with adjusted search criteria.

Filtering a Log Search Using Multiple Criteria

The following procedure is applicable only to the **Device properties**, **Alarm properties**, and **Alarm state** areas of **Event Log Viewer**.

This procedure may be used to filter out non-channel alarms when using the iC Reports feature to create report templates. If this is the case, make sure you specify the Source ID associated with the virtual alarm you created for this purpose (see Creating a Virtual Alarm to Filter Out Non-Channel Alarms (iC Reports), on page 404).

Note: The Ellipsis buttons ( ) in the **Device properties**, **Alarm properties**, and **Alarm State** areas signify a logical **OR** joining several criteria in a single filtered search. By contrast, the Ellipsis buttons in the **Event time** area allow you to specify an event time on a calendar (see Using the Calendar, on page 151).

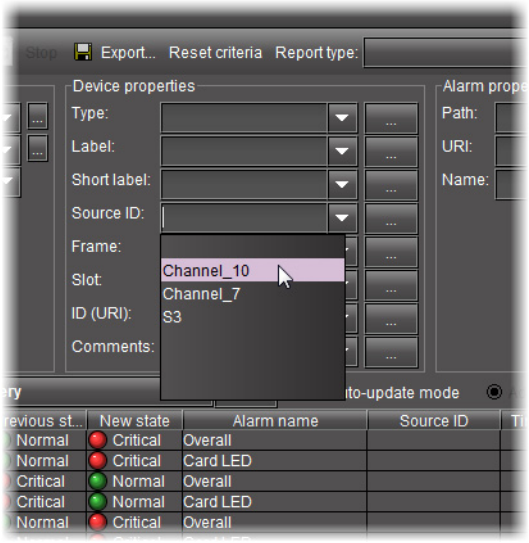
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened either **Event Log Viewer** or **Incident Log Viewer**, as required (see Opening Event Log Viewer and see Opening Incident Log Viewer, on page 701).
- If you are performing this procedure in the context of creating a channel performance report template (see Creating a Virtual Alarm to Filter Out Non-Channel Alarms (iC Reports), on page 404.), make sure:
  - You have created a virtual alarm that filters out non-channel alarms.
  - You know the virtual alarm's **Source ID** string.

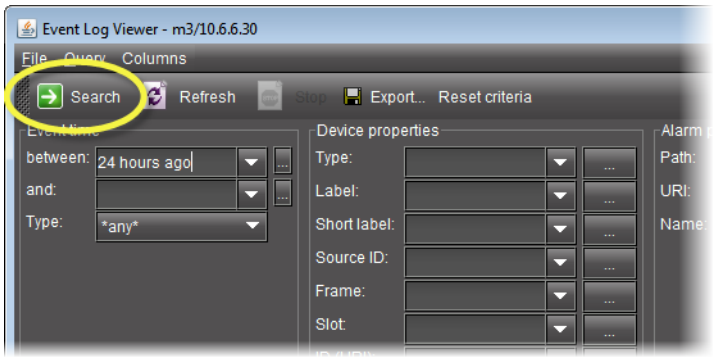
To filter a log search using multiple criteria

1. If you are performing this procedure to create a channel performance report template, perform the following sub-steps:
   a) Select the **Source ID** string associated with your report template's virtual alarm in the **Source ID** list



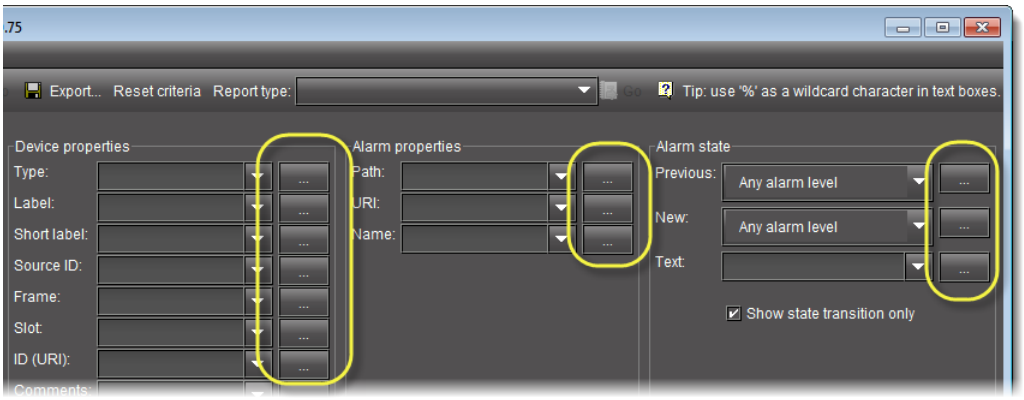
Note: If the virtual alarm has not changed states in the span of the event time of the search query, no logs of the report template's virtual alarm will be displayed.

   b) Click **Search**.

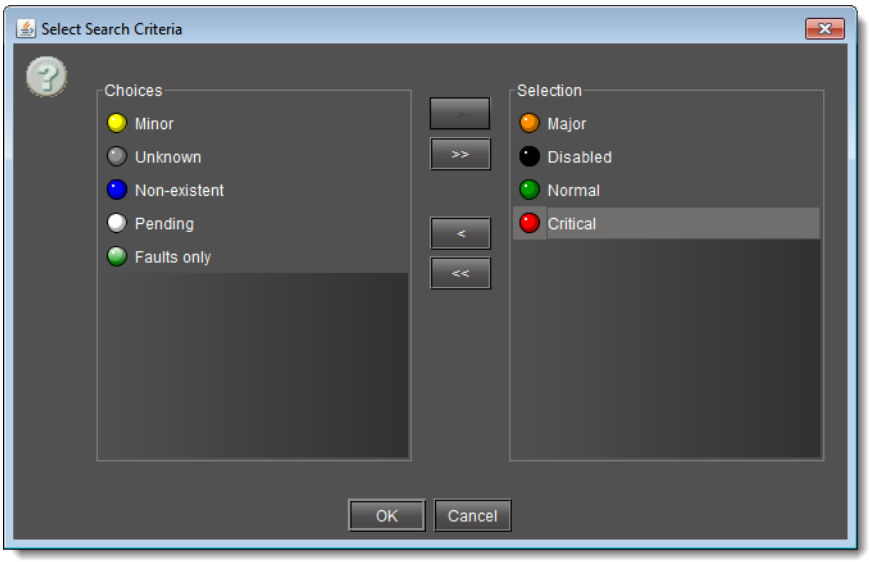


The results table displays only those alarms with the selected Source ID (only the report template's virtual alarm log entries).

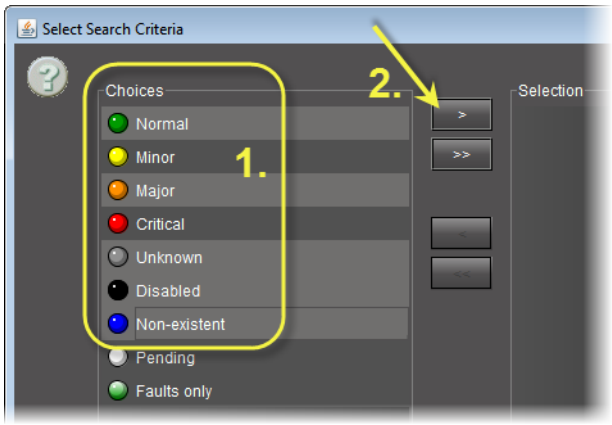
2. In **Event Log Viewer**, in the **Alarm State**, **Device properties**, or **Alarm properties** area, click the Ellipsis button (...) in the row corresponding to the desired parameter.



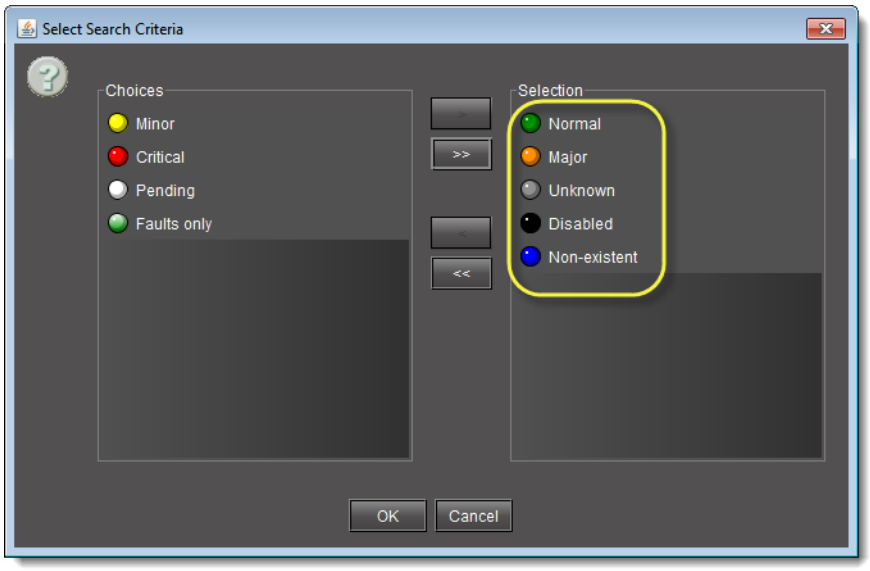
The **Select Search Criteria** window appears.



3. If you would like to select some, but not all, available choices, perform the following sub-steps:
   a) In the **Choices** list, click one of the criteria you would like to select.
   b) Between the **Choices** list and the **Selection** list, click the single arrow pointing toward the **Selection** list (>).

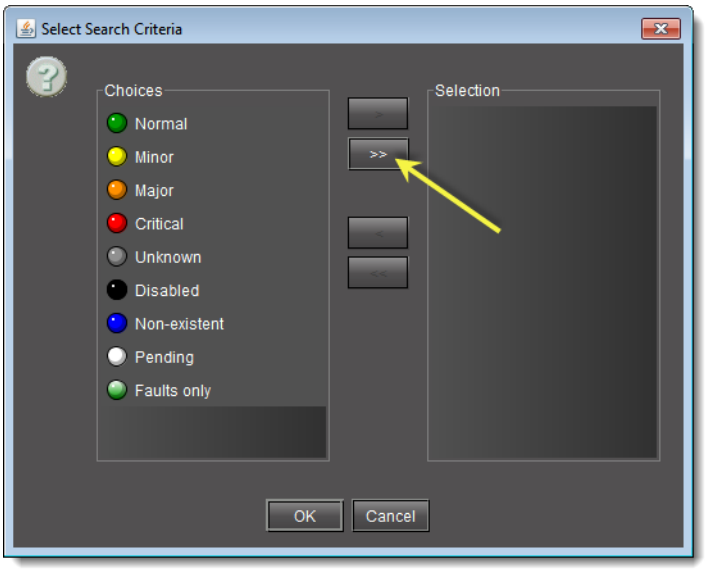


The selected choice appears in the **Selection** list.

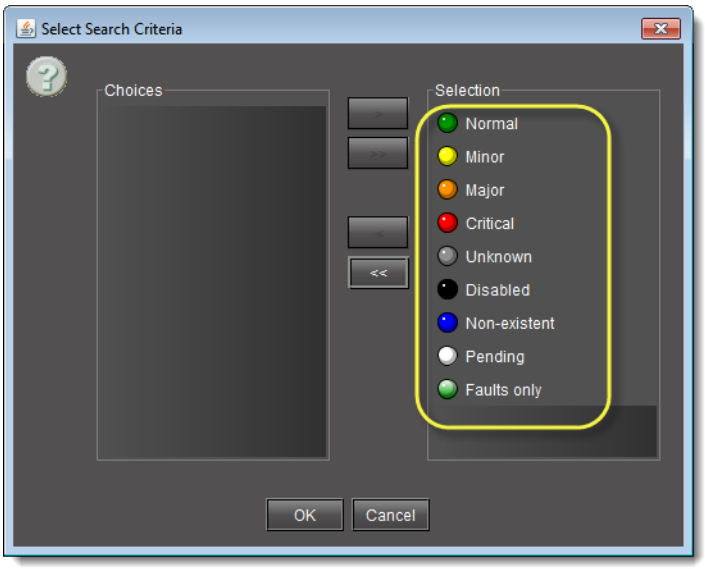


Note: Perform these two sub-steps for each choice you would like to select until they are all in the **Selection** list.

4. If you would like to select all available choices, between the **Choices** list and the **Selection** list, click the double-arrow pointing toward the **Selection** list (>>).



All criteria formerly listed under **Choices** appear in the **Selection** list.



5. Click **OK**.

   The **Select Search Criteria** window disappears and the selected choices appear in the parameter field of **Event Log Viewer**.

Filtering a Log Search using a Log's Textual Elements as Criteria

If you would like to perform a log search using any textual data present in the log database (e.g., a button label or an alarm's label), perform the following procedure.

> **Note:** You may search for multiple criteria of this sort in the same fashion as is done in the procedure see Filtering a Log Search Using Multiple Criteria, on page 143.

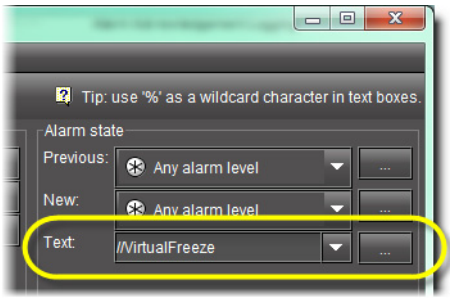
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened either **Event Log Viewer** or **Incident Log Viewer**, as required (see Opening Event Log Viewer and see Opening Incident Log Viewer, on page 701).
- If you are performing this procedure in the context of creating a channel performance report template (see [Workflow]: Channel Performance Reporting, on page 130), make sure you perform step 1 of see Filtering a Log Search Using Multiple Criteria, on page 143 before beginning this procedure.

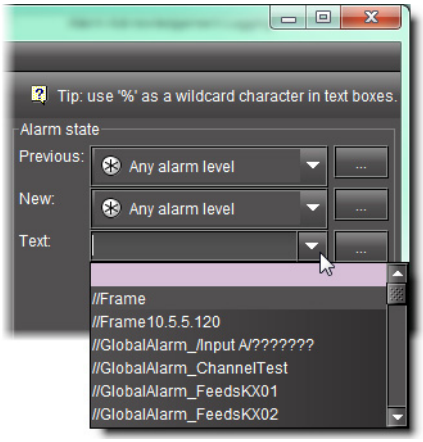
To filter a log search using a log's textual elements as criteria

- In **Event Log Viewer**, in the **Alarm state** area, do only **ONE** of the following actions:
  - In the **Text** field, type the text you would like to use as a filtering criterion.



OR,

- In the **Text** field, click the Down arrow, and then select from the list of textual choices.



Searching the Log Database by Executing a Stored Query

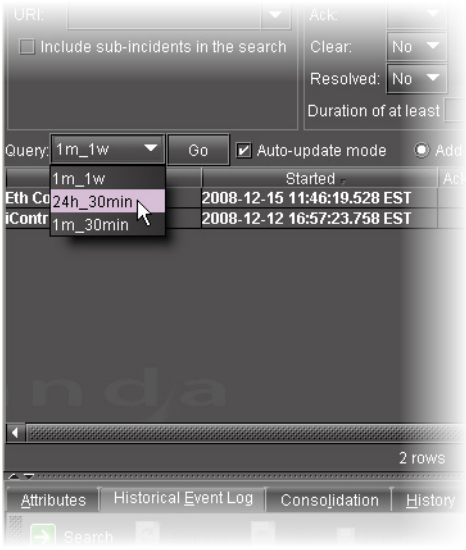
Note: In this procedure, the term *log viewer* refers to either *Event Log Viewer* or *Incident Log Viewer*, depending on which one you are using.

REQUIREMENT

Before beginning this procedure, make sure you have opened either **Event Log Viewer** or **Incident Log Viewer**, as required (see Opening Event Log Viewer and see Opening Incident Log Viewer, on page 701).

To search the log database by executing a stored query

1. In the log viewer, in the **Query** list (next to the **Go** button), click the query you wish to execute.



2. Click **Go**.

   The system returns search results based on the query's criteria.

Filtering Currently Displayed Log Results with Additional Criteria

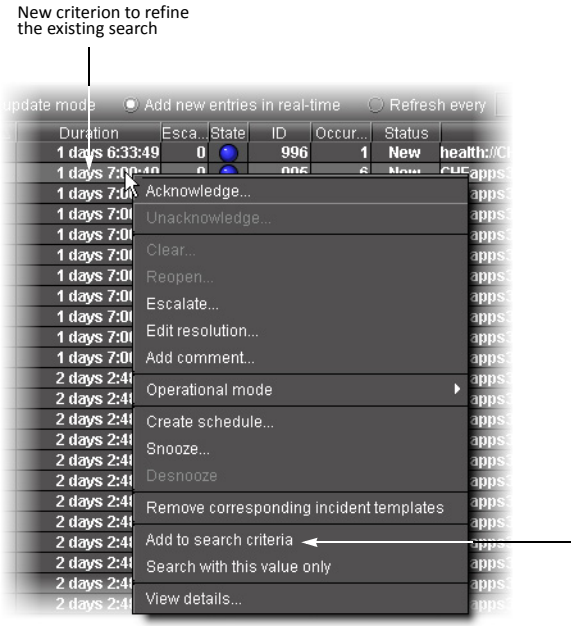
> **Note:** In this procedure, the term *log viewer* refers to either *Event Log Viewer* or *Incident Log Viewer*, depending on which one you are using.

REQUIREMENT

Before beginning this procedure, make sure you have opened either **Event Log Viewer** or **Incident Log Viewer**, as required (see Opening Event Log Viewer and see Opening Incident Log Viewer, on page 701).

To filter currently displayed log results with additional criteria

1. In the log viewer, in the current results, find any incident or event possessing the criterion you would like to add.
2. In this row, right-click the cell with this criterion, and then click **Add to search criteria**.



The system returns a list of only those incidents from the original search that also meet the new criterion.

Refining a Search of the Log Database by Filtering with Only One Criterion from the Current Search Results

> **Note:** In this procedure, the term *log viewer* refers to either *Event Log Viewer* or *Incident Log Viewer*, depending on which one you are using.

REQUIREMENT

Before beginning this procedure, make sure you have opened either **Event Log Viewer** or **Incident Log Viewer**, as required (see Opening Event Log Viewer and see Opening Incident Log Viewer, on page 701).

To refine a search of the log database by filtering with only one criterion from the current search results

1. In the log viewer's current results, find any incident possessing the criterion you would like to use in a new search.
2. In this incident's row, right-click the cell with this criterion, and click **Search with this value only**.

   The system returns results from a new search using only the new criterion as a filter.

Using the Calendar

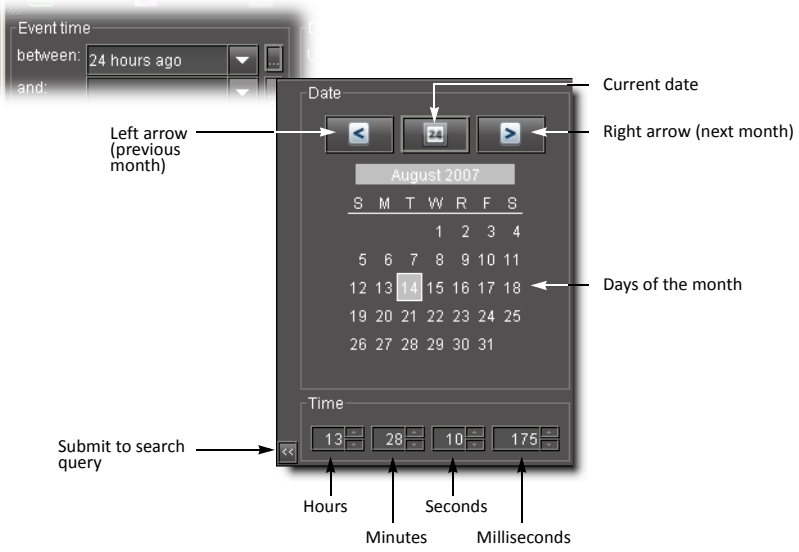
Event Log Viewer has a built-in calendar to help you specify a START and END date/time for a search.

REQUIREMENT

Before beginning this procedure, make sure you have opened **Event Log Viewer** (see page 697).

To use the calendar to specify a search interval

1. In **Event Log Viewer**, click **…** beside the **between** or **and** field.
   The calendar appears.



To do this...	...do this...
Display the previous month.	Click the left arrow. 
Display the next month.	Click the right arrow. 
Return to the current date.	Click the *Today* button. 
Select a date.	Click one of the dates in the calendar
Specify a time of day.	Click the arrows or type a number in the **Time** area
Enter your selection in the search field.	Click the Submit to search button. 

2. Specify a date and time in the calendar.

3. Click the arrow at the bottom left corner of the calendar to transfer the selected date and time to the search field.

Sorting Rows in Event Log Viewer

You can sort the events in **Event Log Viewer** by using the *down* and *up* arrows in the header column. The *down* arrow indicates a sort order of A (top) to Z (bottom), or lowest value (top) to highest value (bottom). The *up* arrow indicates a sort order of Z (top) to A (bottom), or highest value (top) to lowest value (bottom).

REQUIREMENT

Before beginning this procedure, make sure you have opened **Event Log Viewer** (see page 697).

To sort the found rows in Event Log Viewer

1. In **Event Log Viewer**, click the header of the column you wish to sort.

   A *down* arrow or *up* arrow appears beside the header title.

2. Click again on the column header to toggle the sort order.

Sorting Rows in Incident Log Viewer

Sorting in **Incident Log Viewer** is the same as in **Event Log Viewer**, with the following exception:

You can click any column header to toggle the sort order from *up* to *down* based on that column's data. Click a different column header to sort by a different criterion.

Adding, Removing & Repositioning Columns

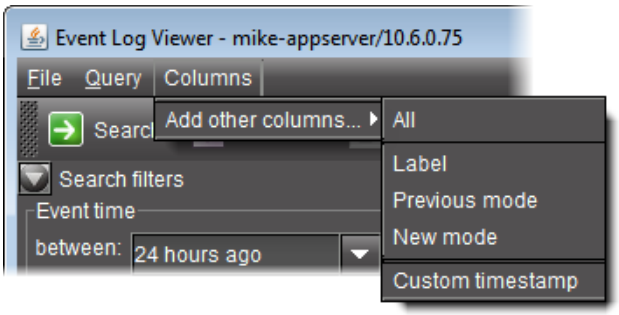
Adding a Column to the Results Table in Event Log Viewer

REQUIREMENT

Before beginning this procedure, make sure you have opened either **Event Log Viewer** or **Incident Log Viewer** as required (see Opening Event Log Viewer on page 697 and Opening Incident Log Viewer on page 701).

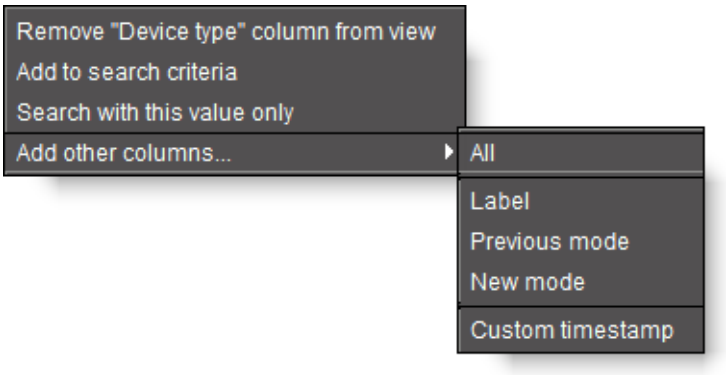
To add a column to the results table of Event Log Viewer

- In **Event Log Viewer**, on the **Columns** menu, point to **Add other columns**, and then click on a column selection.



OR,

Right-click anywhere in the results table, point to **Add other columns**, and then click on a column selection.



The column appears in the results table.

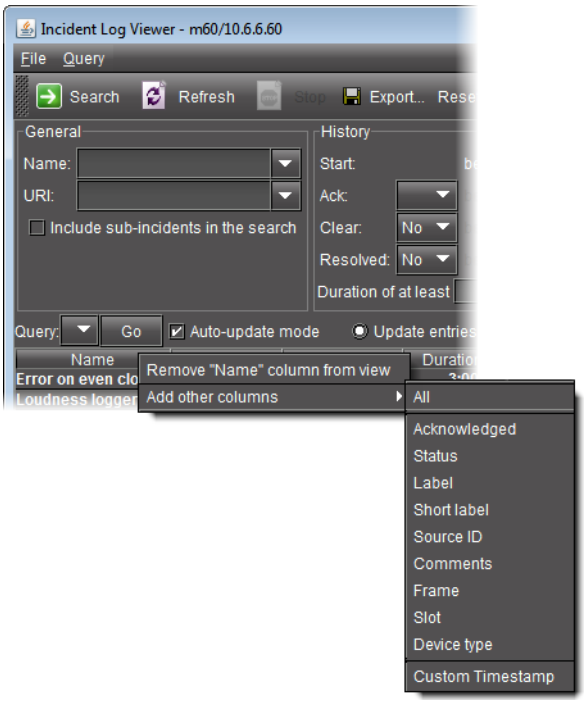
Adding a Column to the Results Table in Incident Log Viewer

REQUIREMENT

Before beginning this procedure, make sure you have opened either **Event Log Viewer** or **Incident Log Viewer** as required (see Opening Event Log Viewer on page 697 and Opening Incident Log Viewer on page 701).

To add a column to the results table of Incident Log Viewer

- In **Incident Log Viewer**, right-click anywhere in the column header row of the results table, point to **Add other columns**, and then click on a column selection.



The column appears in the results table.

Adding a Custom Timestamp Column to the Results Table

You can add a custom timestamp column to the results table of either **Incident Log Viewer** or Events Log Viewer.

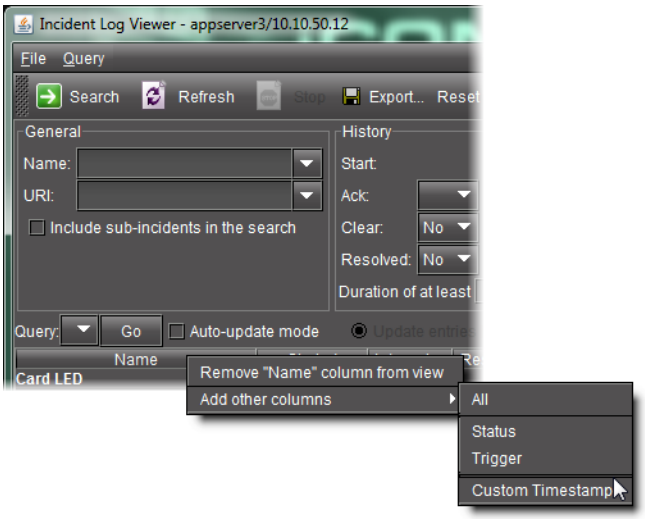
Adding a Custom Timestamp Column to Incident Log Viewer

REQUIREMENT

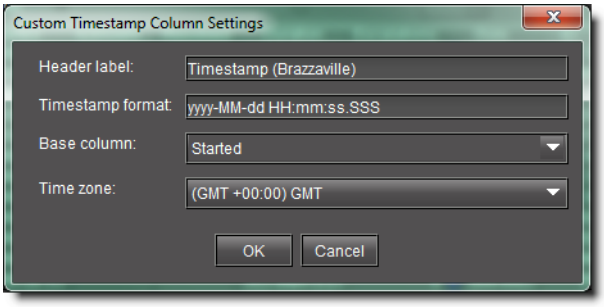
Before beginning this procedure, make sure you have opened either **Event Log Viewer** or **Incident Log Viewer** as required (see Opening Event Log Viewer on page 697 and Opening Incident Log Viewer on page 701).

To add a custom timestamp column to Incident Log Viewer

1. In **Incident Log Viewer**, right-click anywhere on the header row of the results table, point to **Add other columns**, and then click **Custom timestamp**.



The **Custom timestamp column settings** window appears.



2. Fill in a column header label, time format, base column timestamp (**GSM** or **Timestamp**), and time zone.
3. Click **OK**.

   The new custom timestamp column appears as the far right column.

Adding a Custom Timestamp Column to Event Log Viewer

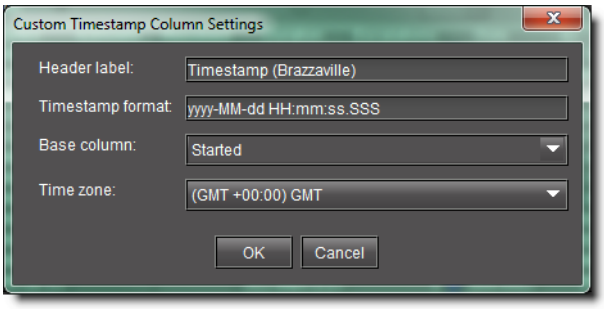
REQUIREMENT

Before beginning this procedure, make sure you have opened either **Event Log Viewer** or **Incident Log Viewer** as required (see Opening Event Log Viewer on page 697 and Opening Incident Log Viewer on page 701).

To add a custom timestamp column to Event Log Viewer

1. In **Event Log Viewer**, on the **Columns** menu, point to **Add other columns** and click **Custom timestamp**.

   The **Custom timestamp column settings** window appears.



2. Fill in a column header label, time format, base column timestamp (**GSM** or **Timestamp**), and time zone.
3. Click **OK**.

   The new custom timestamp column appears as the far right column.

Removing a Column from the Results Table

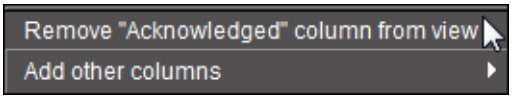
> **Note:** In this procedure, the term *log viewer* refers to either *Event Log Viewer* or *Incident Log Viewer*, depending on which one you are using.

REQUIREMENT

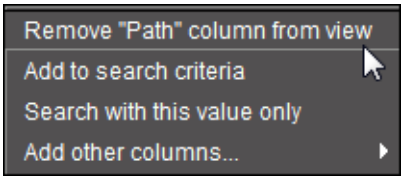
Before beginning this procedure, make sure you have opened either **Event Log Viewer** or **Incident Log Viewer** as required (see Opening Event Log Viewer on page 697 and Opening Incident Log Viewer on page 701).

To remove a column from the results table

1. In the log viewer, right-click anywhere in the column you wish to remove.
2. Click **Remove [name] column from view**.



*Column shortcut menu in **Incident Log Viewer***



Column shortcut menu in Event Log Viewer

The column disappears from the results table.

Changing the Order of the Columns in any Log Viewer

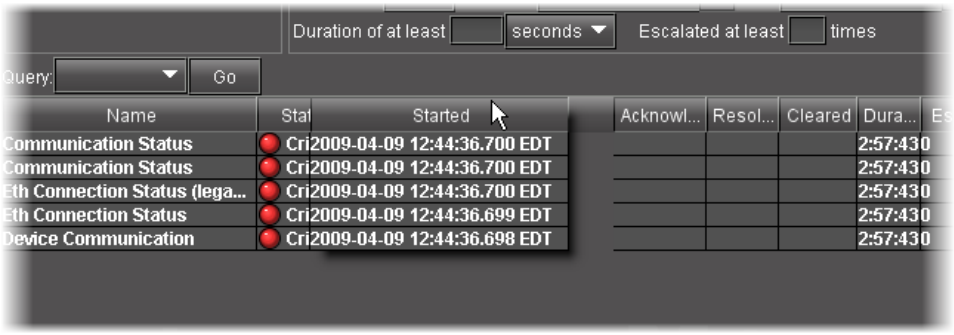
> **Note:** In this procedure, the term *log viewer* refers to either *Event Log Viewer* or *Incident Log Viewer*, depending on which one you are using.

REQUIREMENT

Before beginning this procedure, make sure you have opened either **Event Log Viewer** or **Incident Log Viewer** as required (see Opening Event Log Viewer on page 697 and Opening Incident Log Viewer on page 701).

To change the order of the columns in any log viewer

- Click in a column header and drag it to its new position.



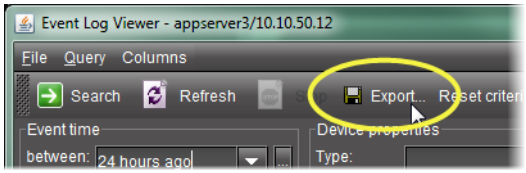
Exporting Search Results

REQUIREMENT

Before beginning this procedure, make sure you have opened **Event Log Viewer** (see page 697).

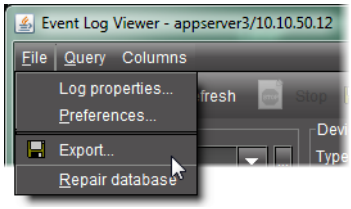
To export the results of an Event Log Viewer search

1. In **Event Log Viewer**, perform only **ONE** of the following two actions:
   - Click **Export**,

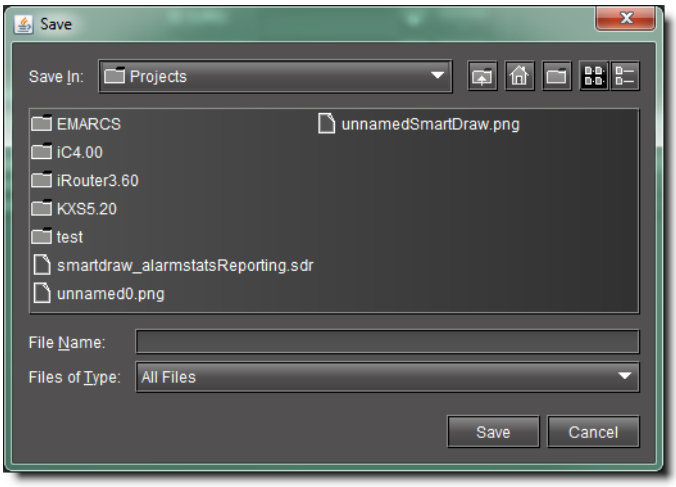


OR,

- On the **File** menu, click **Export**.



The **Save** window appears



2. Type a name for the file to be saved under, browse to the location where you wish to save the file, and then click **Save**.

   The found records are saved to a comma-separated value (`*.CSV`) file that can be opened in any text editor or spreadsheet application (e.g., Microsoft® Excel).

Creating an Incident Template

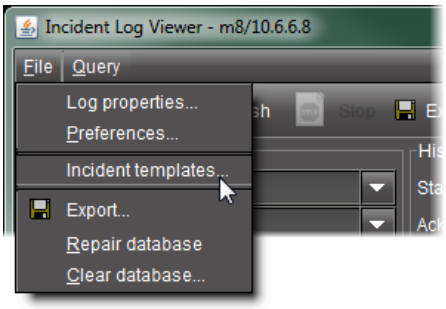
Creating an Incident Template from Incident Log Viewer

REQUIREMENT

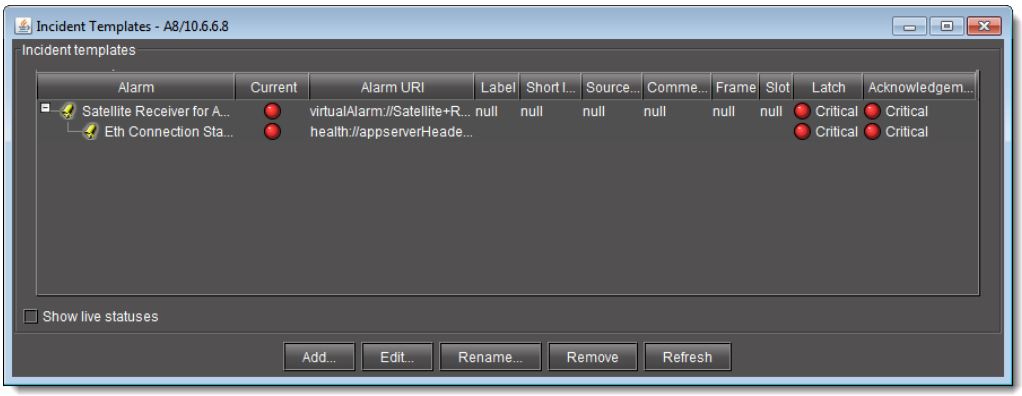
Before beginning this procedure, make sure you have opened **Incident Log Viewer** (see page 701).

To create an incident template using Incident Log Viewer

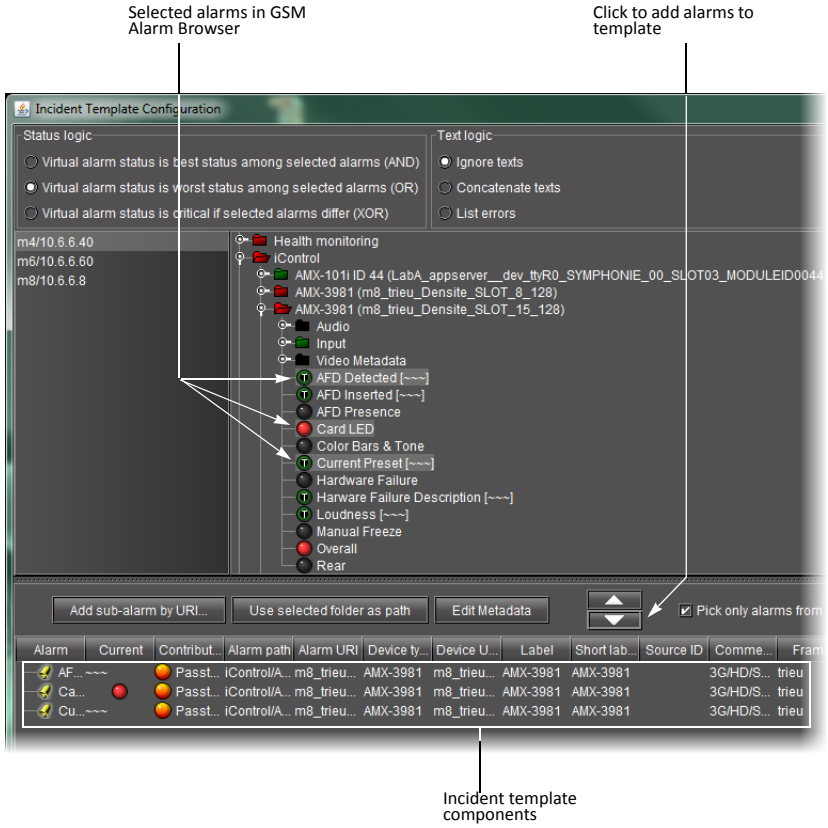
1. In **Incident Log Viewer**, on the **File** menu, click **Incident Templates**.



The **Incident Templates** window appears.



2. In the **Incident Templates** window, click **Add**.
   The **Incident template configuration** window appears.



If there are more than one GSM listed, select a GSM from the list on the left. Its Alarm Browser appears on the right.

3. In the GSM Alarm Browser, find and select alarms upon which to base your incident template.

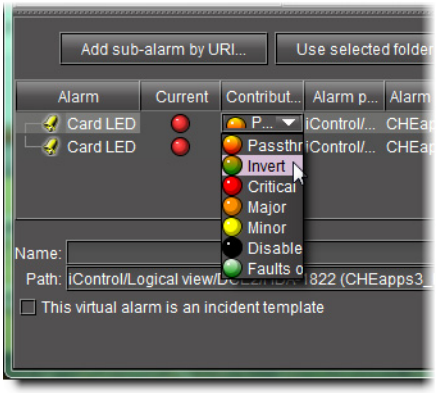
   Tip: Shift + **click** to select multiple alarms, **Ctrl** + **click** to make a non-contiguous selection.

4. Click the down arrow.

   The alarms appear in the incident template components area.

5. The table displays various details about the sub-alarms you have selected, including their Contribution, which defines how a sub-alarm will pass its status on to the incident template. The default contribution value is Passthrough, which means the sub-alarm will pass its status unaltered to the overall calculation of the incident.

   It is possible to override the error status of sub-alarms when they are triggered. This is useful when, for example, a device is only able to report a status of either `normal` (green) or `error` (red), but you want the error condition to be reflected as a `warning` (yellow) in the incident template. To change a sub-alarm's contribution, click in the **Contribution** column, and then select the status you want the incident template to use when an error occurs.



For example, if a sub-alarm goes from green to orange or red, but the selected contribution is yellow, the incident template will interpret it as yellow.

The Invert contribution allows performing a logical **NOT** calculation on sub-alarms. This feature can be used, for example, to report alarms from GPI inputs. It can also be used to handle cases where an error is expected, and not seeing an error is a sign that something probably went wrong. The table below describes the result of inverting sub-alarms:

Sub-alarm Status	Inverted Contribution
NORMAL	ERROR
MINOR	NORMAL
MAJOR	NORMAL
CRITICAL	NORMAL
NON-EXISTENT	NON-EXISTENT
PENDING	PENDING
DISABLED	DISABLED
UNKNOWN	UNKNOWN

Selecting the Faults only contribution causes a sub-alarm to be mapped to NORMAL unless it's in one of the fault statuses—usually CRITICAL, MAJOR, and MINOR. The list of fault statuses can be modified by using the `setFaultSeverities( )` property. See the *GSM Scripting Manual* for details.

> **Note:** If the sub-alarm's fault condition is cleared, its contribution will always be green, unless the value specified in the **Contribution** column is black.

6. Type a name for the new incident template in the **Name** field.
7. Type a path for the new incident template in the **Path** field. The path defines where the overall alarm for the template will appear in the GSM Alarm Browser hierarchy. If you leave this field blank, the overall alarm will appear in the *Virtual alarms* folder.

Tip: Click on a folder in the GSM Alarm Browser, and then click **Use selected folder** to copy its path to the **Path** field. You can then edit the path text, if needed.

8. Click **OK**.

   In a few moments, the new template appears in the **Incident Templates** window. If it does not appear, click **Refresh**.

> **Note:** For a given incident template, there can only be one incident open at a time. Once the open incident is cleared, the template can be triggered at any time by a subsequent alarm, whereupon a new incident (with a new ID) will be opened.

Creating an Incident Template from Event Log Viewer

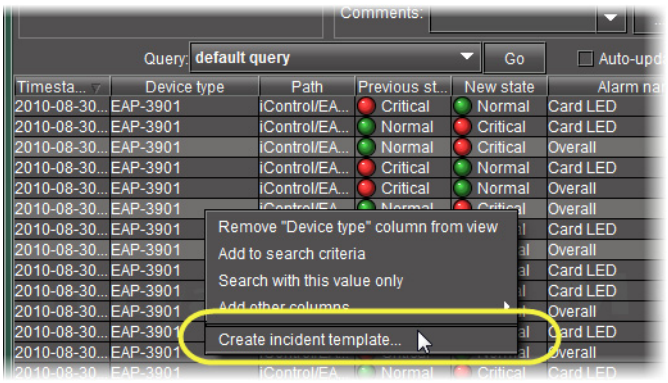
If you have performed a search using **Event Log Viewer** that reveals one or more events of interest, you can use these entries to create an incident template.

REQUIREMENT

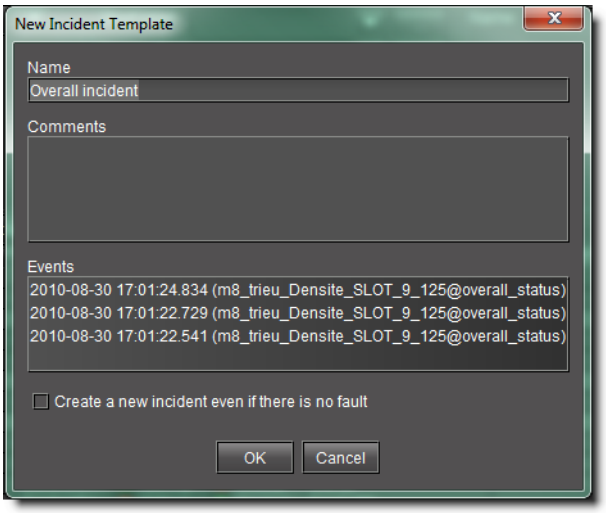
Before beginning this procedure, make sure you have opened **Event Log Viewer** (see page 697).

To create an incident template using Event Log Viewer

1. Select one or more entries of interest in **Event Log Viewer**.
2. Right-click anywhere in the selection and click **Create incident template**.



The **New incident template** window appears.



3. Enter a name to be given to incidents created from this template.
4. Add comments to describe the template.
5. If required, select **Create a new incident even if there is no fault**. Doing so creates an incident even if none of the alarms specified in the selection are in a fault status.
6. Click **OK**.

> **Note:** For a given incident template, there can only be one incident open at a time. Once the open incident is cleared, the template can be triggered at any time by a subsequent alarm, whereupon a new incident (with a new ID) will be opened.

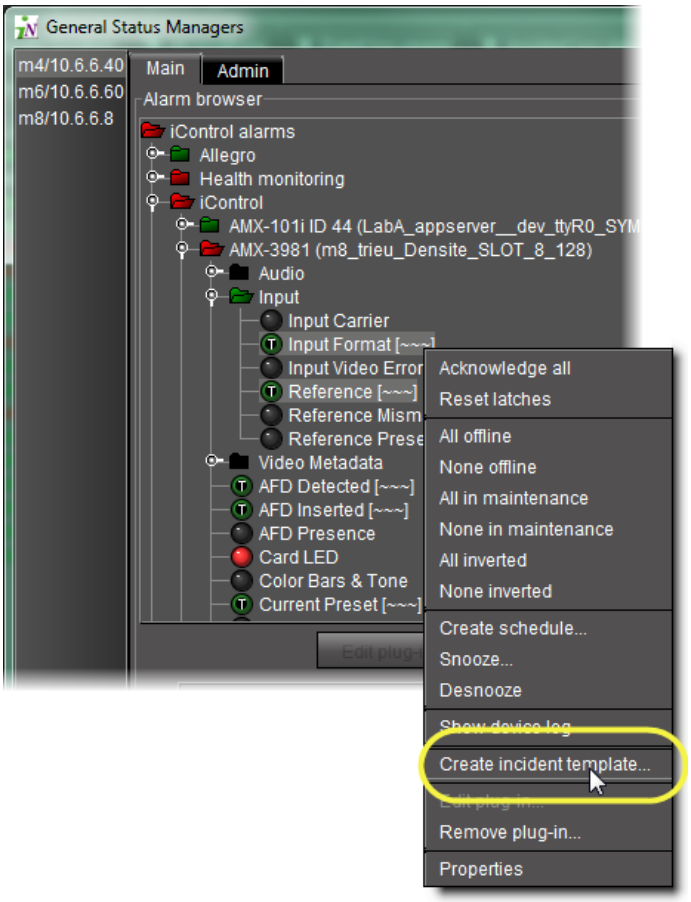
Creating an Incident Template from the GSM Alarm Browser

REQUIREMENT

Before beginning this procedure, make sure you have opened the GSM Alarm Browser (see page 710).

To create an Incident Template using the Alarm Browser

1. In the GSM Alarm Browser, select one or more nodes from the Alarm Browser's tree.
2. Right-click one of the selected nodes and click **Create incident template**.



The **Incident template configuration** window appears with the selected alarms automatically added as sub-alarms.

If there are more than one GSM listed, select a GSM from the list on the left. Its Alarm Browser appears.

3. In the GSM Alarm Browser, find and select alarms upon which to base your incident template.

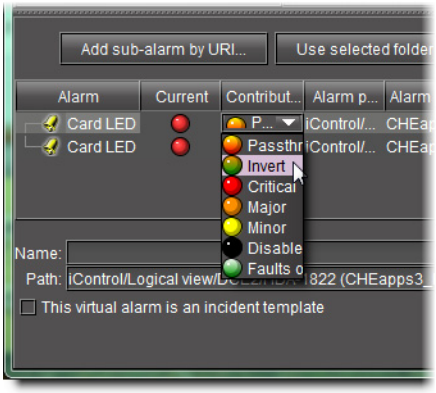
   Tip: Shift + **click** to select multiple alarms, **Ctrl** + **click** to make a non-contiguous selection.

4. Click the down arrow.

   The alarms appear in the incident template components area.

5. The table displays various details about the sub-alarms you have selected, including their Contribution, which defines how a sub-alarm will pass its status on to the incident template. The default contribution value is Passthrough, which means the sub-alarm will pass its status unaltered to the overall calculation of the incident.

   It is possible to override the error status of sub-alarms when they are triggered. This is useful when, for example, a device is only able to report a status of either `normal` (green) or `error` (red), but you want the error condition to be reflected as a `warning` (yellow) in the incident template. To change a sub-alarm's contribution, click in the **Contribution** column, and then select the status you want the incident template to use when an error occurs.



For example, if a sub-alarm goes from green to orange or red, but the selected contribution is yellow, the incident template will interpret it as yellow.

The Invert contribution allows performing a logical *NOT* calculation on sub-alarms. This feature can be used, for example, to report alarms from GPI inputs. It can also be used to handle cases where an error is expected, and not seeing an error is a sign that something probably went wrong. The table below describes the result of inverting sub-alarms:

Sub-alarm Status	Inverted Contribution
NORMAL	ERROR
MINOR	NORMAL
MAJOR	NORMAL
CRITICAL	NORMAL
NON-EXISTENT	NON-EXISTENT
PENDING	PENDING
DISABLED	DISABLED
UNKNOWN	UNKNOWN

Selecting the Faults only contribution causes a sub-alarm to be mapped to NORMAL unless it's in one of the fault statuses—usually CRITICAL, MAJOR, and MINOR. The list of fault statuses can be modified by using the `setFaultSeverities( )` property. See the *GSM Scripting Manual* for details.

> **Note:** If the sub-alarm's fault condition is cleared, its contribution will always be green, unless the value specified in the **Contribution** column is black.

6. Type a name for the new incident template in the **Name** field.
7. Type a path for the new incident template in the **Path** field. The path defines where the overall alarm for the template will appear in the GSM Alarm Browser hierarchy. If you leave this field blank, the overall alarm will appear in the **Virtual alarms** folder.

Tip: Click on a folder in the GSM Alarm Browser, and then click **Use selected folder** to copy its path to the **Path** field. You can then edit the path text, if needed.

8. Click **OK**.

   In a few moments, the new template appears in the **Incident Templates** window. If it does not appear, click **Refresh**.

> **Note:** For a given incident template, there can only be one incident open at a time. Once the open incident is cleared, the template can be triggered at any time by a subsequent alarm, whereupon a new incident (with a new ID) will be opened.

Modifying an Incident Log Template

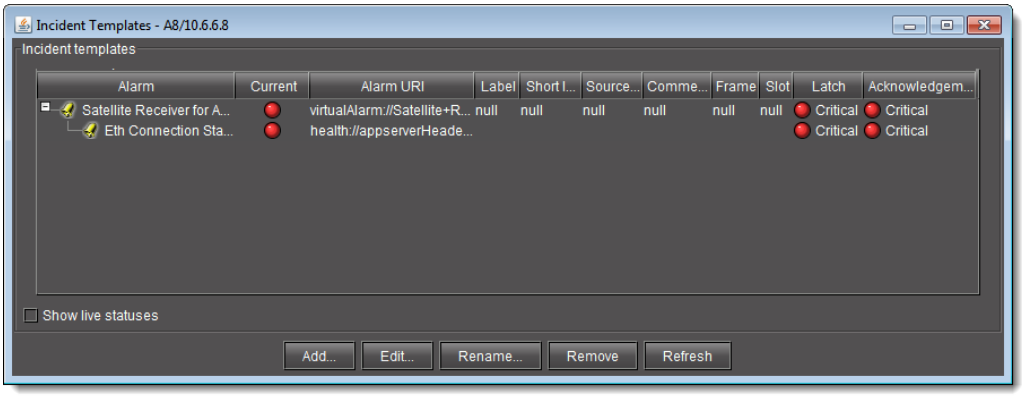
REQUIREMENT

Before beginning this procedure, make sure you have opened **Incident Log Viewer** (see page 701).

To modify an incident log template

1. In **Incident Log Viewer**, on the **File** menu, click **Incident templates**.

   The **Incident Templates** window appears.



2. Select the incident template you wish to modify.
3. Click **Edit**.

   The **Incident template configuration** window appears.
4. Make changes as required, and then click **OK**.

Renaming an Incident Log Template

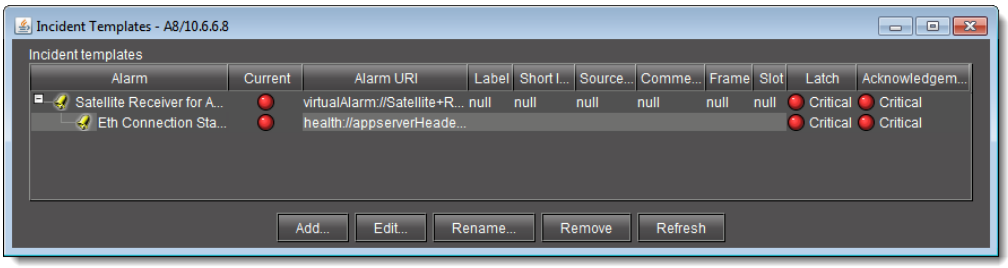
REQUIREMENT

Before beginning this procedure, make sure you have opened **Incident Log Viewer** (see page 701).

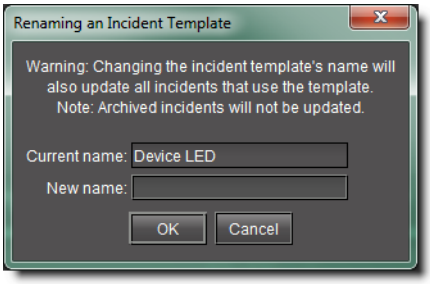
To rename an incident log template

1. In **Incident Log Viewer**, on the **File** menu, click **Incident templates**.

   The **Incident Templates** window appears.



2. Select the incident template you would like to rename.
3. Click **Rename**.
   The **Renaming an incident template** window appears.



4. Enter a new name for the template, and then click **OK**.

Removing an Incident Log Template

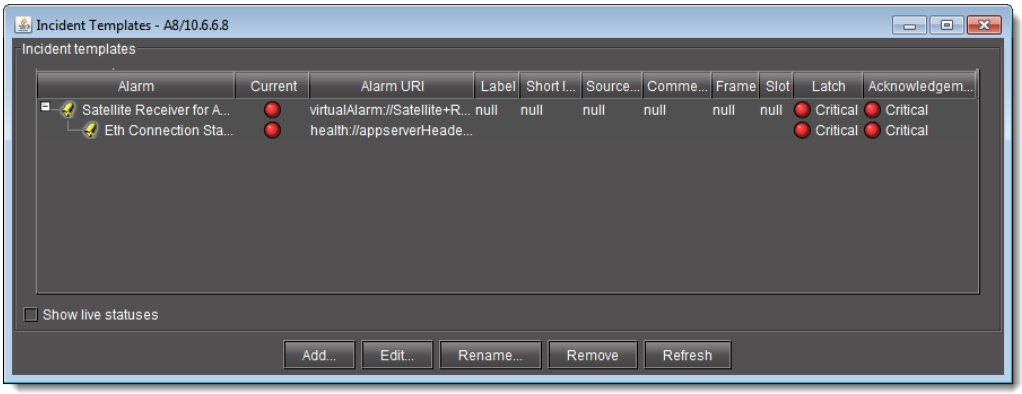
Removing an Incident Template using the Incident Templates Window

REQUIREMENT

Before beginning this procedure, make sure you have opened **Incident Log Viewer** (see page 701).

To remove an incident template using the Incident Templates window

1. In **Incident Log Viewer**, on the **File** menu, click **Incident templates**.
   The **Incident Templates** window appears.



2. Select the incident template(s) you wish to remove.
3. Click **Remove**.

   A confirmation message appears.
4. Click **OK**.

Removing an Incident Template using Incident Log Viewer

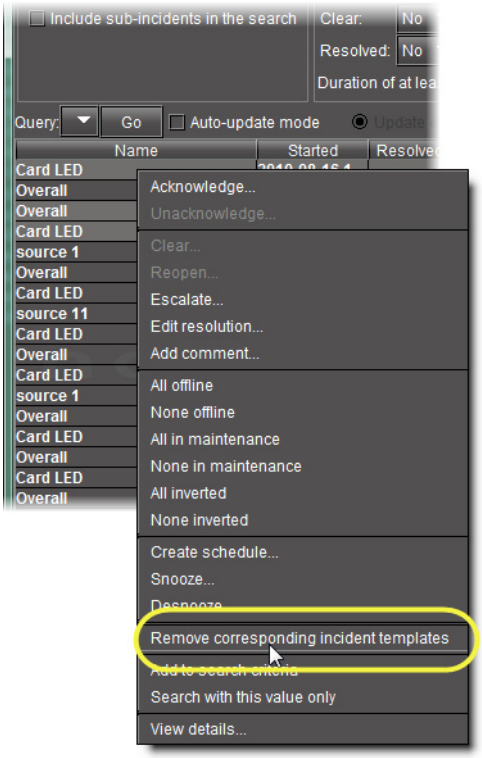
REQUIREMENT

Before beginning this procedure, make sure you have opened **Incident Log Viewer** (see page 701).

To remove an incident template using Incident Log Viewer

1. In **Incident Log Viewer**, perform a search of the Incident database (see Searching the Event or Incident Log Database, on page 142).

   The system returns search results based on the filter criteria.
2. Select one or more entries whose corresponding incident templates you would like to remove.
3. Right-click one of the selected entries and click **Remove corresponding incident templates**.



   A confirmation window appears.
4. Click **Yes**.

   The system removes the incident templates corresponding to the selected entries.

Consolidating Incidents

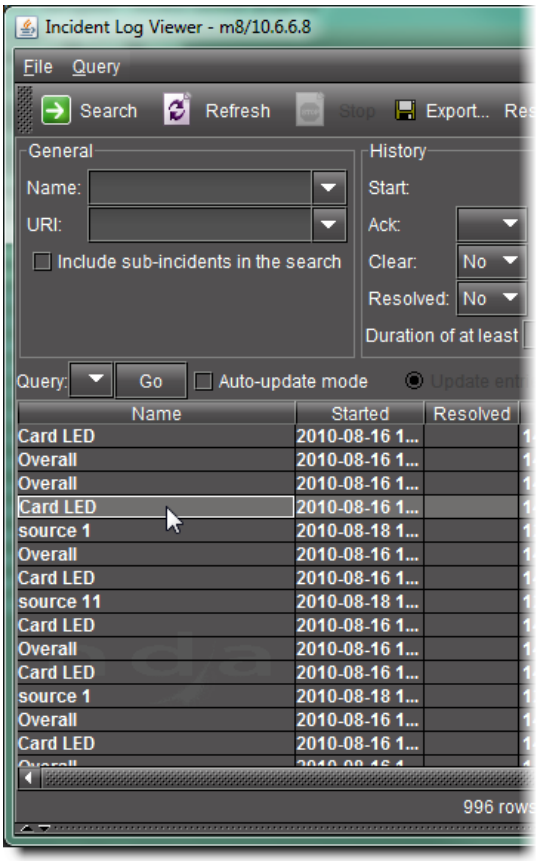
You can consolidate incidents to manage them as a single group. Incidents that have been consolidated under another incident are called *child incidents* or *sub-incidents*.

REQUIREMENT

Before beginning this procedure, make sure you have opened **Incident Log Viewer** (see page 701).

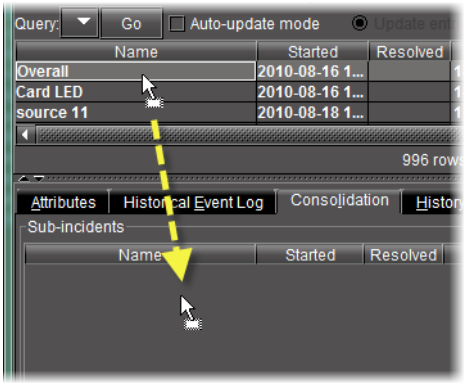
To consolidate incidents

1. In **Incident Log Viewer**, search the database for the incidents you wish to consolidate.
2. Choose one of the incidents to be the main or top-level.
3. Double-click this incident to display its details.



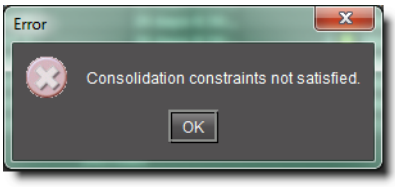
4. Click the **Consolidation** tab.

5. Select the incidents you wish to consolidate under the top-level, and then drag the entries (rows) into the area under the **Consolidation** tab.



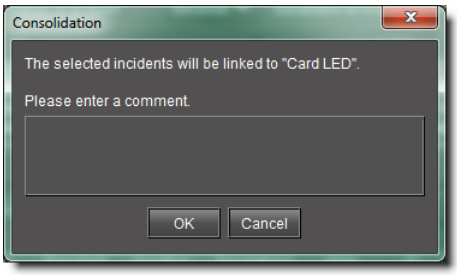
Make sure **Auto-update mode** in **Incident Log Viewer** is off, otherwise it will be difficult to select rows in **Incident Log Viewer** (see Event Log Viewer, on page 93).

> **Note:** If you receive an error message, it may be because one or more of the incidents you are attempting to drag does not qualify as a sub-incident. For example, an incident with a black status cannot be used as a sub-incident.

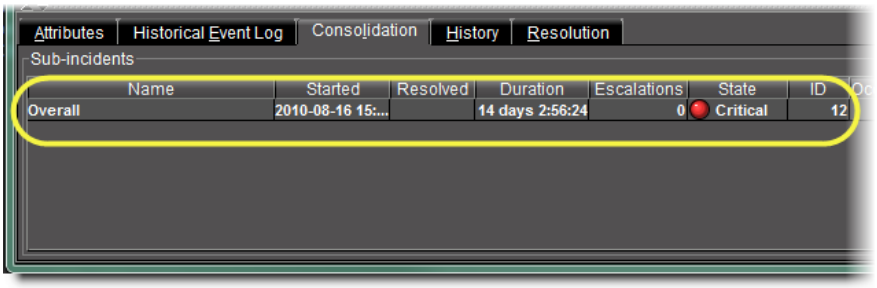


The **Consolidation** window appears.

6. Enter a comment related to the consolidation, and then click **OK**.



The selected incidents appear under the **Consolidation** tab.



7. Select the **Include sub-incidents in search** check box, and then perform a search to display the top-level incident.

> **Note:** Sub-incidents appear in smaller text.

Clearing an Incident

Once a problem has been resolved, the alarms contributing to its associated incident should turn green (normal). Consequently, the incident's overall status will also turn green. At this point, you may wish to clear the incident.

If the **Clear resolved incidents automatically after** check box is selected, the *Event and Incident Log Configuration* (see Event & Incident Log Configuration, on page 123), a resolved incident with normal overall status will automatically be cleared in the specified time period. You can also clear an incident manually.

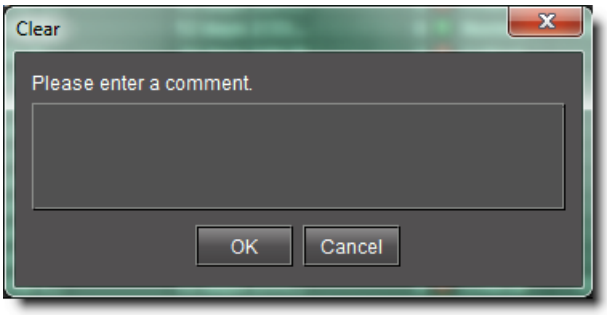
REQUIREMENT

Before beginning this procedure, make sure you have opened **Incident Log Viewer** (see page 701).

To clear an incident

1. In **Incident Log Viewer**, search the database for the incident you wish to clear.
2. Right-click anywhere in the row corresponding to the incident and click **Clear**.

   The **Clear** window appears.



3. Enter a comment, such as your name or other information related to the clearing of the incident.
4. Click **OK**.

   The incident is cleared (the text for the incident entry turns gray).

Reopening an Incident

It is possible to unclear an incident, which will put it back in its resolved state. One reason for doing this is to be able to further investigate a problem.

REQUIREMENT

Before beginning this procedure, make sure you have opened **Incident Log Viewer** (see page 701).

To reopen an incident

1. In **Incident Log Viewer**, search the database for the cleared incident you wish to reopen.
2. Right-click anywhere in the row corresponding to the incident and click **Reopen**.

   The **Reopen** window appears.
3. Enter a comment, such as your name or other information related to the reopening of the incident.
4. Click **OK**.

   The incident is reopened (the text for the incident entry turns white).

Creating an incident template using Event Log Viewer

REQUIREMENT

Before beginning this procedure, make sure you have opened **Event Log Viewer** (see page 697).

To create an incident template using Event Log Viewer

1. If possible, copy the URI of the card in question. For example, if you first noticed the alarm in an Alarm Browser, copy the URI from the alarm's **Properties**.
2. In **Event Log Viewer**, paste (or type) the card's URI in the **Device ID** field.

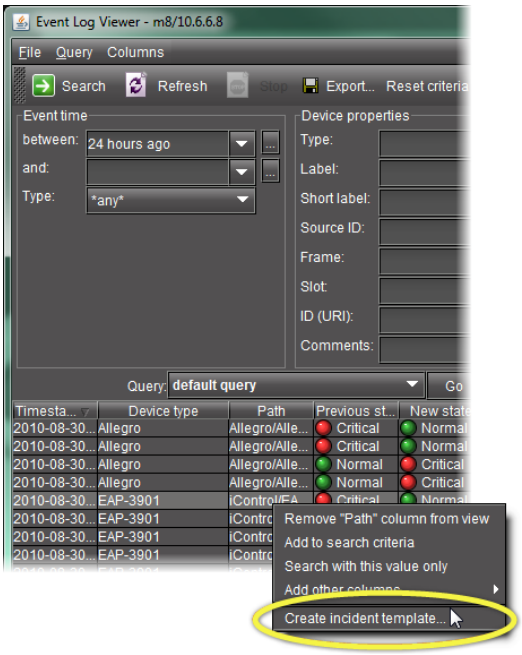
Note: You can also add other information that might narrow the search for related events (e.g., the alarm's name).

3. Click **Search**.

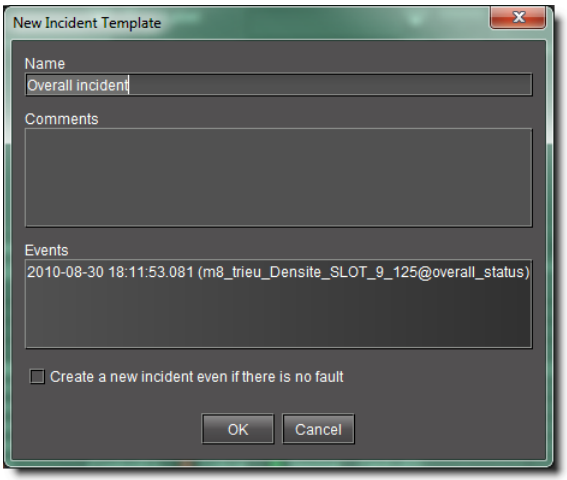
   The events associated with the card appear in the results table.

4. Select the entries of interest in **Event Log Viewer**.

5. Right-click anywhere in the selection and click **Create incident template**.



The **New incident template** window appears.



6. Enter a name for this template.

7. Add comments to describe the template.

8. Select **Create a new incident even if there is no fault**.

   This creates an incident even if none of the alarms specified in the selection is in a fault condition.

9. Click **OK**.

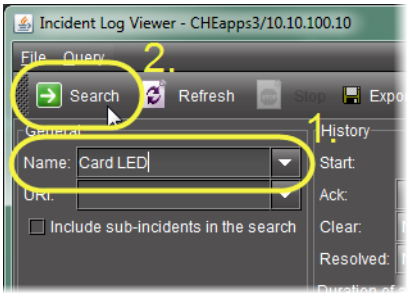
Viewing incident details

REQUIREMENT

Before beginning this procedure, make sure you have completed the procedure Creating an incident template using Event Log Viewer on page 173.

To view the incident details

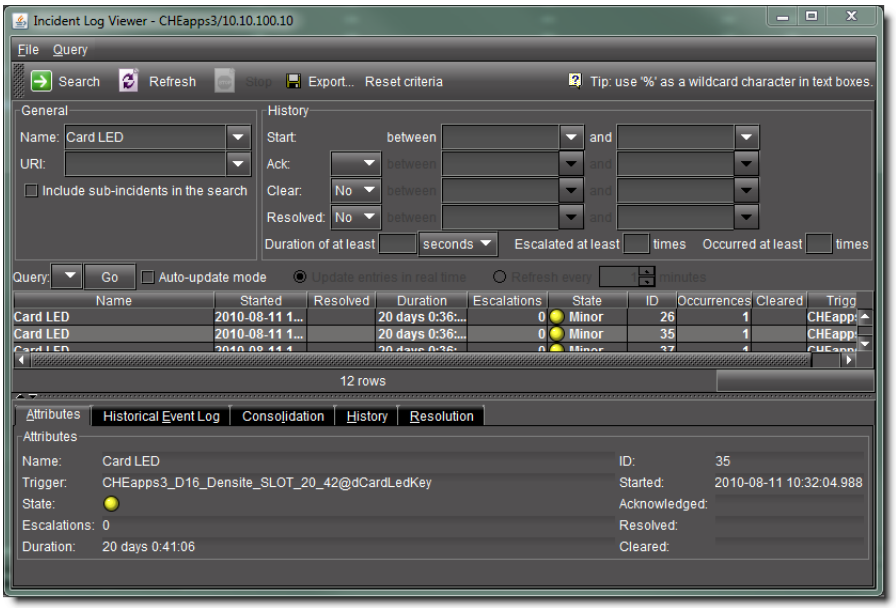
1. In **Incident Log Viewer**, type the name of the new incident in the **Name** field, and then click **Search**.



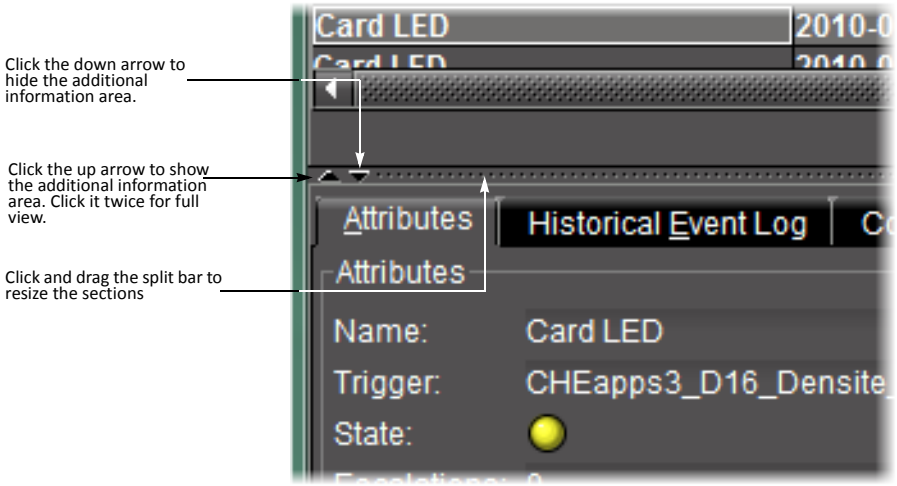
   The incident entry appears in the results table. Since this entry is new (and unacknowledged), the text is bold.

2. Double-click the new incident entry. Alternatively, right-click the new incident entry, and then click **View details**.

   The bottom of **Incident Log Viewer** expands to reveal detailed information about the new incident.



TIP: Once it has been displayed, you can hide, show and resize the additional information area using the *split bar*.



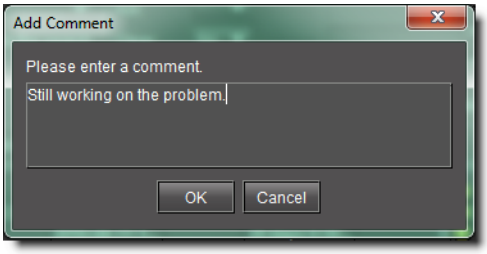
Attaching a comment to an incident

REQUIREMENT

Before beginning this procedure, make sure you have completed the procedure Viewing incident details on page 175.

To attach a comment to the incident

1. Right-click anywhere in the row corresponding to the incident and click **Add comment**.
   The **Add Comment** window appears.



2. Enter a comment, such as a description of the incident or other relevant information.
3. Click **OK**.
   The comment is saved to the incident log database.

Note: You can attach more than one comment to an incident.

Escalating an incident

If the incident needs to be brought to the attention of another individual or group, iControl allows you to designate the incident as **escalated**:

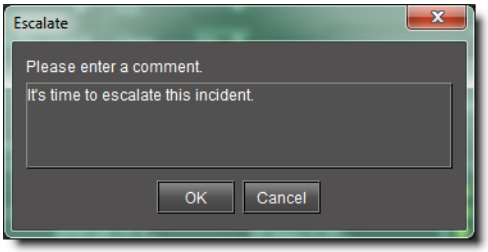
REQUIREMENT

Before beginning this procedure, make sure you have completed the procedure Attaching a comment to an incident on page 176.

To escalate the incident

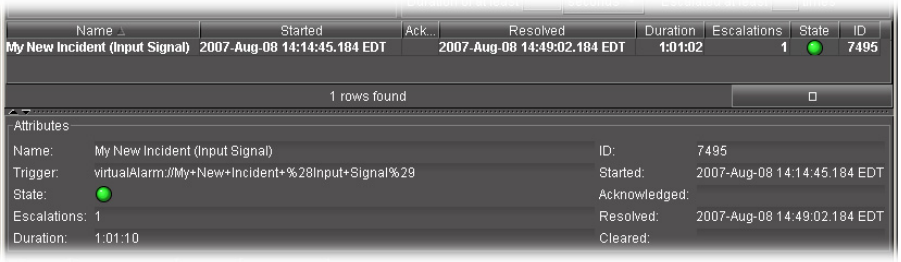
1. Right-click anywhere in the row corresponding to the incident and then click **Escalate**.

   The **Escalate** window appears.



2. Enter a comment, such as the reason for the escalation or other relevant information.
3. Click **OK**.

   The comment is saved to the incident log database. The number 1 appears in the **Escalations** column.



Note: You can escalate an incident more than once. The **Escalations** counter will increment by one each time. Escalations can also be triggered by scripts.

Acknowledging an incident

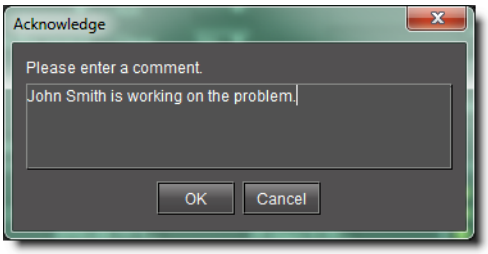
REQUIREMENT

Before beginning this procedure, make sure you have completed the procedure Escalating an incident on page 176.

To acknowledge the incident

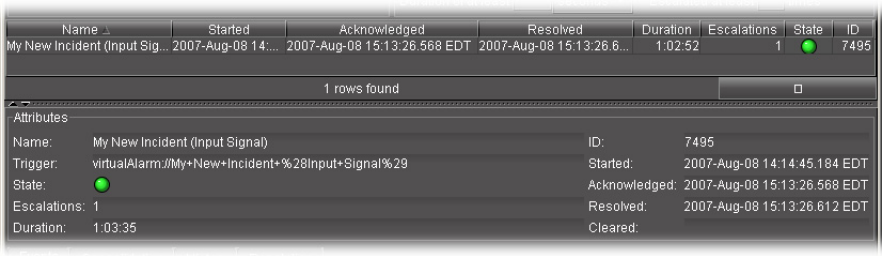
1. Right-click anywhere in the row corresponding to the incident and click **Acknowledge**.

   The **Acknowledge** window appears.



2. Enter a comment, such as your name or other information related to the acknowledgement of the incident.
3. Click **OK**.

   The comment is saved to the incident log database. A timestamp appears in the **Acknowledged** column and in the **Attributes** section.



> **Note:** Changing an incident's **acknowledged** state also changes the associated alarms, but not the other way around.

Exploring an incident's details

Exploring the information in the **Attributes** and **Additional Info** sections of the **Incident Viewer** window can help you in your attempts to track and diagnose a problem.

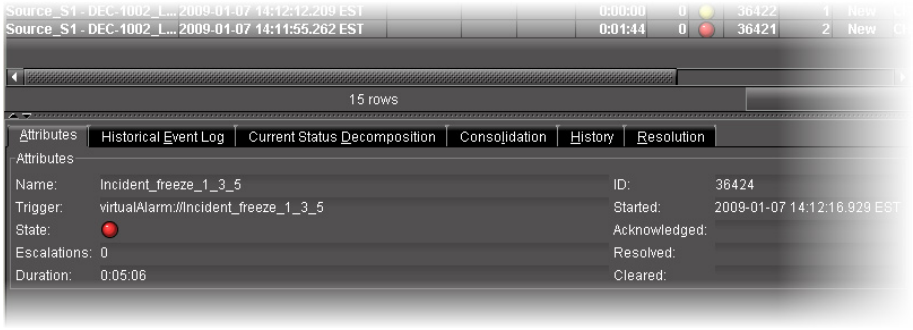
REQUIREMENT

Before beginning this procedure, make sure you have completed the procedure Acknowledging an incident on page 177.

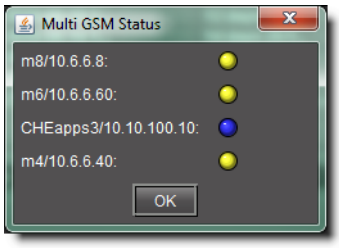
To explore the incident's details

1. In the **Incident details** area, click the **Attributes** tab.

   The **Attributes** tab repeats the description of the incident from the results table.

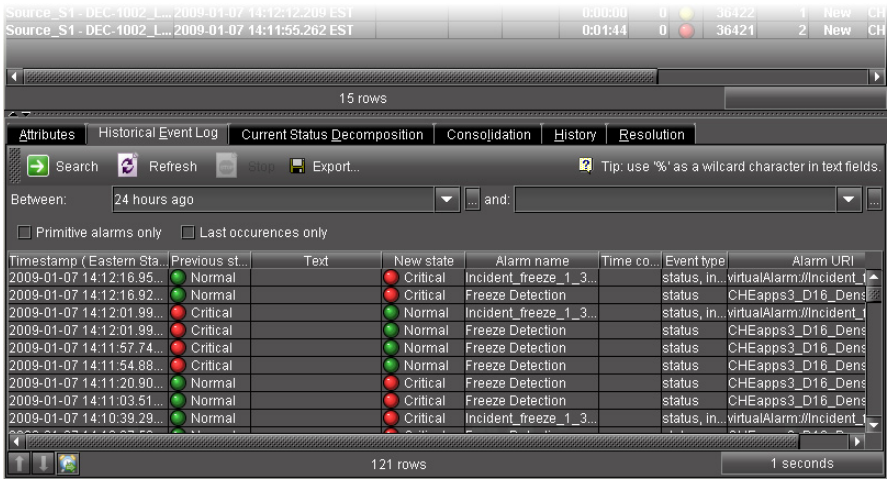


You can right-click **State** to bring up a new shortcut menu.

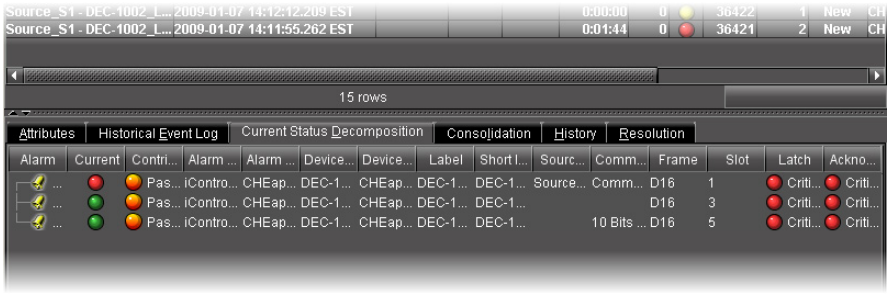
Menu Item	Description
Reset latch	Not used
Acknowledge	Not used
Refresh	Refreshes the log viewer
Show multi-GSM status	In a multiple GSM configuration, displays the overall incident alarm for each GSM: 

The **Duration** is updated in real time (the **Duration** column in the results table is only refreshed at the interval specified in **Event Log Viewer** (see page 93).

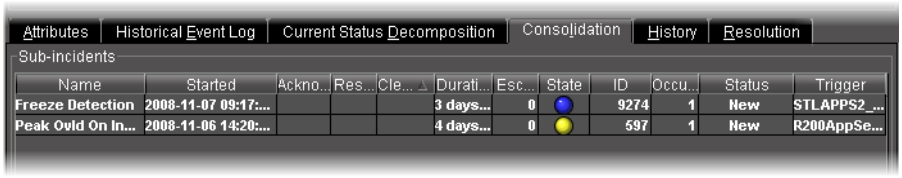
2. The **Historical Event Log** tab is an embedded version of **Event Log Viewer** that displays events associated with the currently selected incident.



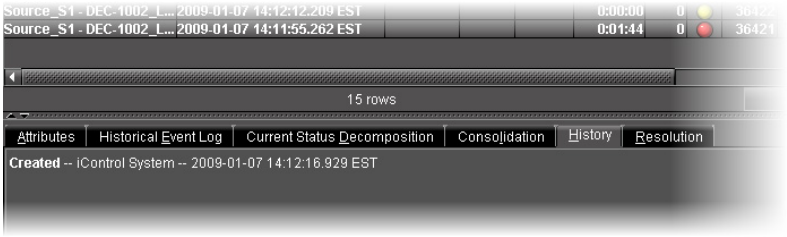
3. The **Current Status Decomposition** tab shows the composition of the incident templates thereby allowing users to find the root causes of individual incidents.



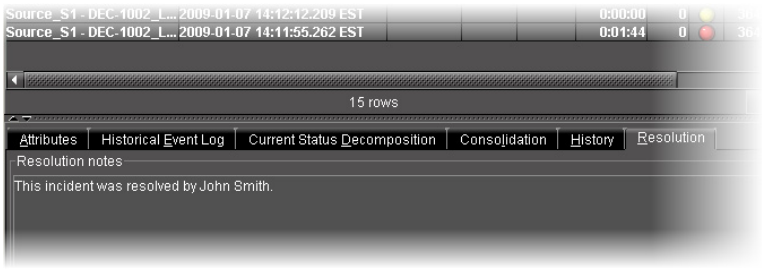
4. The **Consolidation** tab shows any child incidents that have been linked to the current (parent) incident.



5. The **History** tab shows a list of all comments associated with the incident.



6. The **Resolution** tab displays comments associated with the incident's resolution.



Resolving an incident

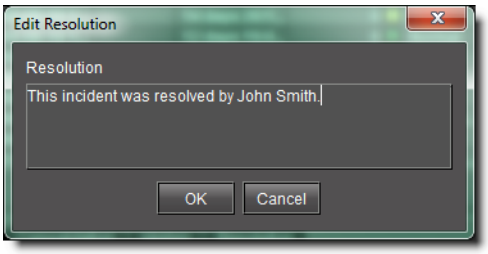
REQUIREMENT

Before beginning this procedure, make sure you have completed the procedure Exploring an incident's details on page 178.

To resolve the incident

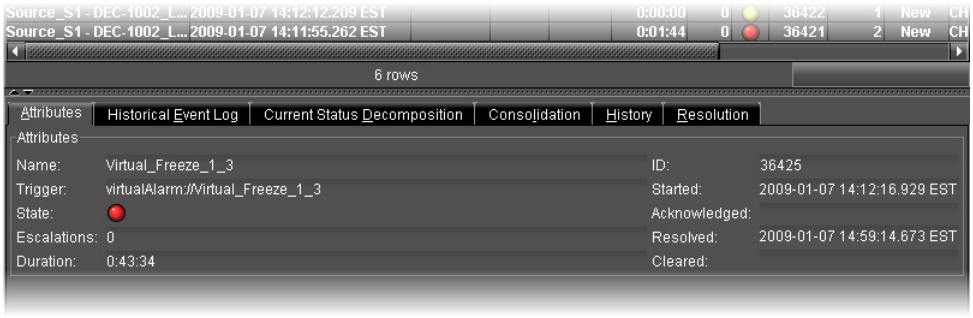
1. Right-click anywhere in the row corresponding to the incident and click **Edit resolution**.

   The **Edit Resolution** window appears.



2. Enter a comment, such as your name or other information related to the resolution of the incident.
3. Click **OK**.

   The comment is saved to the incident log database. The incident's overall status turns green, and a timestamp appears in the **Resolved** column and in the **Attributes** section.



   The comment(s) saved when the incident was resolved can be viewed under the **Resolution** and **History** tabs.

Clearing an incident

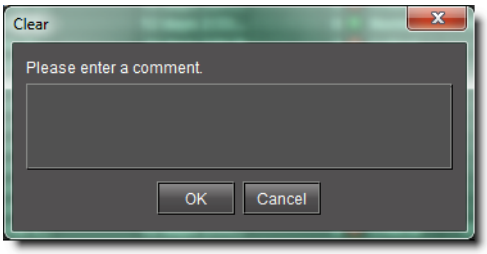
REQUIREMENT

Before beginning this procedure, make sure you have completed the procedure Resolving an incident on page 181.

To clear the incident

1. Right-click anywhere in the row corresponding to the incident, and then click **Clear**.

   The **Clear** window appears.



2. Enter a comment, such as your name or other information related to the clearing of the incident.
3. Click **OK**.

   The incident is cleared (the text for the incident entry turns gray).

Notes

- An incident can only be *cleared* after it has been *resolved*. A resolved incident may get cleared automatically after a certain amount of time if the **Clear resolved incidents automatically after** check box is selected (see Event & Incident Log Configuration, on page 123).
- It is possible to *unclear* an incident, which will put it back in its *resolved* state. One reason for doing this is to be able to further investigate a problem.

Working with Loudness Logger and Audio Loudness Analyzer

Starting Loudness Logger and Loudness Analyzer Services

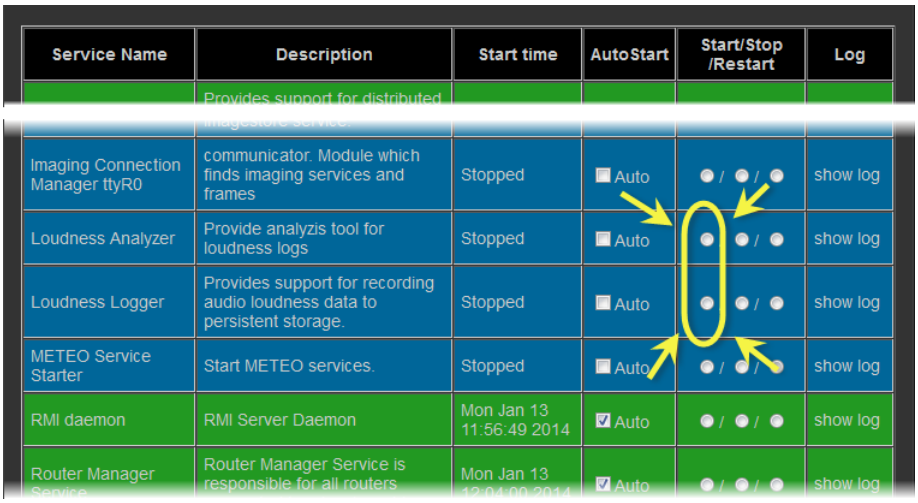
Before you can log loudness data and before you can analyze a loudness log, you must first start **Loudness Logger** and **Loudness Analyzer** services in iControl.

REQUIREMENT

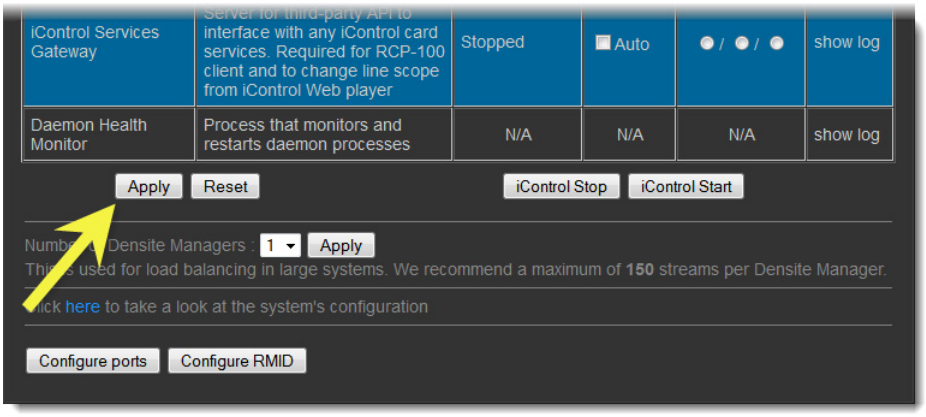
Before beginning this procedure, make sure you have opened the *Services management* page (see page 677).

To start Loudness Logger and Loudness Analyzer services

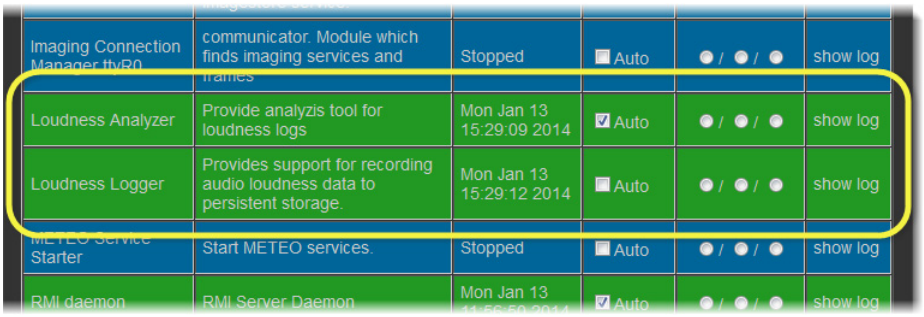
1. On the *Services management* page, in the **Start/Stop/Restart** column, select **Start** for both of the **Loudness Analyzer** and **Loudness Logger** rows.



2. Just beneath the **Services** table, click **Apply**.



The **Loudness Analyzer** and **Loudness Logger** rows become green, indicating that these services are now started.



Mounting a Remote Shared Drive in your Application Server

Loudness logs can grow quickly. Grass Valley recommends mounting an external drive to the designated loudness folder in your Application Server in order to avoid running out of hard drive space as well as causing performance issues.

IMPORTANT: Make sure you have sufficient storage space for loudness data

Ensure you have enough storage space available for loudness data at the specified location. If, when logging loudness data, the logger runs out of space, it will stop logging (guidelines on estimating storage space requirements).

IMPORTANT: The external drive you would like to mount as a remote shared drive must be a NAS (network attached storage) device. Grass Valley only officially supports the use of a NAS in the context of this procedure. To verify your external drive is a NAS, see your network administrator.

Note: When mounting a drive to an Application Server directory, you may only change the configured IP address of the external drive and the name and path of the Application Server shared directory if the shared directory is already unmounted.

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- The external drive you would like to mount to the Application Server is a NAS (network-attached storage) device and not a DAS (direct-attached storage) device. To verify this drive is a NAS, see your local network administrator.
- The external NAS drive must support the Samba network file sharing protocol. To verify this drive supports Samba, see your local network administrator.
- On the external drive, the directory you would like to mount is already a shared directory.

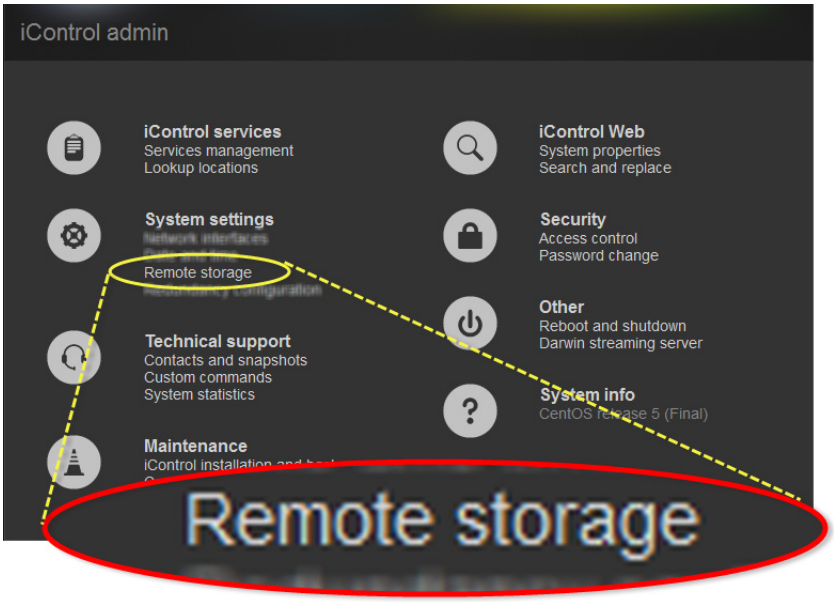
REQUIREMENTS (*Continued*)

Make sure you meet the following conditions before beginning this procedure:

- You have opened the *iControl admin* page (see page 681).
- You have started both the *Loudness Logger* and *Loudness Analyzer* services in iControl (see page 183).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Logging and Analyzing Loudness, on page 131).

To mount a remote shared drive to your Application Server

1. On the *iControl admin* page, under **System settings**, click **Remote storage**.



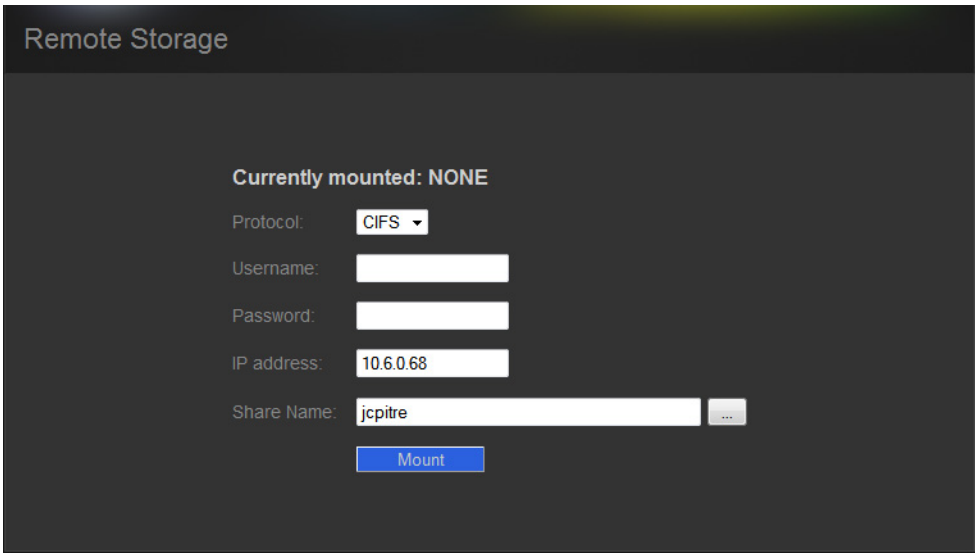
   The *Remote Storage* page appears.

2. Select a file system protocol.

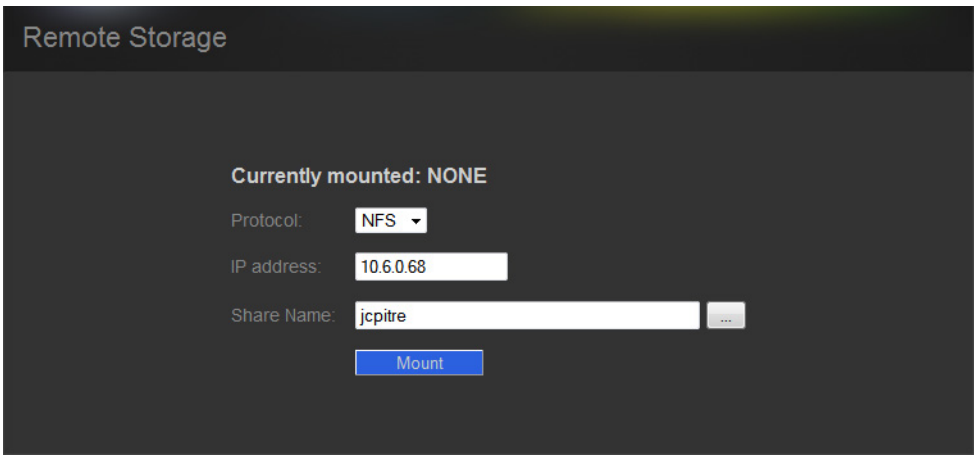
   If you choose CIFS[1] as a protocol, you are prompted for user name and password credentials. If your Remote Storage folder is protected, enter the appropriate credential (user name, password) information.

> **Note:** When mounting a folder using the CIFS protocol, although you are prompted for credentials, you are not obliged to use them. Once a folder is mounted using CIFS and using credentials, accessing that remote storage will **require** using credentials, however.

1. The CIFS (common Internet file system) protocol is not available for the Dell PowerEdge 750, 850, or 860.

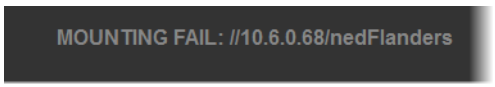


Remote Storage page (CIFS protocol selected)

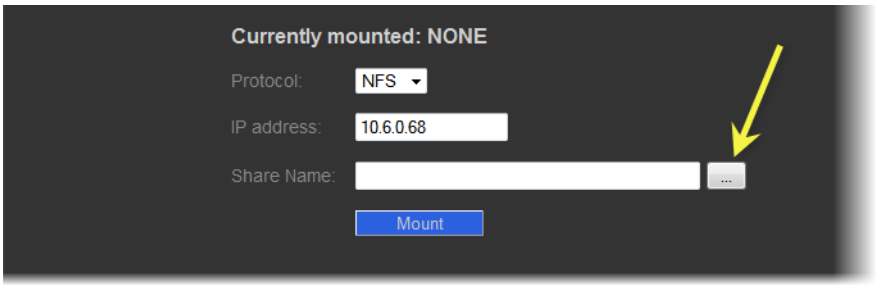


Remote Storage page (NFS protocol selected)

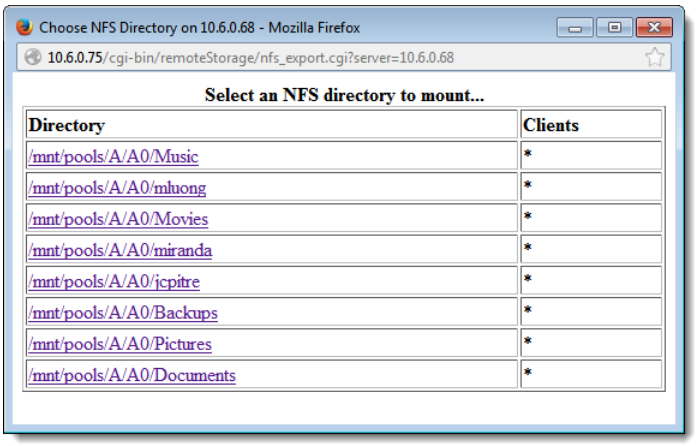
3. If you selected CIFS as a protocol, if required, enter a valid user name and password.

> **Note:** If the remote folder requires credentials and you did not enter any, the mounting process will fail, giving the following message:
>
> 
>

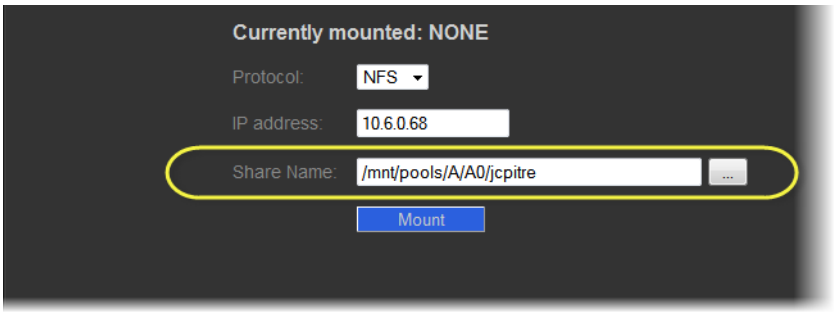
4. Type the IP address of the external drive.
5. Next to **Share Name**, click the Browse button (...).



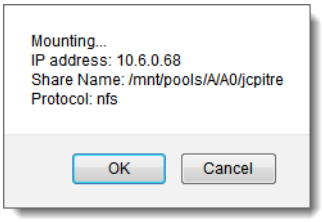
A browser window appears displaying a list of the external drive's shared directories.



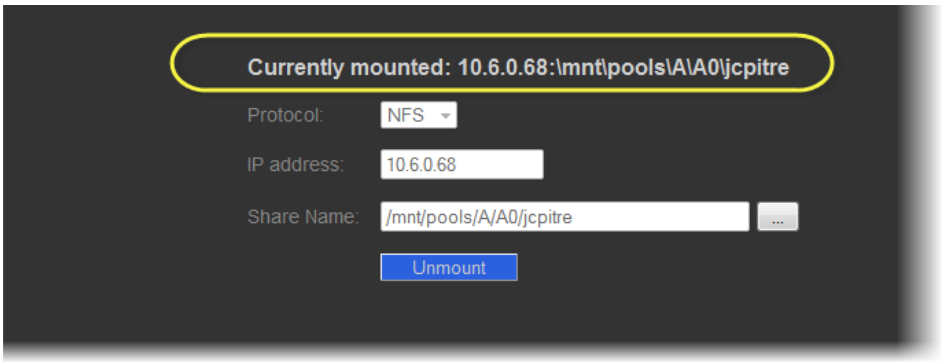
6. Click the shared directory you would like to mount.
   The directory name appears next to **Share Name** in the *Remote Storage* page.



7. Click **Mount**.
   A progress message appears.



8. Click **OK**.
   The mounted directory on the external drive appears on the Remote Storage page.



Logging an Audio Stream's Loudness Data

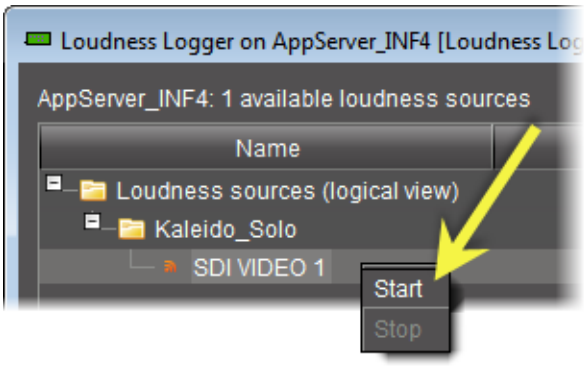
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

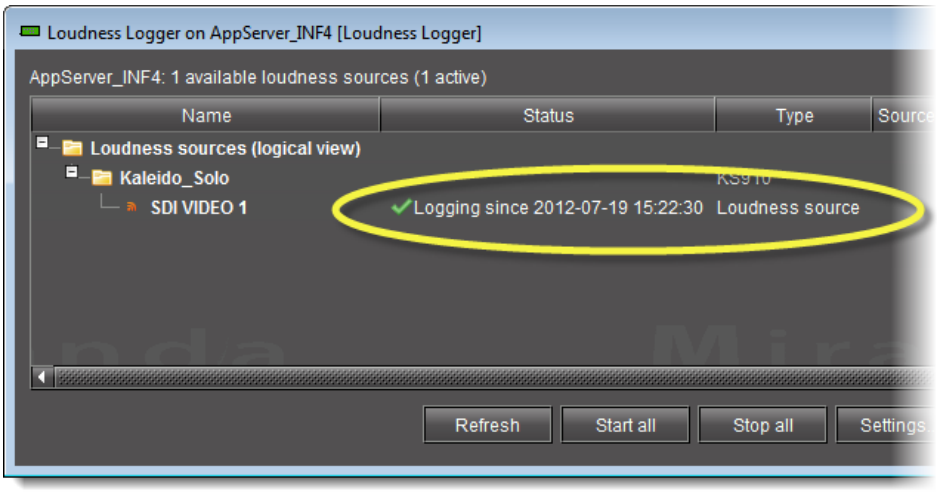
- There is a device streaming loudness values, such as a Kaleido-Solo, visible to your Application Server.
- You have mounted an external storage drive to the designated `/usr/local/repository/loudness` directory on your Application Server (see Mounting a Remote Shared Drive in your Application Server, on page 184).
- You have configured loudness alarms published in GSM (see Configuring Settings for Loudness Logger Alarms, on page 201).
- You have opened **Loudness Logger** (see page 704).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Logging and Analyzing Loudness, on page 131).

To log an audio stream's loudness data

1. In **Loudness Logger**, find the loudness source for which you would like to create a log.
2. Right-click the source and click **Start**.



Loudness Logger begins logging loudness data from the indicated source.



Stopping a Loudness Log Recording

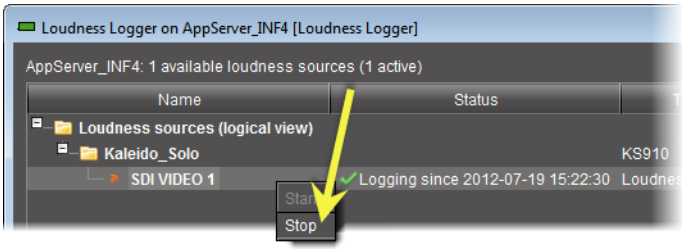
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

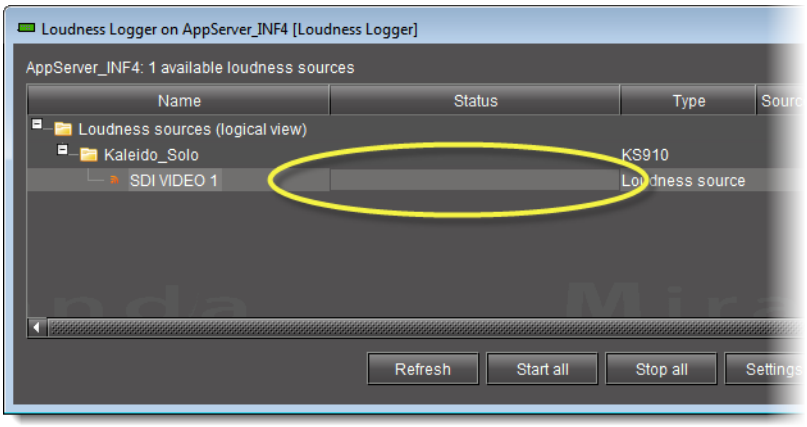
- You have opened **Loudness Logger** (see page 704).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Logging and Analyzing Loudness, on page 131).

To stop a loudness log recording

1. In **Loudness Logger**, find the audio source whose loudness data you would like to stop recording.
2. Right-click this audio source and click **Stop**.



The **Status** column should be blank indicating that logging has stopped for this audio source.



Configuring General Audio Loudness Analyzer Settings

Perform this procedure to define time zone as well as search parameters when searching for loudness log files on the NAS drive.

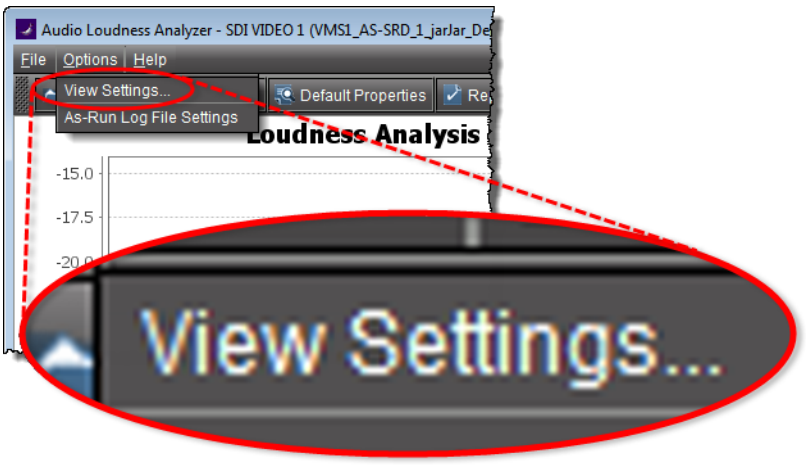
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

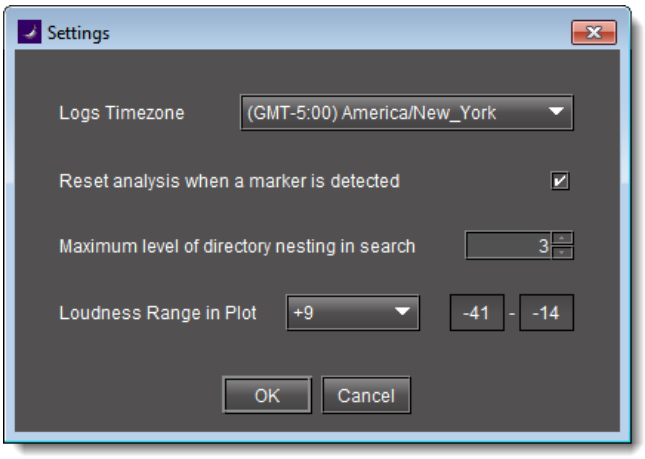
- You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Logging and Analyzing Loudness, on page 131) **[RECOMMENDED]**.
- If the loudness data file you intend to analyze is segmented but segment information is *NOT* contained within the loudness data itself, you may wish to import segment information from an external `As-Run` log file. If this is the case, make sure you have available on your local file system (or on the network) the appropriate `As-Run` log file.

To configure general Audio Loudness Analyzer settings

1. In **Audio Loudness Analyzer**, on the **Options** menu, click **View Settings**.

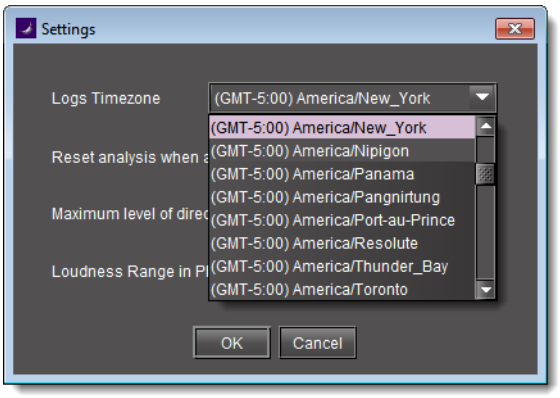


The **Settings** window appears.



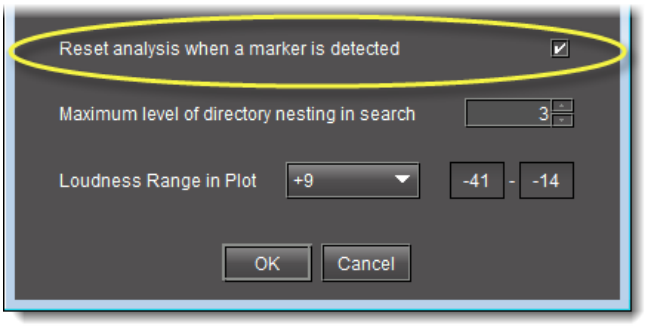
2. Select the time zone that matches your logs.

> **Note:** **Audio Loudness Analyzer** is time zone-agnostic, meaning it displays a data plot's time code as UTC (coordinated universal time). When you configure your general **Audio Loudness Analyzer** settings, make sure you set the time zone to that of the signal being analyzed.

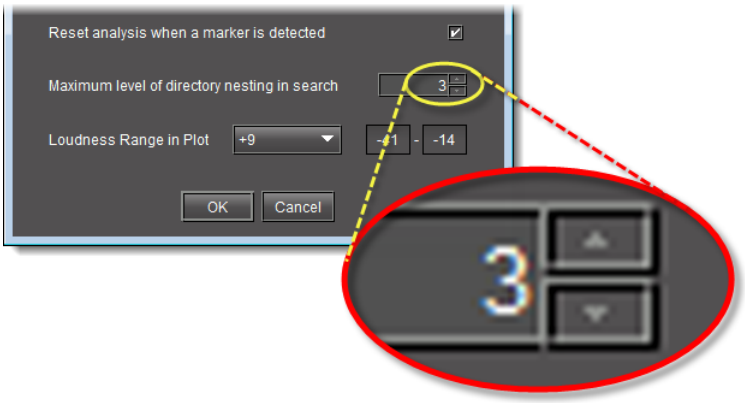


3. Select **Reset analysis when a marker is detected** if you would like for the integrated value to reflect only those data belonging to the segment.

   By contrast, if you would like for your integrated value to reflect the data belonging to the entire analysis range, then clear this check box.



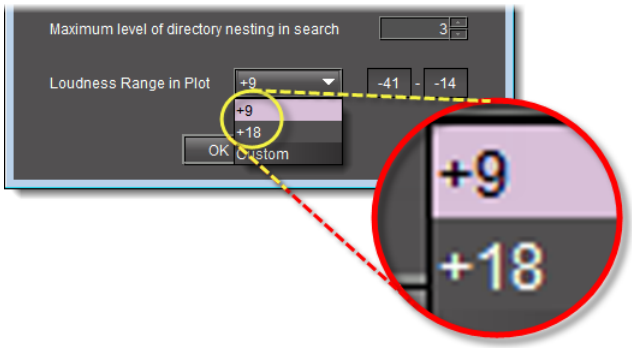
4. Next to **Maximum level of directory nesting in search**, use the *Up* and *Down* arrow buttons to select the number of nested levels in which you would like **Audio Loudness Analyzer** to search for log files.



Notes

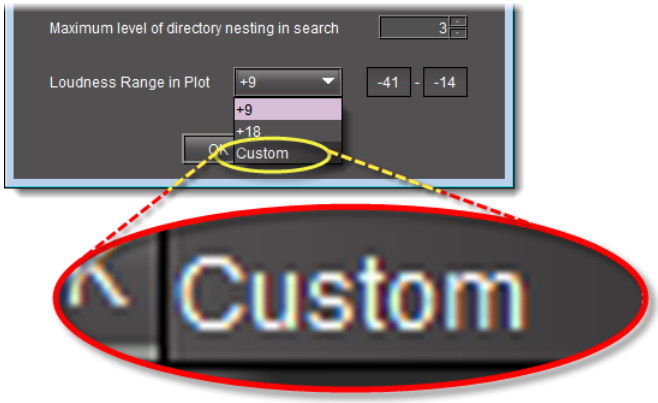
- Selecting **3**, for example, instructs **Audio Loudness Analyzer** to search in the directory named in the path you will define later when you open a loudness log file and then within the next *three* nested levels down.
- If you select **0**, **Audio Loudness Analyzer** only searches for log files within the immediate level of the directory named in the path.
- The deeper you search into nested directories, the slower the search operation will be.

5. Next to **Loudness Range in Plot**, do **ONE** of the following:
   - Select a preset loudness range to be visible in your data plot (taking note of the range values).

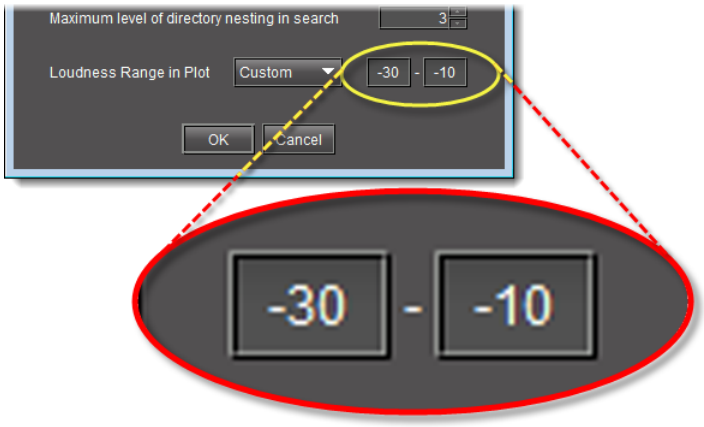


OR,

a) Select **Custom**.



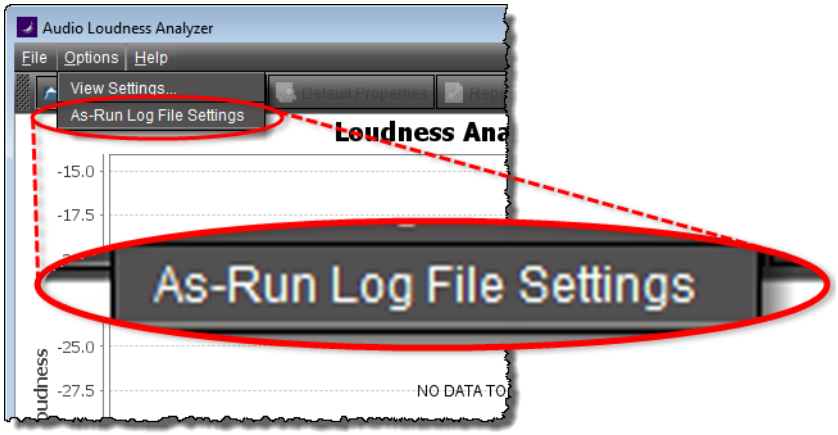
b) Manually enter a custom range.



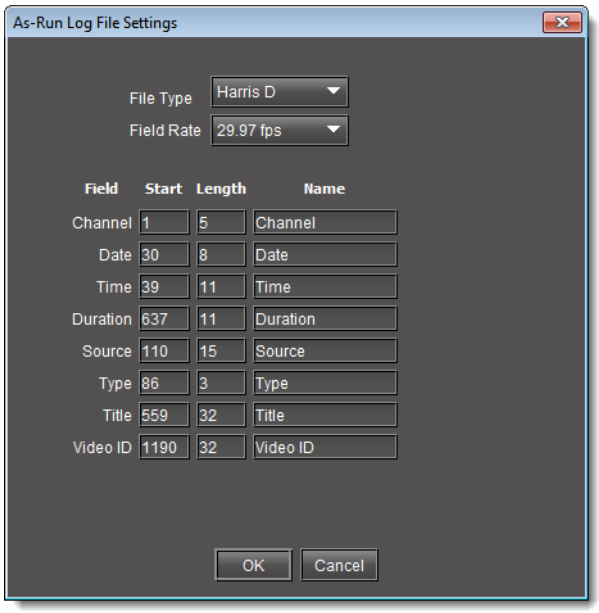
6. Click **OK**.

7. If you intend to analyze a segmented loudness log file using an As-Run log file, perform the following sub-steps:

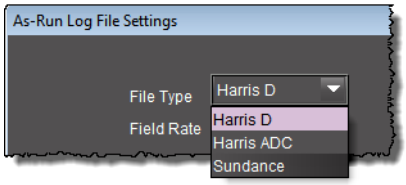
   a) On the **Options** menu (of **Audio Loudness Analyzer**), click **As-Run Log File Settings**.



   The **As-Run Log File Settings** window appears.



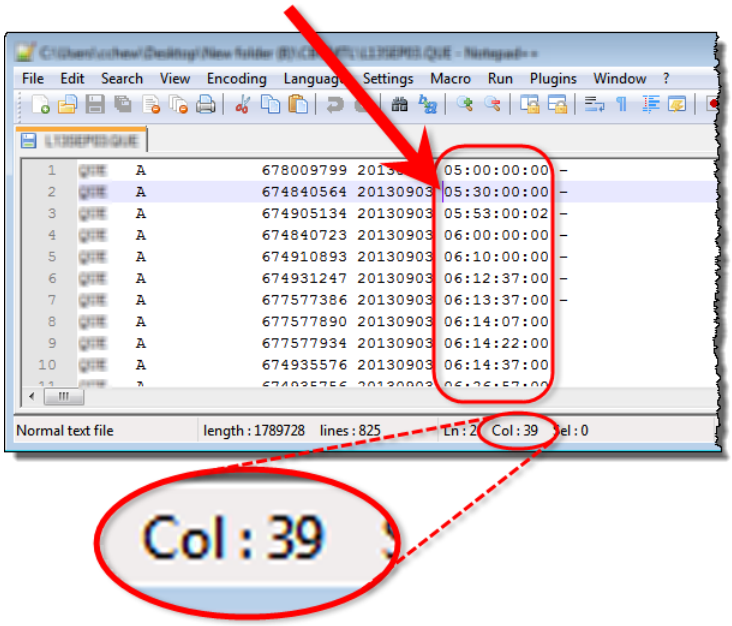
   b) Specify the segment file type used to format your As-Run log file.



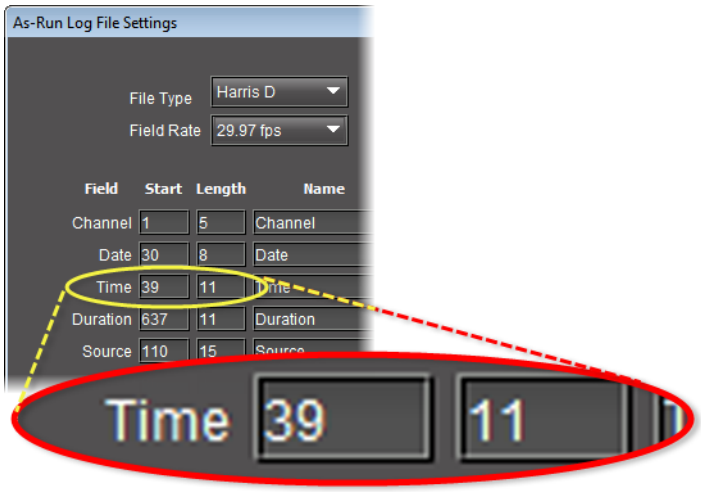
   c) Specify the segment parameters of your loudness log file according to the As-Run file.

The segment parameters allow iControl to read discrete parameter data from the As-Run text file by specifying the starting character in any given row in the file, the maximum length of the string, and the name of the field.

Note: Segment parameter values most likely are already known and defined within your organization. However, if they are not known, you may be able to parse them by examining the As-Run log file in a text editor. See the following two images for an example.



Sample As-Run log file (circling the Time parameter); arrow indicates cursor's starting point is character 39—(see next graphic)



Starting character of Time parameter correctly mapped in As-Run Log File Settings window as 39 (see previous graphic)

d) In the **As-Run Log File Settings** window, click **OK**.

See also

For more information about **Audio Loudness Analyzer** and relevant tasks (including more detail about the As-Run log file), see the *Audio Loudness Analyzer User Manual*, available by clicking **Help** in **Audio Loudness Analyzer**.

Opening a Loudness Log File in Audio Loudness Analyzer

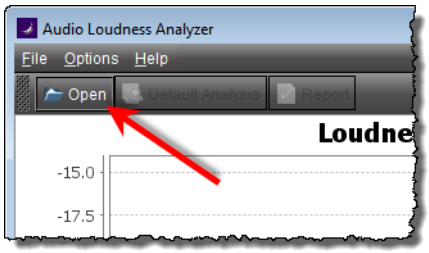
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- The loudness log file you would like to open exists on the mounted external drive.
- You have opened **Audio Loudness Analyzer** (see page 705).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Logging and Analyzing Loudness, on page 131).

To open a loudness log file

1. In **Audio Loudness Analyzer**, do **ONE** of the following:
   - Click **Open**.

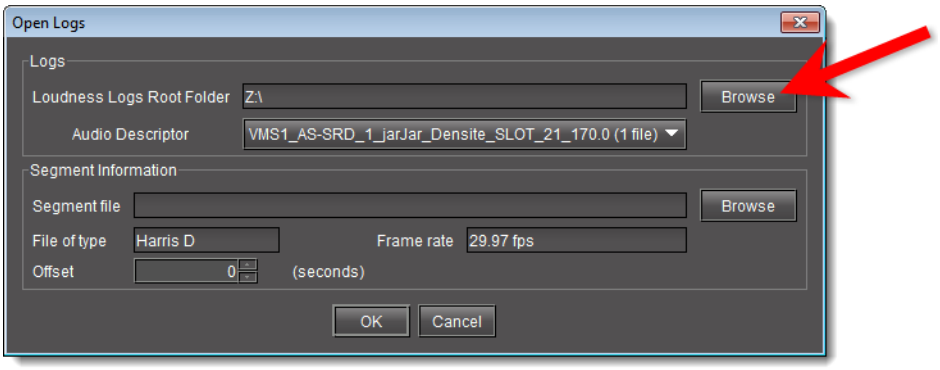


OR,

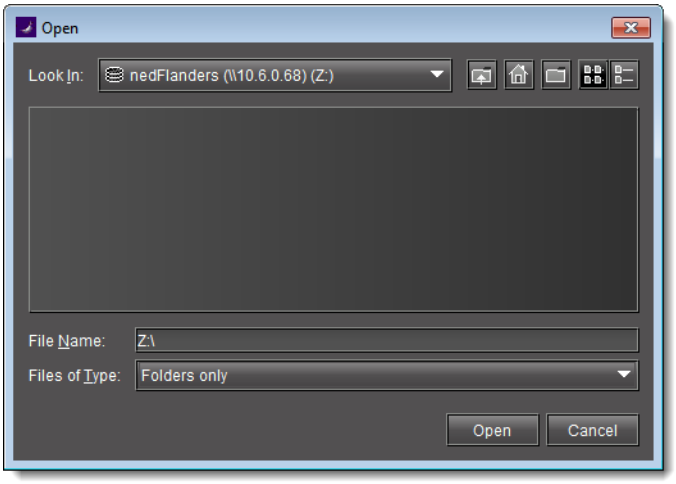
- On the **File** menu, click **Open**.

The **Open Logs** window appears.

2. Next to **Loudness Logs Root Folder**, click **Browse**.



3. In the **Open** window, in the **File Name** box, type the path to the directory on the NAS drive containing the loudness data.



IMPORTANT: System behavior

- If, in addition to mounting the NAS drive to the `loudness` directory of your Application Server, you have also mapped the NAS drive as a local drive on your client PC, then the address you type or paste should point to this mapped local drive, such as the following:

  `Z:\`

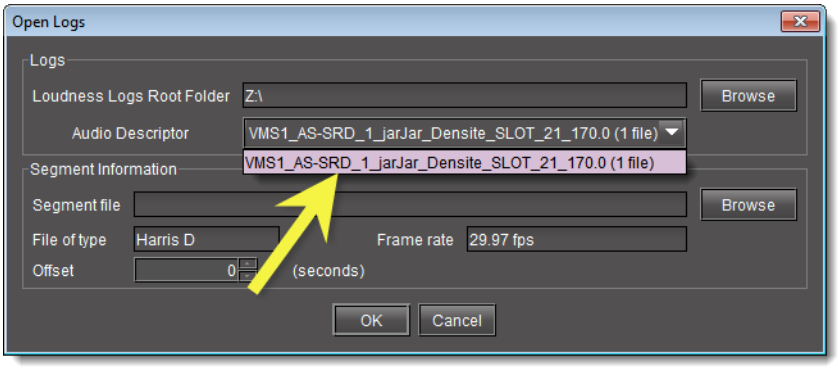
  Otherwise, the address and path should be in the following format:

  `\\<IP address of NAS drive>\<path to directory with loudness data>`

- If you have *NOT* mounted the NAS drive as a local drive on your client PC, when you type the path to the loudness directory, you must include at least one directory level in this path.

  Simply typing **`\\<IP address>\`** is insufficient and you will be unable to browse the NAS directories.

4. In the **Open Logs** window, in the **Audio Descriptor** list, select the desired loudness data set to analyze.



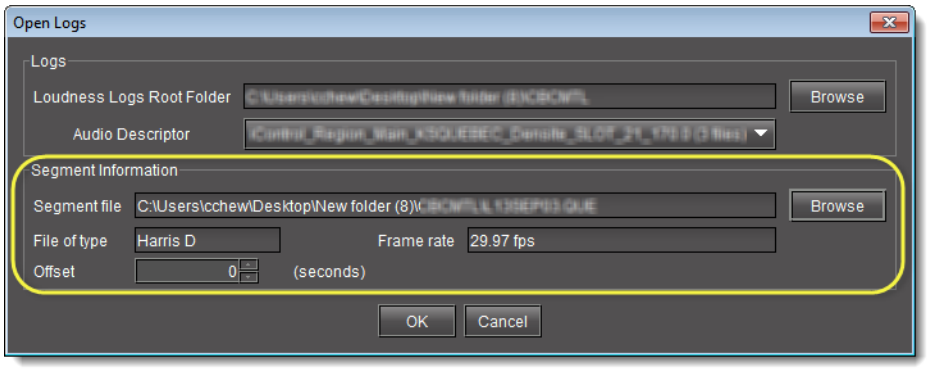
Note: The data set may contain one file or several files. The number of files in each data set is indicated in parentheses.

5. If your loudness log file is a segmented file and you have a a Segment file (As-Run log file) available, perform the following sub-steps:

   a) In the **Segment Information** area, click **Browse**.

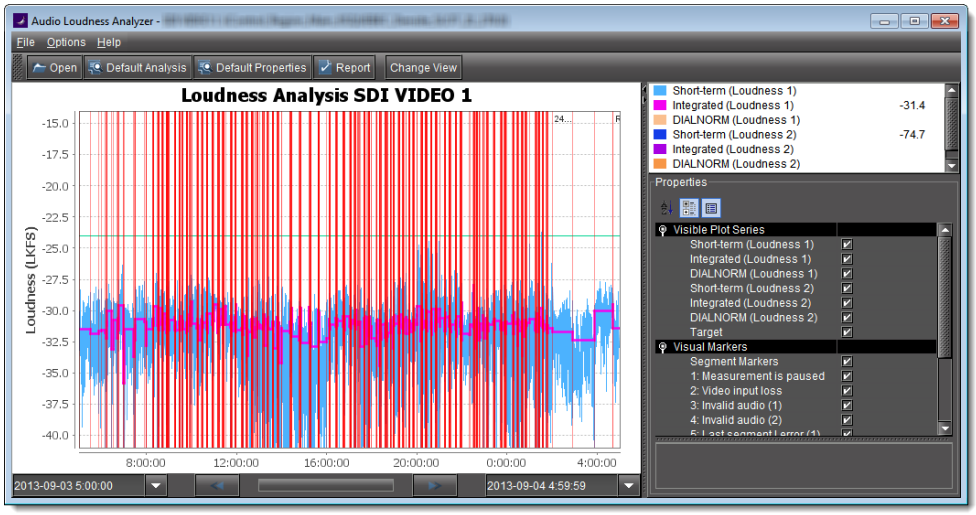
   b) Browse for the appropriate `As-Run` log file on your local file system, and then click **Open**.

   The **Segment Information** area of the **Open Logs** window displays the selected Segment file as well as the mapped segment information settings (see step 7 of Configuring General Audio Loudness Analyzer Settings on page 190).



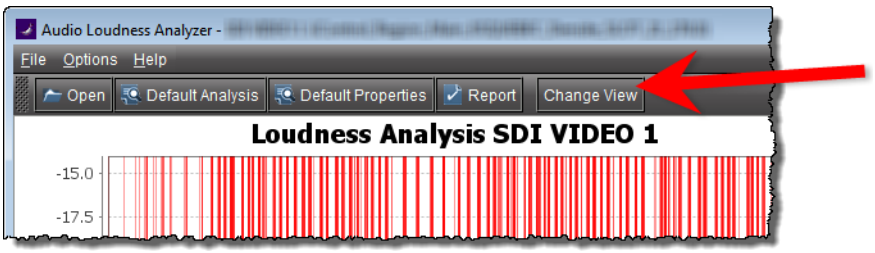
c) Click **OK**.

Audio Loudness Analyzer loads, analyzes, and then presents the loudness data.

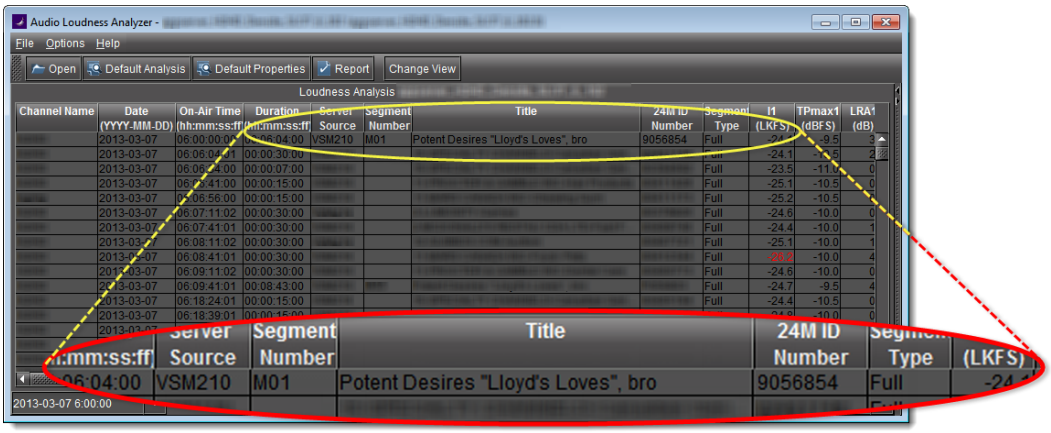


> **Note:** If there is segment information either embedded within the loudness log or extracted from an external As-Run log file, then you will see vertical red lines showing the start and stop times of discrete segments.

6. To see the tabular representation of the data, click **Change View**.



Audio Loudness Analyzer's *Tabular* view appears, displaying a list of the segments (if segment information was present).



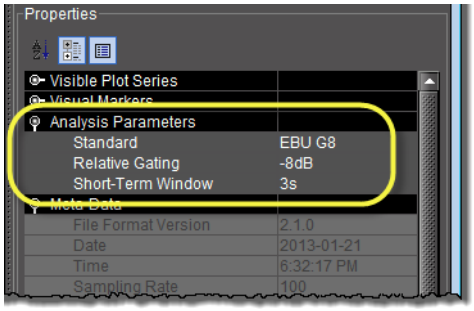
See also

For more information about **Audio Loudness Analyzer** and relevant tasks (including more detail about the As-Run log file), see the *Audio Loudness Analyzer User Manual*, available by clicking **Help** in **Audio Loudness Analyzer**.

Configuring Loudness Analysis Parameters

There are three loudness analysis parameters you may configure:

- Loudness standard
- Relative gating
- Short-term window



Configurable loudness analysis parameters

Parameter name	Description	Data set
Standard	The program compliance loudness standard against which the loudness data will be measured. • *G8* refers to the now-obsolete version of EBU-R128 recommending a gate value of -8LU. The currently recommended value is -10LU. • A85 1770-1 leaves the threshold level up to broadcasters and recommends an anchor when available and a gate if necessary (used in USA, Canada). • A85 1770-2 recommends a gate is **ALWAYS** enabled, having a threshold set to -10LU (used in the European Union). • ARIB TR-B32 is based on A85 1770-2 with a recommended threshold of -24LKFS (absolute gate at -70LKFS, -10LU relative gate, 400ms sample blocks).	• EBU G8 • EBU G10 • ARIB TR-B32 • A85 1770-1 • A85 1770-2
Relative Gating	The concept of filtering out low volume sound by a configurable dB (LU) level below the absolute loudness calculation in order to prevent skewing a loudness calculation with very quiet sounds or silence.	• -10dB • -8dB
Short-Term Window[1]	The *intermediate* length sliding time window.	• 1s • 2s • 3s • 4s • 5s • 6s • 7s • 8s • 9s • 10s

1. Once loudness data is plotted in Analyzer, you should expect for the Short-Term Window plot series not to begin until one cycle of its configured duration to have elapsed. This is due to there not being enough data before this point with which to produce a moving average.

Note: Changes you make to any analysis parameters are immediately applied to a new analysis.

See also

For more information about **Audio Loudness Analyzer** and relevant tasks, see the *Audio Loudness Analyzer User Manual*, available by clicking **Help** in **Audio Loudness Analyzer**.

Configuring Settings for Loudness Logger Alarms

In order to publish **Loudness Logger** alarms to GSM you must perform this procedure.

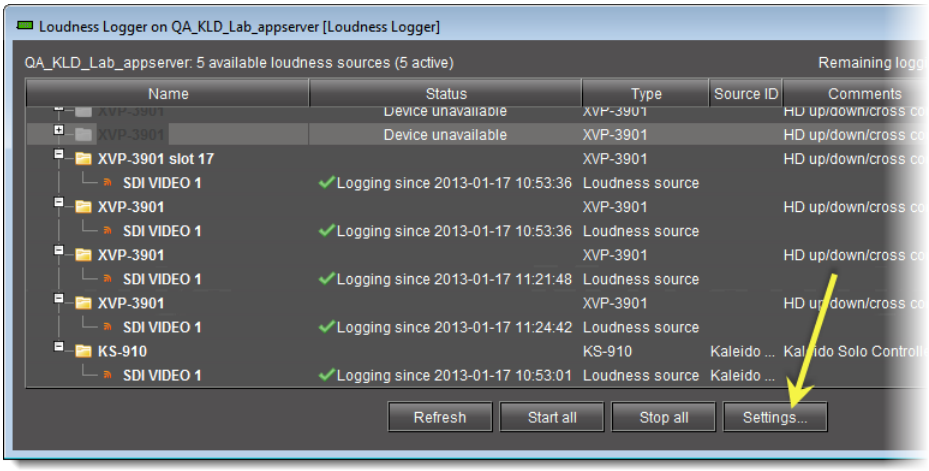
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **Loudness Logger** (see page 704).
- **[RECOMMENDED]:** You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Logging and Analyzing Loudness, on page 131).

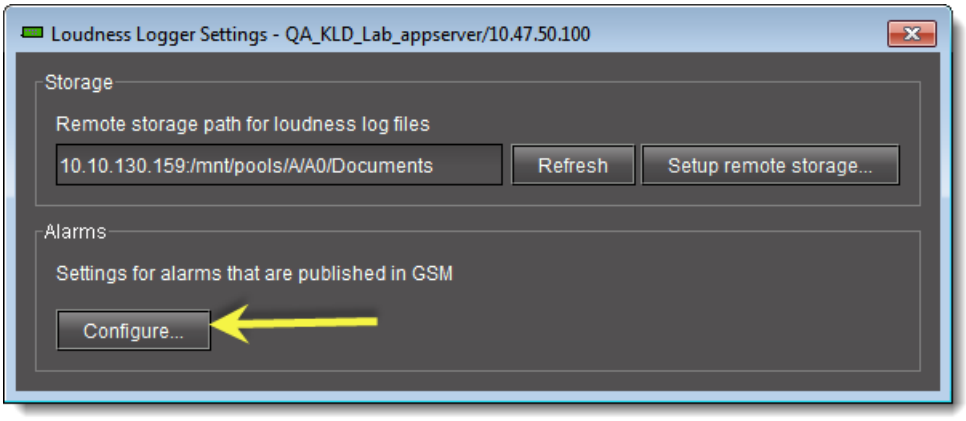
To configure settings for loudness alarms

1. In **Loudness Logger**, click **Settings**.

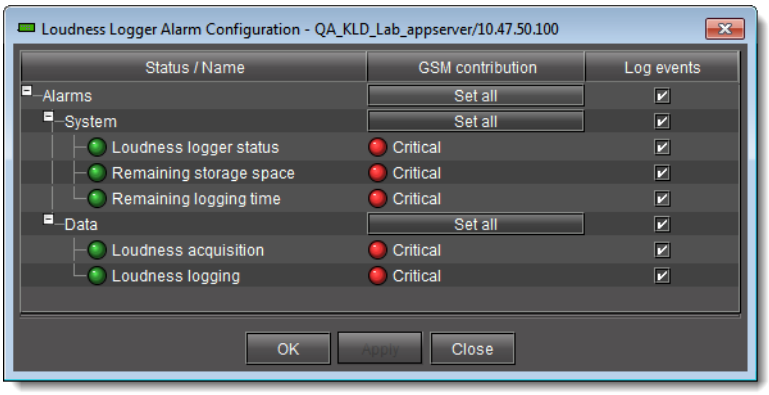


The **Loudness Logger Settings** window appears.

2. Click **Configure**.



The **Loudness Logger Alarm Configuration** window appears.



3. Select loudness-related alarms to be published as required, and then click **OK**.

   The **Loudness Logger Alarm Configuration** window closes.

4. Close the **Loudness Logger Settings** window.

Zooming into Audio Loudness Analyzer's Data Plot

After loading a loudness data file into **Audio Loudness Analyzer**, the plot of the loudness data may not show, by default, the granularity of detail you might like to see at first. Additionally, the time period covered by the data may cover too large a time span.

You can effectively zoom into the data by specifying a subset time period within the initial graph, thereby increasing granularity and removing extraneous data.

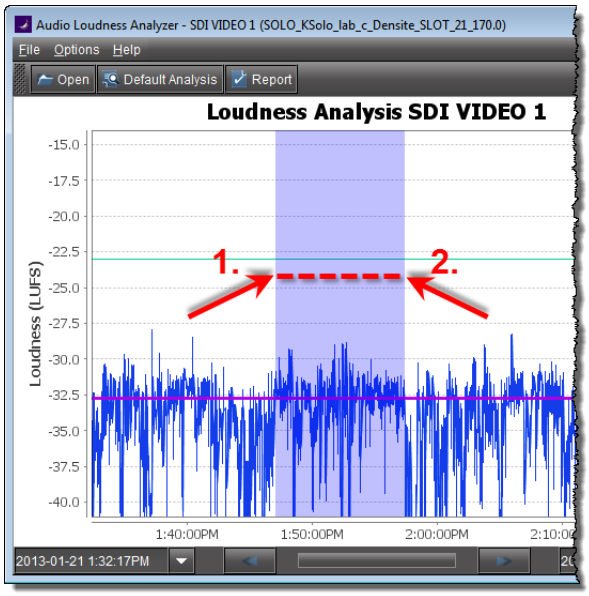
> **Note:** You may choose to either configure analysis parameters before you zoom or after you zoom with the same end-effect. You will lose analysis parameter data **ONLY** when you click **Default Analysis**.

REQUIREMENT

Before beginning this procedure, make sure you have opened a loudness data file in **Audio Loudness Analyzer** (see page 196).

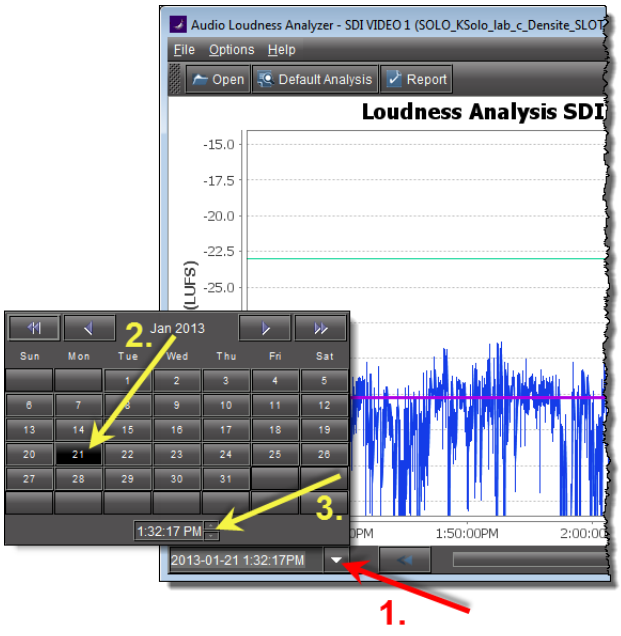
To zoom into Audio Loudness Analyzer's data plot

1. In **Audio Loudness Analyzer**, do **ONE** of the following two sub-procedures:
   a) On the data plot, use your mouse to click and hold on any point along the vertical line marking the desired beginning time of your zoom.
   b) Drag the mouse to any point along the vertical line marking the desired end time of your zoom.
   c) Release the mouse button.



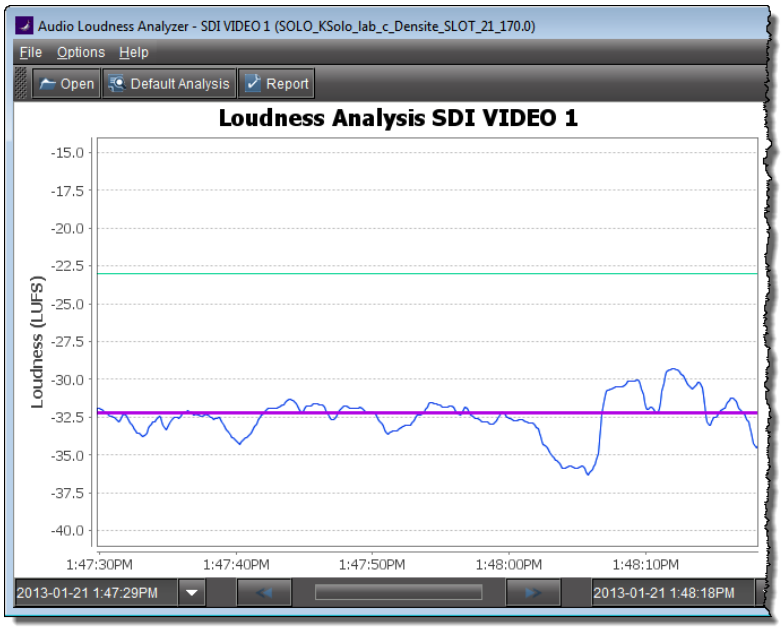
OR,

a) On the bottom-left side of **Audio Loudness Analyzer**, use the *Start-time* calendar to indicate the exact beginning date and time of your zoom.



b) On the bottom-right side of **Audio Loudness Analyzer**, use the *End-time* calendar to indicate the exact end date and time of your zoom.

Audio Loudness Analyzer reloads the data stream using the new time range demarked by the new start- and end-times.



2. Repeat step 1 if you must zoom into the data plot further.

See also

For more information about **Audio Loudness Analyzer** and relevant tasks, see the *Audio Loudness Analyzer User Manual*, available by clicking **Help** in **Audio Loudness Analyzer**.

Generating a Loudness Analysis Report

Audio Loudness Analyzer permits you to generate a report in PDF format. The report provides the data currently displayed in **Audio Loudness Analyzer**, including the chart at its current scaling (zoom), as well as the parameters configured.

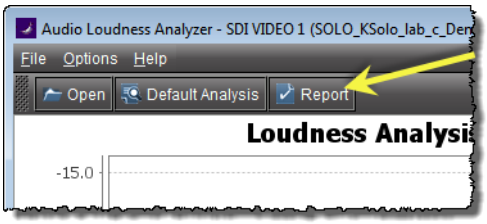
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened a loudness data file in **Audio Loudness Analyzer** (see page 196).
- You have adjusted the scaling of **Audio Loudness Analyzer**'s data plot to the desired level (see Zooming into Audio Loudness Analyzer's Data Plot, on page 203).
- You have selected the plot series you would like to include in your report and selected the desired analysis parameters (see Configuring Loudness Analysis Parameters, on page 200).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Logging and Analyzing Loudness, on page 131).

To generate a loudness analysis report

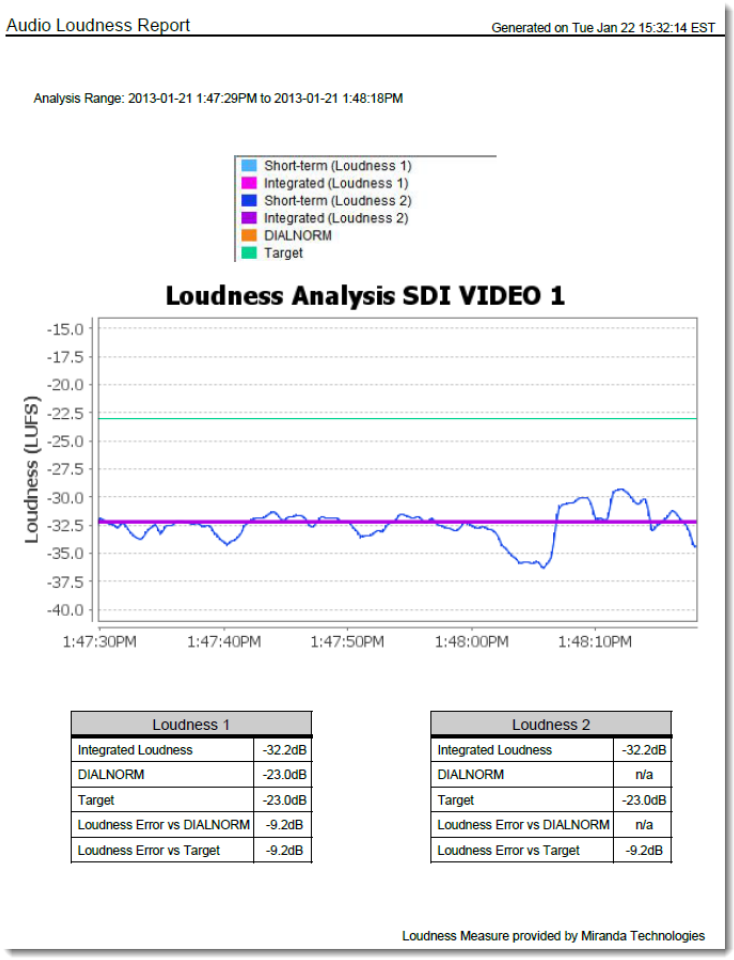
1. In **Audio Loudness Analyzer**, click **Report**.



The **Save** window appears.

2. Save the PDF file to a local directory.

   The PDF file contains all of the information currently in view in **Audio Loudness Analyzer**.



Loudness analysis report (taken from the PDF output)

See also

For more information about **Audio Loudness Analyzer** and relevant tasks, see the *Audio Loudness Analyzer User Manual*, available by clicking **Help** in **Audio Loudness Analyzer**.

Creating, Viewing, and Deleting Channel Performance Reports

Enabling and Disabling the Automatic Incident Resolution Function for iC Reports

Enable this function if you would like to generate reports using any of the *Availability* default report templates[1]. Disable this function only after you have finished using the *Availability* default report templates, and if you would like to avoid using up space in the database (when the function is enabled, each alarm creates an incident).

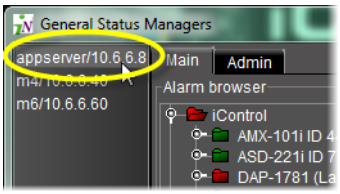
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

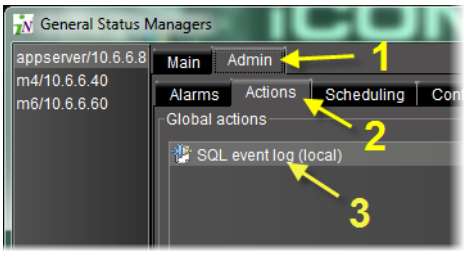
- All incidents are resolved (see page 181).
- You have opened the GSM Alarm Browser (see Opening the GSM Alarm Browser, on page 710).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Channel Performance Reporting, on page 130).

To enable or disable the automatic incident resolution function for iC Reports

1. In the GSM Alarm Browser, select the desired Application Server on the left pane.



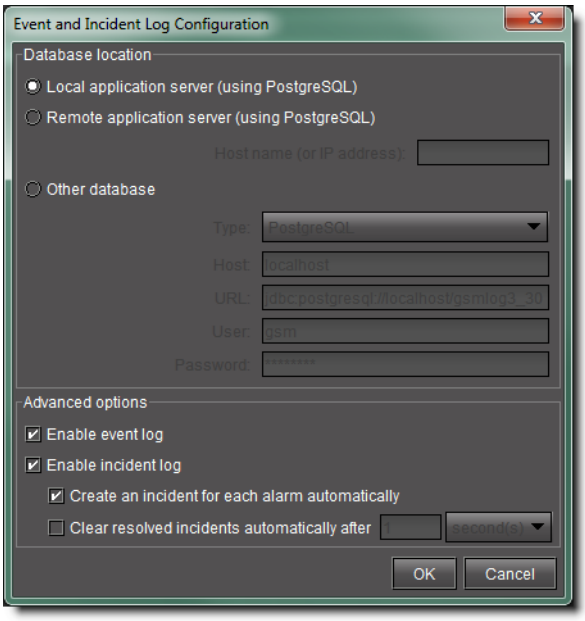
2. Click the **Admin** tab, and then click the **Actions** tab.



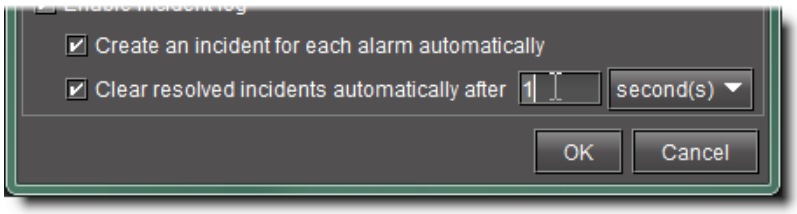
3. Click **SQL event log (local)** to select it, and then click **Edit**.

   The **Event and Incident Log Configuration** window appears.

1. The *Availability* default report templates are as follows: <10 Channels with Highest Availability Last 24 hours>, <10 Channels with Highest Availability Last 7 days>, <10 Channels with Lowest Availability Last 24 hours>, <10 Channels with Lowest Availability Last 7 days>

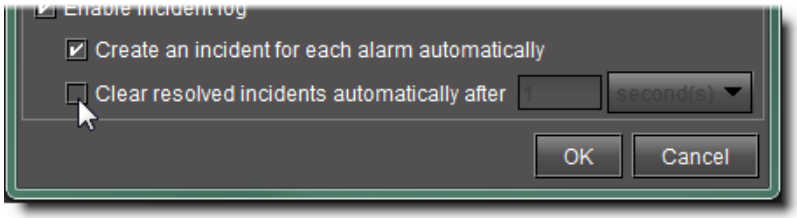


4. Perform only **ONE** of the following two actions:
   - If you would like to set the system to clear resolved incidents automatically, select the **Clear resolved incidents automatically after** check box, and then set it to resolve incidents every second.



   OR,

   - If you would like to set the system **not** to clear resolved incidents automatically, clear the **Clear resolved incidents automatically after** check box.



5. Click **OK**.

Creating a Report Template

Create a report template when you want to customize filter parameters for report generation.

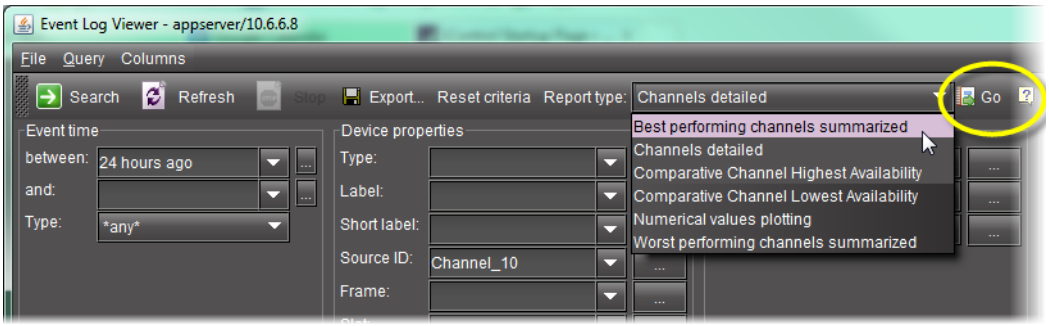
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

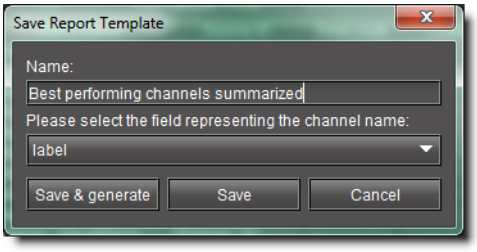
- You have opened **Event Log Viewer** (see page 697).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Channel Performance Reporting, on page 130).

To create a report template

1. In **Event Log Viewer**, configure report filter parameters as desired (see Manually Configuring Event and Incident Logging, on page 139).
2. Select the desired report type from the list on the toolbar, and then click **Go**.



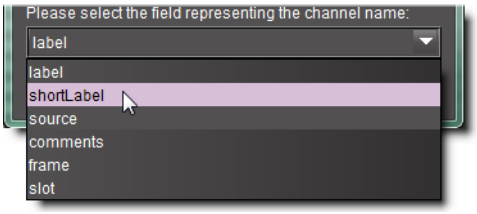
The **Save report template** window appears.



3. If you would like your template to have a unique name, type the desired name for your new template.

> **Note:** The default template name is the same as the name of the report type it originated from.

4. Select the field representing the channel name.



5. Perform only **ONE** of the following three actions:
   - Click **Save & generate** to save the new template to the Application Server and generate a report based on this template.

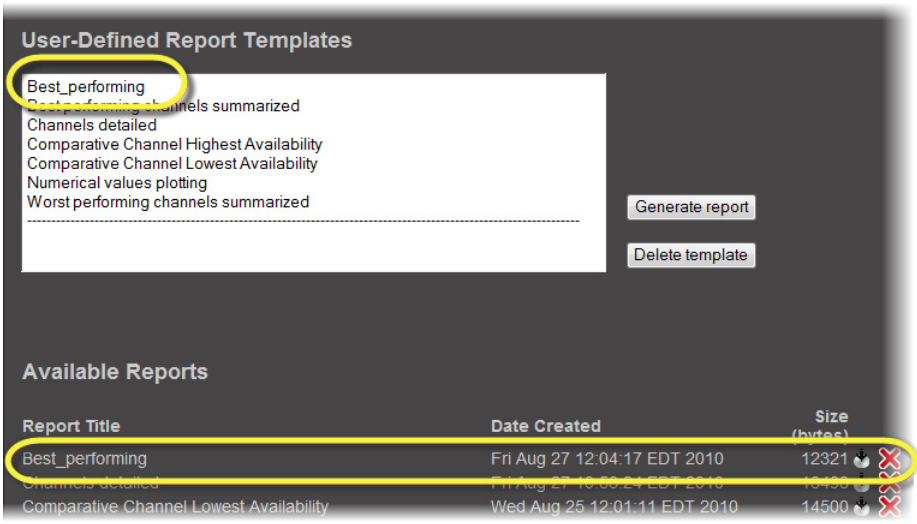
     The system opens the *Reports* page and generates a report.

     Note: Once a report is generated, it appears in the **Available Reports** list, ordered chronologically according to the report generation time (the most recent report at the top of the list). The new user-defined template appears in the **User-Defined Report Templates** list.

     OR,
   - Click **Save** to save the new template to the Application Server.

     The **Save report template** window disappears. The next time you open the *Reports* page, the new template appears in the **User-Defined Reports Templates** list.

     OR,
   - Click **Cancel** to cancel the operation.



Saved report template and generated report on the Reports page of iControl

Selecting an Existing Report Template

In iControl, when generating a report you can select from a list of report templates if an existing template (either default or user-defined) meets your needs.

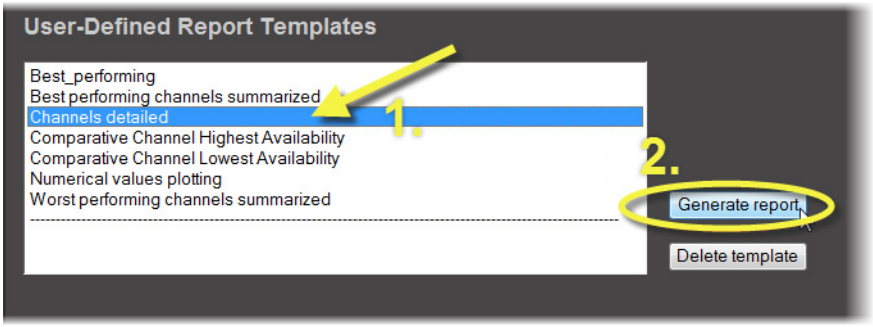
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

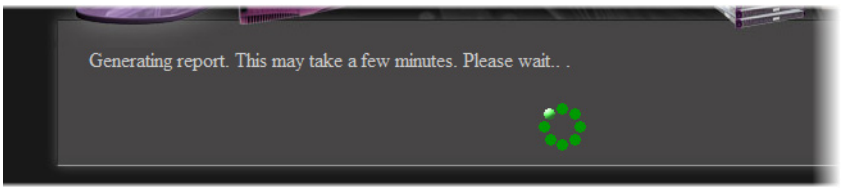
- The URIs referenced in the alarm template you are using correspond to URIs currently existing in your Application Server's database.
- You have opened the *Reports* page (see page 683).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Channel Performance Reporting, on page 130).

To select an existing report template

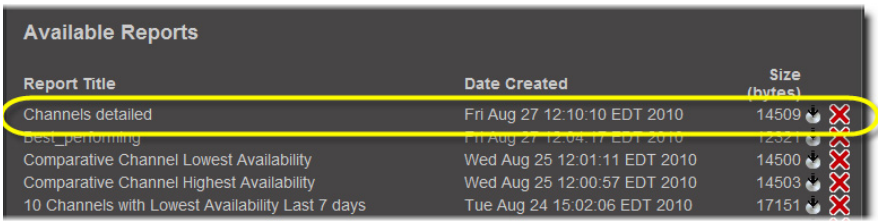
1. On the *Reports* page, select the report template you wish to use from either the **Default Report Templates** list or the **User-Defined Report Templates** list:
2. Click **Generate report** (under the list from which you selected a template).



The system displays a progress page while generating the report.



Once the report is generated, it appears in the list of **Available Reports** with the same name as the template you selected.



Displaying a Report in a Web Browser

Display a graphical representation of a report directly in your Web browser after you have generated a report or from a report generated in an earlier session.

REQUIREMENTS

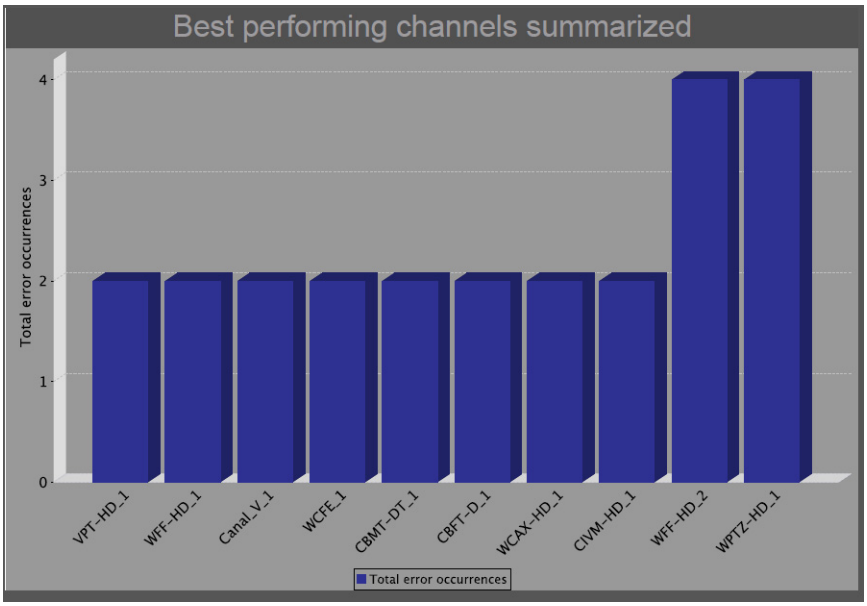
Make sure you meet the following conditions before beginning this procedure:

- You have opened the *Reports* page (see page 683).
- The report you would like to display is listed among the **Available Reports** on the *Reports* page.
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Channel Performance Reporting, on page 130).

To display a report in a Web browser

- On the *Reports* page, under **Available Reports**, click the report title of the report you would like to view.

  A new browser page appears displaying a graphical representation of the report.



Note: The title displayed at the top of the report graphic reflects the name of the original report type and not the name of the report nor the report template.

Downloading a Report (PDF File)

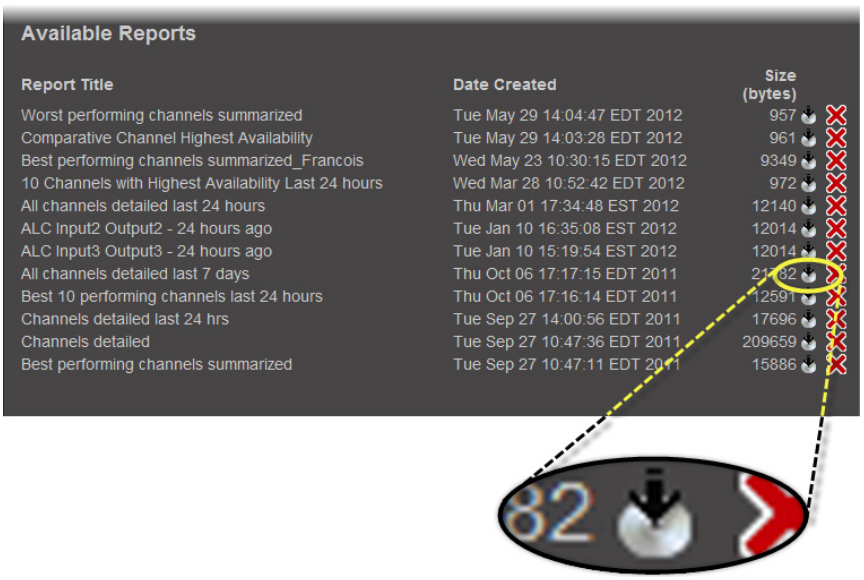
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

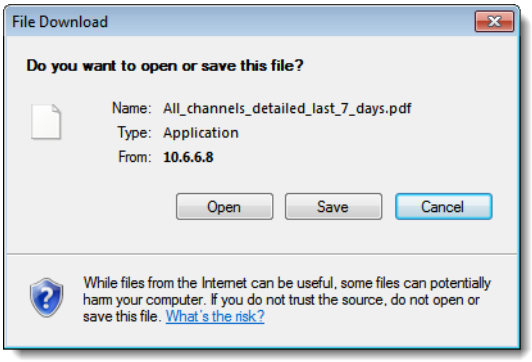
- You have opened the *Reports* page (see page 683).
- The report of which you would like a PDF version is listed among the **Available Reports** on the *Reports* page.
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Channel Performance Reporting, on page 130).

To download a report as a PDF file

1. On the *Reports* page, under **Available Reports**, click the icon resembling an optical disk ( ).

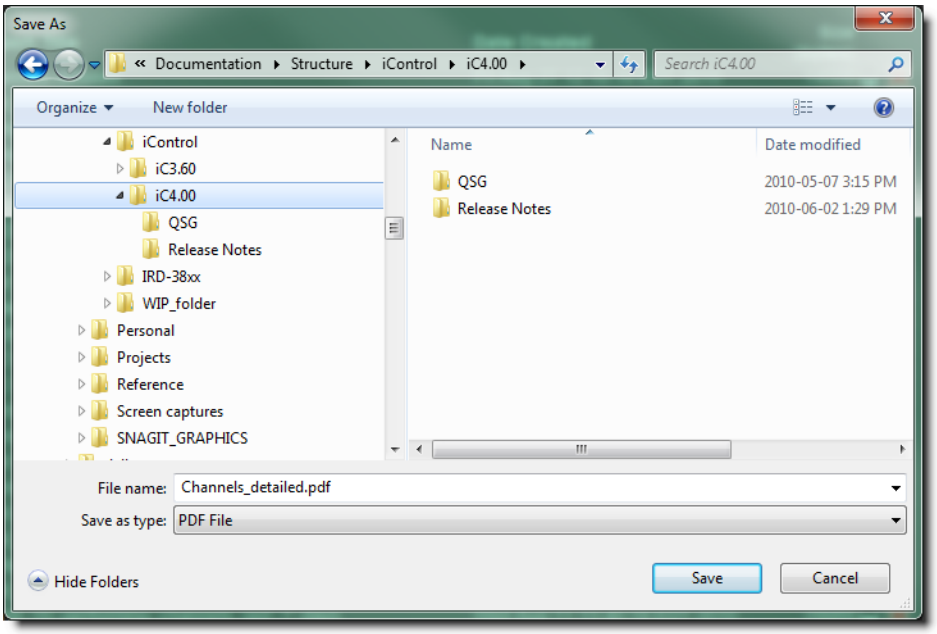


A **File Download** window appears.



2. Click **Save**.

   The **Save As** window appears.



Note: The default file name is the name of the report.

3. Browse to the desired location, type the desired file name (or accept the default), and then click **Save**.

   A PDF version of the report is saved to the designated location.

Deleting a Report

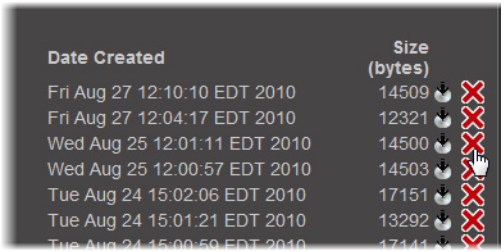
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened the *Reports* page (see page 683).
- The report you would like to delete is listed among the **Available Reports** on the *Reports* page.
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Channel Performance Reporting, on page 130).

To delete a report from an Application Server

1. On the *Reports* page, under **Available Reports**, locate the report you would like to delete.
2. In the row corresponding to the report you would like to delete, click the Delete icon ( ).



Deleting a Report Template

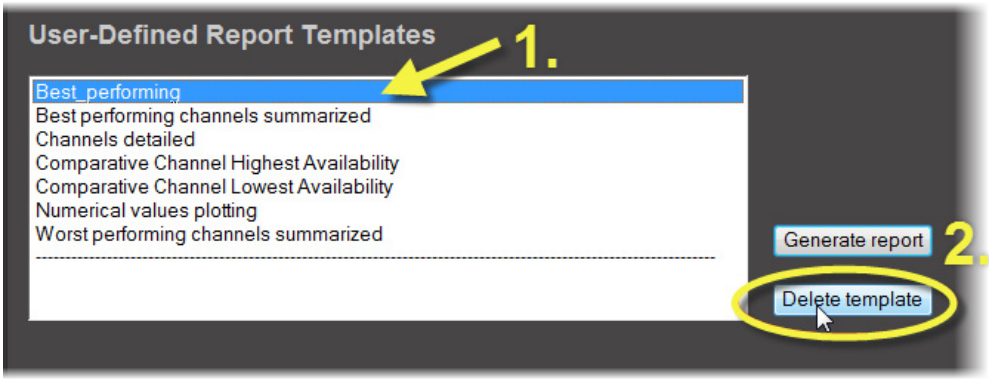
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened the *Reports* page (see page 683).
- The report template you would like to delete is listed among the **User-Defined Report Templates** on the *Reports* page.
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Channel Performance Reporting, on page 130).

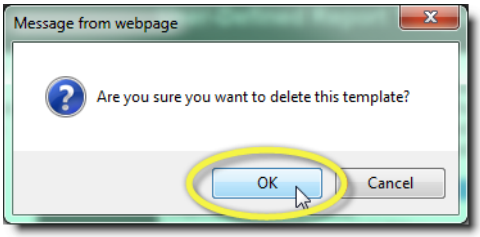
To delete a report template

1. On the Reports page, in the **User-Defined Report Templates** list, locate and select the report template you would like to delete.



2. Click **Delete template**.

   A confirmation message appears.



3. Click **OK**.

   The deleted report template disappears from the **User-Defined Report Templates** list.

Accessing Archived GSM Log Files

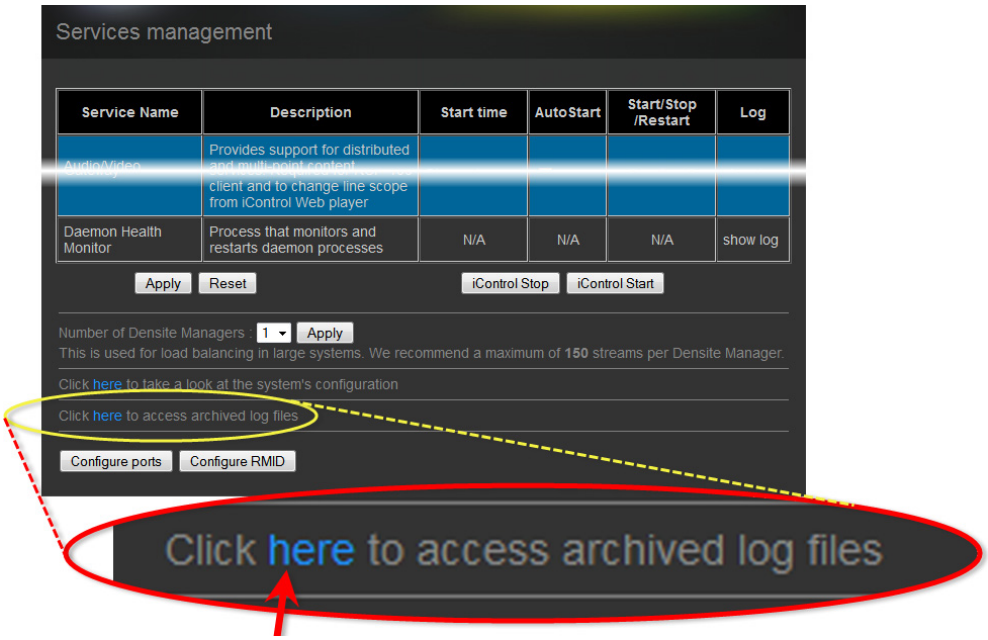
In order to gain access to the latest as well as historic GSM logs—in a comma-separated-values (CSV) format—you must perform this procedure.

REQUIREMENT

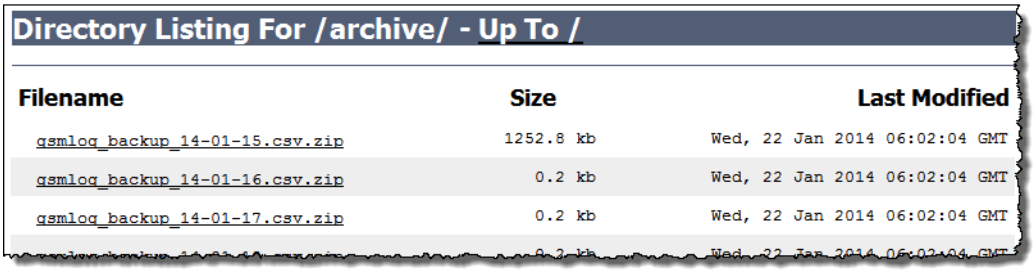
Before beginning this procedure, make sure you have opened the *Services management* page (see page 678).

To access archived GSM log files

1. On the *Services management* page, scroll to the bottom of the page, and then click the link **Click here to access archived log files**.



Your Web browser displays a list of the archived GSM log files.



List of archived GSM log files as seen in Web browser

2. Click the desired log file in the list and follow your browser's instructions to save a local copy.
3. Unzip the log file.
4. Double-click the CSV file to view it in Microsoft Excel.

See also

For more information about interpreting the data in a GSM log file, see GSM Log Files, on page 128.

5 Devices & Services

Summary

Key Concepts

Frame

A *frame* is a modular enclosure used to house a range of processing, interface, and controller modules. iControl can detect frames on a network, and make information about these frames available in iC Navigator—when **Physical view** is selected, iC Navigator displays all devices, including frames. You can click the [+] symbol beside a frame's name (or double-click on a the name itself) to view the contents of its slots.

Services

An iControl service is software running on the Application Server that enables it to communicate with and control devices on the network. Some services, such as the General Status Manager and the RMI Daemon, are available with every iControl system. Others are installed on the Application Server as build-to-order options. The table below describes some common iControl services:

Service Name	Availability	Description
Densité	Default	Densité Manager service responsible for communications with Grass Valley Densité frames over TCP/IP. The Densité Manager starts and stops Densité communicators. It supports multiple instances for load balancing (up to 150 streams per Densité Manager).
GeckoFlex	Default	GeckoFlex Manager service responsible for communications with Grass Valley GeckoFlex frames over TCP/IP. The GeckoFlex Manager starts and stops GeckoFlex communicators.
General Status Manager (GSM)	Default	Service responsible for coordinating the distribution of alarm messages and events on an iControl network.
Global Caché GC100 IR service	Optional	Custom service responsible for communications with the Global Caché GC100 IR Network Adapter.
IRD Service Starter	Optional	Service responsible for communications with Integrated Receiver/Decoder (IRD) devices.

(*Continued*)

Service Name	Availability	Description
Imagestore	Optional	Imagestore Manager service responsible for communications with Grass Valley (Oxtel) Imagestore frames over TCP/IP.
Imaging Connection Manager ttyR0	Optional	Service responsible for serial communications with Grass Valley Imaging series frames. The Imaging Connection Manager starts and stops Imaging Communicators associated with specific serial ports (ttyR0 in the example at left).
RMI daemon	Default	Remote Method Invocation daemon responsible for establishing client/server connections.
Router Manager Service	Default	Router Manager Service responsible serial communications with all routers connected to an Application Server
VTR Control Module ttyR4	Optional	Service responsible for serial communications with a VTR connected to an Application Server. Each VTR Control Module is associated with a specific serial port (ttyR4 in the example at left).
Virtual Service	Default	Virtual Service Manager for building virtual panels such as proc amps
iControl Services Gateway	Default	iControl Services Gateway service for enabling third-party devices and/or monitoring software to interface with an iControl Application Server and devices under its control. Also required for Grass Valley's RCP-100 and RCP-200 clients, and to change line scope from iControl Web player.
Daemon Health Monitor	Default	Process that monitors and restarts daemons (processes)

Communicators

Communicators are software components that implement a specific protocol for controlling a family of devices. Communicators in iControl are responsible for the *discovery* process whereby an Application Server detects Grass Valley devices connected to its serial ports or on the LAN, and initiates services to control these devices.

iControl's communicators are applications that handle the communications between an Application Server and Densité, GeckoFlex, GV Node, or Imaging-series frames on the network. The four types of communicators (Imaging, Densité, GV Node, and GeckoFlex) are configurable services in iC Navigator.

Imaging Communicators allow you to control signal processing and distribution performance modules housed in Grass Valley Imaging series (Symphonie, Quartet) frames. The Imaging series frames are connected to the Application Server using RS-422 serial ports.

Densité Communicators, GV Node Communicators, and GeckoFlex Communicators allow you to control interfacing and distribution modules housed in Densité, GV Node, and GeckoFlex frames, respectively. These frames are connected to the network via their controller card's Ethernet port.

To be able to use a communicator, the service must be configured and activated. If the service is not configured, you will not be able to control the devices even if they are connected. If the service is configured, but there are no cards connected, only the service will be displayed in the navigation pane.

Densité Manager

Densité Manager is a service that allows you to manage multiple Densité, or GV Node frames (using Densité, and GV Node Communicators).

For **Densité Manager** to discover cards and begin controlling services, you need to specify the IP addresses of the Densité, or GV Node frames that it will manage. Depending on the model, a frame may contain up to 24 devices. If you do not add any addresses, or if you add an incorrect address, the Densité Manager will not discover any frames.

GV Node Manager

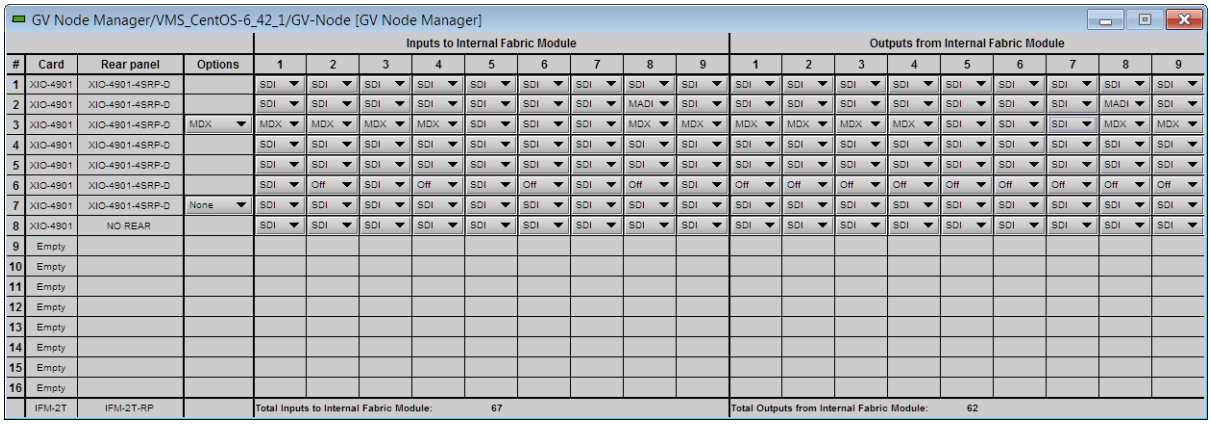
GV Node Manager provides a visual control panel to help you manage a GV Node frame, and the modules it contains.

For **GV Node Manager** to discover the cards housed in a GV Node frame, you must configure a Communicator service for the frame (see Communicators, on page 220). Each frame typically includes at least the following modules:

- the frame controller, which is represented by *two* control panels in iControl: *Frame Controller,* and *Frame Reference;*
- the *IFM-2T* internal fabric module;
- and a number of Densité cards (e.g., XIO-4901, KMX-4911).

The GV Node Manager control panel lists every Densité card in the GV Node frame's slots, and their rear panel model (if present). For a compatible card, you can select signal-type options, and select which inputs and outputs are enabled, *between the card and the Internal Fabric Module,* to match the card's actual physical configuration.

For example, the XIO-4901 3G/HD/SD SDI input/output card supports audio embedding/de-embedding, as a software option (MDX). If this option has been activated, then GV Node Manager allows you to enable or disable audio embedding/de-embedding on a card's SDI inputs and outputs. If your system is monitoring MADI signals (supported at the card's inputs/outputs 8 and 9), then disabling the MDX option lets you select MADI at the inputs and outputs matching your physical configuration. The total numbers of enabled inputs (to the Fabric module), and output (from the Fabric module) are indicated at the bottom of the control panel. These totals exclude MADI inputs and outputs.



See also

For more information, see Working with GV Node on page 247, and Opening GV Node Manager on page 716.

GeckoFlex Manager

GeckoFlex Manager, like **Densité Manager**, is a service that allows you to manage multiple GeckoFlex frames (using GeckoFlex Communicators).

For **GeckoFlex Manager** to discover cards and begin controlling services, you need to specify the IP addresses of the GeckoFlex frames that it will manage. Each frame may contain up to 10 devices. If you do not add any addresses, or if you add an incorrect address, the GeckoFlex Manager will not discover any frames.

See also

For more information, see Working with GeckoFlex Communicators on page 237.

Densité Upgrade Manager

Densité Upgrade Manager is an iControl utility allowing you to manage the firmware and software versions of individual cards without having to put entire Densité frames into operational *Standby* mode. Application Servers can hold several versions of Densité card firmware and software in memory and **Densité Upgrade Manager** allows you to effectively toggle among these versions. From time to time, new versions become available, and **Densité Upgrade Manager** allows you to upload these files to the Application Server.

IMPORTANT: System behavior

The **Densité Upgrade Manager** included with any version of iControl (starting with version 5.00), supports all Densité card types, ***including*** those that do not yet exist.

For example, if a brand new Densité card, *ABC-1234*, is installed in a Densité frame visible to a version of iControl that is, at the time, three years-old (but still version 5.00 or greater), the *ABC-1234* card would be visible within **Densité Upgrade Manager**.

Firmware and software is bundled into single upgrade packages. That is, a package contains one version of firmware for a given Densité card and one version of software. By upgrading a card with a given package, you are changing both the installed firmware and software to those versions of each within the upgrade package.

IMPORTANT: The version numbering of packages represents a system of incrementation belonging **ONLY** to the package and not to the respective version numbering of firmware and software.

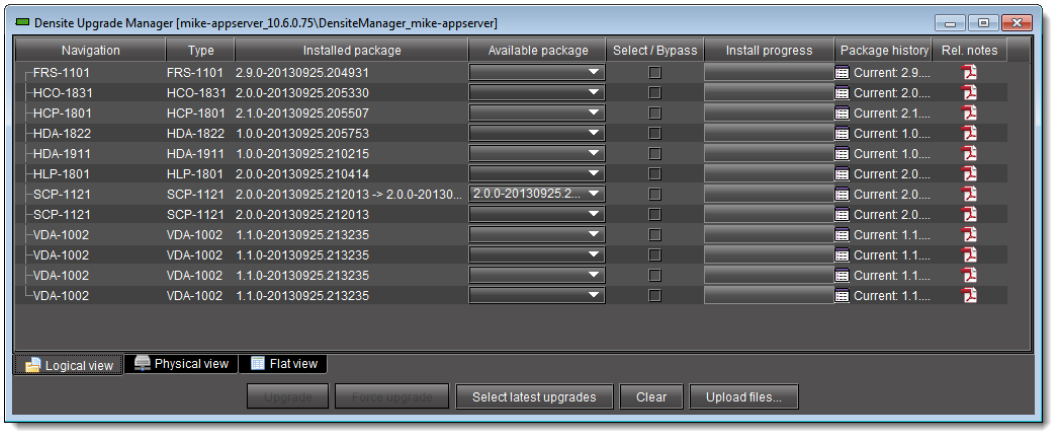
Note: **Densité Upgrade Manager** does not allow you to upgrade, downgrade, or roll back firmware separately from software. Changing an installed package necessarily implies changing the component firmware **AND** software to those versions of each embedded within the introduced package.

See also

For more information about:

- Upgrading, downgrading, and rolling back firmware and software of Densité cards, see Working with Densité Upgrade Manager, on page 288.
- The **Densité Upgrade Manager** user interface including icon colors and their meanings, see User Interface of Densité Upgrade Manager, on page 223.

User Interface of Densité Upgrade Manager



Densité Upgrade Manager

Densité Upgrade Manager UI descriptions

Item	Description
--- ***Columns*** ---	
Navigation	The tree structure in this column graphically situates Densité cards, and their modules if applicable, in the context of several different navigation method, as follows: • ***Logical view***: a logical arrangement (sorted by type) • ***Physical view***: a hierarchy representing the nested physical componentry (e.g., appserver > Densité frame > slot > card) • ***Flat view***: a flat listing of the Densité cards in alphabetical order.
Type	Type of Densité card

Densité Upgrade Manager UI descriptions (*Continued*)

Item	Description
Installed firmware	Installed firmware version and firmware upgrade path. If no package is selected under **Available package**, only the installed firmware version appears in this column. If a package is selected, the upgrade (or downgrade) path appears. If you would like to determine if firmware will be installed in the installation of the selected package, an upgrade path showing **X —> X** in this column indicates there will be no new installation of firmware. By contrast, an upgrade path showing **X —> Y** indicates firmware will be installed.
Installed software	Installed software version and software upgrade path.
Installed package	Installed package version and package upgrade path.
Available package	Selectable list of packages (relevant to a given Densité card) on the Application Server, available to be installed. The version numbers listed are package numbers and not firmware numbers.
Select / Bypass	Selection tool indicating which cards will have their respectively selected available packages installed once the **Upgrade** or **Force upgrade** button is pressed. Additionally, if a package is selected for a card and you would like for it to remain selected but not installed in the next upgrade, you may clear the **Select / Bypass** check box to make this happen.
Install progress	The progress bar measuring the current installation of a package. After an installation, this field displays a status message of the last installation attempt.
Package history	Logs of all package installations for each Densité card.
Rel. notes	Link to the release notes for the version of firmware embedded within the installed package.
--- ***Buttons*** ---	
Upgrade	Click to begin installing the selected packages (whether upgrade, downgrade, or rollback) to their respective cards.
Force upgrade	Click to begin installing the selected packages to their respective cards (same behavior as the **Upgrade** button). However, in all cases where the firmware embedded within selected packages have the same version numbers as the installed firmware, no firmware will be installed from the selected package (in theory because it is the same version). In order to override the **Upgrade** button's behavior of **NOT** installing a save-version firmware from a selected package, you must click **Force upgrade**.
Select latest upgrades	Click to select (for each listed Densité card) the latest[1] package available on the Application Server
Clear	Click to clear all selections from the **Available package** column and all messages from the **Select / Bypass** column.
Upload files	Click to upload an upgrade package file to the Application Server.

1. the package whose version number indicates it is the most recent

Lookup Services

A *lookup service* enables other services and devices to find each other over a network. An iControl client program (e.g., iC Navigator) can use a lookup service to get information on remote services or devices, and use that information to establish communications. By default, there is a lookup service running on each iControl Application Server. When an iControl

service or device is started, it will register with the first lookup service that it finds on the same subnet.

See also

For more information, see Lookup Services on page 27.

Control Panels and Device Parameters

Most Grass Valley devices can be controlled from an iControl workstation using *control panels*. A control panel is a software interface that lets you monitor and control various device parameters.

Note: Grass Valley cards are shipped with *Installation & Operation Guides* that provide detailed descriptions of their respective control panels, along with instructions on their use.

The control panel for a device is accessed from the iC Navigator window, either by double-clicking on the device name, or by right-clicking and choosing **Show Control Panel** from the drop-down menu.

The device name is displayed along the top of its control panel, along with a dashboard containing one or more icons representing the status of key device parameters. Error conditions are indicated by color and by a text message appearing below the icons. Hold the cursor over an icon to continuously display its associated error message; otherwise the display cycles through all reported errors.

Note: If the Control icon in the dashboard is yellow, this indicates that local card control is active—the card is being temporarily controlled using a local hardware control panel. In such a case, any changes made using the iControl interface will have no effect on the card.

To access the control window for a device, double-click the device in the iC Navigator display, or right click, and then click **Show Control**.

Example of an Allegro control panel

Example of a control panel for a DEC-1002 Analog Video to SDI Encoder

Some control panels have tabs that correspond to different groups of parameters. Open control panels are listed under the **View** menu. Select any panel from the menu to bring it to the front.

> **Note:** If you encounter the message `Control Panel Not Available`, it means that your selection has not been implemented as a controllable device in iControl. You can view the status of such a device, but you cannot modify any of its parameters.

Control Panel Tabs

The table below lists examples of typical control panel tabs and their associated parameters:

Tab	Sample Parameters
Config	Audio Destination, Audio Source, Audio Delay, No Signal Delay, Signal Standards Detection, No Signal Delay, Scan, VBI, Video
Info	Comments, Device Type, Label, Long ID, Manufacturer, Remote System Administration, Service Version, Short Label, Source ID, Vendor
Video	Player, Thumbnail Streaming, Streaming Priority Control, Waveform Monitor and Vector Scope.
Timing	Horizontal Fine, Horizontal Position, Horizontal Timing, Vertical Timing, Fine Timing Adjustments
Meta	Aspect Ratio, Copy Control Information, Source

The control panel for some devices contains a **Load Factory** button. Click this button to reset the device parameters in the active tab to their original factory values.

Device Info

The **Info** tab of a control panel displays general information related to a device, and is available for all device types. The **Info** tab includes identification information such as a device's label, short label, type, comments, source ID, configuration status, frame number, and slot number.

TIP: *To quickly display the Info tab for a device, right-click the device in iC Navigator, and then click* **Show info control panel**.

Under the **Info** tab, you can change the name of the selected device, as well as enter comments. By default, the device name is its type identification. However, you may find it helpful to give devices more meaningful names. Once you change the device name in the control panel, the name of the item is also changed in the iC Navigator display, making it easier to locate.

You can also register a device with the lookup service on a remote Application Server using **Remote system administration**.

Device Groups

iC Navigator allows you to organize devices into logical groups, making them easier to locate and to manage. A device group is a folder in iC Navigator into which you drag and drop selected devices. You can create as many device groups and subgroups as you want.

> **Note:** Logical grouping information is stored on the Application Server. Any changes to the device groups will be visible to all users.

Creating a device group automatically creates a virtual alarm that displays the overall status of its member devices. The color of the device group's folder icon changes when the status of one or more of its members changes. For example, if one member device changes status as a

result of a critical error, then the group's folder icon turns red. If no devices are assigned to a group, its folder icon will be gray.

Device groups can only be created in (and are only visible in) iC Navigator's **Logical view** mode (see Working with Device Groups on page 250).

Reference Configuration

A *reference configuration* is a feature of iC Navigator that allows you to keep track of important cards, or groups of cards. If a card is removed from a slot, the default behavior in iC Navigator is for the card to disappear from the list in **Logical view** and **Flat view**. In **Physical view**, the device name is replaced by `Empty Slot`.

iC Navigator allows you to designate a card as part of a *reference configuration,* so that the name of the card and the slot number it occupies are retained. If the card is removed, it will be visible as before, but with the description `Missing from slot` beside its name.

See also

For more information about:

- iC Navigator views, see page 228.
- Adding a card to the reference configuration, see page 262.
- Removing a card from the reference configuration, see page 263.

Devices and Services Views in iC Navigator

When they first start up, devices and services announce themselves to a lookup service (running on an Application Server on the local subnet), which then makes them available to iC Navigator. iC Navigator shows ALL services (GSM, Densité Manager, GeckoFlex Manager, Router Manager, composite panels, third party device drivers, etc.) and devices (Densité/Imaging/GeckoFlex frames and their cards, third party devices, etc.) detected by the lookup process.

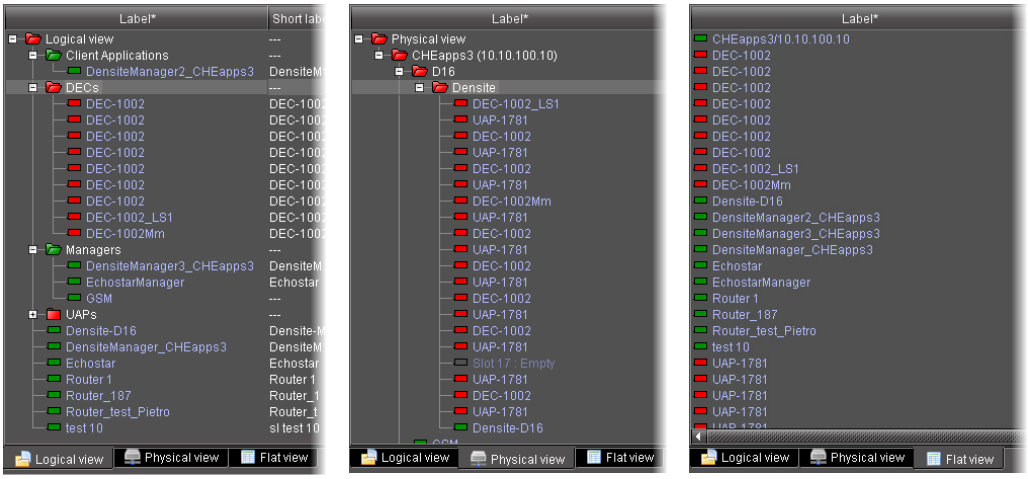
A service can be running, and appear in iC Navigator, even if there are no physical devices associated with it. For example, the Densité Manager can be running, but until you configure it with the addresses of the Densité frames, only the service will appear in iC Navigator. If a service is not running, it will not appear in iC Navigator.

Note: It is possible for a service to appear active (green) on the *Services management* page, yet still not appear in iC Navigator. This can happen if the service stopped after the *Services management* page was displayed. Try restarting the service (see Stopping, Starting, or Restarting a Service, on page 680), and then check iC Navigator again.

There are three icons at the bottom of the iC Navigator window that allow you to change the way devices are sorted in iC Navigator.

- **Logical view** displays all devices registered on the lookup server, as well as active services. The devices and services may be organized into groups, which can be created by any user (see Device Groups, on page 227). Groups and their contents are arranged in alphabetical order. Ungrouped elements are displayed at the end of the list. Empty slots are not shown, unless they are in the Reference Configuration (see Reference Configuration on page 228).
- **Physical view** arranges devices relative to their physical connections and network location. It shows the iControl Application Server itself, and the frames, cards and other devices connected to it via Ethernet or serial ports. Empty slots show up as `empty`, unless the card is designated as `In Ref Config`, in which case it will show up as before, but with the description `missing from slot`.

  Devices are sorted by:
  - the IP address of the iControl Application Server with which they are associated,
  - then, for Grass Valley Imaging frames, by the serial communication port of the Application Server to which the frame is connected, or, for Grass Valley GV Node, Densité or GeckoFlex frames, by the frame's IP address
  - then, within a frame, by slot number.
- **Flat view** shows all devices in alphabetical order without any grouping.



Notes

- In **Logical view** and **Physical view**, you can open and close folders in the list by clicking the [+] and [–] boxes beside the folders.

Notes (*Continued*)

- Activated serial ports (see Configuring Serial Ports for a Specific Application Server, on page 64), are visible in **Logical view**, but only serial ports that are physically connected to a device appear in **Physical view**.
- If an RS-422 serial port is configured to 'None', it does not appear in iC Navigator. iControl treats such a port as a standard RS-422 port, to which a third-party device (e.g., a router) can be connected.

Virtual Service Manager

The iControl Virtual Service Manager (VSM) is used to create *virtual devices*, of which there are two types:

- proc amps
- composite panels

Proc amps (processing amplifiers) are virtual devices that control Grass Valley Imaging-series processing interface cards, such as the ASD-231i, the DVP-101i, and the DAP-712i. Proc amps allow you to monitor and control up to three cards (one video, one audio, and one audio delay card) from a single panel. Unlike composite panels (see below), proc amps cannot be customized—the gains (controls) that appear in a proc amp panel are determined by the type of card selected when the proc amp was created.

Note: Densité-series devices do not support proc amps.

Composite panels, like proc amps, are virtual devices. They are used to control Grass Valley Densité-series and some Imaging-series processing interface cards, such as the DEC-1002, the XVP-811i, and the UAP-1781. Composite panels allow you to monitor and control multiple cards from a single panel. Unlike proc amps, composite panels can be customized—each card has a list of available gains (controls) from which you can choose, in any combination, when you create a composite panel.

Note: A single Application Server can support up to 50 composite panels.

Device Profile Manager

Maintenance personnel and operators can perform quick and accurate, system-wide or focused, card and device configuration management by using **Device Profile Manager**.

Device Profile Manager allows you to:

- export profile data (configuration data about device groups) from one or several devices to a profile file
- import profile data from a profile file to one or several devices
- compare configured parameters, between two or more cards, of the same type and firmware version
- copy configuration data from:

- one card to one card
- one card to several cards
- several cards to several cards

- perform a system snapshot by exporting all card configuration data (for cards supporting profile export)
- load a user-specified preset to one or several cards as the current configuration
- save the current configuration of one or several cards to any available user preset

See also

For more information, see Working with Device Profile Manager on page 263.

Detailed Directions

Working with Imaging Communicators

Imaging Communicators (see Communicators, on page 220) allow you to control signal processing and distribution performance modules contained in Grass Valley Imaging-series (Symphonie and Quartet) frames.

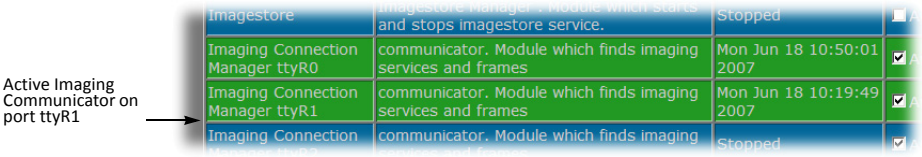
Imaging frames are connected to an Application Server using their respective RS-422 serial ports. A Communicator service, corresponding to a specific serial connection, must be configured and activated. If the service is not configured, you will not be able to control the devices even if they are connected. If the service is configured, but there is no frame connected, only the service will be displayed in the iC Navigator window.

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Services management* page (see page 678).

To configure an Imaging communicator

1. On the *Services management* page, verify that an Imaging Connection Manager has been configured for the port to which the Symphonie or Quartet is connected (see "Configuring the Application Server's Serial Ports" in the *iControl User's Guide* on the Documentation page of iControl), and that the service is active (green).

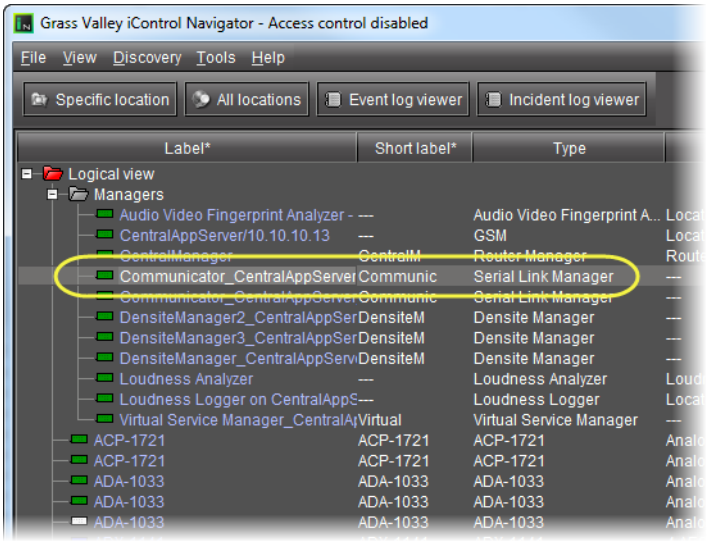


2. Open iC Navigator (see page 697).
3. Click the **Logical view** tab.

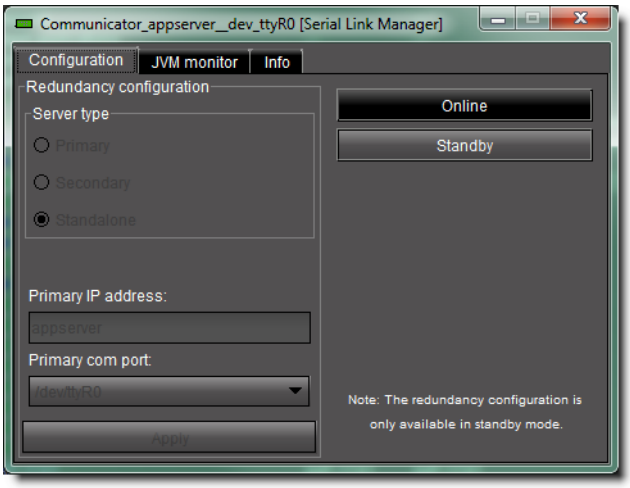
   The **Logical View** tab is displayed.

Note: Make sure that the Imaging Communicator service is visible, and that its status is green.

4. Double-click the **Communicator** row.



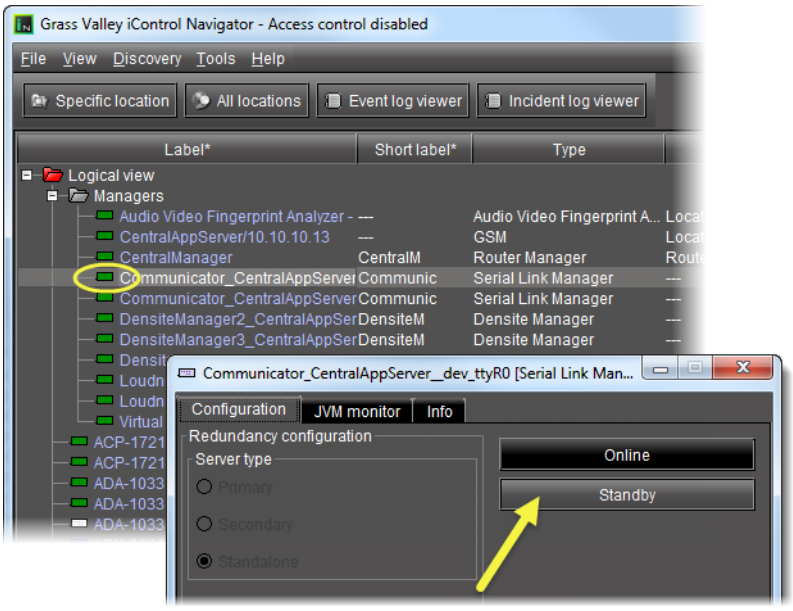
The **Communicator control panel** appears.



By default, the **Online** button is highlighted.

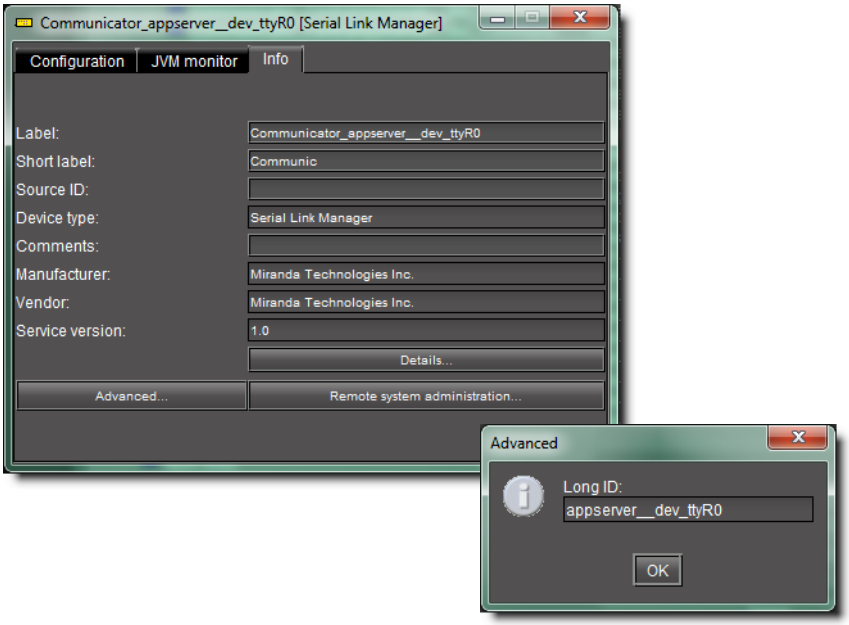
5. Click **Standby**.

   This interrupts the data flow to and from the Imaging Communicator over the serial port. The status of the Communicator changes to yellow in iC Navigator.



Under **Server Type**, the setting standalone should be selected. You can safely ignore all other settings in the **Configuration** tab—this functionality has been superseded by other iControl modules.

6. Click the **Info** tab.



Type (or modify) the values in the **Label**, **Short Label**, **Source ID** and **Comments** fields. These values are typically visible in the main iC Navigator window.

7. Click **Advanced** to view the Long ID.
8. Click **Details** to obtain manufacturing process and window version numbers.

9. Click the **Configuration** tab, and then click **Online** to reactivate the Imaging Communicator.

Working with Densité Communicators

Densité Communicators (see Communicators, on page 220) allow you to monitor and control cards housed in Grass Valley Densité frames.

Densité frames are connected to an Application Server over a standard Ethernet network. In order to establish communications between the Densité frame and the Application Server, a Communicator service must be configured and activated for each frame. If the service is not configured, you will not be able to monitor or control the Densité frame, even if it is connected.

> **Note:** Because of the one-to-one correspondence between Densité frames and Densité Communicators, the terms are used interchangeably.

The Densité Manager is an iControl service that allows you to manage multiple Densité Communicators. If there are Densité frames on your network, you will automatically see the Densité Manager service displayed in the iC Navigator window.

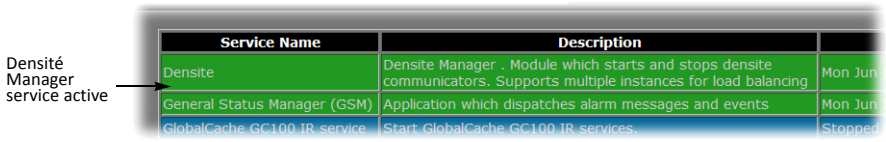
For the Densité Manager to be able to begin controlling services, you must specify the IP address(es) of the Densité frame(s) that it will manage. For each frame specified in this way, the Densité Manager opens a Densité Communicator.

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Services management* page (see page 678).

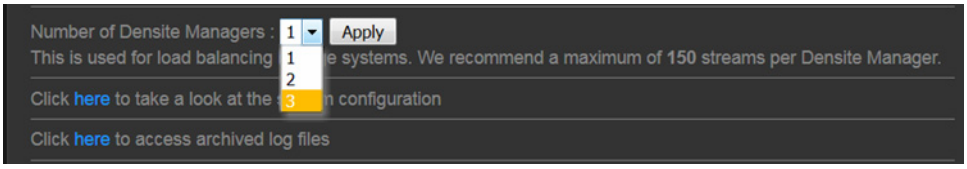
To configure a Densité Communicator

1. On the *Services management* page, verify that at least one Densité Manager is active (green).

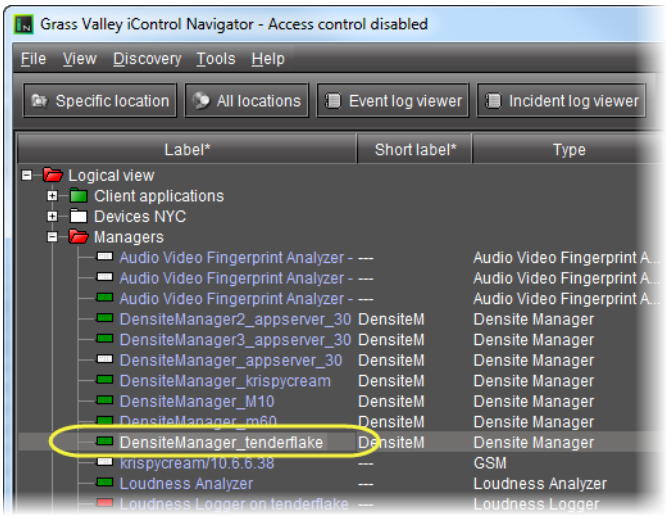


In a network with multiple Densité frames, it may be necessary to run more than one Densité Manager service, and to balance the load between them (Grass Valley recommends a maximum of 150 streams per Densité Manager).

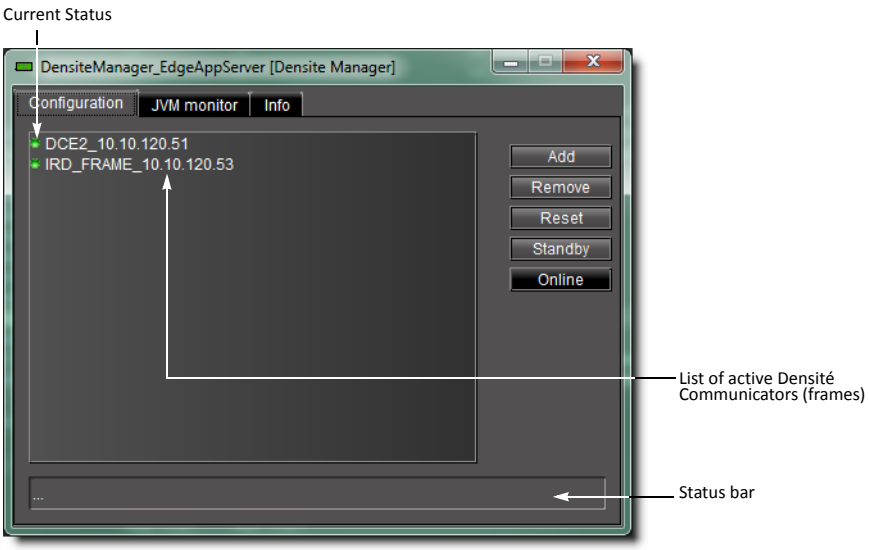
2. To add more Densité Managers, scroll to the bottom of the Services Management page, select the desired number from the list (1–3), and then click **Apply**.



3. Open iC Navigator (see page 697).
4. Click **Logical view**. Make sure that the Densité Manager service is visible, and that its status is green.
5. Double-click the Densité Manager row.



The **Densité Manager** control panel appears.



The **Configuration** tab contains a list of currently configured Densité Communicators. The first time that you access the Densité Manager, this list will be empty. You must manually add the IP address and name of each Densité frame that is to be controlled. The Status bar located at the bottom of the control panel displays Error, Warning and Information messages.

If you select a Densité Communicator (frame) from the list, you can take one of the following actions:

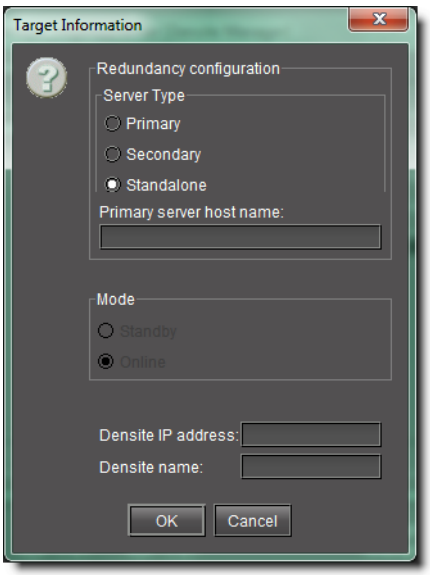
- Click **Remove** to delete the Communicator from the list. If the Communicator had been added to an **iC Web** page, the alarm for that element will turn red.
- Click **Reset** to stop and then restart the selected Communicator.

> **Note:** Use **Reset** when, for example, cards known to be in the frame do not appear in the iC Navigator window.

- Click **Standby** to interrupt the data flow to and from the Densité frame.
- Click **Online** to restore the data flow to and from the Densité frame.

6. Click **Add** to add a new Densité Communicator (frame) to the list.

   The **Target Information** window appears.

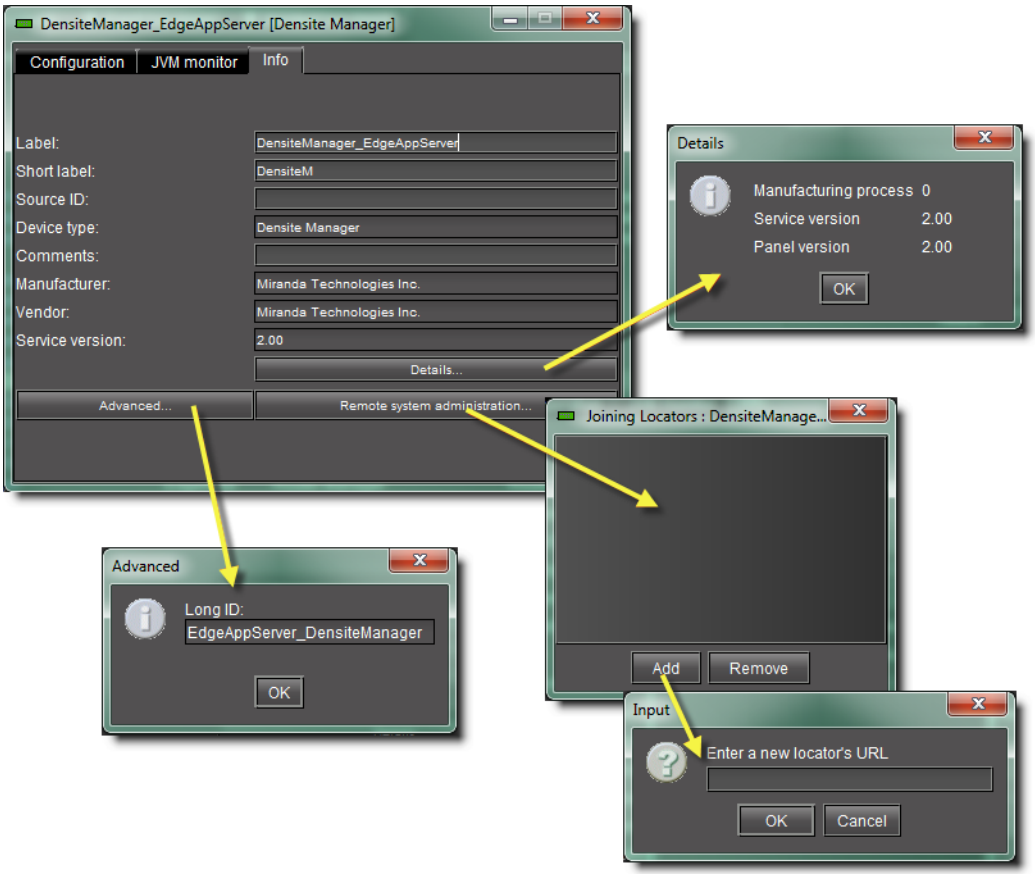


7. Under **Server Type**, select **standalone**.
8. Type the Densité frame's IP address and a descriptive name in the fields provided. These are used to define the alarm IDs in the GSM.

   > **Note:** If the name or IP address for an existing frame is modified at a later date, any **iC Web** pages referring to this frame may no longer work.

   You can safely ignore all other settings in the **Configuration** tab—this functionality has been superseded by other iControl modules.
9. Click **OK**.

   The new Densité Communicator will be started and added to the list. iC Navigator will query that Densité frame, and any devices (cards) it discovers will be displayed.
10. Click the **Info** tab.



11. Type (or modify) the values in the **Label**, **Short Label**, **Source ID** and **Comments** fields, as required.

> **Note:** These values are typically visible in the main iC Navigator window.

12. In addition, you can do the following:
    - Click **Advanced** to view the Long ID.
    - Click **Details** to obtain manufacturing process, service, and panel version numbers.
    - Click **Remote system administration** to view, add or remove the IP address of an Application Server running a lookup service on a remote subnet.

Working with GeckoFlex Communicators

GeckoFlex Communicators (see Communicators, on page 220), like Densité communicators, allow you to monitor and control cards housed in Grass Valley GeckoFlex frames.

GeckoFlex frames are connected to an Application Server over a standard Ethernet network. In order to establish communications between the GeckoFlex frame and the Application Server, a Communicator service must be configured and activated for each frame. If the service is not configured, you will not be able to monitor or control the GeckoFlex frame, even if it is connected.

Note: Because of the one-to-one correspondence between GeckoFlex frames and GeckoFlex Communicators, the terms are used interchangeably.

The GeckoFlex Manager is an iControl service that allows you to manage multiple GeckoFlex Communicators. If there are GeckoFlex frames on your network, you will automatically see the GeckoFlex Manager service displayed in the iC Navigator window.

For the GeckoFlex Manager to be able to control services, you must specify the IP address(es) of the GeckoFlex frame(s) that it will manage. For each frame specified in this way, the GeckoFlex Manager opens a GeckoFlex Communicator.

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Services management* page (see page 678).

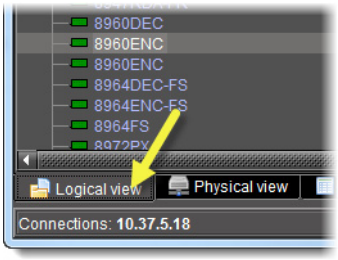
To configure a GeckoFlex Communicator

1. On the *Services management* page, verify that the GeckoFlex Manager is active (green).

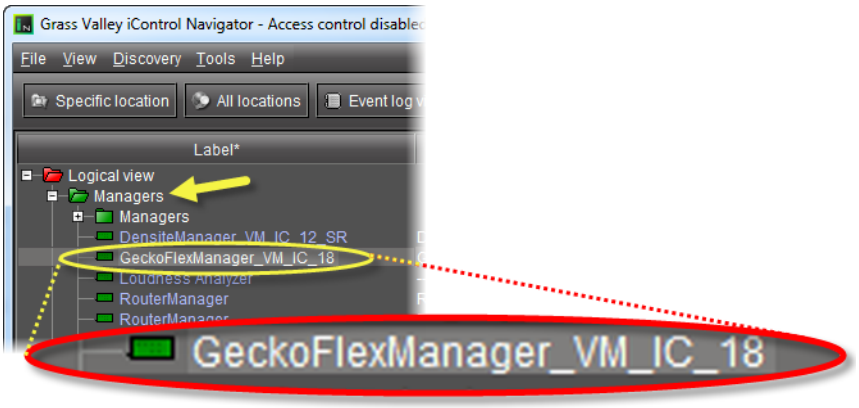
Service Name	Description	Start time	Auto Start	Start/Stop/Restart	Log
Audio/Video Fingerprint Analyzer	Provides support for distributed and multi-point content fingerprint analysis (e.g. lip-sync detection)	Stopped	Auto	/ /	show log
Bridgetech VBC service	Start Bridgetech VBC service.	Stopped	Auto	/ /	show log
CDMP	CDMP Service . Supports multiple instances for load balancing	Stopped	Auto	/ /	show log
Densite	Densite Manager . Module which starts and stops densite communicators. Supports multiple instances for load balancing	Thu Mar 26 09:57:34 2015	Auto	/ /	show log
ETL2745	ETL2745 Manager . Module which starts and stops ETL2745 service	Stopped	Auto	/ /	show log
GeckoFlex	GeckoFlex Manager. Module which starts and stops GeckoFlex Manager.	Mon Mar 30 10:09:58 2015	Auto	/ /	show log
General Status	Application which dispatches alarm messages and	Wed Mar 25	Auto	/ /	show

Services management page: GeckoFlex service showing as active

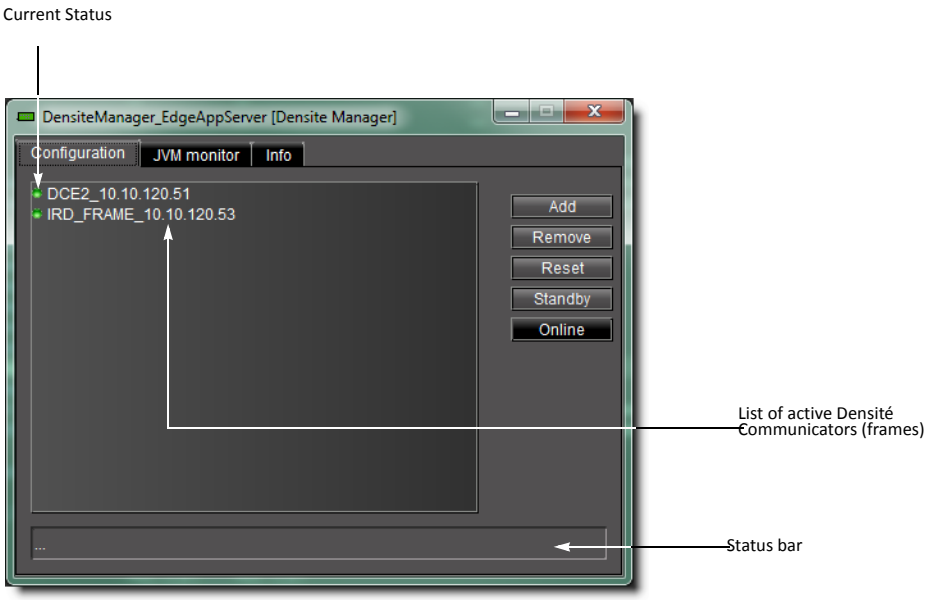
2. Open iC Navigator (see page 697).
3. Click **Logical view**.

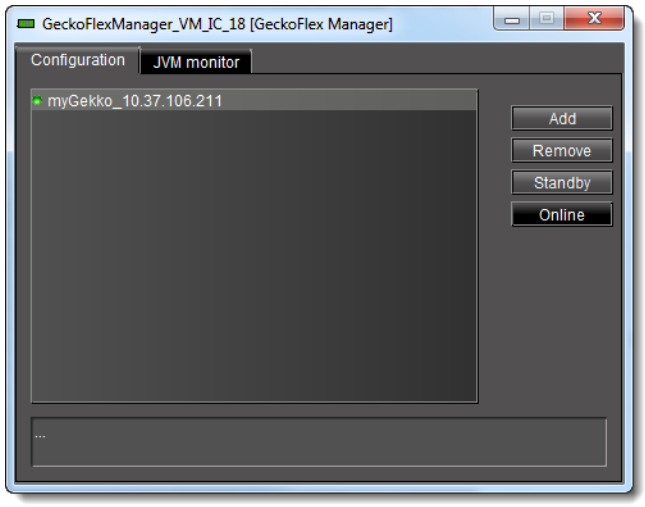


4. In the *Managers* folder, double-click the *GeckoFlex Manager* row.



The **GeckoFlex Manager** control panel appears.





The **Configuration** tab contains a list of currently configured GeckoFlex Communicators. The Status bar located at the bottom of the control panel displays Error, Warning and Information messages.

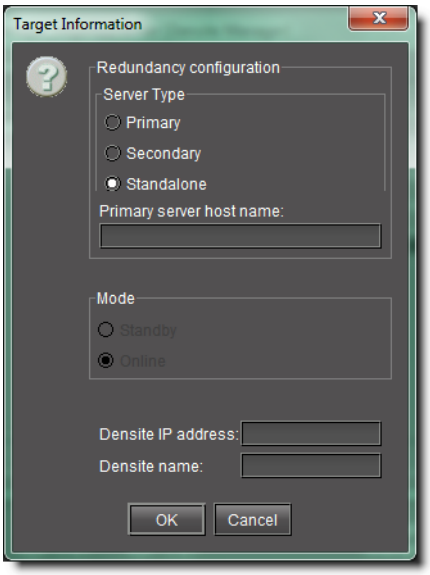
> **Note:** The first time you access the GeckoFlex Manager, this list will be empty. You must manually add the IP address and name of each GeckoFlex frame to be controlled.

If you select a GeckoFlex Communicator (frame) from the list, you can take one of the following actions:

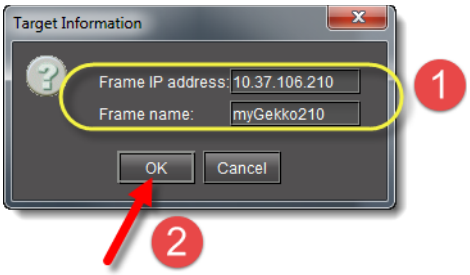
- Click **Remove** to delete the Communicator from the list. If the Communicator had been added to an **iC Web** page, the alarm for that element will turn red.
- Click **Standby** to interrupt the data flow to and from the GeckoFlex frame.
- Click **Online** to restore the data flow to and from the GeckoFlex frame.

5. Click **Add** to add a new GeckoFlex Communicator (frame) to the list.

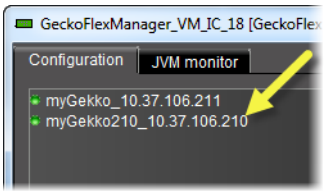
   The **Target Information** window appears.



6. Type the GeckoFlex frame's IP address and name, and then click **OK**.

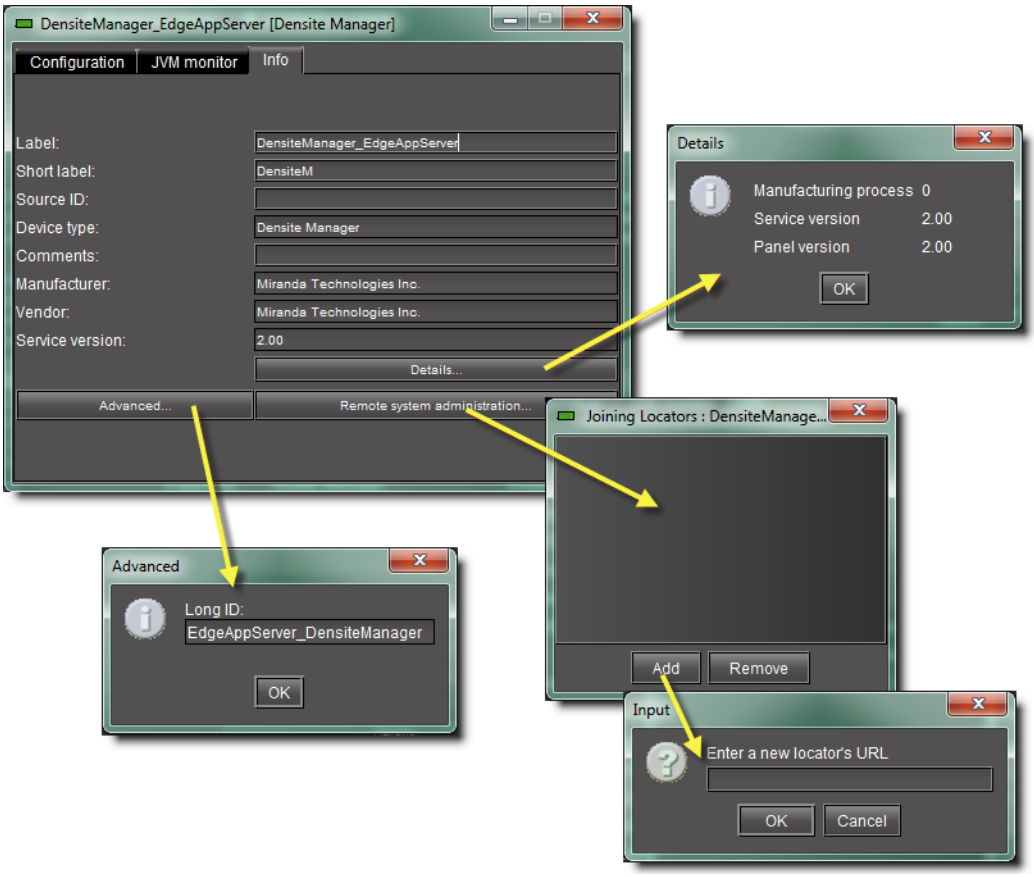


The GeckoFlex Manager displays the newly added GeckoFlex frame in the list. The frame name and IP address are used to define alarm IDs in the GSM.

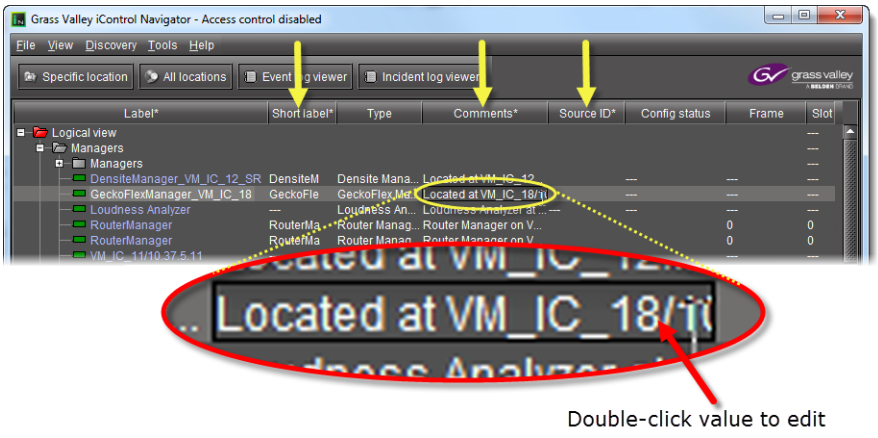


IMPORTANT: If the name or IP address for an existing frame is modified at a later date, any **iC Web** pages referring to this frame may no longer work.

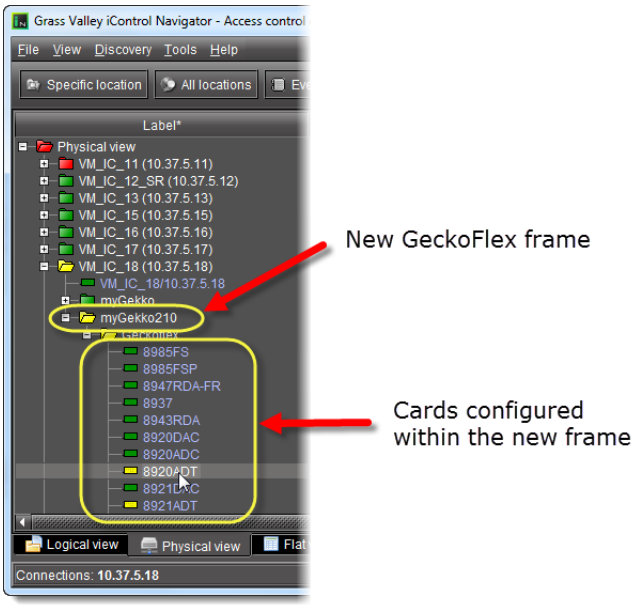
7. Click the **Info** tab.



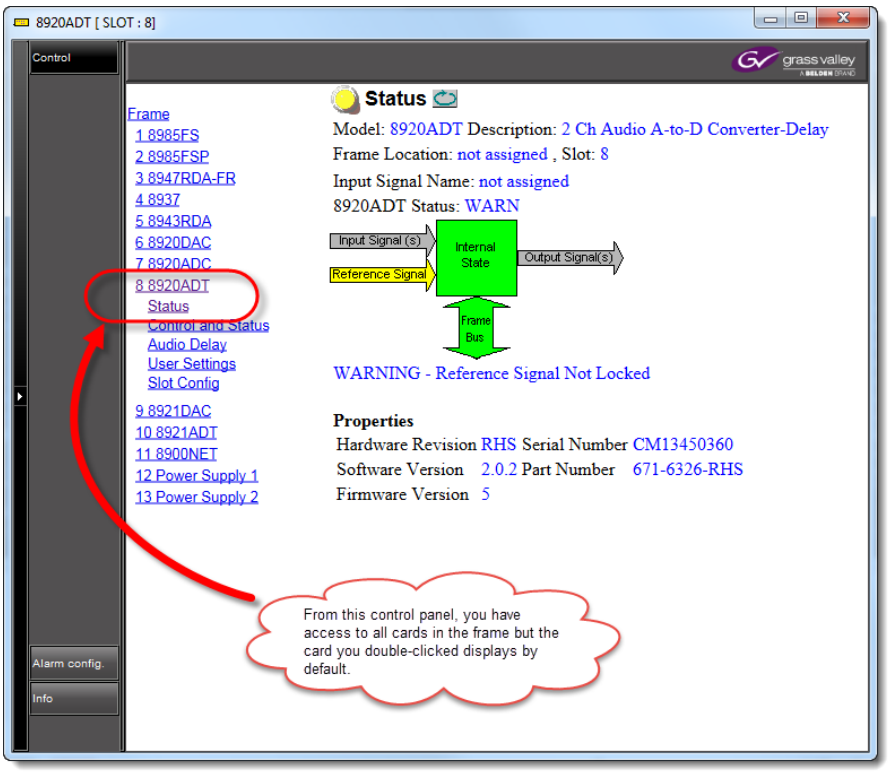
8. In iC Navigator, in the *GeckoFlex Manager* row of the **Logical view** tab, double-click the values in the **Short Label**, **Comments**, and **Source ID**, and type new values as required.



9. To see the GeckoFlex cards in your newly configured frame, click the **Physical view** tab, navigate to the desired GeckoFlex frame, and then double-click any of the cards to launch a card's control panel.



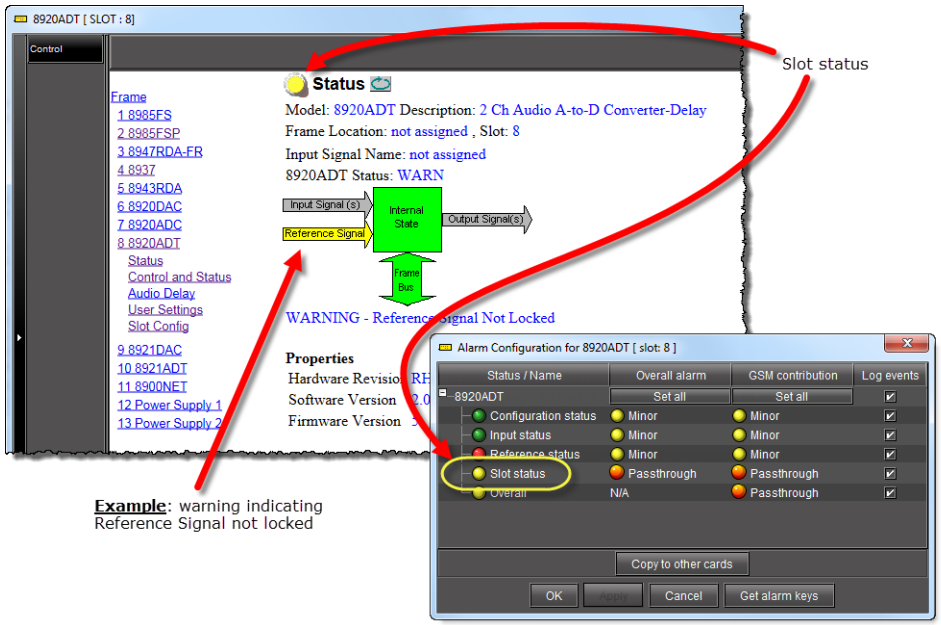
GeckoFlex frame and cards in iC Navigator



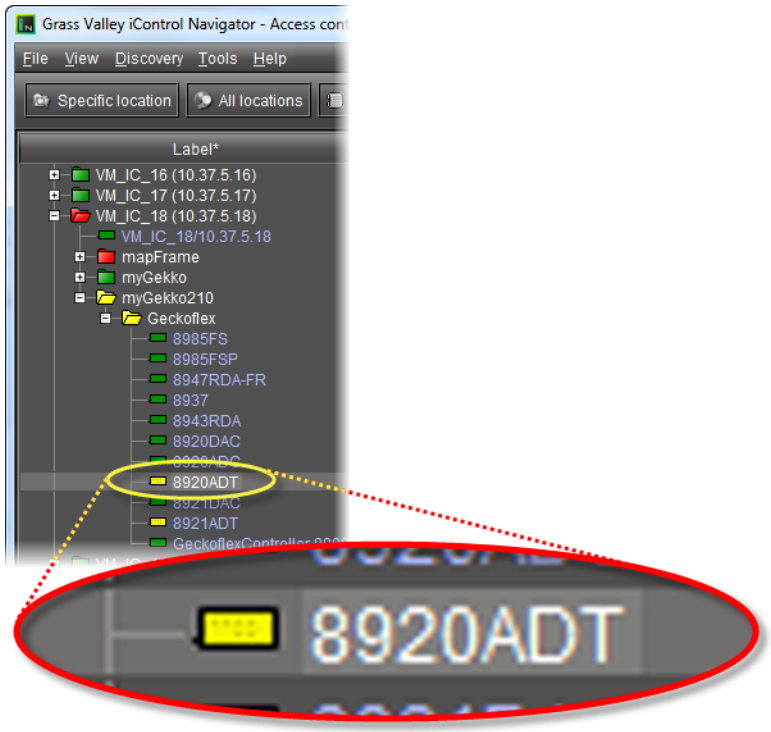
Control panel of a GeckoFlex card

Perform any required card configuration through each card's respective control panels.

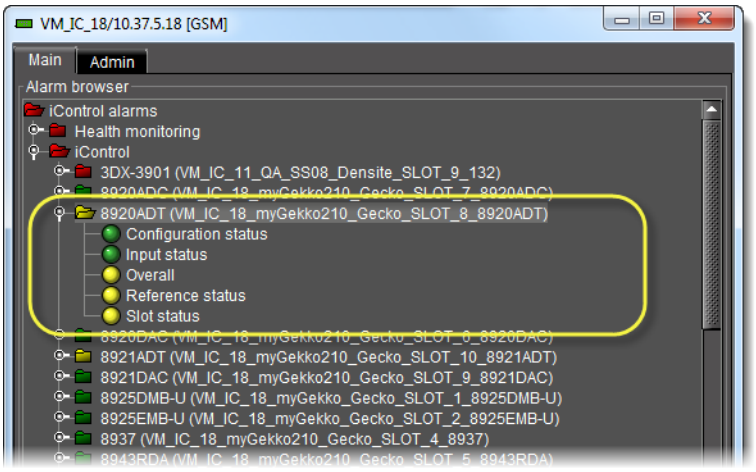
Alarm status can be seen in iC Navigator, the GSM Alarm Browser, and the iControl GeckoFlex card control panel interface.



GeckoFlex card's control panel and alarm configuration window



Card as seen from iC Navigator, showing overall alarm status



Overall and specific alarms' statuses for a GeckoFlex card as seen from the GSM Alarm Browser

See also

For more information about configuring GeckoFlex card parameters, see the documentation native to each card.

Working with Kaleido-Solo

For iControl to monitor and control a Kaleido-Solo device, the Kaleido-Solo must first be added to the list of communicators in the Densité Manager.

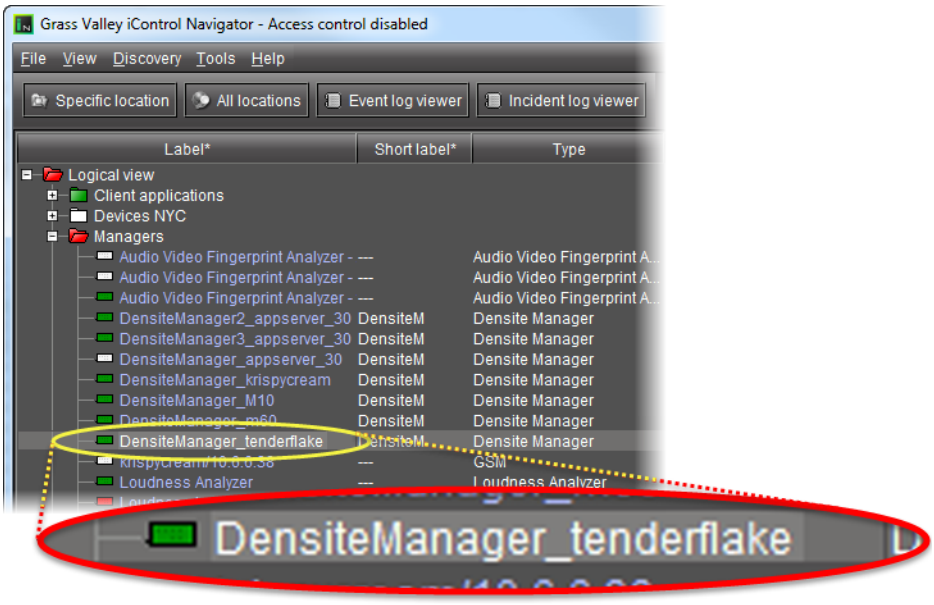
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

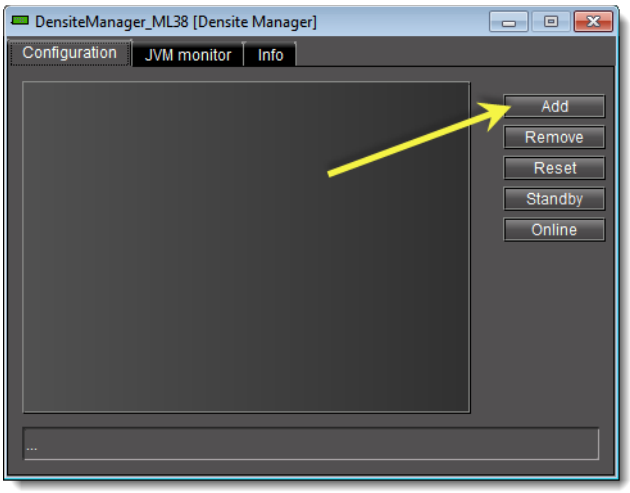
- You know the IP address of the Kaleido-Solo device.
- You have opened iC Navigator (see page 697).
- You have started the *Densité Manager* service in iControl (see Stopping, Starting, or Restarting a Service, on page 680).

To add a Kaleido-Solo service

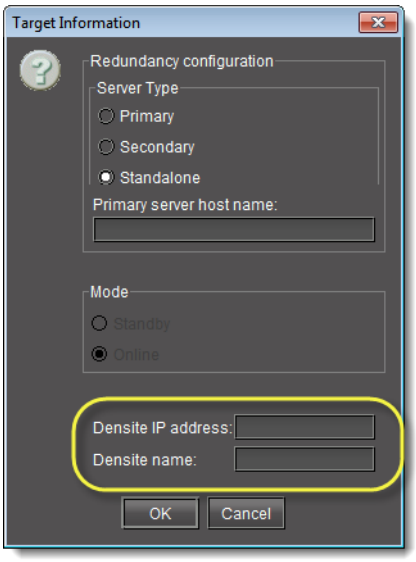
1. In iC Navigator, double-click **DensiteManager** in the logical view.



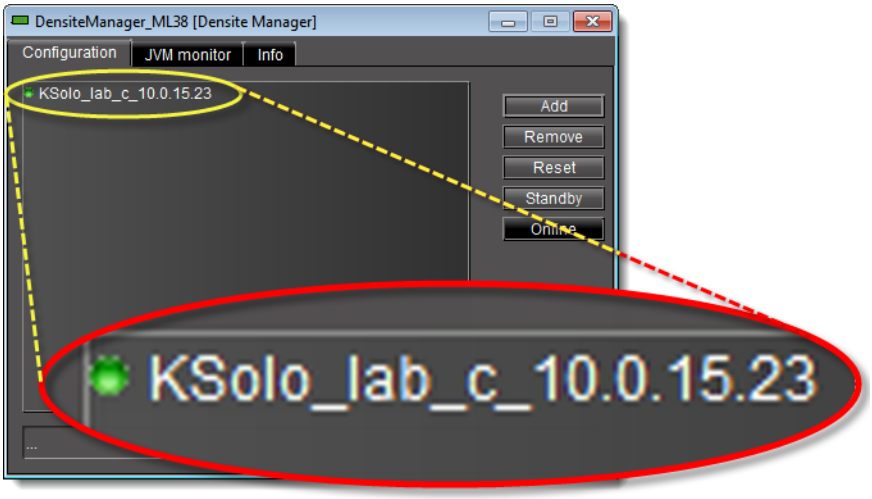
2. In **DensiteManager**, click **Add**.



3. In the **Target Information** window, type the Kaleido-Solo's IP address and a descriptive name for the new service, and then click **OK**.



The new Kaleido-Solo will be started and added to the list.



Working with GV Node

For iControl to monitor and control a GV Node frame, the GV Node must first be added to the list of communicators in a Densité Manager.

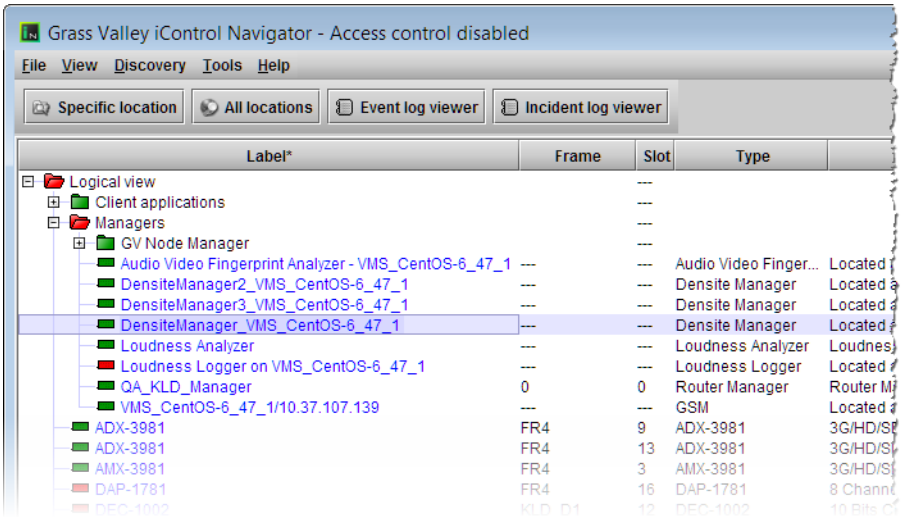
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

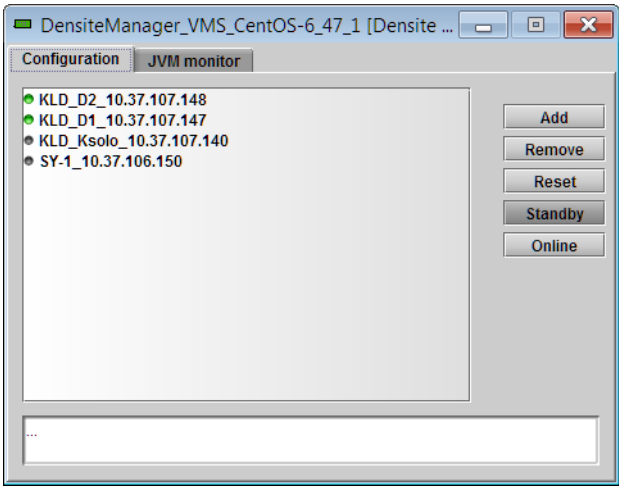
- You know the IP address of the GV Node frame.
- You have opened iC Navigator (see page 697).
- You have started the appropriate *Densité Manager* service in iControl (see Stopping, Starting, or Restarting a Service, on page 680).

To add a GV Node frame

1. In iC Navigator's *Logical view,* expand the *Managers* folder, and then double-click the appropriate Densité Manager element.

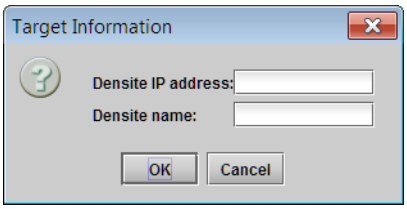


The Densité Manager control panel opens.

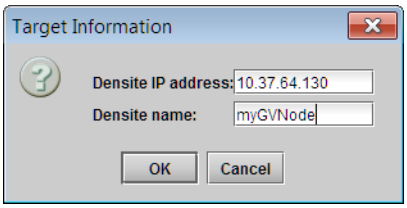


2. In the Densité Manager control panel, click **Add**.

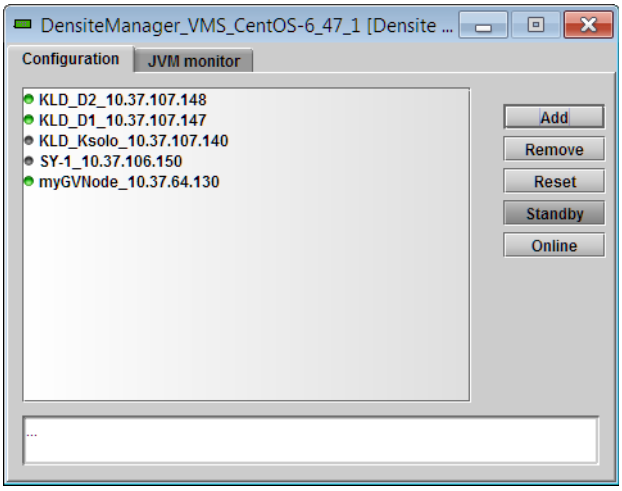
   The **Target Information** window opens.



3. In **Target Information**, type the GV Node frame's IP address, and a name to identify the new service associated with this particular frame.



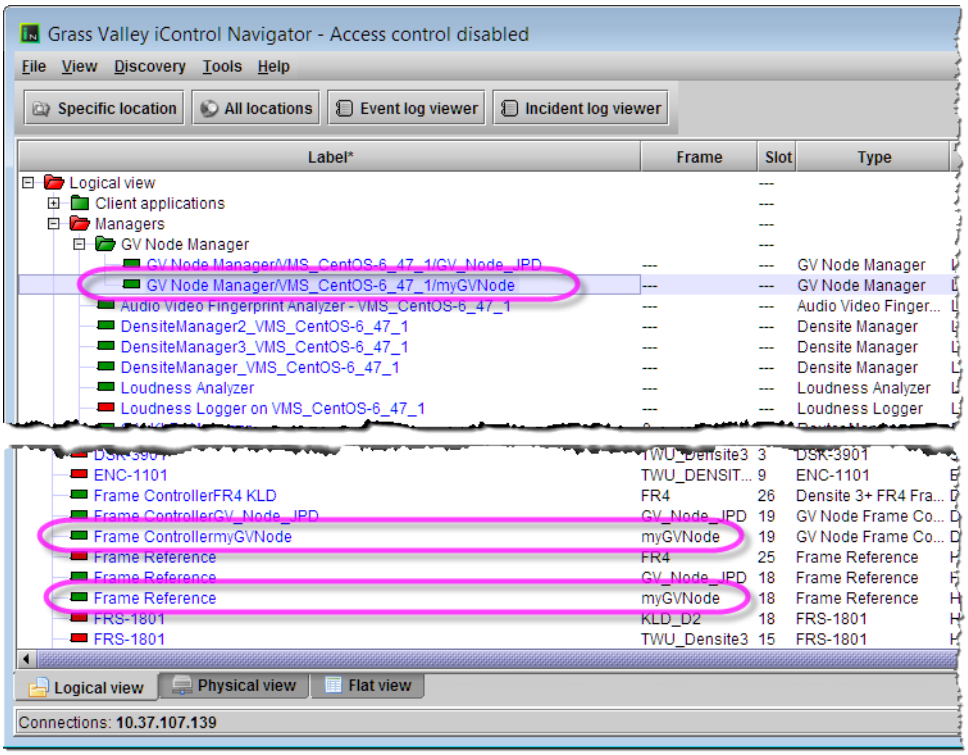
4. Click **OK**. The new GV Node service starts and is added to the list of Densité communicators in the selected Densité Manager control panel.



> **Note:** For more information about the Densité Manager control panel, see Working with Densité Communicators, on page 234.

5. Close the Densité Manager window.

   The *GV Node Manager* control panel, and control panels for all modules housed in your GV Node frame are now available in iC Navigator.



Logical view (partial) showing GV Node Manager, Frame Controller, and Frame Reference (other modules, e.g., IFM-2T, XIO-4901, KMX-4911 are not shown).

Working with Device Groups

iC Navigator allows you to organize devices into groups (see Device Groups, on page 227). In a large configuration, this can help reduce visual clutter, and make it easier to quickly access specific devices. Groups are only visible in iC Navigator's **Logical view**.

A device can only be a member of one group at a time. iControl creates certain groups by default, but you can move devices from these groups into your own custom groups, either by drag-and-drop, or by using cut and paste.

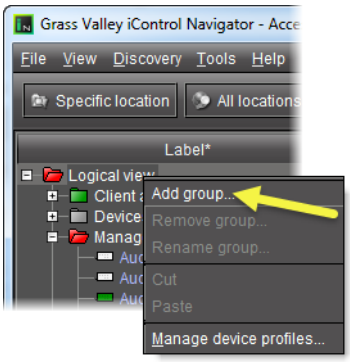
Creating a Device Group

REQUIREMENT

Before beginning this procedure, make sure you open iC Navigator (see page 697).

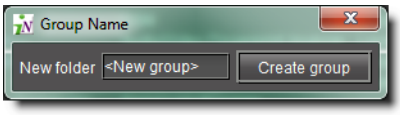
To create a group

1. In iC Navigator, right-click the folder into which you would like to place the new group (e.g., on the top level folder named *Logical*), and then click **Add Group**.

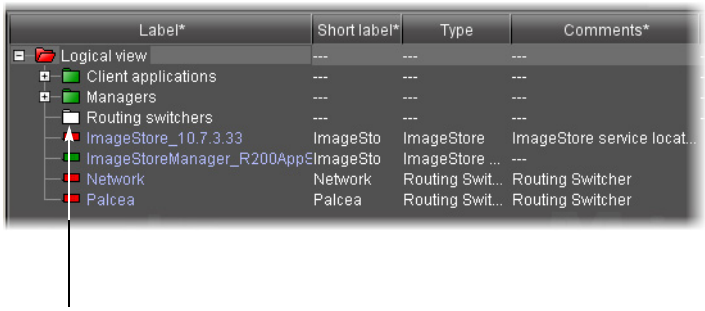


Note: Groups are only visible in **Logical view**.

The **Group Name** window appears.



2. Type a name for the group (e.g., `Routing switchers`), and then click **Create Group**.
   The group appears as a new folder in the chosen location.



Note: The newly created group folder is white because its status is not yet defined.

3. Select devices one at a time and drag them to the newly created group folder. Alternatively, you can perform the following steps:
   a) Select multiple devices.
   b) Right-click one of the selected devices, and then click **Cut**.
   c) Right-click the group folder, and then click **Paste**.
      The group folder takes on the overall status of its contents.

Moving a Device Group

REQUIREMENT

Before beginning this procedure, make sure you open iC Navigator (see page 697).

To cut and paste a group

1. In iC Navigator, right-click the group you wish to move, and then click **Cut**.
2. Right-click the new location (folder or sub-folder) for the group, and then click **Paste**.

   The group appears as a new folder in the chosen location.

Renaming a Device Group

REQUIREMENT

Before beginning this procedure, make sure you open iC Navigator (see page 697).

To rename a group

1. Select the group (folder) you wish to rename.
2. Right-click the group folder, and then click **Rename Group**.

   The **Folder Name** window appears.
3. Type a new name for the group, and then click **Rename Group**.

   The new group name appears for the chosen folder.

Removing a Device Group

REQUIREMENT

Before beginning this procedure, make sure you open iC Navigator (see page 697).

To remove a group

1. Open the group folder you wish to remove.
2. Move (i.e., drag and drop, or cut and paste) all devices out of the group folder to a new location.

   Only empty groups can be removed.
3. Right-click the group folder, and then click **Remove Group**.

   The selected group no longer appears in the iC Navigator window.

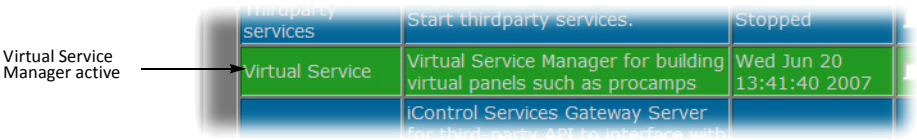
Creating a Proc Amp Device

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Services management* page (see page 678).

To create a proc amp device

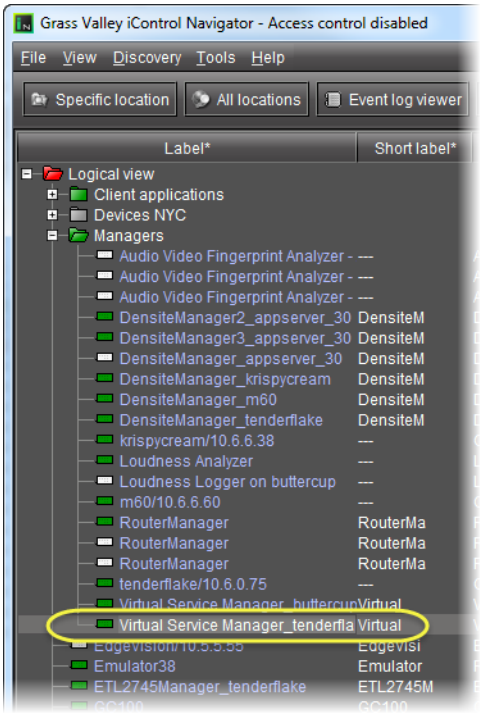
1. On the *Services management* page, verify that the **Virtual Service Manager** is active (green).



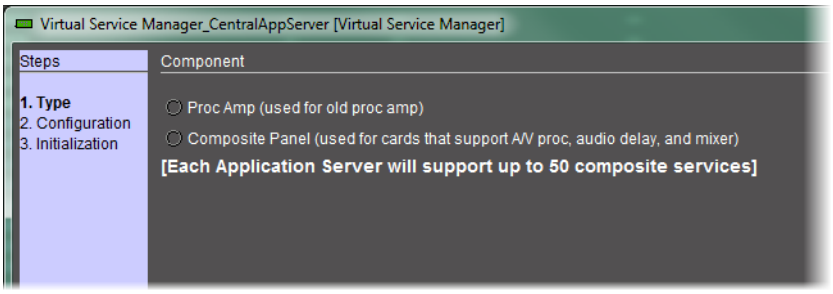
2. Open iC Navigator (see page 697).
3. Click the **Logical view** tab.

> **Note:** Make sure that the **Virtual Service Manager** is visible.

4. Double-click the Virtual Service Manager row.

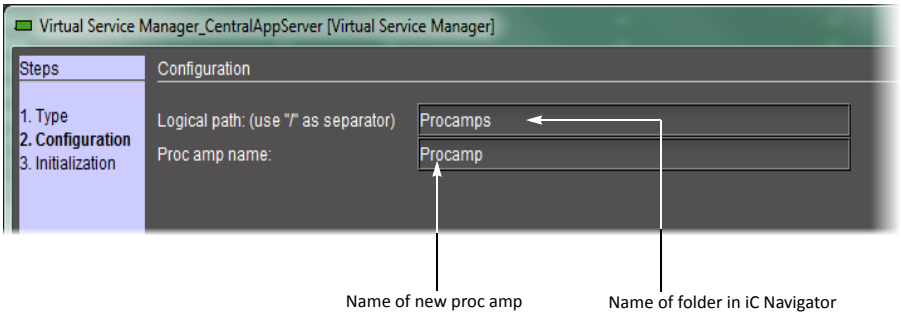


The **Virtual Service Manager** control panel appears, with the first of three pages (**Type**) displayed.



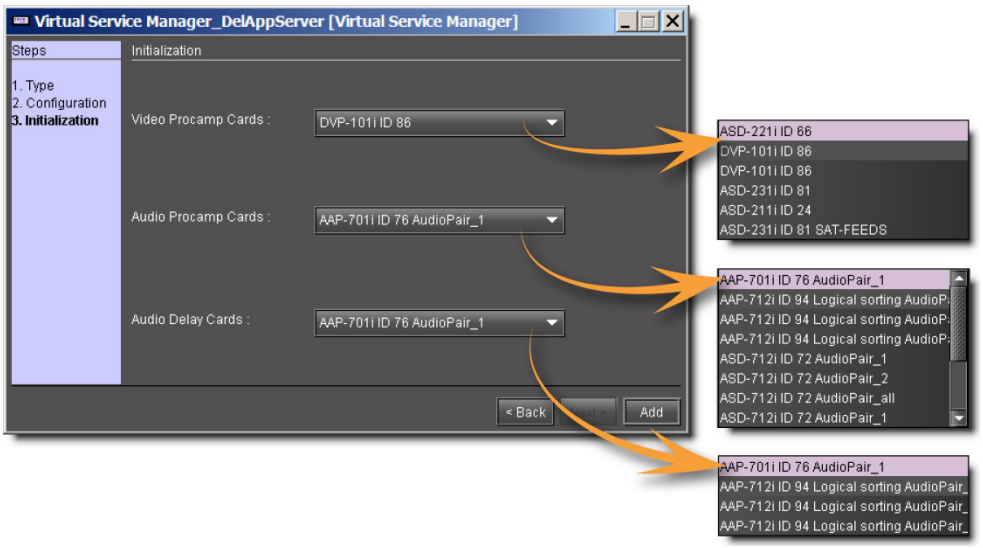
5. Select **Proc amp**, and then click **Next**.

   The Configuration page appears.



6. Type a logical path — this corresponds to the iC Navigator folder in which the new proc amp will appear. If the folder does not exist, a new one will be created automatically.
7. In the **Proc amp name** field, type a name for the proc amp.
8. Click **Next**.

   The Initialization page appears.



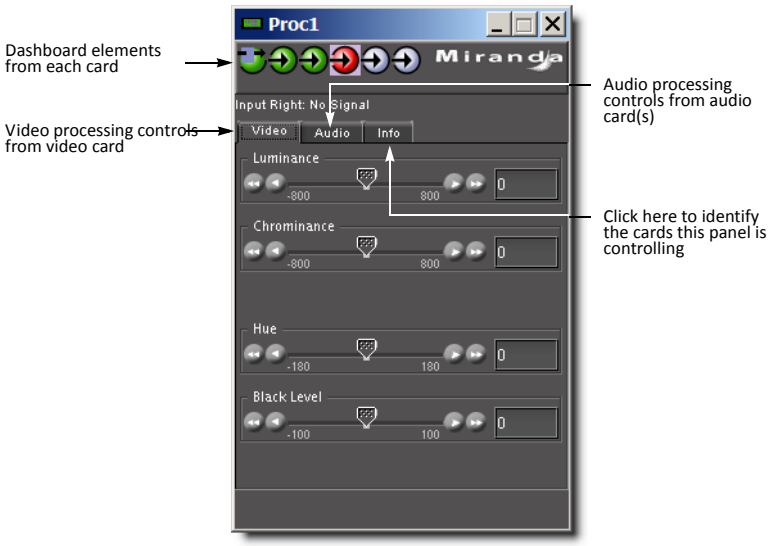
The Virtual Service Manager detects the compatible Imaging-series cards that are available on the network (i.e. visible in iC Navigator), and populates the drop-down menus with their labels.

> **Note:** The menus may contain cards with identical labels. Currently, the only way to tell the difference is by comparing the order of the cards in the menus with their order in iC Navigator.

9. Choose any combination of video proc amp cards, audio proc amp cards, and/or audio delay cards to be used to build the new proc amp.
10. Click **Add**.

    After a few seconds, the new proc amp appears in the iC Navigator window in its designated folder (only visible in **Logical view**).
11. Double-click the new proc amp in the iC Navigator window.

    The proc amp virtual control panel appears, with gains (controls) determined by the card type.



Removing a Proc Amp Device

REQUIREMENT

Before beginning this procedure, make sure you open iC Navigator (see page 697).

To remove a proc amp device from your system

- In iC Navigator (**Logical view**), right-click the proc amp device you wish to remove, and then click **Destroy**.

  The selected proc amp device disappears.

Creating a Composite Panel

Composite Panels are a new type of virtual service for controlling two or more cards with a single GUI. While intended primarily for Densité series cards, some older Imaging series cards are also supported.

Composite Panels can contain certain dashboard elements (e.g., input signal, reference), global audio and video alarms (if supported by the card), video processing elements, audio processing elements, and user presets. You can create up to 50 Composite Panels per Application Server.

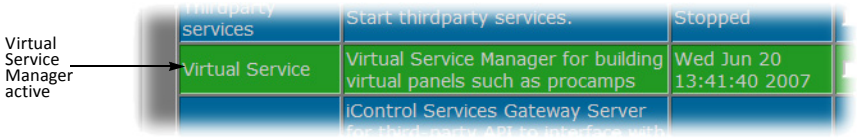
There are three steps involved in creating a Composite Panel: component selection, configuration, and initialization.

REQUIREMENT

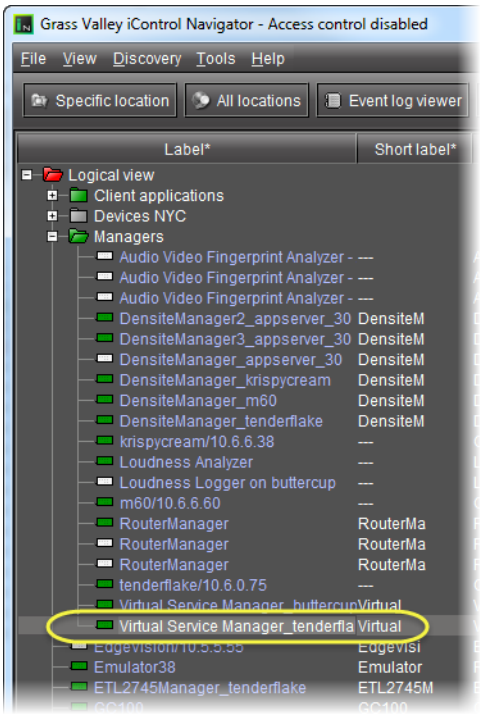
Before beginning this procedure, make sure you have opened the *Services management* page (see page 678).

To create a Composite Panel

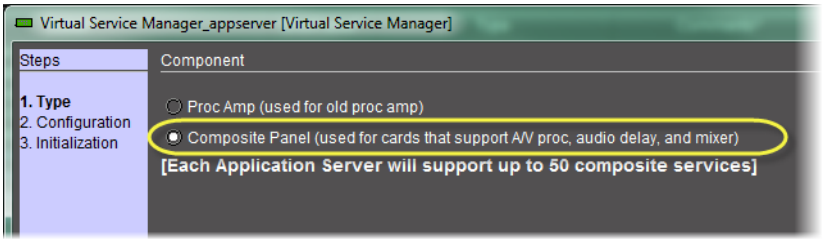
1. On the *Services management* page, make sure the Virtual Service Manager is active (green).



2. Open iC Navigator (see page 697).
3. Click the **Logical view** tab. Make sure that the Virtual Service Manager is visible.
4. Double-click the **Virtual Service Manager** row.

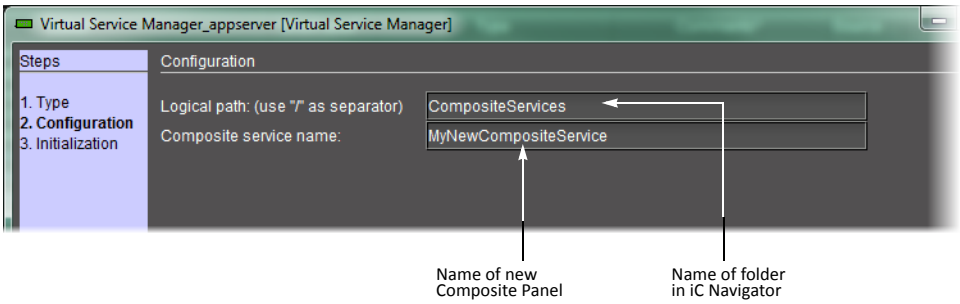


The **Virtual Service Manager** control panel appears, with the first of three pages (**Type**) displayed.



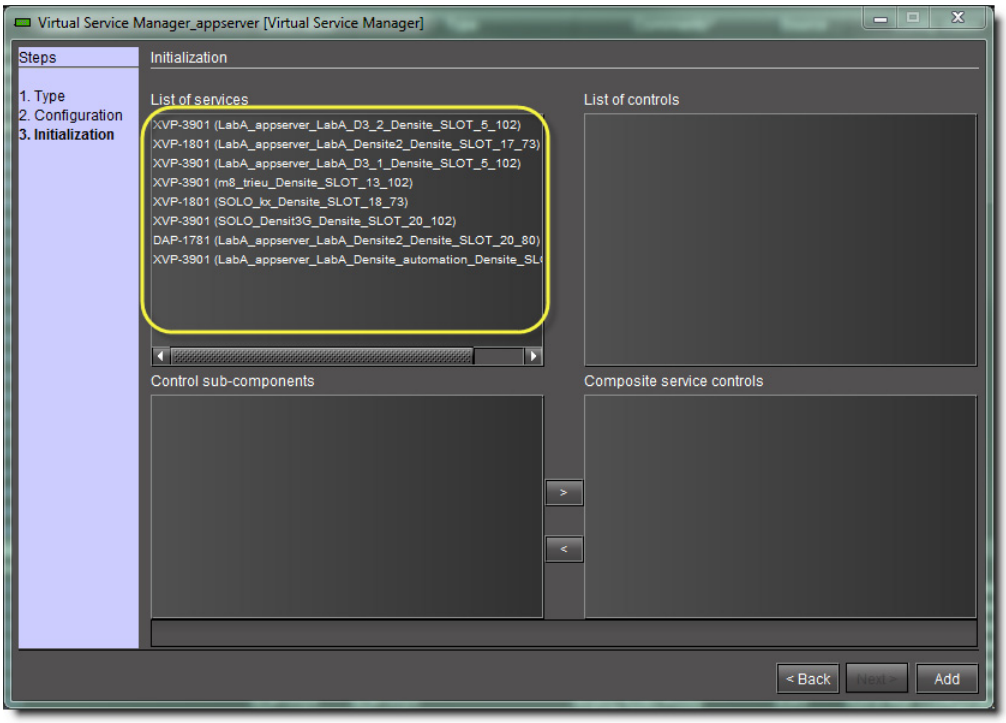
5. Click the **Composite Panel**, and then click **Next**.

   The **Configuration** window appears.



6. Type a logical path — this corresponds to the iC Navigator folder in which the new composite panel will appear. If the folder does not exist, a new one will be created automatically.
7. In the **Composite service name** field, type a name for the Composite Panel.
8. Click **Next**.

   The **Initialization** window appears.

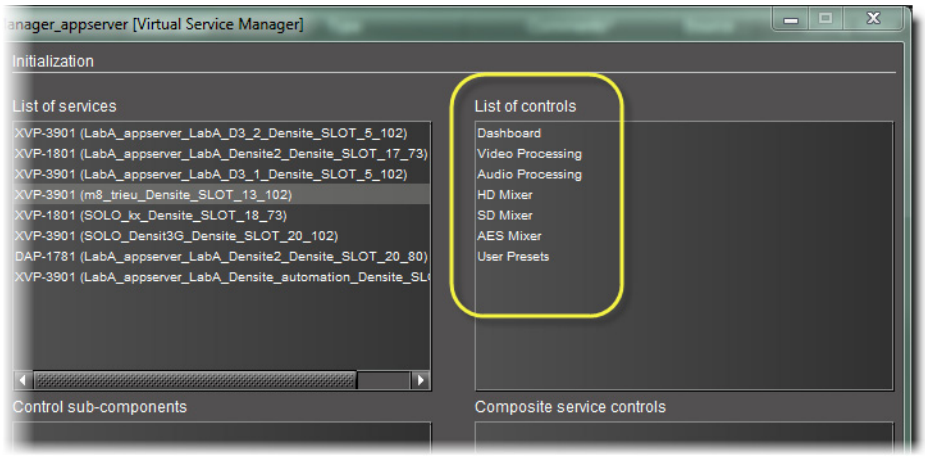


List of available cards and their services (circled) that support composite panels

The Virtual Service Manager detects the cards that are available on the network that support composite services, and populates the **List of Services** field with descriptions of these cards.

9. Choose an item from the **List of Services** field.

   The controls associated with that service appear in the **List of controls** field.

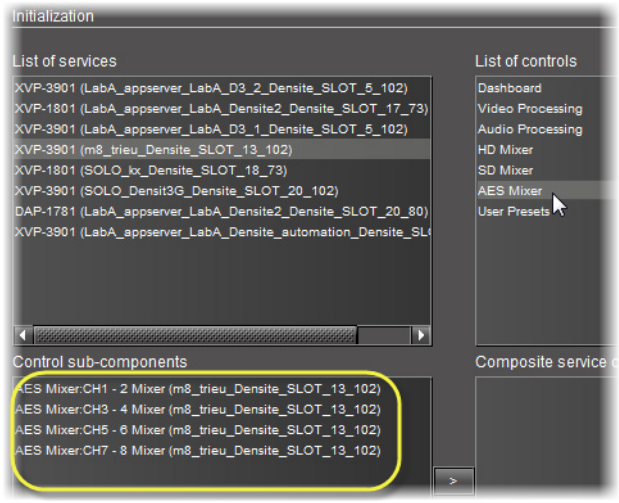


List of controls (circled) available for the selected card / service

10. Choose an item from the **List of controls** field.

    The control panel elements associated with that service appear in the **Control sub-components** field.

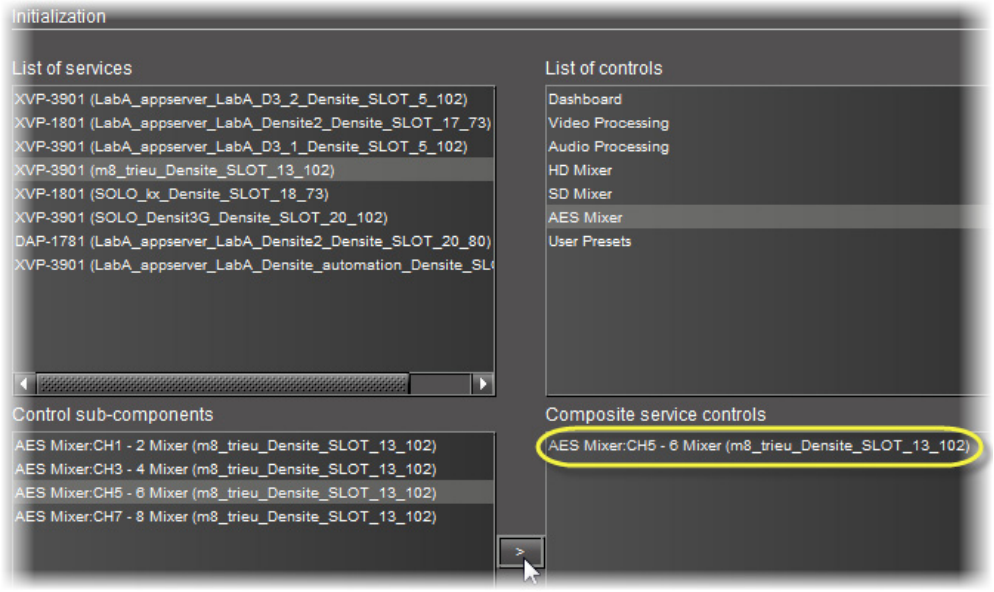
11. Choose an item from the **Control sub-components** field.



List of sub-components (circled) available for the selected control

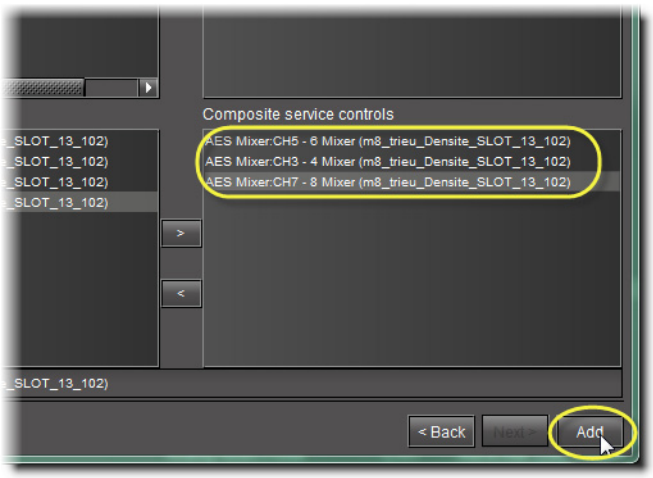
12. Click the right arrow (>) button.

    The selected control sub-components are copied to the **Composite service controls** field.



Composite service controls (circled)

13. Repeat step 7 through step 9 as necessary, until you have selected all the services you want to appear in the new composite panel.

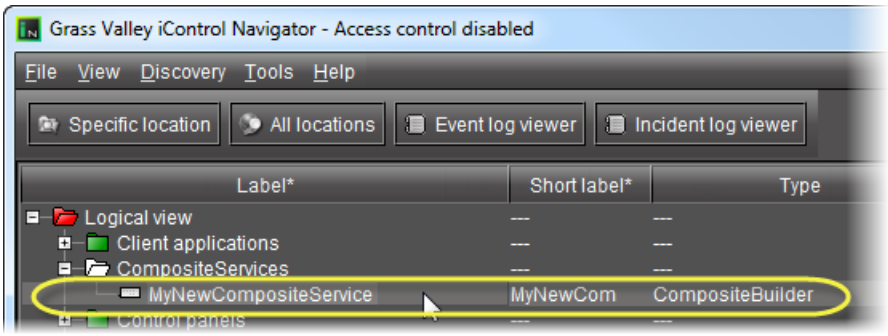


These control sub-components (circled) will all appear in the new Composite Panel

14. Click **Add**.

    After a few seconds, the new Composite Service appears in the iC Navigator window in its designated folder (only visible in **Logical view**).

15. Double-click the new Composite Service in the iC Navigator window.



Newly created composite service (circled)

The **Composite Service virtual** control panel appears.

Destroying a Composite Panel

REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To remove a Composite Panel from your system

- In iC Navigator window (**Logical view**), right-click the Composite Panel that you wish to remove, and then click **Destroy**.

  The selected Composite Panel disappears.

Adding a Card to the Reference Configuration

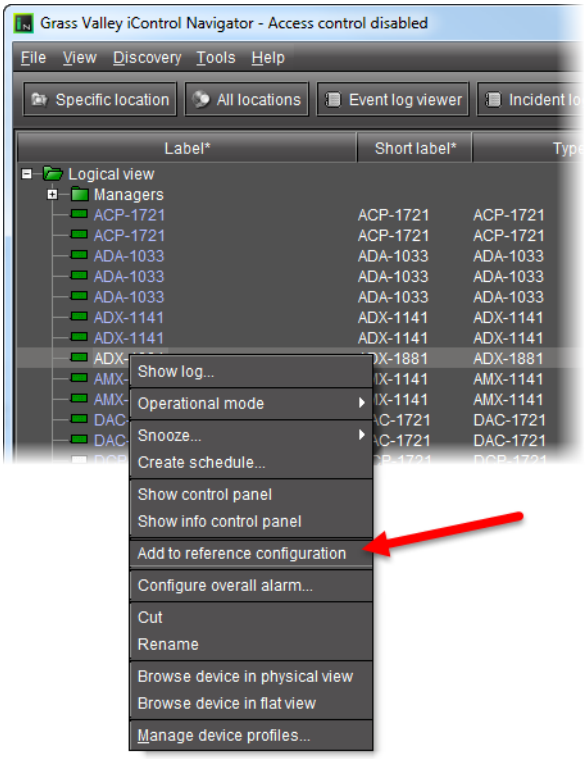
The reference configuration is a way for operators to keep track of cards or groups of cards important to their setup.

REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To add a card to the reference configuration

- In iC Navigator, right-click the card you wish to add, and then click **Add to reference configuration**.



The phrase **In Ref Configuration** appears in the **Config Status** column.

Note: If this card is physically removed from its slot, the card name remains in the **Label** column, along with the phrase **Missing from slot**.

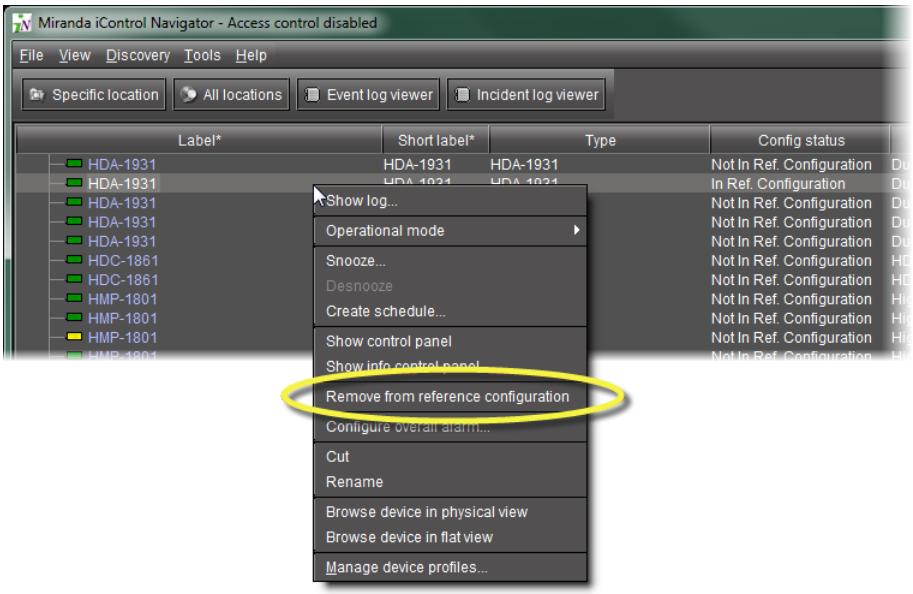
Removing a Card from a Reference Configuration

REQUIREMENT

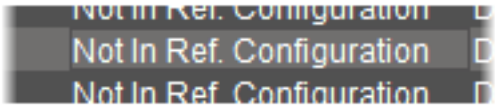
Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To remove a card from a reference configuration

- In iC Navigator, right-click the card you wish to remove, and then click **Remove from reference configuration**.



The phrase `Not In Ref Configuration` appears in the **Config Status** column.



Working with Device Profile Manager

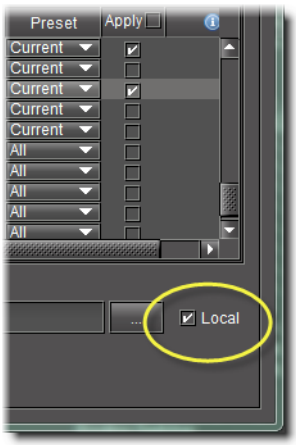
Exporting Selected Device Profiles to a Profile File

REQUIREMENT

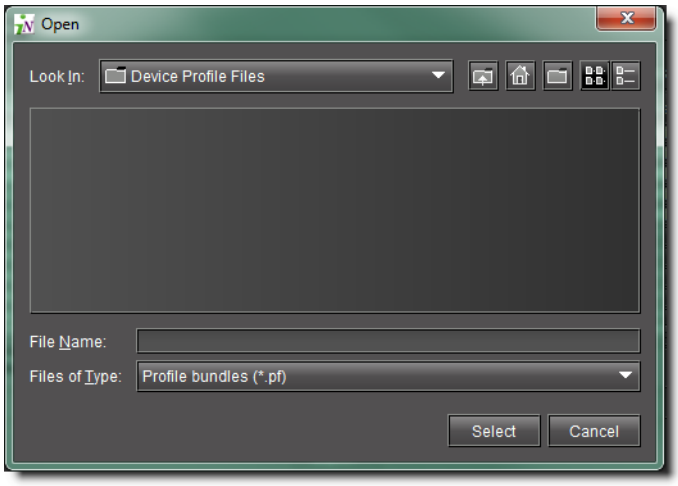
Before beginning this procedure, make sure you have opened **Device Profile Manager** (see page 707).

To export selected device profiles to a profile file

1. In **Device Profile Manager**, click the **Export** tab.
2. In the **Apply** column, select the devices whose profiles you would like to export to a file.
3. If you would like to export to a file on your local PC, perform the following steps:
   a) Select **Local**.

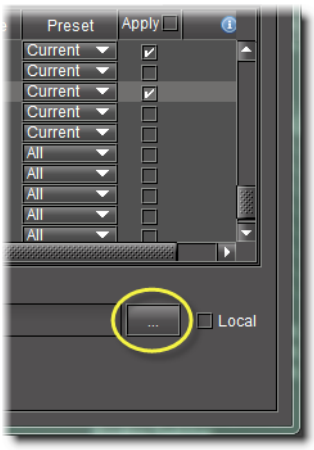


   b) Click **....**
   The **Open** window appears.

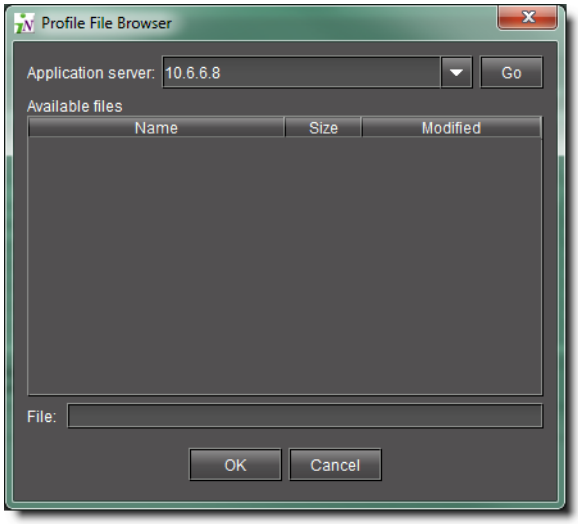


   c) In the **Look In** menu, browse for the directory you would like to export to (see Navigating with the File Browser in the Open Window, on page 278).
   d) In the **File Name** text field, type the name of the new profile file you wish to create.
   e) Click **Select**.
   The **Open** window closes.
4. If you would like to export to a file on an Application Server, perform the following steps:
   a) In **Device Profile Manager**, click **....**

Note: Make sure the **Local** check box is cleared.



The **Profile File Browser** appears.



b) Select the desired Application Server.

c) Click **Go**.

The **Profile File Browser** refreshes with the available profile files on the selected Application Server.

d) Do one of the following:

- In the **File** text field, type the name of a new profile file you wish to create.

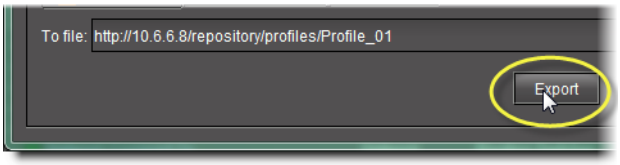
OR,

- From the list of available profile files, select a file you wish to overwrite.

e) Click **OK**.

The **Profile File Browser** closes.

5. In **Device Profile Manager**, click **Export**.



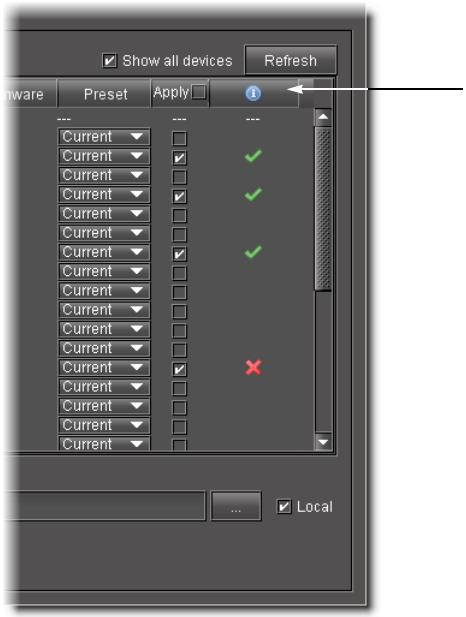
A progress window displays the export progress.

> **Note:** To cancel the operation before this process is complete, click **Cancel**.

When the process is complete, the **Export** confirmation window appears.

6. Click **OK** in the **Export** confirmation window.

The **Export** confirmation window closes. In **Device Profile Manager**, in the Result column (the column with the information icon in the header), either a check mark or an 'X' is displayed for selected devices.



> **Note:** A check mark indicates that the last operation for this device succeeded. An 'X' indicates that the last operation for this device failed.

Importing Profile Data from a File to Selected Devices

REQUIREMENT

Before beginning this procedure, make sure you have opened **Device Profile Manager** (see page 707).

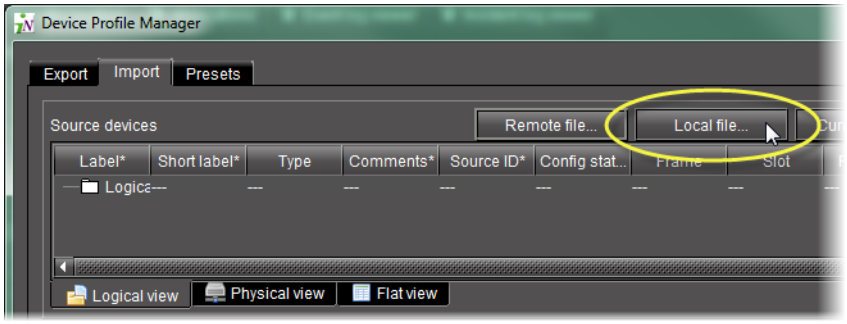
To import profile data from a file to selected devices

1. In **Device Profile Manager**, click the **Import** tab near to the top of **Device Profile Manager**.

   The **Import** tab displays listings of discovered or preset **Source devices** and **Target devices**.

2. If your profile file is on your local PC, perform the following steps:

   a) Click **Local file**.



   The **Open** window appears.

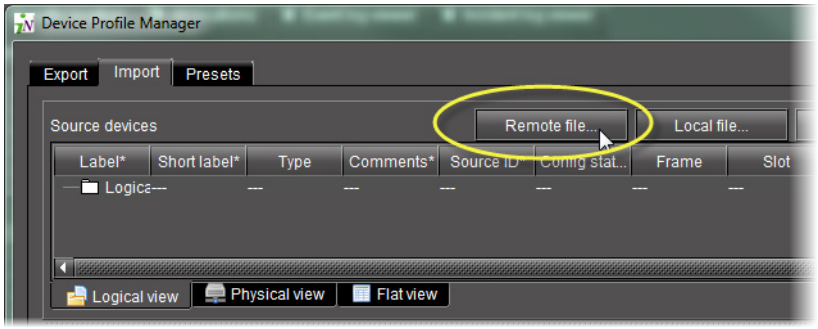
   b) Use the file browser to browse for the profile file from which you would like to import (see page 278).

   c) Click **Select**.

   The file is added to the **Source devices** list in **Device Profile Manager** and the **Open** window closes.

3. If your source device is on a remote Application Server, perform the following steps:

   a) In **Device Profile Manager**, click **Remote file**.

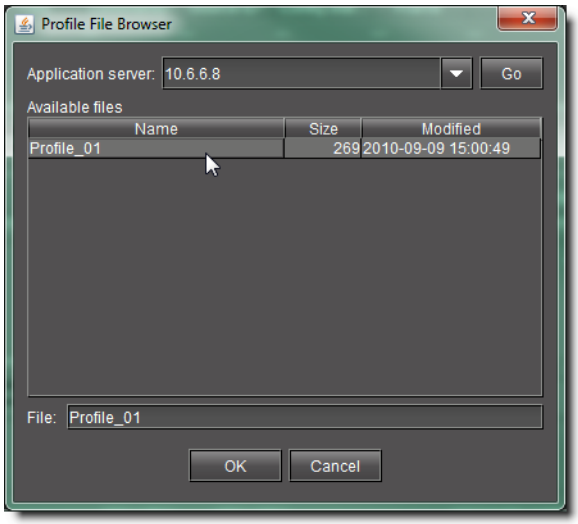


   The **Profile File Browser** appears and automatically searches for available profile files on the current Application Server.

   b) Select the desired Application Server, and then click **Go**.

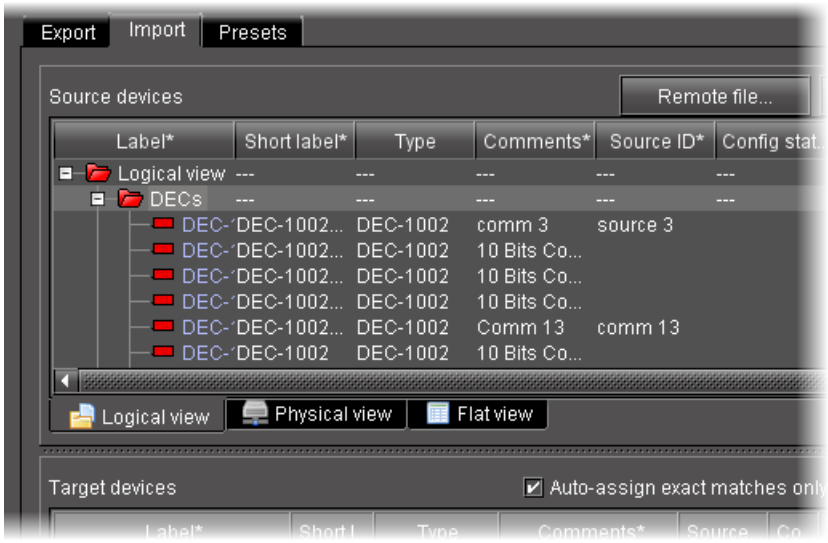
   The list is updated to reflect available files on the selected Application Server.

   c) Select the desired file from the list.



d) Click **OK**.

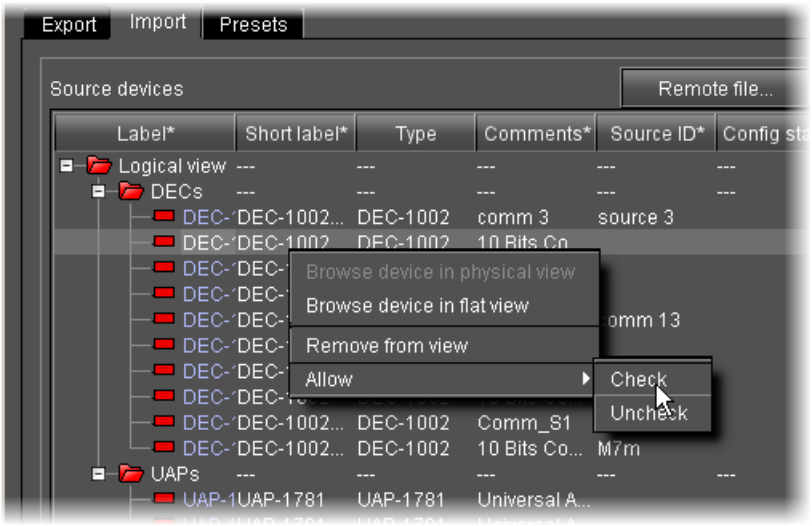
The selected file's profile data is added to the **Source devices** list in **Device Profile Manager** and the **Profile File Browser** closes.



4. In the **Source devices** area of **Device Profile Manager**, select the check box in the **Allow** column for the newly added source device,

   OR,

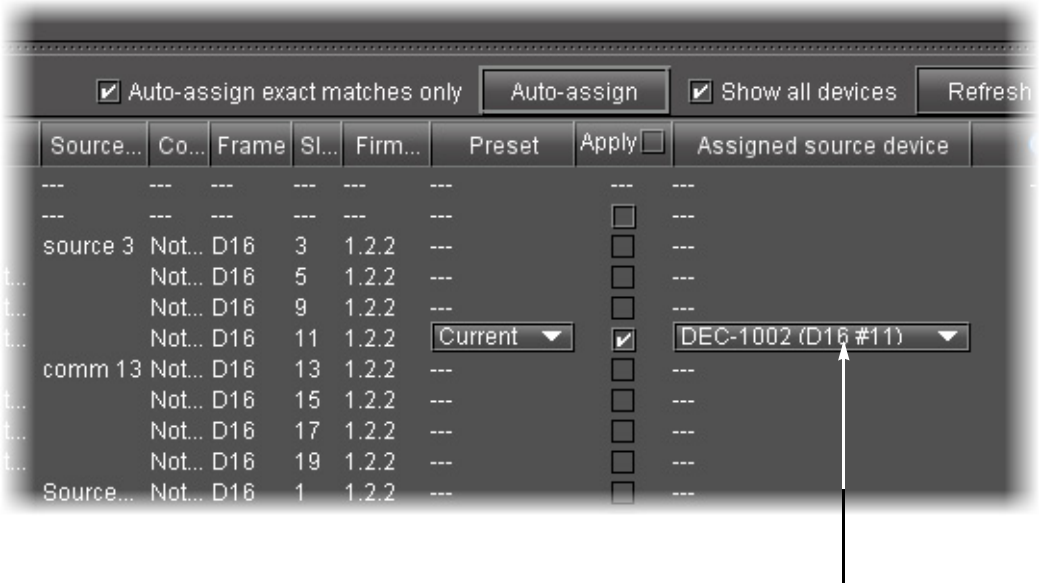
   Right-click the newly added source devices in the list, point to **Allow**, and then click **Check**.



Note: Use the shortcut method if you would like to apply a check mark to multiple selections at a time. To do this, first select the desired rows in **Device Profile Manager**, and then right-click one of them.

5. In the **Target devices** area of **Device Profile Manager**, if the desired target devices are not listed in the list of preset devices, click **Show all devices**.

   The **Target devices** list refreshes with a complete list of discovered devices.



Note: By default, the **Auto-assign exact matches only** check box is selected. For those targets with exact matches to any listed source devices, assigned sources appear in the **Assigned source device** column.

6. In the **Target devices** area, perform the following steps:
   a) Select all devices to which you would like to download imported profile data.
   b) If you would like to perform exact matching of sources to targets, select **Auto-assign exact matches only**, otherwise the system performs lenient matching.

   Note: *Exact matching* allows users to quickly finish the task when they only need to import onto identical devices and are not concerned with extraneous devices. *Lenient matching* is for advanced users who would like to import onto non-identical but compatible devices.

   c) Select the check boxes in the **Apply** column for all devices to which you would like to attempt to import profile data.

   Note: If you want to select check boxes for all listed devices, select the **Apply** check box in the header row.

   d) Click **Auto-assign** to discover matches between the listed source and target devices.

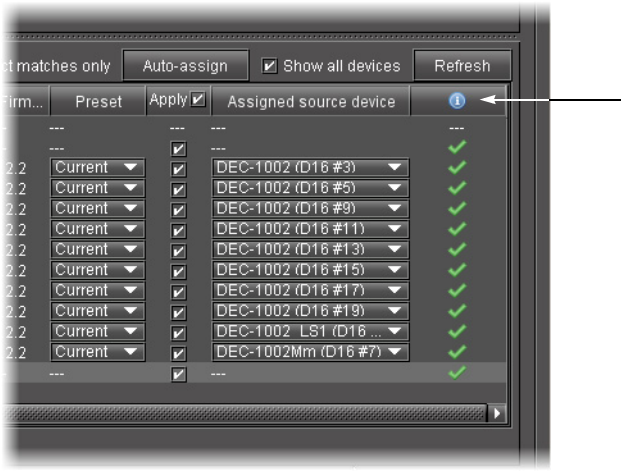
      For each selected target with at least one matching source, possible source devices are listed in the **Assigned source device** column.
   e) In the **Assigned source device** column, select the desired source device match for each selected target.
   f) Click **Import**.

      A progress window displays the import progress.

      Note: To cancel the operation before this process is complete, click **Cancel**.

      When the process is complete, the **Import** confirmation window appears.
   g) Click **OK** in the **Import confirmation** window.

      In the Result column (the column with the information icon in the header) of the **Target devices** area, either a check mark or an 'X' is displayed for selected devices.



Note: A check mark indicates that the last operation for this device succeeded. An 'X' indicates that the last operation for this device failed.

Comparing Configured Parameters Between Selected Devices

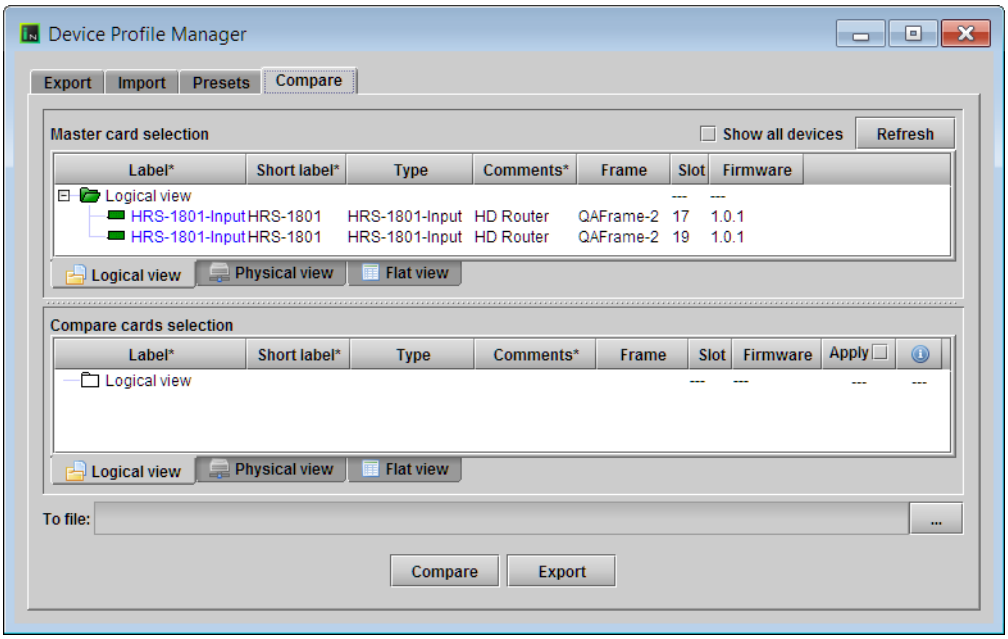
REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To compare configured parameters between selected cards

1. In iC Navigator, select the cards whose configured parameters you wish to compare.
2. Right-click the selection, and then click **Compare**.

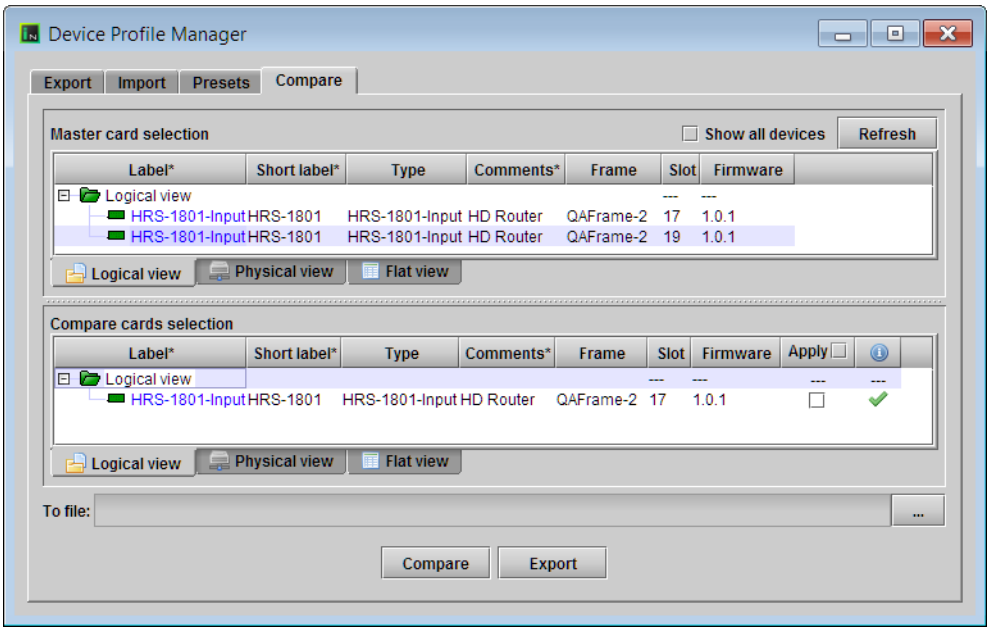
   Device Profile Manager appears, with the **Compare** tab in focus. Both panes are in **Logical view** mode. The selected cards appear in the **Master card selection** pane.



Note: You can select **Show all devices** to display all discovered devices.

3. In the **Master card selection** pane, click the card you wish to use as the reference device for the comparison.

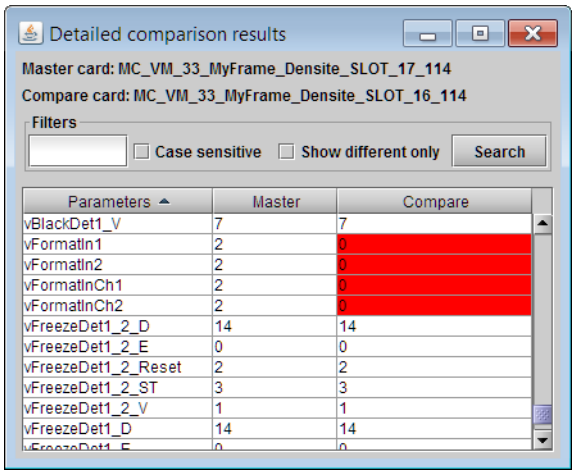
   Cards *of the same type and firmware version* appear in the **Compare card selection** pane.



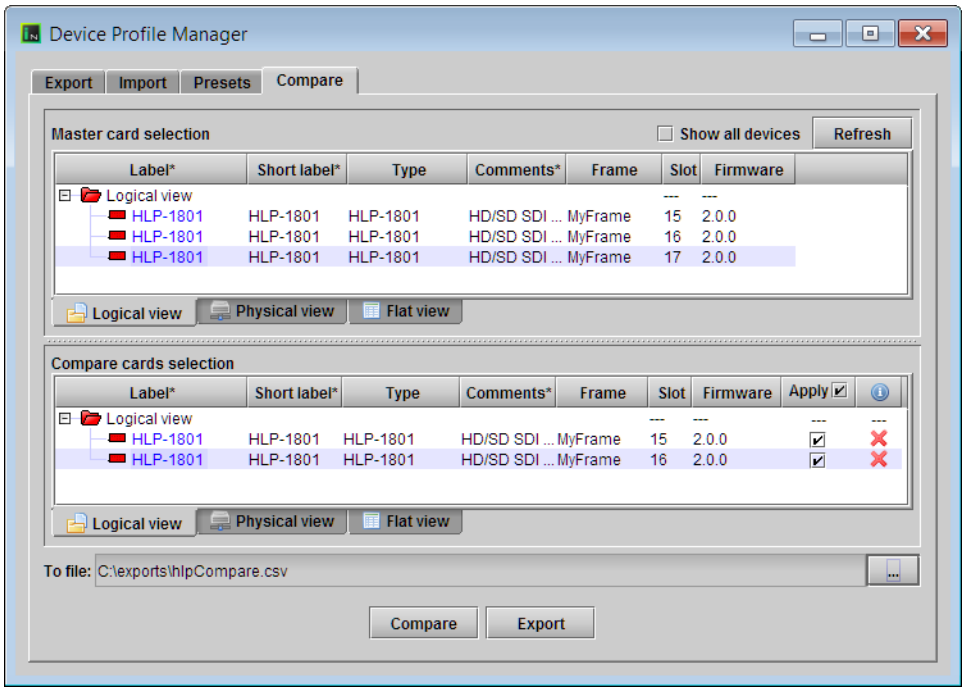
A green check mark in the Information column for a card indicates that this card and the master card have the same settings. A red cross indicates that there are differences between the cards' configured parameters.

- **To review a card's configured parameters, against the master card's:** In the **Compare cards selection** pane, click the card you wish to compare against the master, and then click the **Compare** button.

  The **Detailed comparison results** window appears, with differences highlighted in red. You can filter the comparison results by typing text in the **Filters** box, selecting **Case sensitive**, or **Show different only**, and then clicking **Search**.



- **To export card configuration details to a CSV file:** In the **Apply** column, select the cards whose parameters you wish to export by clicking the corresponding check boxes, click the Browse button to specify the CSV file name and location, and then click **Export**.



The exported CSV file lists all configured parameters, with one column for the master card, and a column for each of the cards you selected for export.

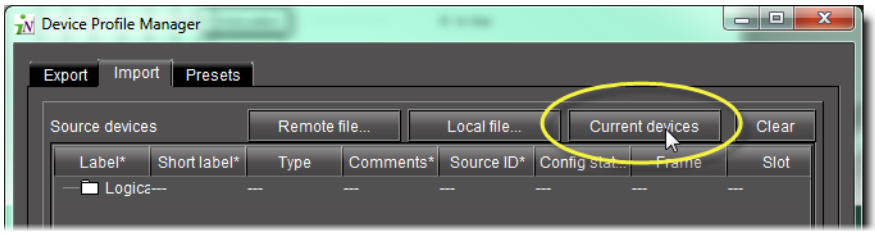
Copying Profile Data from Selected Devices to Other Selected Devices

REQUIREMENT

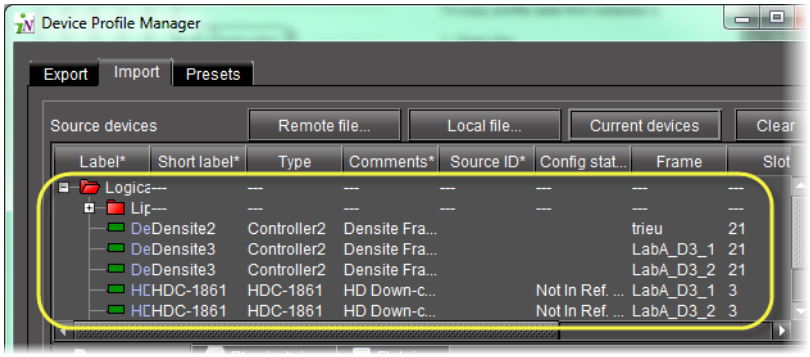
Before beginning this procedure, make sure you have opened **Device Profile Manager** (see page 707).

To copy profile data from selected devices to other selected devices

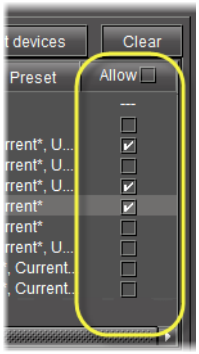
1. In **Device Profile Manager**, click the **Import** tab.
2. In the **Source devices** area, perform the following steps:
   a) Click **Current devices**.



The **Source devices** area is populated with all discovered current devices.

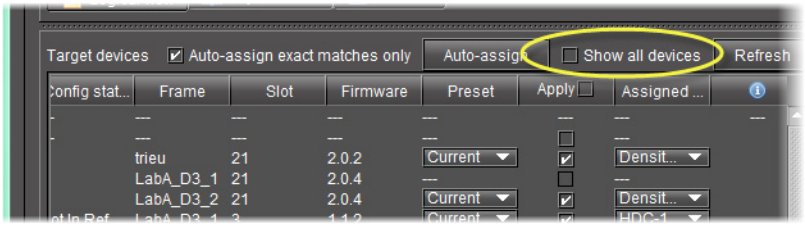


   b) In the **Allow** column, select each device whose configuration data you would like to copy from.



3. In the **Target devices** area, perform the following steps:

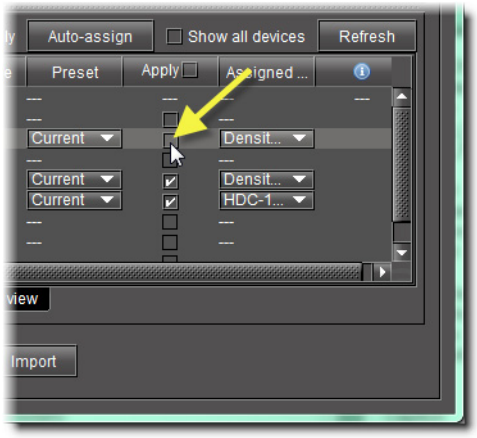
   a) Select **Show all devices** to display all discovered devices.



   The **Target devices** area is populated with all discovered devices.

> **Note:** The target devices all display auto-assigned matches (the check box in the **Apply** column is selected for each device).

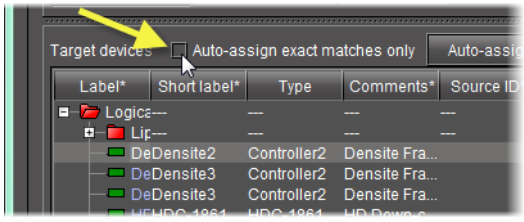
   b) For each target device you do not want to copy configuration data to, clear the **Apply** check box.



   c) For each target device you would like to copy configuration data to, make sure the assigned source device is the appropriate choice. If it is not, select a more appropriate source device from the list in the **Assigned source device** column.

4. In the **Assigned source device** column, if you do not find the source device you would like to assign, perform the following steps:

   a) Clear the **Auto-assign exact matches only** check box.



   b) Click **Auto-assign**.

The lists of possible source device matches, in the **Assigned source device** column, are expanded to include non-exact matches.

c) Select the appropriate source device match from the expanded lists.

5. Click **Import**.

   The configuration data from the selected source devices is copied to the selected target devices.

   In the **Result** column (the column with the in the header) of the **Target devices** area, either a check mark or an 'X' is displayed for selected devices.

> **Note:** A check mark indicates that the last operation for this device succeeded. An 'X' indicates that the last operation for this device failed.

Loading a Device's Preset Configuration Data as its Current Configuration

REQUIREMENT

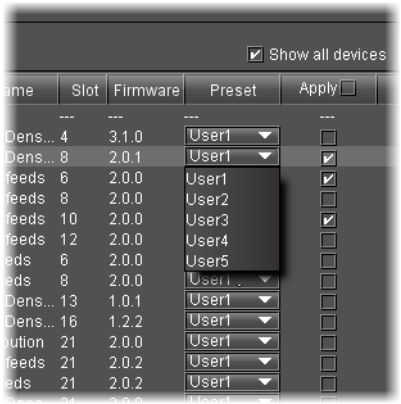
Before beginning this procedure, make sure you have opened **Device Profile Manager** (see page 707).

To load a device's preset configuration data as its current configuration

1. In **Device Profile Manager**, click the **Presets** tab near to the top of the window.

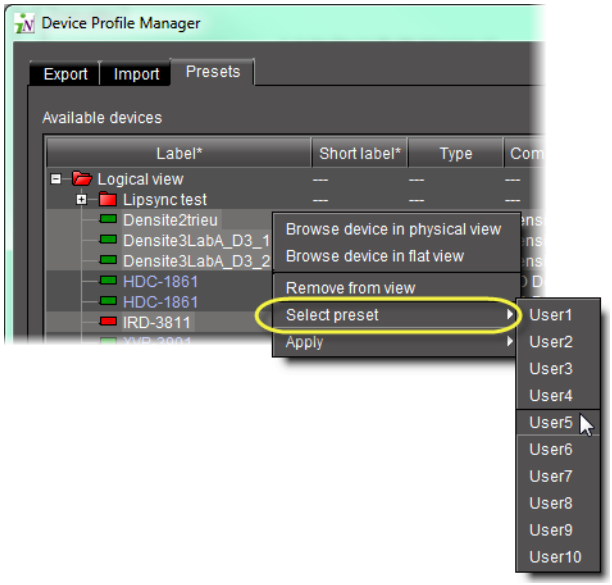
   The **Presets** tab displays listings of discovered or preset devices.

2. Click **Show all devices** to populate the list.
3. In the **Available devices** area, select those devices with presets you would like to set as the active configuration.
4. If you would like to assign presets individually for each of the selected devices, select the preset you would like to load as the active configuration.

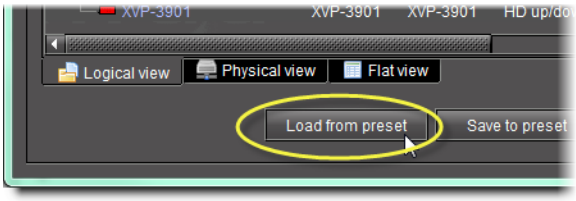


Note: When a preset is selected in the **Preset** column, the corresponding **Apply** check box is automatically selected.

5. If you would like to assign one preset to multiple devices, perform the following steps:
   a) Select those devices for which you would like to assign a preset as the active configuration.
   b) Right-click on any one of the selected devices, point to **Select preset**, and then click the desired preset from the list.



6. Click **Load from preset**.



A confirmation window appears.

7. Click **OK** in the confirmation window.

Saving a Device's Current Configuration Data as One of its Presets

REQUIREMENT

Before beginning this procedure, make sure you have opened **Device Profile Manager** (see page 707).

To save a device's current configuration data as one of its presets

1. In **Device Profile Manager**, click the **Presets** tab near to the top.

   The **Presets** tab displays listings of discovered or preset devices.

2. For each of the selected devices, perform the following steps:

   a) In the **Preset** column, select the preset to which you would like to save configuration data.

   b) In the **Apply** column, for each device with active configuration data you would like to save to a preset, select the check box.

3. Click **Save to preset**.

   A confirmation window appears.

4. Click **OK** in the confirmation window.

Navigating with the File Browser in the Open Window

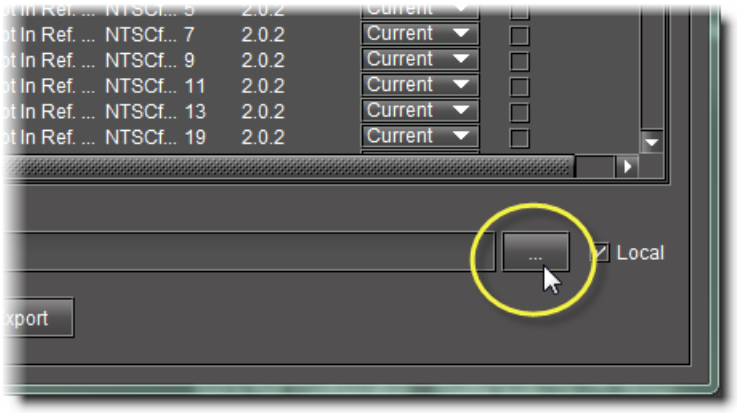
REQUIREMENT

Before beginning this procedure, make sure you have opened **Device Profile Manager** (see page 707).

To navigate with the file browser in the Open Window

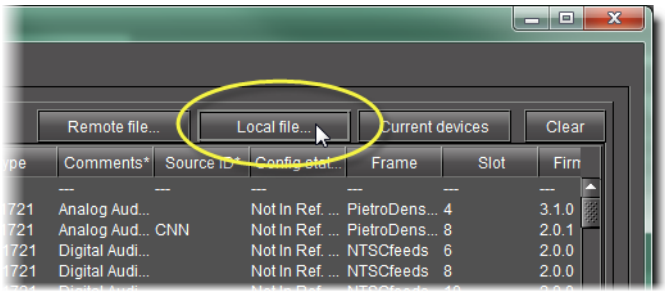
1. In **Device Profile Manager**, perform only **ONE** of the following steps, depending on your requirements:

   - If you are exporting, on the **Export** tab, click the File browser button ( ) near the bottom, right side of the window.



OR,

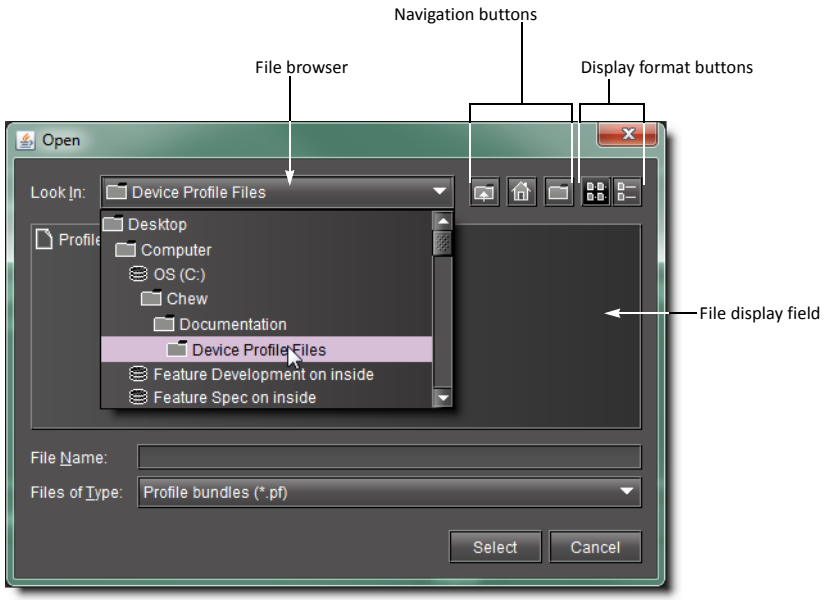
- If you are importing, on the **Import** tab, click **Local file**.



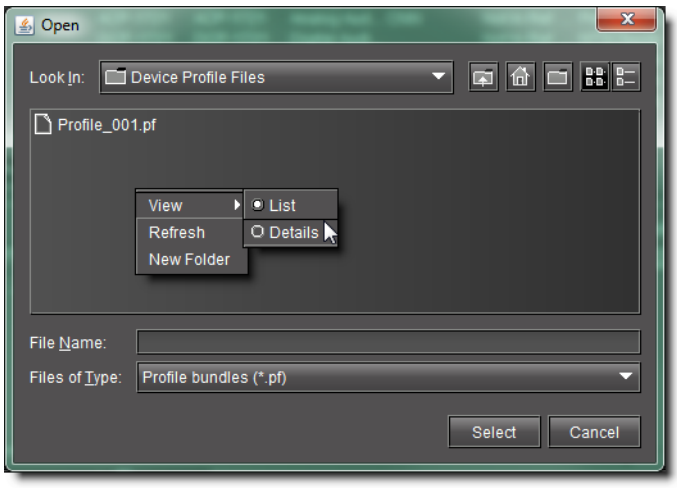
The **Open** window appears.

2. In the **Open** window, browse to the local directory where the desired profile file is located or where you wish to create a profile file.

Note:	Use the **Navigation** buttons to help you browse.



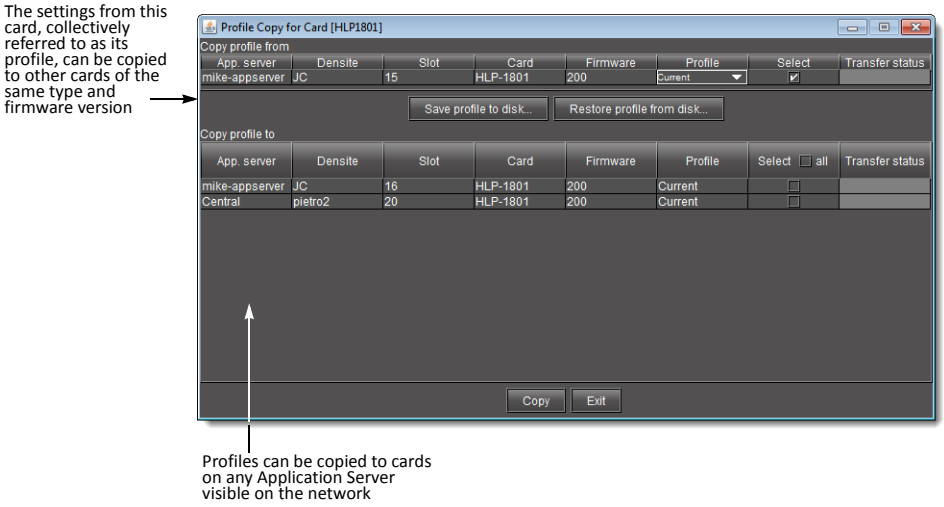
3. To change the view format of the displayed files, use the **Display format** buttons, or perform the following steps:
   a) Right-click anywhere in the **File display** field.
   b) Point to **View**, and then click either **List** or **Display**, as required.



The view format changes to the selected mode.

Copying Densité Card Profiles

When a card, such as a video or audio probe, is added to a Densité-series frame, it must be configured for monitoring and control. The configuration settings are referred to as a *card profile*. In iControl, a card profile can be copied from one card to another of the same type and firmware version.



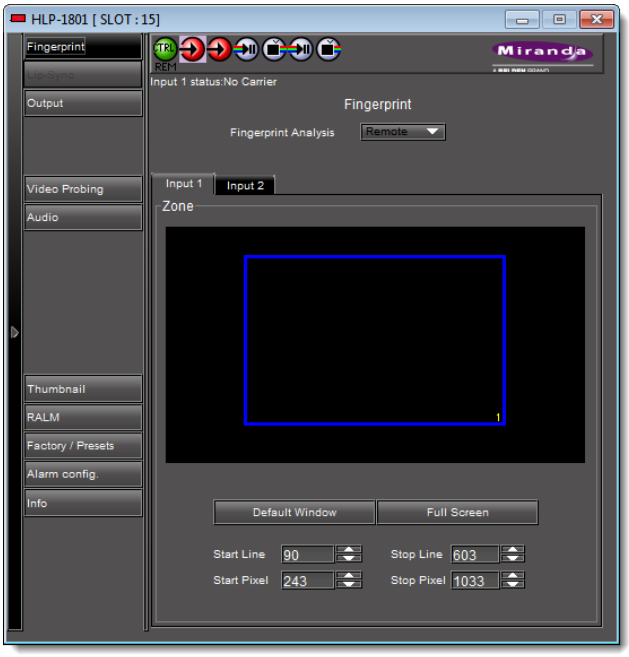
REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

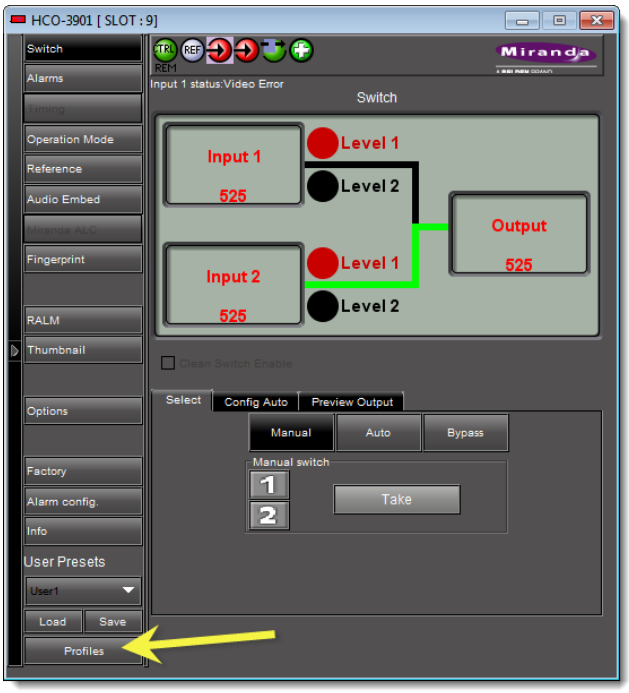
To copy a card profile

1. In iC Navigator, double-click the card whose profile you would like to copy.

   The *info control panel* for the card appears.



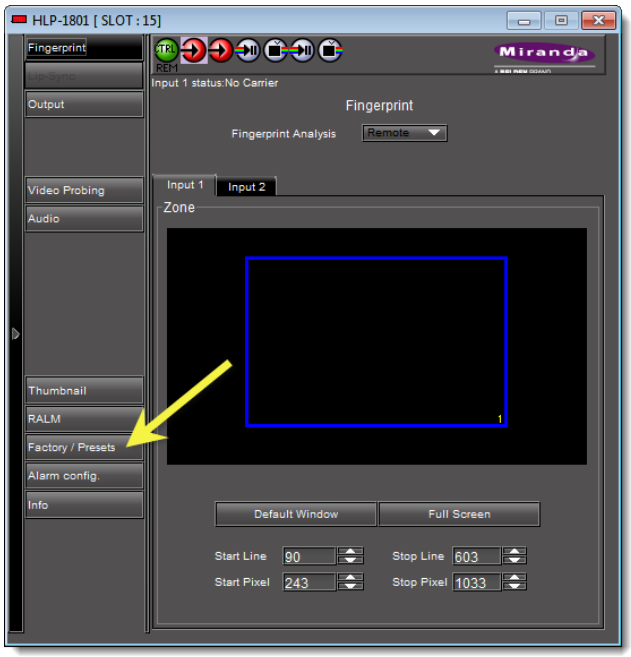
*Info control panel with NO **Profiles** button in left navigation bar*



*Info control panel WITH **Profiles** button in left navigation bar*

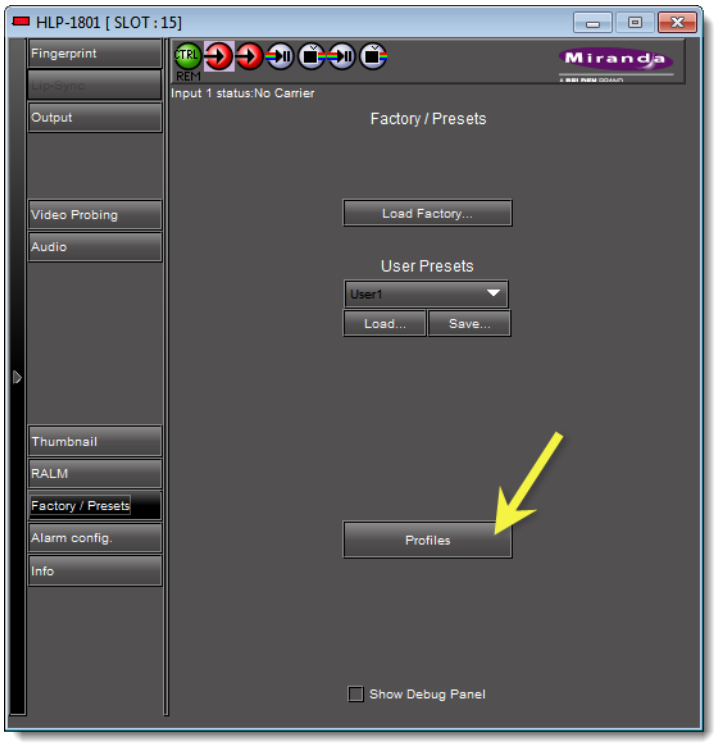
2. If the info control panel of your card *does not* have a **Profiles** button on the left navigation bar, perform the following sub-steps:

   a) Click **Factory/Presets**.



The **Factory/Presets** pane appears.

b) Click **Profiles**.



The **Profile Copy for Card** window appears.

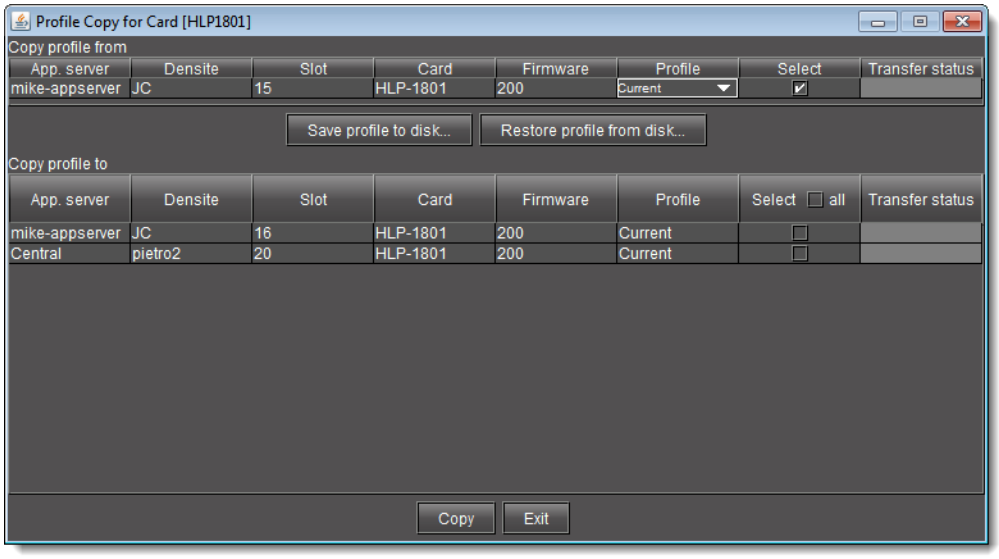
c) Proceed to step 4.

3. If the info control panel of your card *does* have a **Profiles** button on the left navigation bar, click **Profiles**.

The **Profile copy for card** window appears.

4. For each card to which you would like to copy the current profile, perform the following steps:

   a) In the **Profile copy for card** window, select the corresponding check box in the **Select** column.



Notes

- Select **Select All** at the top of the column to select all the available cards. Click **Clear Selections** at the bottom of the window to remove all check marks from the **Select** column.
- The copy profile operation is prohibited when a target card does not have the same firmware version as the source card. In such cases, the designation 'N/A' will appear on a yellow background in the **Transfer status** column.

   b) Click **Copy**.

   A successful copy is indicated for each card by the appearance of the word 'Succeeded' in the **Transfer status** column.

   c) Click **Exit** to close the **Profile Copy for Card** window.

Copying Card Alarm Configurations

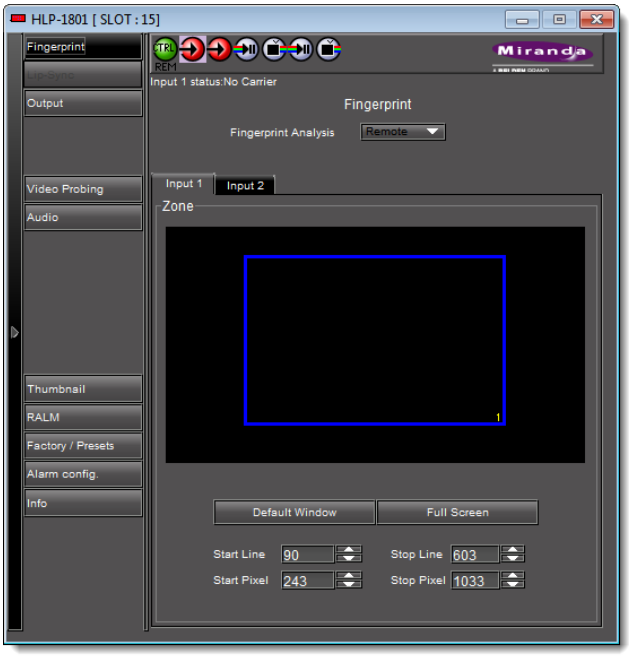
Densité, GeckoFlex, and Imaging cards have default settings for the alarms that they will pass on to iControl. This alarm configuration can be modified (e.g., non-essential alarms can be turned off). Once a particular card's alarm configuration has been modified, it be copied to others of the same type and firmware version.

REQUIREMENT

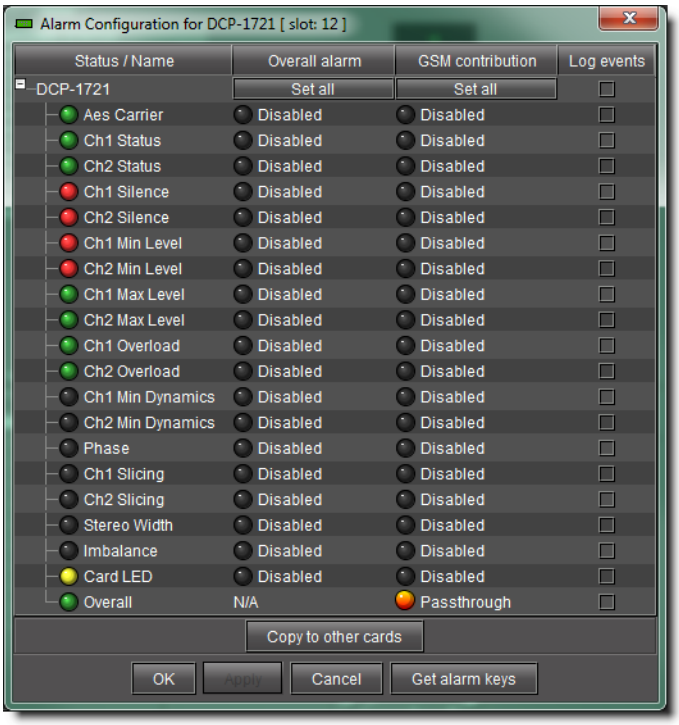
Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To copy a card's alarm configuration to one ore more other cards

1. In iC Navigator, double-click the card whose alarm configuration you would like to copy.
   The **Info** Control Panel for the card appears.

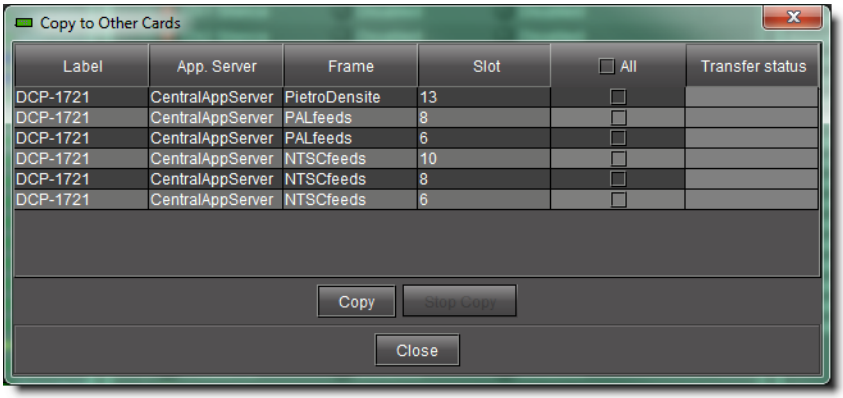


2. Click **Alarm config** at the bottom left of the **Info** Control Panel.
   The card's **Alarm Configuration** panel appears.



3. Click **Copy to other cards**.

   The **Copy to other cards** window appears, displaying a list of all cards of the same type.



4. For each card to which you wish to copy the current alarm configuration, select the corresponding check box.
5. Select the **All** check box at the top of the column to select all the available cards.
6. Select the **All** check box a second time to remove all check marks.
7. Click **Copy**.

   A successful copy is indicated for each card by the appearance of the word Succeeded in the **Transfer status** column.
8. Click **Close** to close the **Copy to other cards** window.

Getting Alarm Keys

Each alarm provided by a given Densité, GeckoFlex, or Imaging series card has an associated value, or *key*, that serves as a unique identifier. An alarm's URI, for example, contains its key. The alarm key can also be useful when creating scripts.

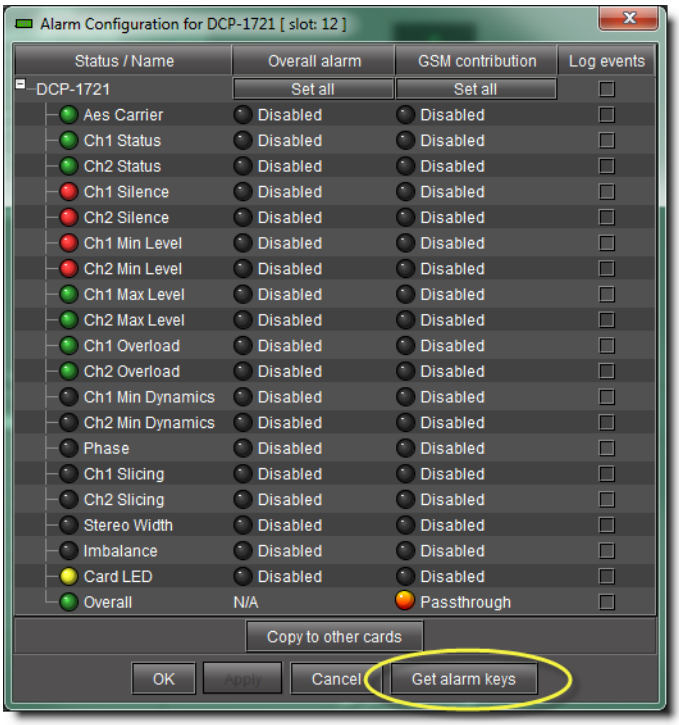
It is possible to save a list of a card's alarms and associated keys in a CSV file that can be viewed in any text editor or spreadsheet application.

REQUIREMENT

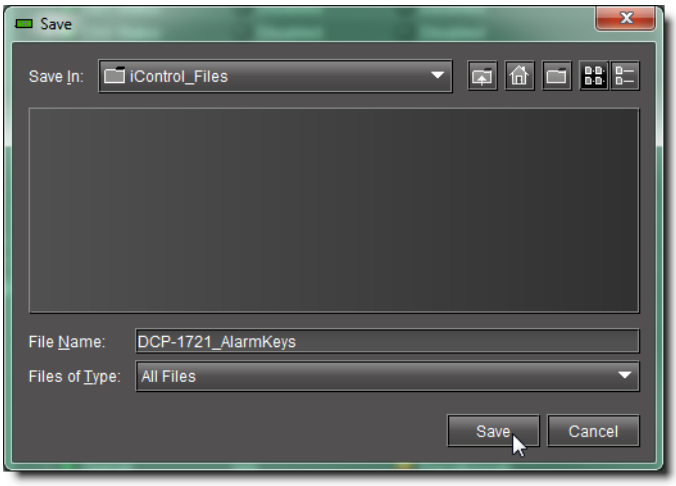
Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To save a card's alarm keys

1. In iC Navigator, double-click a card to open its control panel, and then click **Alarm config**.
   The **Alarm configuration** window appears.
2. Click **Get alarm keys**.

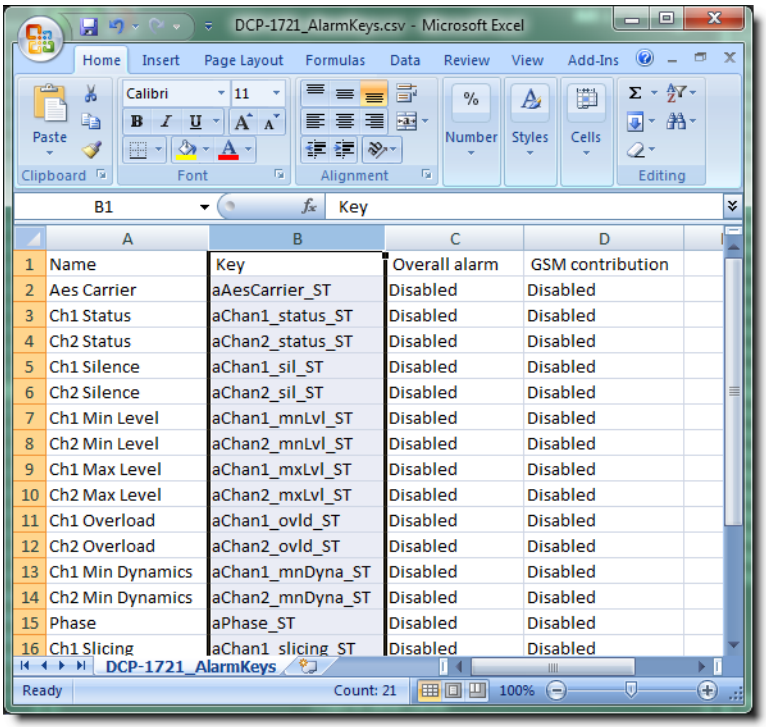


3. In the **Save** window, specify a location and type a name for the CSV file, and then click **Save**.



A CSV file is created in the specified location.

4. Open the CSV file to view a list of the card's alarms, the associated keys, as well as the currently configured Overall and GSM contributions.



	A	B	C	D
1	Name	Key	Overall alarm	GSM contribution
2	Aes Carrier	aAesCarrier_ST	Disabled	Disabled
3	Ch1 Status	aChan1_status_ST	Disabled	Disabled
4	Ch2 Status	aChan2_status_ST	Disabled	Disabled
5	Ch1 Silence	aChan1_sil_ST	Disabled	Disabled
6	Ch2 Silence	aChan2_sil_ST	Disabled	Disabled
7	Ch1 Min Level	aChan1_mnLvl_ST	Disabled	Disabled
8	Ch2 Min Level	aChan2_mnLvl_ST	Disabled	Disabled
9	Ch1 Max Level	aChan1_mxLvl_ST	Disabled	Disabled
10	Ch2 Max Level	aChan2_mxLvl_ST	Disabled	Disabled
11	Ch1 Overload	aChan1_ovld_ST	Disabled	Disabled
12	Ch2 Overload	aChan2_ovld_ST	Disabled	Disabled
13	Ch1 Min Dynamics	aChan1_mnDyna_ST	Disabled	Disabled
14	Ch2 Min Dynamics	aChan2_mnDyna_ST	Disabled	Disabled
15	Phase	aPhase_ST	Disabled	Disabled
16	Ch1 Slicing	aChan1_slicing_ST	Disabled	Disabled

Working with Densité Upgrade Manager

From time to time, improvements or fixes may become available that can be applied to an existing Densité card by upgrading its firmware and software. Firmware and software updates are available as a bundled package. To determine if an update package is available for a specific card, please contact *Grass Valley Technical Support* (see Contact Us, on page 739).

Changing a Densité Card's Installed Package

The package of a Densité card consists of a version of software and a version of firmware bundled together. You can upgrade your card's firmware and software simply by upgrading the installed package. Use iC Navigator's **Densité Upgrade Manager** to manage your card packages and Densité card upgrades.

IMPORTANT: System behavior

Regardless of whether your installed package is upgraded, downgraded or rolled back, software always installs from a package stored on your Application Server. If you use the **Upgrade** button, firmware installs *ONLY IF* it has a different version number (either newer or older) than the currently installed firmware.

If you would like to force your Densité card to install same-version firmware, use the *Force upgrade* functionality (see page 292).

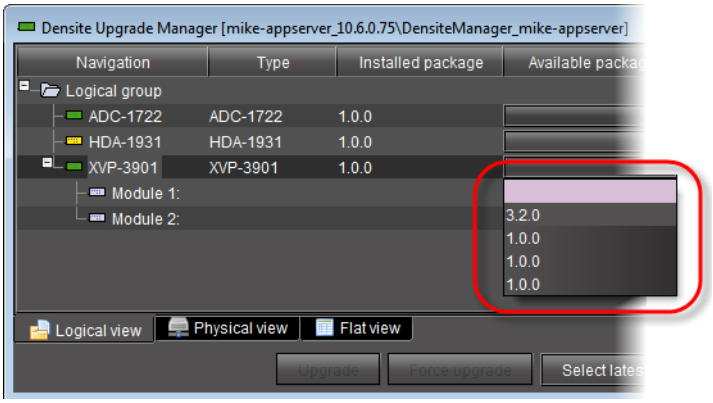
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **Densité Upgrade Manager** (see page 709).
- The Densité cards whose installed packages you would like to change are visible in **Densité Upgrade Manager**.
- The package you would like to install on your Densité card has already been uploaded to your Application Server (see Uploading a Densité Card Package to an Application Server, on page 296).

To change a Densité card's installed package

1. In **Densité Upgrade Manager**, verify if the package you would like to install on your Densité card is available on the Application Server in the **Available package** column.

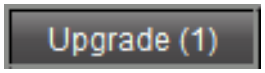


2. In the **Available package** column, in the row corresponding to the card to be upgraded or downgraded, select the package you would like to use.

   In the row corresponding to each Densité card you are upgrading or downgrading, the following should occur:

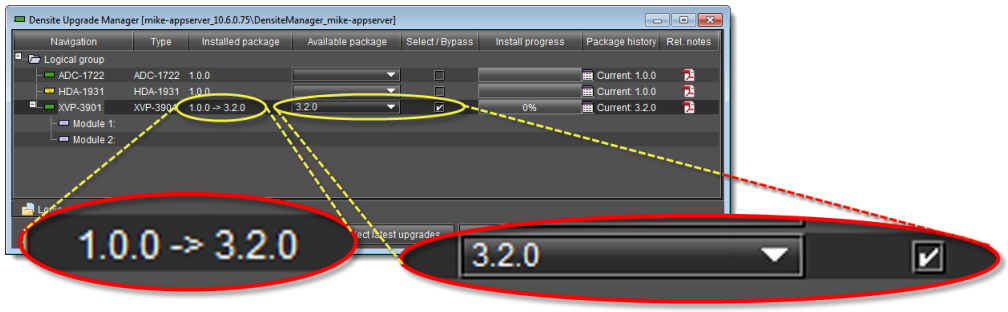
   - The **Select/Bypass** check box is selected.

- The **Upgrade** button bears the **(N)** suffix, where *N* indicates the number of cards selected for package installation.



- The selected package appears in the **Available package** column.
- The upgrade/downgrade paths of firmware, software, and package are displayed respectively in the **Installed firmware**, **Installed software**, and **Installed package** columns.

Note: The paths for firmware and software are displayed only if you have first manually made visible the **Installed firmware** and **Installed software** columns of **Densité Upgrade Manager** (see page 298).



Selected package with package upgrade path displayed

IMPORTANT: In rare circumstances, you may have a ***Beta*** version of firmware installed on your Densité card and may wish to upgrade to a full production version of firmware bearing the same version number. In this situation, if you use the **Upgrade** button, **Densité Upgrade Manager** will not install the firmware.

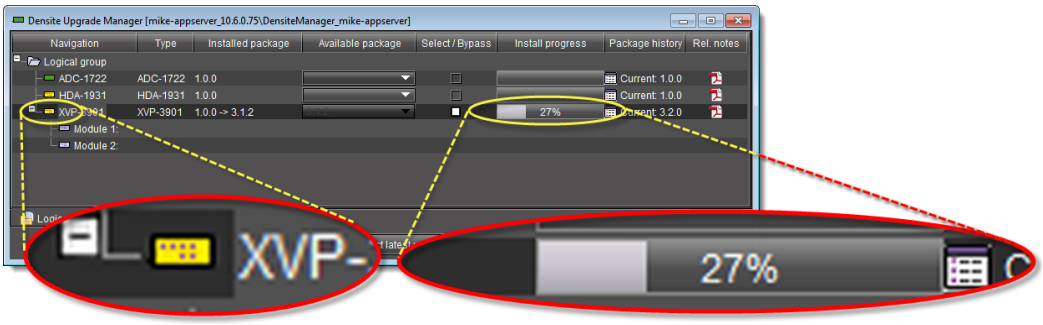
To force **Densité Upgrade Manager** to install firmware of the same-version as the currently installed firmware, click **Force upgrade** instead of **Upgrade**. (see Forcing a Same-Version Firmware Installation onto a Densité Card, on page 292).

3. Click **Upgrade** (or in the rare situation detailed above, click **Force upgrade**).

   The **Upgrade confirmation** window appears.

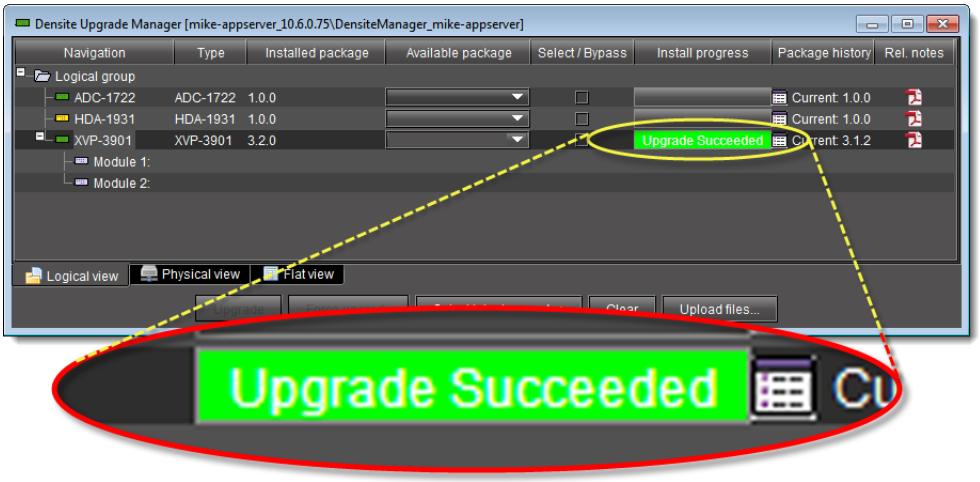
4. Click **Yes**.

   During the upgrade, a progress bar appears in the **Install progress** column and the card icon becomes yellow.

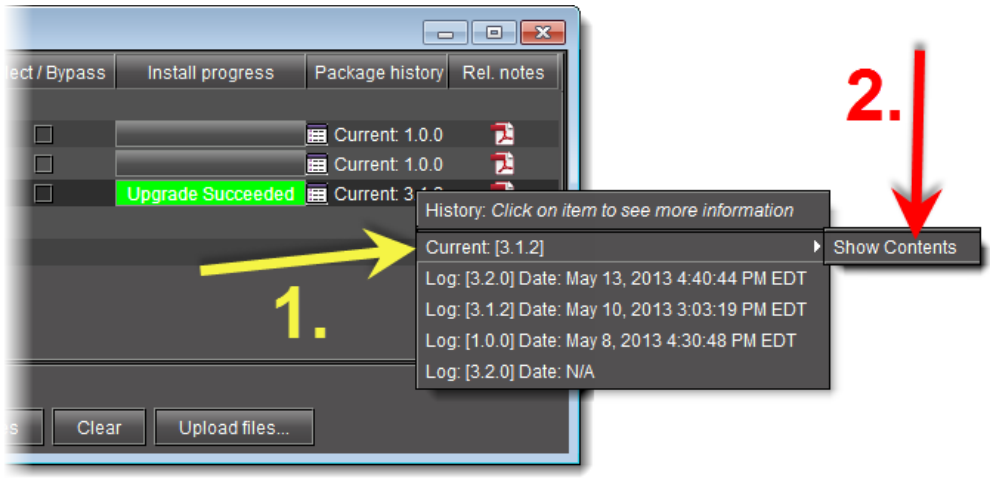


Upgrade in progress signified by yellow card icon; progress bar

When the process is finished, the **Upgrade Succeeded** message appears.



5. If you would like to view a log of this upgrade session, click the cell at the intersection of the **Package history** column and the row corresponding to the Densité card whose installed package you just changed.
6. Point to **Current**, and then click **Show Contents**.



The last upgrade's status (the status of the currently installed package) is displayed on a *per component* basis.

Forcing a Same-Version Firmware Installation onto a Densité Card

Perform this procedure **ONLY** in the rare situation that the card you would like to upgrade currently has a *Beta* version of firmware. If this is the case, using the **Upgrade** button will not upgrade the firmware to the full production version of firmware bearing the same official release number (even if **Densité Upgrade Manager** indicates both the package and software versions have been upgraded). Only the **Force upgrade** button successfully installs same-version firmware.

Note: After performing a forced upgrade of firmware, executing a *rollback* operation will roll back the card to the pre-upgrade firmware even if the two versions carry the same version number. In effect, after a forced upgrade, by selecting a *Rollback* version (under **Available package**), you are in fact performing a *forced rollback* operation.

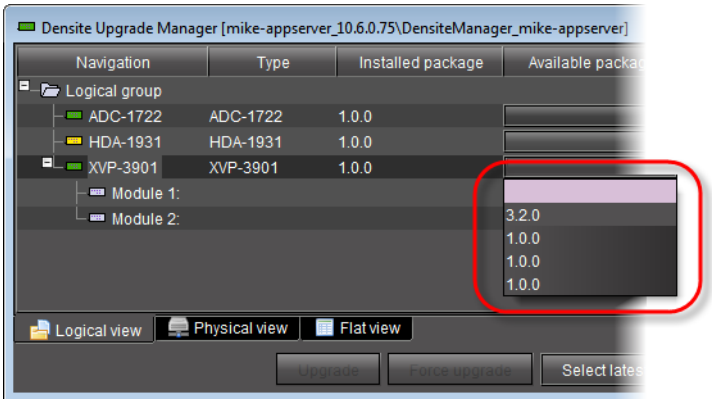
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **Densité Upgrade Manager** (see page 709).
- The Densité cards whose firmware and software you would like to upgrade are visible in **Densité Upgrade Manager**.
- The package you would like to use to upgrade your Densité card has already been uploaded to your Application Server (see Uploading a Densité Card Package to an Application Server, on page 296).

To force a same-version firmware installation onto a Densité card

1. In **Densité Upgrade Manager**, verify if the package you would like to install on your Densité card is available on the Application Server in the **Available package** column.



2. Grass Valley recommends displaying the **Installed firmware** and **Installed software** columns of **Densité Upgrade Manager** for this procedure. For steps on how to display these columns, see Viewing a Densité Card's Installed Firmware and Installed Software

Versions, on page 298.

3. In the **Available package** column, select the desired package.
4. In the **Installed firmware** column, take note of the upgrade path.

   If the displayed upgrade path indicates that the card is not moving to a different firmware version (for example, if the displayed upgrade path is `3.1.2 -> 3.1.2`), then to override the firmware you must use the *Force upgrade* functionality. Otherwise, you may use the *Upgrade* functionality.[1]
5. Click **Force upgrade**.

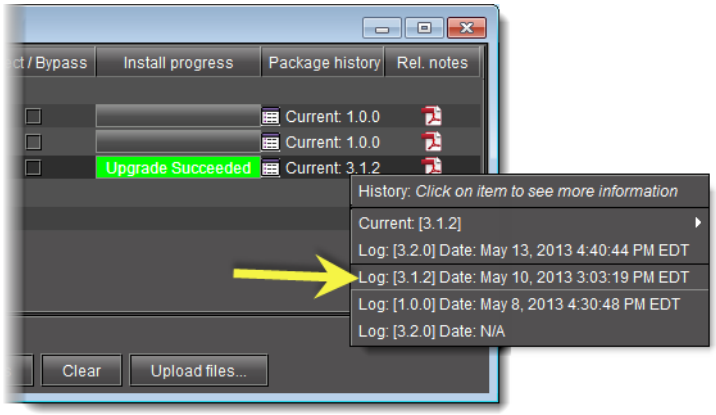
Viewing Upgrade Logs

REQUIREMENT

Before beginning this procedure, make sure you have opened **Densité Upgrade Manager** (see page 709).

To view upgrade logs

1. In **Densité Upgrade Manager**, in the row corresponding to the card whose upgrade history you would like to view, click in the **Package history** column.
2. Click the upgrade log you wish to view.



The selected log is displayed.

Rolling Back a Card's Installed Package to the Pre-Upgrade Version

Perform this procedure if, after installing a package on a Densité card, you decide to restore both the firmware and software of the card to their respective pre-installation versions.

1. The real-world situation in which you will find it necessary to override typical **Upgrade** button functionality (that is, to force an upgrade of same-version firmware from a selected package) would be if your installed firmware is a *Beta* version and the embedded firmware in the selected package is the production version of firmware bearing the same release number.

Note: In the case where you are rolling back a package installation resulting from a *Force upgrade* operation, the rollback operation effectively becomes a *Force rollback* operation. That is, even though the firmware currently installed and the firmware you are rolling back to bear the same version number, the rollback will proceed.

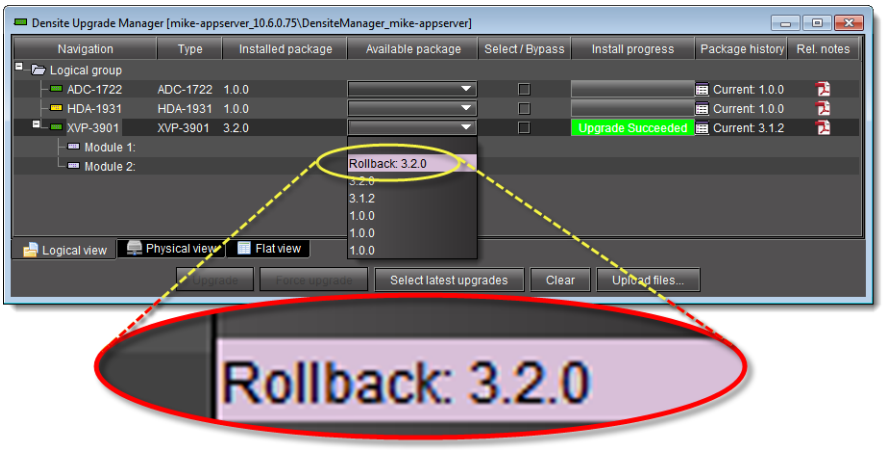
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

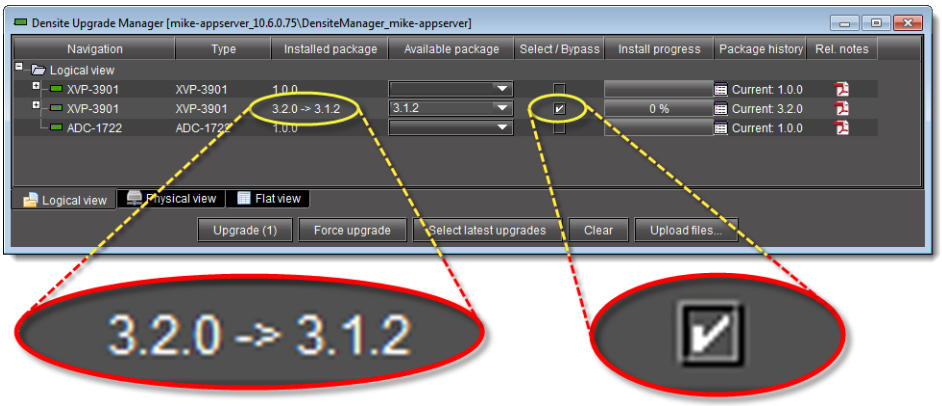
- You have opened **Densité Upgrade Manager** (see page 709).
- The Densité cards whose firmware and software you would like to downgrade are visible in **Densité Upgrade Manager**.
- The package you would like to use to downgrade your Densité card has already been uploaded to your Application Server (see Uploading a Densité Card Package to an Application Server, on page 296).

To roll back a Densité card's installed package to the pre-upgrade version

1. In **Densité Upgrade Manager**, in the row corresponding to the card whose installed package you would like to roll back, select **Rollback <version #>** in the **Available package** column.

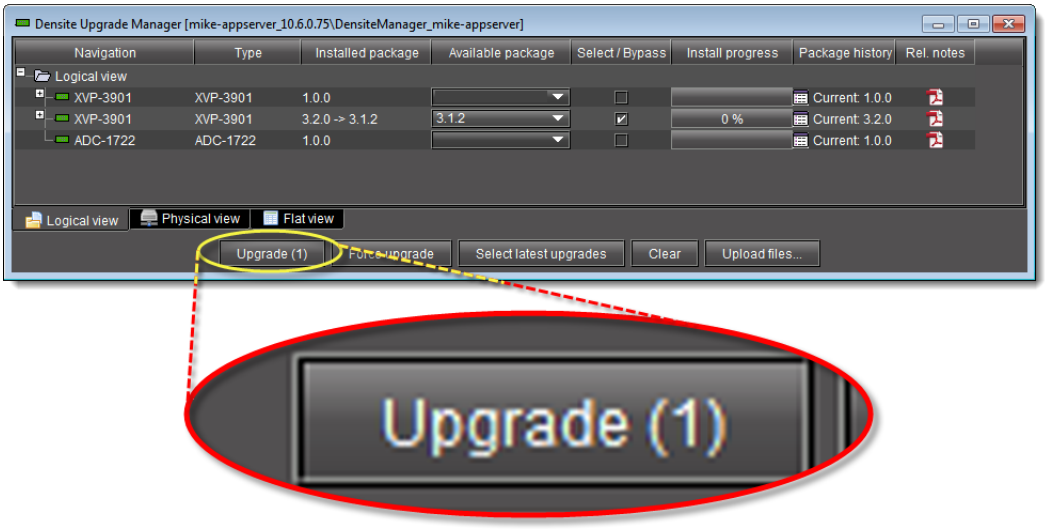


The **Select/Bypass** check box for that card is selected, indicating that this card will undergo a change in its installed package, and the rollback path is indicated in the **Installed package** column.

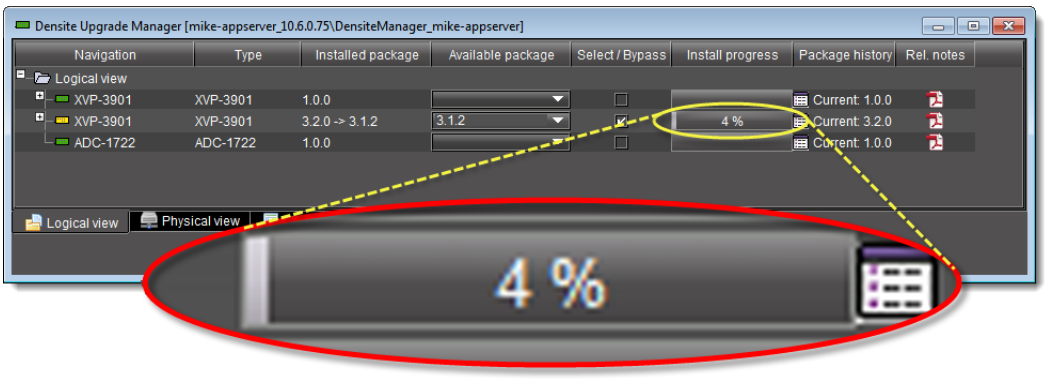


Rollback package selected for card installation (note the rollback path)

2. Click **Upgrade**.



The rollback operation begins. You can monitor the progress of the rollback with the progress bar in the **Install progress** column.



When the rollback operation is complete, the **Install progress** column displays a success message.

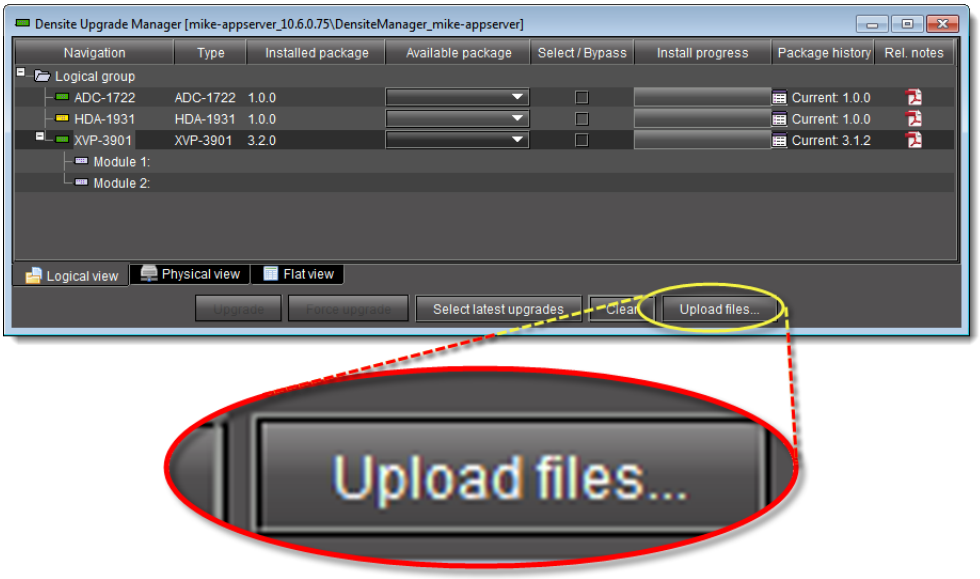
Uploading a Densité Card Package to an Application Server

REQUIREMENT

Before beginning this procedure, make sure you have access to the upgrade package file on your local file system. If you do not have the correct upgrade package, contact *Grass Valley Technical Support* (see Contact Us, on page 739).

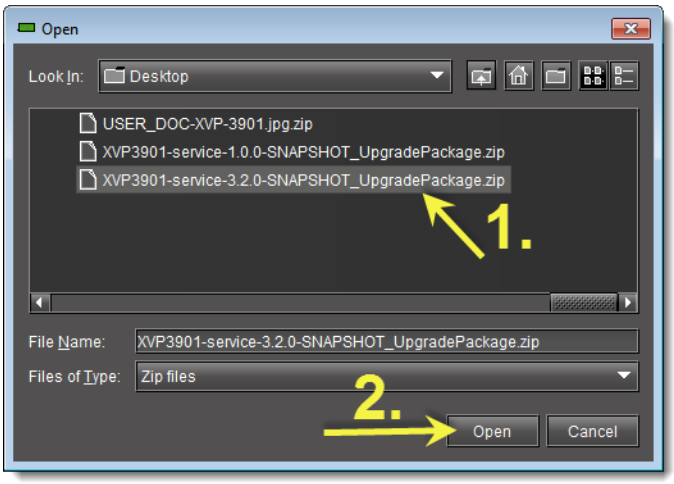
To upload an upgrade package

1. In **Densité Upgrade Manager**, click **Upload files**.



A file browsing window appears.

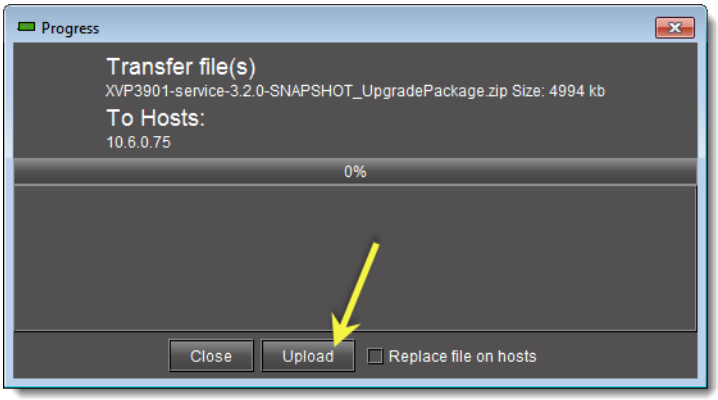
2. Navigate to the appropriate directory in your local file system, select the required upgrade package file, and then click **Open**.



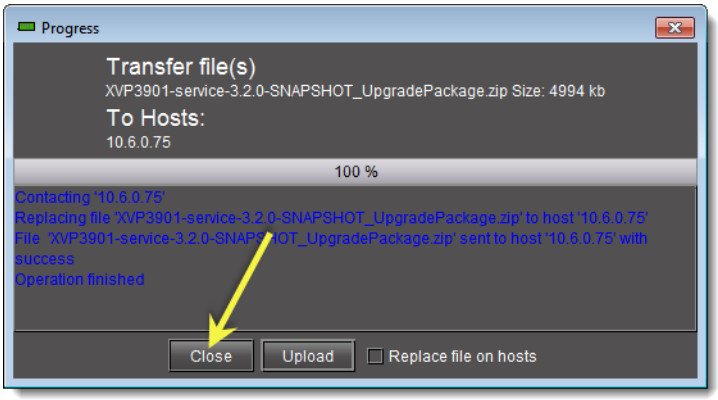
Note: You may select more than one package file to upload at a time.

A message window appears, prompting you to start the upload process.

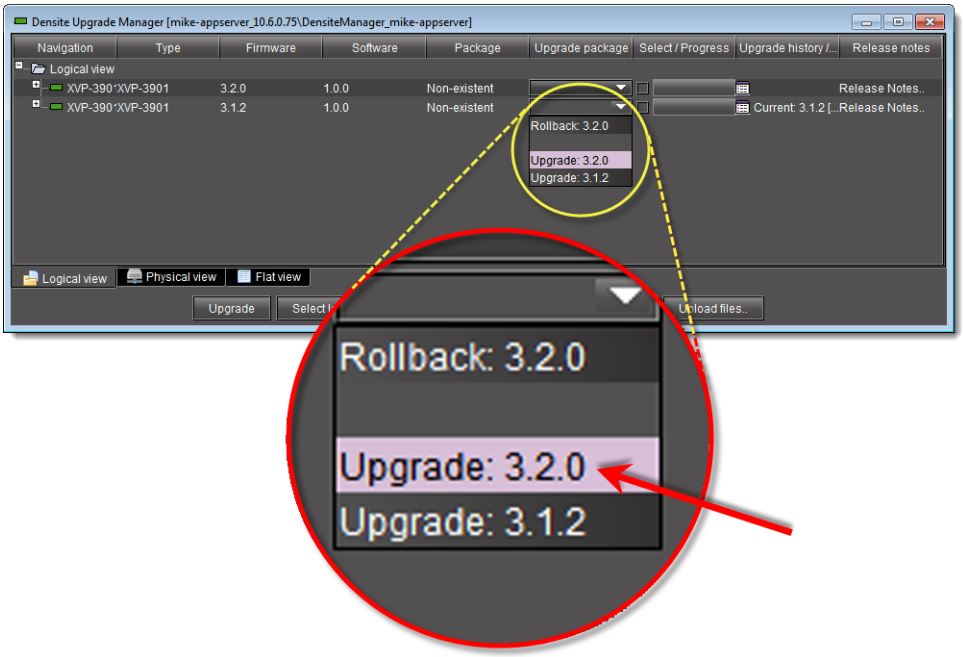
3. Click **Upload**.



4. Click **Close** to close the window.



5. In the **Upgrade package** column of **Densité Upgrade Manager**, verify that the new upgrade package is present.



Note: In order to see the newly uploaded package in the **Available package** column, you must make sure you are reading from a row corresponding to a Densité card compatible with the newly uploaded package firmware and software (i.e. If you uploaded an XVP-3901 package, check the available packages in a row corresponding to an XVP card.)

Viewing a Densité Card's Installed Firmware and Installed Software Versions

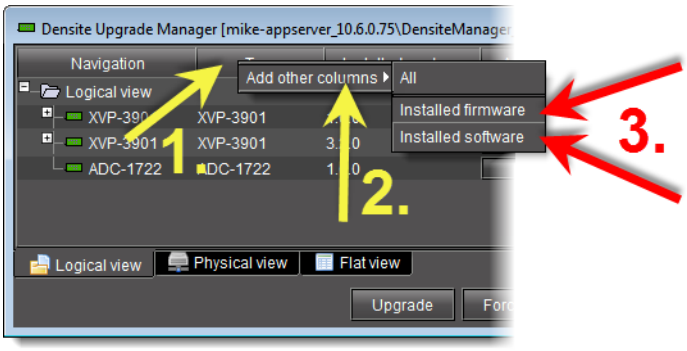
You may decide to make the installed firmware and installed software versions of your Densité cards visible in **Densité Upgrade Manager**. This may be desired, for example, if you would like to see more clearly if a package upgrade resulted in an installation of its firmware as well.

REQUIREMENT

Before beginning this procedure, make sure you have opened **Densité Upgrade Manager** (see page 709).

To view a card's firmware and software versions

1. In **Densité Upgrade Manager**, right-click anywhere in the header row, point to **Add other columns**, and then select either **Installed firmware** or **Installed software**.



2. Perform the action of step 1 again, this time selecting whichever of **Installed firmware** or **Installed software** you *did not* select before.

6 Access Control

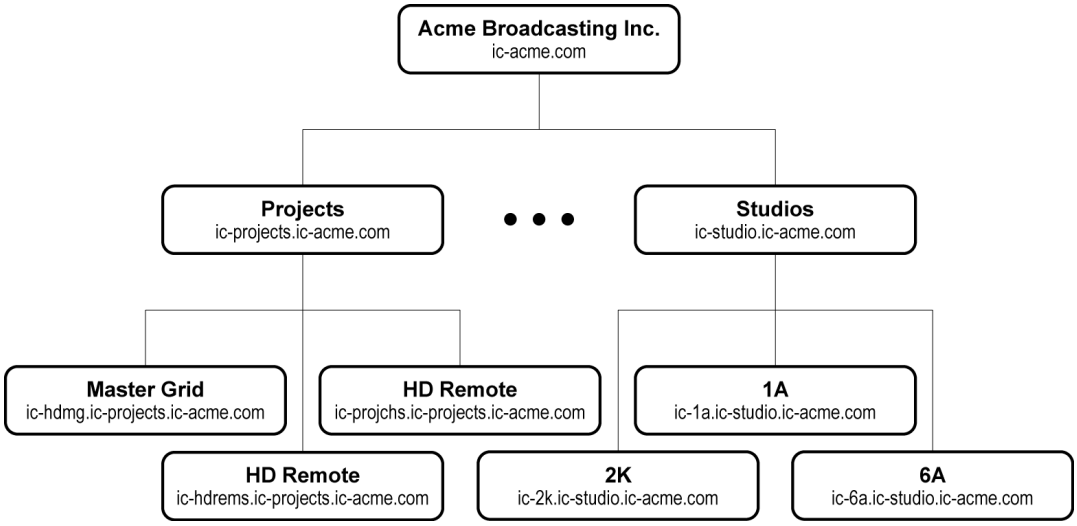
Summary

Overview

As shipped, an Application Server can be used by any user on the same network to open any program, view any pages, modify any device parameters, and so on. Access control, also called *user authentication* or *privilege management*, allows you to make iControl system resources (such as cards, services, and Web pages) available only to designated users.

While not meant to be a foolproof security system, access control allows you to manage users in a way that minimizes the potential for errors. For example, you can prevent a guest user from opening critical Web pages. Access control also associates user names with events, so that you can see, for example, who acknowledged a specific alarm or reset a latch.

A typical iControl configuration consists of multiple rooms, areas or groups for processing and distributing content. Each room/area/group has its own hardware equipment including Grass Valley Densité and Imaging (Symphonie/Quartet) cards and various third-party equipment. Each room/area/group also has its own private local area network (LAN). It is convenient to map these rooms to iControl domains for security considerations. The figure below illustrates a typical domain architecture.



iControl provides multiple domain- and role-based authentication based on the Lightweight Directory Access Protocol (LDAP). In a typical system, each domain has one LDAP server (i.e., LDAP running as a service on an iControl Application Server), and manages its own accounts with top down referrals. In such a configuration, users from a higher level domain can log in to a lower level one. For example, in the architecture shown above, users from the `ic-projects.ic-acme.com` or `ic-acme.com` domains can log in directly to `ic-hdmg.ic-projects.ic-acme.com`.

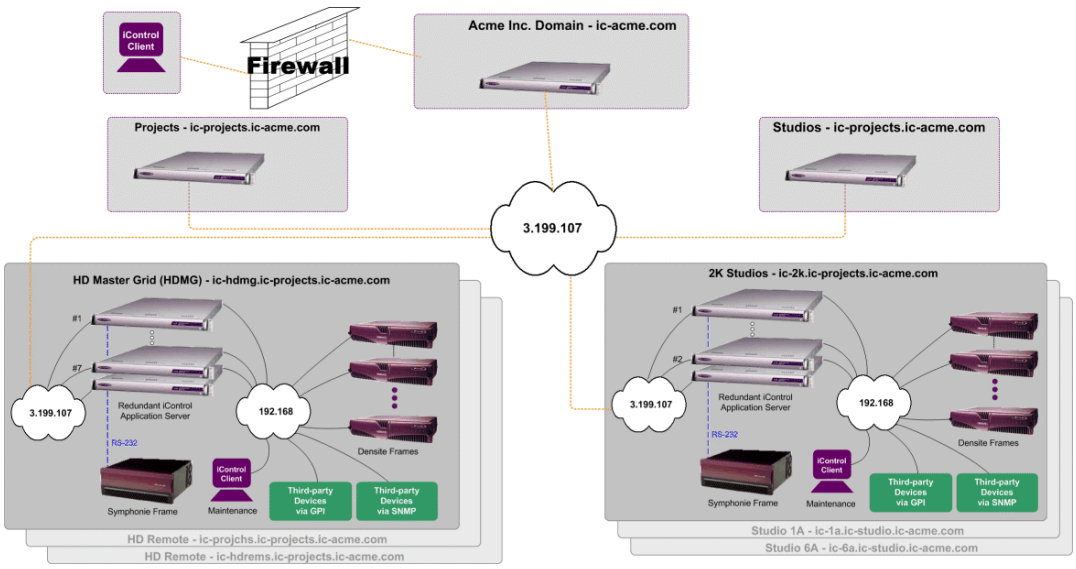
Users from a higher level domain log in to a lower level one with *role inheritance*. For example, a user registered as an *operator* at the top level `ic-acme.com` could log in to `ic-projects.ic-acme.com` as an *operator*, but would inherit the permissions from the *operator* role in the lower-level domain.

Each domain has a default user defined—the *admin* user. This user has the role of *super* assigned to it, which means that anyone who logs in as *admin* has access to everything in the domain. The default *admin* user has a default password, which is also `admin`. This password can be changed. You might want to do this to improve security. The *admin* user profile can also be restored to its original state if accidentally deleted. For more information about resetting the *admin* user profile, see Resetting a Domain's Admin User Account, on page 337.

Sample Network Topology

The figure below illustrates a general network topology with some sample domains. All domains are configured with their own private local LAN (192.168) connected to a second iControl Application Server NIC (**eth1**). A client PC is configured on the LAN for maintenance engineers to configure and control equipment in the room. All equipment in the room is also configured on the local LAN for private access. External PCs on the public network cannot access any equipment directly.

Each room has one or more iControl Application Server(s), depending on the amount of equipment to monitor and control. The Application Servers within each room are connected to the same local LAN (`192.168`). The primary NIC (**eth0**) is configured for the public subnet (`3.199.107`). This is the only subnet available to connect all Application Servers from all rooms to the public LAN. PC clients can be connected on the public subnet, but typically monitoring and control will be from PCs on the corporate LAN behind the firewall as shown.



Single Sign-on and External Integration

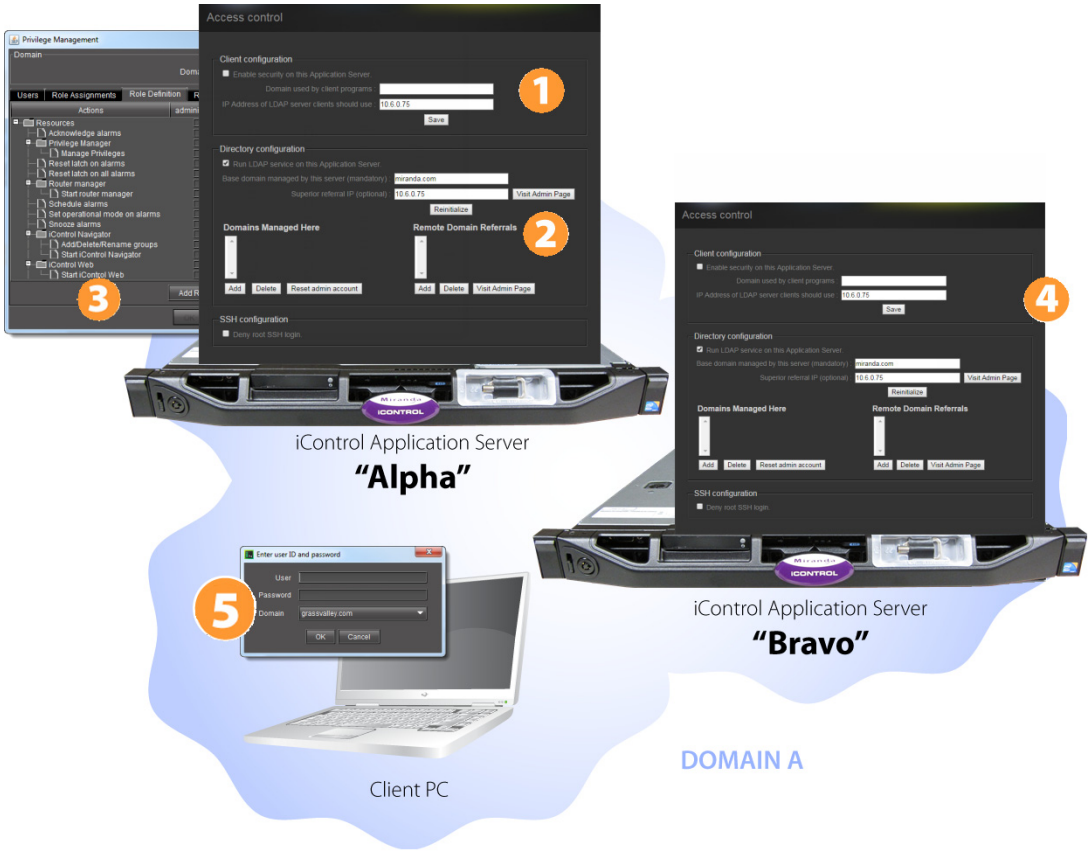
The iControl architecture is open and uses standard schemes, allowing integration with existing security infrastructures. iControl supports integration with existing directory services using standard schemes for authentication. The system can be configured to use an external LDAP server or directory services server instead of using the iControl LDAP server.

It is also possible to use multiple LDAP servers with referral capabilities. For example, iControl can bind and authenticate with an external LDAP server, but manage its permissions on the iControl LDAP server for iControl-specific resources. Referrals are supported between LDAP databases to support multiple domain authentication.

In the case where it is not possible to get direct access to directory services, iControl can be integrated with an existing enterprise "single sign-on" system. For example, iControl interfaces with Microsoft *Active Directory,* or with *Netegrity SiteMinder* from Computer Associates, to authenticate users.

Setting up Access Control

The figure below depicts a simple scenario — a single domain with two iControl Application Servers.



Here are the steps you would follow to set up Access Control in this scenario, along with references to the associated procedures in this chapter:

To set up Access Control in the preceding example

1. **Activate LDAP service** — Open the *Access control* page (see page 682) of an Application Server (e.g., *Alpha*) to set up and activate an LDAP service, including building a list of managed domains and remote domain referrals (if any) (see page 311).
2. **Enable access control** — Enable access control on *Alpha* (see page 317).
3. **Configure users, roles, and permissions** — Open **iC Navigator** from *Alpha*, and then use the **Privilege Management** window to create users, assign roles (e.g., *operator*, *admin*), and assign permissions (e.g., ability to open a control panel). Then open **iC Creator** and use the **Page Privilege Management** window to assign Web-based permissions (e.g., ability to open a Web site).

   See:

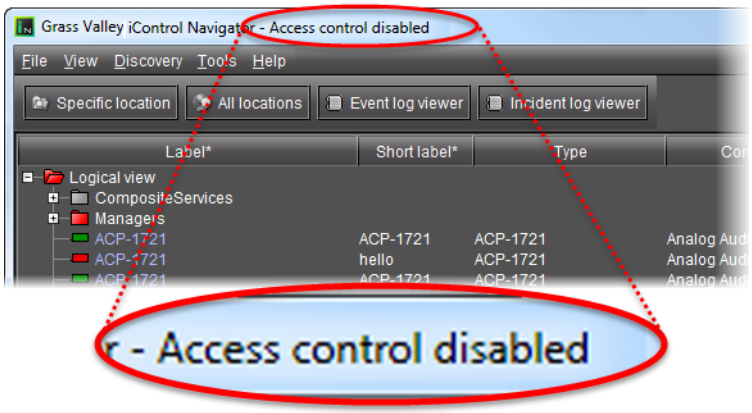
   - Opening the Privilege Management Window on page 709
   - Opening the Pages Privilege Management Window on page 727
4. **Configure other Application Servers** — Open the *Access control* page of other Application Servers in the same domain (e.g., *Bravo*) to enable access control and to point to the LDAP service running on *Alpha*.

5. **Client login** — When a user opens an application (e.g., **iC Navigator**, **iC Web**) from *Alpha* or *Bravo*, he/she must log in to begin an iControl session. From that point on, their ability to perform various operations will depend upon what role they have been assigned (and how that role was configured).

Key Concepts

Access Control

Users can open any application (e.g., iC Navigator) from an Application Server on which access control has **not** been enabled. In such cases, the message **Access control disabled** appears in the title bar of the application window.



Enabling access control on an Application Server causes its applications and services to require users to log in, and to enforce role assignments and permissions. See Enabling Access Control on page 317, and Enabling Active Directory Single Sign-on on page 317.

LDAP

iControl Access Control employs the Lightweight Directory Access Protocol (LDAP) for user authentication. LDAP is an application protocol for searching and editing directories.

A directory is a database containing similar "objects" organized hierarchically. An LDAP directory is similar to a telephone book, where entries consisting of names, addresses, and phone numbers are organized into higher level groups. In an LDAP directory, the topmost level corresponds to a *domain* (e.g., `myCompany.com`).

Domains

Access control in iControl makes use of the concept of *domains*. A domain is a logical grouping of users, resources and applications.

Domains are specified using dot notation (e.g., `myCompany.com`), and are hierarchical—there is typically one top level domain for a company, with several lower level domains organized in some pattern. For example, a company might have `myCompany.com` as the top level domain,

and then one lower level domain per city (e.g., `montreal.myCompany`, `toronto.myCompany`).

- every iControl resource is located in a domain
- every iControl client application (e.g., iC Navigator) is opened from a domain
- every server process is run within a domain
- a domain can contain more than one iControl Application Server
- a domain is also considered a resource
- a domain contains higher level permissions such as *startNavigator*, *manageUsers*, etc.

Resources

A resource is any device (e.g., a Densité card), service (e.g., Densité Manager) or Web object (e.g., a Web page) that can have a permission assigned to it. It is defined by three elements: a unique ID, a resource type, and a domain. Some examples are given in the table below:

Resource	Unique ID	Type	Domain
Densité card	`dev4.icontrol.com_H_Densité_SLOT_1_31`	DEC-1002	`myCompany.com`
Web page	`http://10.2.0.251/icw/sites/SkyAssure2.0.0.0_0007/Web_pages/home.mpf`	webpage	`myCompany.com`

Templates

Each time you add a new resource (card or service), it will obtain a set of default permissions from a template stored in the LDAP directory. The template is created automatically the first time you add a new card or service, and can be modified in the **Resource Assignment** panel of the **Privilege Management** window (see Assigning Resources, on page 333).

Templates are particularly useful for cards, allowing you to define the basic permissions for all roles for a certain card type. As new cards (of the same type) are added, they copy the permission set.

Users

iControl distinguishes between the user profiles used to log in to client-side applications (like **iC Navigator**, **iC Creator**, etc.) and user profiles used to log in to the Application Server itself (through a secure shell or the server's Web client pages).

User Profile Management for Client-Side Applications

For client-side operations, iControl offers access control based on individual user credentials and the role assigned to that user.

A user is an individual registered in iControl, usually attached to a single domain. A user is designated by a UID, followed by the @ symbol, followed by a domain (e.g., `joeuser@montreal.myCompany`).

A user can access resources in his/her own domain or any domain below on the condition that permission is given to that user at the domain level. To access a domain, the user has to be authenticated by providing a password.

See also

For more information about creating, editing, and deleting user profiles for *client-side* applications, see Creating, Modifying, and Removing Users (Client-Side Applications), on page 325.

User Profile Management for Application Server Administration

For Application Server administration, if you log in to *iControl admin* using credentials associated with the *super* role, you can change the passwords associated with the two default user profiles for server-side operations. Additionally, you can import lists of user profiles, from CSV files, or export your Application Server's current user profiles to a CSV file. For added server-side security, administrators may decide to deny ***root*** user profile login over a secure shell (SSH). You can accomplish this on the *Access control* page of your Application Server.

The set of tasks available from *iControl admin* depends on the current user's role.

Role	Default credentials	Description
Super	User: `admin` Password: `icontrol`	Has access to everything.
Administrator	User: `miranda` Password: `icontrol`	Cannot change the password associated with the predefined users *admin* and *miranda*. Cannot export or import user profiles. These access control features are only available to super users.
Operator	User: `user` Password: `icontrol`	Does not have access to the *Access control* page. Cannot upgrade/downgrade iControl. Can back up and restore the system.

Note: The default *iControl admin* users (*admin, miranda,* and *user*), and any additional users you might have imported from a CSV file, do not have access to LDAP or Active Directory sub-domains, and should not be used to access client-side applications when LDAP is enabled. In such cases, use the domain-specific default user *admin* (default password: `admin`) or an LDAP (or AD) user with the adequate permissions.

See also

For more information about:

- Exporting user profiles to a spreadsheet, see page 336.
- Importing user profiles from a file, see page 337.
- Resetting a Domain's Admin User Account, see page 337.
- Allowing or denying ***root*** SSH login on the Application Server, see page 338

Actions

Actions are used to define what can be done on a resource that requires access control. Typically every resource type will have a set of possible actions assigned to it. For example, there are two actions that can be associated with a Web page: *edit* and *delete*.

It is important to distinguish between actions that apply to particular resources and actions that are more general. For example, the *editGroups* action does not apply to a particular group, but refers to the capability of a user to edit all groups. For that reason its resource type is *domain*. On the other hand, the *viewWebPage* action can be applied to a specific Web page, so its resource type is *Webpage*.

Currently, actions are assigned in either **iC Navigator** or **iC Creator** (see Assigning Resources, on page 333).

The table below lists actions that can be used to assign permissions. The *user readable name* is what is visible on screen, as are the *action categories*, which correspond to folders:

Action Category	Action Name	User Readable Name	Description
--- ***The following actions are available within iC Navigator*** ---			
Resource	acknowledgeAlarms	Acknowledge alarms	Ability to acknowledge any alarm
	resetLatchAlarms	Reset latch on alarms	Ability to perform a reset latch on a alarm
	resetLatchAllAlarms	Reset latch on all alarms	Ability to perform a reset latch command on all alarms
	setOperationalModeAlarms	Set operational mode on alarms	Ability to place an alarm in operational mode
	scheduleAlarms	Schedule alarms	Ability to schedule alarms
	snoozeAlarms	Snooze alarms	Ability to snooze alarms
iC Navigator	editGroups	Add/Delete/Rename groups	Ability to manipulate folders and group views
	startNavigator	Start iControl Navigator	Ability to log in to **iC Navigator**
iC Web	startiControlWeb	Start iControl Web	Ability to log in to **iC Web**
iC Creator	startCreator	Start iControl Web Creator	Ability to log in to **iC Creator**
Privilege Manager	managePrivileges	Manage privileges	Ability to access the application-specific privilege management system.
Resource assignment tab	openControlPanel	Open control panel	Ability to open the control panel of a service. This is managed on a per service basis.
--- ***The following actions are available within iC Creator*** ---			

(*Continued*)

Action Category	Action Name	User Readable Name	Description
Web sites (site name)	openWebsite	Open Web site	Ability to open a Web site in **iC Web** or **iC Creator**
	publishWebsite	Publish Web site	Ability to publish a local site to an Application Server (remote) site
	deleteWebsite	Delete Web site	Ability to delete a site from an Application Server (remote)
Web pages (page name)	openWebpage	Open Web page	Ability to open a Web page in **iC Web** or **iC Creator**. User must also have view access on the Web site to view Web page.
	deleteWebpage	Delete Web page	Ability to delete a page from a site
Widgets (widget name)	openWidgetpage	Edit widget	Ability to open a widget in **iC Web** or **iC Creator**
	deleteWidgetpage	Delete widget	Ability to delete a widget from a site

Permissions

A permission is an association between an action and a *resource* in a specific *domain*, for example:

view control panel for `dev4.icontrol.com_H_Densité_SLOT_1_31` of type *SCP-112* in `toronto.myCompany`

If a user is given a permission (see note below), then he or she can perform the action on the specified resource, in the specified domain.

> **Note:** Permissions are not assigned directly to users. They are assigned to roles that are, in turn, assigned to users.

Roles

Roles are a mechanism for describing groups of users, with names that typically reflect real world job descriptions, such as *administrator*, *operator*, or *maintenance*. A set of permissions is associated with each role, which can then be assigned to one or more users. For example, the *guest* role in the `toronto.myCompany` domain could have this set of permissions:

Resource Type	Resource Name	Resource Domain	Action
Domain	`toronto.myCompany`	`toronto.myCompany`	startNavigator
SCP-1121	`dev4.icontrol.com_H_Densité_SLOT_1_31`	`toronto.myCompany`	openControlPanel
Website	`http://10.2.0.251/icw/sites/SkyAssure`	`toronto.myCompany`	openWebsite

Notice that all resources in this example are located in `toronto.myCompany`. A role in a given domain can only give permissions for resources in its domain.

> **Note:** A user cannot have different roles in different domains. For example, `joeuser@myCompany` with the administrator role in the *myCompany* domain could not be given an operator role in the `montreal.myCompany` domain.

Roles are usually defined and assigned by an administrator, although there are special roles that exist by default. A user with no assigned role (no permission) in a domain cannot do anything with resources under access control. A special role (*super*) exists in every domain — a super user has permission to do everything in his/her domain. Permissions are given to users based on their roles and domains as defined by the security administrator.

Roles can be created, deleted, and customized. A typical set of roles could be defined as follows:

Role	Description
Super	Access to all resources, full administrative privileges, plus ability to change the password for the two predefined *iControl admin* users (the super user *admin,* and the default administrator *miranda*).
Administrator	Full access to all resources plus administrative privileges. For example, an administrator can create accounts and assign permissions for roles.
Maintenance	Access to all resources but no administrative privileges. For example, maintenance personnel can change hardware configurations and settings but cannot modify user privileges or create accounts.
Operator	Limited to operational tasks only. For example, an operator may not be able to change hardware settings.
Guest	Limited to very specific applications and views. Cannot change anything.
IT	Limited to IT tasks, NMS type monitoring of servers including iControl Application Server health monitoring.

Role Inheritance

Each domain maintains associations between users and roles, and implements role inheritance. Role inheritance means that there is no explicit role for a given user in a domain, the role this user has in the superior domain (if any) will be used.

For example, if `joe@myCompany.com` has the role *operator* in `myCompany.com`, then `joe@myCompany.com` will have role *operator* in domain `montreal.myCompany.com` also.

Access Control Page

The *Access control* page is used to enable or disable access control on an Application Server, to set up directory (LDAP, Active Directory) services, to download logs, as well as to allow or deny root SSH login to the Application Server. This is also where *super* users can change the password for the two predefined *iControl admin* users (the super user *admin,* and the default administrator *miranda*). See Managing Users for Server-Side Operations on page 336.

Client Configuration

The **Client configuration** section is used to define information required by Application Servers to enable access control. Client applications (**iC Navigator**, **iC Creator**, etc.) and services (GSM, Densité Manager, etc.) will use the information entered here to know which domain they run in, and where to go to access an LDAP server.

LDAP Configuration

The **LDAP configuration** section is used to define information required by Application Servers that will be running an LDAP service. See Configuring LDAP on an Application Server on page 311.

External Active Directory Configuration

The **External Active Directory configuration** section is used to define information required to allow single sign-on to the Application Server. See Enabling Active Directory Single Sign-on on page 317.

Detailed Directions

Configuring LDAP on an Application Server

The way in which you configure LDAP depends upon your network configuration. The procedures below describe how to configure LDAP in single and multiple domain networks.

Configuring the LDAP Service on an iControl Application Server for a Single Domain

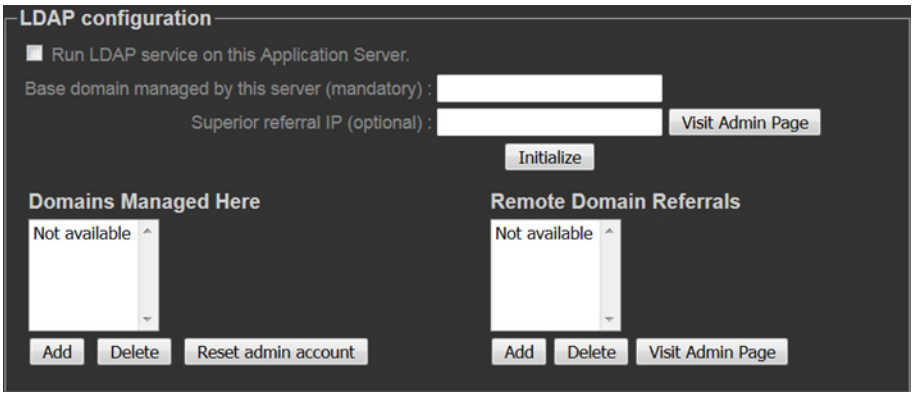
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened the *Access control* page (see page 682).
- You have read Rules for Local Domains on page 316.

To configure the LDAP service on an iControl Application Server for a single (local) domain

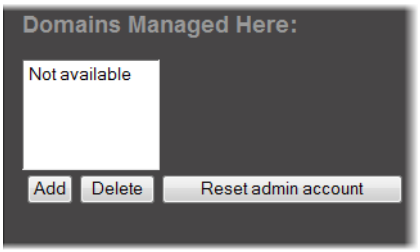
1. On the *Access control* page, in the **Base Domain managed by this server** field, type the name of the domain (e.g., `toronto.myCompany.com`) that this Application Server will manage.



2. Leave the **Superior referral IP** field empty.
3. Click **Initialize**.

> **Note:** If this Application Server has previously been used to run an LDAP service, the button will be labelled **Reinitialize**.

4. Select the **Run LDAP service on this Application Server** check box.
   As the LDAP service starts up, the *iControl admin* page reloads.
5. In the **Domains Managed Here** area, click **Add**.



   SYSTEM RESPONSE: A window appears, prompting you to type a domain name.
6. Type the local domain name, and then click **OK**.
   SYSTEM RESPONSE: The newly added local domain appears in the list under **Domains Managed Here**.
   At this point, the LDAP service is running on the Application Server, and configured for a single domain.

Configuring the LDAP Service on an iControl Application Server for Multiple Domains

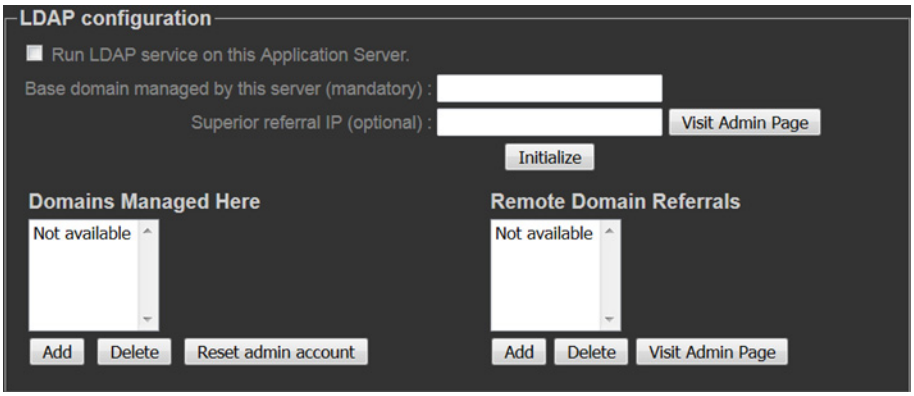
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened the *Access control* page (see page 682).
- You have read Rules for Local Domains on page 316.
- You have the illustration Sample Multi-Domain Setup on page 315 available as a reference.

To configure the LDAP service on an iControl Application Server for multiple domains

1. On the *Access control* page, in the **Base Domain managed by this server** field, type the name of the domain (e.g., `myCompany.com`) that this Application Server will manage.



2. Leave the **Superior referral IP** field empty.
3. Click **Initialize**.

> **Note:** If this Application Server has previously been used to run an LDAP service, the button will be labelled **Reinitialize**.

4. Select the **Run LDAP service on this Application Server** check box.

   System Response: As the LDAP service starts up, the *iControl admin* page reloads.

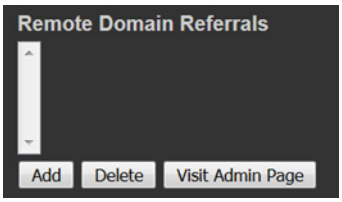
5. In the **Domains Managed Here** section, click **Add**.

   System Response: A window appears, prompting you to type a domain name.

6. Type the local domain name (`from`), and then click **OK**.

   System Response: The newly added local domain appears in the list under **Domains Managed Here**.

7. Repeat step 5 through step 6 as needed to add additional domains, which must be children of the local (base) domain (e.g., `montreal.myCompany.com`, `winnipeg.myCompany.com`, etc.).
8. In the **Remote Domain Referrals** section, click **Add**.



SYSTEM RESPONSE: A window appears, prompting you to type a referral domain.

> **Note:** You should add a referral domain if you want a user to be able to have access to resources in the remote domain.

9. Type the referral domain name followed by the IP address of the LDAP server (i.e., Application Server) that manages that domain (e.g., `ottawa.myCompany.com 10.10.20.10`), and then click **OK**.

   SYSTEM RESPONSE: The newly added local domain appears in the list under **Remote Domain Referrals**.

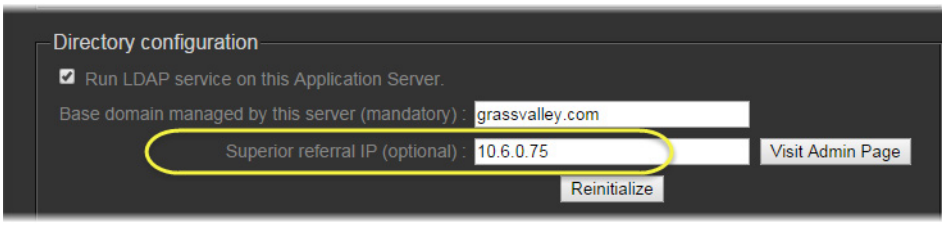
> **Note:** There is no need to add sub-domains (e.g., `operations.ottawa.myCompany.com`) since the referral to a domain implicitly refers to its children.

10. Select the new referral domain name in the list, and then click **Visit Admin Page**.

    SYSTEM RESPONSE: A new window or tab (from the referral server) appears in your Web browser.

11. In the **Base domain managed by this server** field, type the name of this referral server's domain (from).

12. In the **Superior referral IP** field, type the IP address of the Application Server you originally logged in to.



> **Note:** The **Superior referral IP** is used as an alternative when the LDAP server cannot resolve the distinguished name (DN) of an entry. The **Superior referral IP** should point to an LDAP server that will be able to resolve the DN, such as the LDAP server that manages the parent of the base domain.

13. Click **Initialize**.

Note: If this Application Server has previously been used to run an LDAP service, the button will be labelled **Reinitialize**.

14. Select the **Run LDAP service on this Application Server** check box.

    SYSTEM RESPONSE: As the LDAP service starts up, the *iControl admin* page reloads.

15. In the **Domains Managed Here** section, click **Add**.

    SYSTEM RESPONSE: A window appears, prompting you to type domain name.

16. Type the local domain name (from), and then click **OK**.

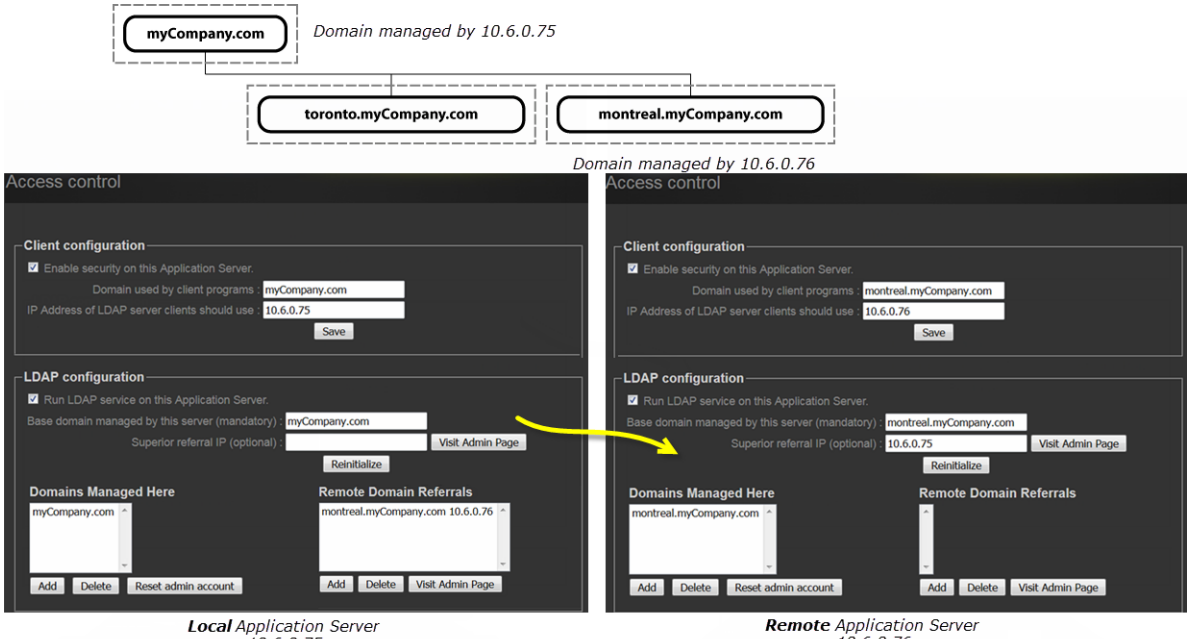
    SYSTEM RESPONSE: The newly added local domain appears in the list under **Domains Managed Here**.

17. Repeat as needed to add additional domains.

    At this point, the LDAP service is running and configured on both the local and the referral Application Servers. You should also enable Access Control on these servers if this has not already been done (see page 317).

Note: If you configured the LDAP service immediately after enabling Access Control on the Application Server, you must now restart iControl (see Starting & Stopping iControl Services, on page 678).

Sample Multi-Domain Setup



***Local** Application Server*
10.6.0.75

***Remote** Application Server*
10.6.0.76

An operator from a parent domain (e.g. *myCompany.com*) can log onto an application (e.g. *iC Web*) opened from this server, but will have the permissions associated with role ***Operator*** on 10.6.0.76. An operator from a sibling domain (e.g. *toronto.myCompany.com*) will be denied access.

Rules for Local Domains

- **One locally managed domain must be the base domain.**

  For example, the IP address `10.6.0.75` could have `grassvalley.com` as the base domain. It is also possible for the IP address `10.6.0.76` to have `Canada.Toronto.grassvalley.com` as the base domain.

- **All additional locally managed domains must relate to the base domain.**

  For example, the IP address `10.6.0.75` could have `grassvalley.com` as a base domain and the following other valid domains: `Canada.grassvalley.com`, `Toronto.grassvalley.com`, and `Canada.Toronto.grassvalley.com`.

- **All additional locally managed domains must relate to a base domain and existing subdomains.**

  For example, for IP address `10.6.0.75`, the additional locally managed domain *Toronto.Canada.grassvalley.com* requires that *Canada.grassvalley.com* and *Toronto.grassvalley.com* exist. with *grassvalley.com* as the base domain.

Rules for Remote Domains

- **Remotely managed domains must be the child of a locally managed domain.**

  For example, for IP address `10.6.0.75`, `Toronto.Canada.grassvalley.com` is the child of `Canada.grassvalley.com` which is also managed by IP address `10.6.0.75`.

Removing Domains

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened the *Access control* page (see page 682).
- You have read Rules for Local Domains on page 316.
- You have the illustration Sample Multi-Domain Setup on page 315 available as a reference.

To remove a domain

1. On the *Access control* page, select a domain in the list under **Domains Managed Here** or **Remote Domain Referrals**.
2. Click **Delete** (the **Delete** button corresponding to the list from which you are removing a domain).

   SYSTEM RESPONSE: The domain is removed from the list.

> **Note:** Removing a domain deletes all users and privilege settings associated with that domain (all of its LDAP entries are cleared).

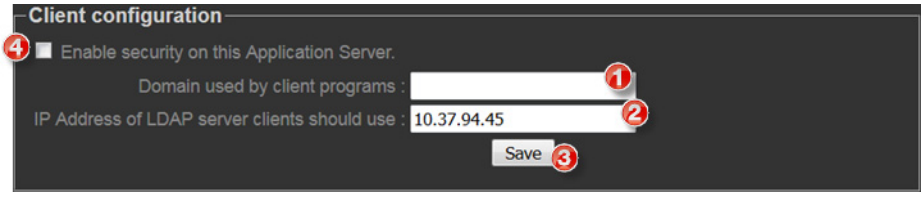
Enabling Access Control

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Access control* page (see page 682).

To enable access control on an iControl Application Server

1. On the *Access control* page, under **Client configuration**, in the field **Domain used by client programs**, type the name of the domain (e.g., `myCompany.com`) that is to be used by client applications and services opened from this Application Server.



2. In the field **IP Address of LDAP server clients should use**, type the IP address of the Application Server where the LDAP server is to be running.

   For a given Application Server, the LDAP server can be running either on the (local) Application Server itself, or on a remote machine. If the LDAP server is to run on the local machine, you must configure the LDAP service (see Configuring LDAP on an Application Server, on page 311).

3. Click **Save**.
4. Select the **Enable security on this Application Server** check box.

   A message appears advising you that you must restart iControl services in order for security (Access Control) to take effect.

5. Click **OK**.
6. Restart iControl (see Starting & Stopping iControl Services, on page 678).

Enabling Active Directory Single Sign-on

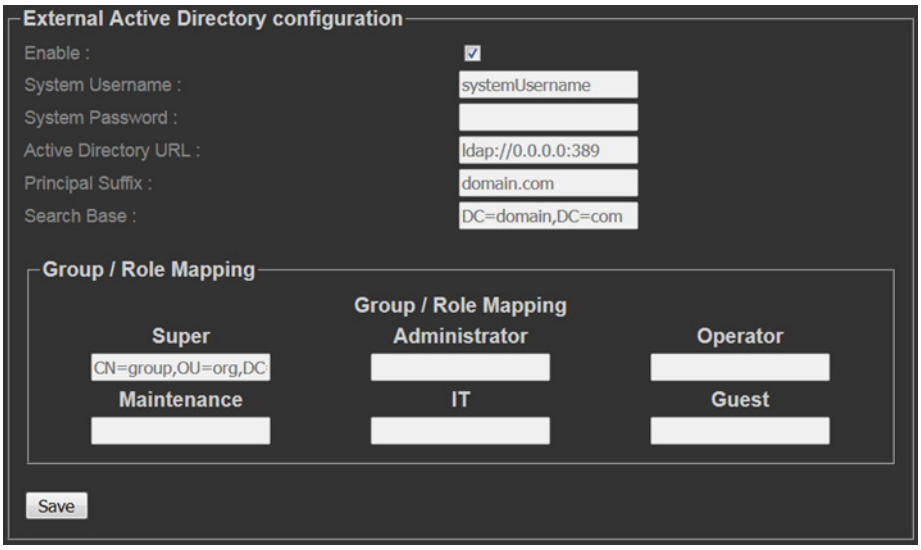
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have enabled security (see Enabling Access Control, on page 317).
- You have enabled the LDAP service (see Configuring LDAP on an Application Server, on page 311).
- You have opened the *Access control* page (see page 682).

To enable Active Directory single sign-on, on an iControl Application Server

1. On the *Access control* page, under **External Active Directory configuration**, select the **Enable** check box.



The related configuration fields become editable.

2. Type the required system credentials (i.e., the user name and password required for iControl to communicate with the Active Directory server), the Active Directory URL, principal suffix, and search base string.
3. Under **Group / Role Mapping**, define the mapping between the roles established in iControl (i.e., Super, Administrator, Operator, Maintenance, IT, Guest), and roles configured in Active Directory.
4. Click **Save**.

   The user profiles from Active Directory become available, and can be used to log in to client-side applications, and to iControl admin.

Viewing Current User Info

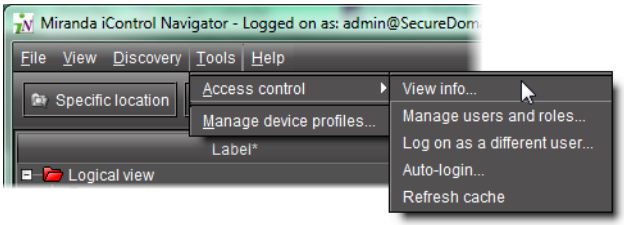
Viewing Information About a User Currently Logged in to iC Navigator

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Navigator** (see page 697).

To view information about a user currently logged in to iC Navigator

- In **iC Navigator**, on the **Tools** menu, point to **Access Control**, and then click **View Info**.



SYSTEM RESPONSE: The **Access Control Info** window appears, displaying the ID of the current user, as well as the subdomain to which that user belongs.

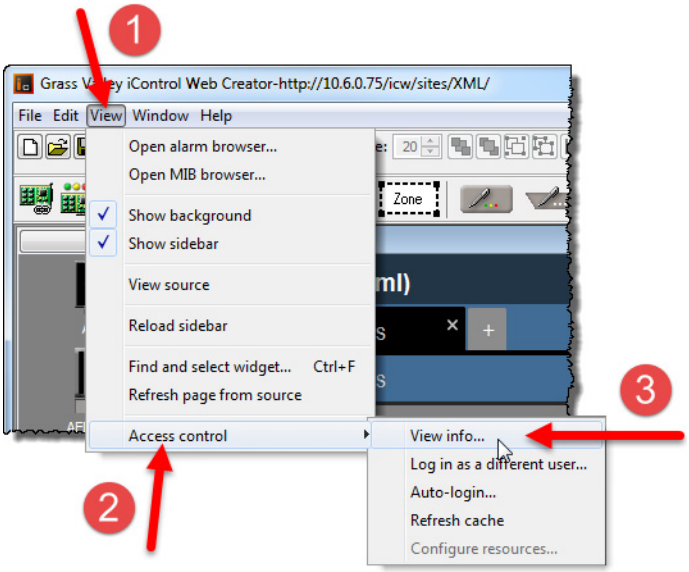
Viewing Information About a User Currently Logged in to iC Creator

REQUIREMENT

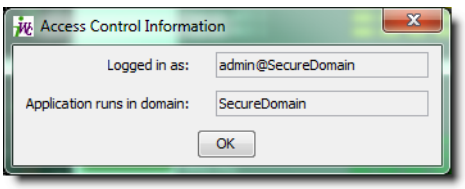
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To view information about a user currently logged in to iC Creator

- In **iC Creator**, on the **View** menu, point to **Access Control**, and then click **View info**.



SYSTEM RESPONSE: The **Access Control Info** window appears, displaying the ID of the current user, as well as the subdomain to which that user belongs.



Logging on as Different User

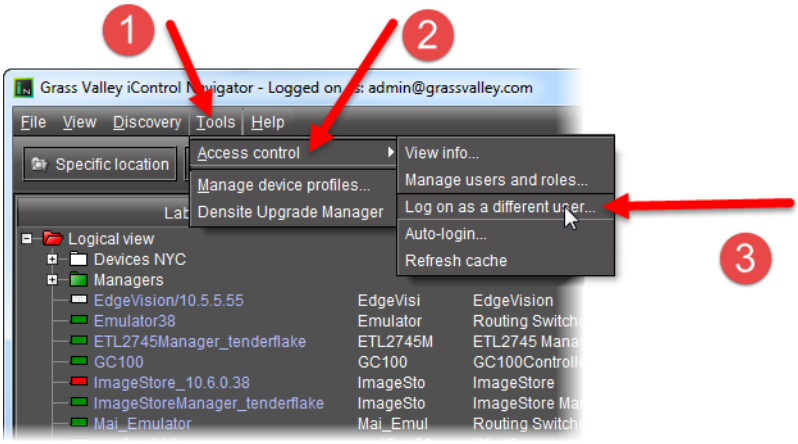
Logging on as a Different User in iC Navigator

REQUIREMENT

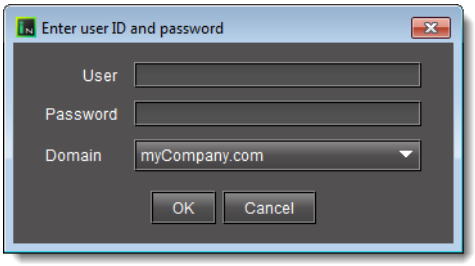
Before beginning this procedure, make sure you have opened **iC Navigator** (see page 697).

To log on as a different user in iC Navigator

1. In **iC Navigator**, on the **Tools** menu, point to **Access Control**, and then click **Log on as a different user**.



SYSTEM RESPONSE: The **Enter User ID and Password** window appears.



2. Type a user name and password in the fields provided.
3. In the **Domain** list, click the desired domain.
4. Click **OK**.

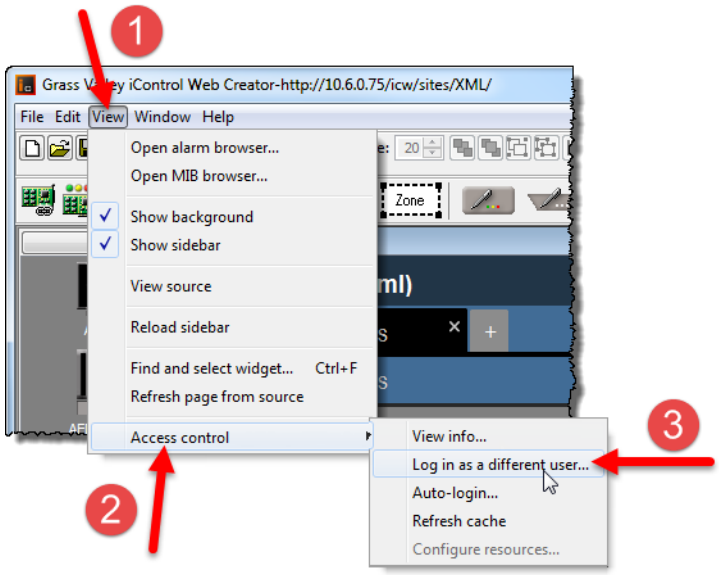
Logging on as a Different User in iC Creator

REQUIREMENT

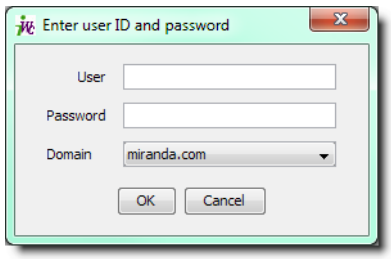
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To log on as a different user in iC Creator

1. In **iC Creator**, on the **View** menu, point to **Access Control**, and then click **Log in as a different user**.



SYSTEM RESPONSE: The **Enter User ID and Password** window appears.



2. Type a user name and password in the fields provided.
3. Choose a domain from the **Domain** menu.
4. Click **OK**.

Logging in Automatically

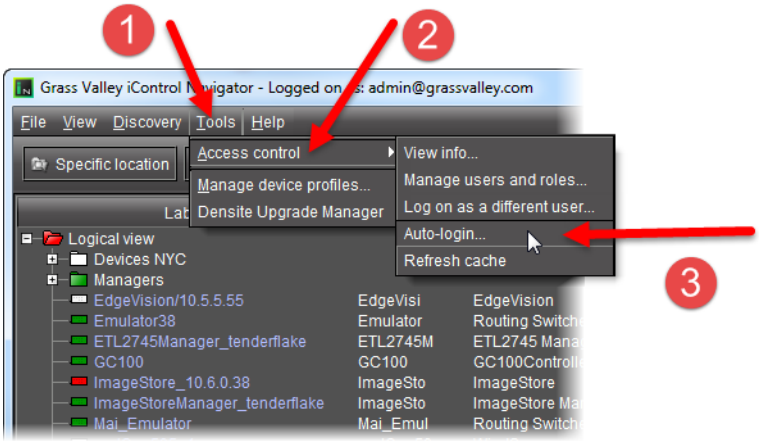
Configuring Auto-Login in iC Navigator

REQUIREMENT

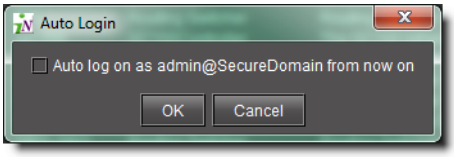
Before beginning this procedure, make sure you have opened **iC Navigator** (see page 697).

To configure auto login in iC Navigator

1. In **iC Navigator**, on the **Tools** menu, point to **Access Control**, and then click **Auto-login**.



SYSTEM RESPONSE: The **Auto Login** window appears.



2. Select **Autologin as <current user> at next startup**.
3. Click **OK**.

   SYSTEM RESPONSE: The current user will automatically be logged in next time **iC Navigator** opens (the **Enter User ID and Password** window will no longer appear).

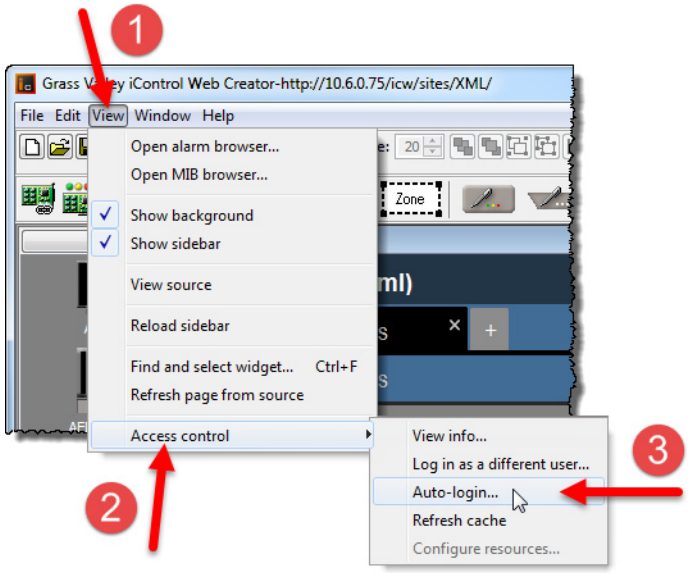
Configuring Auto-Login in iC Creator

REQUIREMENT

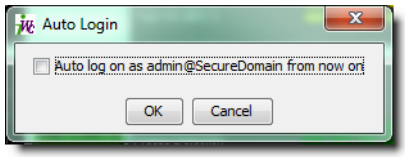
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To configure auto login in iC Creator

1. In **iC Creator**, on the **View** menu, point to **Access Control**, and then click **Auto-login**.



SYSTEM RESPONSE: The **Auto Login** window appears.



2. Select **Autologin as <current user> at next startup**.
3. Click **OK**.

   SYSTEM RESPONSE: The current user will automatically be logged in next time **iC Creator** opens (the **Enter User ID and Password** window will no longer appear).

Refreshing the Cache

When a client application (e.g., **iC Navigator**) is opened from an Application Server, it reads the current access control settings from the LDAP service on its Application Server, and keeps those settings in a local cache. Subsequent changes made to the LDAP settings (made, for example, by an administrator at another location) are only periodically sent to the client application. Refreshing the cache causes the client application to re-read the settings immediately from its LDAP server.

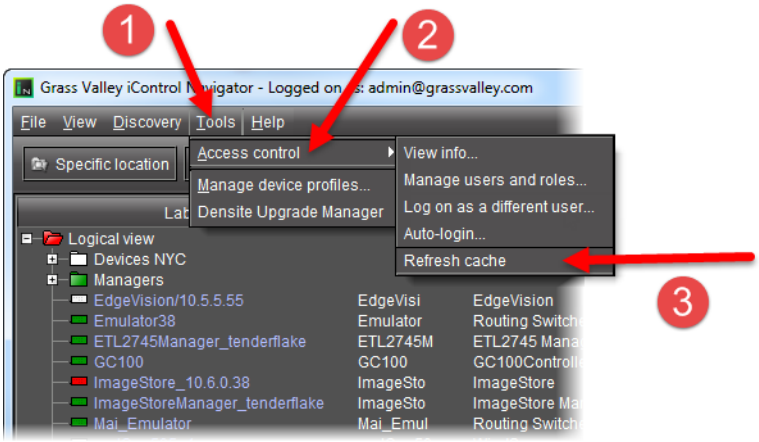
Refreshing the Cache in iC Navigator

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Navigator** (see page 697).

To refresh the cache in iC Navigator

- In **iC Navigator**, on the **Tools** menu, point to **Access control**, and then click **Refresh cache**.



SYSTEM RESPONSE: This causes **iC Navigator** to re-read the settings from its LDAP server.

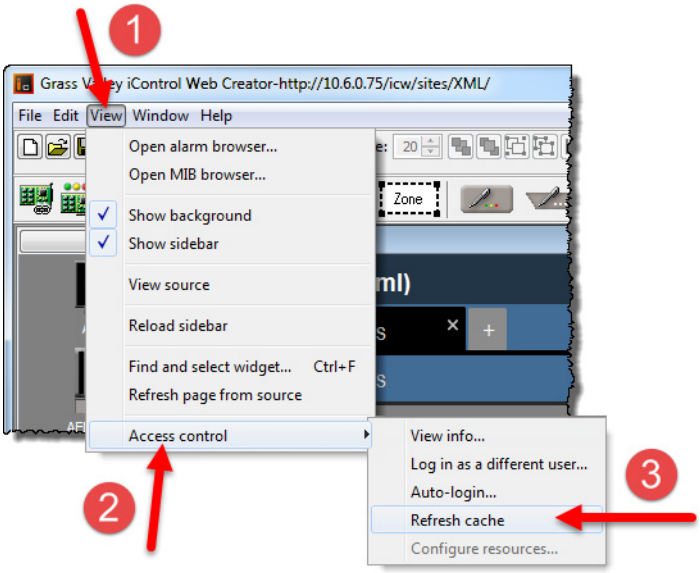
Refreshing the Cache in iC Creator

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To refresh the cache in iC Creator

- In **iC Creator**, on the **View** menu, point to **Access control**, and then click **Refresh cache**.



SYSTEM RESPONSE: This causes **iC Creator** to re-read the settings from its LDAP server.

Creating, Modifying, and Removing Users (Client-Side Applications)

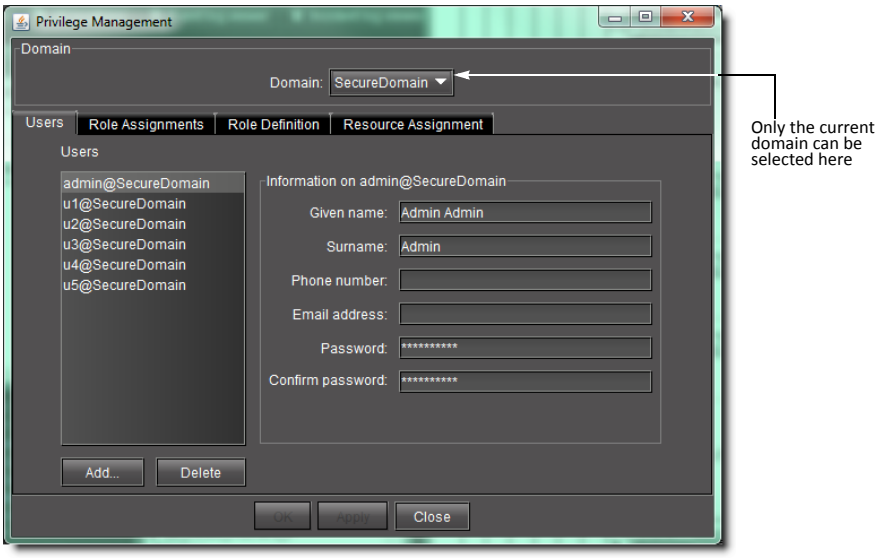
Creating a User

REQUIREMENT

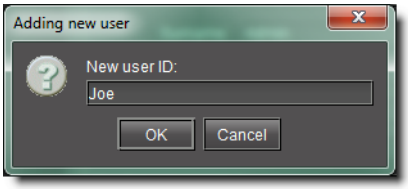
Before beginning this procedure, make sure you have opened the **Privilege Management** window (see page 709).

To create a user

1. On the *iControl admin* page, if necessary, click the **Users** tab to display the **Users** panel.



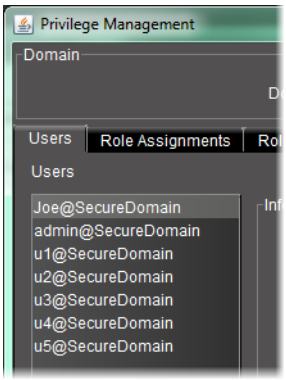
2. Click **Add**.
3. In the window that appears, type a name for the new user.



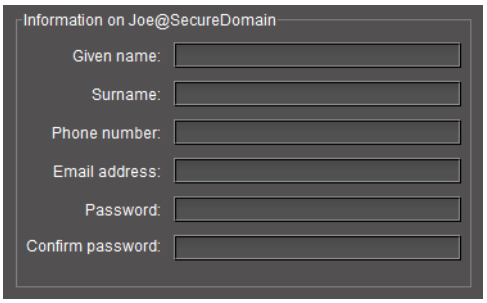
User names in iControl are case-sensitive, and may contain letters, numbers, periods and/or underscore characters, but not spaces. The @ symbol and current domain (e.g., `@myCompany.com`) are appended to the name automatically.

4. Click **OK**.

SYSTEM RESPONSE: The new name appears in the list on the left of the **Users** panel.



5. With the new user name highlighted, type a **Given Name** (first name), a **Surname** (family name), **Phone Number** (optional), and **Email Address** (optional) in the fields provided.



6. Type a password for this user, and the retype the password to confirm it.

Notes

- If a user has permission to manage privileges, he or she can change the password at any time.
- You may also elect to have a minimum length associated with passwords. To configure a minimum length, do the following:
  1. Use WinSCP (available from the *Useful downloads* link in iControl) to navigate to `/usr/local/iControl/www/java_generic.properties`.
  2. Change the setting of the `PrivilegeManager.minimumPasswordLength` property to the desired value.

By default, there is no minimum length.

7. Click **Apply** to save your changes and continue, or click **OK** to save the changes and close the **Privilege Management** window.

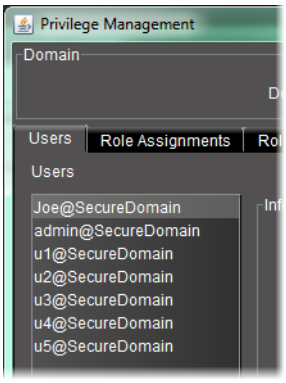
Modifying a User's Settings

REQUIREMENT

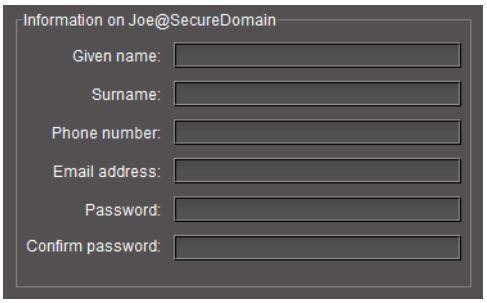
Before beginning this procedure, make sure you have opened the **Privilege Management** window (see page 709).

To modify a user's settings

1. In the **Privilege Management** window, if necessary, click the **Users** tab to display the **Users** panel.
2. Click on a user name in the list on the left of the **Users** panel.



3. With the user name highlighted, add or modify the **Given Name** (first name), **Surname** (family name), **Phone Number** (optional), and/or **Email Address** (optional) in the fields provided.



4. If you change the password for this user, retype the password to confirm it.

> **Note:** If the user has permission to manage privileges, he or she can change the password at any time.

5. Click Apply to save your changes and continue, or click **OK** to save the changes and close the **Privilege Management** window.

Removing a User

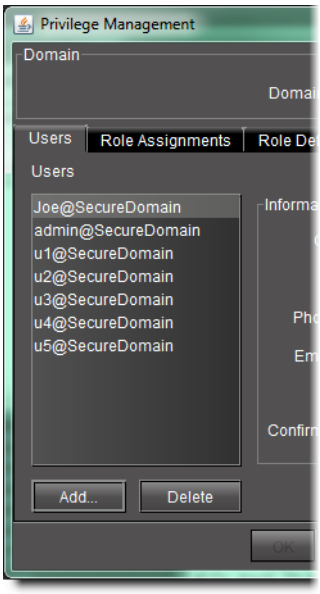
REQUIREMENT

Before beginning this procedure, make sure you have opened the **Privilege Management** window (see page 709).

To remove a user

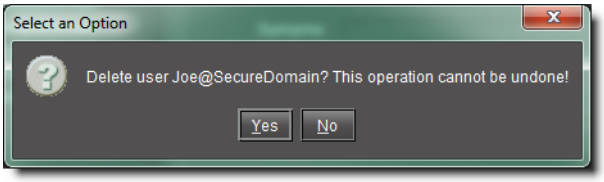
1. In the **Privilege Management** window, if necessary, click the **Users** tab to display the **Users** panel.

2. Click on a user name in the list on the left of the **Users** panel.



3. Click **Delete**.

   SYSTEM RESPONSE: A confirmation window appears.



4. Click **Yes** to permanently delete the user.

Assigning Roles

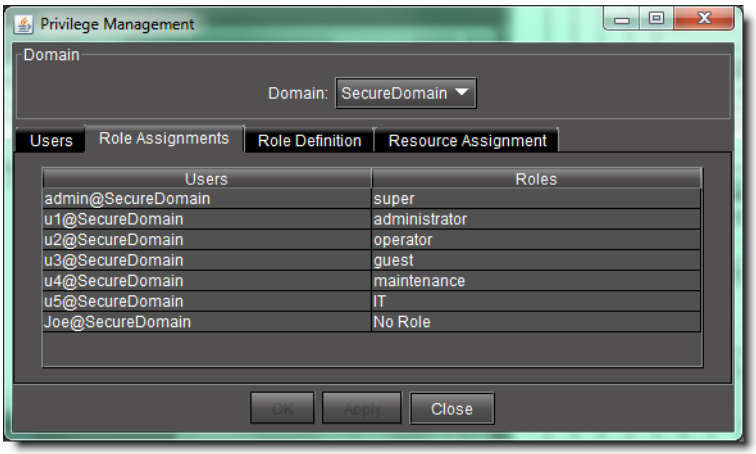
REQUIREMENT

Before beginning this procedure, make sure you have opened the **Privilege Management** window (see page 709).

To assign a role to a user

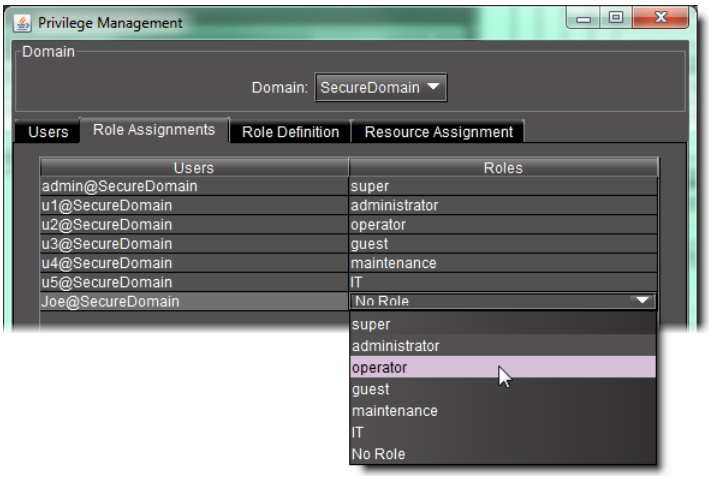
1. In the **Privilege Management** window, click the **Role Assignments** tab.

   SYSTEM RESPONSE: The **Role Assignments** panel appears.



Note: Currently, you can only manage users, roles and privileges for the domain of the Application Server from which you opened **iC Navigator**. The **Domain** drop down menu contains only the name of this local domain.

2. Click on a row in the **Roles** column and choose a role for the corresponding user.



Note: Permissions can be modified only for the roles of *administrator, operator, guest, maintenance,* and *IT* (see Defining Roles (Permissions), on page 330, below). The *super* role has all permissions. *No role* has no permissions. Currently, it is not possible to add a new role to the existing set.

3. Click **Apply** to save your changes and continue, or click **OK** to save the changes and close the **Privilege Management** window.

Defining Roles (Permissions)

Before assigning a role to a user or resources to a role, it may be necessary to modify permissions of an existing role or add a new role to the list of available roles. Additionally, you may also delete a role if desired.

IMPORTANT: Currently, you can only manage users, roles and privileges for the domain of the Application Server from which you opened **iC Navigator**. The Domain drop down menu contains only the name of this local domain.

Adding a New Role

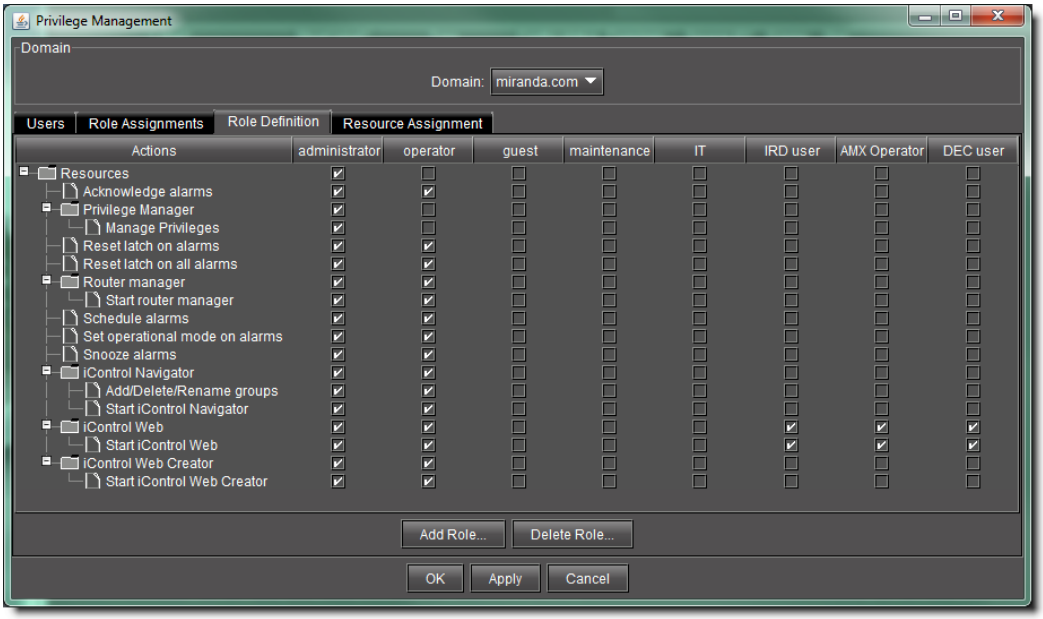
REQUIREMENT

Before beginning this procedure, make sure you have opened the **Privilege Management** window (see page 709).

To add a new role

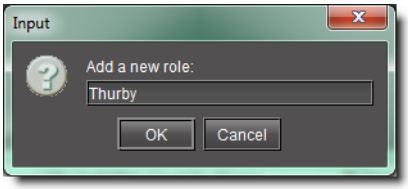
1. In the **Privilege Management** window, click the **Role Definition** tab.

   SYSTEM RESPONSE: The **Role Definition** panel appears.



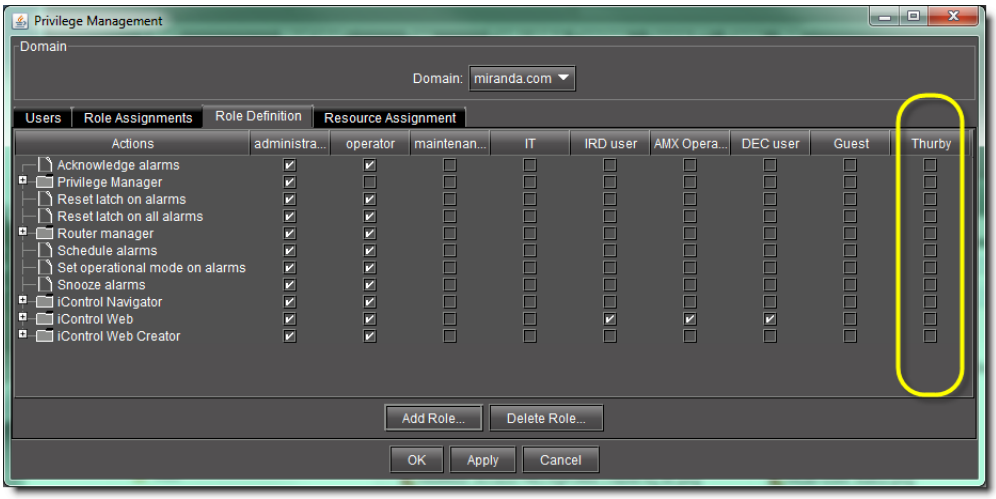
2. Click **Add Role**.

   SYSTEM RESPONSE: The **Input** window appears.



3. Type a new role name, and then click **OK**.

   SYSTEM RESPONSE: The new role appears in the **Privilege Management** window as a new check box column.



Deleting a Role

REQUIREMENT

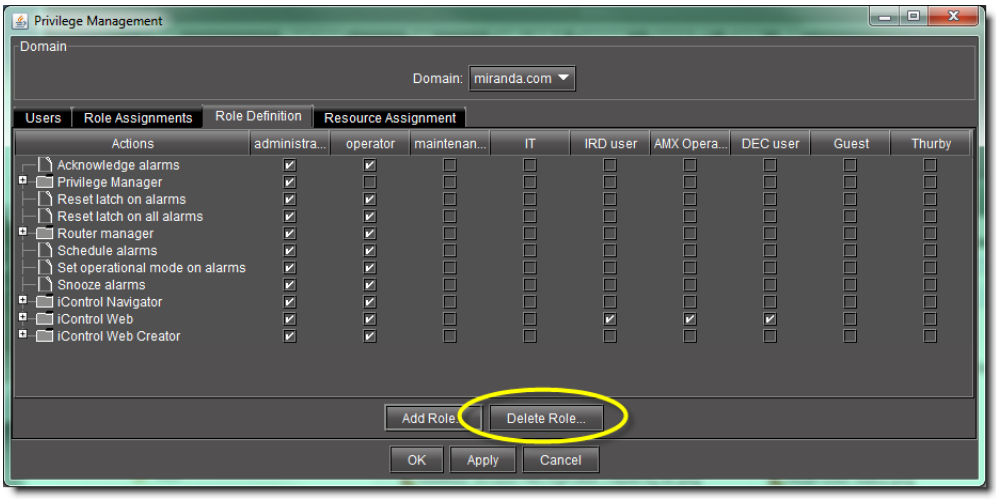
Before beginning this procedure, make sure you have opened the **Privilege Management** window (see page 709).

To delete a role

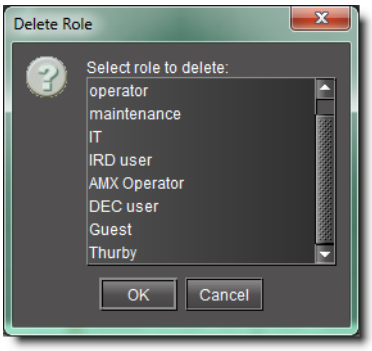
1. In the **Privilege Management** window, click the **Role Definition** tab.

   SYSTEM RESPONSE: The **Role Definition** panel appears.

2. Click **Delete Role**.



SYSTEM RESPONSE: The **Delete Role** window appears.



3. Select the role you would like to delete, and then click **OK**.

   SYSTEM RESPONSE: The role you deleted disappears from the **Role Definition** tab of the **Privilege Management** window.

   SYSTEM RESPONSE: If there are users currently assigned the role you are deleting, however, a **Cannot delete role** message appears. In this case, you must first assign a different role to this user.

Defining Permissions in a Role

REQUIREMENT

Before beginning this procedure, make sure you have opened the **Privilege Management** window (see page 709).

To define permissions in a role

1. In the **Privilege Management** window, click the **Role Definition** tab.

   SYSTEM RESPONSE: The **Role Definition** panel appears.

   Note: The *superuser* role always has all permissions.

2. In each role column, click to put a check mark in the row corresponding to a permission you wish to assign.

   Note: Click in the row corresponding to a folder to assign all of the folder's actions.

3. Click **Apply** to save your changes and continue, or click **OK** to save the changes and close the **Privilege Management** window.

Assigning Resources

Cards and services make themselves available as resources under access control when they first start up. For example, as a card inside a Densité frame boots, it starts a service on the GSM that checks to see if access control is enabled. If it is, then the card adds itself to the LDAP directory, and appears as a resource within the Privilege Management window.

Assigning Permissions to Cards and Services Based on Role Types

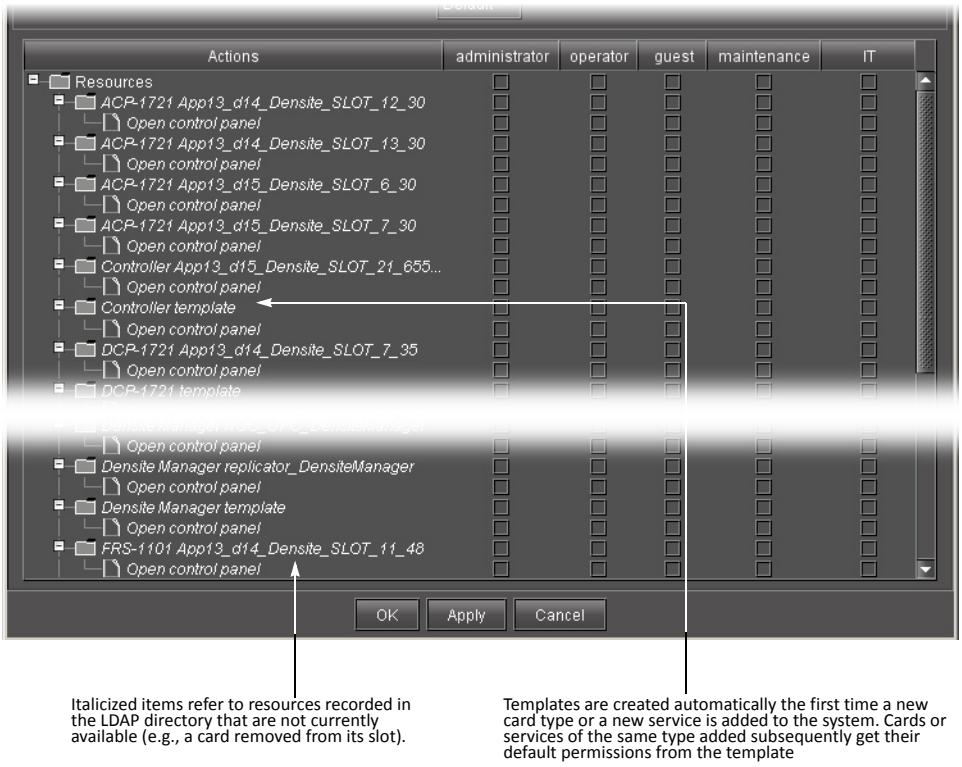
REQUIREMENT

Before beginning this procedure, make sure you have opened the **Privilege Management** window (see page 709).

To assign permissions to cards and services based on role types

1. In the **Privilege Management** window, click the **Resource Assignment** tab.

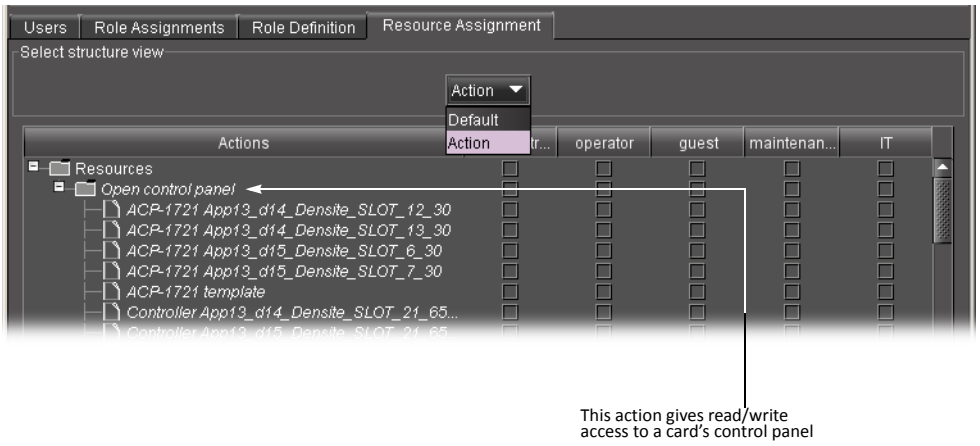
   SYSTEM RESPONSE: The **Resource Assignment** panel appears.



Note: Currently, you can only manage users, roles and privileges for the domain of the Application Server from which you opened **iC Navigator**. The **Domain** drop down menu contains only the name of this local domain.

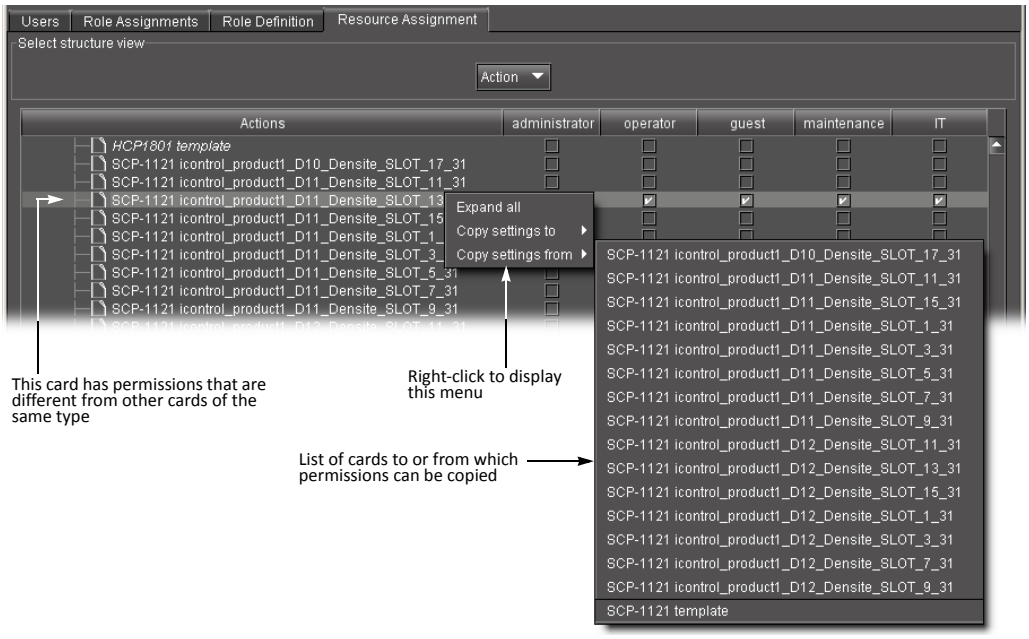
2. By default, resources (cards and services) are displayed in the same order in which they appear in **iC Navigator**'s main window. Each resource is represented by a folder containing

its associated actions. You can, if you prefer, change the display to show actions as folders containing resources. To do this, choose **Action** from the drop down menu under **Select structure view**.



Note: You should click **Apply** before choosing **Action**—check marks made but not applied will be lost.

3. In each role column, click to put a check mark in the row corresponding to a permission you wish to assign. Click in the row corresponding to a folder to assign all of the folder's actions.
4. To quickly copy settings to or from another resource, right-click on a resource and choose from the drop-down menu.



5. Click **Apply** to save your changes and continue, or click **OK** to save the changes and close the **Privilege Management** window.

Assigning Permissions to Web Sites, Pages and Widgets Based on Role Types

IMPORTANT: Currently, you can only manage users, roles and privileges for the domain of the Application Server from which you opened **iC Creator**.

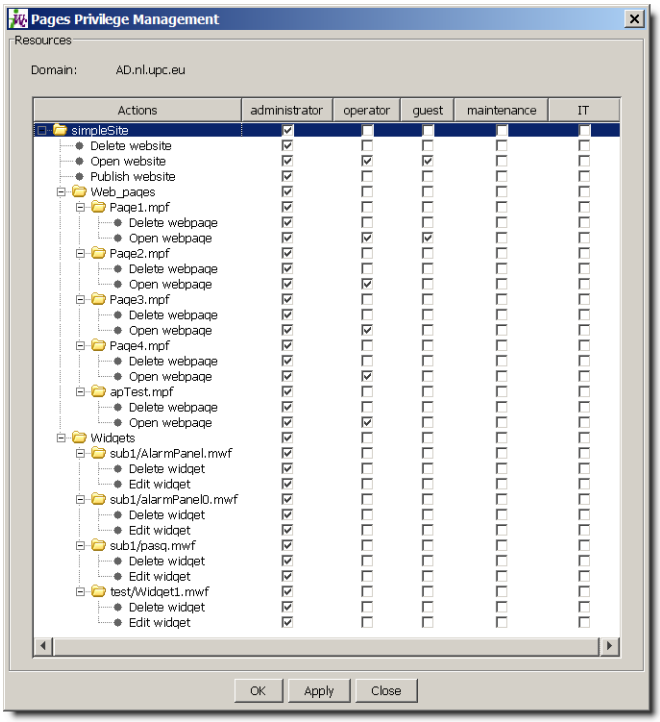
Note: By default, in the **Pages Privilege Management** window, resources (Web sites, pages and widgets) are displayed in the same order in which they were created. Each resource is represented by a folder containing its associated actions.

REQUIREMENT

Before beginning this procedure, make sure you have opened the **Privilege Management** window (see page 709).

To assign permissions to Web sites, pages and widgets based on role types

1. In the **Pages Privilege Management** window, in each role column, click to put a check mark in the row corresponding to a permission you wish to assign. For example, to allow all operators to open the current Web site, put a check mark in the box under **Operator** on the **Open Web site** row.



2. Click in the row corresponding to a folder to assign all of the folder's actions.

Note: Currently, it is not possible to add a new role to the existing set (*administrator, operator, guest, maintenance, IT*).

3. Click Apply to save your changes and continue, or click **OK** to save the changes and close the **Privilege Management** window.

Managing Users for Server-Side Operations

Changing the Password for the Default User Accounts

REQUIREMENT

Before beginning this procedure, make sure you have opened the *User management* page (see page 683), after having logged in to iControl admin, as a user associated with the *super* role.

To change the password for the default super user and administrator profiles

1. On the *User management* page, type a new password for the super user (admin), and for the administrator (miranda), as desired.
2. Click **Save**.

   The new passwords can be used to log in to iControl admin.

Exporting Users to a CSV File

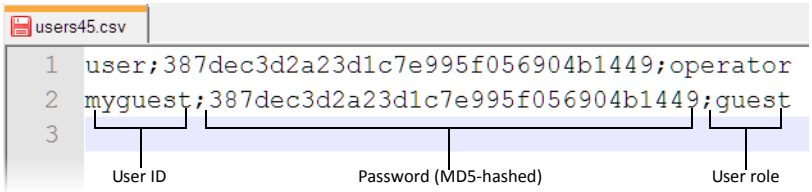
REQUIREMENT

Before beginning this procedure, make sure you have opened the *User management* page (see page 683), after having logged in to iControl admin, as a user associated with the *super* role.

To export users to a CSV file

- On the *User management* page, click **Export Users to CSV**.

  The user data is exported to a CSV file.



Note: The exported file does *not* include user profiles with the *super* or *administrator* roles.

Importing Users from a File

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened the *User management* page (see page 683), after having logged in to iControl admin, as a user associated with the *super* role.
- The file containing the user data you wish to import is a CSV file, in the format presented below:

```
1 boss;387dec3d2a23d1c7e995f056904b1449;administrator
2 oscar;05bba995168eadca4e611be452c17b8e;operator
3 matt;60c90d27e68013c09fdc541c9e003428;maintenance
4 gaston;387dec3d2a23d1c7e995f056904b1449;guest
5
```

User ID | Password (MD5-hashed) | User role

The password MUST be MD5-hashed in the spreadsheet.

To import users from a file

1. On the *User management* page, click **Import Users from CSV**.

   A file selection window appears.

2. Navigate to the CSV file containing the user data you wish to import, select it, and then click **Open**.

   The user profiles from the CSV file become available, and can be used to log in to iControl admin.

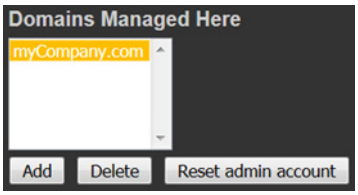
Resetting a Domain's Admin User Account

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Access control* page (see page 682).

To reset a domain's admin user password

1. On the *Access control* page, in the list under **Domains Managed Here**, select the current domain (the one to which the Application Server belongs).



2. Click **Reset admin account**.

   A window appears, prompting you for a new password.

3. Type the new password, and then click **OK**.
4. When prompted to confirm, type the new password again, and then click **OK**.

In a few moments, the page reloads, indicating the *admin* account has been reset.

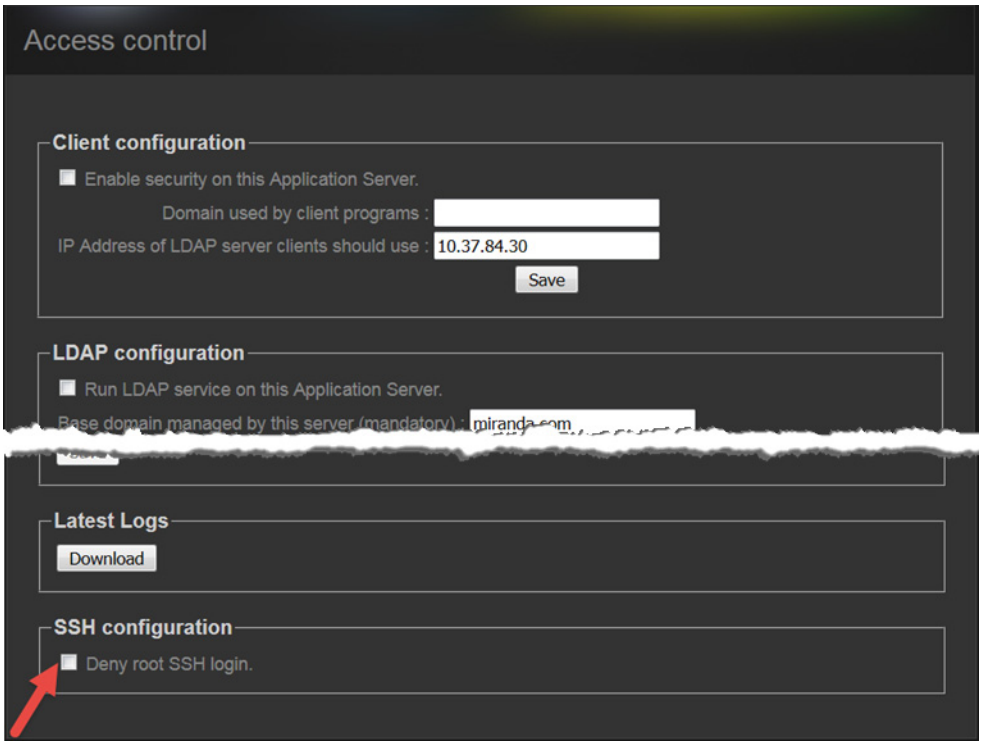
Allowing or Denying Root user Login over SSH

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Access control* page (see page 682).

To allow or deny root user login over SSH

- On the *Access control* page, in the **SSH configuration** area, select the check box to deny root user access over SSH, or clear the check box to allow it.



7 Alarms in iControl

Summary

Key Concepts

Alarms

Alarms are the central feature of monitoring in iControl. There are three types of alarms in the General Status Manager (GSM): events, statuses, and text alarms.

An alarm:

- is a status report on a specific condition within a site
- can inform and/or alert
- refers to a single defined condition, usually generated by a device
- can cause an event, status, text, or a combination of status and text to result depending on the configuration of the alarm

The following table provides a brief description of the various types of alarms available within iControl.

Alarm Type	System Created	Description
Health Monitor	Yes	This alarm indicates the health of the system devices and automatically appears in the Alarm Browser window.
iControl	Yes	This alarm indicates if all the connected cards and devices are available to the system by automatically appearing in the Alarm Browser window.
iC Web		This alarm indicates if the services required by **iC Web** are available by automatically appearing in the Alarm Browser window. When the **iC Creator** page is saved it is automatically saved on the Application Server and appears in the alarm list. The link to the Web page has a status as a virtual alarm.
Third Party Devices		These alarms indicate the operational status of third-party devices such as SNMP plug-ins
Virtual		This alarm is a combination of one or more sub-alarms that can cause a status or text to result depending on the configuration of the alarm and is configured entirely by the user.

Alarm Acknowledgement

Alarm acknowledgement is a feature that provides on-line live acknowledgement of alarms from Web pages and the iControl Alarm Browser. Alarm acknowledgement provides a way of communicating to operators who may not be located in the same location. When these operators are viewing the same Web page, acknowledgement of an alarm is visible for all to see.

When a channel within a group of channels has an alarm status that is not normal then the group background turns red, and the affected individual channel button flashes red until the alarm is acknowledged. When acknowledged the alarm changes to solid red.

If the affected individual channel clears before being acknowledged, the group background changes to a color designated by your configuration team that represents normal status and the individual channel button flashes green.

An alarm acknowledgement:

- causes the alarm to flash at all locations when the alarm status changes from normal status to any other status
- causes the alarm to continue to flash until acknowledged
- can indicate that somebody is working on resolving specific issues that caused alarms when acknowledgment occurs
- simultaneously acknowledges all sub-alarms associated with a virtual alarm that represent channel paths or groups of channels when the virtual alarm is acknowledged
- also allows one-by-one acknowledgement of virtual alarm sub- alarms
- requires that all sub-alarms be acknowledged for the associated virtual alarm to display an acknowledged status

IMPORTANT: Select Show status details to display alarm acknowledgement in the Alarm Browser

Alarm acknowledgement only displays in the GSM Alarm Browser when **Show status details** is selected for the applicable GSM (see Enabling the Display of Alarm Acknowledgement for a Particular GSM Alarm Browser, on page 397).

See also

For more information, see:

- Alarm Acknowledgement in the GSM Alarm Browser on page 340
- Alarms: Pessimistic Status on page 341
- Acknowledging Alarms on page 397

Alarm Acknowledgement in the GSM Alarm Browser

In the GSM alarm browser, the status buttons are divided into three sections. The left side provides the current status, the upper left area provides the server latched status, and the

lower right area provides the acknowledgement status. The combination of all three statuses is part of the alarm acknowledgement functionality.

Current: This is the status of the alarm state of the alarm as it currently stands.

Latched: This is the last alarm state that the alarm has been through since the latch was last reset.

Acknowledgment: This alarm status indicates alarms that require immediate attention when displaying yellow or red. When an operator has acknowledged the alarm, the status becomes solid red if the cause has not yet been resolved OR solid green if the cause of the alarm is resolved.

See also

For more information, see:

- Alarm Acknowledgement on page 340
- Alarms: Pessimistic Status on page 341
- Acknowledging Alarms on page 397

Alarms: Pessimistic Status

Acknowledgement behavior is shown in the following table. The top row represents the current acknowledgement status; the left most column represents the current alarm status. The result according to pessimistic logic is the *new* acknowledgement status that will appear the next time the alarm updates. For example, a red current acknowledgement status and a black current alarm status results in a red *new* acknowledgement status.

Current Alarm Status	Current Acknowledgement Status					
	Green	**Yellow**	**Red**	**Gray**	**Black**	**Blue**
Green	Green	Yellow	Red	Gray	Green	Green
Yellow	Yellow	Yellow	Red	Gray	Yellow	Yellow
Red	Red	Red	Red	Red	Red	Red
Gray	Gray	Gray	Red	Gray	Gray	Gray
Black	Green	Yellow	Red	Gray	Black	Black
Blue	Blue	Blue	Blue	Blue	Blue	Blue

See also

For more information, see:

- Alarm Acknowledgement on page 340
- Alarm Acknowledgement in the GSM Alarm Browser on page 340
- Acknowledging Alarms on page 408

Alarm States

The current state of each alarm is shown as an icon next to the alarm name. Each possible alarm state is represented by a color where the states are dynamically updated.

The statuses in iC Navigator are not handled by the GSM. (These are the JINI statuses.) These are not the same as GSM statuses. For example, iC Navigator can run without a GSM and can provide statuses but not the same type when a GSM is running.

All iControl alarm notifications are managed through a central system called the General Status Manager (GSM). For purposes of load sharing on the client side, alarm notifications from multiple distributed GSMs may be managed by the multi GSM Manager which computes the virtual alarm, gets its status and dispatches the alarm status to the client

For example, a Grass Valley FRS-111i frame synchronizer reports on six operating conditions (e.g., Video input presence), and generates a seventh *overall status* alarm based on the state of the other six alarms.

> **Note:** Some applications may represent alarm states differently or use different color schemes.

When the system starts for the first time the GSM appears on the network while the device is already running, the device is expected to add its alarms to the GSM and to send their status. In that case, both the previous state and next state of the alarm should be initialized to the current state of the alarm.

The following list indicates the color scheme and hierarchy of alarm statuses. The alarm states are positioned from greater value (top of list) to lesser value (bottom of list).

Color scheme and hierarchy of alarm statuses

Color	Meaning
White	No ID assigned to the link - first status on the page before changing to another color Waiting for the GSM to reply such as a slow VPN connection (a new client service)
Green	Normal - an operation status driven by the service
Yellow	Warning - an operation status driven by the service - usually not used
Red	Error
Gray	Unknown - lost connection. The default status for a new alarm that has been added to GSM before its state is known is gray. Therefore if the initial state of the alarm is also gray, there is no need to update the GSM status (but doing it anyway won't have any adverse effect either).
Blue	Non existent: this is a pseudo-status representing an alarm that has been removed (or was never added). You should never see it in the GSM tree, but you'll see it in client applications that listen to specific alarms and the log viewer. When the device starts up and sends its initial state, the **previous state** box should be initialized to blue.
Black	Disabled at the source. Some devices have the ability to deactivate some alarms on the hardware itself; these alarms will show up as black when they are deactivated in this manner.

Alarm Statuses

Each alarm is made up of three different status types: current, latched, and acknowledgment. Each of these alarm statuses is available at any given time.

Current: This is the status of the alarm state that the alarm as it currently stands.

Latched: This is the worst alarm state that the alarm has been through since the latch was last reset.

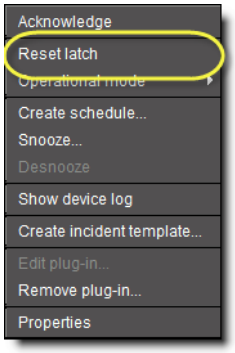
Acknowledgment: This alarm status indicates alarms that require immediate attention when displaying yellow or red. When an operator has acknowledged the alarm, the status becomes green.

> **Note:** For virtual alarms, the *Latched* and *Acknowledgement* statuses are the result of the combination of the statuses for the latched sub alarms and acknowledgements, respectively. This has the side effect that for AND/pessimistic virtual alarms, resetting the latch on a virtual alarm will not necessarily make the status of the latched virtual alarm equal to its current status. Also, acknowledging or resetting the latch on a virtual alarm will recursively affect its subalarms.

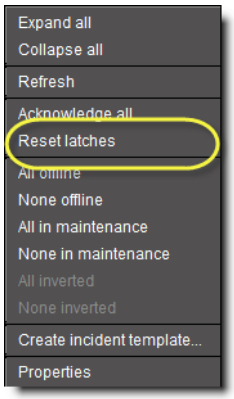
Latches

A latch status shows the last error entry to the log. If the latch has been reset, the latch status will be the same as the current status.

Latches remain in an error state even after the alarm condition has disappeared, and will remain so until an operator resets the latch to the current alarm status. However, the latch will not reset until the alarm condition goes away. Latches are system wide and all clients see the same latch.



Resetting individual alarm's latch



Resetting alarm latches of all alarms in an alarm folder

See also

For more information, see:

- Alarm Components on page 348
- Latches, Acknowledgment and Virtual Alarms on page 358
- Resetting Latches on Web Pages on page 410

Alarm Types

There are a number of different types of iControl alarms, described briefly below and in greater detail later in this chapter. The diagrams on the following pages show how the various alarm types appear in iControl.

Virtual Alarms

A virtual alarm is a special type of alarm that allows you to derive a new result from the status(es) of one or more existing alarms.

Overall Alarms

An overall alarm is a type of virtual alarm that indicates the overall condition of a device or service based on the combined statuses of the constituent alarms for that device or service. Overall alarms are often generated automatically.

Sub-alarms

A sub-alarm is an alarm that contributes to the status of a higher level virtual alarm. Sub-alarms can be grouped together, and the group itself can become a sub-alarm of a higher-level alarm. Each sub-alarm may or may not have the same status as its higher-level alarm. The effect of a sub-alarm's contribution is determined by the way in which the higher-level alarm is configured. A sub-alarm's contribution to a higher-level alarm can, in some cases, be modified.

Grass Valley Device Alarms

All Grass Valley devices in an iControl system automatically generate an overall alarm status that can be viewed in iC Navigator (the icon beside the device name), in the GSM Alarm Browser (the *Overall* sub-alarm inside the folder associated with the device), and on Web pages—any Web page component that is associated with the device, such as a button or a

UMD, can be configured to display the device's overall alarm status. The overall alarm status comes from the device's hardware or firmware, and is based on the status(es) of one or more sub-alarms corresponding to specific device parameters.

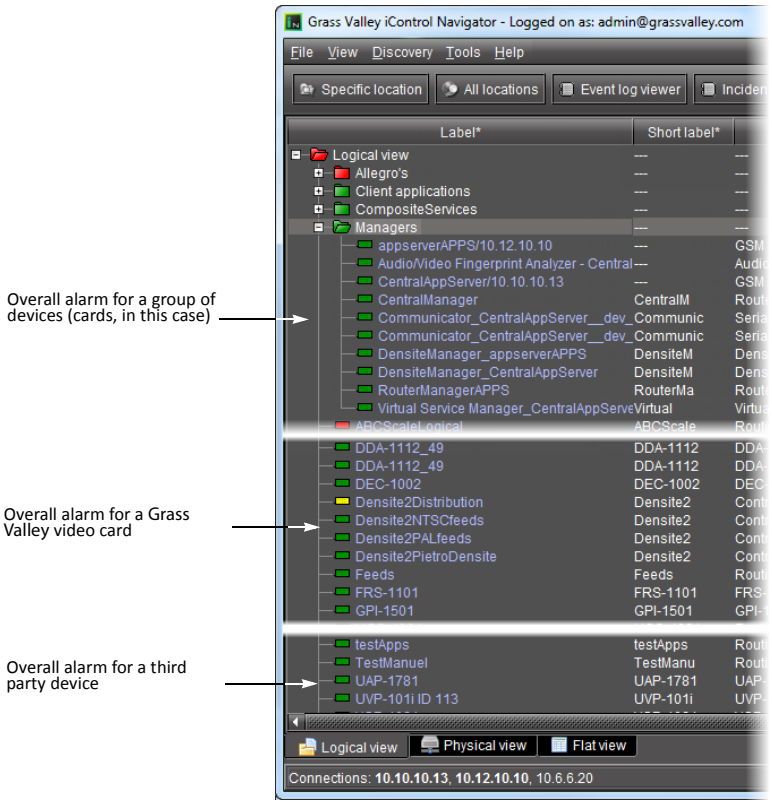
Grass Valley Service Alarms

All Grass Valley services in an iControl system automatically generate an overall alarm status that can be viewed in iC Navigator, in the GSM Alarm Browser, and on Web pages.

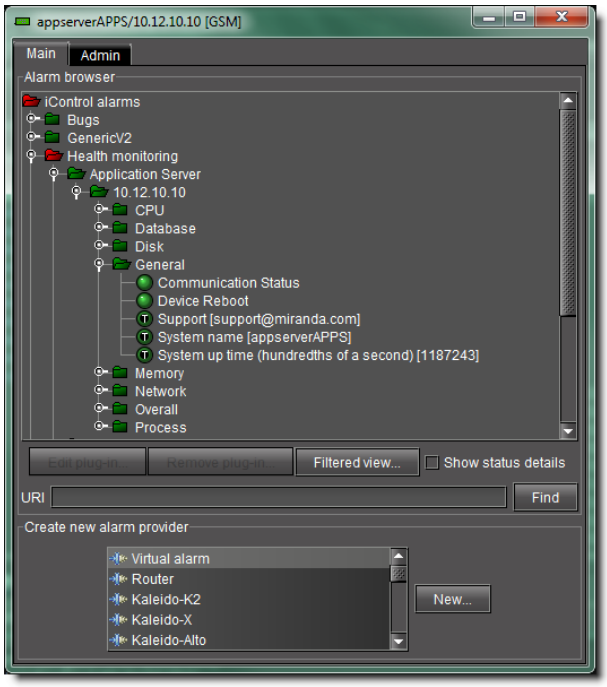
Third Party Alarms

iControl can recognize and display alarms for devices and services from third party companies. As a minimum, all such devices/services are represented by overall alarms that can be viewed in iC Navigator, in the GSM Alarm Browser, and on Web pages. In many cases, a broader set of alarms can also be displayed.

The relationship between alarms in iC Navigator and in the GSM Alarm Browser is shown below.

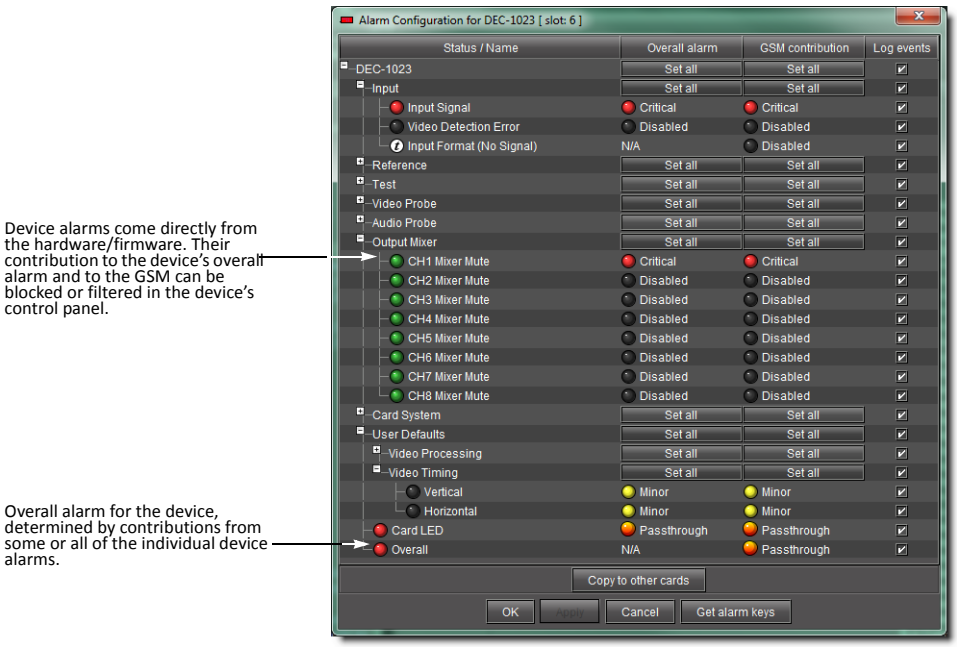


Alarms and groups in the iC Navigator window

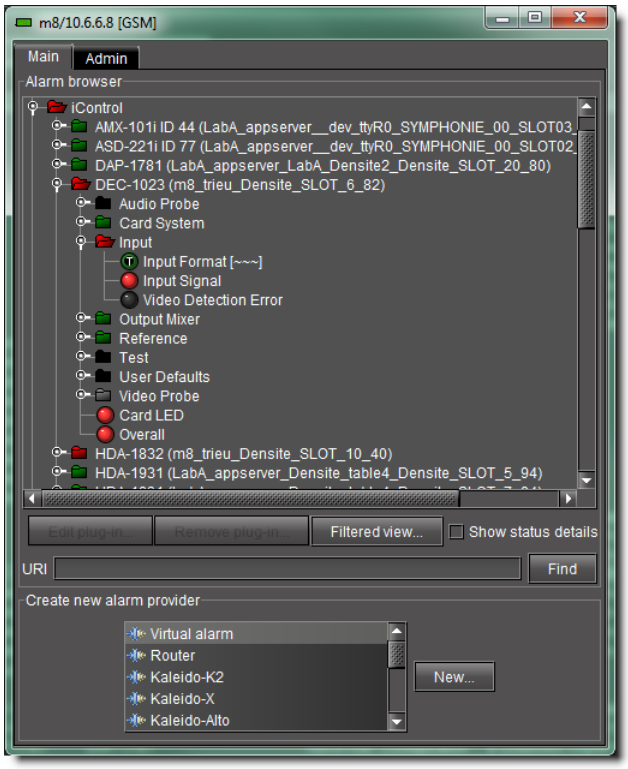


Alarms, groups, and sub-alarms in the GSM Alarm Browser

The relationship between alarms in a device control panel and in the GSM Alarm Browser is shown below.



Alarm Configuration section of a video card's Control Panel



Video card's alarms in GSM Alarm Browser

The following table provides a brief description of some of the alarm categories available within iControl:

Alarm Category	Created by	Description
Health Monitor	System	Alarms of this type indicate the health of system devices, such as a Densité frame, a Symphonie frame, or an Application Server. A folder named "Health Monitor" automatically appears in the Alarm Browser window.
iControl	System	Alarms of this type indicate whether cards and devices on the network being monitored are available to the iControl system. A folder named "iControl" automatically appears in the Alarm Browser window.
iC Web	User	Alarms of this type indicate whether the services required by **iC Web** are available. A folder named "iControl Web" automatically appears in the Alarm Browser window. When an **iC Creator** page is saved, it appears in the list of alarms in this folder.
Router	User	Alarms of this type indicate the operational status of routers
Third Party Devices	User	Alarms of this type indicate the operational status of third party devices
Virtual	User	Alarms of this type are a combination of one or more sub-alarms.

Alarm Components

In addition to knowing the status of an alarm, it is often useful to know the history of the alarm, and whether or not someone has taken any action in response to it. iControl represents these changes in alarm status over time using three components: **current**, **latched**, and **acknowledgment**.

Current

This is the component of an alarm corresponding to its current status. If a freeze alarm is red, it means the video is currently frozen. As soon as it starts again, the alarm is cleared and becomes green.

Latched

This is the component of an alarm corresponding to the worst status that the alarm has recently exhibited. For example, a transient fluctuation in a video signal may cause an alarm configured to detect a video signal freeze to turn red for a moment, and then return to green. iControl keeps track of the fluctuation by setting the latched component of the alarm to red, giving the operator a visual cue that this alarm may need to be watched more closely. A latch can be reset by an operator, causing iControl to set the latch status to green and then begin tracking status changes all over again.

The latched component of an alarm can be configured to track the alarm on either the server side (in which case the latch can be reset by any operator from any client workstation), or on the client side (in which case the client workstation "remembers" the latch status from a previous session, regardless of what has happened on the server in the interim).

Latches can be reset by an operator when an alarm's current status is green. Resetting a server-side latch for an overall (virtual) alarm simultaneously resets the latches on all associated sub-alarms. Resetting a client-side latch for an overall (virtual) alarm has no effect on the latches of associated sub-alarms (these must be reset one by one).

Acknowledgment

This is the component of an alarm that reflects an operator's response. If an alarm changes to an error status, its *acknowledgment* component (if it is visible) will also change color. When an operator acknowledges the alarm (by clicking on a button or choosing a menu item), the acknowledgment component turns green. If, however, the issue that initially triggered the alarm is not resolved within a certain period of time, the acknowledgment component will once again change color to attract the operator's attention.

Alarm acknowledgment can provide visual feedback to operators at different locations. An alarm acknowledgment by one operator will be seen by all operators viewing the same **iC Web** page, and is usually an indication that somebody is attempting to resolve the cause of an alarm.

iC Web has a feature that allows operators to have all alarms on a page blink when an acknowledgment is required.

Acknowledging a virtual alarm automatically acknowledges its constituent sub-alarms. Sub-alarms can also be acknowledged individually.

Note: Alarm acknowledgment is only visible in the GSM Alarm Browser when **Show status details** is selected (see Displaying Alarm Status Details, on page 407).

Alarm Acknowledgment Behavior in Channel Selectors

A *channel selector* is a Web page element consisting of a group of buttons used to select individual channels. When one channel in a group has an alarm status that is not normal, the group background turns red, and the affected individual channel button flashes red until the alarm is acknowledged. If the affected individual channel clears before being acknowledged, the group background changes to a color that represents normal status, and the individual channel button flashes green.

Alarm Acknowledgment Scenarios

Here is an example of a *simple* alarm acknowledgment scenario.

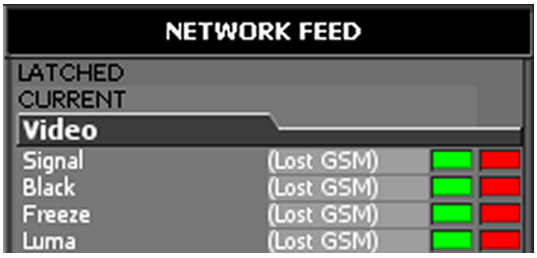
1. An alarm has an initial status of normal (green).
2. A critical error occurs, causing the alarm's *current*, *latched* and *acknowledgment* states to change from green to red.
3. After a few seconds, an operator acknowledges the alarm, which changes the *acknowledgment* state back to green. Other operators can see that the error is still present, but that someone is working on it.
4. If the problem is fixed before the *acknowledgment* period expires, the alarm's *current* state reverts to green (the *acknowledgment* state remains green).
5. If the problem is not fixed before the *acknowledgment* period expires, the *acknowledgment* state reverts to red.

Here is an example of a *recurring* alarm acknowledgment scenario.

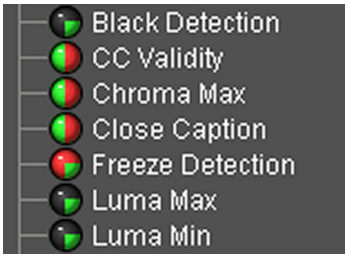
1. As in the previous scenario, the alarm is acknowledged and the *acknowledgment* state reverts to green.
2. If the problem is not fixed before the *acknowledgment* period expires, the *acknowledgment* state reverts to red, which triggers a second alarm (that gets logged) with a note that the issue has now escalated once.
3. A scripted action might, at this point, send an SMS message to a supervisor.

Alarm Component Appearance

For any given alarm, it is possible to have an on-screen representation of the components as separate icons/buttons, or in one combined icon.

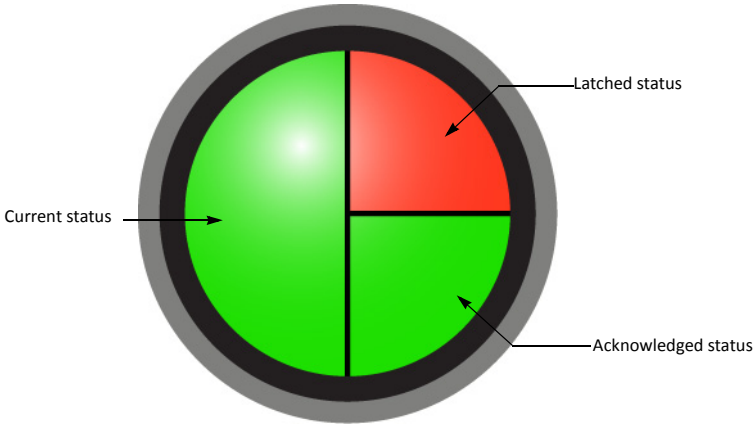


Alarms on a Web page showing separate components (latched and current)



Alarms in the GSM showing combined components (current, latched, and acknowledged)

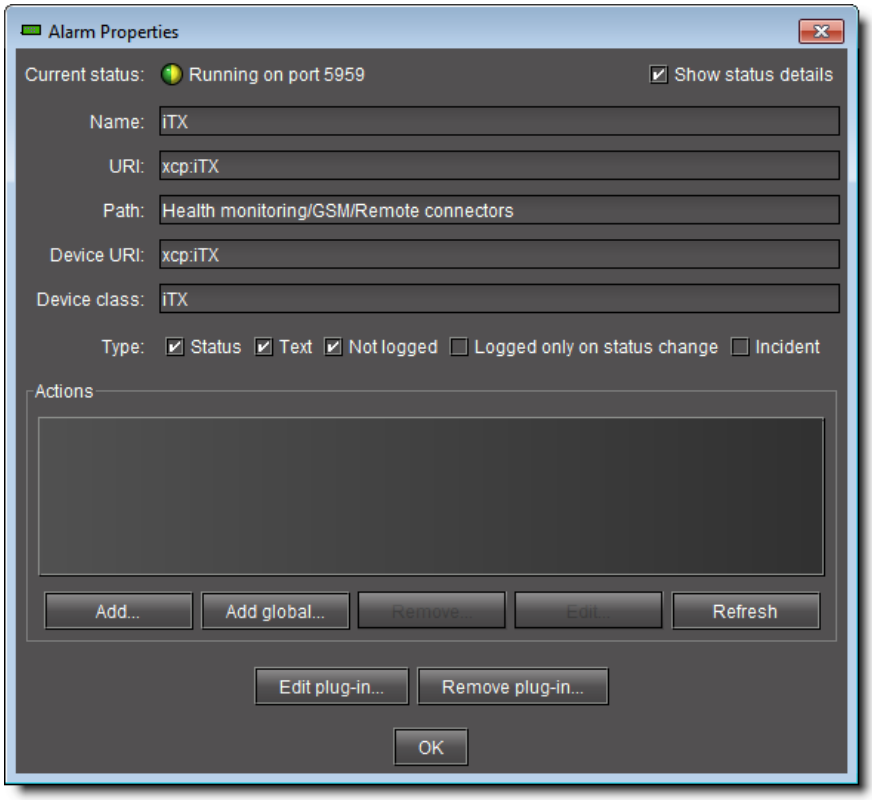
When an icon is configured to show the combined alarm components, it is divided into parts as shown in the diagram below.



The entire left half of the icon changes color to indicate the *current* alarm status. The upper right quadrant represents the *latched* status, while the lower right quadrant represents the *acknowledged* status.

Alarm Attributes

Several fields comprise the **Alarm Properties** window (to which you can navigate by double-clicking an alarm in the Alarm Browser). Together, the values these fields hold define the alarm.



The following table describes these attributes and their respective guidelines:

Attributes of an alarm

Attribute	Description
Name	A meaningful name for the alarm. The alarm name appears in the GSM Alarm Browser tree and several other locations. By convention, the name uses *Sentence case* (as opposed to, for example, *Title Case* or even ALL CAPS).
URI	A unique identifier for the alarm. This is what uniquely identifies an alarm. Everything else could, potentially, change over time, but if you change URI, then you have, by definition, created a new alarm. Consequently, alarms with the same URI but coming from different GSMs are considered to be the same and interchangeable. This is useful and efficient in terms of scalability and redundancy when coupled with tools such as the GSM Aggregator.
Path	Tree path of the alarm[1].

Attributes of an alarm (*Continued*)

Attribute	Description
Device URI	A unique identifier for the (hardware) device providing the alarm. The device URI is used to group together alarms that pertain to the same device. Typically, one device handles one channel or signal. This attribute allows us to see all alarms related to a given channel or signal as well. The GSM contextual log viewer uses the Device URI to find alarms related to one another. Perhaps more importantly, a number of metadata fields are attached to each GSM device using this field as a key. This should influence the way device URIs are built so that for devices with multiple ports (usually sources), their URIs should include an indication of the port number, so each source gets its own source metadata and the alarms are grouped by source. • Separate the various parts of the URI with a forward slash (/)[2]. This allow us to have relative URIs. • Device URIs and Long IDs should be the same. In the past, long IDs were sometimes allowed to contain spaces, which is forbidden in URIs, so they need to be encoded "just in case". Some URIs are derived from long IDs, but with only selected parts encoded.
Device class	Device model name. Typically, this is product marketing name; for instance, for the Densité line this would be something like DEC-1002. iControl doesn't use this in any particular fashion, but occasionally users will use this field when searching the logs to identify problems across a product family. For instance, if you see a specific problem with an XVP-3901 you might search for similar problems with other XVP-3901's, and not just the one where you noticed the problem—do I experience audio losses on all my XVP-3901 cards?

1. Multiple paths for the same alarm are not supported. The last specified path will be used. By convention, each segment of the path uses Sentence case (as opposed to, e.g., Title Case or ALL CAPS).
2. Legacy Densité/Imaging URIs use the _ character.

General Guidelines for Alarm Attributes

Make URIs Meaningful

Typically, administrators want URIs are identifiers that administrators want to hide as much as possible from end users, but it doesn't mean we want them to be totally opaque identifiers like GUIDs. It is often useful to actually look at the URIs when troubleshooting, and when that happens it's very hard to tell at first glance if an assignment is correct if all you have to look at is a GUID or something equally cryptic. URIs don't have to be self-documenting or even especially user-friendly, but they should be meaningful to humans. This way they can be memorized, transcribed and understood more reliably.

Avoid redundancy

Information redundancy in URIs is bad. A bad example would be to include both a host name and corresponding IP address in URIs "so they are readily available". Not only does it make URIs longer, it also makes them brittle (if any one of the host name or IP address changes, it breaks all uses) and impractical (users need to remember/store both elements of information when they want to use the alarm). Pick one or the other and stick with it.

Likewise, avoid packing all sorts of information in a URI that does not serve to uniquely identify it. For instance there were proposals to embed SNMP OIDs in the URIs of the derived GSM alarms, but that requires all users to know that bit of information on top of everything else, unless you make it optional (but that would require more complex parsing which doesn't exist today). The approach here is to make a call to GSM (or one of its plug-ins) to obtain more information when required, like we do for instance when we "resolve" an alarm URI to obtain

the alarm path, alarm name and so on. We don't embed the path and name in the alarm URI "just in case".

Physical vs. logical

Very often you have to make the choice between physical and logical concepts. The most obvious example of this is whether to use host names or IP addresses in URIs. Ideally we want to support both (see Future directions), but until we do, in general we chose to favor logical representations over physical ones, at least when there are no other compelling arguments to sway the decision either way. That means preferring host names over IP addresses in general. If you don't have a meaningful host name for the device however, don't make one up -- just use the IP address until you do have something better.

Avoid irrelevant parts

Often we include things such as the Application Server host name/IP address in URIs. Unless we are referring to something that is connected directly an Application Server, or that resides only in an Application Server, the Application Server where the service runs is merely an implementation detail. Not including it in the URI allows us to move the service to another Application Server if required (for instance to rebalance the load) and it also allows for redundant services. For instance, assuming its protocol allows it, a router could be configured on two separate Application Servers, each one publishing its own copy of the alarms. These are logically the same and therefore interchangeable, and we can leverage this to provide improved fault tolerance.

Encoding

Sometimes URIs will need to include some parts that are based on more or less free-form user input, and in those cases the possibility exists that users will enter special characters which either are not allowed in URIs at all, or may cause problems with the automated parsing of your URIs. In those cases, instead of restricting what users can enter (except when it makes sense, for instance for a slot or port number), it is preferable to escape or encode the user-entered string. Our preferred mechanism to achieve this is to URL-encode those parts using a UTF-8 encoding.

Derived (alarm) URIs

There is sometimes a case for generating meaningful URIs that are associated to other existing (and presumably also meaningful) URIs. This occurs when you publish an alarm that depends directly on another alarm. A good example are the alarms published by the cycling engine; we want these alarms to be derived from the base alarms that they relate to, adding a notion of channels into the mix. Another example are event URIs for events that are closely related to alarms, for instance an event that pertains to acknowledging an alarm, or switching a router crosspoint.

The approach that we favor is to add a prefix to the existing alarm (which is less problematic than adding a suffix). For instance you might get:

```
cycled:<channelID>:<baseAlarmURI>

event:ack:<relatedAlarmURI>
```

Virtual Alarms

A virtual alarm is a special type of alarm that allows you to derive a new result from the status(es) of one or more existing alarms.

Any alarms in iControl — including other virtual alarms — can be combined together to form a new, higher-level virtual alarm. You cannot, however, create a virtual alarm that includes itself as a sub-alarm, since this creates a cyclical dependency. iControl automatically checks for this dependency, and will alert you of any potential problems.

> **Note:** When building virtual alarms, *do not* include alarms from an **EdgeVision** edge signal monitoring device. Always use native alarms from EdgeVision, by themselves, instead of virtual alarms.

Since a virtual alarm can be composed of virtual alarms other than itself, there can be many levels of virtual alarms within a particular virtual alarm. At this time there is no limit to the number of levels that a virtual alarm can have.

Overall Alarms

The alarms that are visible in iC Navigator correspond to a special kind of *virtual alarm*, called an *Overall* alarm, that are published by devices and services to the GSM. If you right-click on a device in iC Navigator and choose **Configure overall alarm**, a small window appears identifying the URI of this virtual alarm. Click the **Browse** button, and the GSM Alarm Browser opens, with the Overall alarm highlighted. From here, you can access the Overall alarm properties as you would for any other alarm.

IMPORTANT: Overall and GSM contribution alarms are disabled by default for all Densité services. Make sure all alarms and levels are configured as required.

Alarm Logic Tables

The status of a virtual alarm is determined by comparing the values of its sub-alarms. The outcome of such comparisons is defined in *alarm logic tables* built into iControl. Outcomes can be defined *pessimistically* (choose the more severe of two statuses), or *optimistically* (choose the less severe of two statuses). The pessimistic determination of a status is sometimes referred to as an *OR* operation. The optimistic determination of a status is sometimes referred to as an *AND* operation.

[OR]

Subalarm #2 Current Status \ Subalarm #1 Current Status	White	Green	Yellow	Orange	Gray	Red	Blue	Black
White	White	Green	Yellow	Orange	Gray	Red	Gray	Black
Green	Green	Green	Yellow	Orange	Gray	Red	Gray	Green
Yellow	Yellow	Yellow	Yellow	Orange	Gray	Red	Gray	Yellow
Orange	Orange	Orange	Orange	Orange	Gray	Red	Gray	Orange
Gray	Gray	Gray	Gray	Gray	Gray	Red	Gray	Gray
Red	Red	Red	Red	Red	Red	Red	Gray	Red
Blue	Gray	Gray	Gray	Gray	Gray	Gray	Gray	Gray
Black	Black	Green	Yellow	Orange	Gray	Red	Gray	Black

Virtual Alarm's Current Status

*Pessimistic **OR** logic table for determining the status of the CURRENT or LATCHED component of a virtual alarm*

[AND]

Subalarm #2 Current Status \ Subalarm #1 Current Status	White	Green	Yellow	Orange	Gray	Red	Blue	Black
White	White	Green	Yellow	Orange	Gray	Red	Gray	Black
Green	Green	Green	Green	Green	Green	Green	Green	Green
Yellow	Yellow	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Orange	Orange	Green	Yellow	Orange	Orange	Orange	Orange	Orange
Gray	Gray	Green	Yellow	Orange	Gray	Gray	Gray	Gray
Red	Red	Green	Yellow	Orange	Gray	Red	Red	Red
Blue	Gray	Green	Yellow	Orange	Gray	Red	Gray	Gray
Black	Black	Green	Yellow	Orange	Gray	Red	Gray	Black

Virtual Alarm's Current Status

*Optimistic **AND** logic table for determining the status of the CURRENT or LATCHED component of a virtual alarm*

When you create a virtual alarm, you can specify the use of either a pessimistic or optimistic table for determining CURRENT an LATCHED statuses.When the virtual alarm is in operation, iControl uses that table to calculate the combined statuses of the sub-alarms. Where more than two sub-alarms are involved, iControl starts by comparing one pair of sub-alarms, then takes that result and compares it with the next sub-alarm, and so on.

A third type of comparison—XOR—can be used to have a virtual alarm reflect whether or not all of its sub-alarms have the same status. If all sub-alarms are the same, the virtual alarm will be green. Otherwise, it will be red.

ACKNOWLEDGED Status

The ACKNOWLEDGED status of a virtual alarm is always calculated in the same way (i.e. there is no distinction made between pessimistic or optimistic combinations).

Subalarm #2 Ack. Status \ Subalarm #1 Acknowledgement Status	White	Green	Yellow	Orange	Gray	Red	Blue	Black
White	—	—	—	—	—	—	—	—
Green	—	Green	Yellow	Orange	—	Red	Green	—
Yellow	—	Yellow	Yellow	Orange	—	Red	Yellow	—
Orange	—	Orange	Orange	Orange	—	Red	Orange	—
Gray	—	—	—	—	—	—	—	—
Red	—	Red	Red	Red	—	Red	Red	—
Blue	—	Green	Yellow	Orange	—	Red	Green	—
Black	—	—	—	—	—	—	—	—

Virtual Alarm's Acknowledgement Status

Logic table for determining the status of the ACKNOWLEDGED component of a virtual alarm

Understanding the Alarm Logic Tables

Understanding how the alarm logic tables work is important to being able to get predictable results when you create a virtual alarm. Here are some points to keep in mind:

- When a GREEN sub-alarm status is compared with a YELLOW sub-alarm status, a pessimistic table will define the result as YELLOW, because YELLOW is a worse condition than GREEN. Conversely, an optimistic table will define the result as GREEN, because GREEN is a better condition than YELLOW.
- When a sub-alarm has a status of BLUE (the alarm currently does not exist), and it is compared with a GREEN sub-alarm, a pessimistic table would, in theory, define the result as BLUE, because BLUE is a worse condition than GREEN. But, since BLUE means "status does not exist", it makes more sense to provide a result of GRAY, or "status undefined", to the virtual alarm. An optimistic table would define the result as GREEN, because GREEN is a better condition than either BLUE or GRAY.
- Results based on sub-alarms with BLACK or WHITE status are exceptions to the rule, in that it is not always evident which is better or worse.
- The acknowledgment component of an alarm status can only be GREEN, YELLOW, ORANGE, RED or BLUE.
- Critical (red) has priority over Unknown (gray) by default in the calculation of a virtual alarm. For example, if a signal loss occurs, the Signal Presence alarm turns red, while every other alarm that depends on the signal presence is set to Unknown. In previous versions of iControl, the Unknown alarms would take precedence in the calculation of the overall status of the device, which would also be displayed as Unknown, even though a Critical error has occurred (i.e. the signal was lost). As of iControl 3.20, the Critical alarm in this example would have priority, making the overall alarm status red.

  To revert to the old alarm priority behavior, set the system property:
  `com.grassvalley.icontrol.gsm.virtualAlarm.errorSupercedesUnknown`

  to false.

Note: It is possible to globally reverse the priorities of *critical error* (red) and *unknown* (gray) statuses as they pertain to virtual alarms. This is done by setting the following system property to *true*:

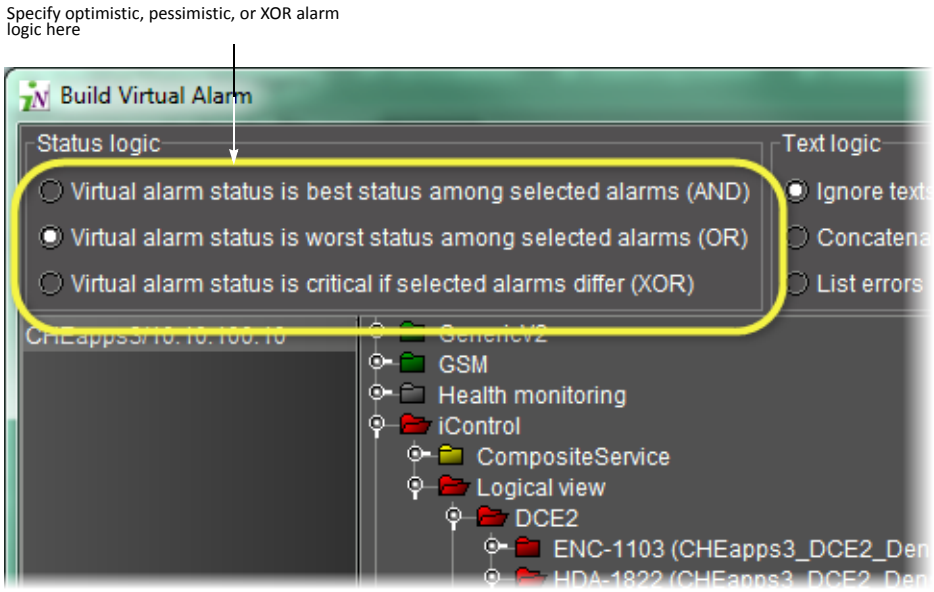
`com.miranda.icontrol.gsm.virtualAlarm.errorSupercedesUnknown`

Doing so slightly alters the combination rules of the alarm logic tables.

Additionally, we recommend setting the system property in the following properties file on the server (not in a script) to avoid losing changes after an upgrade:

`/usr/local/iControl/bin/conf/java_generic.properties`

When you build a virtual alarm in iControl, you must choose which alarm logic table is to be used to evaluate the statuses of its sub-alarms.



Example — Using Pessimistic and Optimistic Alarm Logic

Consider a broadcast network with two identical signal pipelines: Pipeline #1 is on-air, while Pipeline #2 is off-line, but configured to automatically take over should anything go wrong with Pipeline #1. A typical use of iControl would be to create one virtual alarm to indicate a problem on either pipeline, and another to monitor the status of the signal, regardless of which pipeline is in use.

The first virtual alarm would use a *pessimistic* logic table to compare the status of each pipeline. If both pipelines show GREEN, the virtual alarm shows GREEN. If, however, either pipeline develops a critical error, the virtual alarm would turn RED.

The second virtual alarm would use an *optimistic* logic table to compare the status of the signal on both pipelines. As long as the signal is active on either Pipeline #1 or #2, the virtual alarm would remain GREEN.

Latches, Acknowledgment and Virtual Alarms

The status of a virtual alarm's *latched* and *acknowledgment* components are derived from the corresponding statuses of its sub-alarms. This has a side effect—for virtual alarms that are calculated using pessimistic (AND) logic tables, resetting the latch will not necessarily make the status of the *latched* component of the virtual alarm the same as the status of its *current* component.

Resetting a latch on a virtual alarm sets the *latched* component of each of its sub-alarms to the value of its *current* component. In turn, the statuses of each of the sub-alarms contribute to the reset status for the virtual alarm. If there were virtual alarms included as sub-alarms, then their sub-alarms are reset to the current status, and all these sub-alarms contribute to the status of the top level virtual alarm. This pattern continues through all the levels of the virtual alarm and is referred to as *virtual alarm recursion*.

In some circumstances, performing actions affecting a large number of complex virtual alarms—such as Reset all latches, or Acknowledge all—may result in a loss of communication with a controlled device. A system property is available to prevent an iControl GSM server from broadcasting alarm actions to specific GSMs. On the server where the broadcasts originate, in `/usr/local/iControl/bin/conf/java_gsm.properties/`, set the `icontrol.gsm.disableActionDispatch` property to the appropriate value for your purposes. For example, to disable action dispatches to all remote GSMs, set `icontrol.gsm.disableActionDispatch` to *true;* to disable action dispatches to specific GSMs, list the IP addresses of the GSMs you wish to exclude from action dispatches (e.g., `icontrol.gsm.disableActionDispatch=10.10.10.10, 10.20.20.20`).

When iControl displays a virtual alarm's *latched* or *acknowledged* component, it determines the status (or color) by comparing its sub-alarms according to a *pessimistic* logic table.

[OR]	Subalarm #1 Acknowledgement Status							
Subalarm #2 Ack. Status	White	Green	Yellow	Orange	Red	Gray	Blue	Black
White	—	—	—	—	—	—	—	—
Green	—	Green	Yellow	Orange	Red	—	Red	—
Yellow	—	Yellow	Yellow	Orange	Red	—	Red	—
Orange	—	Orange	Orange	Orange	Red	—	Red	—
Red	—	Red	Red	Red	Red	—	Red	—
Gray	—	—	—	—	—	—	—	—
Blue	—	Red	Red	Red	Red	—	Red	—
Black	—	—	—	—	—	—	—	—
	Virtual Alarm's Acknowledgement Status							

Alarm Operational Modes

iControl has three operational modes that are used to temporarily stop alarms from reporting errors: the *In maintenance* mode, the *Offline* mode, and the *Snooze* mode.

Offline

The *Offline* mode is generally employed in the execution of an automated task. Setting alarms to Offline mode has a similar effect, except that each latch is also reset when alarms are put back online.

Consider the case where several TV channels go "off air" every morning between 02:00 a.m. and 06:00 a.m. A schedule could be established (see note below), or a script could be created, to turn off the alarm display for these channels automatically during the specified intervals. Such a schedule or script would set the appropriate alarms to *Offline* mode at 02:00, to avoid having iControl report a sudden flood of alarms due to loss of signal.

Similarly, the schedule/script would put the alarms back online at 06:00, at which point, with the signals restored, the alarms would normally all return to green. Anything that happened during the offline period, however, would not be visible in iControl, because each latch is also reset when an alarm is put back online.

> **Note:** Alarms can be set to *In maintenance* or *Offline* mode according to a predetermined schedule using the Alarm Scheduling feature (see Alarm Scheduling, on page 378).

In Maintenance

The *In Maintenance* mode is generally employed in the execution of a manual task.

In a typical scenario, a technician might want to effect repairs on a device in the path of a signal being monitored by iControl. Before beginning, the technician would manually set the corresponding alarms to *In Maintenance* mode, to avoid having iControl report a sudden flood of errors. Once the repairs are done, the technician would then manually take the alarms out of *In Maintenance* mode, putting them back online, but the alarm latches would not be automatically reset. In this mode, alarm transitions affect the latch and the acknowledgement states of alarms (see Acknowledging Alarms, on page 408).

Inverted

The *Inverted* mode is used to configure a GSM to publish the inverted value of a specific alarm's state rather than its actual state. This is useful when one would like to report an error condition when an alarm would normally not be in error, and a normal condition when it would normally be in error. An inversion action can be configured manually (you invert the alarm and it remains inverted until you turn off the inversion mode) or by scheduling an inversion for a specific time and duration. If you would like to schedule an alarm inversion, you can report certain error conditions during certain periods of the day and the exact opposite during other periods of the day. For example, you may want a video freeze condition while on-air during the day to be reported. But during the night, if there is a movie being broadcast by accident, you may want for this condition to be reported as well.

Like the *Offline* and *In Maintenance* operational modes, the *Inverted* mode is Boolean (that is, the *Inverted* mode can be either *On* or *Off*). A primitive alarm's *Inverted* mode (*On* or *Off*) is propagated up to parent virtual alarms' *Inverted* modes.

IMPORTANT: System behavior

You cannot directly edit the Inverted mode of a virtual alarm or alarm folder; you can only change a virtual alarm's Inverted mode indirectly: by changing the Inverted mode of one or more of its primitive alarms.

You can switch an alarm's Inverted mode to *On* or *Off* either manually or by scheduling. A manual switch is operator-driven and causes a mode change instantaneously. A scheduled switch is preconfigured by an operator to occur at a preset time and frequency.

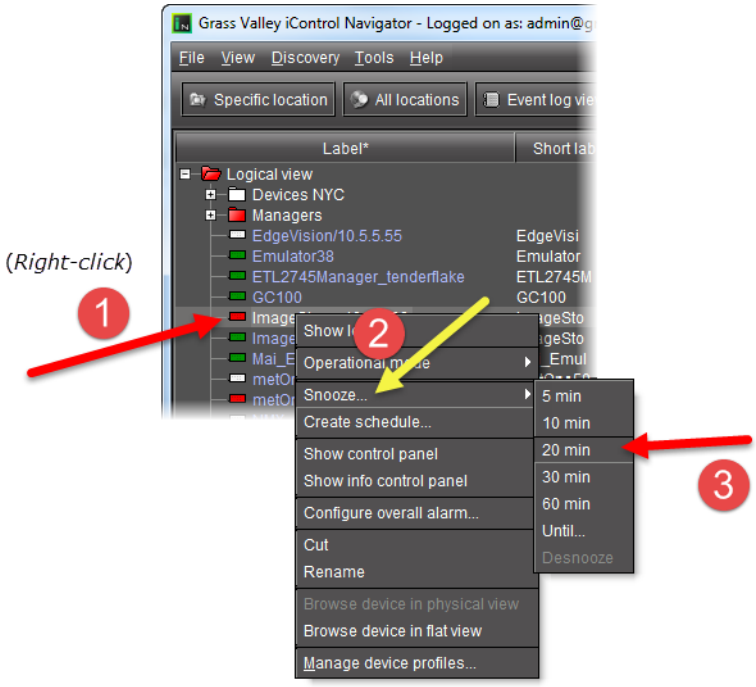
See also

For more information about:

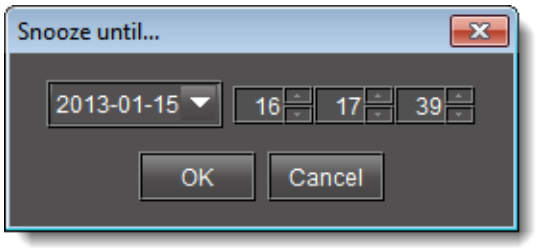
- Manual alarm inversions, see:
  - Manual Alarm Inversions on page 375, and
  - Inverting Alarms Manually on page 416
- Alarm inversion scheduling, see:
  - Alarm Inversion Scheduling on page 378, and
  - Setting a Schedule for an Alarm Inversion on page 421

Snooze

When dealing with unscheduled events, operators sometimes need the ability to quickly suppress alarms for a certain period. The *Snooze* operational mode allows you to turn off an alarm temporarily, either for one of the preset durations or until a later time of your own choosing.



Shortcut menu to access the Snooze function

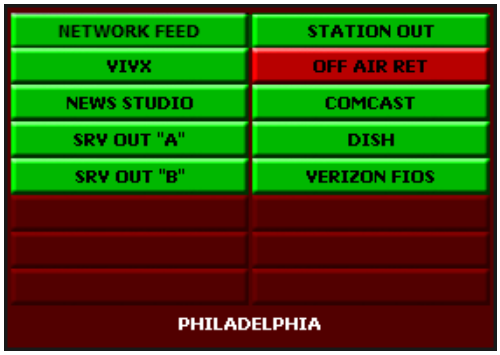


***Snooze until** window*

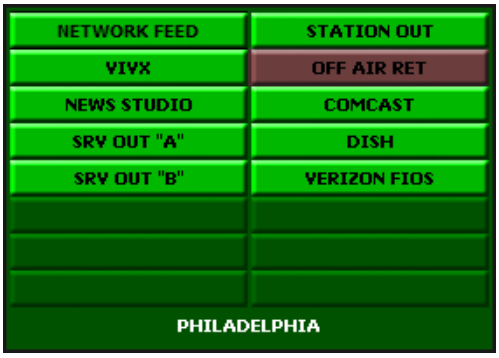
> **Note:** Changing an alarm status to *Offline*, *In Maintenance* or *Snooze* mode does not interrupt monitoring. All alarm events are still logged and can be viewed using **Event Log Viewer**.

Appearance

When an alarm has been set to *In Maintenance*, *Offline*, or *Snooze* mode, its color turns to a darker shade, and any text associated with the alarm becomes orange.

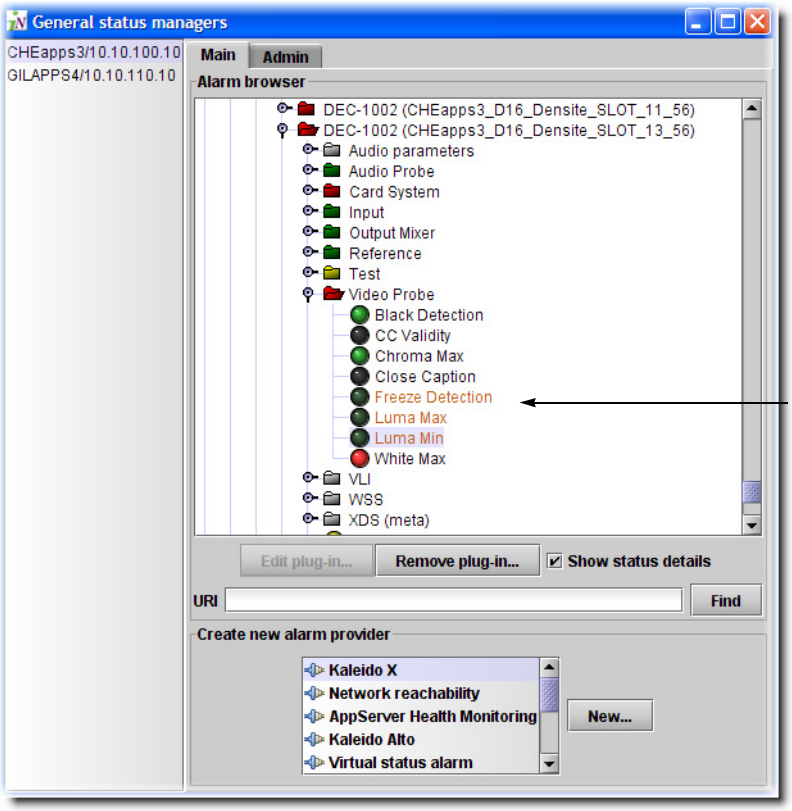


Online alarm in error status (red)



Same alarm set to In Maintenance mode (dark red)

In some places, such as in the Alarm Browser, the text appearing next to a status icon will also be displayed in a different color. The illustration below shows a DEC-1002 card for which the video Freeze, Luma Max, and Luma Min alarms have been suppressed by being set to the Offline operational mode.



Your iControl system may have been configured to show the suppressed alarm as normal (green) instead of the darker colors listed above. The default is to show the real status using the darker colors.

Virtual Alarm Operational Modes

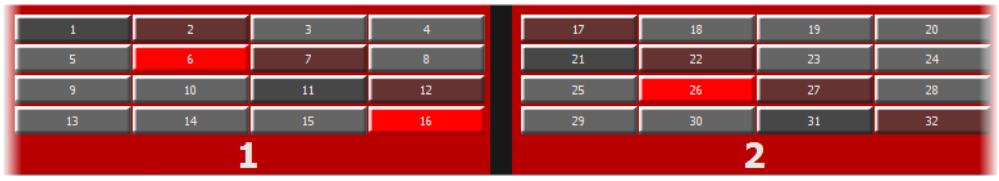
Virtual alarms don't have their own operational modes. They reflect the operational modes of their sub-alarms (just as they do for current, latched and acknowledgement statuses). If a sub-alarm has an operational mode set, then the virtual alarm inherits it.

If you select a virtual alarm and then set an operational mode on it, this setting is applied to all of its sub-alarms. The normal rules of inheritance then apply, so that the status of the virtual alarm ends up reflecting the mode setting of its sub-alarms.

IMPORTANT: System behavior

You cannot directly edit the *Inverted* mode of a virtual alarm or alarm folder; you can only change a virtual alarm's *Inverted* mode indirectly: by changing the *Inverted* mode of one or more of its primitive alarms.

In the case of virtual alarms, such as in a Source selector panel, the overall status icons for suppressed alarms reflect their real status, but in a darker shade, as shown below.



An operator can right-click the status icon for any alarm (including virtual alarms) to snooze the alarm or manually activate or deactivate its operational mode, through the shortcut menu. In the case of a virtual alarm, the selected mode will be applied to all of the constituent sub-alarms.

Alarm Propagation & Operational Modes

The following cases describe how a system could behave upon activation of an operational mode, depending on the logic table used by the virtual alarm.

Example: Sub-alarm is 'In maintenance' (or 'Offline'), overall status green

The status icon for the sub-alarm will appear in a darker shade and the status will be propagated to the overall (virtual) alarm. The status icon for the overall alarm will be shaded accordingly.

Example: Sub-alarm is 'In maintenance' (or 'Offline'), overall status red

The status icon for the sub-alarm will appear in a darker shade and the status will be propagated to the overall alarm. If there is another red sub-alarm, the overall alarm will stay red. Otherwise, the overall alarm will reflect the state of the sub-alarm that is in maintenance mode.

Example: Overall (virtual) alarm is 'In maintenance' (or 'Offline')

When an overall alarm is set to maintenance mode, all of its constituent sub-alarms are also set to maintenance mode and their status icons are shaded accordingly.

Operational Modes for Maintenance Purposes

As discussed in the section on Alarm Modes, operational modes allow you to suppress alarms so that operators are not distracted unnecessarily. It is possible, however, to set the view in **iC Navigator** and **iC Web** so that, even if alarms are in an operational mode, their actual status is displayed. We refer to this as the application's operational mode.

In a typical scenario, a technician wanting to make repairs on a device being monitored would manually enable the In maintenance operational mode for the corresponding alarms (to prevent operators from seeing a sudden flood of alarms on their iC Web pages). The technician could then start a separate iControl session, where he could set the operational mode of the iControl application (e.g., iC Web) to reveal the actual status of these alarms. With the repairs completed, the technician would then be able to verify that these alarms had returned to normal status before manually taking them out of the In maintenance operational mode.

Once a technician has configured iControl to filter alarms based on their operational modes, alarms are selectively displayed according to the following system behaviors:

See also

For more information, see:

- Configuring iControl Web to View Alarms with Specific Operational Modes on page 366
- Configuring iC Navigator to View Alarms with Specific Operational Modes on page 367

System Behaviors After Configuring the Display Settings of Alarms

IMPORTANT: If an operational mode view in iC Navigator is not specified and you turn on the Offline or In Maintenance operational modes for a specific incident in **Incident Log Viewer**, this incident is immediately hidden in **Incident Log Viewer**.

GSM Alarm Browser Behaviors After Configuring Display Setting of Alarms

In the GSM Alarm Browser, the following behaviors occur:

Scenario	Alarm icon color	Alarm text color
Scenario 1: • iControl is configured to display *Offline* alarms • Alarm operational mode is *Online* • Alarm status is one of *Critical*, *Major*, or *Minor*	Bright color	White
		
Scenario 2: • iControl is configured to display *Offline* alarms • Alarm operational mode is *Offline* • Alarm status is one of *Critical*, *Major,* or *Minor*	Bright color	Orange
		
Scenario 3: • iControl is **NOT** configured to display *Offline* alarms • Alarm operational mode is *Offline* • Alarm status is one of *Critical*, *Major,* or *Minor*	Dark color	Orange
		
Scenario 4: • Alarm operational mode is *Snooze* • Alarm status is one of *Critical*, *Major,* or *Minor*	Dark color	Orange
		

Note: This behavior occurs for alarms with an operational mode of *In Maintenance*, as well, provided the appropriate conditions are met (e.g., iControl is configured to display *In Maintenance* alarms and the operational mode for a given alarm is *In Maintenance*).

Incident Log Viewer Behavior After Configuring Display Setting of Alarms

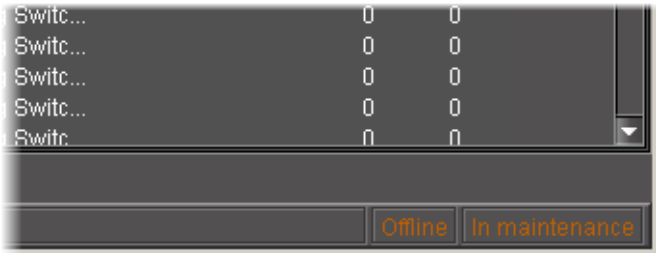
In **Incident Log Viewer**, the following behaviors occur:

Scenario	Alarm icon color	Alarm text color
Scenario 1: • iControl is configured to display *Offline* alarms • Alarm operational mode is *Online* • an incident trigger has occurred	Bright color	White
Scenario 2: • iControl is configured to display *Offline* alarms • Alarm operational mode is *Offline* • an incident trigger has occurred	Bright color	Orange
Scenario 3: • iControl is **NOT** configured to display *Offline* alarms • Alarm operational mode is *Offline* • an incident trigger has occurred	Incident is not visible	
Scenario 4: • Alarm operational mode is *Snooze* • an incident trigger has occurred	Incident is not visible	

> **Note:** This behavior occurs for alarms with an operational mode of *In Maintenance*, as well, provided the appropriate conditions are met (e.g., iControl is configured to display *In Maintenance* alarms and the operational mode for a given alarm is *In Maintenance*).

Main iC Navigator Behavior After Configuring Display Setting of Alarms

In the main iC Navigator window, if iControl is configured to display *Offline* alarms, the *Offline* indicator appears in the bottom, right corner. The same applies for the *In Maintenance* operational mode.



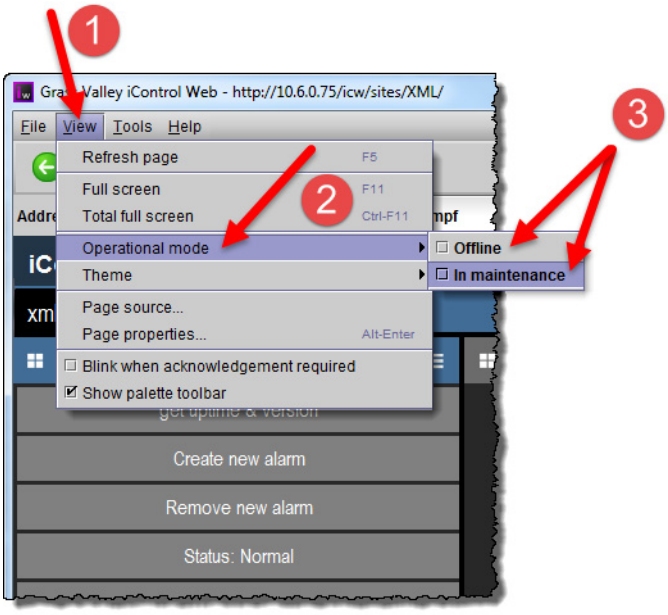
Configuring iControl Web to View Alarms with Specific Operational Modes

REQUIREMENT

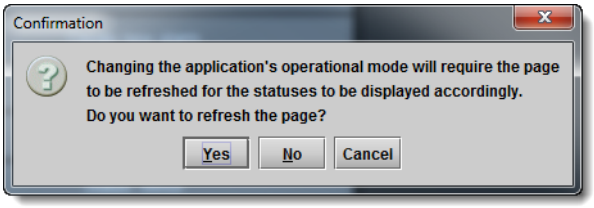
Before beginning this procedure, make sure you are already logged in to the required **iC Web** site (see page 718).

To set the view of an operational mode in iC Web

1. On the **View** menu of the **iC Web** browser, point to **Operational mode**, and then click **In maintenance** or **Offline**, or both, as required.



SYSTEM RESPONSE: A confirmation window appears.



2. Click **Yes**.

SYSTEM RESPONSE: The page reloads and all alarms currently in *In maintenance* mode (or *Offline*, or both, depending on what you specified in step 1) will reveal their actual status (e.g., alarms that were dark red will appear red). The words `In maintenance` (or `Offline`, or both) will appear at the right side of the status bar.

Note: An operational mode view only applies *for the particular client session* where it was enabled. The view of other users remains unaffected.

Configuring iC Navigator to View Alarms with Specific Operational Modes

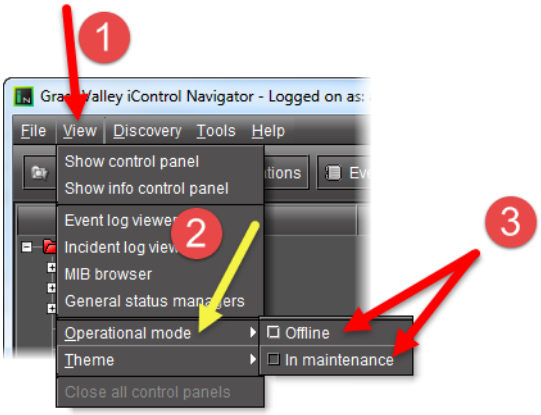
REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To set the view of an operational mode in iC Navigator

- On the **View** menu of iC Navigator, point to **Operational mode**, and then click **Offline** or **In maintenance** (or both) as required:

  There are several different system behaviors that occur depending on how you have configured iControl to display alarms.



IMPORTANT: System behavior

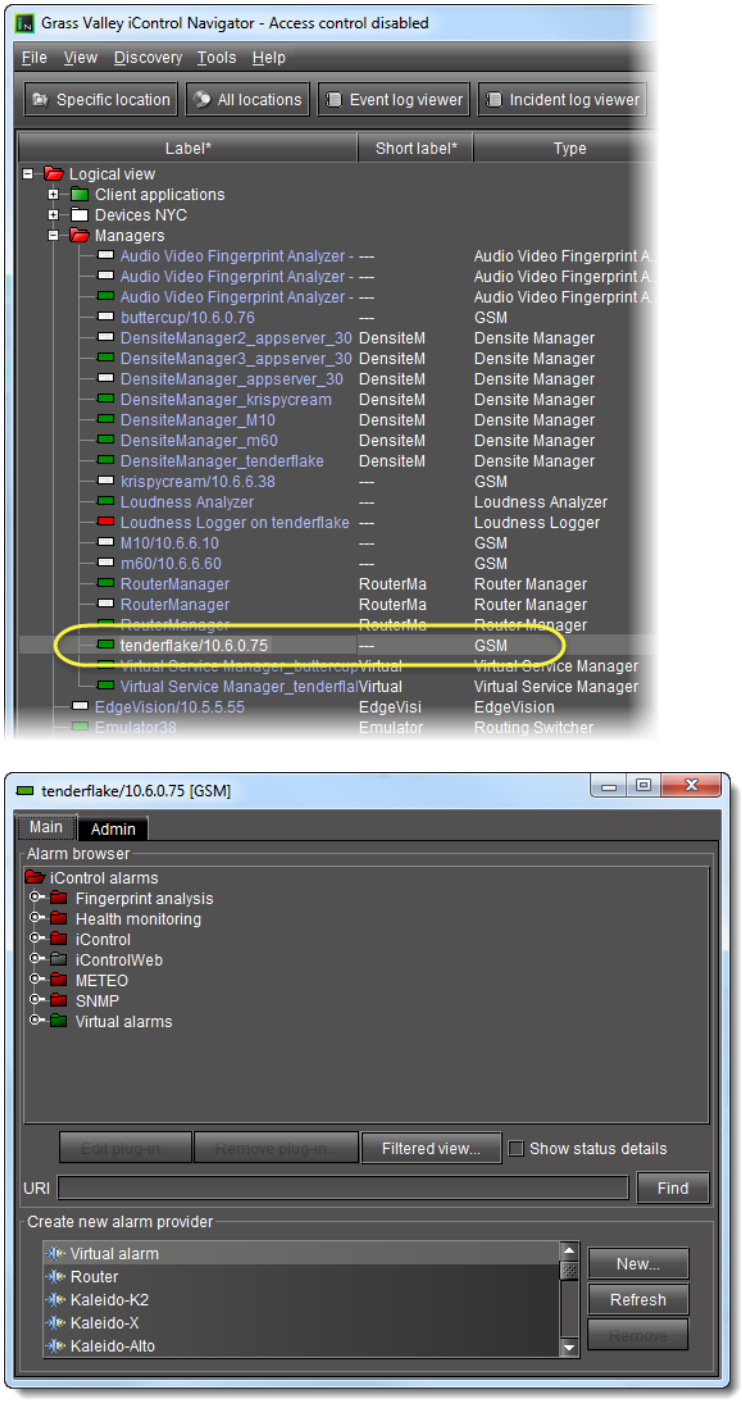
An operational mode view only applies for the particular client session where it was enabled. The view of other users remains unaffected.

See also

For more information about system behaviors after you have configured iControl to display alarms based on their operational modes, see System Behaviors After Configuring the Display Settings of Alarms, on page 364.

Alarm Browser

The Alarm Browser is a window, accessible from within iC Navigator and elsewhere, used to view, create, modify and remove alarms. It provides access to alarms for both Grass Valley and third party devices. The information that appears in the Alarm Browser is generated by a specific GSM.



GSM Alarm browser

Note: Technically, the window that opens when you double-click on a GSM, or choose **General status managers** from the **View** menu, is the control panel for the GSM, of which the Alarm Browser is just one component. By convention, however, we tend to refer to this window as the *GSM Alarm Browser*, or simply the *Alarm Browser*.

The **Main** tab of the *Alarm Browser* displays a hierarchical view of all the alarms that have been discovered by the GSM. The alarms are organized into folders. The current state of each alarm is shown as an icon next to its name. These states are dynamically updated.

If the **Edit plug-in** and **Remove plug-in** buttons become enabled when you select an alarm in the *Alarm Browser*, it means that you can edit the properties of the alarm provider plug-in that provides this alarm, or remove the plug-in instance altogether. Be careful when using these buttons, however—some plug-ins are responsible for multiple alarms, so that changes may have an impact beyond the currently selected alarm.

Note: In the case of an SNMP plug-in, the **SNMP Plug-in Configuration** window allows you to enable the SNMP version 3 protocol (as opposed to the default version 2c protocol). If you choose the SNMP version 3 option, you must know:

- the user ID
- the authentication password
- the authentication protocol
- the privacy password
- the privacy protocol

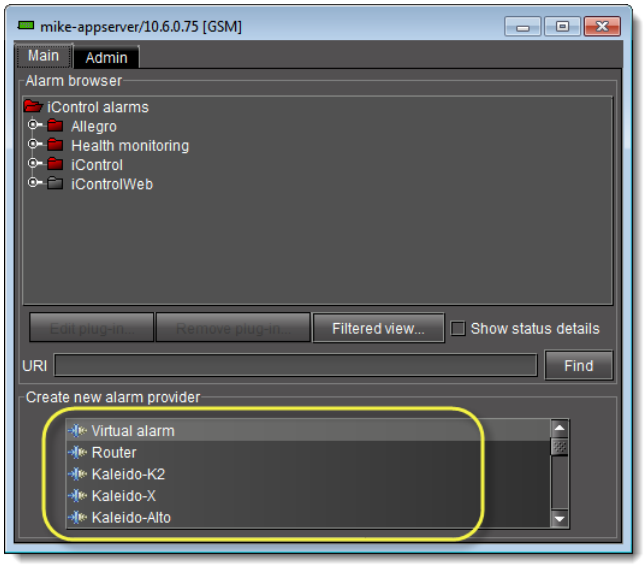
This information is configured on the remote SNMP Manager polling this Application Server. See your network administrator for more information.

The **Refresh** button is disabled until the *Alarm Browser* hierarchy changes on the server in a way that would affect the current display—for example, when a new folder is created.

Alarm Providers

An alarm provider is a small program responsible for publishing alarm data. Alarm providers are based on plug-ins—a kind of software template. The provider is like a clone of the plug-in, but it is customized to work with a specific device (e.g., the Kaleido-Alto at IP `10.10.50.3`), or a specific category of devices (e.g., routers).

Some alarm providers are built right into the core of the iControl system. Others can be created as required from the *GSM Alarm Browser* window. These include alarm providers for video routers, Kaleido frames, GPI inputs, iTX, VBI, UMD and various third party SNMP devices.



List of alarm providers (plug-ins) in a GSM Alarm Browser

When you create a new alarm provider, an instance of the plug-in starts running on the Application Server, and begins publishing its alarms to the GSM. There are two types of alarm providers: single instance and multiple instance.

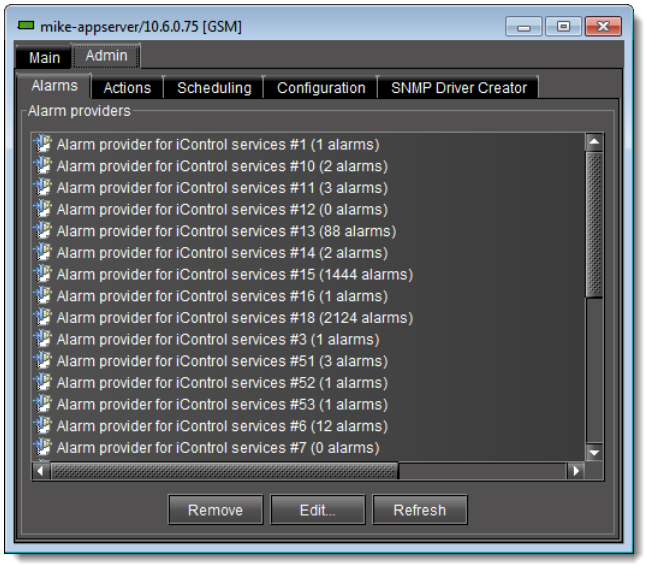
Single-instance Alarm Providers

For certain plug-ins, once an instance has been created on the Application Server, the plug-in name is removed from the list of alarm providers. An example of a single-instance plug-in is the *Router* plug-in, since only one instance is required to monitor all the routers on a local network.

Multiple-instance Alarm Providers

Most alarm provider plug-ins can have multiple instances, each monitoring a specific device on a network. For example, multiple instances of the Kaleido plug-in might be running simultaneously, each one assigned to a different Kaleido frame. Another example is virtual alarms—every virtual alarm is an instance of the virtual alarm plug-in.

A list of currently active alarm providers can by viewed in the **Admin** > **Alarms** tab of the GSM Alarm Browser.



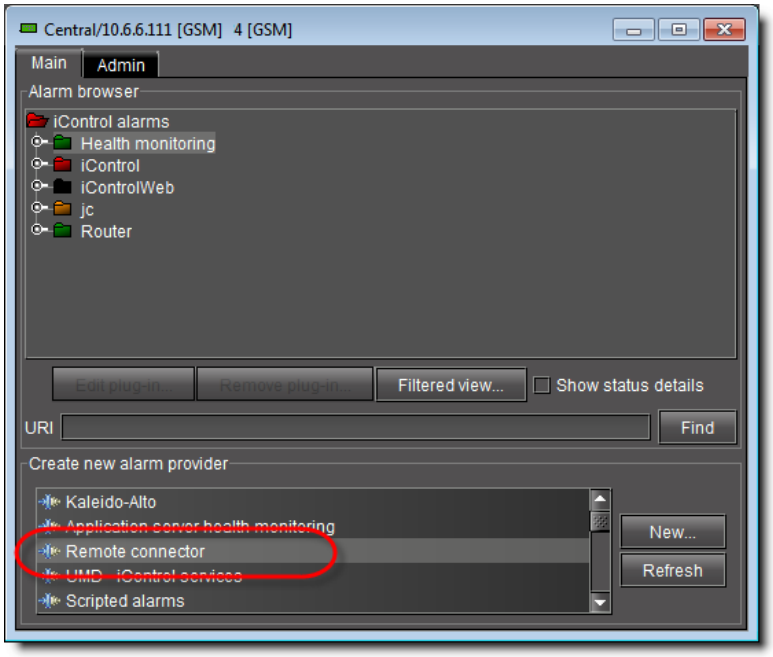
Default vs. Optional Plug-ins

Some alarm provider plug-ins are included in every iControl system. Others are available as options. The table below provides an overview of some common plug-ins. For a more complete list, please refer to the *iControl Third Party Device Support* document, available from the *Startup* page of your Application Server.

Plug-in Name	Type	Instance	Plug-in Description	Availability
App Server Health Monitoring	SNMP	Multiple	Enables monitoring of alarms from iControl Application Server	Basic
Kaleido Alto	SNMP	Multiple	Enables monitoring of alarms from Kaleido-Quad/Alto	Option
Kaleido K2	SNMP	Multiple	Enables monitoring of alarms from Kaleido-X	Option
Network reachability	GSM	Single		Option
Router	GSM	Single	Enables monitoring of serial routers; provides the status of all crosspoints as pseudo-alarms	Basic
Scripted alarms	GSM	Multiple		Option
SNMP Generic manager	GSM	Multiple		Option
SNMP sysUpTime manager	GSM	Single		Option
UMD iControl services	GSM	Single		Option
VBI iControl services	GSM	Single		Option
Virtual alarm	GSM	Multiple	Enables monitoring of virtual alarms	Basic

Remote Connector Alarm Providers

There may be occasions when you would like a device to be able to initiate connections with iControl and autonomously send requests to it in a language-independent and standardized way. It is possible to achieve this type of device-GSM relationship using the *Remote Connector* plug-in in the GSM Alarm Browser.



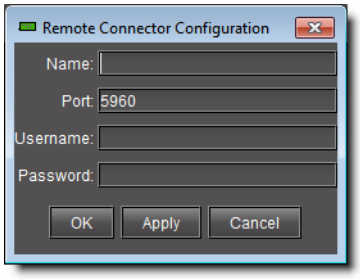
The *Remote Connector* plug-in connects a device (one that supports the Connector protocol) to the GSM via XML. Once configured, the device should begin publishing alarms to the GSM in the same fashion as other GSM alarms.

One instance of the Remote Connector plug-in is the iTX alarm provider. iControl automatically creates an iTX instance, assigning it port 5959. This instance is available for you to use, or, alternatively, you may choose to create another instance of the Remote Connector plug-in. The latter may be desirable, for example, if you would like to specify a particular port to use.

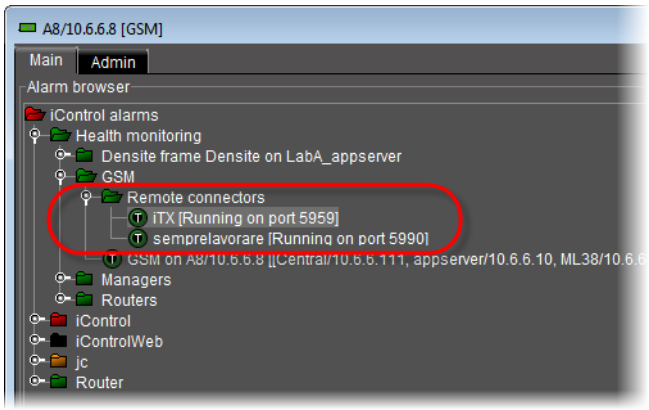
IMPORTANT: Make sure each instance of an alarm plug-in has a unique name

Each instance of an alarm plug-in must have a unique name.

When configuring a new Remote Connector plug-in instance, iControl asks you for a name and port. You may optionally also provide a user name and password, as applicable.



All Remote Connector instances appear as alarms in the `Remote connectors` sub-folder of the `GSM` folder.



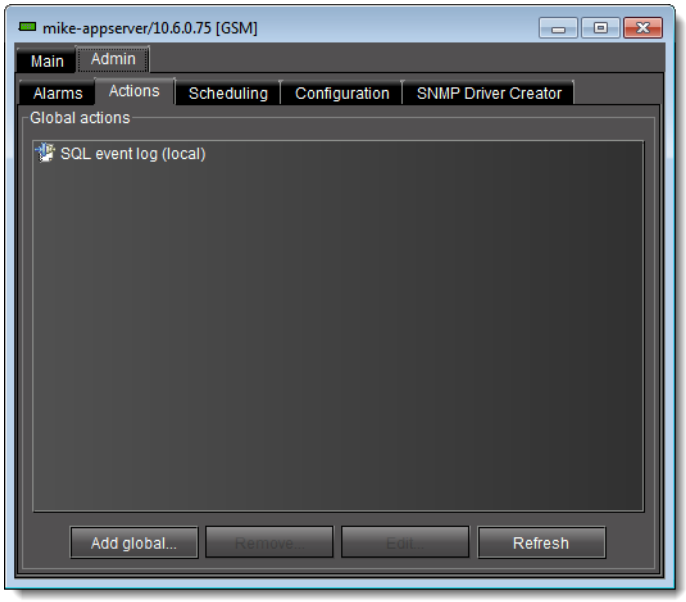
Alarm Consumers

Alarm consumers are actions that are triggered when specific alarms occur. For example, an alarm consumer might send an e-mail to a supervisor when a certain alarm turns red. Like alarm providers, alarm consumers are based on *plug-ins*.

Alarm consumers can trigger a variety of actions, including:

- logging an event to a database
- enabling the GSM to act as an SNMP agent
- sending SNMP traps
- sending an e-mail or SMS message
- activating a GPI output
- launching a script
- switching a router crosspoint

Alarm consumers are often referred to in iControl as *actions*, and are managed via the **Admin** > **Actions** tab of the *GSM Alarm Browser*.



Some alarm consumer plug-ins are included in every iControl system. Others are available as options. The table below provides an overview of some common plug-ins.

Plug-in Name	Type	Instance	Plug-in Description	Availability
Event and incident log	GSM	--		Option
GPI VNODE relay	GSM	--		Option
Scripted action	GSM	--		Option
Send email	GSM	--	Enables iControl to send e-mail messages (SMTP) in response to an alarm	Option
SNMP agent	GSM	Single	Enables the GSM to act as an SNMP agent	Option
SNMP trap sender	GSM	Multiple	Enables the GSM to send SNMP traps (based on any GSM alarm) to a third party manager	Option

Global Actions vs. Specific Actions

Alarm consumer actions can be either *specific* to an individual alarm, or *global*.

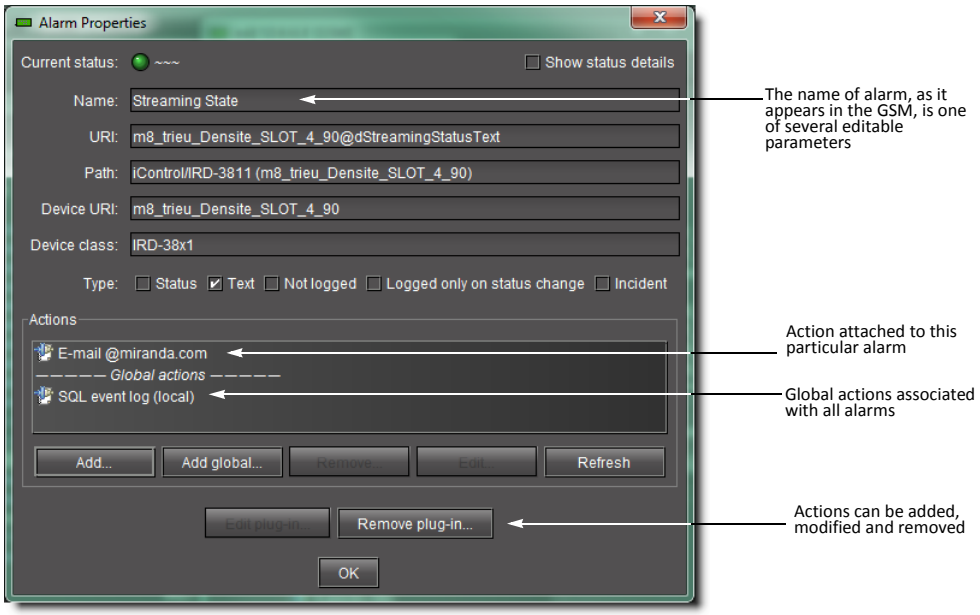
Global actions are associated with, and can be triggered by, every alarm in the system. For example, the *SQL event log* plug-in is normally used to create a global action that causes every alarm event to be logged to a database on the Application Server. When new alarms are added, any global actions in effect will apply to them as well.

Specific actions can apply to one or several alarms. For example, you can apply a `Send e-mail` action to the `Disk used space (%)` alarm, so when that alarm is triggered, an e-mail is sent automatically to a system administrator. The same action could similarly be applied to a range of health monitoring alarms, with an e-mail being sent if any of them is triggered.

Alarm consumers (actions) are created via the GSM Alarm Browser window. They can also be created by scripts using the `addAction()` function.

Alarm Properties

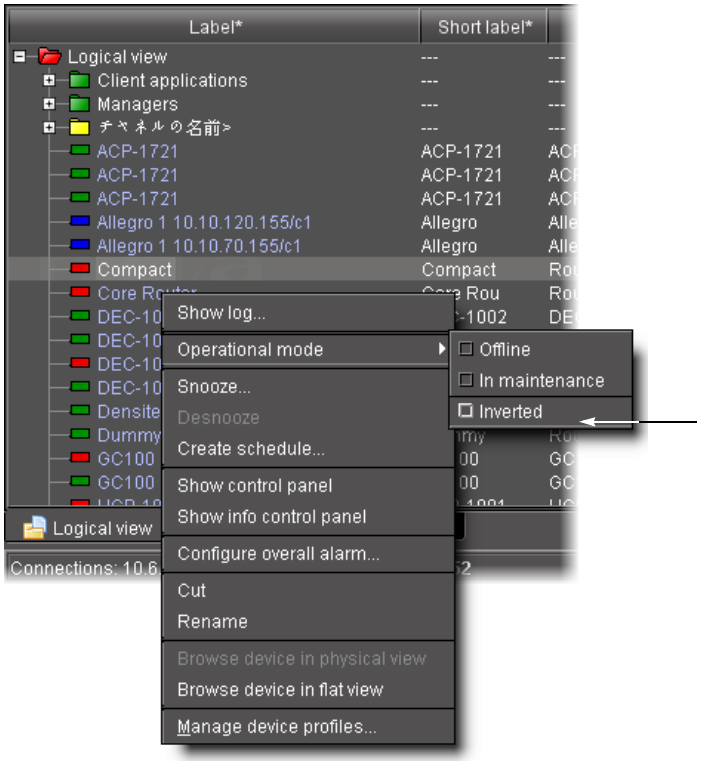
Parameters associated with an alarm, such as its name and URI, can be viewed and modified via the **Alarm Properties** window, which can be accessed by right-clicking on any alarm in the Alarm Browser. This window can also be used to attach, remove, or modify the actions associated with an alarm.



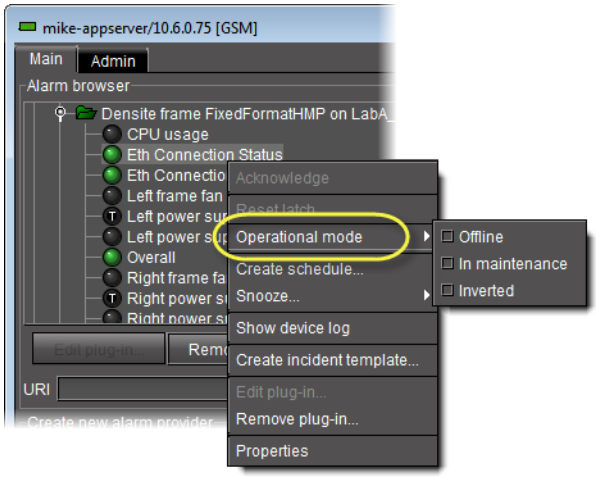
Manual Alarm Inversions

You can invert an alarm manually and instantaneously within iC Navigator and iC Web through the context menus of:

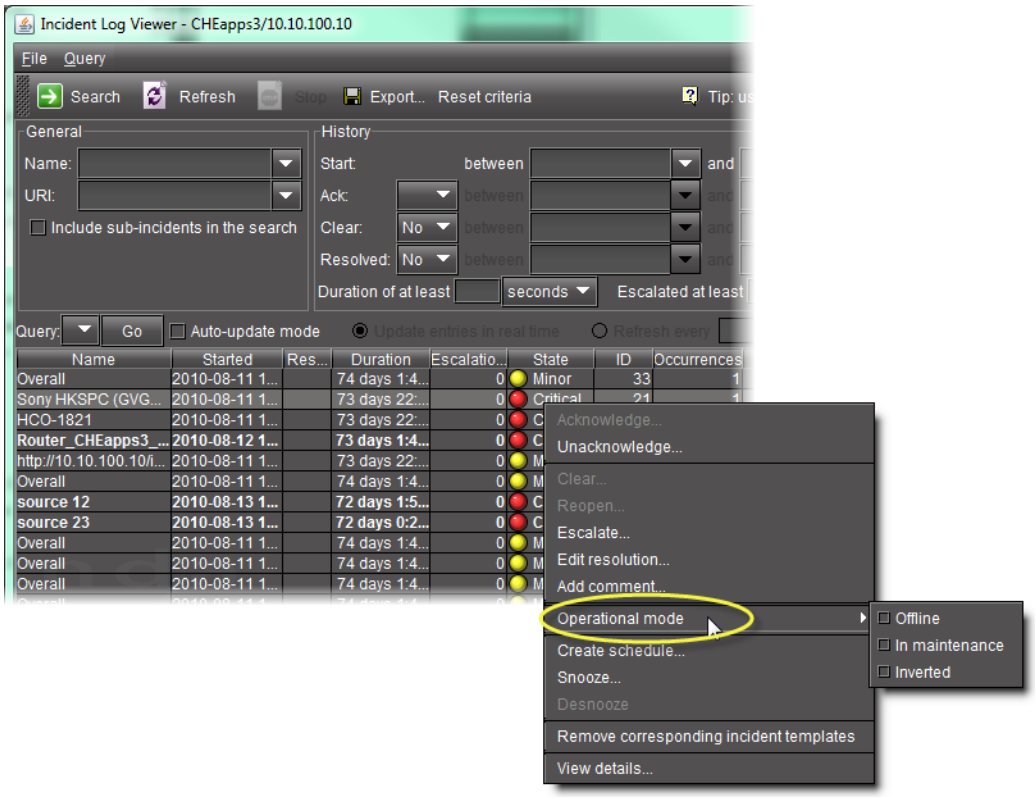
- the main Navigator window
- the GSM Alarm Browser
- **Incident Log Viewer**
- the alarm status icons in iC Web



Example of setting operational mode for an alarm in iC Navigator's main window



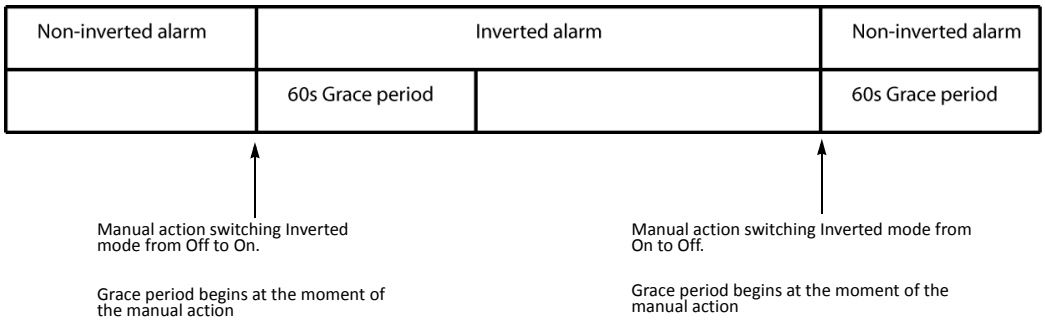
Example of setting operational mode for an alarm in the GSM Alarm Browser



Example of setting operational mode for an alarm in Incident Log Viewer

As with scheduled alarm inversions, the concept of the Grace period exists with manual inversions. However, for manual inversions, there is only one Grace period and it begins exactly when the inversion action takes place. When you are ready to manually change the Inverted mode of an alarm back to *Off*, the *Grace* period for this action begins at the moment of the manual action.

> **Note:** The default Grace period for manual inversions is 0 seconds.



Manual alarm inversion example with 60s Grace period

IMPORTANT: If your network is configured to report alarms to multiple GSMs, it is recommended that you configure the same Grace period duration for manual inversions among all GSMs. Similarly, it is recommended in this case that you configure the same Grace period duration for scheduled inversions among all GSMs.

See also

For more information about:

- the *Inverted* operational mode, see Inverted, on page 359.
- Manual inversion actions, see Manual Alarm Inversions and Inverting Alarms Manually on page 416.
- Scheduling inversion actions, see Alarm Inversion Scheduling and Setting a Schedule for an Alarm Inversion on page 421.

Alarm Scheduling

iControl includes tools to schedule alarm suppression on a per-channel and per-alarm basis. The objective of alarm scheduling is to provide the means to configure an iControl system in order to suppress generation of alarms according to a schedule.

In some situations, normal events in the network would be reported as errors by iControl. Operators now have the ability to schedule certain alarms not to be generated during specific periods of the day.

- Some TV channels only broadcast during a certain period of the day. Outside of the regular broadcast period, the signals consist, for example, of a slate with music. Instead of reporting a "signal freeze" alarm during these periods, iControl can suppress the reporting of "freeze" alarms, while continuing to report alarms for video black and audio silence.
- Some broadcasters perform a sign-off at the end of the broadcast day. Many signals monitored by iControl therefore switch to an invalid format. Because sign-off is a normal, and predictable, event, it is useful for iControl operators to configure their system for alarms to be automatically suppressed during specified periods, and revert to their normal behavior outside of those periods.

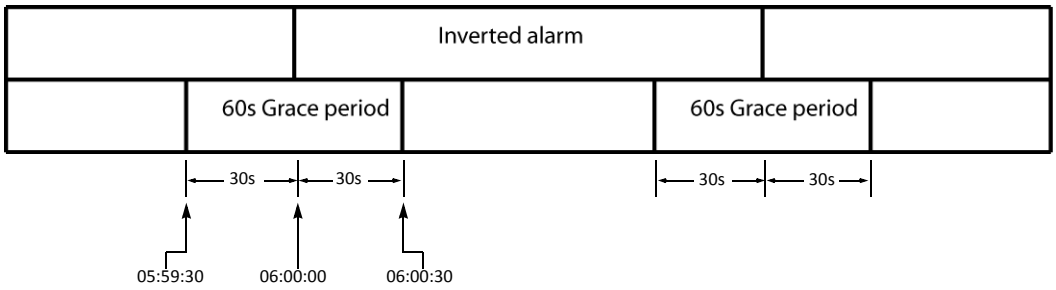
Operational modes can be enabled manually or based on a schedule with the exception of the snooze mode which can only be enabled manually. Alarm suppression changes the operational mode of an alarm for a certain period of time.

Alarm Inversion Scheduling

You can schedule an alarm inversion action (switching to *On* or to *Off*). When you schedule an inversion action, you configure the system to change the *Inverted* mode at a set time and then to switch back at another set time. Scheduled inversion actions occur during a *Grace period*. The purpose of the Grace period is to provide a buffer span of time during which the alarm state is ignored. Without a Grace period the following scenario could happen: If a channel goes off-air at 02:00 and there is a scheduled inversion changing a Freeze alarm to Non-freeze at 02:00, but the feed doesn't stop until five seconds later, the Non-freeze alarm will go red for

five seconds and may trigger unwarranted actions. A Grace period ignores these transitional alarm states and prevents unwanted behaviors.

Each scheduled inversion action (either switching to *On* or to *Off*) occurs exactly at the midway point of a Grace period. For example, if we assume the Grace period is set to 60s, and there is an alarm inversion scheduled for 06:00, a Grace period will begin at 05:59:30 and end at 06:00:30. During this Grace period, the alarm's state is ignored.



Scheduled alarm inversion example with 60s Grace period and a set inversion duration

IMPORTANT: If your network is configured to report alarms to multiple GSMs, it is recommended that you configure the same Grace period duration for manual inversions among all GSMs. Similarly, it is recommended in this case that you configure the same Grace period duration for scheduled inversions among all GSMs.

When you configure a scheduled alarm inversion, you can choose whether to configure a set duration during which the alarm is inverted. If a scheduled alarm inversion action does not have a set duration, only the first Grace period (the one in which the alarm becomes inverted) applies. Scheduled alarm inversions with no set duration require an operator to manually switch the Inverted mode of an alarm back to *Off*.

Note: The default Grace period is 60 seconds.

IMPORTANT: System behavior

- Because an inversion action occurs at exactly the midway point within a Grace period, a scheduled inversion duration cannot be shorter than the Grace period. Otherwise, the 'beginning' and 'end' Grace periods would overlap one another.
- For a scheduled inversion **with** a set duration, the maximum duration of the inversion is 24 hours minus the configured Grace period.
- For a scheduled inversion **without** a set duration, the maximum duration of the inversion is 24 hours minus **half** the configured Grace period.

See also

For more information about:

- the *Inverted* operational mode, see Inverted, on page 359.

See also (*Continued*)

For more information about:

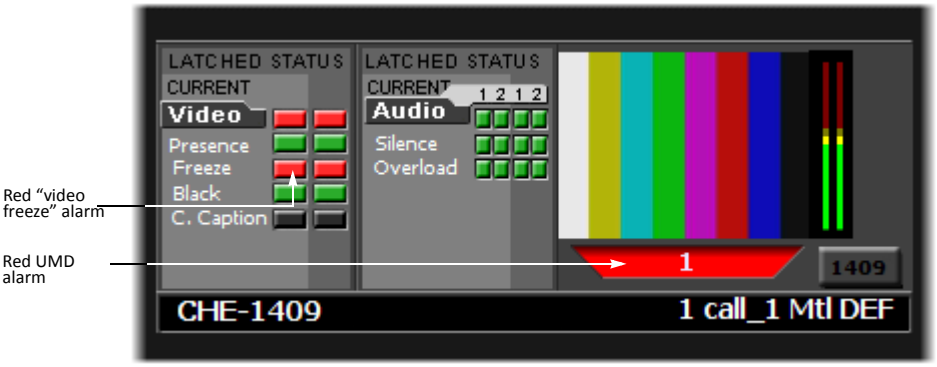
- Manual alarm inversions, see Manual Alarm Inversions and Inverting Alarms Manually on page 416.
- Scheduling inversion actions, see Setting a Schedule for an Alarm Inversion, on page 421.

Alarm Suppression

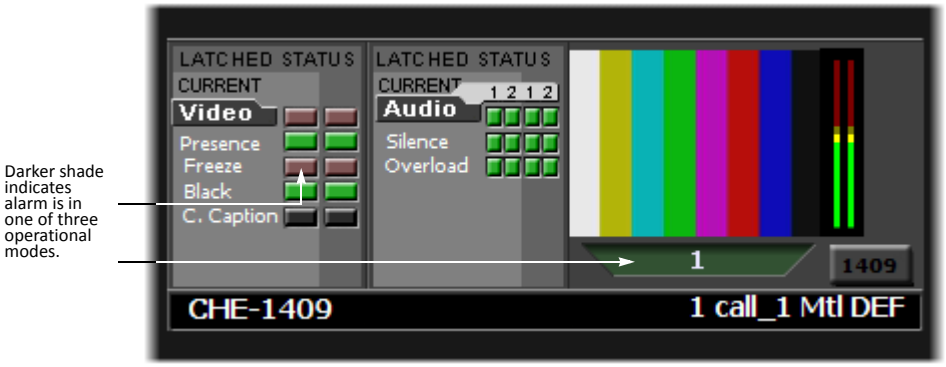
iControl can be configured to automatically suppress the generation of certain signal alarms for specific periods of time, and then to automatically revert back to its normal alarm-generation behavior to match the expected behavior of particular channels.

For example, if channel 1409 is known to sign off at 2:00 a.m. and to resume normal programming at 6:00 a.m., operators may find that iControl distracts their attention by reporting alarms due to the presence of the color bars and audio tone that are broadcast during the night.

With an iControl system not configured for alarm scheduling, the color bars and audio tone would continuously generate alarm states on channel 1409, which would keep being reported as invalid signals in the iC Web user interface. Notice the red status icons and red UMD in the image below.



As shown below, once alarm scheduling is configured in iControl, the generation of video freeze alarms for channel 1409 will be suppressed every day from 2:00 a.m. to 6.00 a.m., while the other signal parameters, such as video presence and video black, are still verified. During the alarm suppression period, the overall status of the signal remains valid, and none of the video freeze status icons for channel 1409 turns red.

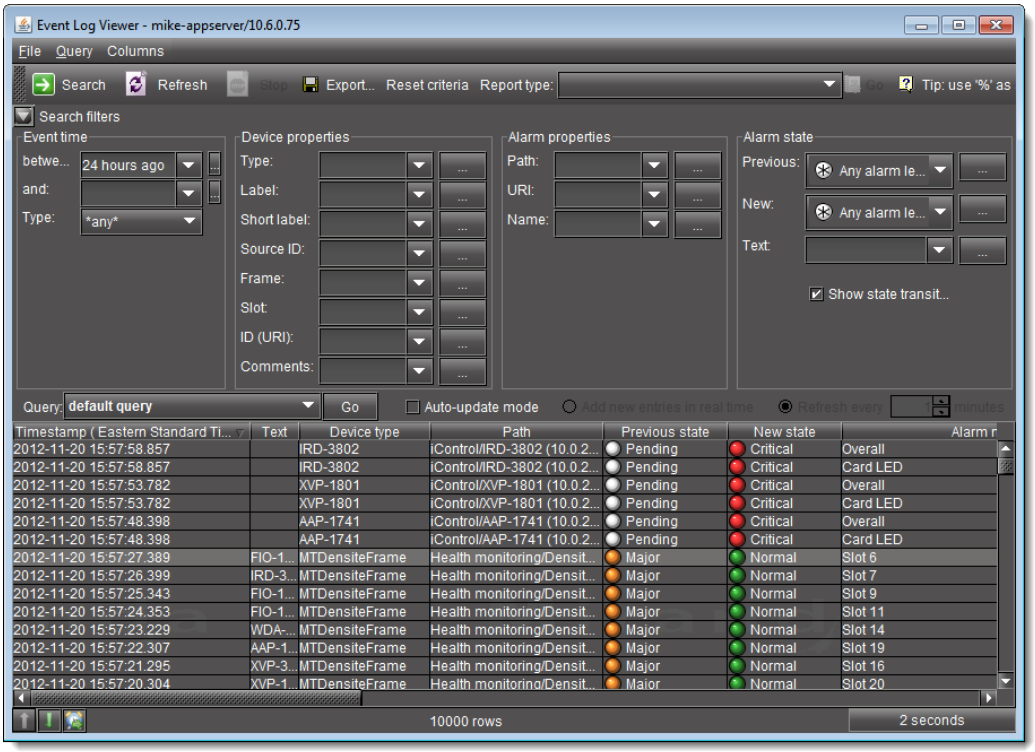


Instead, the status icons representing detailed alarms appear in a darker shade of green or red to indicate that the alarm is suppressed. The real status is thus still visible, but in a non-obtrusive way.

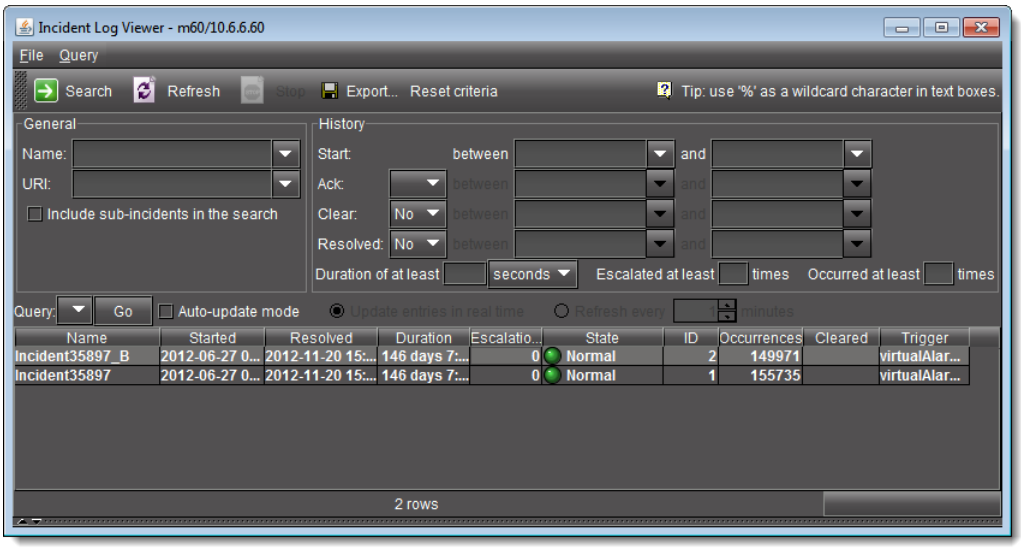
Log Viewer

Each iControl Application Server maintains a database of log entries, providing a historical record of system activities that can assist in tracking problems. There are three viewers built into iC Navigator that allow you to access the log database:

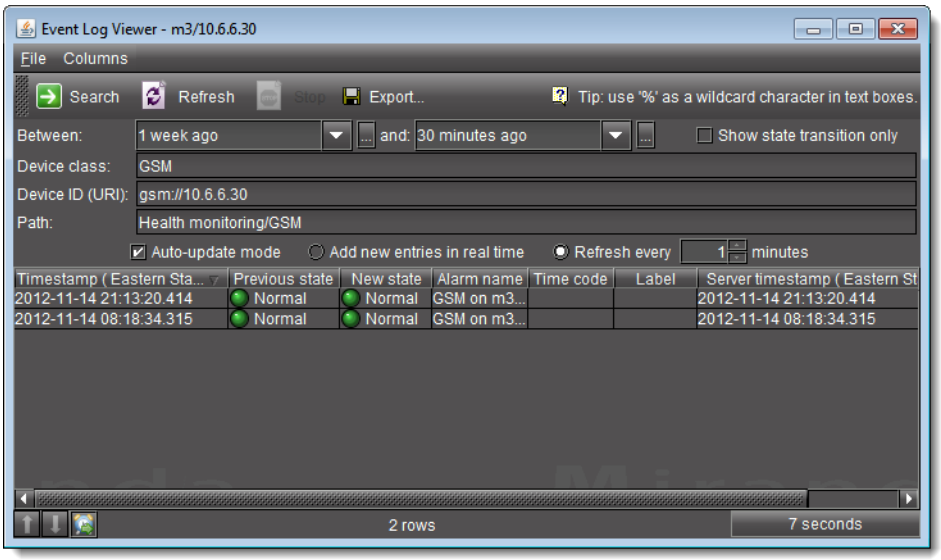
- **Event Log Viewer** allows you to perform simple searches and elaborate queries on all entries in the log database. To open this viewer, choose **Event log viewer** from the **View** menu.



- **Incident Log Viewer** allows you to perform simple searches and elaborate queries on incidents, which are log entries that have been filtered according to a pre-defined relationship. To open this viewer, choose **Incident log viewer** from the **View** menu



- The in-context log viewer allows you to quickly view and search the log entries associated with a specific device. To open this viewer, right-click on a device in iC Navigator and choose **Show log** from the drop-down menu.



Note: While all three log viewers are accessible from within iC Navigator, your iControl configuration may also include Web pages that contain embedded versions of these viewers.

Detailed Directions

Viewing Alarms on iControl Web Pages

iC Web pages provide a wealth of information, including alarm statuses for the devices and signals being monitored. Alarm statuses can be displayed on a Web page in a number of ways: in embedded versions of the GSM Alarm Browser or iC Navigator, in specific Web components such as alarm status panels, or even attached to Web graphic elements such as buttons or borders.

Viewing Alarms in iC Navigator

There are two ways of viewing alarms in iC Navigator. The main iC Navigator window displays overall alarms for all devices and services registered with iControl. The GSM Alarm Browser displays these overall alarms plus a detailed hierarchy of sub-alarms.

Viewing Alarms in iC Navigator's Main Page

REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To view alarms in iC Navigator

- In iC Navigator, click the **Physical view** or **Flat view** tabs to change the view (see Devices and Services Views in iC Navigator, on page 228).

  SYSTEM RESPONSE: The color of the device or device folder in the main iC Navigator window indicates the alarm status of that device or group of devices.

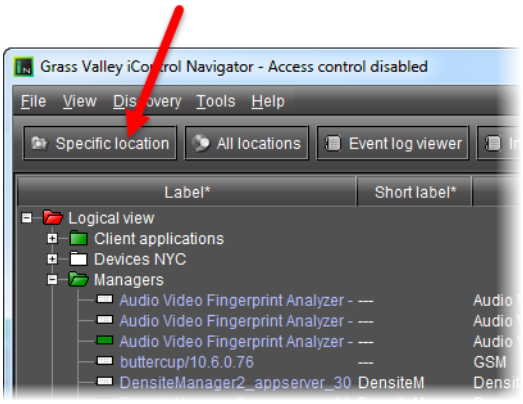
Viewing Alarms on Another Application Server

REQUIREMENT

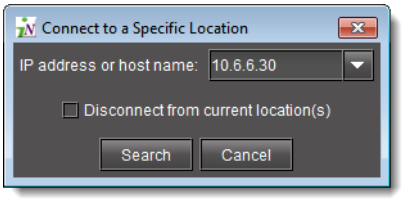
Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To view alarms on another Application Server

1. In iC Navigator, click **Specific location**.



System Response: The **Connect to a specific location** window appears.



2. Type the IP address of another Application Server, or choose one from the list.
3. Select or clear the **Disconnect from current location(s)** check box.

> **Note:** If this check box is selected, the devices/service currently displayed in iC Navigator will be replaced by those from the Application Server to which you are about to connect.

4. Click **Search**.

Viewing Alarms on All Available Application Servers

REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To view alarms on all available Application Servers

- Click **All locations**.

  System Response: iC Navigator contacts the iControl Application Servers registered on the Edit Service Locations page of the current Application Server (see Configuring Lookup Services, on page 53). After a few moments, iC Navigator will display devices and/or services from all Application Servers it discovers on the network. The IP addresses of the Application Servers will be displayed at the bottom of iC Navigator.

Viewing Alarms in the GSM Alarm Browser

The GSM Alarm Browser displays alarms and sub-alarms for every device and service associated with a given Application Server. Depending on your configuration, more than one GSM may be displayed in iC Navigator. The Alarm Browser can only display information for one GSM at a time.

See also

For more information about opening the GSM Alarm Browser, see page 710.

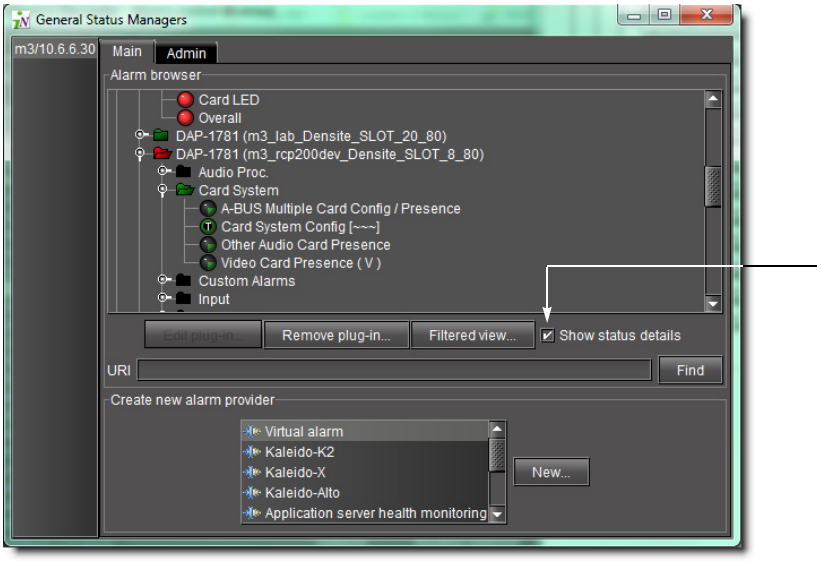
Enabling the Display of Alarm Acknowledgement for a Particular GSM Alarm Browser

REQUIREMENT

Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

To enable the display of alarm acknowledgement for a particular GSM Alarm Browser

- In the GSM Alarm Browser, select **Show status details**.



Note: Alarm acknowledgements are displayed immediately.

Adding Alarm Providers

To have an alarm appear in the *Alarm Browser* hierarchy, you must first add an appropriate alarm provider.

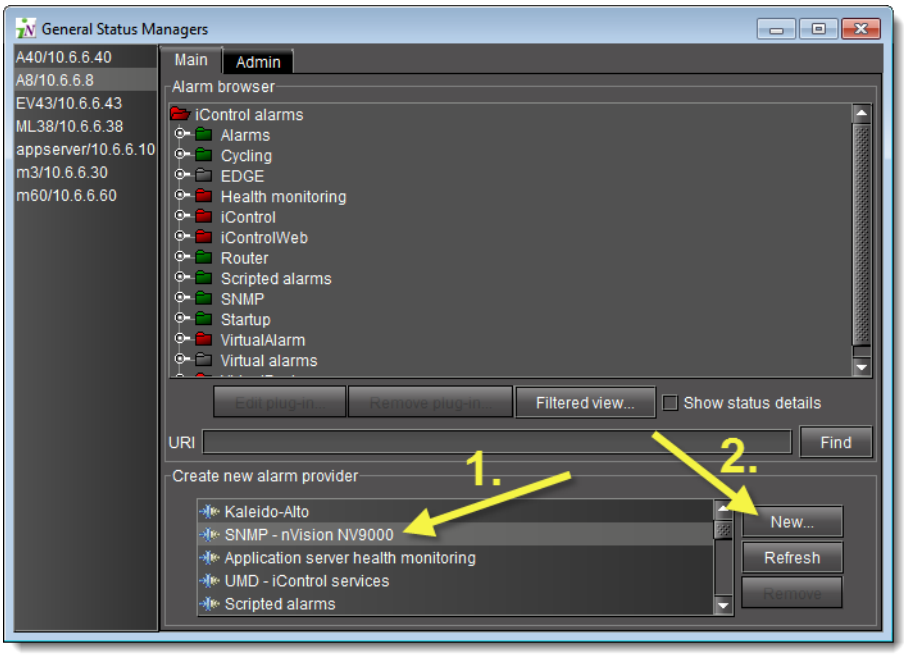
Note: When working with multi-instance plug-ins be careful not to create more than one plug-in for the same device.

REQUIREMENT

Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

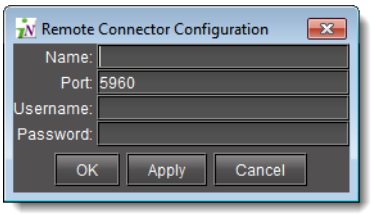
To add an alarm provider

1. In the GSM Alarm Browser, under **Create new alarm provider**, click an appropriate alarm provider type, and then click **New**.

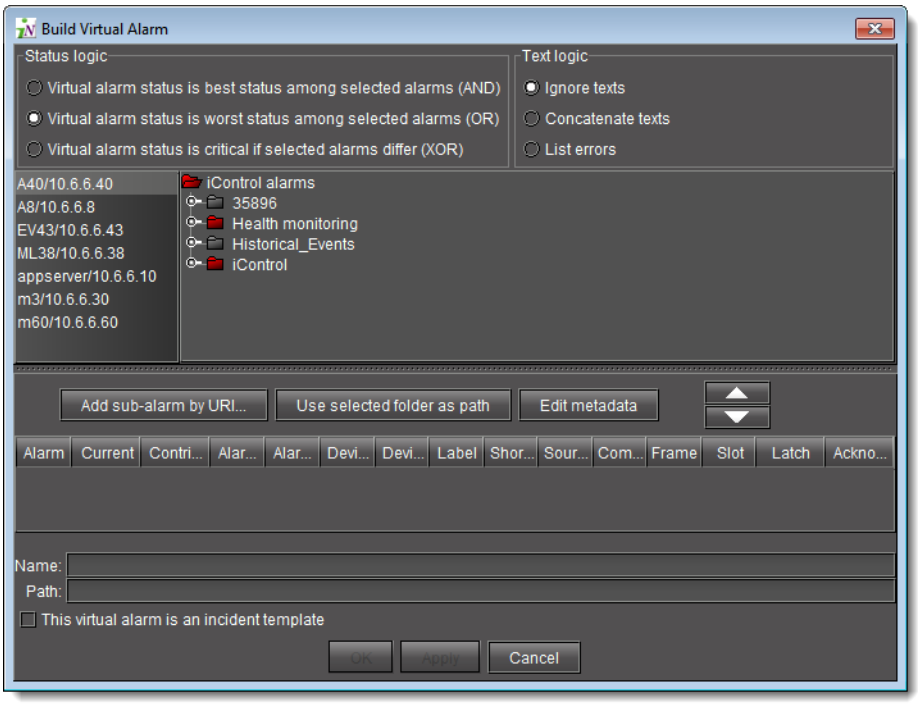


SYSTEM RESPONSE: A window appears allowing you to configure an instance of the alarm provider plug-in.

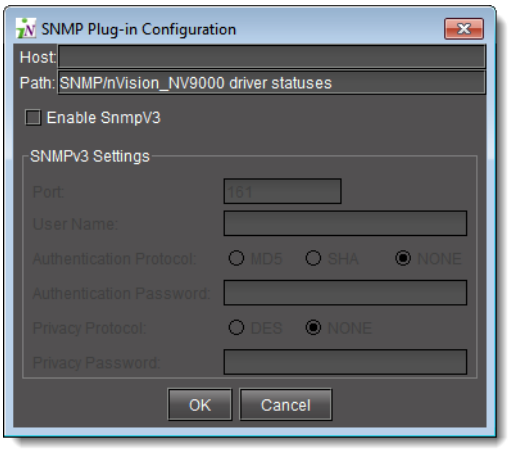
The contents of this window vary according to the type of alarm provider you have chosen.



Sample alarm provider configuration #1: Remote Connector Config



Sample alarm provider configuration #2: Virtual Alarm Config



Sample alarm provider configuration #3: SNMP Plug-in Instance Config

IMPORTANT: Important considerations for instantiating SNMP plug-ins

If you are creating an alarm provider using the SNMP plug-in and several conditions (below) are all true, you must choose either **SNMPv2c** or **SNMPv3** as the SNMP protocol. The above-mentioned conditions which must be met are:

- Your Application Server is running iControl version 7.00 or later.
- The device that will take on the role of SNMP agent supports the SNMPv3 protocol.

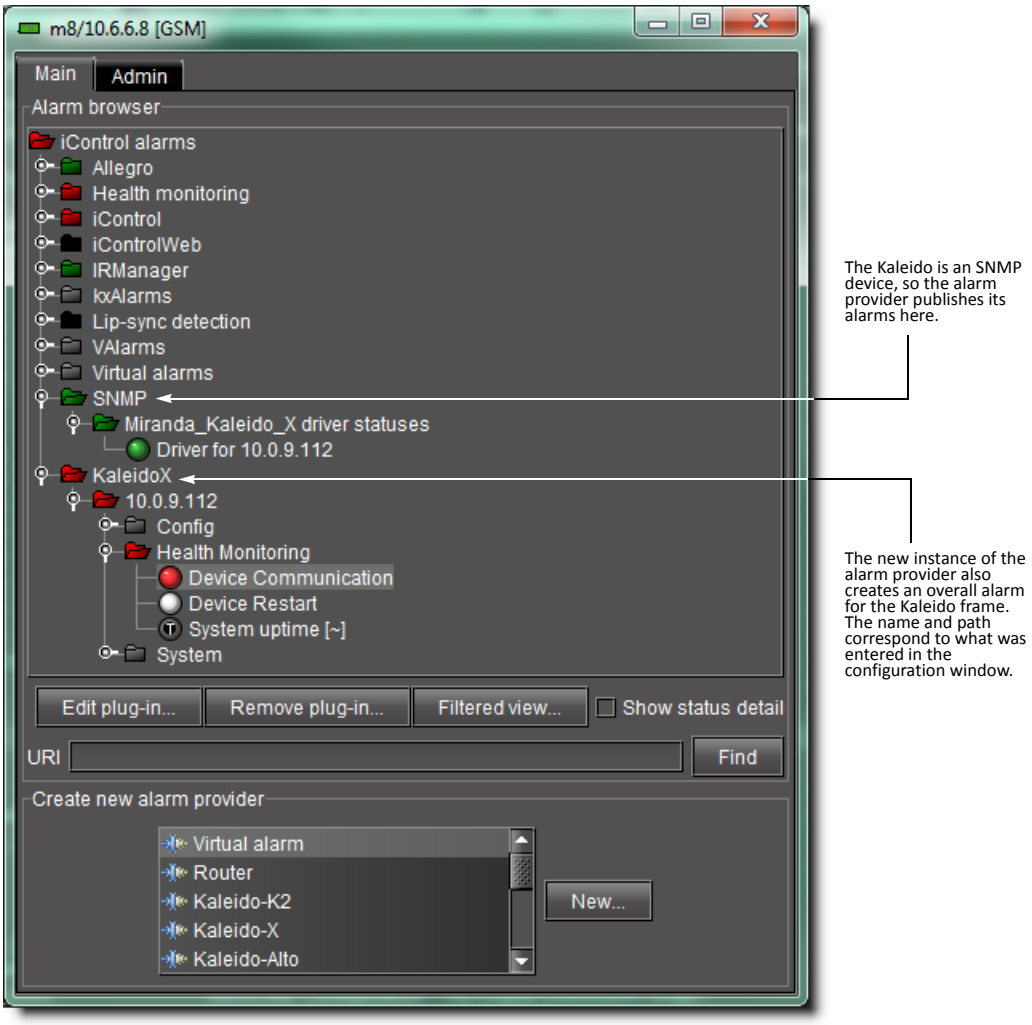
If either of these conditions are not met, the instantiated SNMP plug-in (the new alarm provider) necessarily defaults to using the SNMPv2c protocol.

If you choose SNMPv3, you must have available to you the user account information stored on the SNMP agent, namely the following:

- User name
- Authentication password
- Authentication protocol
- Privacy password
- Privacy protocol

2. Once you have finished typing configuration details, click **OK**.

   SYSTEM RESPONSE: A new instance of the alarm provider starts running as a process on the Application Server, and publishes one or more alarms (as defined by the plug-in) to the GSM. The alarms appear in the Alarm Browser, and, within a few moments, their statuses are updated to reflect the current condition of the device being monitored.



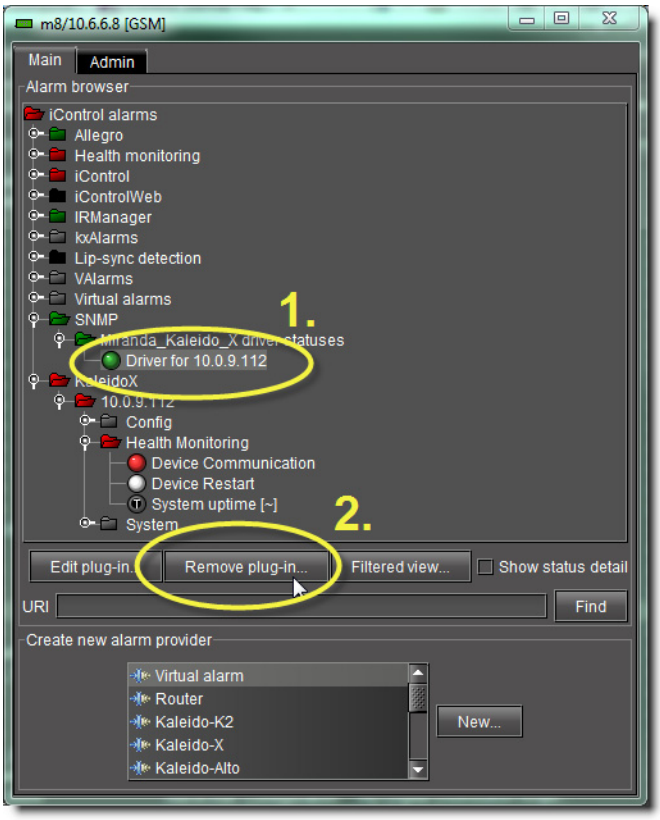
Removing Alarm Providers

REQUIREMENT

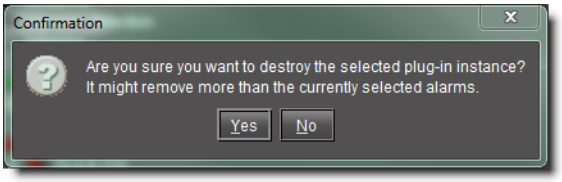
Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

To remove an alarm provider

1. In the GSM Alarm Browser, select the alarm provider to be removed, and then click **Remove plug-in**.



SYSTEM RESPONSE: A confirmation message appears.



2. Click **Yes** to remove the action.

Adding Alarm Consumers

Alarm consumers, or *actions*, can be either *global* or *specific*.

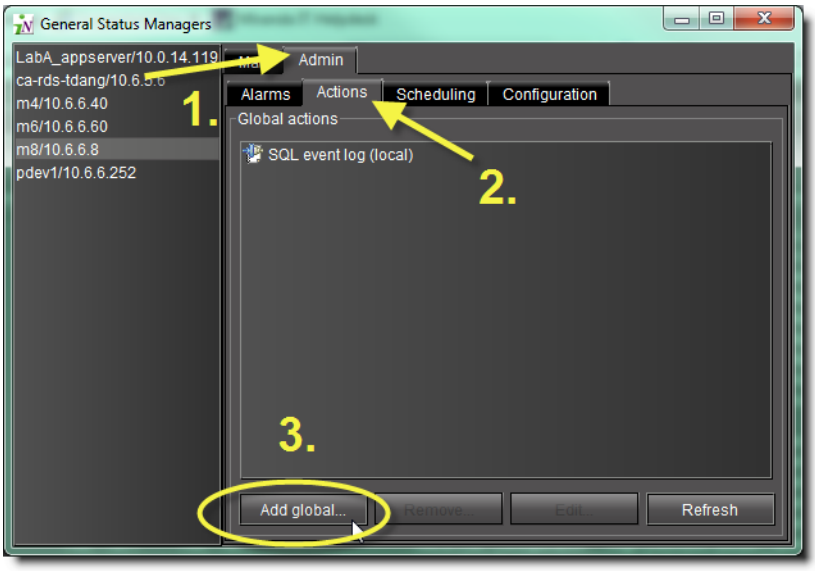
Adding a Global Action

REQUIREMENT

Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

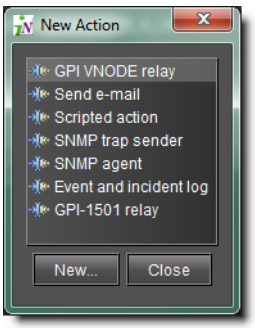
To add a global action

1. In the GSM Alarm Browser, click the **Admin** tab, and then click the **Actions** tab.



2. Click **Add global**.

   SYSTEM RESPONSE: The **New action** window appears.

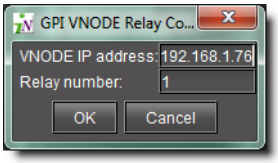


3. Choose an appropriate action.

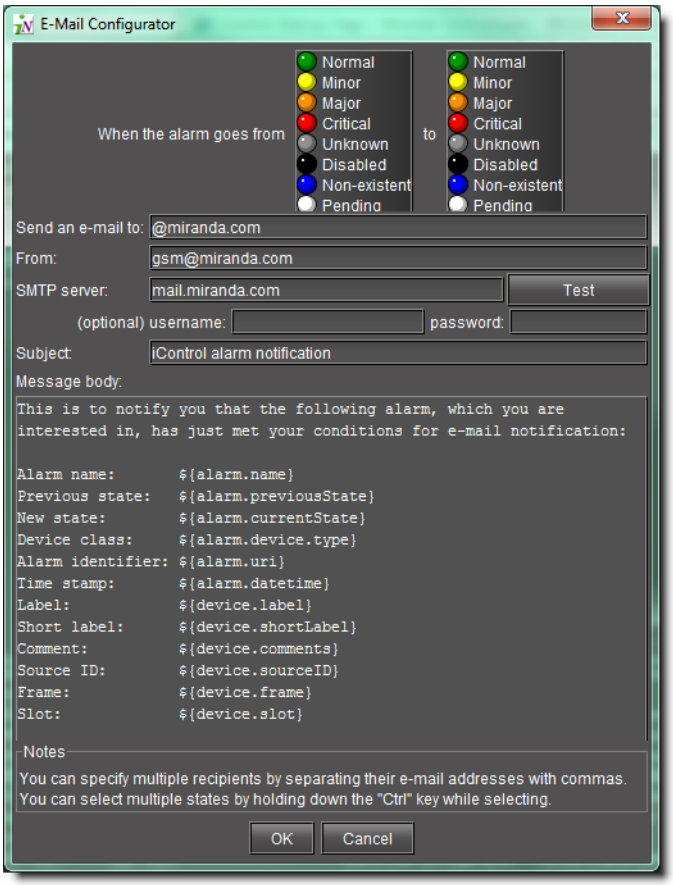
   For example, if you wish to have a script run whenever any alarm is triggered, choose **Scripted action**.

4. Click **New**.

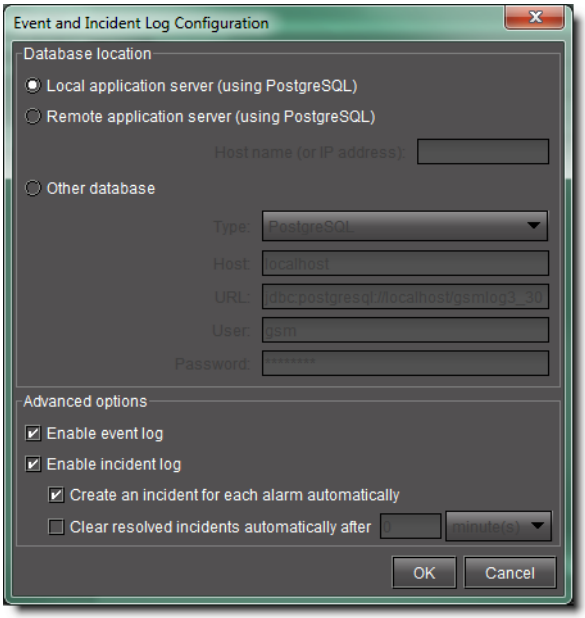
   SYSTEM RESPONSE: A window appears allowing you to configure the global action. The contents of this window varies according to the type of action you have chosen. Here are some examples.



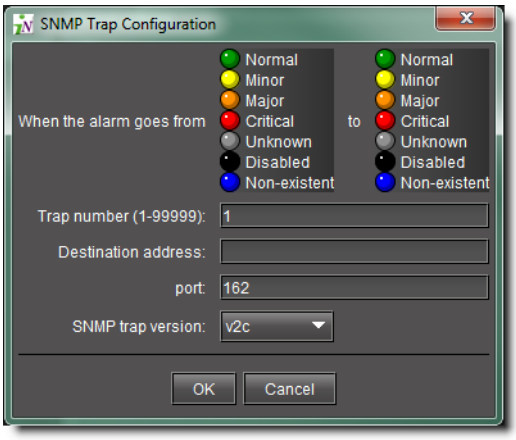
GPI VNODE Relay action configuration window



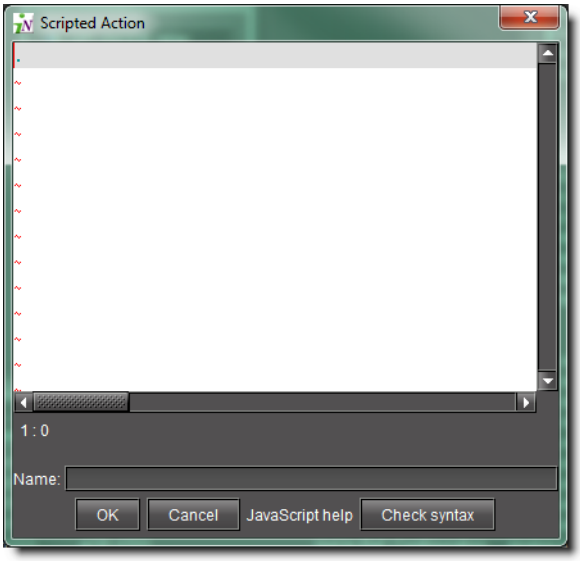
E-mail Configurator window



Event and incident log action configuration window



SNMP trap action configuration window



Script action window

> **Note:** There is no configuration required for the SNMP agent action. Once activated, it appears in the list of current global alarms in the Alarm Browser. For more information please see Configuring the GSM as an SNMP Agent, on page 489.

5. Once you have finished typing configuration details for the action, click **OK**.

   SYSTEM RESPONSE: The new action appears in the **Global actions** section of the GSM window (*Admin* > *Actions* tab).

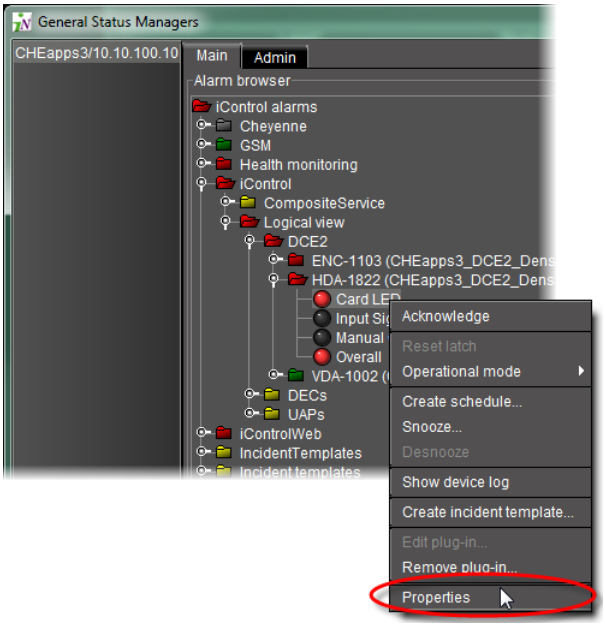
Adding an Action to a Specific Alarm

REQUIREMENT

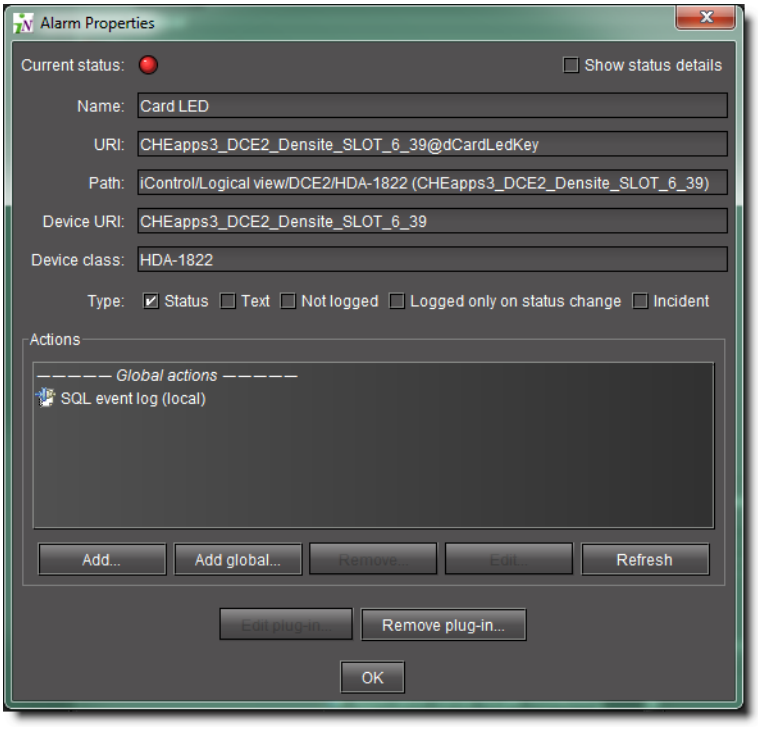
Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

To add an action to a specific alarm

1. In the GSM Alarm Browser, right-click the alarm to which you would like to associate an action, and then click **Properties**.

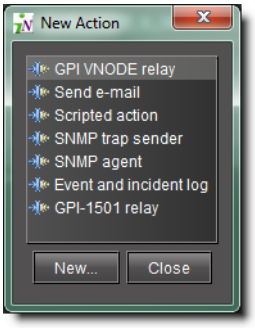


SYSTEM RESPONSE: The **Alarm properties** window appears.



2. In the **Actions** area, click **Add**.

SYSTEM RESPONSE: The **New action** window appears.



3. Select an appropriate action from the list (e.g., if you wish to have an e-mail sent to someone when the specified alarm is triggered, choose the **Send e-mail** action).
4. Click **New**.

   SYSTEM RESPONSE: A window appears allowing you to configure the global action.

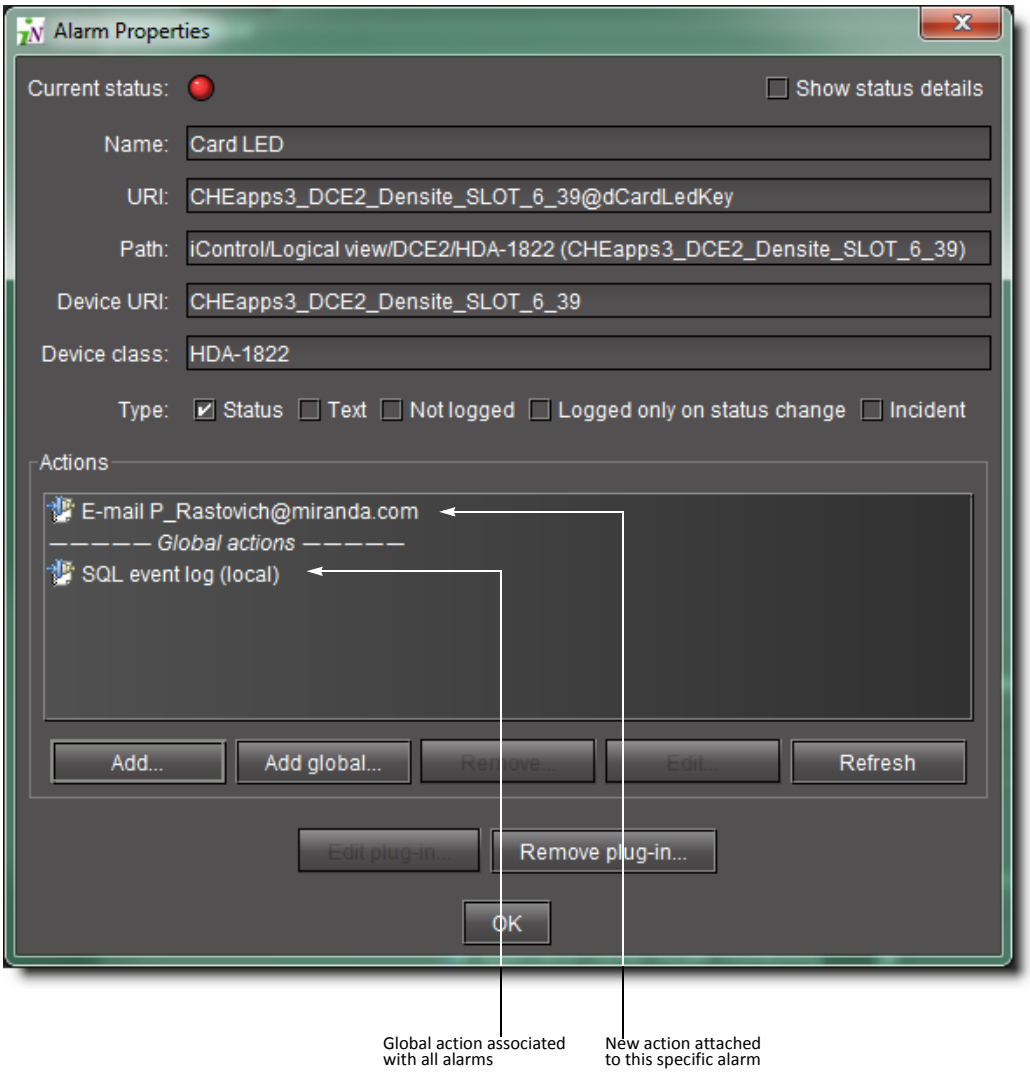
   Note: The content of this window varies according to the type of action you have chosen.

IMPORTANT: System behavior

Even though the SNMP agent plug-in appears in this list, it is, by definition, a global action, and cannot be attached to a specific alarm. For more information please see Configuring the GSM as an SNMP Agent, on page 489.

5. Once you have finished typing configuration details, click **OK**.

   SYSTEM RESPONSE: The new action appears in the **Actions** section of the **Alarm properties** window.



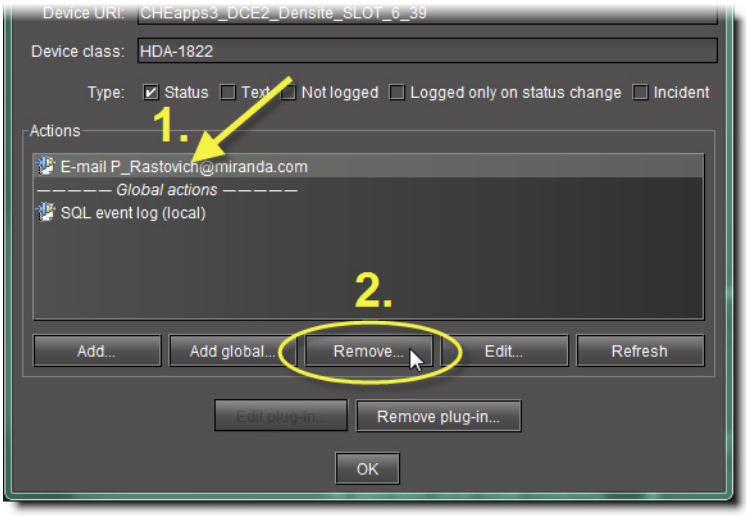
Removing Alarm Consumers

REQUIREMENT

Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

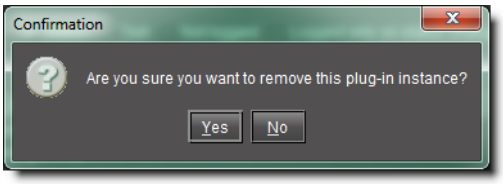
To remove an action attached to an alarm

1. In the GSM Alarm Browser, open the **Alarm properties** window of the alarm to which the action is attached (see step 1 of Adding a Global Action on page 390).
2. Select the action to be removed from the **Actions** list.



3. Click **Remove**.

   SYSTEM RESPONSE: A confirmation message appears.



4. Click **Yes** to remove the action.

Acknowledging Alarms

See also

For more information about alarms, see Acknowledging Alarms, on page 408.

Enabling the Display of Alarm Acknowledgement for a Particular GSM Alarm Browser

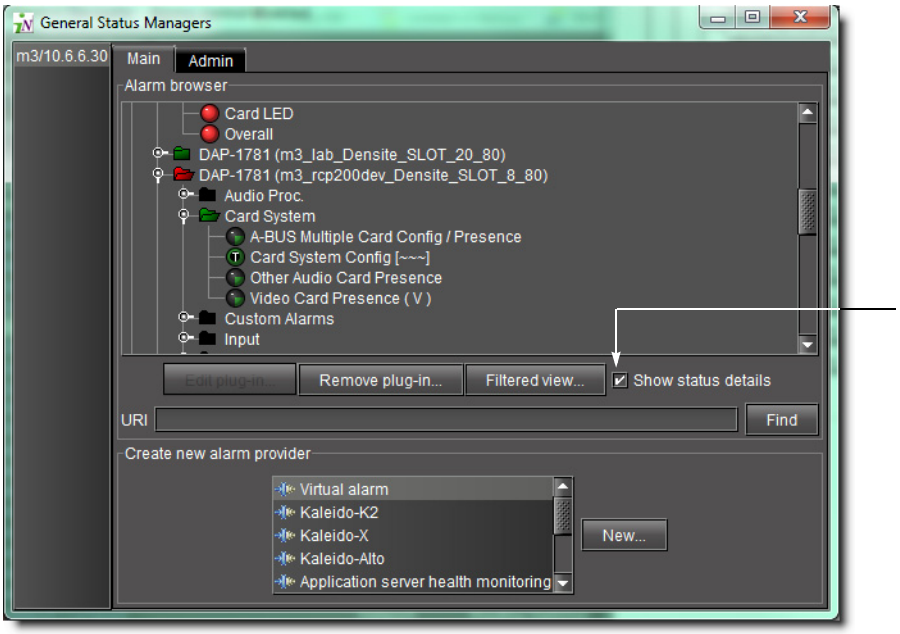
REQUIREMENT

Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

To enable the display of alarm acknowledgement for a particular GSM Alarm Browser

- In the GSM Alarm Browser, select **Show status details**.

Note: Alarm acknowledgements are displayed immediately.



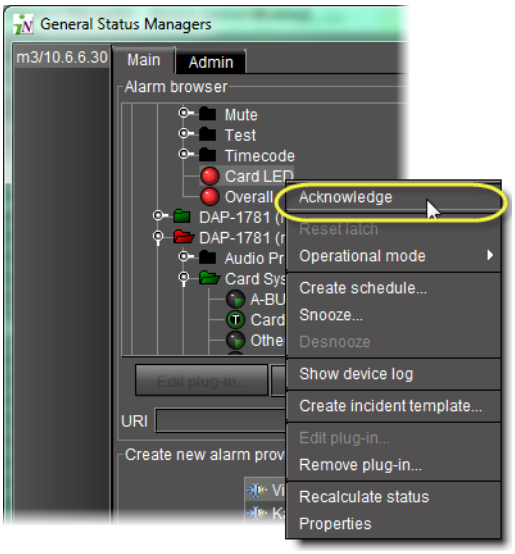
Acknowledging an Individual Alarm

REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To acknowledge an individual alarm

1. If you would like to acknowledge an alarm with the GSM Alarm Browser, perform the following steps:
   a) Open the GSM Alarm Browser for the appropriate GSM (see page 710).
   b) Right-click the alarm and click **Acknowledge**.



2. If you would like to acknowledge an alarm from a channel's Web page, perform the following steps:
   a) Open the **iC Web** page (see page 717).
   b) In the channel's Web page, right-click the alarm, and then click **Acknowledge**.

> **Note:** Once the affected individual channel is acknowledged the button changes from flashing red to solid red.

Resetting Latches

To reset a latch from the GSM Alarm Browser

1. Open the GSM Alarm Browser (see page 710).
2. Right-click the alarm and then click **Reset client latch** or **Reset server latch**, as required.

To reset a latch from a channel's Web page

1. Open the required **iC Web** page (see page 710).
2. Right-click the individual alarm and then click **Reset client latch** or **Reset server latch**, as required.

Working with Virtual Alarms

Creating a Virtual Alarm

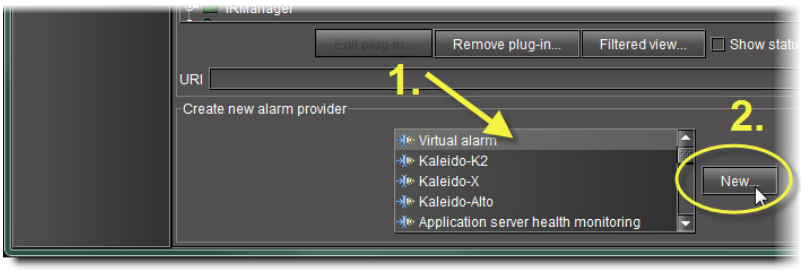
> **Note:** In addition to alarms found in GSMs within the same subnet as your local Application Server, you can also create virtual alarms with sub-alarms from remote GSMs residing on Application Servers *outside* the local subnet. In order to do this, you must first type the IP addresses of the remote GSMs within the **Service and alarm discovery** area of the *Lookup locations* page of iControl.

REQUIREMENT

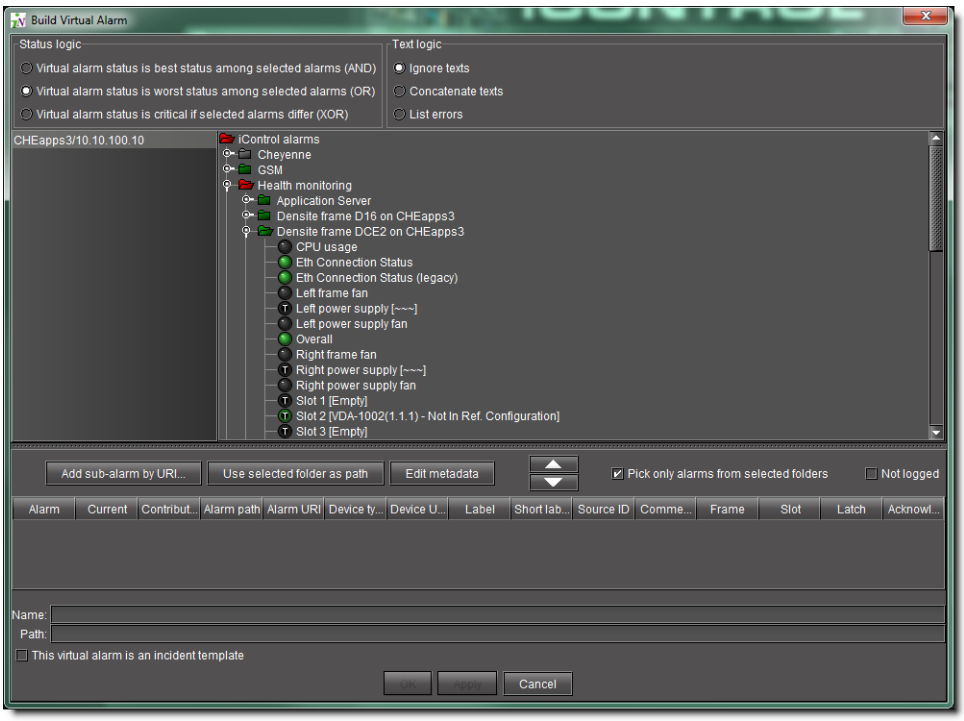
Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

To create a virtual alarm

1. In the **Create a new alarm provider** area of the GSM Alarm Browser, click **Virtual alarm**.
2. Click **New**.



SYSTEM RESPONSE: The **Build virtual alarm** window appears.



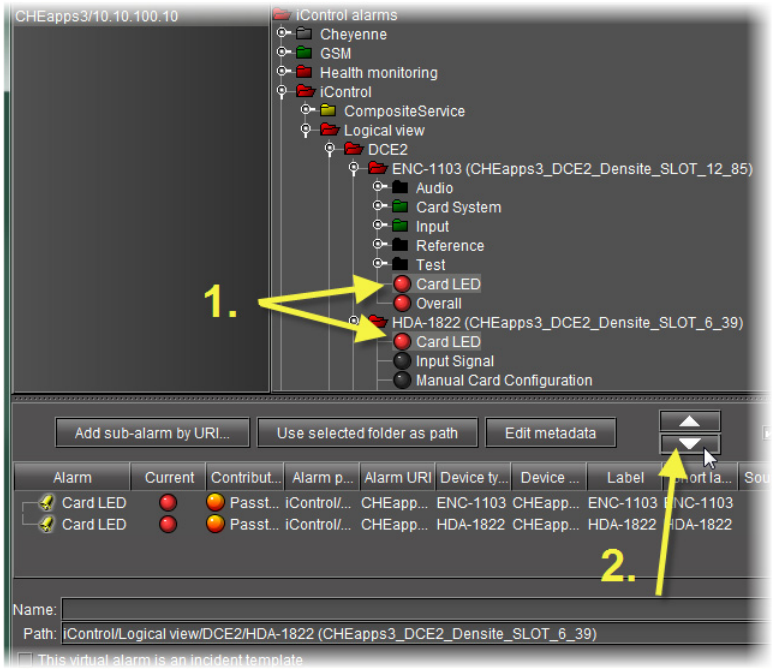
3. In the **Status logic** section, select one of the following three options:
   - **Virtual alarm status is best status among selected alarms (AND)** — Choose this option to have the contribution of the sub-alarms calculated using the *optimistic* version of the alarm logic tables.

- **Virtual alarm status is worst status among selected alarms (OR)** — Choose this option to have the contribution of the sub-alarms calculated using the *pessimistic* version of the alarm logic tables. This is the most common option, since it brings changes in the status of any sub-alarms to the attention of the operators.
- **Virtual alarm status is critical if selected alarms differ (XOR)** — Choose this option to have the contribution of the sub-alarms calculated using the *XOR* version of the alarm logic tables. This causes the virtual alarm to reflect whether or not all of its sub-alarms have the same status. If all sub-alarms are the same (and in error), the virtual alarm will be green. If, among the errored sub-alarms, there are one or more discrepancies in status, the virtual alarm's status will be red.

For a more detailed description of the difference among these three options, refer to Understanding the Alarm Logic Tables on page 356

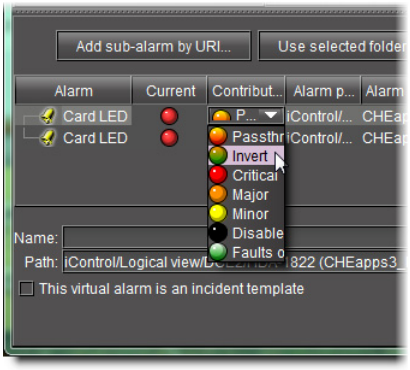
4. Select the alarms that are to be sub-alarms of the new virtual alarm, and then click the large down arrow button to transfer them to the table in the bottom half of the window.

   The alarm hierarchy displayed in the **Build virtual alarm** window is the same as the one in the GSM *Alarm Browser*.



5. The table displays various details about the sub-alarms you have selected, including their *Contribution*, which defines how a sub-alarm will pass its status on to the virtual alarm. The default contribution value is **Passthrough**, which means the sub-alarm will pass its status unaltered to the overall calculation of the virtual alarm.

   It is possible to override the error status of sub-alarms when they are triggered. This is useful when, for example, a device is only able to report a status of either *normal* (green) or *error* (red), but you want the error condition to be reflected as a *warning* (yellow) in the virtual alarm. To change a sub-alarm's contribution, click in the **Contribution** column, and then select the status you want the virtual alarm to use when an error occurs.



For example, if a sub-alarm goes from green to orange or red, but the selected contribution is yellow, the virtual alarm will "see" yellow (the virtual alarm's overall status may still depend on other sub-alarms).

The **Invert** contribution allows performing a logical "NOT" calculation on sub-alarms. This feature can be used, for example, to report alarms from GPI inputs. It can also be used to handle cases where an error is expected, and not seeing an error is a sign that something probably went wrong. The table below describes the result of inverting sub-alarms:

Sub-alarm Status	Inverted Contribution
NORMAL	ERROR
MINOR	NORMAL
MAJOR	NORMAL
CRITICAL	NORMAL
NON-EXISTENT	NON-EXISTENT
PENDING	PENDING
DISABLED	DISABLED
UNKNOWN	UNKNOWN

Selecting the **Faults only** contribution causes a sub-alarm to be mapped to NORMAL unless it's in one of the fault statuses—usually CRITICAL, MAJOR, and MINOR. The list of fault statuses can be modified by using the setFaultSeverities( ) property. See the *GSM Scripting Manual* for details.

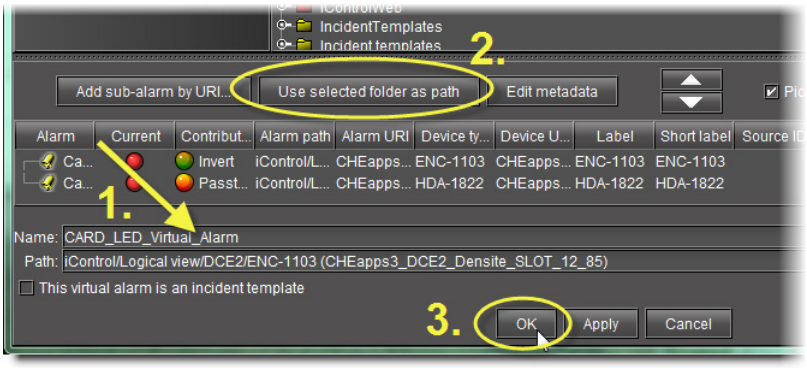
> **Note:** If the sub-alarm's fault condition is cleared, its contribution will always be *green*, unless the value specified in the **Contribution** column is *black*.

6. Specify a name for the new virtual alarm in the **Name** field.
7. Specify a path for the new virtual alarm.

   By default, virtual alarms are created under the **Virtual alarms** folder in the *Alarm Browser* hierarchy, but you can organize your virtual alarms however you see fit. Type the path to the

destination folder for the virtual alarm in the **Path** field. Use a forward slash character (/) to separate folder names. If the folder doesn't exist, it will be created automatically.

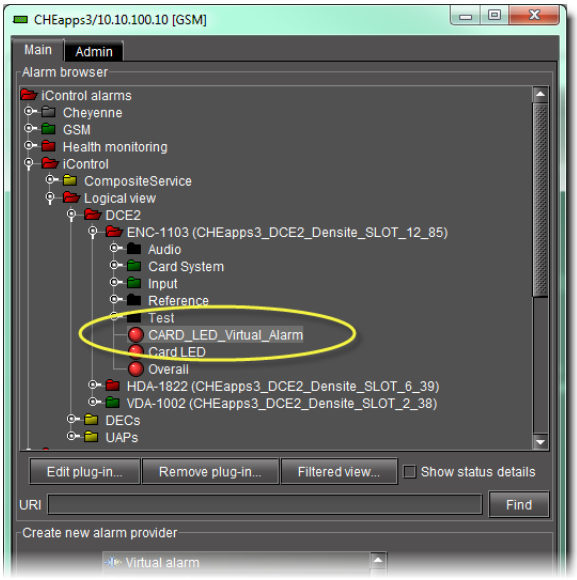
Alternatively, as a shortcut for existing folders, you can select an existing folder in the alarm browser hierarchy, and then click the **Use selected folder as path** button. The location of the selected folder will appear in the **Path** field.



Using the selected folder as a destination folder

8. Click **OK**.

   System Response: The **Build virtual alarm** window closes and the newly created alarm appears in the specified folder in the **Alarm Browser** window.



Newly created virtual alarm (circled)

Creating a Virtual Alarm to Filter Out Non-Channel Alarms (iC Reports)

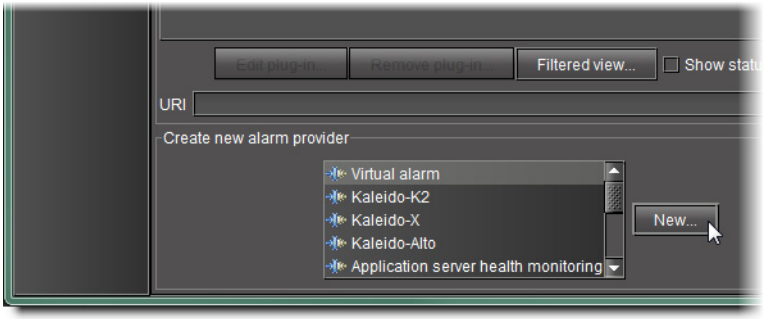
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

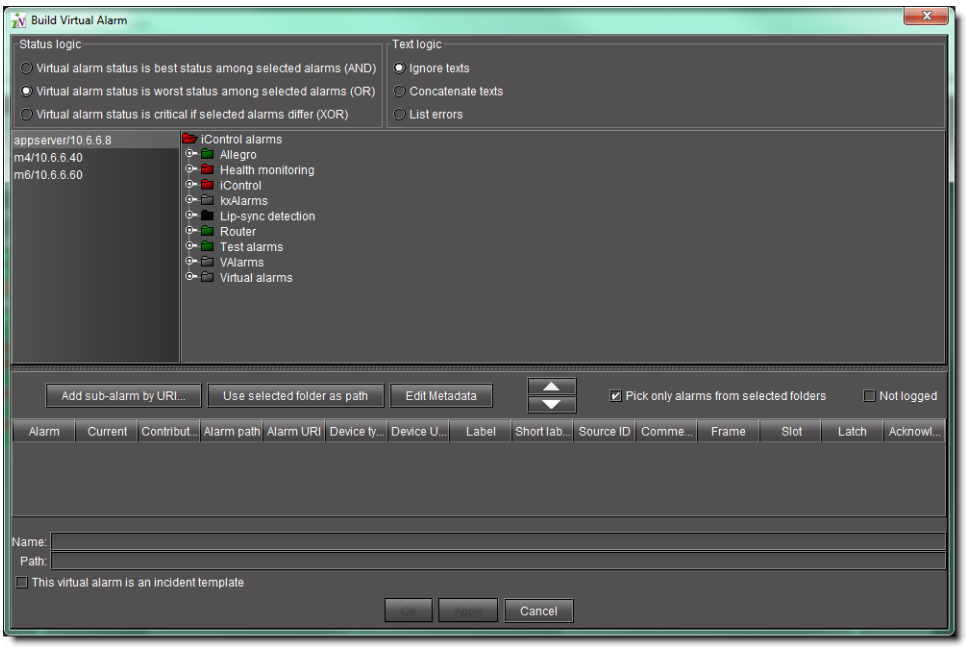
- You have opened the GSM Alarm Browser (see page 710).
- **[RECOMMENDED]:** You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Channel Performance Reporting, on page 130).

To create a virtual alarm to filter out non-channel alarms

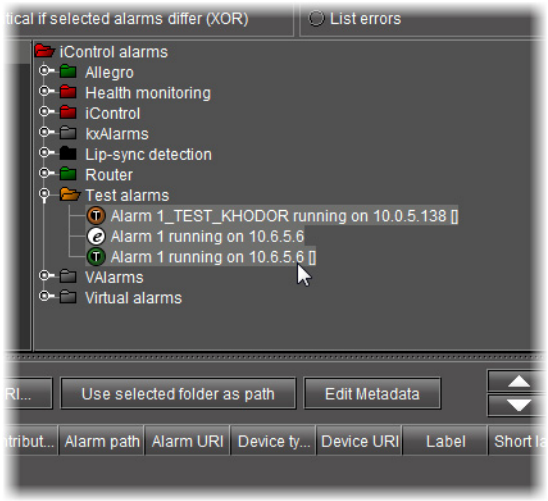
1. In the GSM Alarm Browser, in the **Create new alarm provider** area, click **Virtual alarm** and then click **New**.



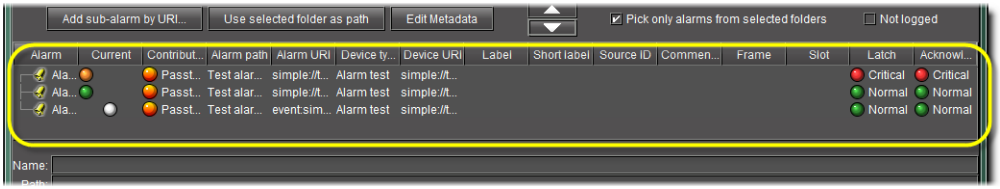
SYSTEM RESPONSE: The **Build Virtual Alarm** window appears.



2. Select the channel alarms you would like to group into a virtual alarm.

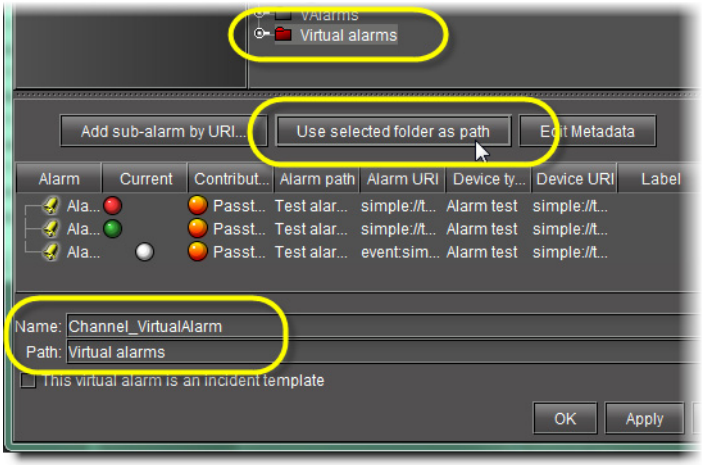


3. Click the *Down* arrow ( ) to associate the selected alarms with the new virtual alarm.
   SYSTEM RESPONSE: The sub-alarms appear in the list below the *Down* arrow.

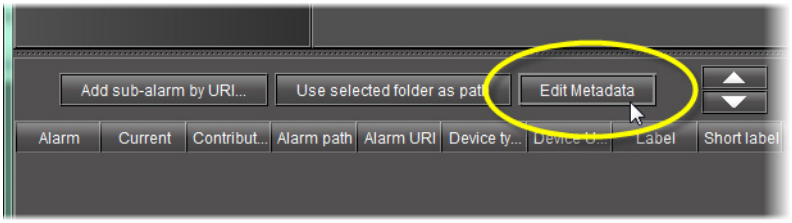


4. Type a name for the new virtual alarm.
5. Type a path in which the virtual alarm will appear.

> **Note:** The path of the virtual alarm can be anywhere you choose. You can select an alarm folder, and then click **Use selected folder as path**.

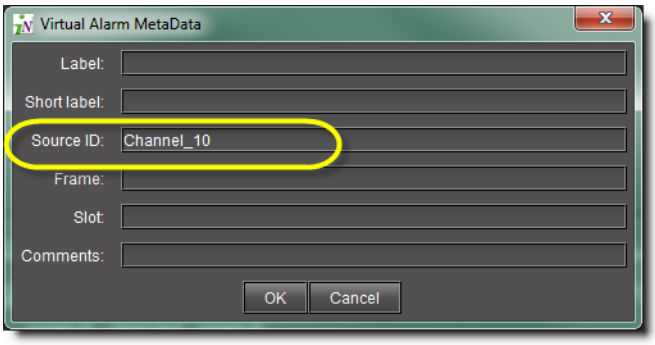


6. Click **Edit Metadata**.



SYSTEM RESPONSE: The **Virtual Alarm MetaData** window appears.

7. In the **Source ID** box, type a meaningful identifier string to distinguish this virtual alarm's sub-alarms from other alarms.



8. If desired, fill in the other boxes of the **Virtual Alarm Metadata** window.
9. Click **OK** in the **Virtual Alarm MetaData** window.
10. Click **OK** in the **Build Virtual Alarm** window.

SYSTEM RESPONSE: The **Build Virtual Alarm** window disappears.

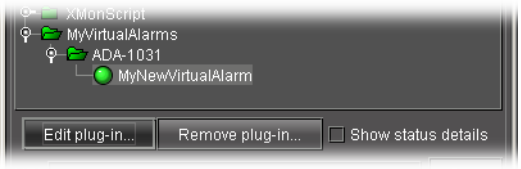
Modifying a Virtual Alarm

REQUIREMENT

Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

To modify a virtual alarm

1. Select the virtual alarm to be edited in the GSM Alarm Browser.



2. Click **Edit plug-in**.

System Response: The **Build virtual alarm** window appears, displaying the configuration information for the selected virtual alarm.

3. Make changes as required, and then click **OK**.

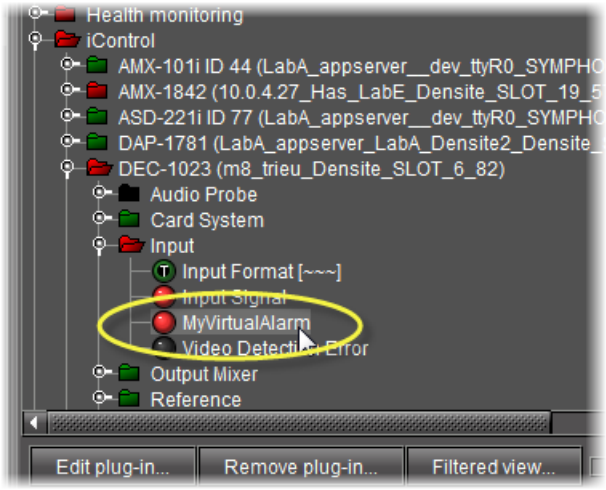
Removing a Virtual Alarm

REQUIREMENT

Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

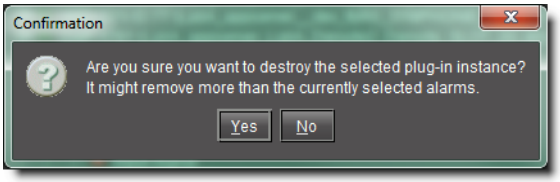
To remove a virtual alarm

1. Select the virtual alarm to be removed in the GSM Alarm Browser.



2. Click **Remove plug-in**.

   System Response: A confirmation window appears.



3. Click **Yes**.

Displaying Alarm Status Details

REQUIREMENT

Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

To enable the display of alarm status details in a GSM Alarm Browser

- In the GSM Alarm Browser, select **Show status details**.

  SYSTEM RESPONSE: All alarms in the GSM Alarm Browser display their *current*, *latched* and *acknowledgment* status components (see Alarm Component Appearance, on page 349).

Acknowledging Alarms

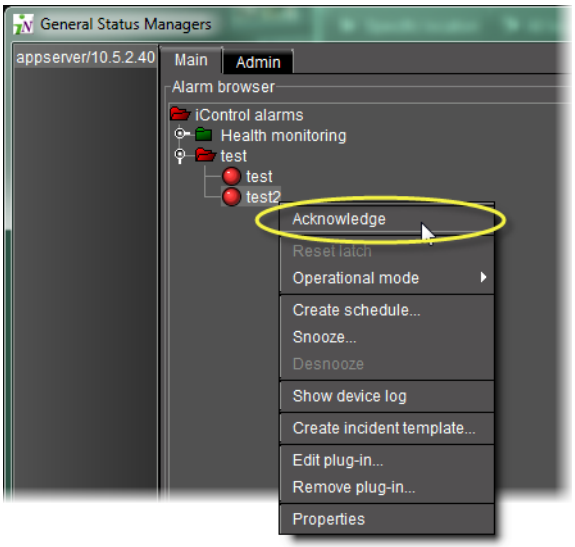
Acknowledging Alarms in iC Navigator

REQUIREMENT

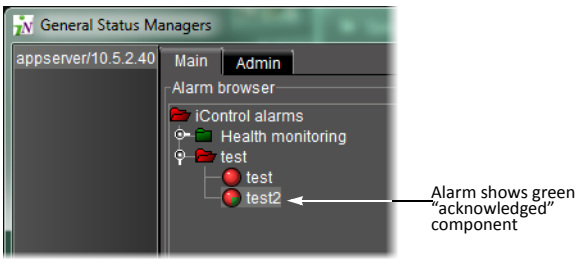
Before beginning this procedure, make sure you have opened the GSM Alarm Browser for the appropriate GSM (see page 710).

To acknowledge an alarm in the GSM Alarm Browser

- In the GSM Alarm Browser, right-click the alarm you would like to acknowledge., and then click **Acknowledge**.



Note: If **Show status details** is enabled, the *acknowledged* component of the alarm's status icon is displayed.



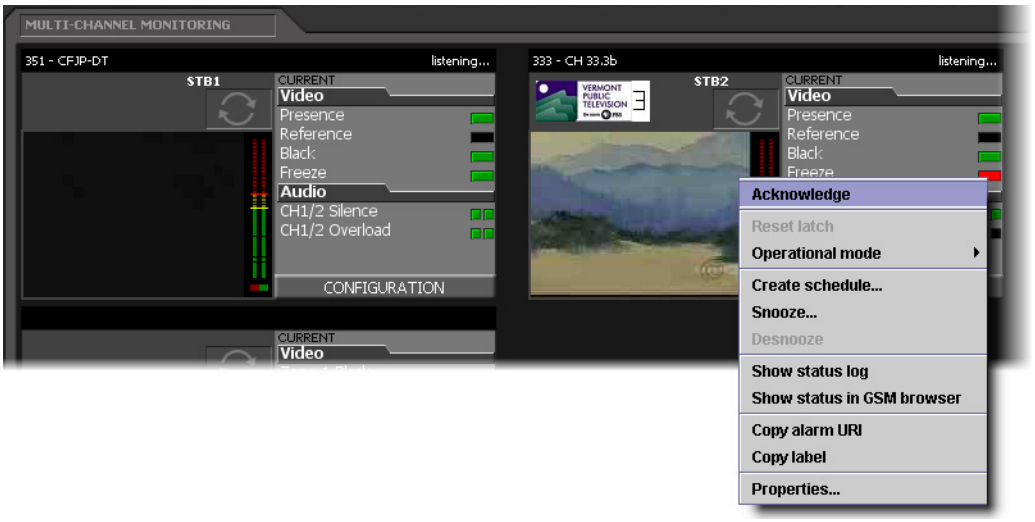
Acknowledging Alarms on iC Web Pages

REQUIREMENT

Before beginning this procedure, make sure you have opened the appropriate **iC Web** page (see Working with iC Web, on page 717).

To acknowledge an alarm on an iC Web page

- Right-click the alarm in the Web page panel, and then click **Acknowledge**.



SYSTEM RESPONSE: The alarm's *acknowledged* component turns green.

> **Note:** The *acknowledged* component of alarms is not always visible on **iC Web** pages. You can still determine if an alarm has been acknowledged by right-clicking—if the `Acknowledge` command is grayed out, it means someone has already acknowledged the alarm. In some cases, acknowledging an alarm on a Web page will also stop it from flashing.

Acknowledging a Channel Alarm

REQUIREMENT

Before beginning this procedure, make sure you have opened the appropriate iC Web page (see page 718).

To acknowledge a channel alarm

- Perform **only one** of the following steps:
  - Right-click on a thumbnail, and then click **Acknowledge**.
  - Right-click an individual alarm on the channel's Web page, and then click **Acknowledge**.

SYSTEM RESPONSE: Once the channel alarm is acknowledged, the button changes from flashing red to solid red.

Acknowledging More Than One Channel Alarm

REQUIREMENT

Before beginning this procedure, make sure you have opened the appropriate **iC Web** page (see page 718).

To acknowledge more than one channel alarm

- Right-click on a channel group number, and then click **Acknowledge**.

  SYSTEM RESPONSE: All the channels within the selected group are acknowledged and the buttons change from flashing red to solid red.

Resetting Latches on Web Pages

REQUIREMENT

Before beginning this procedure, make sure you have opened the appropriate **iC Web** page (see page 718).

To reset a latch

- Perform **only one** of the following steps:
  - Right-click on a thumbnail, and then click **Reset client latch** or **Reset server latch**, as required.
  - Right-click an individual alarm on the channel's Web page, and then click **Reset client latch** or **Reset server latch**, as required.

  SYSTEM RESPONSE: Once the channel alarm is acknowledged the button changes from flashing red to solid red.

Viewing Acknowledgments and Latches in Event Log Viewer

A new log entry is created for each change in a particular status, including changes to a server latch or alarm acknowledgment.

It is possible to query the log database for specific acknowledgment or latch events. The **Alarm state** area of the log viewer has an **Extra** field that enables searching for additional state information. For example, the text value of a button that was acknowledged in **iC Web** could be typed in the **Extra** field. The query results obtained might provide valuable information about the acknowledged channel ID.

Logging Acknowledgements as Events

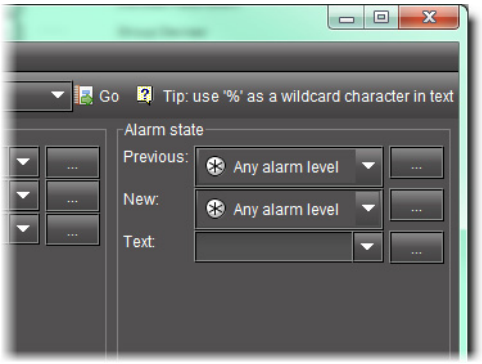
Acknowledgements can be logged as events in the log viewer and log database.

In **Event Log Viewer**, there are columns for previous and new acknowledge statuses.

> **Note:** By default, the acknowledgement columns do not display in the log viewer.

There is also a column for the user ID which is the IP address of the client. A new log entry is created for each change in a particular status including changes to the server latch or alarm acknowledgement. It is possible to query the database for specific acknowledgement transitions and alarm statuses.

The **Alarm State** area of the log viewer has an extra field labeled **Text**, that enables searching for additional information. For example, the text value of the button that was acknowledged in **iC Web** could provide valuable in-context information about the acknowledged channel ID.



*Alarm state filter area in **Event Log Viewer***

In the **Alarm state** area, the Ellipsis button (...) allows you to filter with multiple criteria selected.

> **Note:** The system reads multiple criteria as a logical **OR** (e.g., selecting Critical and Disabled alarms will yield a single list that includes all Critical alarms and all Disabled alarms).

See also

For more information about:

- Filtering log searches with multiple criteria, see page 143.
- Filtering log searches using textual elements as criteria, see page 148.

Working with Operational Modes

Setting an Alarm's Operational Mode

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- If you are working in iC Web, make sure you have opened the appropriate iControl Web page (see page 718).
- If you are working in iC Navigator, make sure you have opened iC Navigator (see page 697).

To edit an alarm's Offline, In maintenance, or Inverted mode

- Right-click the alarm, point to **Operational mode**, and then click one of **Offline**, **In maintenance**, or **Inverted**.

  System Response: The color of the alarm's status icon changes to a darker shade, and the text label (if any) becomes orange.

See also

For more information about:

- the *Inverted* operational mode, see Inverted, on page 359.
- manual alarm inversions, see Manual Alarm Inversions on page 375 and Inverting Alarms Manually on page 416.
- scheduling inversion actions, see Setting a Schedule for an Alarm Inversion, on page 421.

Checking the Operational Mode of an Alarm

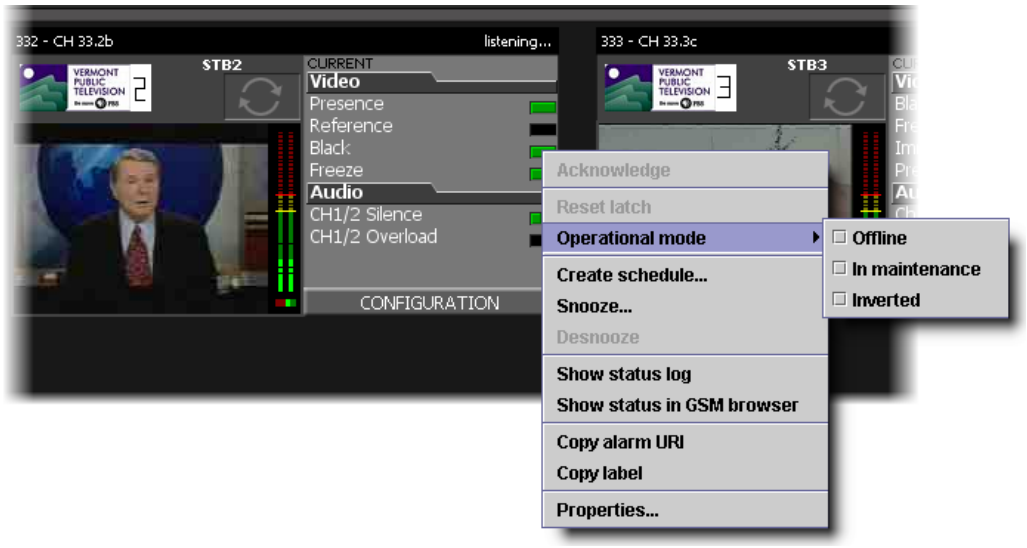
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

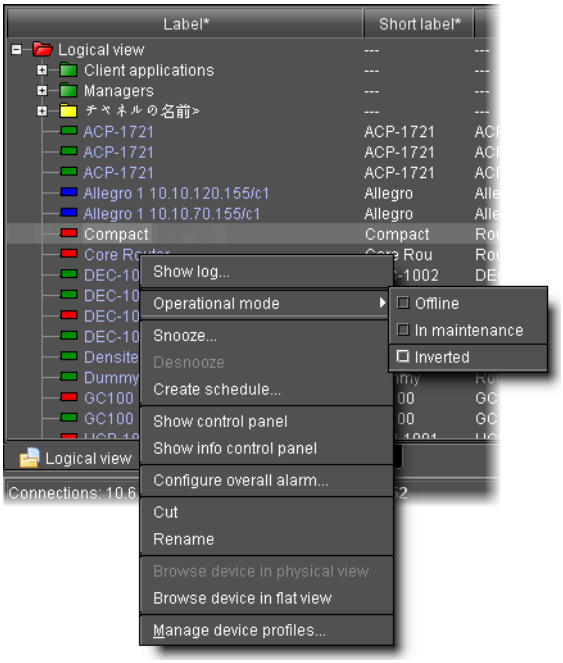
- If you are working in iC Web, make sure you have opened the appropriate iControl Web page (see page 718).
- If you are working in iC Navigator, make sure you have opened iC Navigator (see page 697).

To check the operational mode of an alarm

- Right-click the status icon of the alarm, point to **Operational mode**, and verify which of the operational modes are active, if any.



Note: The same shortcut menu is available in both iC Web and iC Navigator, to make it easy for operators to manually enable, disable, or check the operational mode for selected alarms.



Note: The system can be configured to always report a normal status instead of the real status for suppressed alarms. In such a case, the overall channel status icon would be green instead of showing the real status. The default behavior is to show the real alarm status. Should you need your system configured in such a way, please contact the Grass Valley technical support team (see Contact Us, on page 739).

Snoozing an Alarm

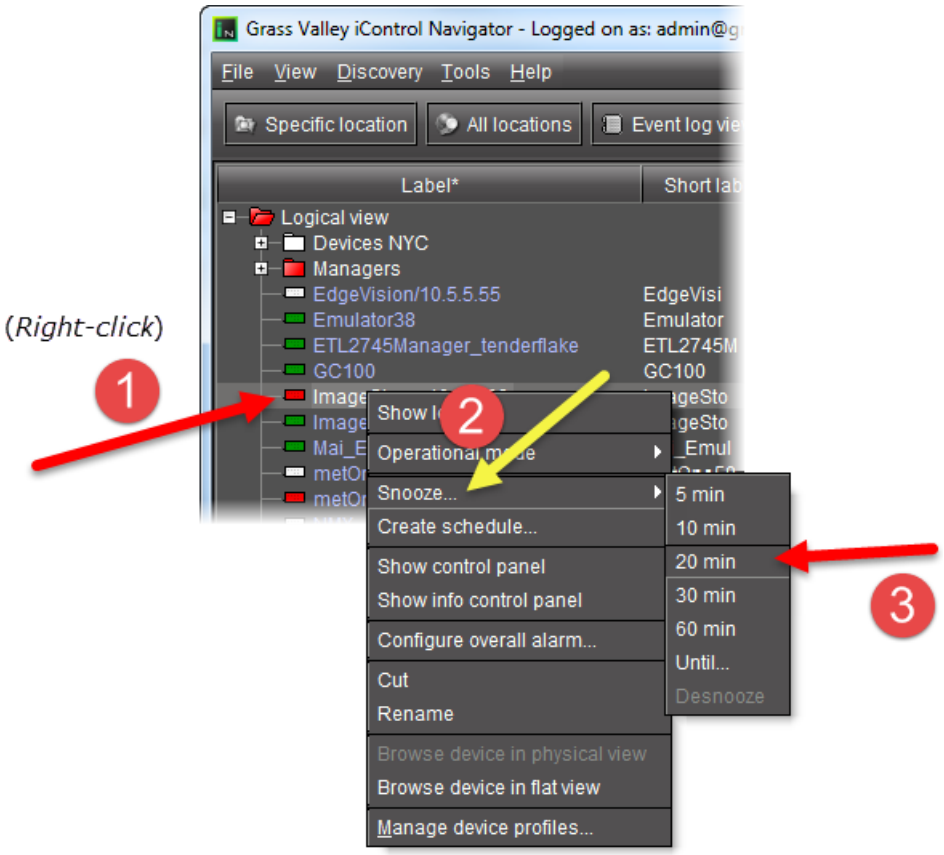
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- If you are working in iC Web, make sure you have opened the appropriate iControl Web page (see page 718).
- If you are working in iC Navigator, make sure you have opened iC Navigator (see page 697).

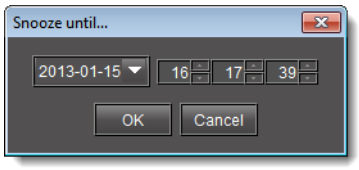
To snooze an alarm

- In either the iC Web page, iC Navigator, the GSM Alarm Browser, or **Incident Log Viewer**, right-click the appropriate status icon, point to **Snooze**, and then do one of the following:
  - Click one of the preset durations (**5 min**, **10 min**, **20 min**, **30 min**, or **60 min**).



OR,

- Click **Until**, and then in the **Snooze until** window, perform the following sub-steps:
  1. Specify the date and time when you would like the alarm to return to its original state.
  2. Click **OK**.



Desnoozing an Alarm

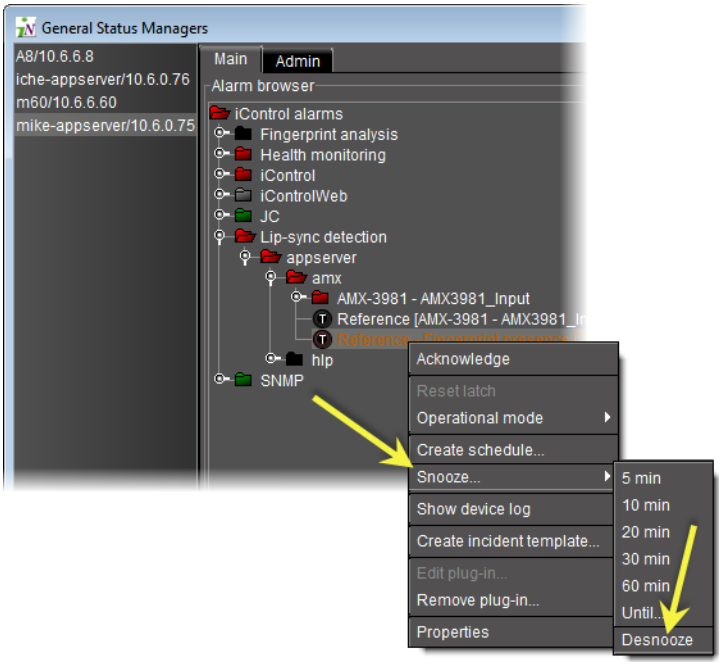
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- If you are working in **iC Web**, make sure you have opened the appropriate iControl Web page (see page 718).
- If you are working in **iC Navigator**, make sure you have opened **iC Navigator** (see page 697).

To desnooze an alarm

- In either the **iC Web** page, **iC Navigator**, the GSM Alarm Browser, or **Incident Log Viewer**, right-click the appropriate status icon, point to **Snooze**, and then click **Desnooze**.



Inverting Alarms Manually

IMPORTANT: If your network is configured to report alarms to multiple GSMs, it is recommended that you configure the same Grace period duration for manual inversions among all GSMs. Similarly, it is recommended that you configure the same Grace period duration for scheduled inversions among all GSMs.

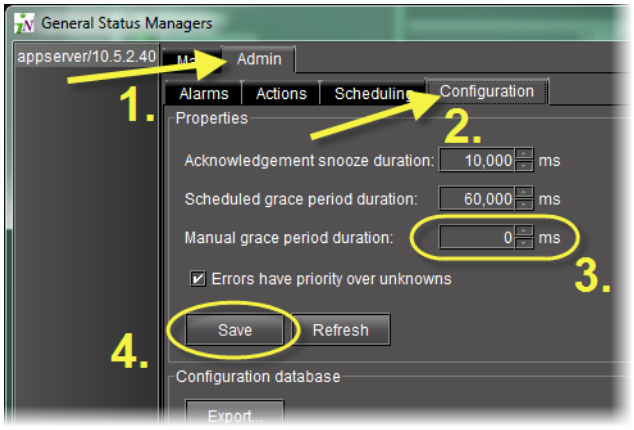
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

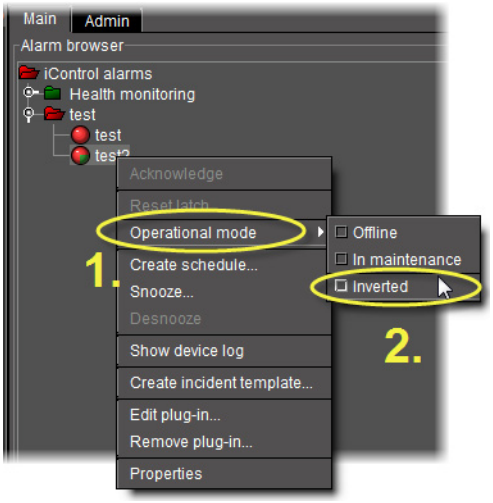
- If you are working in iC Web, make sure you have opened the appropriate iControl Web page (see page 718).
- If you are working in iC Navigator, make sure you have opened iC Navigator (see page 697).

To manually invert alarms in iC Web or iC Navigator

1. Open the GSM Alarm Browser (see page 710).
2. If you would like to perform the inversion action in iC Navigator's **Incident Log Viewer**, open **Incident Log Viewer** (see page 701).
3. Make sure the current setting for manual grace period duration is the desired duration period by performing the following steps.
   a) In the GSM Alarm Browser, click the **Admin** tab, and then click the **Configuration** tab.



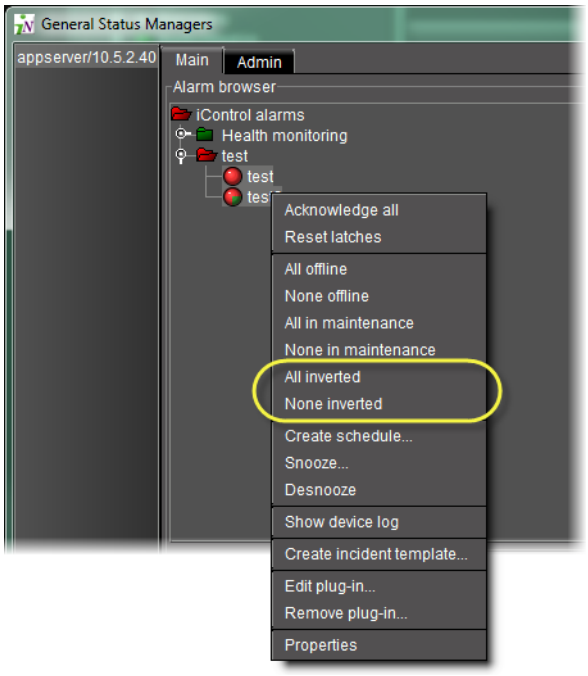
   b) In the **Properties** area, edit the grace period in the **Manual grace period duration** field, as required.
   c) Click **Save**.
4. If you would like to invert only one alarm, right-click the appropriate alarm, point to **Operational mode**, and then select (or clear) **Inverted**, as required.



SYSTEM RESPONSE: The associated alarm's *Inverted* mode is set to *On* (or to *Off*, depending on your inversion action).

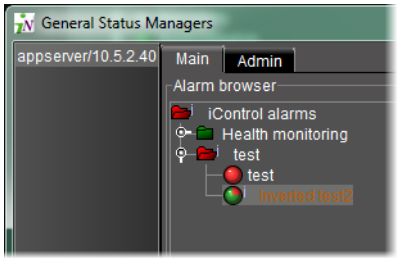
5. If you would like to invert more than one alarm, perform the following steps:
   a) Click the first alarm you would like to invert.
   b) Hold down the **Ctrl** key and individually click the remaining alarms.
   c) Release the **Ctrl** key.
   d) Right-click one of the selected alarms, and then click **All inverted** (or **None inverted**, as required).

> **Note:** **All inverted** inverts all selected alarms. **Non inverted** reverts all selected alarms' *Inverted* modes to *Off*.



SYSTEM RESPONSE: The selected alarms' *Inverted* modes immediately are set to *On* (or to *Off*, depending on the action).

SYSTEM RESPONSE: Orange alarm labels indicate there is a selected operational mode associated with that alarm. In the case of alarm inversion, an inverted alarm's label is orange when **Inverted** is selected, but turns back to white lettering when the alarm's *Inverted* mode returns to *Off*.



Note: Manual alarm inversion actions occur in real-time. The Grace period begins when the inversion action is initiated

See also

For more information about:

- the *Inverted* operational mode, see Inverted, on page 359.
- manual alarm inversions, see Manual Alarm Inversions, on page 375.
- scheduling inversion actions, see Alarm Inversion Scheduling on page 378 and Setting a Schedule for an Alarm Inversion on page 421.

Setting a Schedule for an Alarm

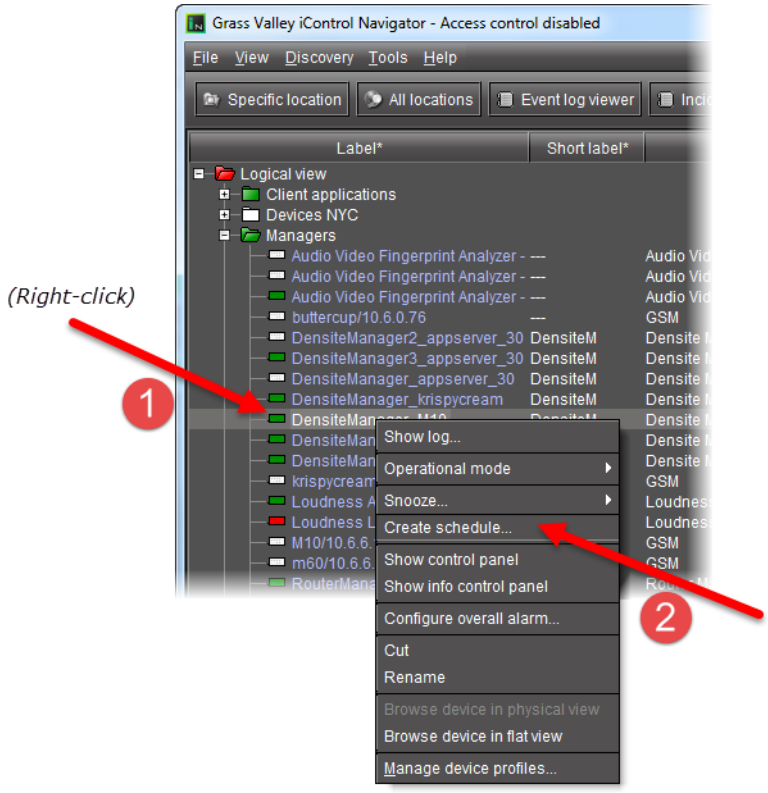
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

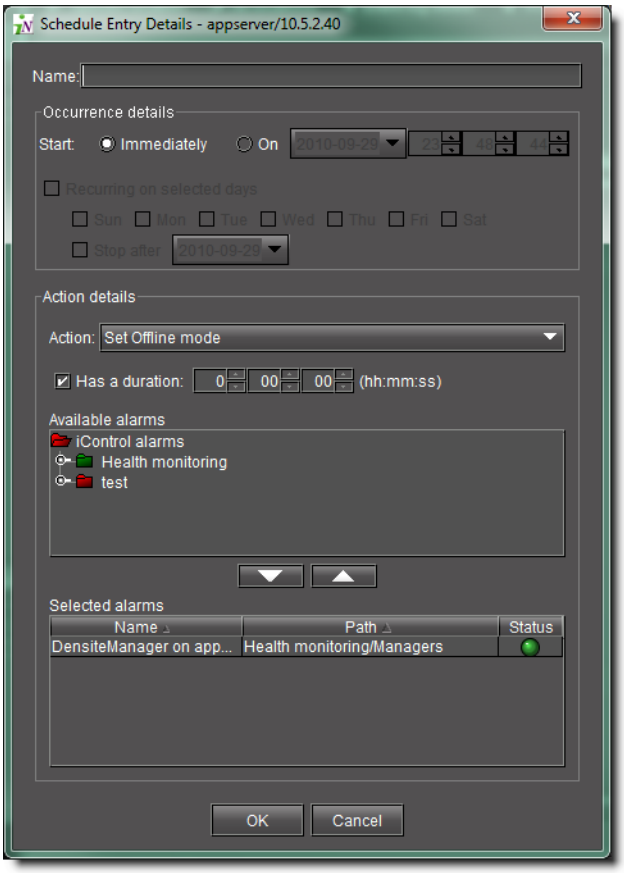
- If you are working in iC Web, make sure you have opened the appropriate iControl Web page (see page 718).
- If you are working in iC Navigator, make sure you have opened iC Navigator (see page 697).

To define a schedule for an alarm in iC Web or iC Navigator

1. Right-click the alarm, and then click **Create schedule**.



2. In **Schedule Entry Details**, type a name for the schedule, and set the appropriate options such as the start date and time recurrence pattern, and the end date.



3. In the **Action details** section, select the appropriate action in the list, and specify the length of the period during which the specified action will apply.
4. The selected alarm already appears in the **Selected alarms** list. To add other alarms to this schedule, select them in the Available alarms list, and click the down arrow button to add them to the Selected alarms list.

   TIP: Multiple alarms can be selected at once by holding down the **Shift** or **Ctrl** key while clicking.
5. To remove alarms from the **Selected alarms** list, select them and click the up arrow button.
6. Click **OK**.

Using the Calendar

The *Alarm Scheduler* has a built-in calendar to help you specify scheduling dates.

To use the calendar

1. Click the arrow button beside the date field.

   SYSTEM RESPONSE: The calendar appears.

2. Click the arrows to specify a month and year.
3. Click a date in the calendar to choose it.

Setting a Schedule for an Alarm Inversion

Schedule an alarm inversion action to automate an alarm inversion or the restoration of an inverted alarm to its normal mode. You can create or edit an alarm inversion schedule entry in either iC Navigator or iC Web.

IMPORTANT: If your network is configured to report alarms to multiple GSMs, it is recommended that you configure the same Grace period duration for manual inversions among all GSMs. Similarly, it is recommended that you configure the same Grace period duration for scheduled inversions among all GSMs.

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- If you are working in iC Web, make sure you have opened the appropriate iControl Web page (see page 718).
- If you are working in iC Navigator, make sure you have opened iC Navigator (see page 697).

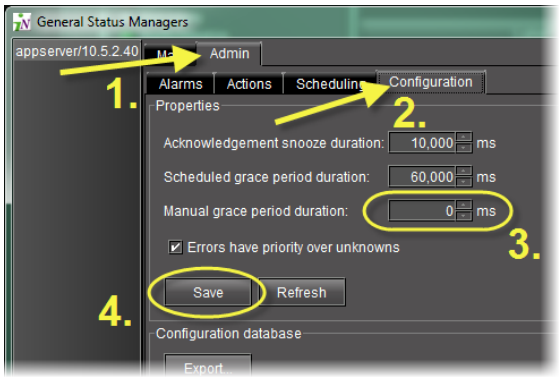
To set a schedule for an alarm inversion

1. If you would like to edit the configured Grace period (scheduled or manual), perform the following steps.

IMPORTANT: System behavior

Configuring the grace period for a scheduled inversion changes the grace period for all scheduled alarm inversions.
Configuring the grace period for a manual inversion changes the grace period for all manual alarm inversions.

a) Open the GSM Alarm Browser (see page 710).
b) In the GSM Alarm Browser, click the **Admin** tab, and then click the **Configuration** tab.



c) In the **Properties** area, type the desired grace period for scheduled alarm inversions in the **Scheduled grace period duration** field.

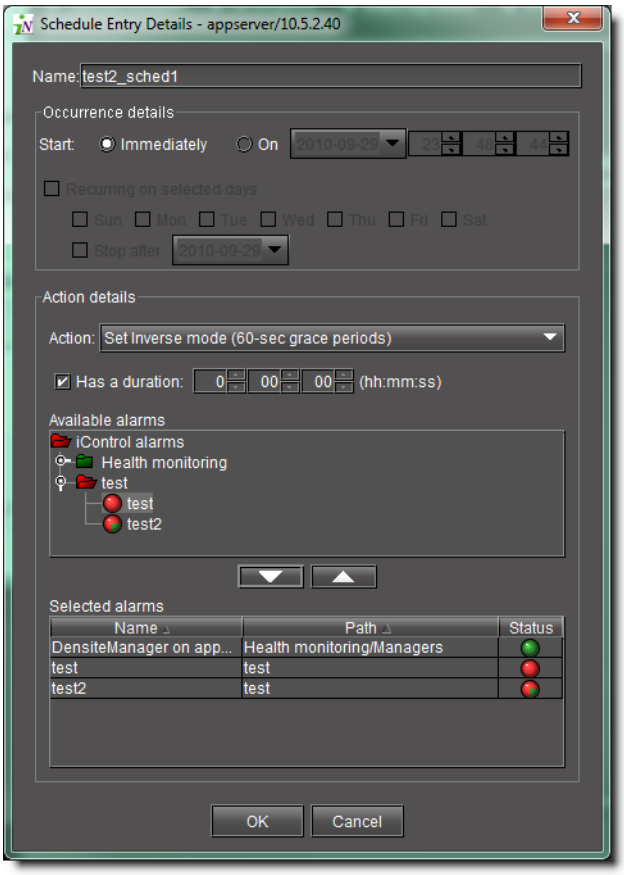
d) Type the desired grace period for manual alarm inversions in the **Manual grace period duration** field.

e) Click **Save**.

2. In either the iC Web page, iC Navigator, the GSM Alarm Browser, or **Incident Log Viewer**, right-click the alarm, device, or incident for which you would like to create a scheduled event.

3. Click **Create schedule**.

   SYSTEM RESPONSE: The **Schedule Entry Details** window appears.



4. Type in a schedule entry name in the **Name** field.
5. To configure the inversion to begin immediately after the schedule entry is complete, select **Immediately** in the **Occurrence details** area.
6. To configure the inversion to occur at a future time, perform the following steps:
   a) Select **On** in the **Occurrence details** area.
   b) Select a date and time for the event to occur (see Using the Calendar, on page 420).
7. To configure the inversion to recur, perform the following steps:
   a) Select **Recurring on selected days** in the **Occurrence details** area.
   b) Select the days on which you would like the inversion to recur.
   c) If you would like the recurrence to end after a specified date, select **Stop after**, and then use the calendar function to select the date (see Using the Calendar, on page 420).
8. In the **Action details** area, click **Set Inverse mode** in the **Action** list.
9. If you would like to configure this inversion to have a set duration, select **Has a duration**, and then type the duration period in hours, minutes, and seconds.
10. In the **Available alarms** list, select one or more alarms you would like to invert with this schedule entry by performing the following steps:

Note: If you would like to invert only one alarm with this schedule entry, simply click the alarm to select it.

a) Click the first alarm you would like to invert.
b) Hold down the **Ctrl** key and individually click the remaining alarms.
c) Release the **Ctrl** key.

11. Click the Down arrow button ( ).

SYSTEM RESPONSE: The selected alarms appear in the **Selected alarms** list.

Note: If you would like to remove an alarm from the **Selected alarms** list, select the alarm, and then click the 'up' arrow button ( ).

12. Click **OK**.

SYSTEM RESPONSE: The **Schedule Entry Details** window closes.

13. Verify the schedule entry is correctly configured by performing the following steps:

a) Open the GSM Alarm Browser (see page 710).
b) In the left pane of the GSM Alarm Browser, select the appropriate GSM.
c) Click the **Admin** tab then click the **Scheduling** tab.

SYSTEM RESPONSE: In the **Schedule entries** area, the schedule entry you created should be listed.

d) Select the schedule entry you would like to verify, and then click **Edit**.

SYSTEM RESPONSE: The **Schedule Entry Details** window appears.

e) In the **Schedule Entry Details** window, verify the alarms affected by this schedule entry (in the **Selected alarms** list) are the desired alarms.
f) Click **OK**.

SYSTEM RESPONSE: The **Schedule Entry Details** window closes.

g) In the GSM Alarm Browser, click the **Configuration** tab.
h) In the **Properties** area, verify the scheduled and manual grace period settings are correct.

Note: You can also verify whether an inversion (or reversion from an inversion) has occurred in **Incident Log Viewer**.

IMPORTANT: System behavior

Event Log Viewer records inversion events only for the duration of the Grace period during which the alarm is offline, but does not display the *Inverted* mode (Off or On).

See also

For more information about:

- the *Inverted* operational mode, see Inverted, on page 359.
- manual alarm inversions, see Manual Alarm Inversions on page 375 and Inverting Alarms Manually on page 416.
- scheduling inversion actions, see Alarm Inversion Scheduling, on page 378.

Viewing Alarm Schedules

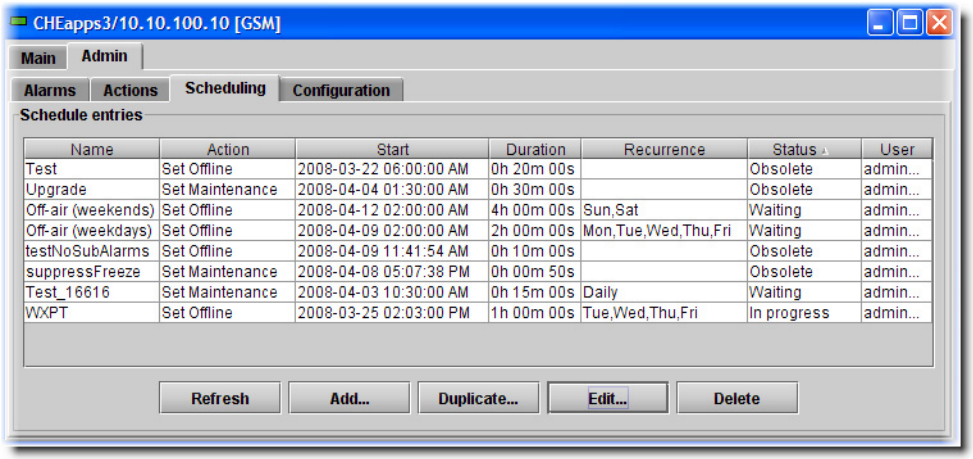
REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To view all existing schedule entries

1. In iC Navigator, or in an iC Navigator widget on an iC Web page, double-click the appropriate GSM.
2. In the Alarm Browser, click the **Admin** tab, and then click the **Scheduling** sub-tab.

   SYSTEM RESPONSE: All schedule entries are displayed.



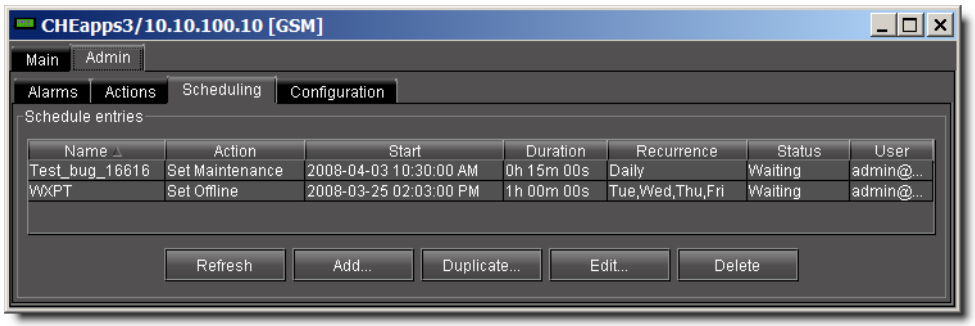
The following table describes the possible statuses for a schedule entry.

Status	Description
Waiting	The scheduled action is waiting to be executed at the time specified.
In progress	The scheduled action has started and is currently in progress. It has neither ended, nor been reverted.
Obsolete	The scheduled action has expired and will not be repeated.

Note: All the alarm scheduling events are logged by the system, and the log entries can be viewed using the Log Viewer application.

Managing Alarm Schedules

In the GSM Alarm Browser's Admin > Scheduling sub-tab, you can manage the Alarm Schedule entries in a number of ways.



Changing the Sort Order of the List of Alarm Schedule Entries

To change the sort order of the list of alarm schedule entries

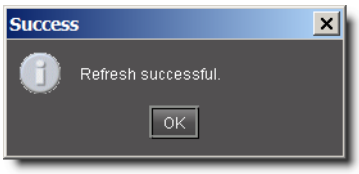
- Click on any of the column headers.

Refreshing the View of Current Alarm Schedule Entries

To refresh the view of current alarm schedule entries

- Click **Refresh**.

  SYSTEM RESPONSE: A message appears confirming that the list of alarm schedule entries has been updated.



Duplicating an Alarm Schedule Entry

To duplicate an alarm schedule entry

1. Click the entry you wish to duplicate.
2. Click **Duplicate**.

   SYSTEM RESPONSE: The **Schedule entry details** window appears.
3. Type a new name for the duplicate entry.
4. Modify the alarm schedule entry settings as necessary (see Setting a Schedule for an Alarm, on page 419).

5. Click **OK**.

Editing an Alarm Schedule

To edit an alarm schedule entry

1. Click the entry you wish to modify.
2. Click **Edit**.

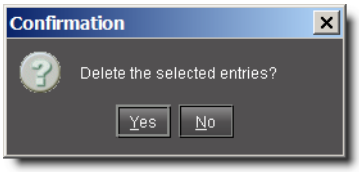
   System Response: The **Schedule entry details** window appears.
3. Modify the alarm schedule entry settings as necessary (see Setting a Schedule for an Alarm, on page 419).
4. Click **OK**.

Deleting an Alarm Schedule

To delete an alarm schedule entry

1. Click the entry you wish to delete.
2. Click **Delete**.

   System Response: A message appears prompting you to confirm the deletion.



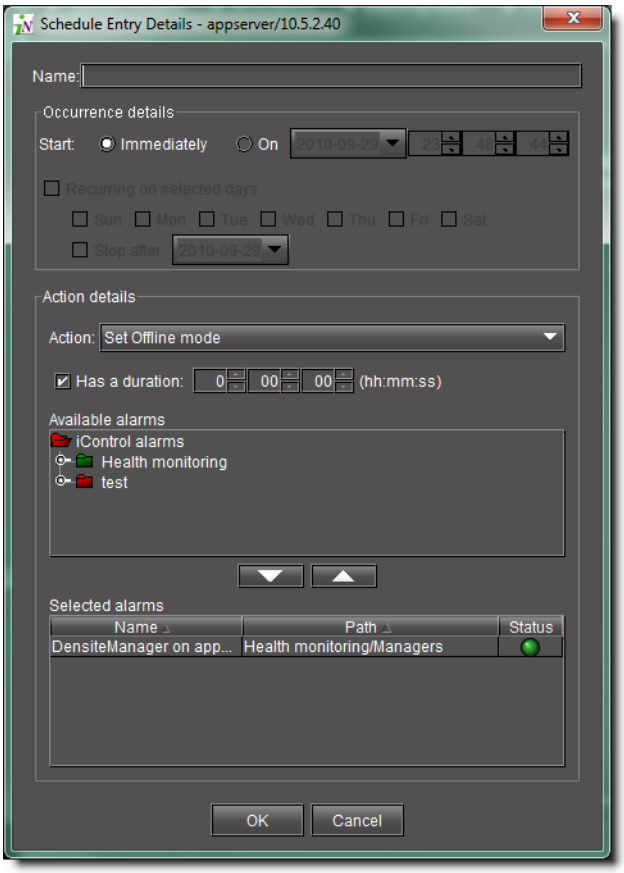
3. Click **Yes** to delete the selected alarm schedule entry.

Adding a New Alarm Schedule

To add a new alarm schedule entry

1. Click **Add**.

   System Response: The **Schedule entry details** window appears.
2. Type the alarm schedule entry settings as necessary (see Setting a Schedule for an Alarm, on page 419).
3. Click **OK**.
4. In **Schedule Entry Details**, type a name for the schedule, and set the appropriate options such as the start date and time (see Using the Calendar, on page 420), recurrence pattern, and the end date.



5. In the **Action details** section, select the appropriate action in the list, and specify the length of the period during which the specified action will apply.

   SYSTEM RESPONSE: The selected alarm already appears in the **Selected alarms** list.

6. To add other alarms to this schedule, select them in the **Available alarms** list, and click the down arrow button to add them to the **Selected alarms** list.

   TIP: Multiple alarms can be selected at once by holding down the **Shift** or **Ctrl** key while clicking.

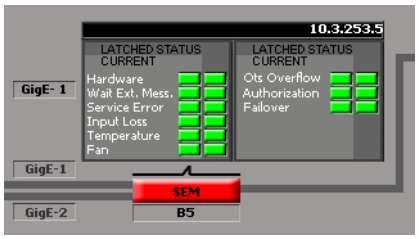
7. To remove alarms from the **Selected alarms** list, select them and click the up arrow button.
8. Click **OK**.

Example — Monitoring a Virtual Alarm

The following example shows how to investigate the error status of a virtual alarm. In this example, let's consider a Web page set up to monitor a signal path that contains an SNMP device such as a Motorola SmartStream Encryptor/Modulator (SEM). The Web page might represent the SEM portion of the signal path as shown below.

The SEM is represented by a button that corresponds to a virtual alarm with several sub-alarms. Some of the sub-alarms are displayed in a panel on the Web page (**Hardware**,

Temperature, **Fan** etc.). The panel shows the *current* and *latched* statuses of these sub-alarms, while the button shows the *overall* status of the SEM virtual alarm.

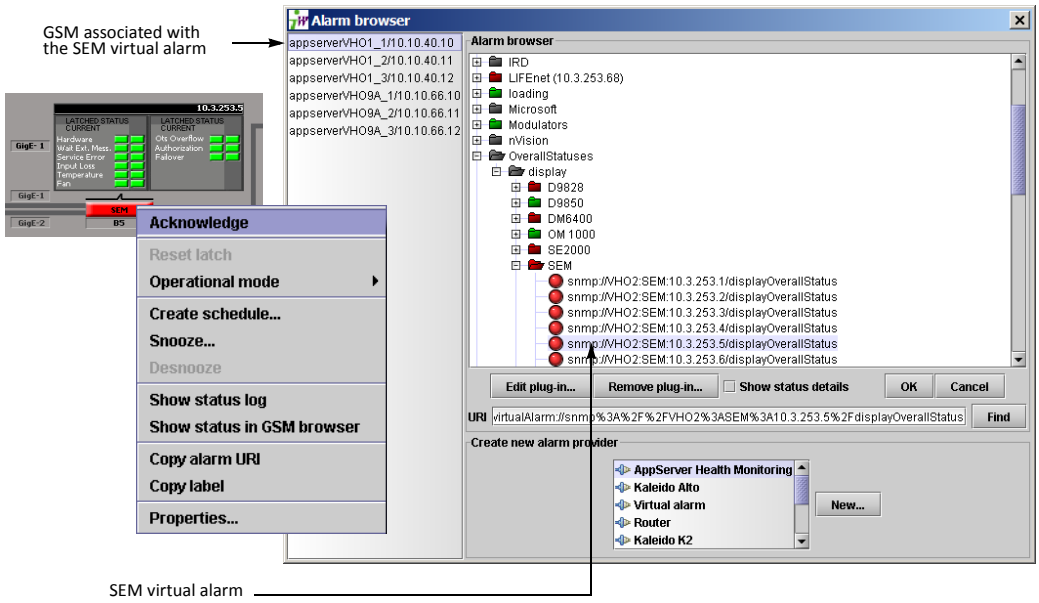


The button is red, indicating a problem with the SEM. But the status panel is all green, indicating that the problem must come from another source. Here's how to go about tracking the problem down:

To track the problem

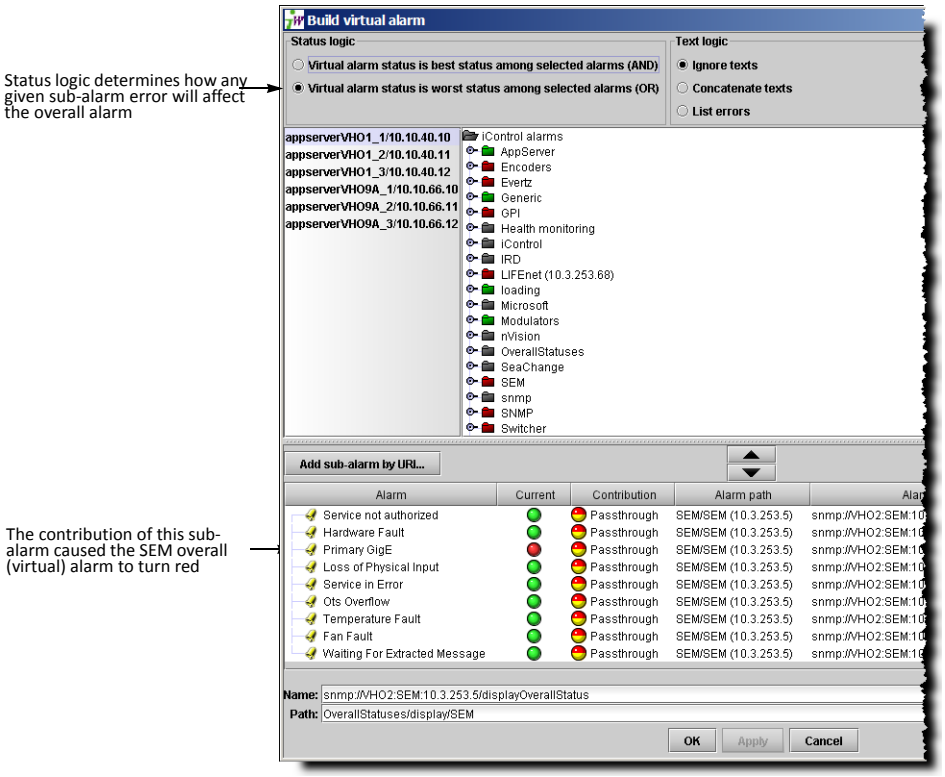
1. Right-click the SEM button, and then select **Show status in GSM browser** from the drop-down menu.

   SYSTEM RESPONSE: The GSM Alarm browser window appears, with the virtual alarm highlighted (the GSM running the SNMP plug-in instance for this particular SEM is also highlighted).



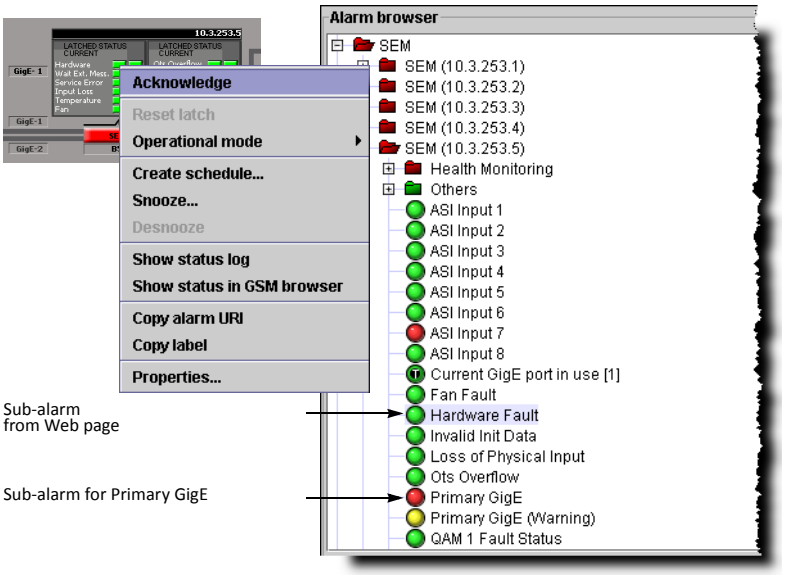
2. Click **Edit plug-in**.

   SYSTEM RESPONSE: The **Build virtual alarm** window appears, revealing the setup of the SEM virtual alarm, including a list of its sub-alarms. In this case, the Primary GigE sub-alarm is red—this is the likely source of the problem.

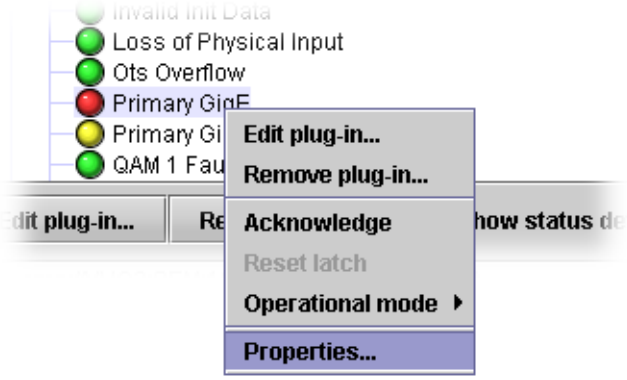


3. So far, we have only been looking at the SEM's overall alarm. At this point, it might be useful to look at the alarms for the device. The fastest way to do this is to return to the Web page and right-click any one of the SEM sub-alarms, and then select **Show status in GSM browser** from the drop-down menu.

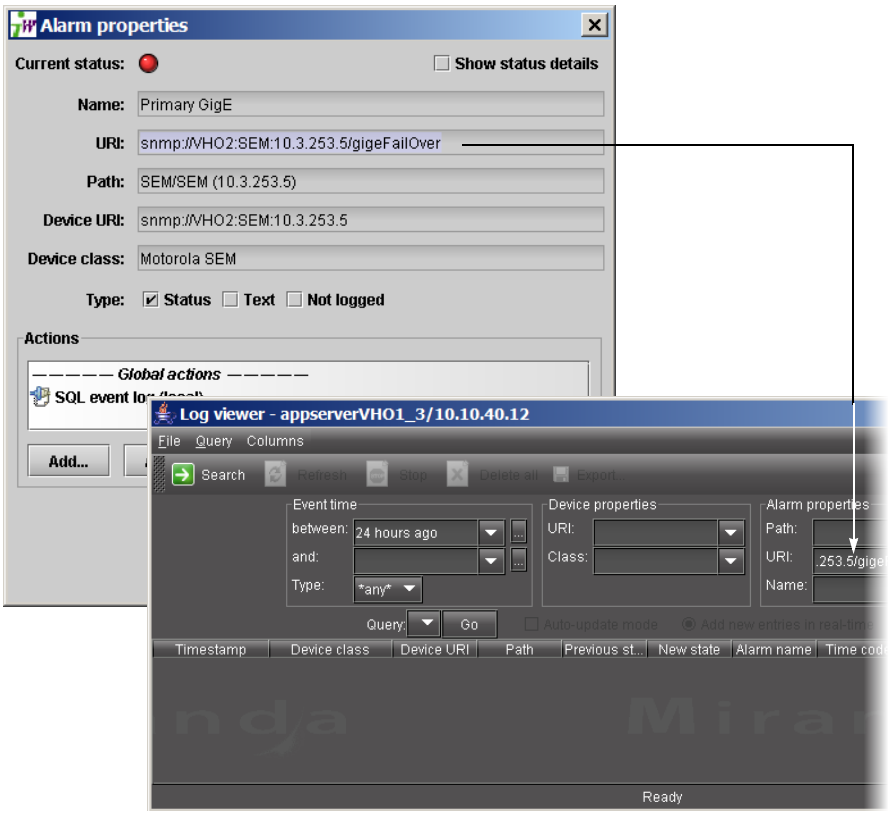
   SYSTEM RESPONSE: The GSM Alarm browser window appears, with the sub-alarm highlighted inside the folder containing all of the SEM's sub-alarms. Looking a little further down the list, we can se the Primary GigE sub-alarm is red.



4. Right-click the *Primary GigE* sub-alarm and click **Properties**.



SYSTEM RESPONSE: The **Alarm properties** window appears. You can copy the URI for this alarm and use it to search the Event and Incident Logs (see Searching the Event or Incident Log Database, on page 142).



5. Assuming you are able to resolve the problem, you would observe the following changes in iControl:
   - The SEM alarm status on the Web page returns to normal (green).
   - The Log Viewer displays a new entry reflecting the changed alarm status (returning from error to normal).
   - In the GSM Alarm Browser, the status of the SEM overall alarm and of the Primary GigE sub-alarm return to normal (green).
   - In iC Navigator, the status of the SEM overall alarm returns to normal (green).

8 iControl and SNMP

Summary

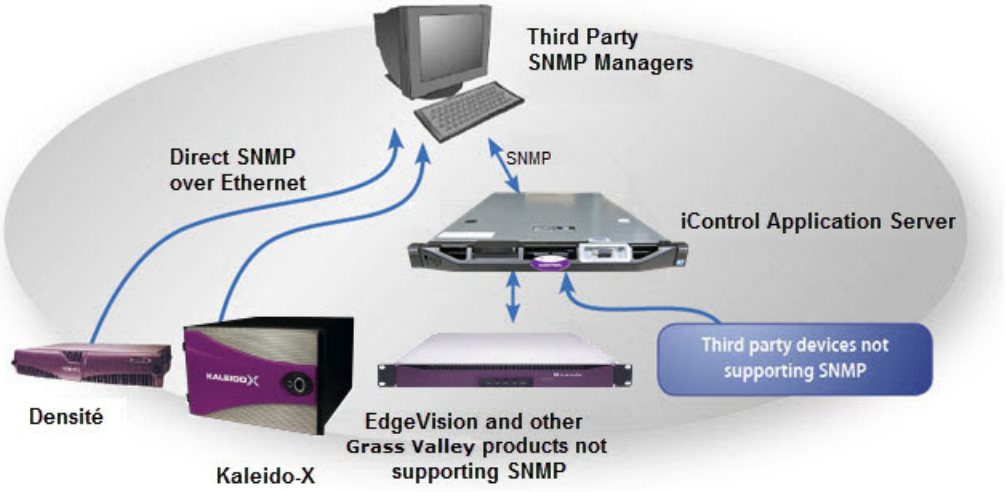
Overview

SNMP (Simple Network Management Protocol) has emerged as an important standard in the broadcast industry, allowing broadcasters to monitor the equipment from multiple vendors using a single, IP-based protocol. iControl provides SNMP support in two distinct and important ways.

iControl acts as an *SNMP manager* by reading the status of third party devices that support SNMP and have published their SNMP MIB (Management Information Base). It augments the status information using streaming video, audio and scope telemetry data gathered using Densité series cards and the Allégro streaming encoder/server.

In those cases where a third party SNMP management application (i.e. *Network Management Service*, or *NMS*) is deployed, iControl acts as an *SNMP agent* (or *north-bound interface*) reporting errors and status to the SNMP manager using the SNMP protocol and Grass Valley's own SNMP MIB.

For devices that do not provide IP connectivity, the iControl Application Server acts as an SNMP translator and provides SNMP agent functionality. The Application Server receives status information from the devices using their existing protocols, and will issue SNMP TRAPs and respond to SNMP GET messages on behalf of the devices below it. The Application Server further enhances SNMP agent capability by allowing users to create virtual alarms, which can be enabled or disabled according to a schedule, or slaved to an automation system.



Note: Grass Valley devices that provide IP connectivity at the frame—such as Densité and Kaleido—also offer direct SNMP support, allowing third party SNMP Manager applications to get status information using an SNMP GET and/or TRAP command.

Key Concepts

iControl as an SNMP Manager

iControl has integrated SNMP management functionality that enables it to both monitor and (where possible) control SNMP-enabled devices such as routers, encoders, multiplexers, etc. (for a list, see the *Third Party SNMP Device* document available from iControl's *Startup* page).

iControl SNMP management functions are implemented by SNMP drivers. Once installed and configured, they allow iControl to communicate with the corresponding SNMP agents running on the devices being monitored. For example, if you install the driver for an

integrated receiver/decoder (IRD), and then enable the SNMP agent on the IRD itself, iControl will be able to get status information on the device by polling or querying the IRD's agent, and to issue controls (such as *restart*), if they are supported.

A generic SNMP manager is also available that allows you to write your own SNMP drivers.

> **Note:** The generic SNMP manager and third party SNMP drivers are not included in the basic iControl package. They must be purchased separately. Contact your Grass Valley sales representative for details.

iControl SNMP Agents

iControl SNMP agents allow third party SNMP managers, such as Spectrum, to monitor an iControl configuration.

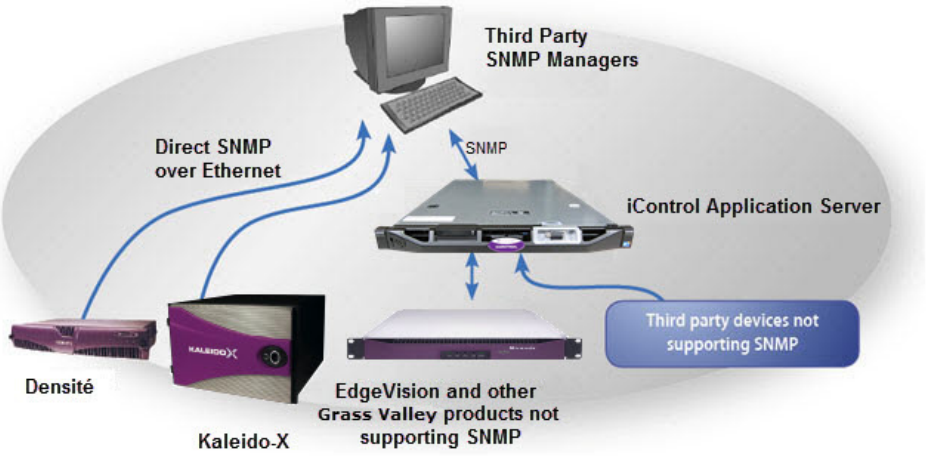
> **IMPORTANT:** If you choose to take advantage of iControl's support for the SNMP version 3 protocol for its added security, and your Application Server is an SNMP agent, you must first create default user templates and then create user profiles with the desired privilege levels. For more information, see Preparing an Application Server (as SNMP Agent) to use SNMPv3, on page 440.

There are two types of iControl SNMP agents:

- the *GSM SNMP Agent*, which is an iControl plug-in
- the *Net-SNMP* agent, part of a popular open-source package (www.net-snmp.org)

GSM SNMP Agent

The GSM SNMP agent is an iControl plug-in that allows reporting statuses and alarms for all managed devices over SNMP. It reports the status and alarms of cards in the form of an SNMP table that can be queried or polled by a third party SNMP manager. The GSM SNMP agent also enables iControl to send traps to a third party SNMP manager.



Net-SNMP Agent

Net-SNMP is a popular open-source health monitoring package consisting of an SNMP daemon (*snmpd*), an SNMP agent, and several utilities. Net-SNMP allows a third party SNMP manager to monitor various aspects of an Application Server, such as its network interface statistics, processor usage, disc usage, and memory usage.

MIB Browser

The MIB Browser enables loading, browsing, and searching MIBs, browsing the MIB tree, and performing all other SNMP-related functions. The MIB Browser also enables viewing and operating the data available through an SNMP agent in a managed device.

The MIB Browser:

- enables saving of MIB Browser settings.
- provides the capability to load and view MIB modules in a MIB tree.
- helps in traversing the MIB tree to view the definitions of each node for a particular object defined in the MIB.
- enables performing the basic SNMP operations, such as `GET`, `GETNEXT`, `GETBULK`, and `SET`.
- supports multi-varbind requests.
- enables real-time plotting of SNMP data in a graph. Line graph and bar graph are the two types of graphs that are currently supported.
- provides a user-friendly view of the SNMP table data. The table data can be viewed in a separate window called SNMP Table Panel.
- enables viewing the incoming traps using Trap Viewer and parsing of traps.

See also

For more information about the MIB Browser, see Opening the MIB Browser, on page 712.

Supported Alarms

All GSM alarms are supported by the iControl SNMP trap sender and can be polled via the GSM SNMP Agent.

iControl automatically discovers devices in the system. All Densité cards have their own sub-folders under the folder **iControl**, and each card's respective sub-folder contains all the alarms and statuses provided by this card.

The alarms for other Grass Valley (as well as third-party) solutions are visible in the GSM Alarm Browser under descriptive category folders such as **EDGE** (for iC Edge alarms and statuses), **Cycling** (for cycling engine alarms and statuses), and **Router** (for router alarms and statuses). Additionally, other alarms related to either the Application Server itself or to generally abstract categories appear in the GSM Alarm Browser in functional category folders like **Health monitoring** (for Application Server health), **Scripted alarms**, and **Virtual alarms**.

Further Reading

- *Getting Started with SNMP* — `http://www.linux-mag.com/id/1054/`
- *Monitoring Linux Hosts with SNMP* — `http://www.linux-mag.com/id/1080/`
- *Network Device Interrogation* — `http://www.linux-mag.com/id/899`

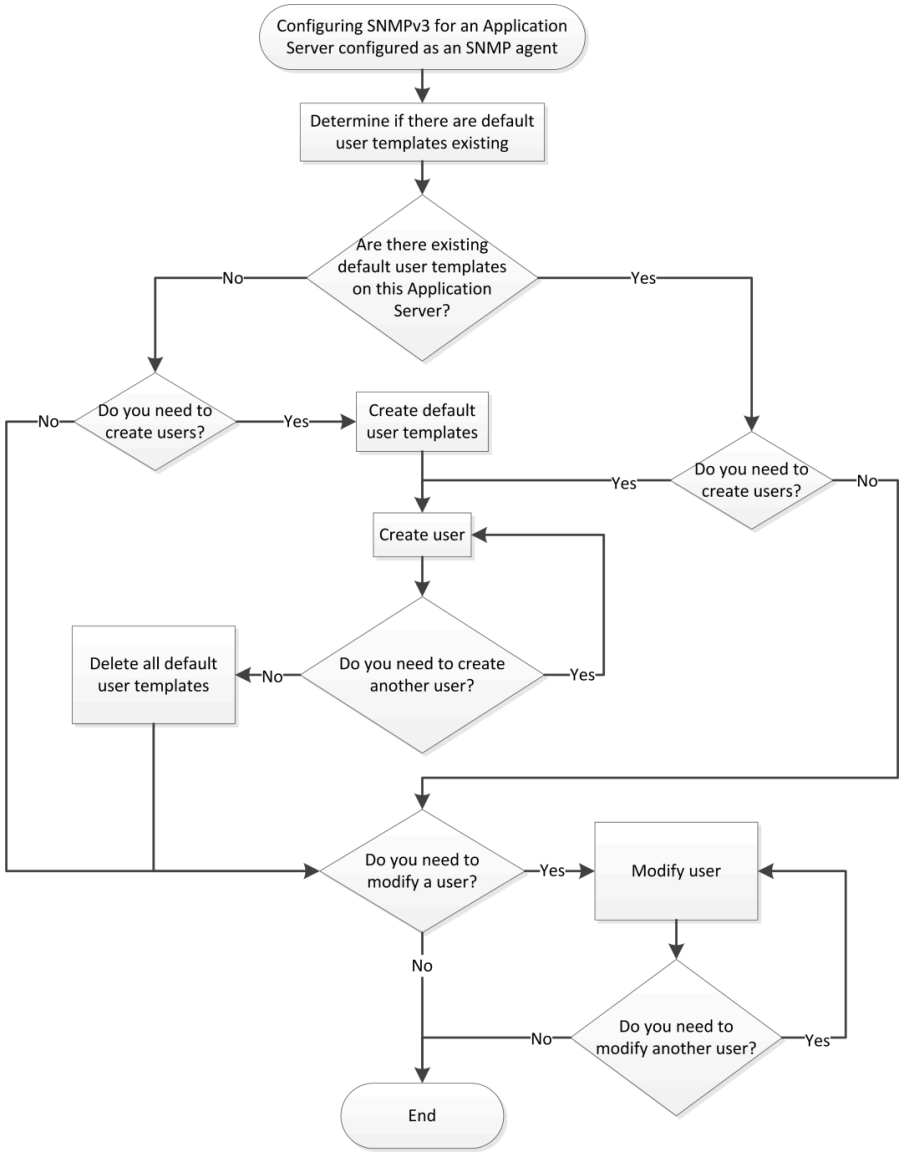
Sample Workflows

[Workflow]: Configuring SNMPv3 User Profiles in iControl

If you would like to take advantage of iControl's support of SNMPv3 and its enhanced security features, you will have to perform some initial tasks on the Application Server, first. These tasks require a PuTTY client application on your client PC and network access to your Application Server.

IMPORTANT:

- iControl's default setting is to use SNMPv1. If you would like to use SNMPv3 and your Application Server will take on the role of SNMP agent, you must first perform user configuration tasks.
- It is not necessary to configure user profiles or user templates if your Application Server is polling external devices in SNMPv3 mode (that is, if your Application Server is **NOT** an SNMP agent).
- Grass Valley highly recommends deleting your default user templates after you have finished creating your user profiles. Failure to do so could pose a security risk since the template passwords are hard-coded.



Flowchart for configuring SNMPv3 on an SNMP agent Application Server

Note: Use the following sequence of workflow procedures only in the context of the flowchart.

Workflow: Configuring SNMPv3 user profiles in iControl

1.	Determine if there are default user templates existing on your Application Server using the `list` command (see Miscellaneous User Configuration Tasks, on page 450). If the `list` command returns the `userNone`, `userAuthPriv`, and `userAuthNoPriv` template profiles, then these templates exist on this Application Server.
2.	Create default user templates (see Creating Default User Templates, on page 440).

Workflow: Configuring SNMPv3 user profiles in iControl (*Continued*)

3.	Create users, as required (see page 441).
4.	Delete default user templates (see Deleting a User Profile, on page 446).
5.	Modify users, as required (see page 446).

Additionally, there are several other user actions you may perform within the context of user configuration. They do not necessarily fall within the workflow, above, and you may perform them as stand-alone procedures (see Miscellaneous User Configuration Tasks, on page 450).

[Workflow]: Creating an SNMP Driver

iControl's **SNMP Driver Creator** allows you to create, modify, delete, publish, and initiate SNMP drivers. Once you have entered the required information into **SNMP Driver Creator** using the **SNMP driver configuration** tab and **Alarms** tab, you can click the **Script editor** tab to work directly with the generated script.

Note: In addition to those procedures called upon from this workflow, there are several other procedures involving **SNMP Driver Creator** that you may wish to perform as standalone tasks. They are:

- Editing an Alarm on page 482
- Editing a Driver's Generated Script on page 483
- Editing an Alarm Map, Trap Map, or Poller Profile on page 483
- Loading a Driver into SNMP Driver Creator on page 487
- Removing a Custom SNMP Driver from an Application Server on page 487

The following is a sample workflow for creating an SNMP driver:

Sample workflow: Creating an SNMP Driver

1.	Open **SNMP Driver Creator** (see page 713).
2.	Load the required MIB modules for the device you intend to link to with the new SNMP driver (see Loading a MIB Module into SNMP Driver Creator, on page 457).
3.	Configure the new driver (see Configuring an SNMP Driver's Settings, on page 462).
4.	Create an alarm (see page 464).
5.	**[OPTIONAL]** Create a poller (see page 474).
6.	**[OPTIONAL]** Create an alarm map (see page 467).
7.	**[OPTIONAL]** Create a trap map (see page 470).
8.	Add a MIB OID getter and variable getter to the script (see page 476).
9.	Verify the driver script syntax (see page 485).
10.	Package the generated JavaScript source code (see page 478).
11.	Publish the generated script (see Publishing a Driver, on page 481).

Detailed Directions

Preparing an Application Server (as SNMP Agent) to use SNMPv3

Creating Default User Templates

IMPORTANT: Perform this procedure only once

You only need to perform this procedure once: prior to the first time SNMPv3 is used with your Application Server in the role of SNMP agent.

REQUIREMENTS

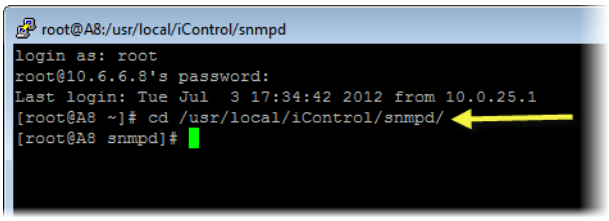
Make sure you meet the following conditions before beginning this procedure:

- You have logged in to your Application Server with a PuTTY secure shell (see page 674).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Configuring SNMPv3 User Profiles in iControl, on page 437).

To create default user templates

1. In your PuTTY secure shell, change directories to iControl's `snmpd` directory:

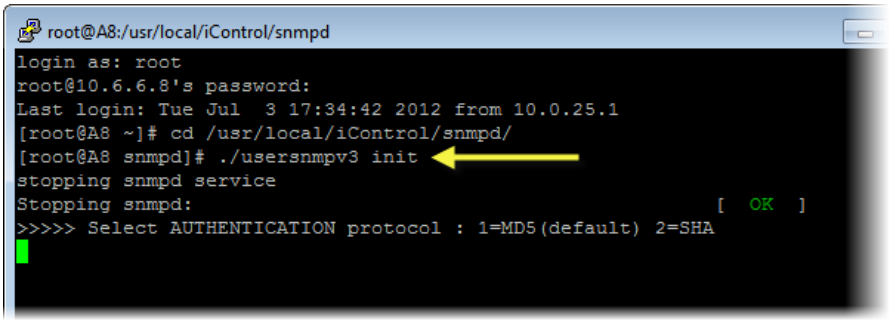
   `cd /usr/local/iControl/snmpd/`



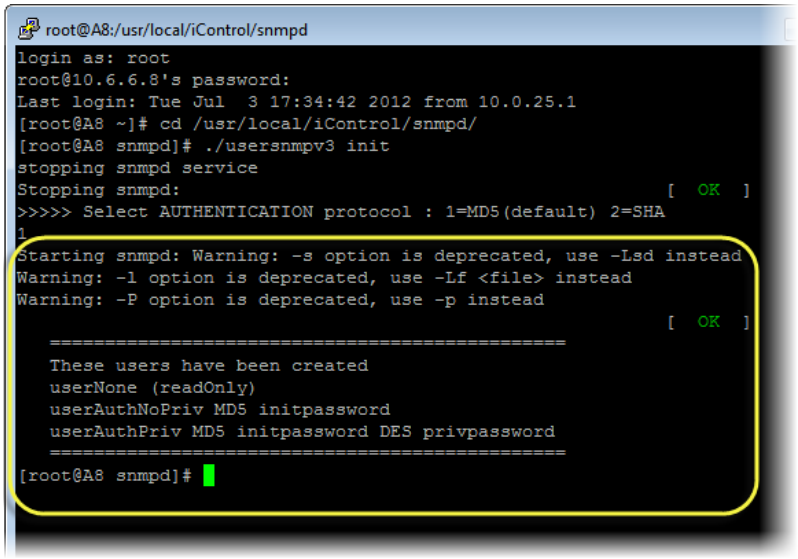
Command prompt after `cd` *command to change directories to* ***snmpd***

2. Create three default user profiles each representing one of the three possible security levels:

   `./usersnmpv3 init`



System response of the `init` *command*



Selecting MD5 as authentication protocol

As shown, the three user templates created have the following characteristics:

User template passwords and their security parameters

User template name	Authentication?	Privacy?	Authentication password	Privacy password
`userNone`	NO	NO		
`userAuthPriv`	YES	YES	`initpassword`	`privpassword`
`userAuthNoPriv`	YES	NO	`initpassword`	

Creating SNMPv3 User Profiles

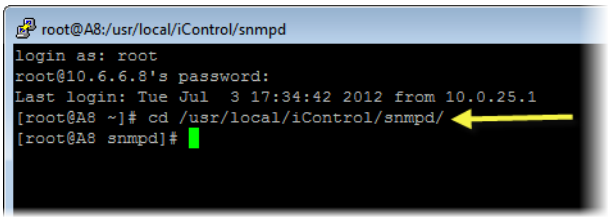
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- Default user templates currently exist on this Application Server. To verify that they exist, perform the `list` command. (see Miscellaneous User Configuration Tasks, on page 450). The SNMPv3 commissioning procedure has already been performed once for this Application Server (see page 440).
- You have logged in to your Application Server with a PuTTY secure shell (see page 674).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Configuring SNMPv3 User Profiles in iControl, on page 437).

To create an SNMPv3 user profile

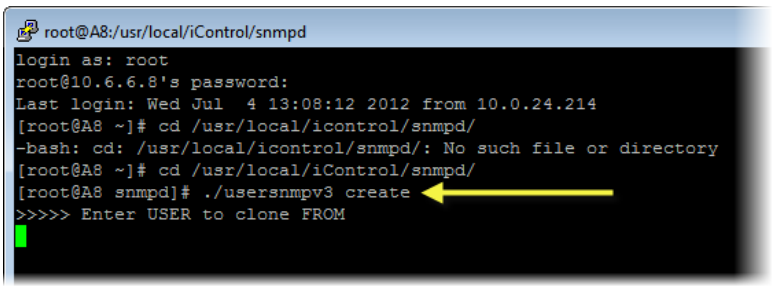
1. In your PuTTY secure shell, change directories to iControl's `snmpd` directory:
   `cd /usr/local/iControl/snmpd/`



Command prompt after `cd` *command to change directories to* ***snmpd***

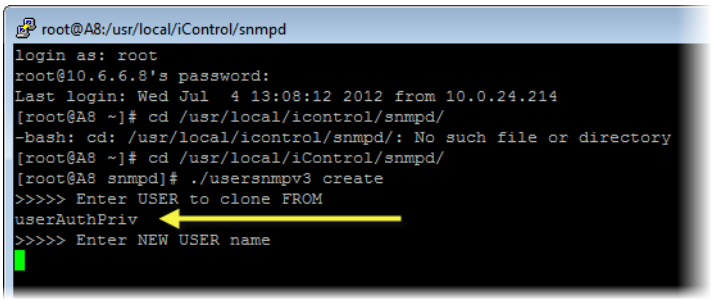
2. Create a new user profile:

   `./usersnmpv3 create`



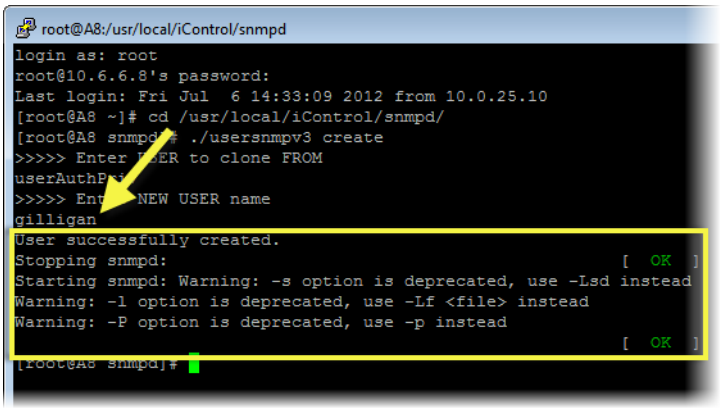
System response after `create` *command*

3. Specify the user template to clone from.



Specifying user template from which to clone new user

4. Specify the name you would like to assign to the new user profile.



Specifying a name for a new user profile

5. Change the new user profile's authentication and privacy passwords by performing the following sub-steps:

   a) Type:

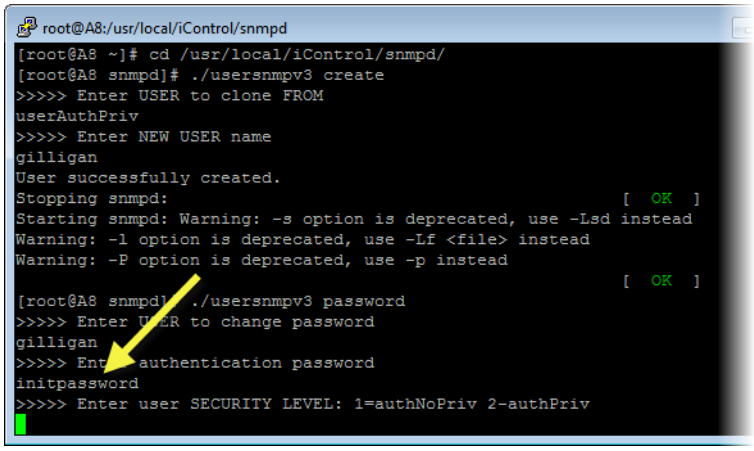
   `./usersnmpv3 password`

   SYSTEM RESPONSE: The system prompts you for the name of the new user profile.

   b) Type the new user profile name.

   SYSTEM RESPONSE: The system prompts you for the existing authorization password.

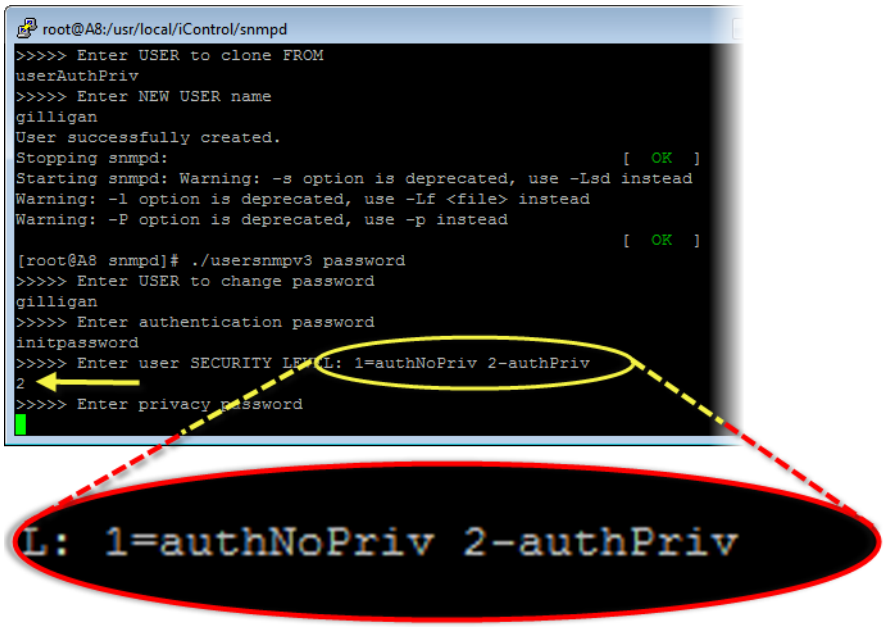
   c) Type the existing authentication password.



Specifying authentication password (change user passwords)

   SYSTEM RESPONSE: The system prompts you for the user security level.

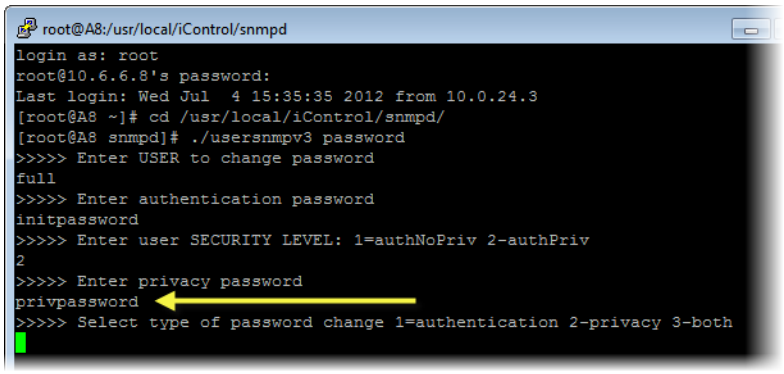
   d) Type the number corresponding to the security level of this user.



Specifying user security level (change user passwords)

SYSTEM RESPONSE: The system prompts you for the user's privacy password.

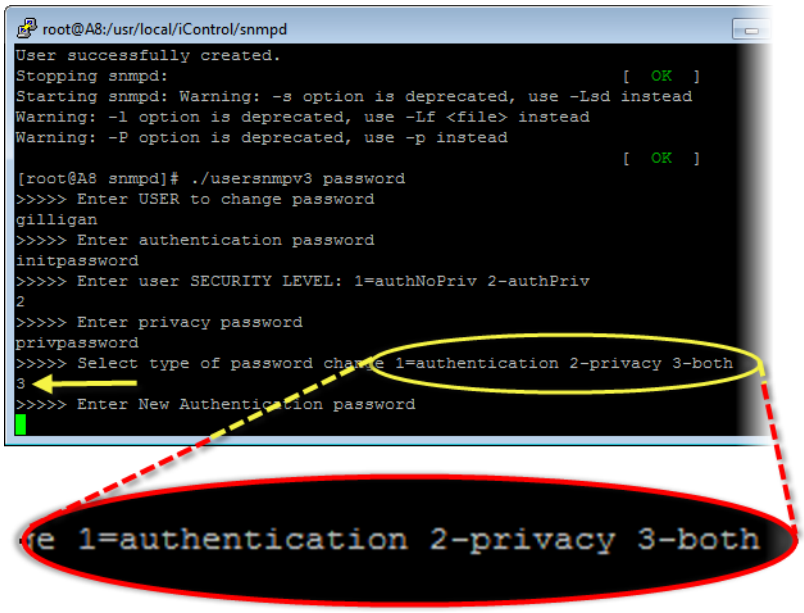
e) Type the user's privacy password (if applicable).



Specifying privacy password (change user passwords)

SYSTEM RESPONSE: The system prompts you for the type of password change.

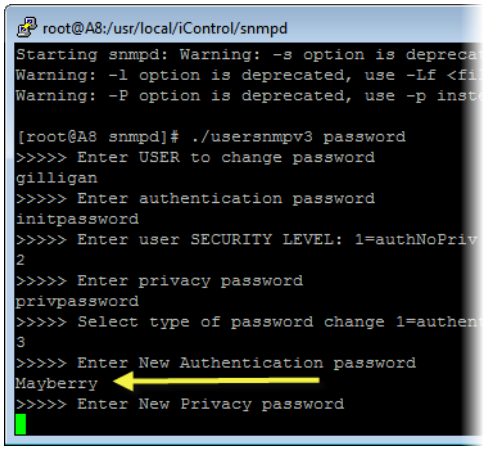
f) Type the number corresponding to the type of password change you would like to do.



Specifying which password to change

SYSTEM RESPONSE: The system prompts you for a new authentication password.

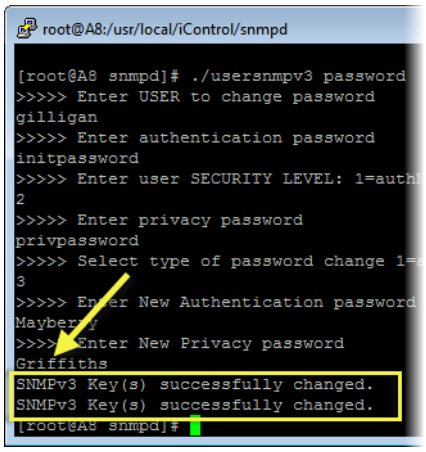
g) Type the new authentication password.



Specifying new authentication password

SYSTEM RESPONSE: The system prompts you for a new privacy password.

h) Type the new privacy password.



Specifying new privacy password; system response

SYSTEM RESPONSE: If the password change operation is successful, the system returns a confirmation message.

Modifying SNMPv3 User Profiles

Once a user profile has been created, you may later decide to change the authorization password or the privacy password, or else you may want to delete the user profile altogether.

Deleting a User Profile

REQUIREMENTS

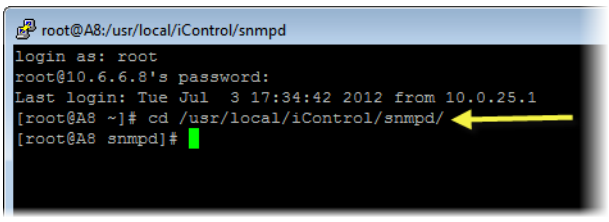
Make sure you meet the following conditions before beginning this procedure:

- The SNMPv3 commissioning procedure has already been performed once for this Application Server (see page 440).
- You have logged in to your Application Server with a PuTTY secure shell (see page 674).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Configuring SNMPv3 User Profiles in iControl, on page 437).

To delete an existing user profile

1. In your PuTTY secure shell, change directories to iControl's `snmpd` directory:

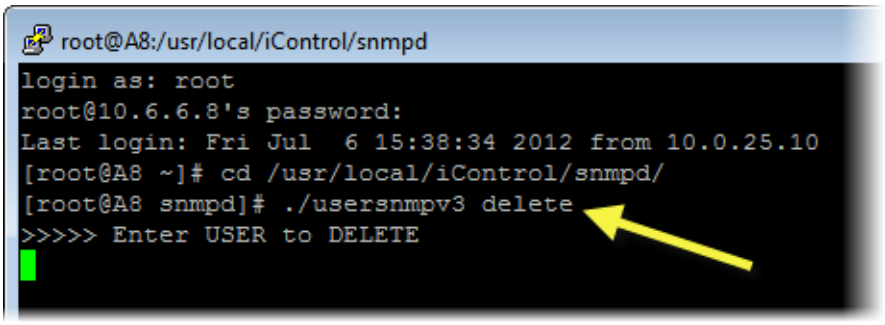
   ```
   cd /usr/local/iControl/snmpd/
   ```



Command prompt after `cd` *command to change directories to* ***snmpd***

2. Type the following:

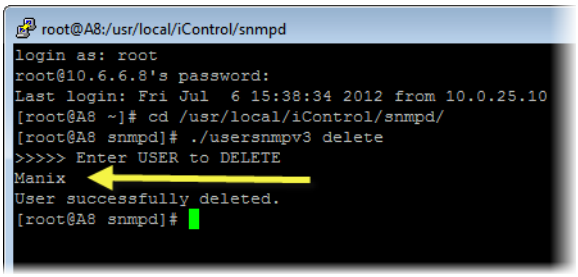
   ```
   ./usersnmpv3 delete
   ```



System response after `delete` *command*

The system prompts you for the name of the user profile to delete.

3. Type the name of the user profile you would like to delete.



Specifying user profile to delete; system response

SYSTEM RESPONSE: If the deletion operation is successful, the system returns a confirmation message.

Changing a User Profile's Passwords

REQUIREMENTS

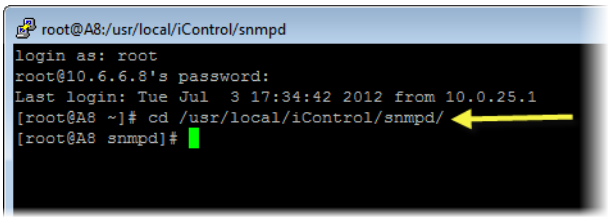
Make sure you meet the following conditions before beginning this procedure:

- The SNMPv3 commissioning procedure has already been performed once for this Application Server (see page 440).
- You have logged in to your Application Server with a PuTTY secure shell (see page 674).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Configuring SNMPv3 User Profiles in iControl, on page 437).

To change a user's authentication or privacy passwords

1. In your PuTTY secure shell, change directories to iControl's `snmpd` directory:

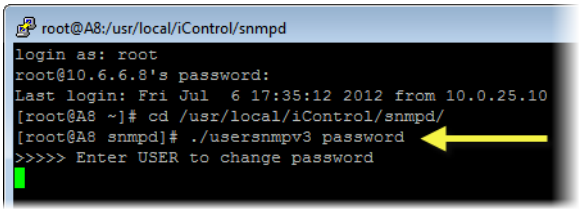
   ```
   cd /usr/local/iControl/snmpd/
   ```



Command prompt after `cd` *command to change directories to* ***snmpd***

2. Type the following command:

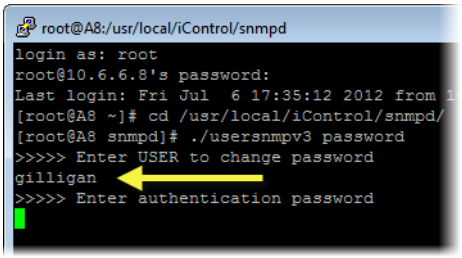
   `./usrsnmpv3 password`



System response after `password` *command*

   The system prompts you for the name of the user profile you would like to modify.

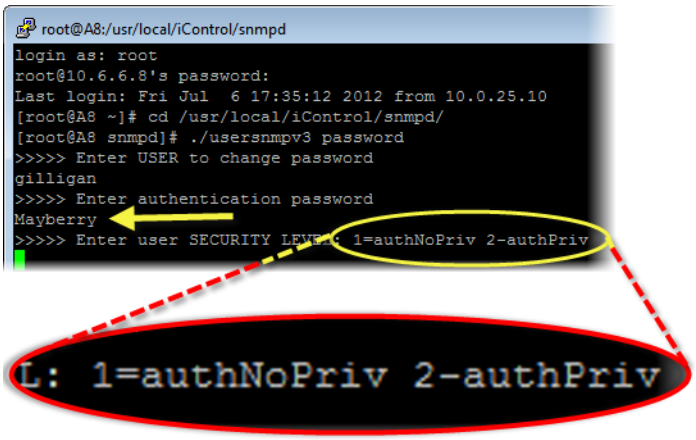
3. Type the name of the user profile you would like to modify.



Specifying user whose password(s) you want to change

   System Response: The system prompts you for the authentication password of the user you would like to modify.

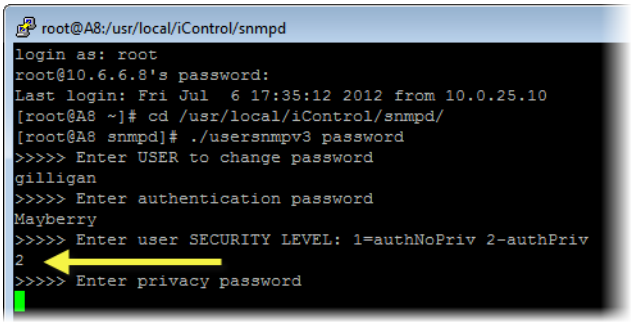
4. Type the authentication password.



Specifying existing authentication password

SYSTEM RESPONSE: The system prompts you for the user security level.

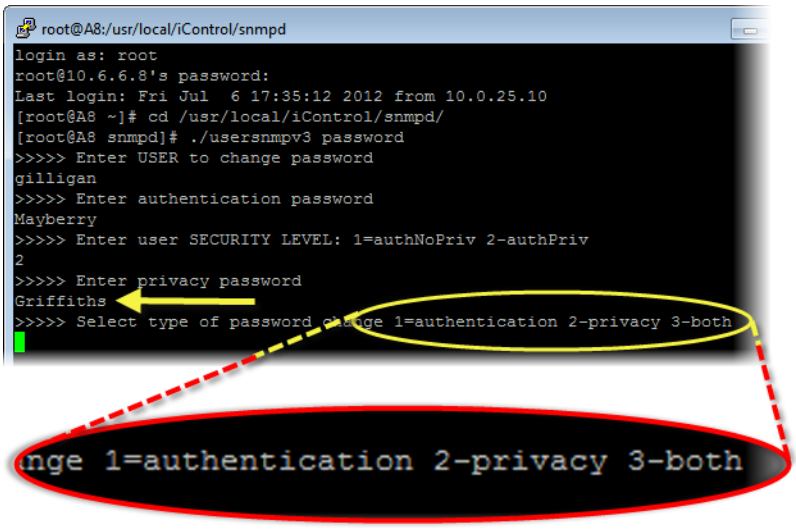
5. Type the number corresponding to this user profile's security level.



Specifying existing user security level

SYSTEM RESPONSE: The system prompts you for this user profile's privacy password.

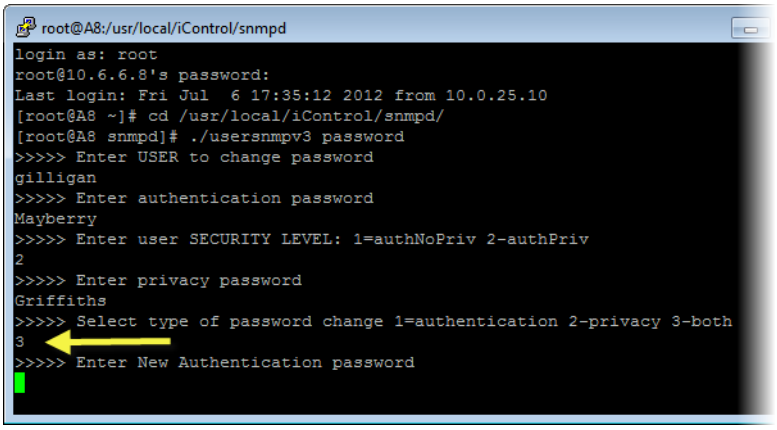
6. Type the privacy password.



Specifying existing privacy password

SYSTEM RESPONSE: The system prompts you for the desired type of password change.

7. Type the number corresponding to the desired type of password change.



Specifying which passwords to change

SYSTEM RESPONSE: The system prompts you for a new Authorization password (if either 1 or 3 was chosen).

8. Type a new Authorization password.

Miscellaneous User Configuration Tasks

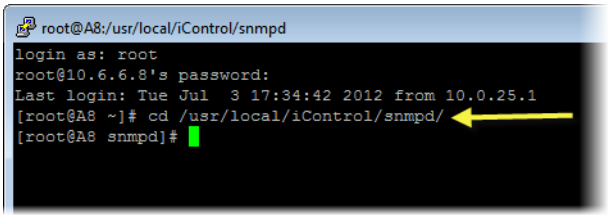
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- The SNMPv3 commissioning procedure has already been performed once for this Application Server (see page 440).
- You have logged in to your Application Server with a PuTTY secure shell (see page 674).

To perform miscellaneous user configuration tasks

1. In your PuTTY secure shell, change directories to iControl's `snmpd` directory:
   `cd /usr/local/iControl/snmpd/`



Command prompt after `cd` *command to change directories to* ***snmpd***

2. Type one of the following commands according to your needs:

To do this...	...do this...
List all existing user profiles.	Type the following in your PuTTY secure shell: `./usersnmpv3 list`
Test a user profile.	Type the following in your PuTTY secure shell: `./usersnmpv3 test`

iControl as an SNMP Manager

Enabling iControl to Manage SNMP Devices

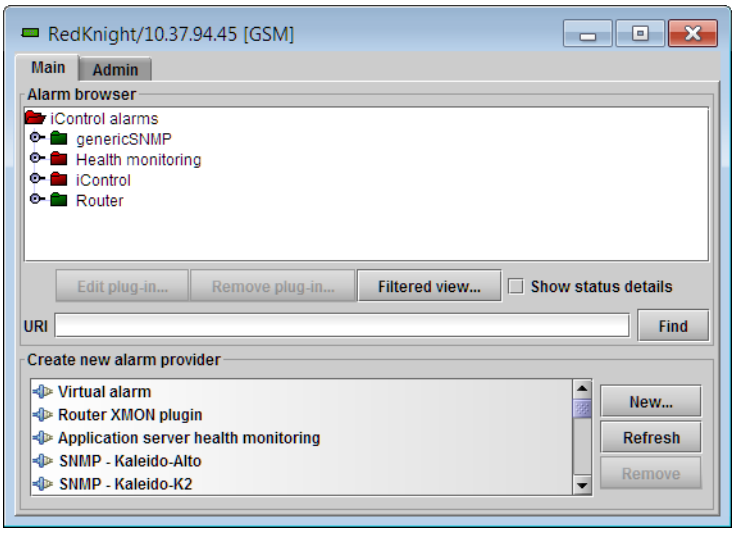
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

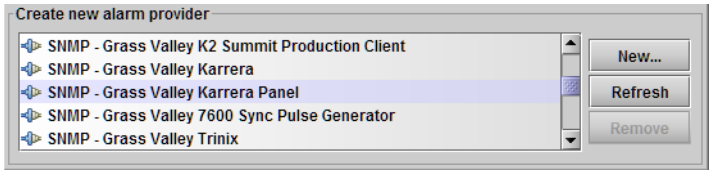
- There is an active connection between the iControl Application Server and the SNMP device.
- The SNMP agent on the device is enabled. Please consult the documentation that came with the device for instructions.
- You have opened iC Navigator (see page 697).

To enable iControl to manage an SNMP device

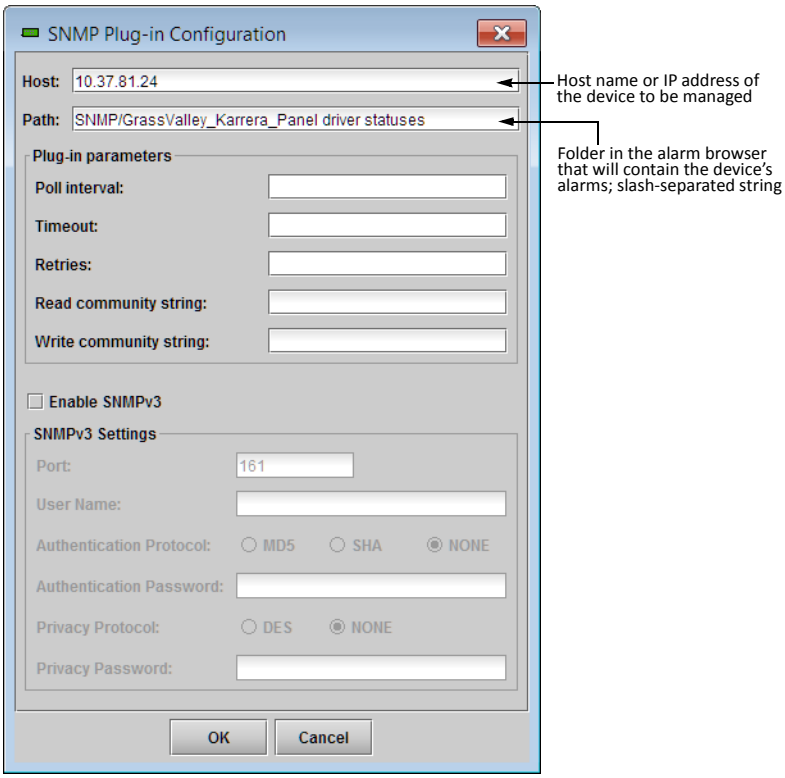
1. In **iC Navigator**, double-click on a GSM to open its **Alarm Browser** window.



2. In the **Create new alarm provider** list, select the SNMP driver that corresponds to the device you wish to manage, and then click **New**.

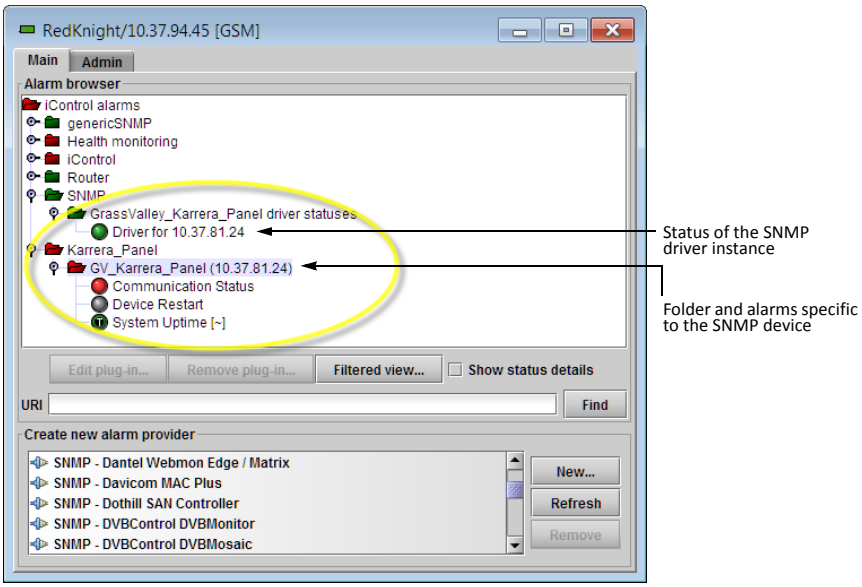


3. In the **SNMP Plug-in Configuration** window that appears, type the host name or IP address of the SNMP device, in the **Host** field.



4. Define the other parameters and settings as needed, and then click **OK**.

   In the *GSM alarm browser* window, alarms for the device will appear in a folder whose name includes the SNMP device type and its IP address. In a separate folder, under the path specified in the previous step, an alarm will be created to monitor the status of the SNMP driver instance. In both cases, iControl will create the folders if they do not already exist.



Enabling iControl to run Custom SNMP Drivers

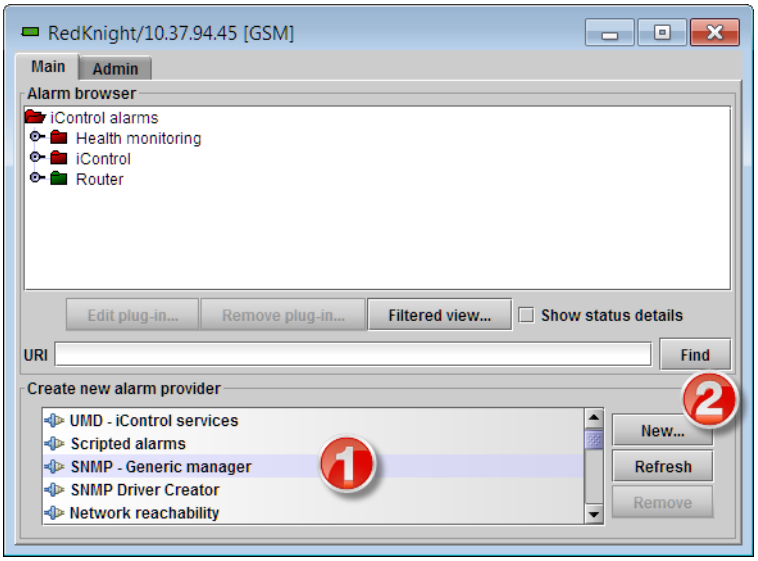
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

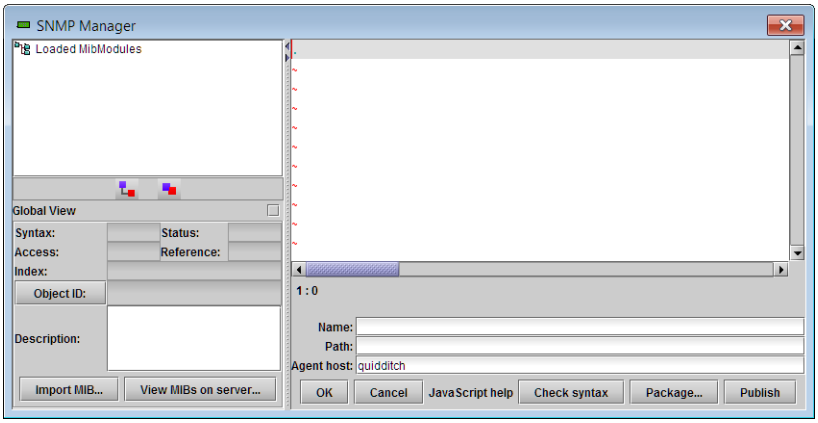
- There is an active connection between the iControl Application Server and the SNMP device.
- The SNMP agent on the device is enabled. Please consult the documentation that came with the device for instructions.
- You have a copy of any required MIB file on your hard drive.
- You have opened iC Navigator (see page 697).

To enable iControl to run a custom SNMP driver

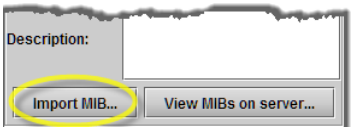
1. In **iC Navigator**, double-click on a GSM to open its **Alarm Browser** window.
2. In the **Create new alarm provider** list, select **SNMP - Generic manager**, and then click **New**.



SYSTEM RESPONSE: The **SNMP Manager** window appears.



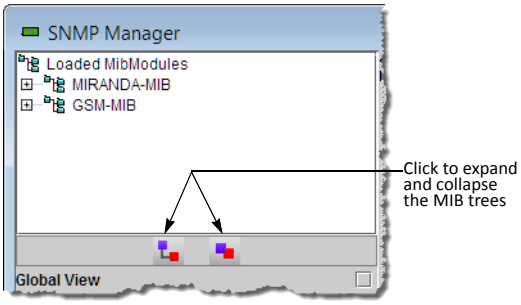
3. Click **Import MIB**.



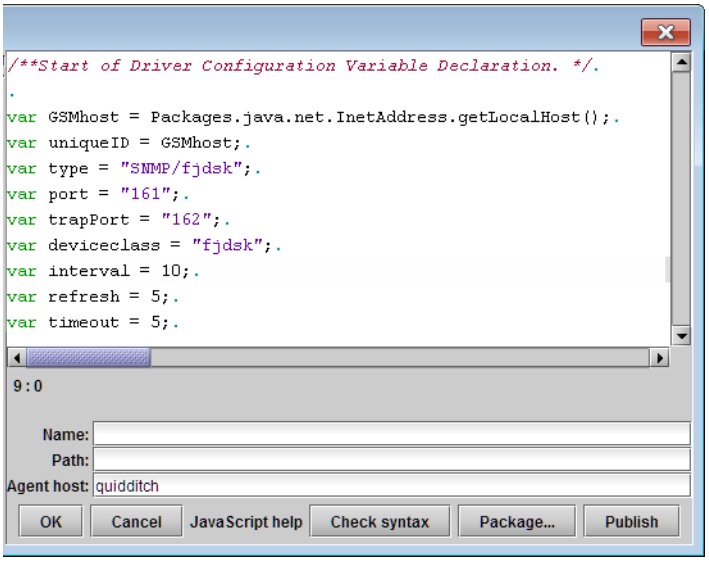
SYSTEM RESPONSE: The **Open** window appears.

4. Navigate to the appropriate MIB file, select it, and then click **Open**.

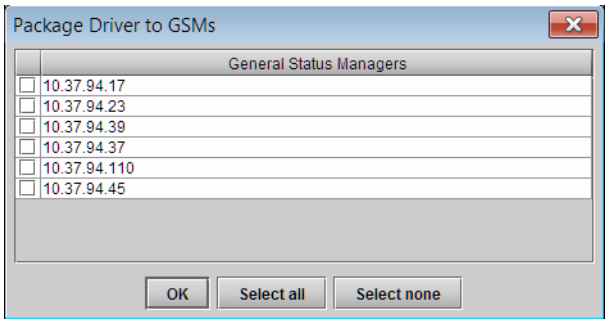
SYSTEM RESPONSE: The elements of the loaded MIB appear in the MIB browser pane.



5. Type or paste the script for your custom SNMP driver in the text editing area.



6. Type a name for your driver or driver template (depending on your purposes).
7. Type the path where you wish instances of this driver to be located in the GSM.
8. To create a driver *template:*
   a) Click **Publish**.
   The **Package Driver to GSMs** window appears.



b) Select the GSMs to which you wish to publish your new driver template, along with the loaded MIB file, and then click **OK**.

A message appears confirming that the driver template was sent to the selected GSMs.

c) Click **OK** to dismiss the message.

> **Note:** In the *GSM alarm browser* window, click **Refresh** to see the new driver template in the list of alarm providers.

9. To create a driver *instance:*
   - Type the host name or IP address of the SNMP device for which this driver is intended, and then click **OK**.

     The GSM will run your custom SNMP driver and begin publishing associated alarms.

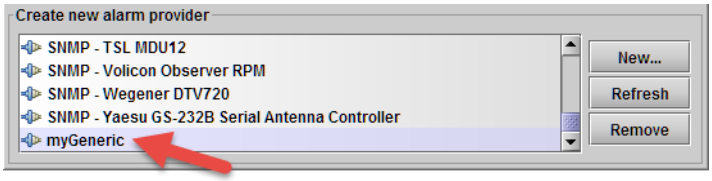
Republishing Custom SNMP Drivers

REQUIREMENT

Before beginning this procedure, make sure you have opened the Alarm Browser for the GSM where the SNMP driver you wish to republish is available (see page 710).

To republish a custom SNMP driver

1. In the **Create new alarm provider** list, select the custom SNMP driver you wish to republish, and then click **New**.



The **Generic SNMP User Plug-in** window appears.

2. In **Generic SNMP User Plug-in**, edit the custom script, or path, as needed.
3. Change the driver *name* (this is required), and then click **Republish**.
4. When prompted to confirm your intention, click **Yes**.

   The revised driver template is sent to the selected GSM.

Note: In the *GSM alarm browser* window, click **Refresh** to see the republished driver template in the list of alarm providers.

5. If you wish to also create a driver *instance* based on the revised driver template:
   - Type the host name or IP address of the SNMP device for which this driver is intended, and then click **OK**.

     The GSM will run your custom SNMP driver and begin publishing associated alarms.

Using SNMP Driver Creator

The documented procedures involving **SNMP Driver Creator** contain graphics showing **SNMP Driver Creator** as it appears when opened from **iC Navigator**. The user interface appears slightly different when opened from **iC Creator**.

Loading a MIB Module into SNMP Driver Creator

Loading a MIB Module from a Local File System

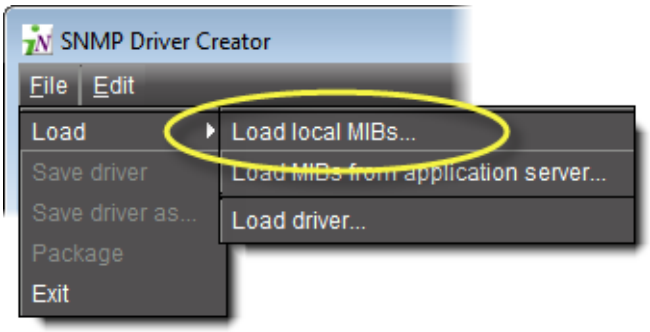
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

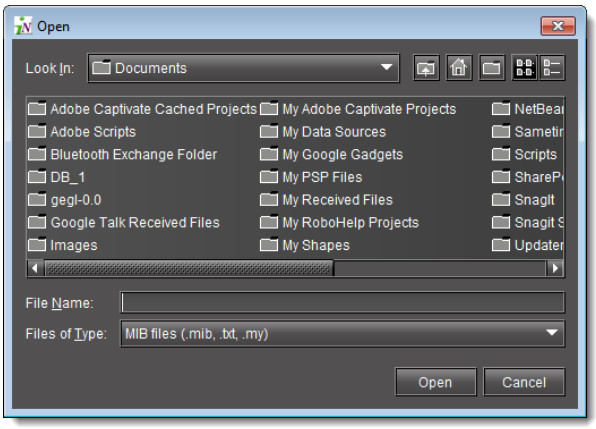
- You have opened the **SNMP Driver Creator** window (see page 713).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

To load a MIB module from a local file system

1. In the **SNMP Driver Creator** window, on the **File** menu, point to **Load**, and then click **Load MIB - Local**.

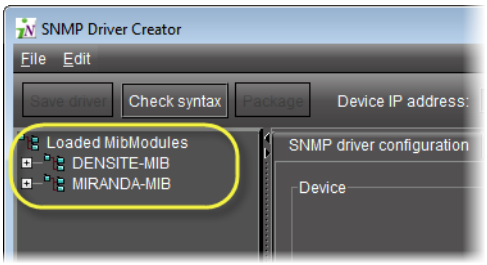


SYSTEM RESPONSE: The **Open** window appears.



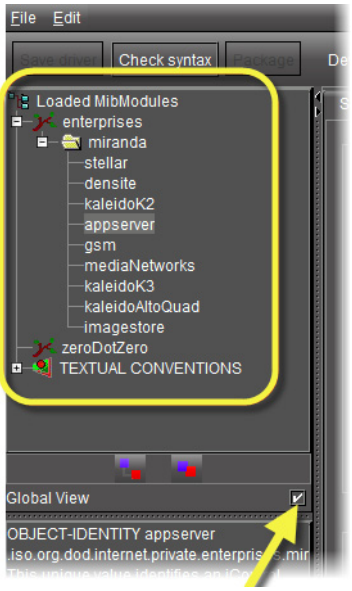
2. Browse for the MIB you would like to load, select it, and then click **Open**.

   SYSTEM RESPONSE: The loaded MIB's elements appear under **Loaded MibModules** in **SNMP Driver Creator**'s MIB Browser (left pane).

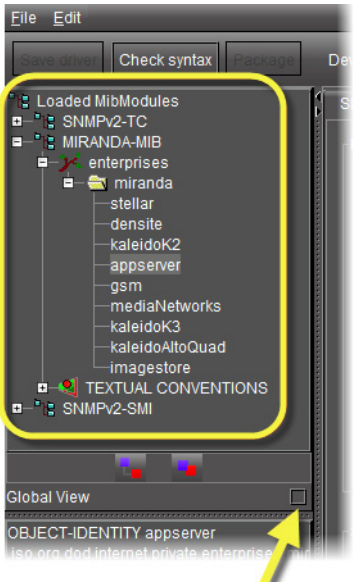


3. In the MIB browser (left pane), do one of the following:

   a) To display only the modules belonging to the selected MIB, select the **Global View** check box.



   b) To display a combined tree of all the loaded MIBs, clear the **Global View** check box.



Loading a MIB Module from an Application Server

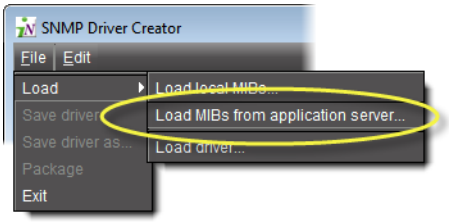
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened the **SNMP Driver Creator** window (see page 713).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

To load a MIB module from an Application Server

1. In the **SNMP Driver Creator** window, on the **File** menu, point to **Load**, and then click **Load MIB - Application Server**.

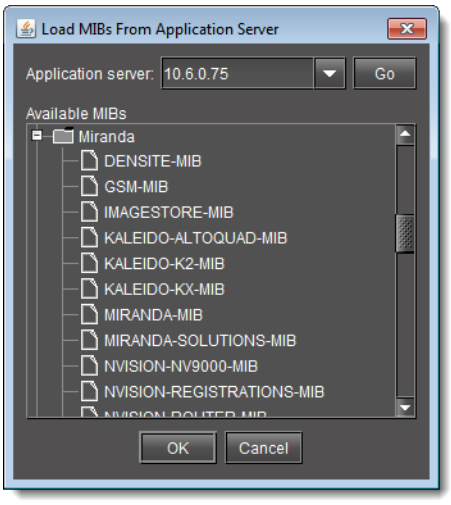


   System Response: The **Load MIBs from application server** window appears.

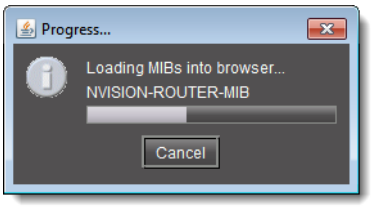
2. In the **Application Server** list, if your Application Server is not already displayed, select the IP address of the Application Server from which you would like to load a MIB, and then click **Go**.

   System Response: All visible MIBs on the selected Application Server appear in the **Available MIBs** list.

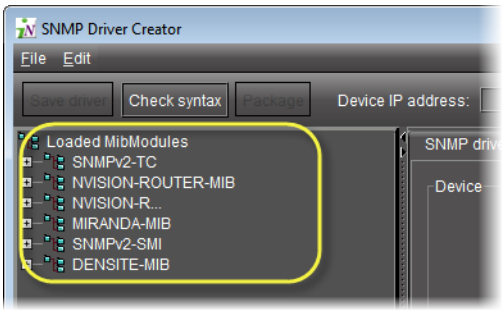
3. Select the MIB you would like to load and then click **OK**.



System Response: You may see a progress message.

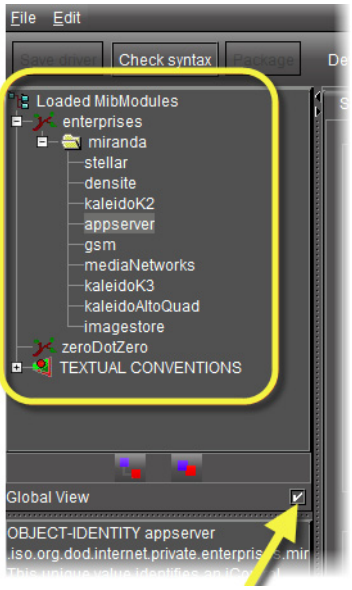


SYSTEM RESPONSE: The loaded MIB's elements appear under **Loaded MibModules** in **SNMP Driver Creator**'s MIB Browser (left pane).

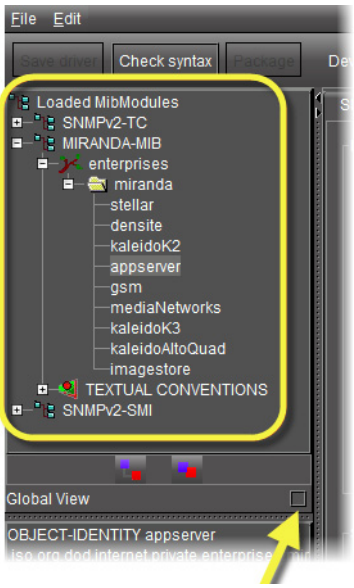


4. In the MIB browser (left pane), do one of the following:

   a) To display only the modules belonging to the selected MIB, select the **Global View** check box.



   b) To display a combined tree of all the loaded MIBs, clear the **Global View** check box.



Configuring an SNMP Driver's Settings

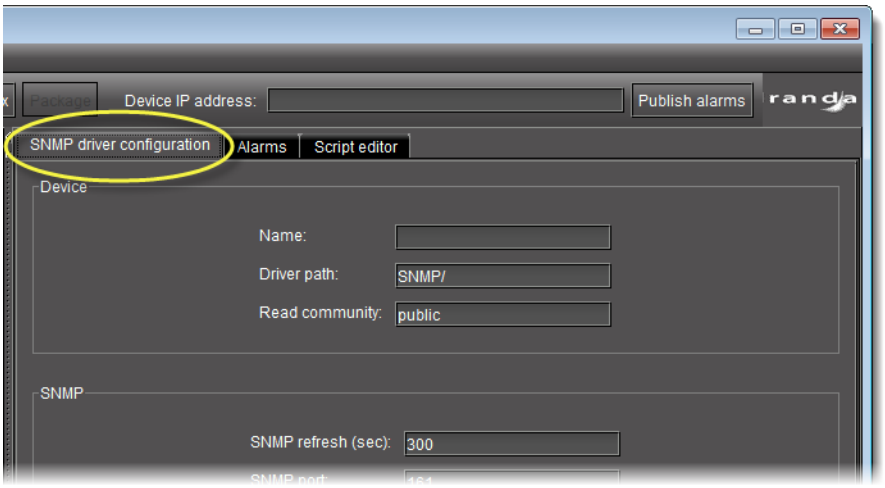
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened the **SNMP Driver Creator** window (see page 713).
- **[RECOMMENDED]:** You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

To configure an SNMP driver's settings

1. In the **SNMP Driver Creator** window, click on the **SNMP driver configuration** tab.

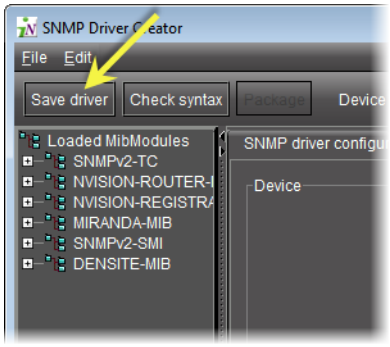


2. Input the required parameter information in the **Device** and **SNMP** areas.

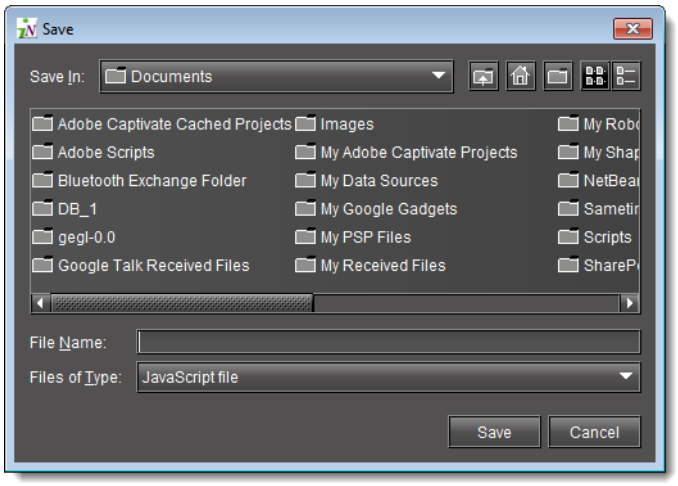
Note: The **Read community** field is optional. The remaining five fields are mandatory.

Parameter	Default value	Description
Name		Name of the driver
Driver path	`SNMP/[driver name]`	Location of the driver file
Read community **[OPTIONAL]**	`public`	SNMP password allowing retrieval of information from the SNMP agent.
SNMP refresh	300 seconds	Amount of time allowed to elapse between refreshes of the driver information (seconds); This parameter can be useful in the following situations: • If you have lost a trap that you are not also polling, but can and do poll on start-up. • If you are polling a table whose size may change over time • If you are generating virtual alarms and they might change over time
SNMP port	`161`	Port on the agent (target host) where `GET` and `PUT` requests are sent
SNMP trap port	`162`	Port on the Application Server where traps are received; typically corresponds to a configuration element on the agent (target host)

3. **[OPTIONAL]** Perform the following sub-steps if you would like to backup your script:
   a) Click **Save driver**.



SYSTEM RESPONSE: The **Save** window appears.



b) Navigate to the desired location on your local system, and then click **Save**.

SYSTEM RESPONSE: The new SNMP driver is saved as a JavaScript file (`*.js`).

Creating an Alarm in SNMP Driver Creator

Creating an Alarm by Dragging a MIB Element from the Alarm Browser Pane

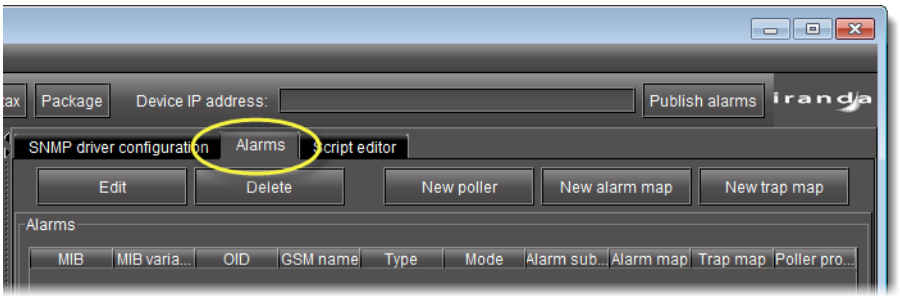
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

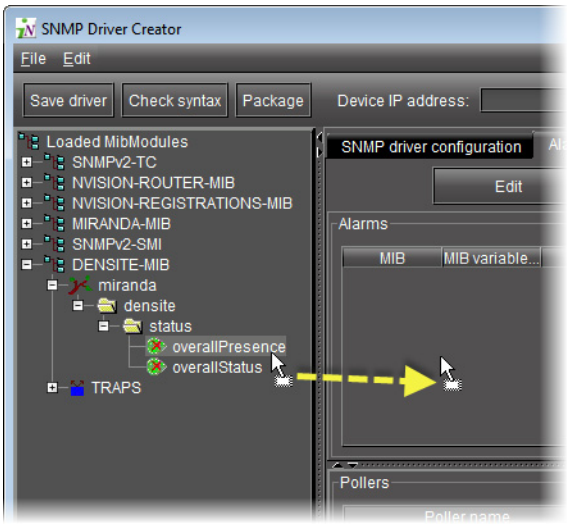
- You have opened **SNMP Driver Creator** (see page 713).
- You have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- You are displaying the **Design** view in **SNMP Driver Creator**.
- You have configured your driver settings (see page 462).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

To create an alarm by dragging a MIB element

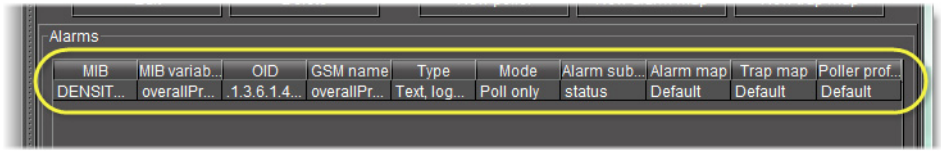
1. In **SNMP Driver Creator**, click the **Alarms** tab.



2. In the MIB Browser pane, select the desired MIB element from the loaded MIB modules (you may need to expand the folder tree to see it), and then drag the element to the **Alarms** table.



SYSTEM RESPONSE: A new alarm is created and listed in the **Alarms** table.



See also

For more information about editing an existing alarm any time after it has been created, see page 482.

Creating an Alarm with a MIB Element Shortcut Menu

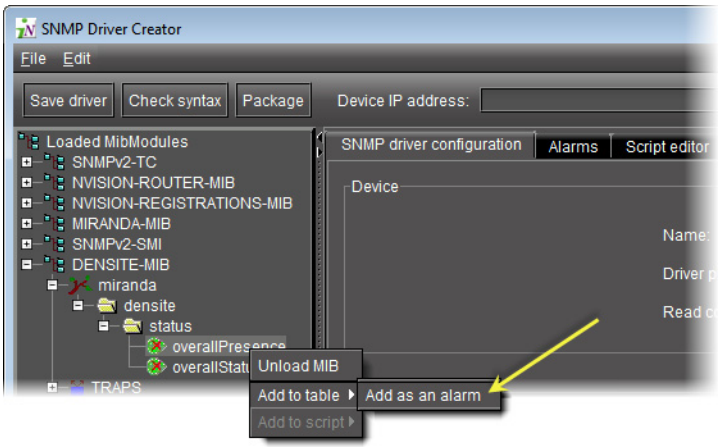
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

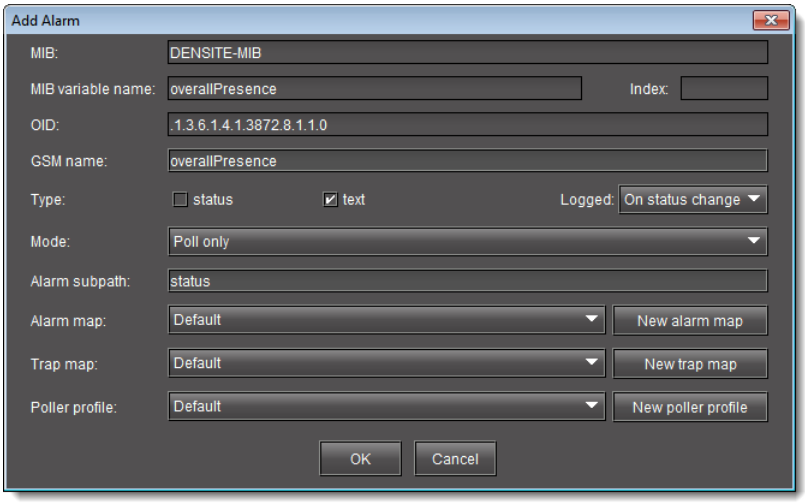
- You have opened **SNMP Driver Creator** (see page 713).
- You have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- You have configured your driver settings (see page 462).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

To create an alarm with a MIB element shortcut menu

1. In **SNMP Driver Creator**, click on the **SNMP driver configuration** tab in the main pane.
2. In the **MIB Browser** pane, right-click the desired MIB node from the loaded MIB modules, point to **Add to table**, and then click **Add as an Alarm**.



SYSTEM RESPONSE: The **Add Alarm** window appears, displaying relevant information about the MIB node.



3. Modify the alarm parameters as required.
   The parameters are as follows:

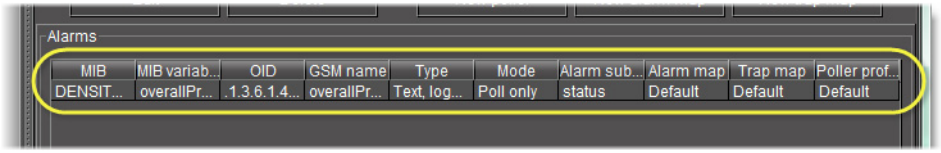
Parameter	Description
MIB	The MIB where the OID was retrieved from
MIB variable name	The label of the MIB node
OID	The object identifier (OID) value of the MIB node
GSM name	The name to be shown on the GSM for this alarm
Type	The type of alarm (status, text, or both). For more information about alarm types, see page 344.
Mode	The mode of the alarm

(*Continued*)

Parameter	Description
Alarm subpath	The path in the Alarm Browser tree where the alarm is created
Alarm map	The associated alarm map for this alarm
Trap map	The associated trap map for this alarm
Poller profile	The associated poller for this alarm

4. Click **OK**.

   SYSTEM RESPONSE: A new alarm is created and listed in the **Alarms** table.



See also

For more information about editing an existing alarm any time after it has been created, see page 482.

Creating an Alarm Map

There are several ways in which you can create an alarm map. The differences lie in the way in which you navigate to the **Create Alarm Map** window.

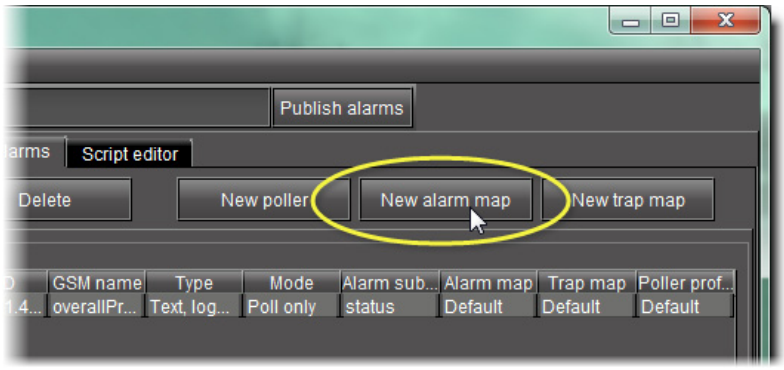
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **SNMP Driver Creator** (see page 713).
- You have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

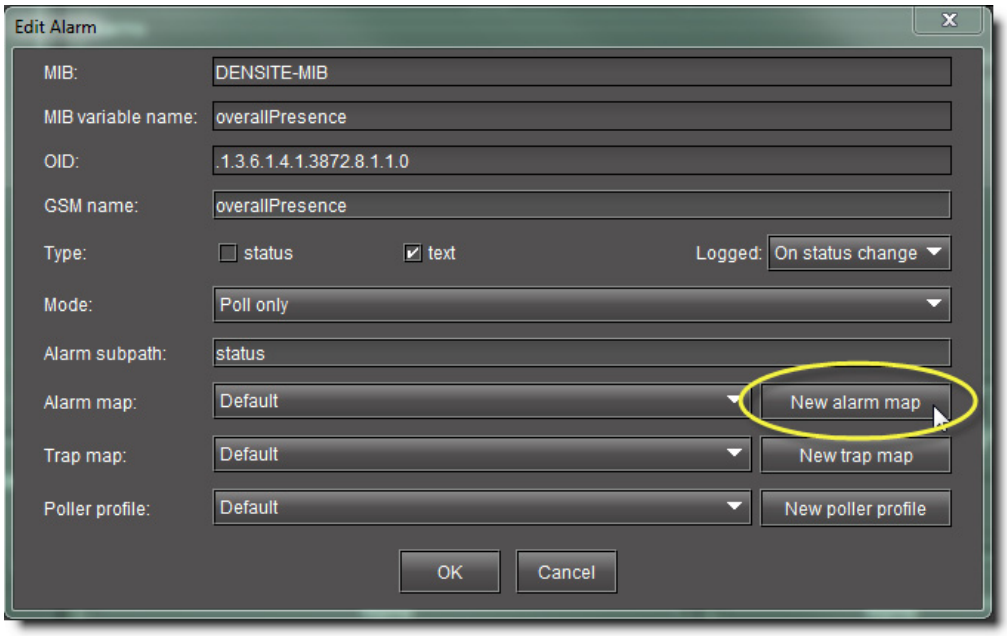
To create an alarm map

1. Open the **Create Alarm Map** window by doing only **ONE** of the following:
   - In **SNMP Driver Creator**, on the **Alarms** tab, click **New alarm map**.

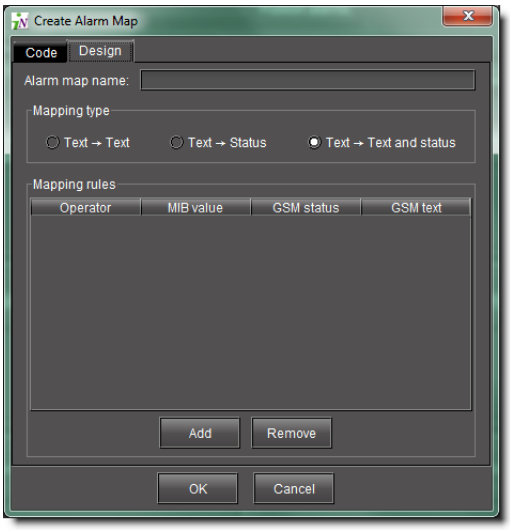


OR,

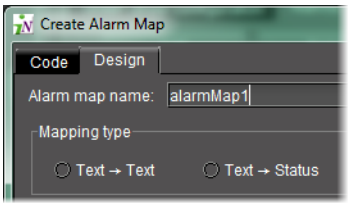
- In either the **Add Alarm** window or the **Edit Alarm** window, click **New alarm map**.



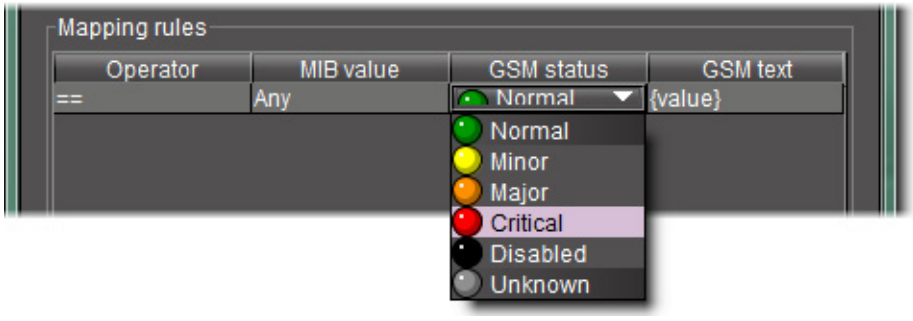
SYSTEM RESPONSE: The **Create Alarm Map** window appears.



2. On the **Design** tab, type a name into the **Alarm map name** field.



3. Click on one of the options in the **Mapping type** area.
4. For each mapping rule you would like to add, perform the following substeps:
   a) Click **Add** to generate an instance of the mapping rule template.
   SYSTEM RESPONSE: An unconfigured mapping rule appears in the **Mapping rules** list.
   b) In the row corresponding to the new mapping rule, click and configure each cell.



Notes

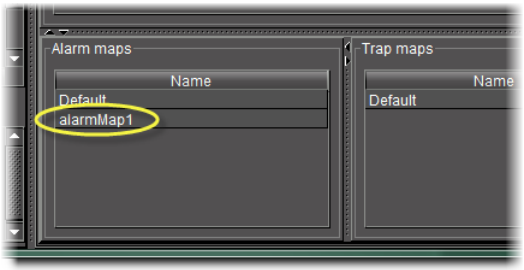
- In the case of the **Operator** and **GSM status** columns, you must click once. In the case of the **MIB value** and **GSM text** columns, you must double-click.

Notes (*Continued*)

- Depending on which cell you click, either select from one of the listed options or type the desired value to configure the parameter.

5. Click **OK**.

   SYSTEM RESPONSE: The new map appears in the **Alarm maps** area of the **Alarms** tab in **SNMP Driver Creator**.



See also

For more information about editing an existing alarm map any time after it has been created, see Editing an Alarm Map, Trap Map, or Poller Profile, on page 483.

Creating a Trap Map

There are several ways in which you can create a trap map. The differences lie in the way in which you navigate to the **Create Alarm Map** window.

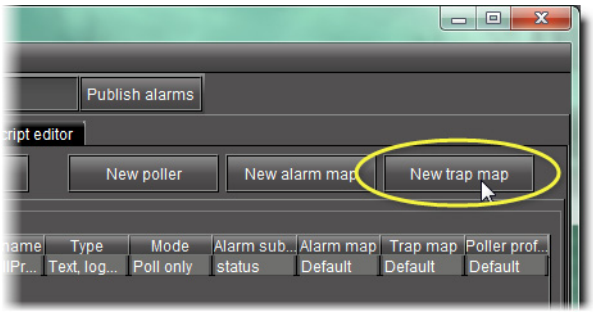
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **SNMP Driver Creator** (see page 713).
- you have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

To create a trap map

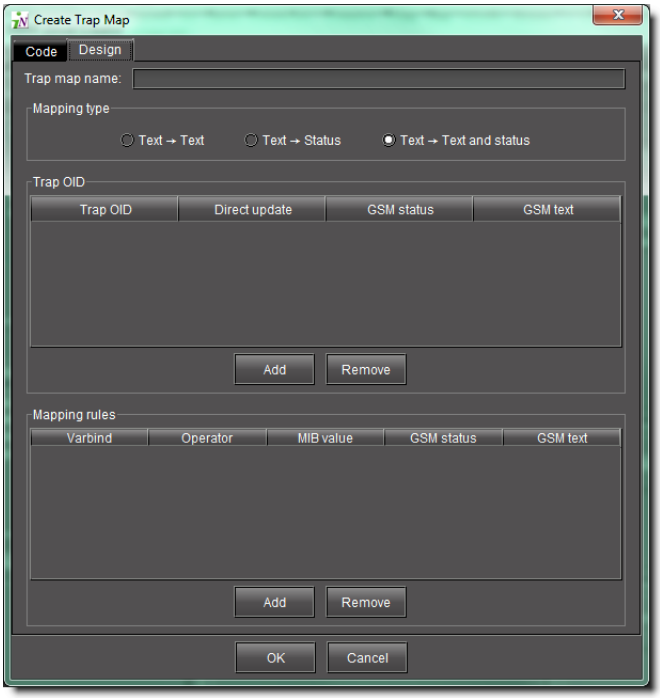
1. Open the **Create Trap Map** window by doing **ONE** of the following:
   - In **SNMP Driver Creator**, on the **Alarms** tab, click **New trap map**.



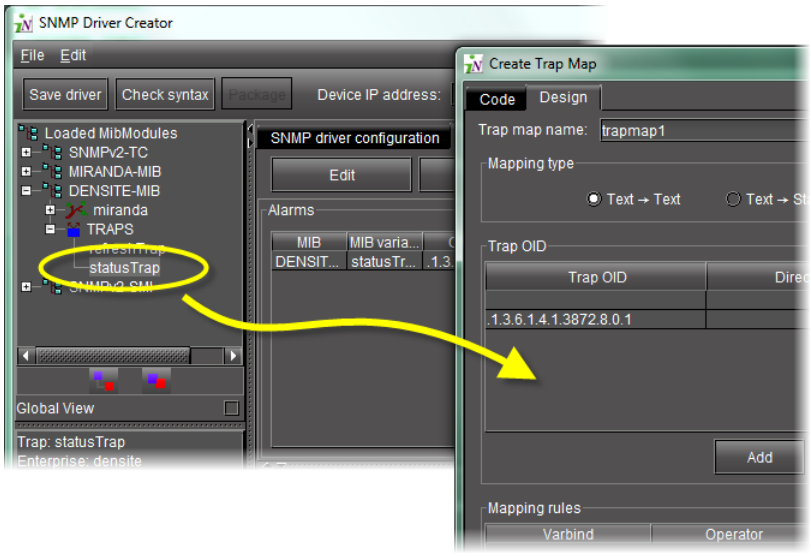
OR,

- In either the **Add Alarm** window or the **Edit Alarm** window, click **New trap map**.

SYSTEM RESPONSE: The **Create Trap Map** window appears.



2. On the **Design** tab, type a new trap map name.
3. Select a mapping type.
4. Do one of the following:
   - In the MIB pane of **SNMP Driver Creator**, drag a trap node to the **Trap OID** area of the **Create Trap Map** window.

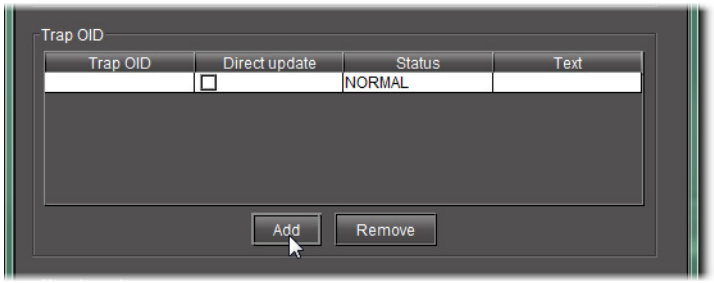


OR,

Perform the following sub-procedure in the **Trap OID** area of the **Create Trap Map** window.

a) Click **Add**.

SYSTEM RESPONSE: A highlighted, unconfigured trap OID row appears.

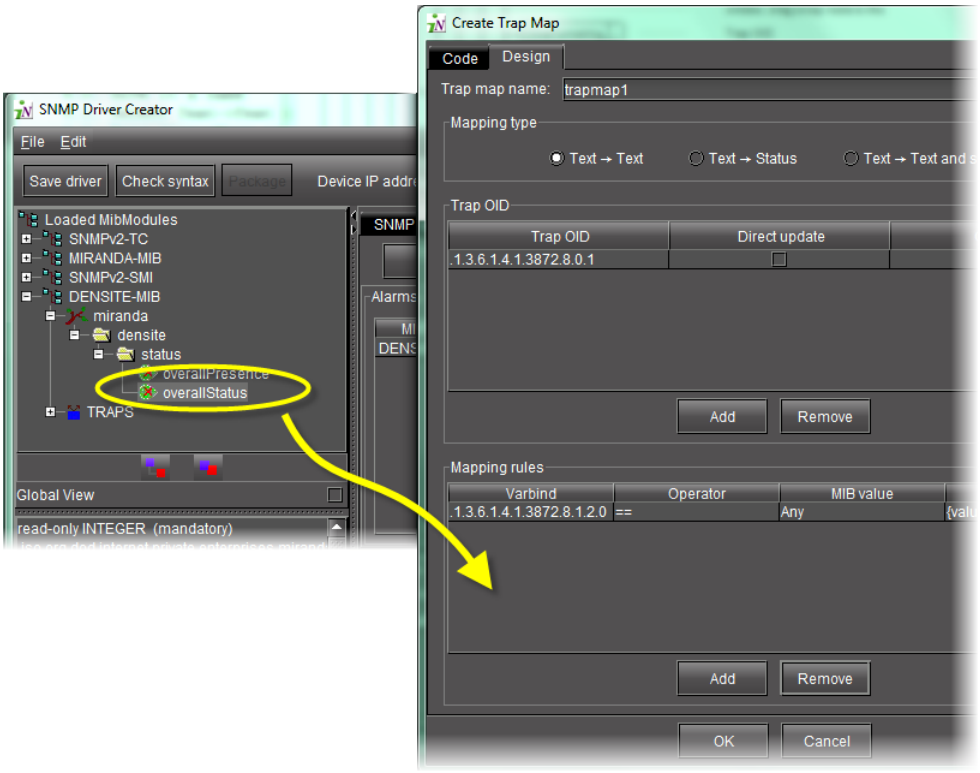


b) In the row corresponding to the new trap OID, click or double-click the cells in each column to enter the required data.

> **Note:** Depending on which cell you click, either select from one of the listed options or type the desired value to configure the parameter.

5. Do one of the following:

   In the MIB pane of **SNMP Driver Creator**, drag a the desired MIB node to the **Mapping rules** area of the **Create Trap Map** window.

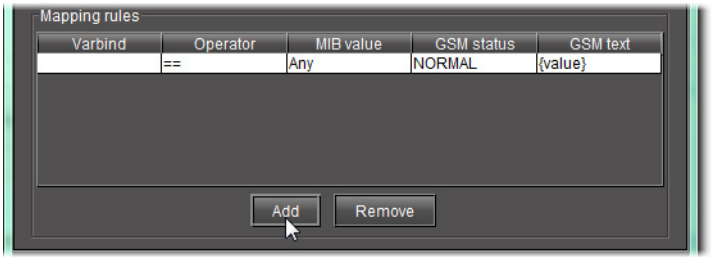


OR,

Perform the following sub-procedure in the **Mapping rules** area of the **Create Trap Map** window.

a) Click **Add**.

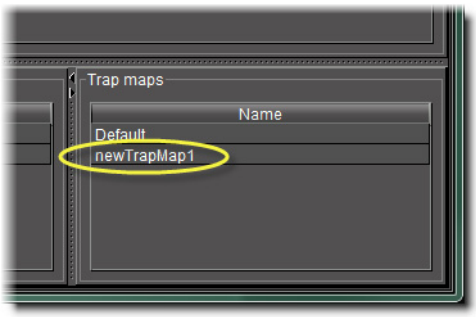
SYSTEM RESPONSE: A highlighted, unconfigured mapping rule row appears.



b) In the row corresponding to the new mapping rule, click or double-click the cells in each column to enter the required data.

6. Click **OK**.

SYSTEM RESPONSE: The new map appears in the **Trap map** area of the **Alarms** tab in **SNMP Driver Creator**.



Note: The **Trap maps** area of the **Alarms** tab only displays the new trap map if the alarm mode is set either to *Polling and trap* or *Traps only*.

See also

For more information about editing an existing alarm map any time after it has been created, see Editing an Alarm Map, Trap Map, or Poller Profile, on page 483.

Creating a Poller

There are several ways in which you can create a poller. The differences lie in the way in which you navigate to the **Create New Poller** window.

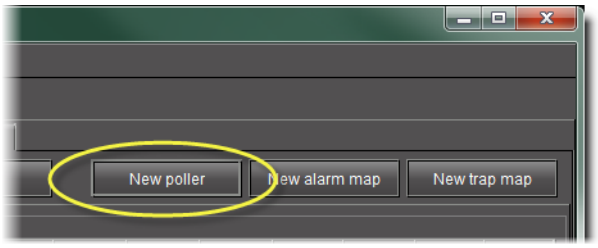
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **SNMP Driver Creator** (see page 713).
- you have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

To create a poller

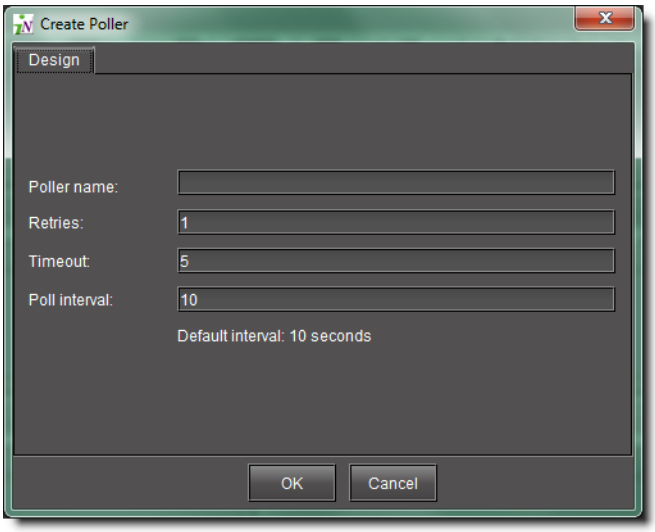
1. Open the **Create Poller** window by doing only **ONE** of the following:
   - In **SNMP Driver Creator**, on the **Alarms** tab, click **New poller**.



   OR,

   - In either the **Add Alarm** window or the **Edit Alarm** window, click **New poller profile**.

   SYSTEM RESPONSE: The **Create Poller** window appears.

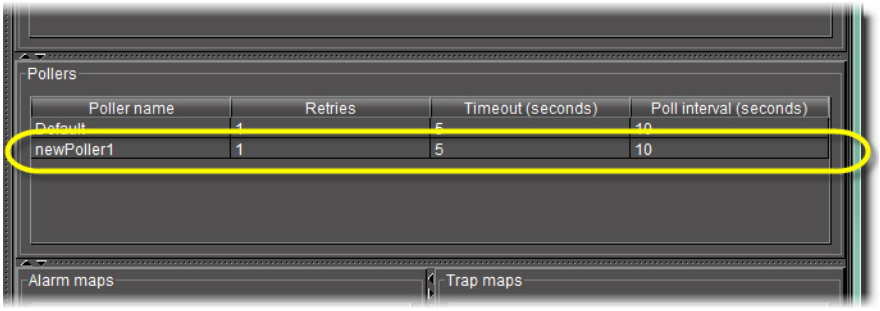


2. On the **Design** tab, type a new poller name.
3. Modify the other parameter fields as required.

Parameter	Default	Description
Poller name		User-defined name for the poller (Alpha-numeric)
Retries	1	Number of times the poller will attempt to poll (Numeric).
Timeout	5	Period of time of inactivity before the poller times out (Number of seconds)
Poll interval	10	Duration of a poll (Number of seconds).

4. Click **OK**.

   SYSTEM RESPONSE: The new poller appears in the **Pollers** area of **SNMP Driver Creator**.



See also

For more information about editing an existing alarm map any time after it has been created, see Editing an Alarm Map, Trap Map, or Poller Profile, on page 483.

Adding an OID Getter and Variable Getter from a MIB Module

Adding an OID Getter

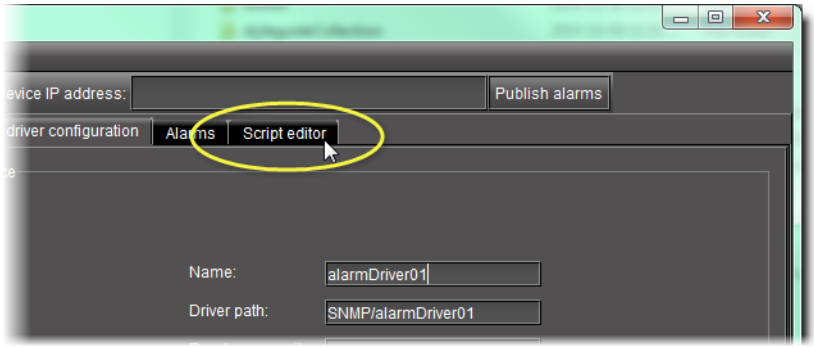
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

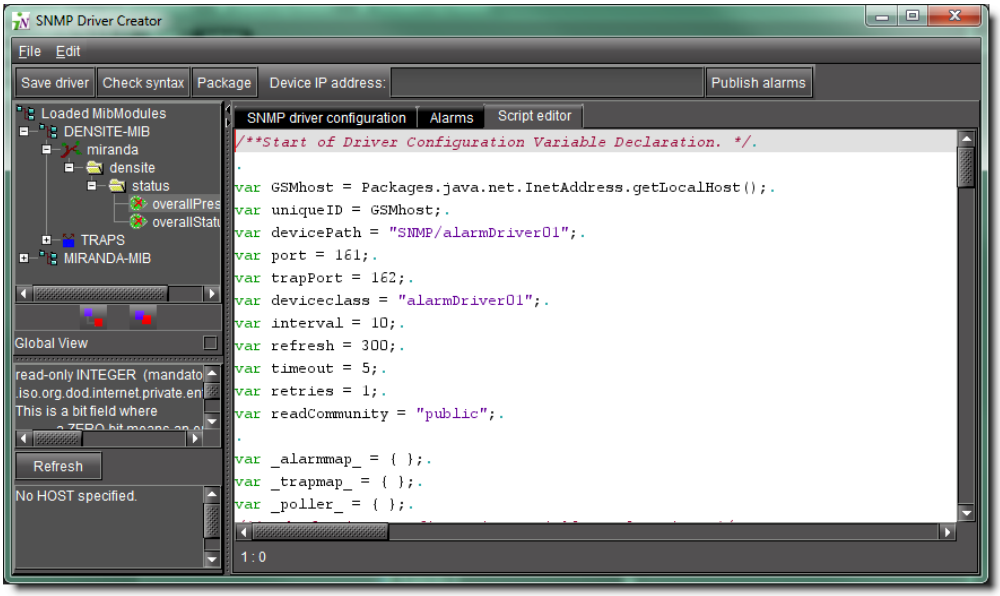
- You have opened **SNMP Driver Creator** (see page 713).
- You have configured a name for your SNMP driver (see page 462).
- You have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

To add an OID getter to the script

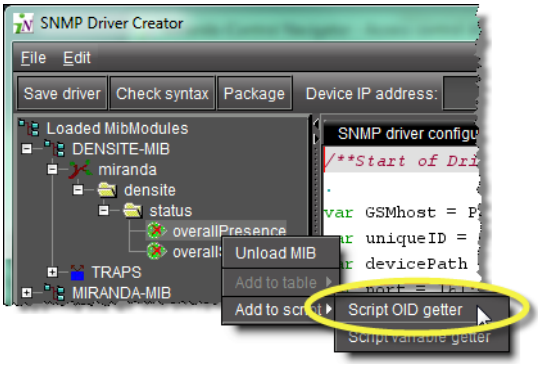
1. In **SNMP Driver Creator**, click the **Script editor** tab.



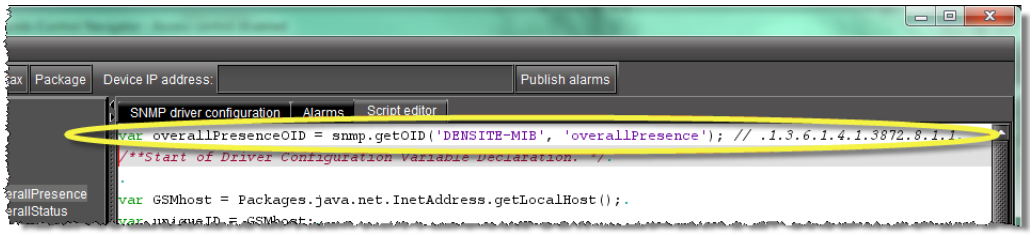
SYSTEM RESPONSE: The Script editor appears in the main pane.



2. In the **MIB Browser** pane (left pane), right-click the MIB node, point to **Add to script**, and then click **Script OID getter**.



SYSTEM RESPONSE: The OID getter is added to the script.



Adding a Variable Getter

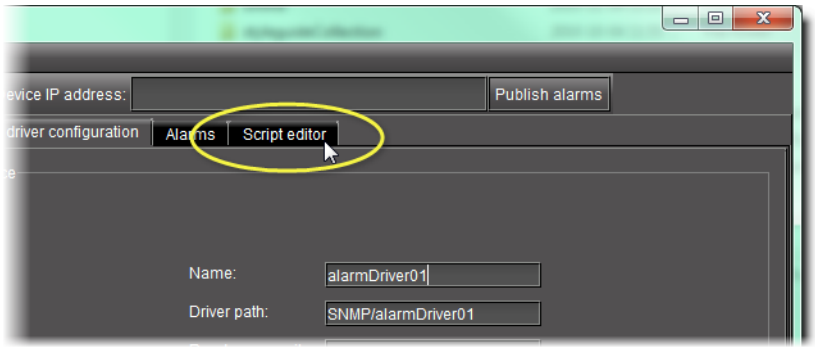
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **SNMP Driver Creator** (see page 713).
- You have configured a name for your SNMP driver (see page 462).
- You have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- **[RECOMMENDED]:** You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

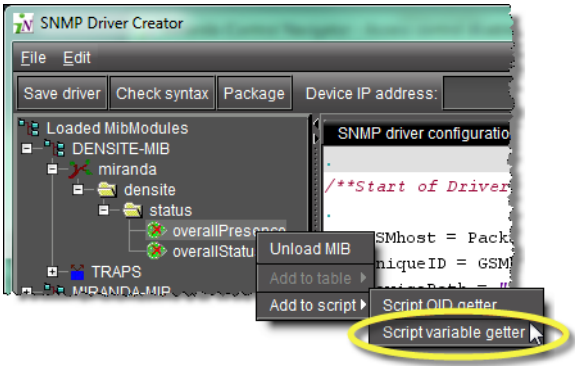
To add a variable getter to the script

1. In **SNMP Driver Creator**, click the **Script editor** tab.

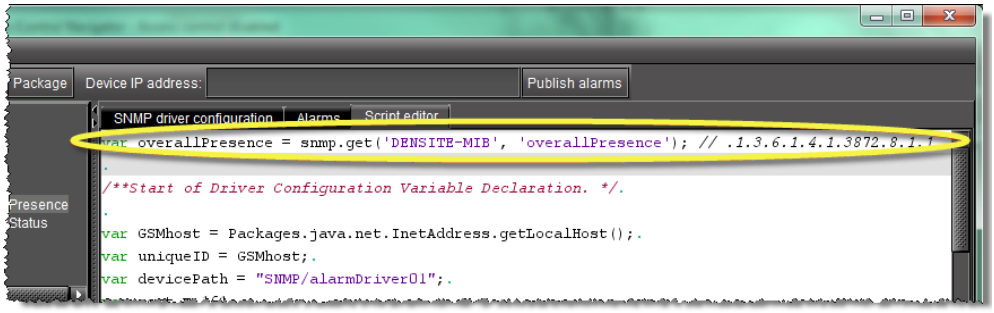


SYSTEM RESPONSE: The Script editor appears in the main pane.

2. In the **MIB** pane (left pane), right-click the MIB node, point to **Add to script**, and then click **Script variable getter**.



SYSTEM RESPONSE: The variable getter is added to the script.



Packaging the JavaScript Source Code as a Plug-In

After you generate and modify your JavaScript source code, you can package the script file as a plug-in.

> **Note:** Uploading a packaged driver will not overwrite factory MIBs on the server.

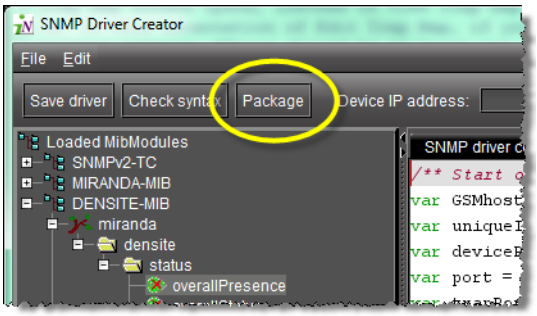
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

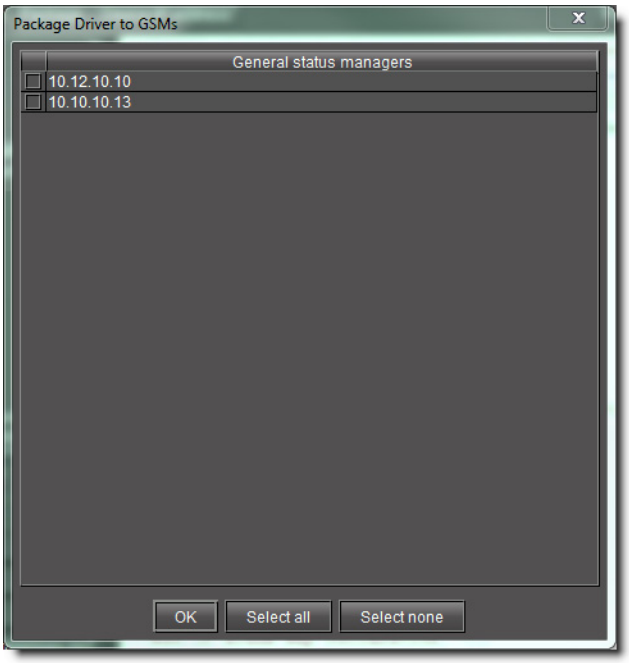
- You have opened **SNMP Driver Creator** (see page 713).
- you have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

To package the JavaScript source code as a plug-in

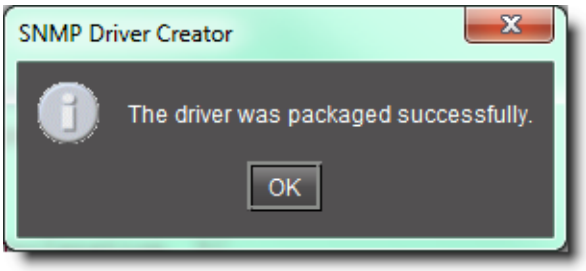
1. In **SNMP Driver Creator**, click **Package**.



SYSTEM RESPONSE: The **Package Driver to GSMs** window appears.



2. Select the check box corresponding to each desired Application Server, and then click **OK**.
SYSTEM RESPONSE: If the operation is a success, a confirmation message appears.



3. Click **OK**.

> **IMPORTANT: Requirement for viewing new driver in GSM alarm browser**
>
> If, when creating and packaging your driver, the GSM alarm browser is currently open, you will not see the new driver in GSM after packaging is complete. At this time, you must close your GSM alarm browser, then reopen it to see the new driver.

Saving a Driver's JavaScript File on a Local Machine

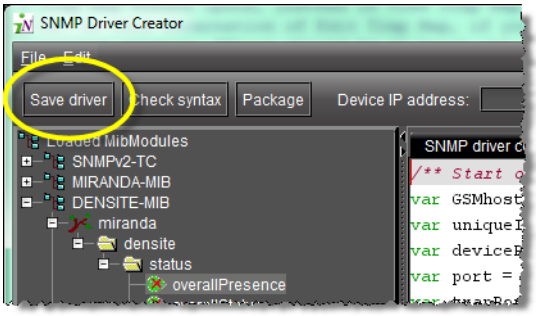
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

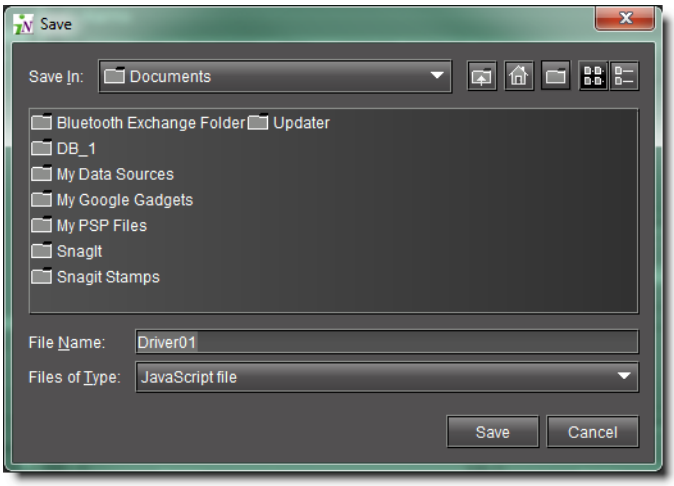
- You have opened **SNMP Driver Creator** (see page 713).
- you have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

To save a driver's JavaScript file to a local file system

1. In **SNMP Driver Creator**, click **Save driver**.



SYSTEM RESPONSE: The **Save** window appears.



2. Navigate to the desired location on your local file system and then click **Save**.

   SYSTEM RESPONSE: The driver's JavaScript file is saved.

Publishing a Driver

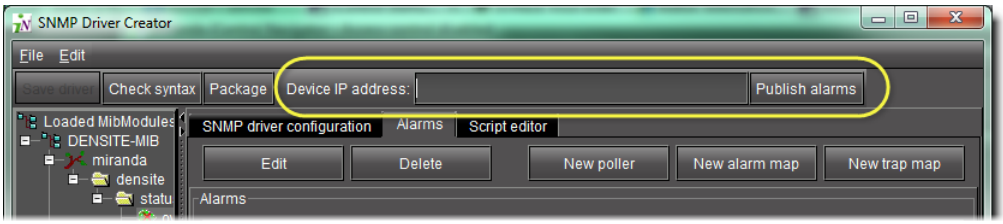
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **SNMP Driver Creator** (see page 713).
- you have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439).

To publish an SNMP driver

- In the **SNMP Driver Creator** window, type the IP address of the device, and then click **Publish alarms**.



SYSTEM RESPONSE: The alarms are published.

Editing Procedures

Editing an Alarm

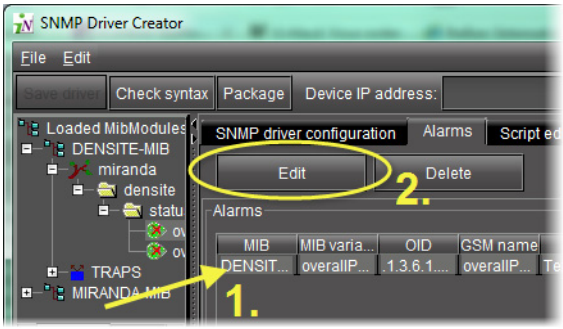
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

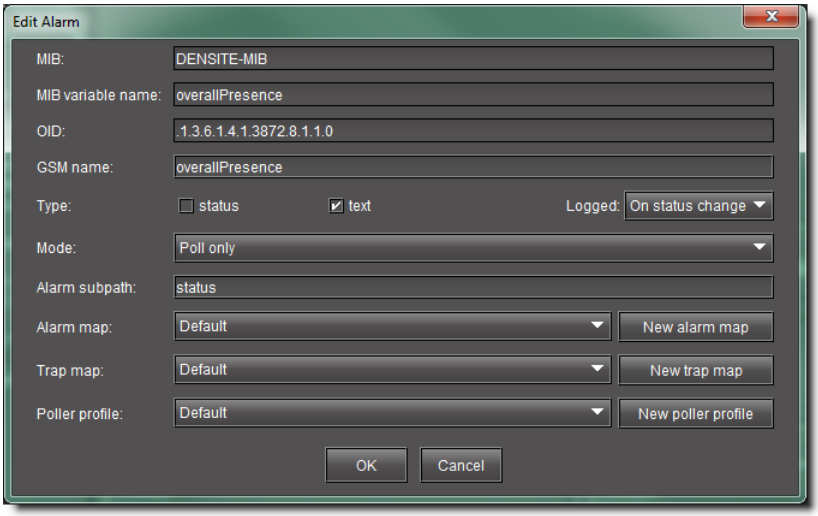
- You have opened **SNMP Driver Creator** (see page 713).
- You have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- You are displaying the **Alarms** tab in **SNMP Driver Creator**.
- You have configured your driver settings (see page 462).

To edit an alarm

1. In **SNMP Driver Creator**, in the **Alarms** list, select the alarm you would like to edit, and then click **Edit**.



SYSTEM RESPONSE: The **Edit Alarm** window appears.



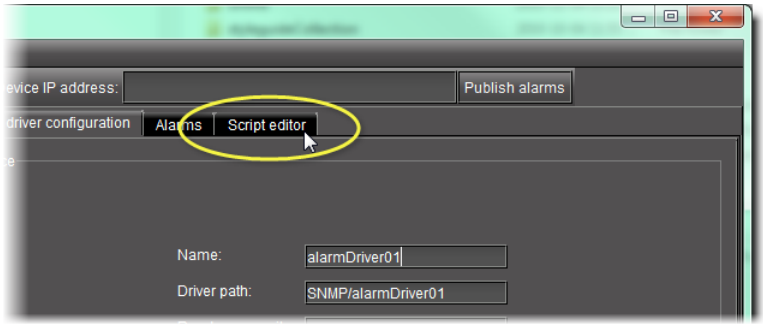
2. Modify the alarm's parameters as required, and then click **OK**.

Note: From the **Edit an Alarm** window, you may also create new alarm maps, trap maps, and pollers.

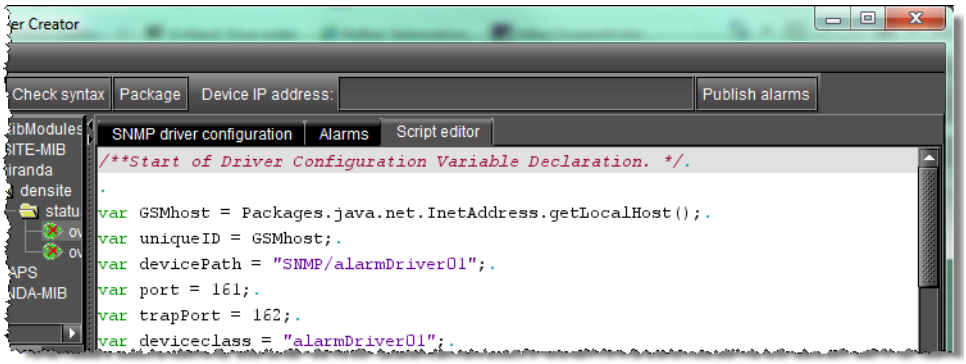
Editing a Driver's Generated Script

To edit a driver's generated script

1. In the **SNMP Driver Creator** window, click the **Script editor** tab.



SYSTEM RESPONSE: The Script editor appears in the main pane.



2. Modify the JavaScript code directly or if you would like to add a script OID getter or script variable getter, perform the procedure see Adding an OID Getter and Variable Getter from a MIB Module, on page 476.
3. Use the *Check Syntax* function to verify your code as required (see page 485).

Editing an Alarm Map, Trap Map, or Poller Profile

You can edit alarm map, trap map, and poller configuration data after an initial configuration is performed. The following procedure details steps for an alarm map. However, the procedures for editing trap maps and pollers are principally the same.

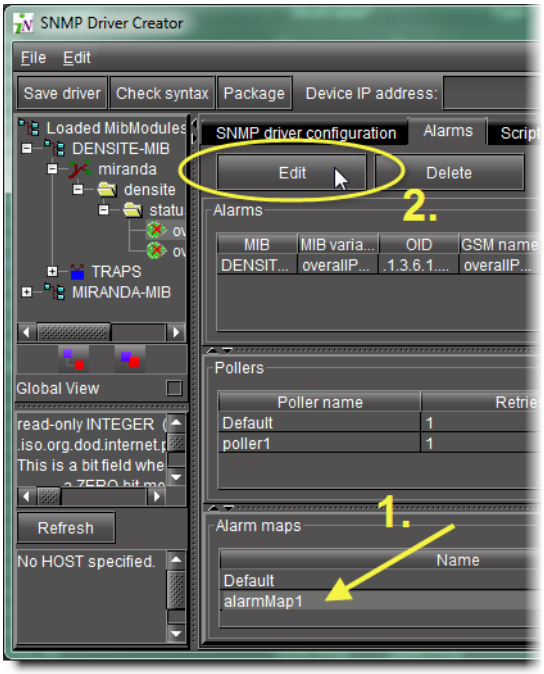
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

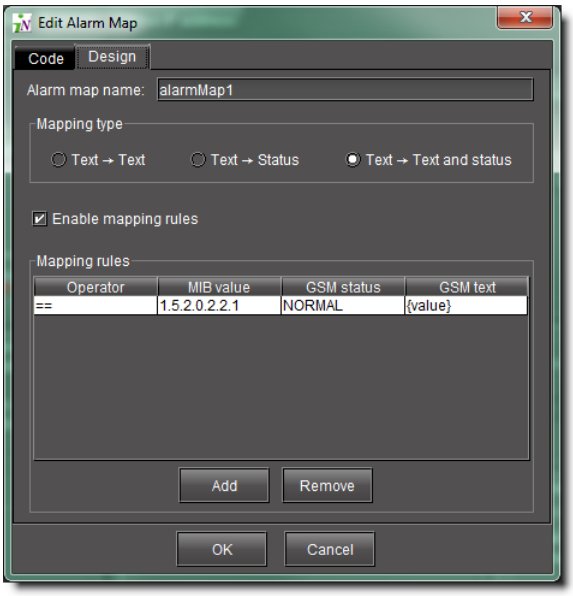
- You have opened **SNMP Driver Creator** (see page 713).
- You have loaded a MIB module into **SNMP Driver Creator** (see page 457).
- You are displaying the **Alarms** tab in **SNMP Driver Creator**.
- You have configured your driver settings (see page 462).
- The alarm map you would like to edit is visible in the **Alarm maps** area on the **Alarms** tab of the **SNMP Driver Creator**.

To edit an alarm map

1. In the **SNMP Driver Creator** window, in the **Alarm maps** area, select the map you would like to edit.
2. Click **Edit**.



SYSTEM RESPONSE: The **Edit Alarm Map** window appears.



3. Modify alarm map parameters as required, including the map name, mapping type, and editing, adding, or deleting mapping rules.

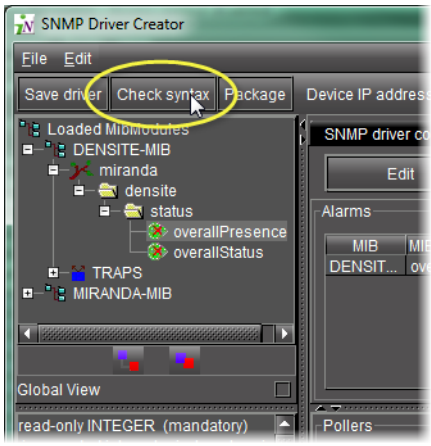
> **See also**
>
> For more information about adding mapping rules, see Creating an Alarm Map, on page 467.

Verifying a Driver's Script Syntax

> **REQUIREMENT**
>
> Before beginning this procedure, make sure you are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439) **[RECOMMENDED]**.

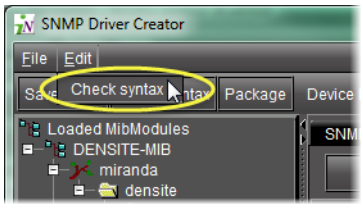
To verify a driver's script syntax

- In the **SNMP Driver Creator** window, do **ONE** of the following:
  - Click **Check syntax**.

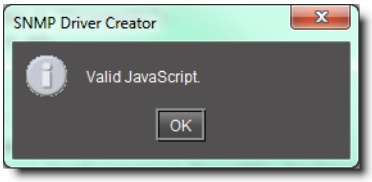


OR,

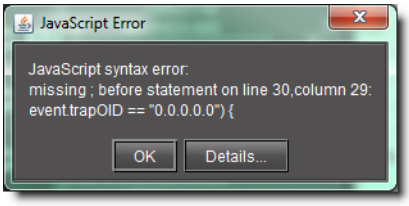
- On the **Edit** menu, click **Check syntax**.



SYSTEM RESPONSE: The system returns either the `Valid JavaScript` message or the `JavaScript error` message.



Valid JavaScript message



JavaScript error message

Notes

- In cases wherein your script contains an error, the JavaScript error message states the location of the error in the script.

Notes (*Continued*)

- If your script contains several errors, the JavaScript error message only states the location of the first-found error (starting from line 1, column 1).

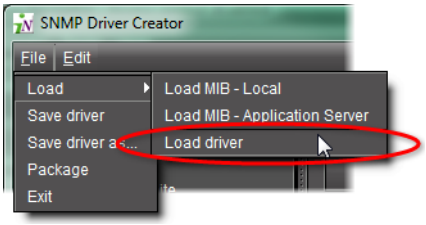
Loading a Driver into SNMP Driver Creator

REQUIREMENT

Before beginning this procedure, make sure you are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Creating an SNMP Driver, on page 439) **[RECOMMENDED]**.

To load a driver

1. In **SNMP Driver Creator**, on the **File** menu, point to **Load**, and then click **Load driver**.



   SYSTEM RESPONSE: The **Open** window appears.

2. Browse for the desired driver file, select it, and then click **Open**.

   SYSTEM RESPONSE: The driver is loaded.

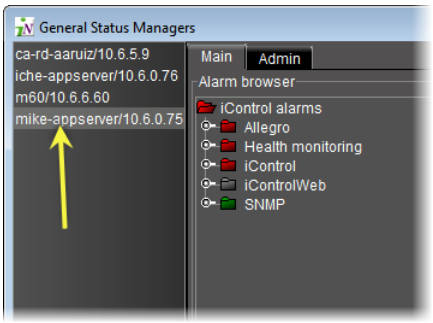
Removing a Custom SNMP Driver from an Application Server

REQUIREMENT

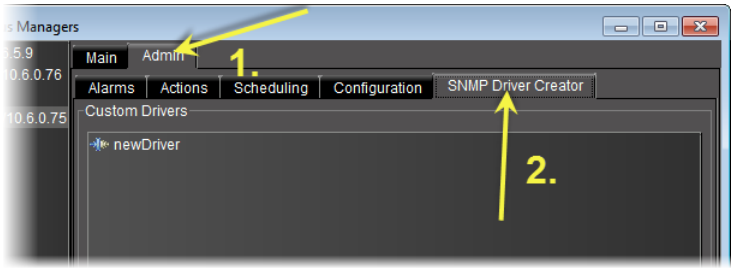
Before beginning this procedure, make sure you have opened the GSM Alarm Browser of the Application Server (see Opening the GSM Alarm Browser, on page 710).

To remove a custom SNMP driver from an Application Server

1. In the GSM Alarm Browser, if there is a left pane with a list of Application Servers, select the Application Server where the driver you would like to remove is located.

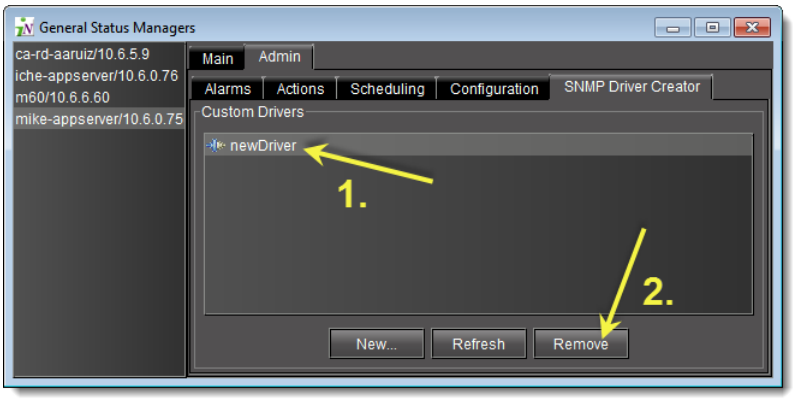


2. In the right pane, click the **Admin** tab, then click the **SNMP Driver Creator** tab.

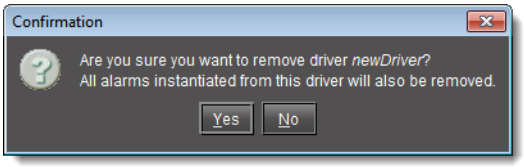


SYSTEM RESPONSE: The SNMP drivers created in **SNMP Driver Creator** are listed.

3. Select the driver you would like to remove from the Application Server, and then click **Remove**.



SYSTEM RESPONSE: A confirmation message appears.



4. Verify this is the driver you would like to remove.

   If this is the driver you would like to remove, click **Yes**.

   If this is ***NOT*** the driver you would like to remove, click **No**.

iControl as SNMP Agent

iControl SNMP agents allow third party SNMP managers, such as Spectrum, to monitor an iControl configuration. There are two types of iControl SNMP agents:

- the GSM SNMP agent
- the AppServer Health Monitoring agent

AppServer Health Monitoring Agent

The AppServer Health Monitoring agent is an iControl plug-in based on *Net-SNMP* — a popular open-source health monitoring package (see `www.net-snmp.org`) consisting of an SNMP daemon (*snmpd*), an SNMP agent, and several utilities. iControl's customized version of Net-SNMP allows a third party SNMP manager to monitor various aspects of an Application Server (e.g., network interface statistics, processor/memory usage, disk space) as well as the condition of essential iControl services (GSM, RMID, Densité Manager, etc.).

Both types of agents are discussed in detail in the following pages.

Configuring the GSM as an SNMP Agent

Any iControl GSM can be made to act as an SNMP agent. The GSM SNMP agent reports the status and alarms of Grass Valley's Densité and Imaging cards and frames (along with every other alarmable entity visible in the GSM Alarm Browser) in the form of an SNMP table (see The GSM Alarm Status Table, on page 504). This table can be queried or polled for alarms and statuses by any third party SNMP Manager.

You can configure the GSM to act as an SNMP agent for all alarms or you can configure the GSM as an SNMP agent for an individual alarm. Additionally, you may have multiple instances of the GSM-as-SNMP-agent when the agents represent different alarms.

Creating a GSM SNMP Agent for all Alarms

WARNING: Depending on the scale of your GSM-visible alarm footprint, performing this procedure may have a detrimental impact upon iControl, a destination SNMP manager, or general network performance. Care should be taken when configuring GSM SNMP agents for all alarms.

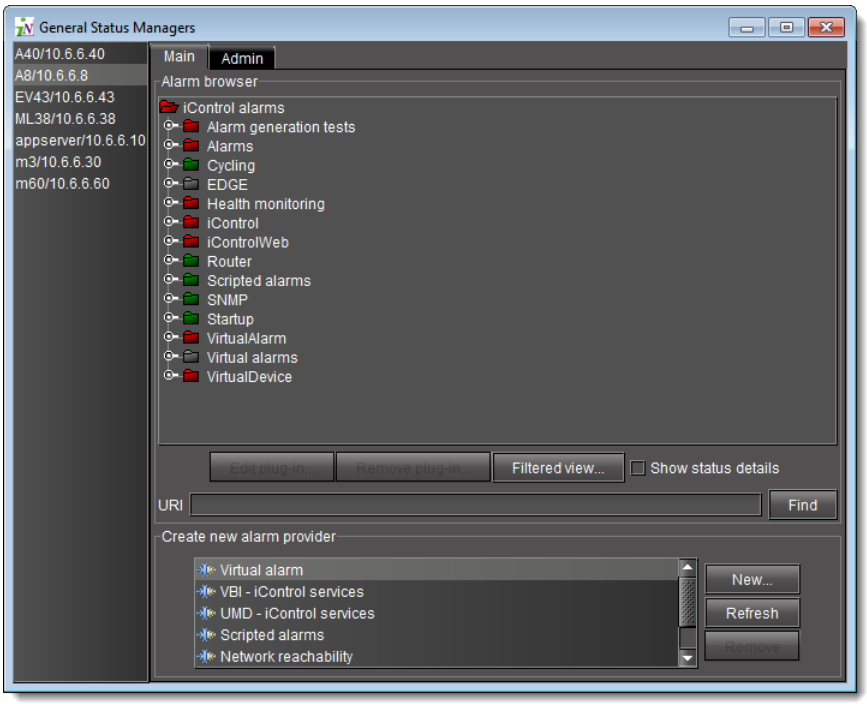
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have separately ordered and installed the *SNMP Agent* plug-in option. To order this, contact Grass Valley Technical Support (see Contact Us, on page 739).
- You have opened the GSM Alarm Browser (see Opening the GSM Alarm Browser, on page 710).

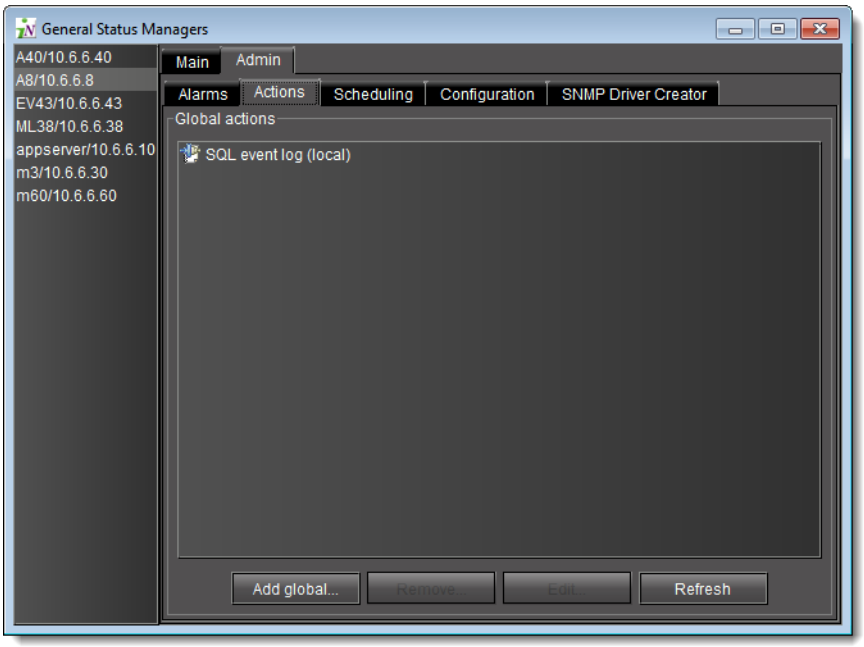
To create a GSM SNMP agent for all alarms

1. In the GSM Alarm Browser, select a GSM from the list on the left pane.



Note: The graphics depicted above and below show the GSM Alarm Browser if it is opened from the **View** menu of **iC Navigator**. If, however, you have opened the GSM Alarm Browser by double-clicking a GSM in **iC Navigator**'s *Logical View*, you will not see a left pane with a list of GSMs.

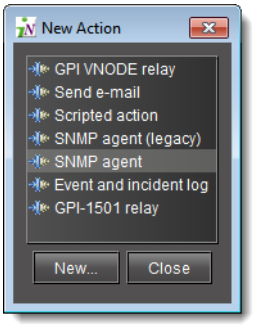
2. On the right pane, click on the **Admin** tab, and then click on the **Actions** sub-tab.



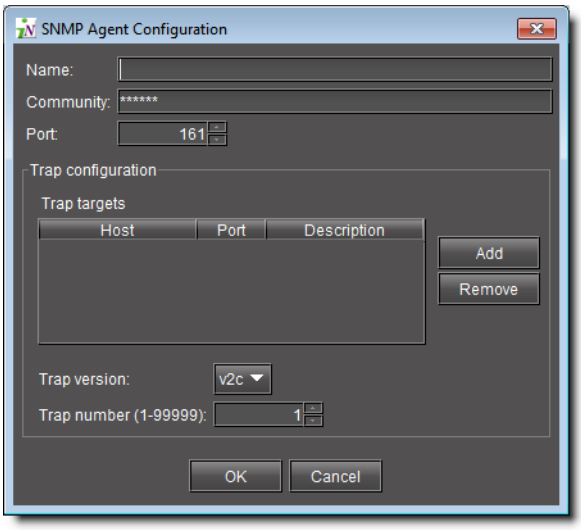
3. Click **Add global**.

   SYSTEM RESPONSE: The **New Action** window appears.

4. Select **SNMP agent** in the list of new actions, and then click **New.**



SYSTEM RESPONSE: The **SNMP Agent Configuration** window appears.

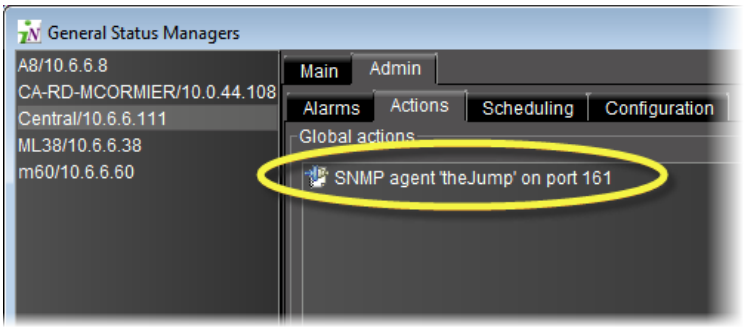


5. Enter values for the following parameters depending upon your needs:

To do this...	...do this...
Configure an SNMP agent.	1. In the **SNMP Agent Configuration** window, type a name for this plug-in. 2. In the **Community** box, type an SNMP community string. Only client requests with identical text are processed. By default, the value is set to `public`. 3. In the **Port** list, select the Application Server port number to which the agent listens for client requests.[1] 4. In the **Trap configuration** area, click **Add**. 5. In the trap target that appears, in the **Host** column, type an IP address for the trap target. 6. In the same row (same trap target), in the **Port** column, type the trap target's port number to which the trap will be sent. 7. **[OPTIONAL]** In the same row, in the **Description** column, type a description of the trap target. 8. Specify the trap version. 9. Assign a trap number (used to identify this trap from others). 10. Click **OK**.
Remove a trap target from an SNMP agent.	1. In the **SNMP Agent Configuration** window, in the **Trap targets** list, select the target you would like to remove. 2. Click **Remove**. 3. Click **OK**.

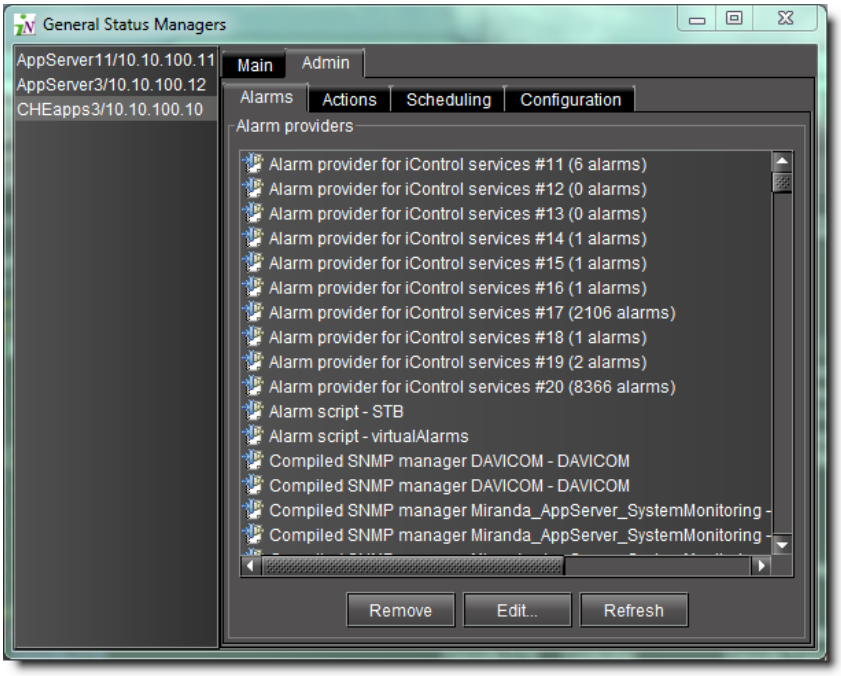
1. Make sure the port is not already being used by another process running on the same Application Server.

System Response: An icon labeled **SNMP Agent** appears in the **Global actions** list.



Note: The **Global actions** list may take several seconds to update. Alternatively, you may click **Refresh** to manually update the list.

All alarms located in the iControl folder of the GSM Alarm Browser of the currently selected GSM are now available to be polled or queried by a third party SNMP Manager.



Note: The SNMP OIDs specific to Grass Valley devices and to the iControl GSM agent and traps are contained in MIB files (`GSM-MIB.mib` and the `MIRANDA-MIB.mib`) available from Grass Valley Technical Support (see Contact Us, on page 739).

Creating a GSM SNMP Agent for an Individual Alarm

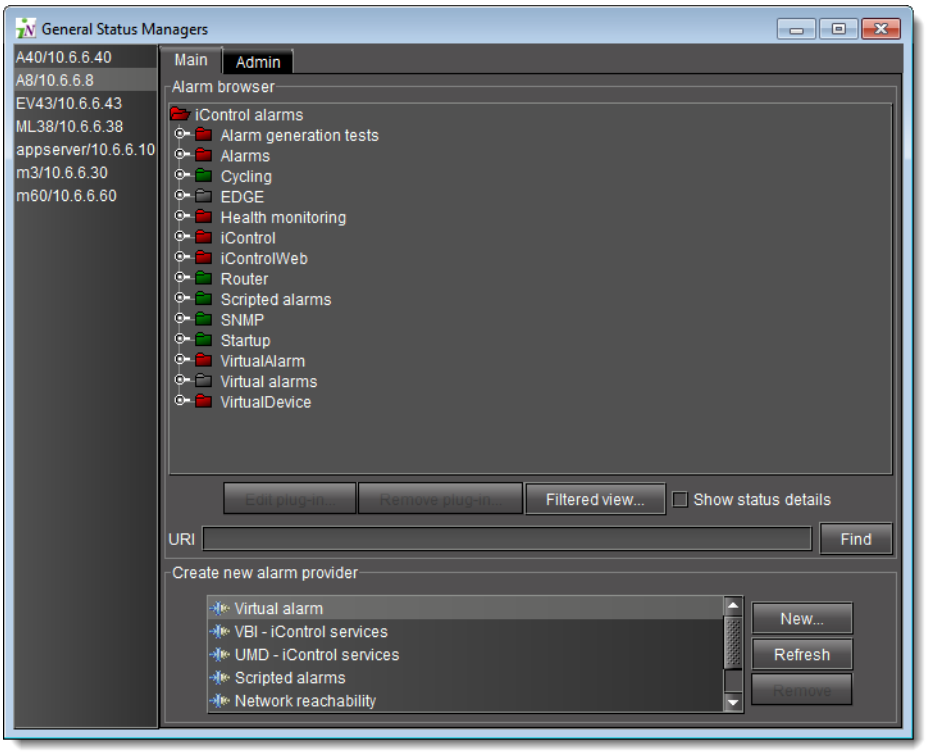
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

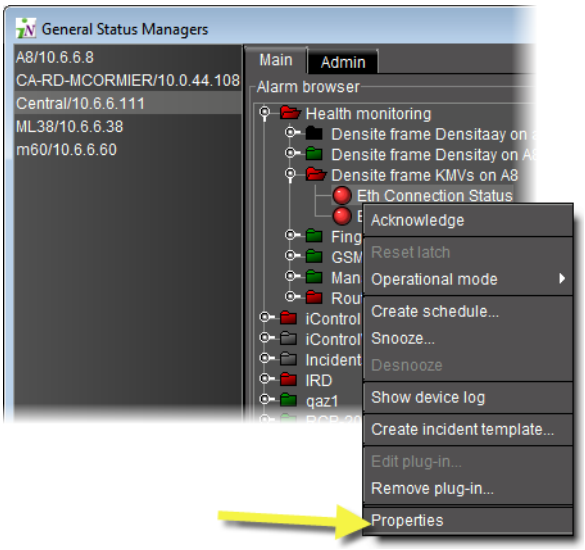
- You have separately ordered and installed the *SNMP Agent* plug-in option. To order this, contact Grass Valley Technical Support (see Contact Us, on page 739).
- You have opened the GSM Alarm Browser (see Opening the GSM Alarm Browser, on page 710).

To create a GSM SNMP agent for an individual alarm

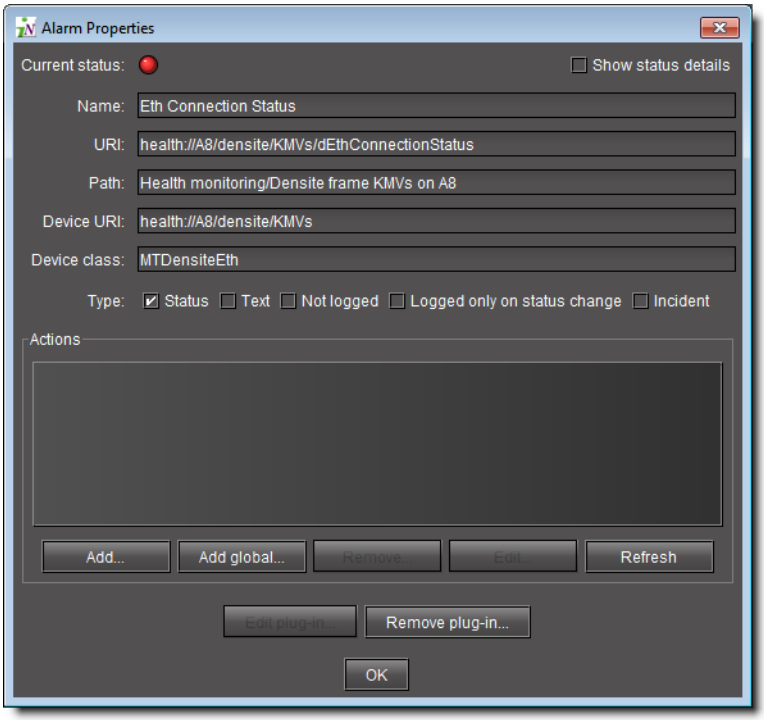
1. In the GSM Alarm Browser, select a GSM from the list on the left pane.



2. In the right pane, on the **Main** tab, navigate to – and right-click – the desired alarm, and then click **Properties**.



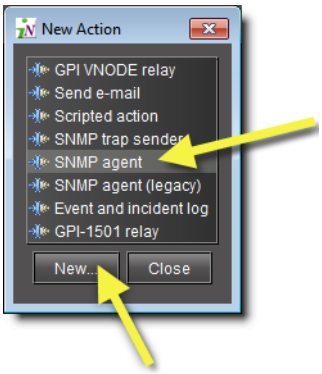
SYSTEM RESPONSE: The **Alarm Properties** window appears.



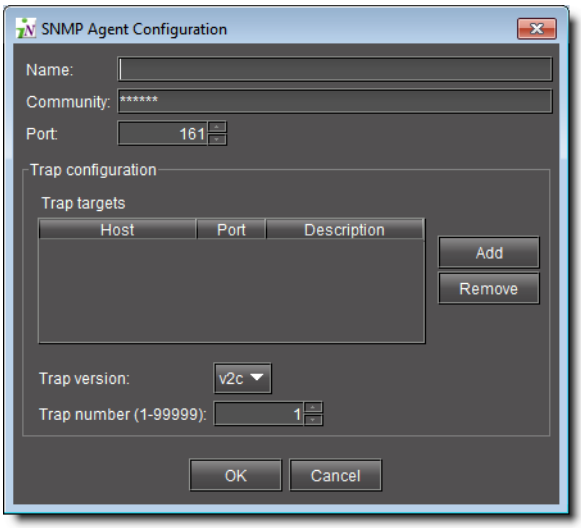
3. Click **Add**.

   SYSTEM RESPONSE: The **New Action** window appears.

4. Select **SNMP agent** and then click **New**.



SYSTEM RESPONSE: The **SNMP Agent Configuration** window appears.

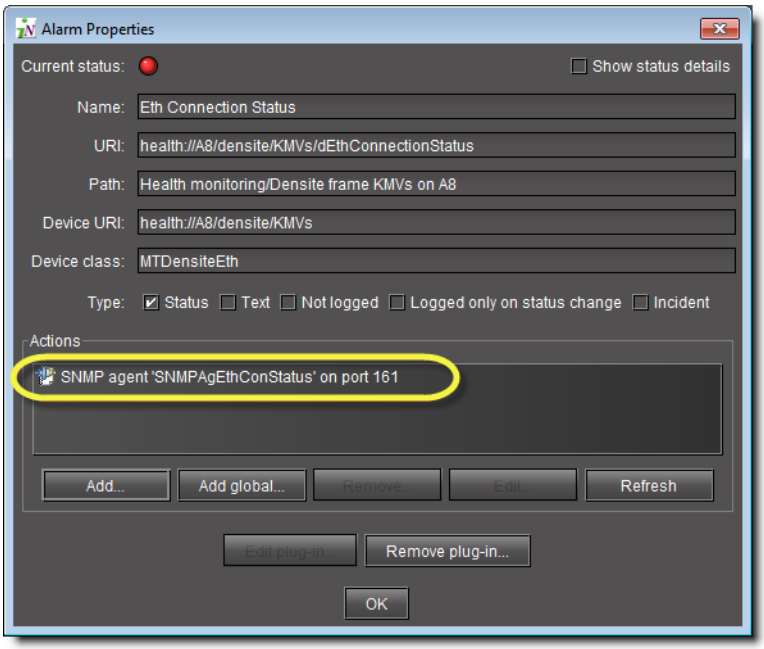


5. Enter values for the following parameters depending upon your needs:

IMPORTANT:	**Make sure each port is used by, at most, one SNMP agent** When configuring multiple SNMP agents for multiple individual alarms, it is important to make sure any given port is not used for more than one SNMP agent.

To do this...	...do this...
Configure an SNMP agent.	1. In the **SNMP Agent Configuration** window, type a name for this plug-in. 2. In the **Community** box, type an SNMP community string. Only client requests with identical text are processed. 3. In the **Port** list, select the Application Server port number to which the agent listens for client requests. 4. In the **Trap configuration** area, click **Add**. 5. In the trap target that appears, in the **Host** column, type an IP address for the trap target. 6. In the same row (same trap target), in the **Port** column, type the trap target's port number to which the trap will be sent. 7. **[OPTIONAL]** In the same row, in the **Description** column, type a description of the trap target. 8. Specify the trap version. 9. Assign a trap number (used to identify this trap from others). 10. Click **OK**.
Remove a trap target from an SNMP agent.	1. In the **SNMP Agent Configuration** window, in the **Trap targets** list, select the target you would like to remove. 2. Click **Remove**. 3. Click **OK**.

SYSTEM RESPONSE: An icon labeled **SNMP Agent** appears in the **Actions** list of the **Alarm Properties** window.



This alarm is now available to be polled or queried by a third party SNMP Manager.

Viewing the GSM SNMP Agent Alarms

Alarms located in the iControl folder of the GSM Alarm Browser are available for polling via the GSM SNMP Agent. This folder contains the alarms associated with Densité and Imaging devices—for the frames themselves and for the cards they contain.

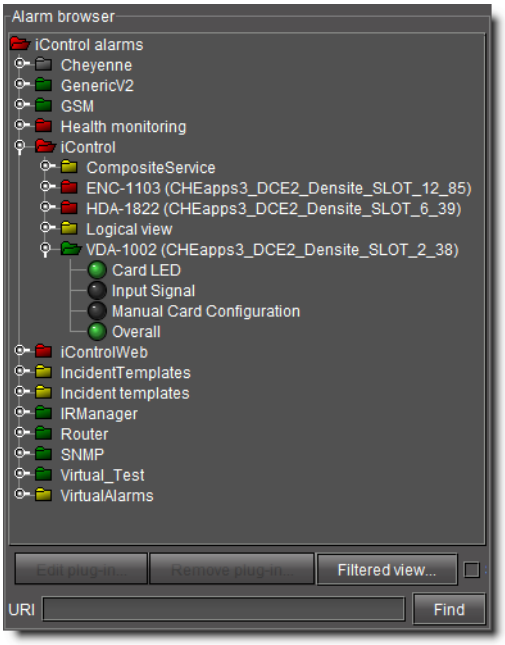
REQUIREMENT

Before beginning this procedure, make sure you have opened the GSM Alarm Browser (see Opening the GSM Alarm Browser, on page 710).

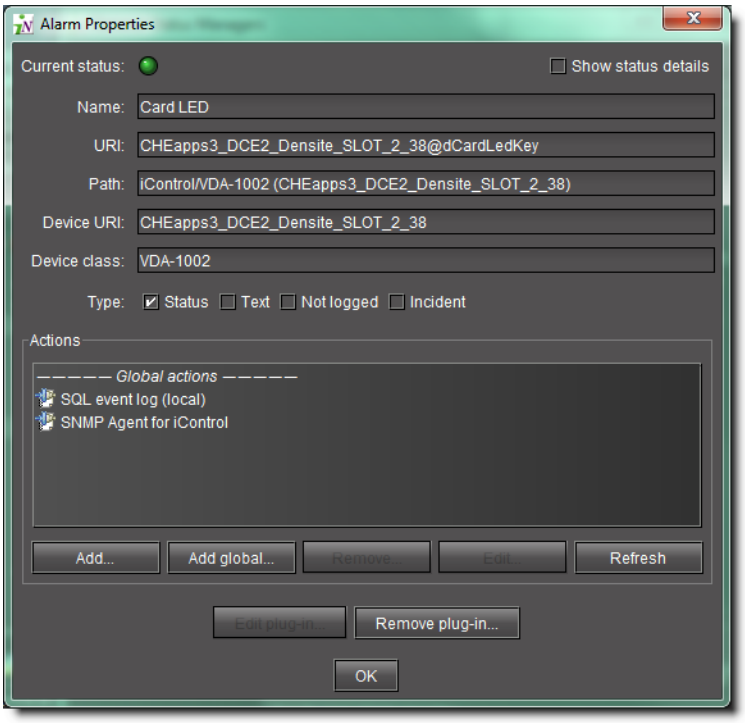
To view a list of the alarms available for polling via the GSM SNMP agent

1. In the GSM Alarm Browser, double-click the **iControl** folder in the **iControl alarms** folder to display its contents.

> **Note:** You can double-click on subfolders to reveal their contents, and so on. Ultimately, you will reveal all of the alarms available for polling via the GSM's SNMP agent. Each card has its own folder which contains all the alarms and statuses provided by this card (some cards have multiple folders).



2. Double-click an alarm to view its details.



Configuring iControl to Send Traps

Once an iControl GSM has been configured to act as an SNMP agent, all alarms in its database can be polled by a third-party SNMP Manager. You can give special attention to individual alarms (or combinations of alarms) by assigning SNMP traps. When these alarms change state, they will send a trap, via the GSM, to the third-party SNMP Manager.

Assigning an SNMP Trap to One or More Alarms

REQUIREMENT

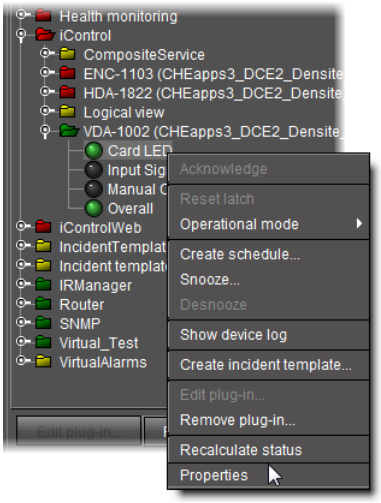
Before beginning this procedure, make sure you have opened the GSM Alarm Browser (see Opening the GSM Alarm Browser, on page 710).

To assign an SNMP trap to one or more alarms

1. In the GSM Alarm Browser, select the alarm(s) to which you would like to assign SNMP traps.

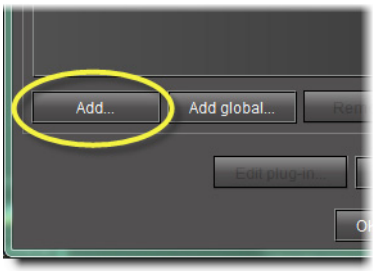
   Note: You can assign the same trap to more than one alarm by making a multiple selection (Shift+click or Ctrl+click).

2. Right-click an alarm, and then click **Properties**.

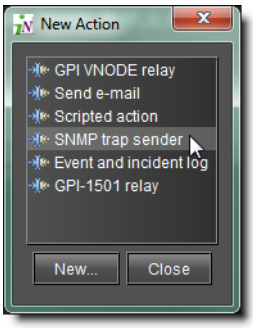


SYSTEM RESPONSE: The **Alarm Properties** window appears.

3. Click **Add**.



4. In the **New action** window, click **SNMP trap sender**, and then click **New**.

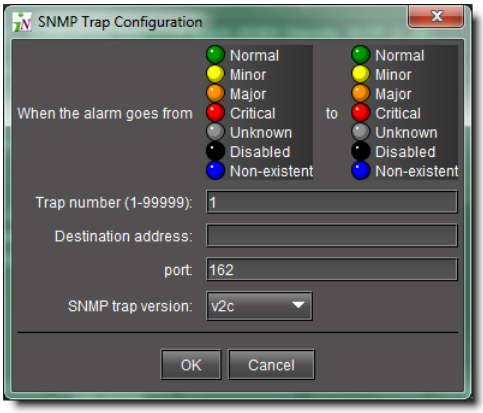


5. In the **SNMP trap configuration** window, specify an alarm transition that will trigger the SNMP trap; select one or more alarm states in the left column (*from*), and then one or more in the right column (*to*). For example, if you select from **Minor**, **Major** or **Critical** to **Normal**, an SNMP trap will be sent whenever a yellow, orange or red alarm is cleared.

   Next, specify a trap number (between 1 and 99999) that describes the trap event. Some numbers are pre-defined in your Grass Valley MIB files. You can also define your own trap numbers.

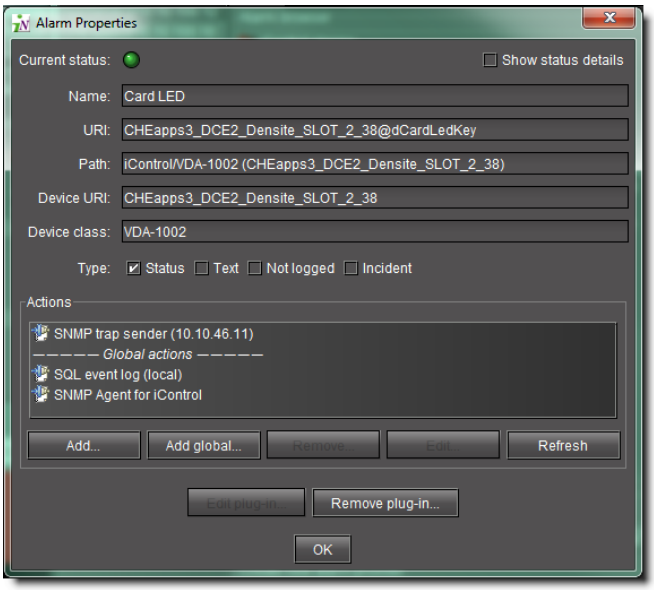
Note: Values 1 to 99999 are reserved for user-defined virtual alarms and for third party SNMP devices. Values of 100000 and up are iControl alarms.

6. In the **Destination address** field, type the IP address of the SNMP Manager that is to receive the trap. Choose **v1** from the **SNMP trap version** menu, and then click **OK**.



SYSTEM RESPONSE: In the **Alarm properties** window, an entry labelled **SNMP trap sender** appears (with an associated SNMP Manager address) in the **Actions** list.

7. Click **OK**.



Note: The SNMP OIDs specific to Grass Valley devices and to the iControl GSM agent and traps are contained in MIB files (`GSM-MIB.mib` and the `MIRANDA-MIB.mib`) available from Grass Valley Technical Support (see Contact Us, on page 739).

Configuring iControl to Generate SNMP Traps for All Alarms

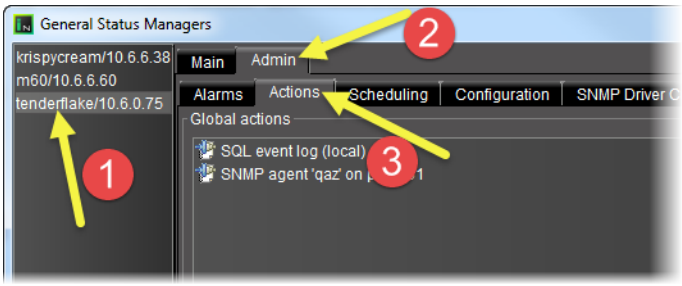
WARNING: Depending on the scale of your GSM-visible alarm footprint, performing this procedure may have a detrimental impact upon iControl, a destination SNMP manager, or general network performance. Care should be taken when configuring GSM SNMP agents for all alarms.

REQUIREMENT

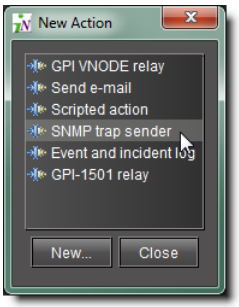
Before beginning this procedure, make sure you have opened the GSM Alarm Browser (see Opening the GSM Alarm Browser, on page 710).

To configure iControl to generate SNMP traps for all/any alarms

1. In the GSM Alarm Browser, click the **Admin** tab, and then click the **Actions** tab.



2. Click **Add global**.
3. In the **New action** window, select **SNMP Trap Sender**, and then click **New**.



4. Select **SNMP Trap Sender**, and then click **New**.

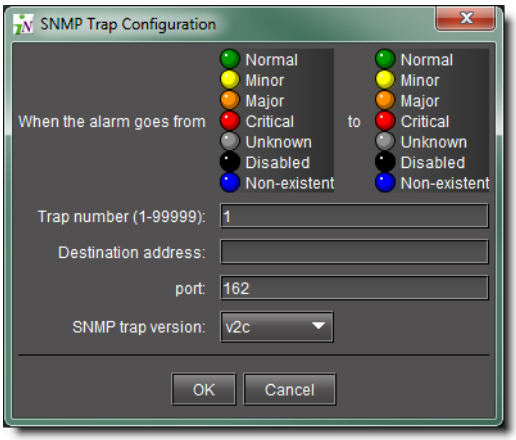
   System Response: The **SNMP trap configuration** window appears.

5. In the **SNMP trap configuration** window, specify an alarm transition that will trigger the SNMP trap; select one or more alarm states in the left column (from), and then one or more in the right column (to). For example, if you select from **Normal** to **Critical**, an SNMP trap will be sent whenever a green alarm turns to red.

   Next, specify a trap number (between 1 and 99999) that describes the trap event. Some numbers are pre-defined in your Grass Valley MIB files. You can also define your own trap numbers.

Note: Values 1 to 99999 are reserved for user-defined virtual alarms and for third party SNMP devices. Values of 100000 and up are iControl alarms.

In the **Destination address** field, type the IP address of the SNMP Manager that is to receive the trap. Choose **v1** from the **SNMP trap version** menu, and then click **OK**.



6. In the **Admin** tab of the **General status managers** window, an entry labelled **SNMP trap sender** appears (with an associated SNMP Manager address) in the **Global actions** list.
7. Close the window.

Note: The SNMP OIDs specific to Grass Valley devices and to the iControl GSM agent and traps are contained in MIB files (`GSM-MIB.mib` and the `MIRANDA-MIB.mib`) available from Grass Valley Technical Support (see Contact Us, on page 739).

Exploring the GSM SNMP Agent

In order to be able to establish useful communications between the GSM SNMP agent and a third party SNMP manager, it is important to understand some of the agent's implementation details, such as its MIB structures and syntax.

iControl MIBs

OIDs specific to Grass Valley and to the iControl GSM SNMP agent and traps can be resolved to a textual convention using two Management Information Base (MIB) files available from Grass Valley: `GSM-MIB.mib` and `MIRANDA-MIB.mib`.

The root file is `MIRANDA-MIB.mib`, which contains:

- the root level definition for `GSM-MIB.mib`
- an enumeration of all the different types of alarms that can be reported by an iControl GSM SNMP agent. This enumeration covers most of the alarms reported by all Grass Valley Densité and Imaging series cards. The textual convention for this enumeration is GsmTraps. Some examples of alarm types are: *black detect*, *freeze detect*, and *audio silence*.
- an enumeration of the different states of an alarm (e.g., *error, warning, ok*).

The GSM-MIB.mib file describes the GSM alarm table and the traps variable bindings. GSM trap numbers are configurable by the user, which results in the creation of a custom MIB based on the configuration of the GSM SNMP trap actions.

The GSM Alarm Status Table

The GSM SNMP agent makes a special MIB object available for polling by third party managers. This object is the GSM alarm status table. It contains statuses for all the Densité and Imaging card alarms contained in the GSM, and is defined in the GSM-MIB file.

SNMP Table - .iso.org.dod.internet.private.enterprises.miranda.gsm.statusTable

deviceIndex	slotIndex	trapIndex	type	name	status
12	9	vCCPresAlarm(100074)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Close Caption	disabled(-1)
12	9	vFreezeDet_ST(100075)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Freeze Detection	normal(10000)
12	9	vChromaMax_ST(100076)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Chroma Max	normal(10000)
12	9	vAplMax_ST(100077)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	APL Max Expected	normal(10000)
12	9	vAplMin_ST(100078)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	APL Min Expected	normal(10000)
12	9	vLumaMax_ST(100079)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Luma Max Expected	normal(10000)
12	9	vLumaMin_ST(100080)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Luma Min Expected	normal(10000)
12	9	vWhiteLimitMax_ST(100081)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	White Max	error(30000)
12	9	vBlackLimitMin_ST(100082)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Black Min	normal(10000)
12	9	vEDH_Det_ST(100083)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	EDH ANC EDH	disabled(-1)
12	9	vAP_Det_ST(100084)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	EDH Active Picture	normal(10000)
12	9	vFF_Det_ST(100085)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	EDH Full Field	disabled(-1)
12	9	vTRS_ST(100086)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	[illegible] Detection	disabled(-1)
12	9	vSigPres_ST(100087)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Carrier Detect	normal(10000)
12	9	vBlackDet_ST(100088)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Black Detection	normal(10000)
12	9	aChan1_sil_ST(100096)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Silence	error(30000)
12	9	aChan2_sil_ST(100097)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Silence	normal(10000)
12	9	aChan1_mxLvl_ST(100098)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Max Level	disabled(-1)
12	9	aChan2_mxLvl_ST(100099)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Max Level	disabled(-1)
12	9	aChan1_mnLvl_ST(100100)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Min Level	normal(10000)
12	9	aChan2_mnLvl_ST(100101)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Min Level	normal(10000)
12	9	aChan1_ovld_ST(100102)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Overload	normal(10000)
12	9	aChan2_ovld_ST(100103)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Overload	normal(10000)
12	9	aPhase_ST(100104)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Phase	normal(10000)
12	9	aStWidth_ST(100105)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Stereo Width	disabled(-1)
12	9	aChan1_mnDyna_ST(100106)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Min Dynamics	disabled(-1)
12	9	aChan2_mnDyna_ST(100107)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Min Dynamics	disabled(-1)
12	9	aChan1_slicing_ST(100108)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Slicing	normal(10000)
12	9	aChan2_slicing_ST(100109)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Slicing	normal(10000)
12	9	overall_status(100121)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Overall	error(30000)
12	9	avStatusIn(100122)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Immediate Signal A...	normal(10000)

Alarm status table generated by a GSM SNMP agent

The alarm status table (*statusTable*) is composed of alarm entries (*statusEntry*) which are categorized by device index (*deviceIndex*), slot index (*slotIndex*) and status type index (*trapIndex*)

- The device index is a unique number attributed to each Imaging or Densité frame the first time it is discovered by the GSM.
- The slot index corresponds to the physical slot containing a card.
- The trap index maps to a type of alarm such as freeze detect or black detect.

The different alarm types available for all Grass Valley Imaging and Densité Cards are enumerated in the MIRANDA-MIB file.

The table also contains the type, the name and the status of each alarm.

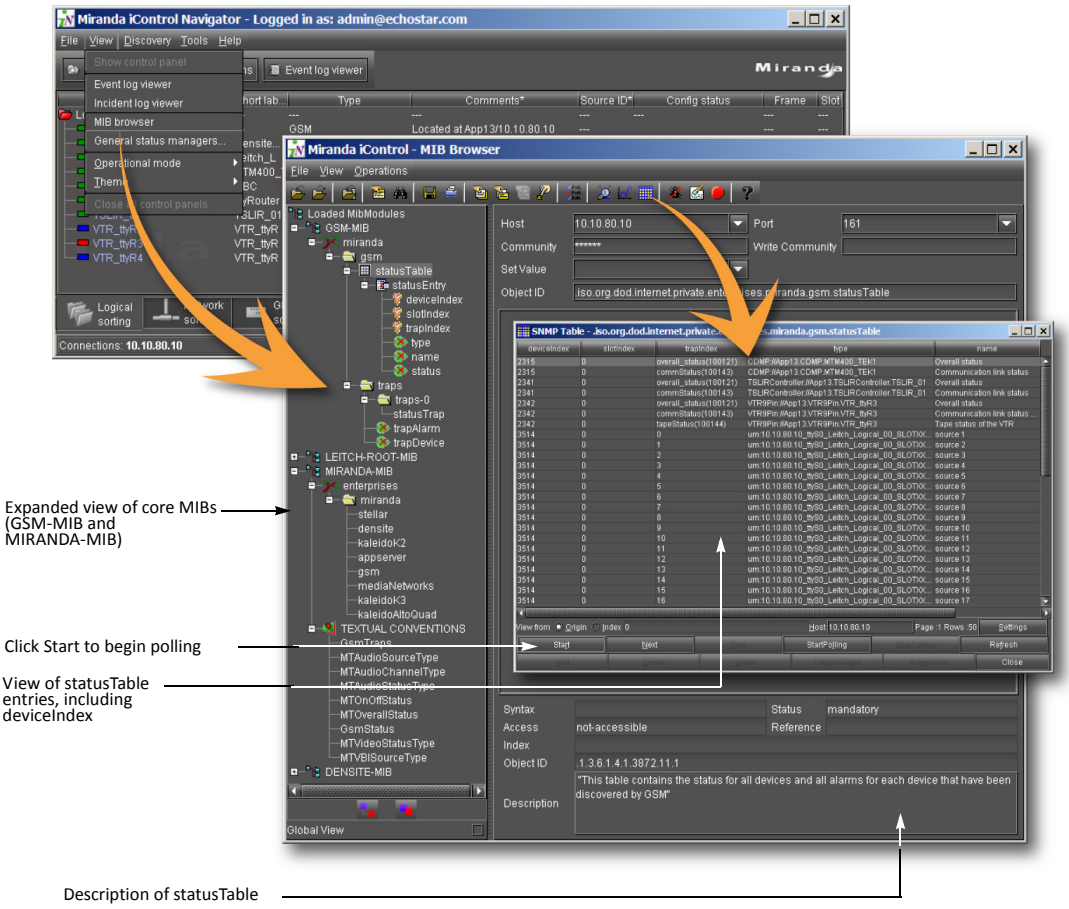
- The **type** field corresponds to the long ID of a card. This is a unique identifier made up of a device identifier (Application Server host name, Densité frame name, or COM port number for Imaging frames) plus the slot number and the card model number.
- The **name** field contains a human readable label for the alarm name.
- The **status** field contains the status of the alarm.

Device Index

The iControl GSM uses auto-discovery to find the Grass Valley Densité and Imaging frames present in the system. These devices may originate from the Application Server where the GSM is running, or from other Application Servers that the GSM has discovered.

The GSM SNMP agent arbitrarily allocates a unique device index to each device the first time it is discovered. The device index starts at 1, and increments by one for each newly-discovered device.

There is no way to know ahead of time the device index for a given Densité or Imaging frame. The only way to determine the device index for a specific frame is to browse the GSM SNMP alarm table using an SNMP MIB browser loaded with the MIRANDA-MIB and the GSM-MIB definitions. You can do this by using **iC Navigator**'s integrated MIB Browser.



*Viewing device index values using **iC Navigator**'s integrated MIB Browser*

Devices are distinguished based on the host name of the Application Server and either the Densité frame name, or the Imaging frame ID and com port. If these settings are not changed, the device index will not change, even if the system is rebooted or restarted.

The index will change if one of the following occurs:

- a Densité frame name changes

- an Application Server host name (or IP address, if there is no DNS) changes
- the RS422 ID of an Imaging frame changes
- an Imaging frame's serial (com) port connection to the Application Server changes

GSM-MIB

The following is a useful excerpt from the GSM-MIB file:

```
statusTable OBJECT-TYPE
      SYNTAX  SEQUENCE OF StatusEntry
      ACCESS  not-accessible
      STATUS  mandatory
      DESCRIPTION "This table contains the status for all devices and all alarms for
      each device that have been discovered by GSM"
       ::= { gsm 1 }
statusEntry OBJECT-TYPE
      SYNTAX StatusEntry
      ACCESS  not-accessible
      STATUS  mandatory
      DESCRIPTION "status entry is indexed by deviceIndex (arbitrary device index
      assigned when device is first discovered, permanent across reboots), slotIndex
      (for frames with multiple slots), and trapIndex (an alarm type as defined in
      the GsmTraps of the MIRANDA-MIB)."
      INDEX { deviceIndex, slotIndex, trapIndex }
      ::= { statusTable 1 }
StatusEntry ::= SEQUENCE {
      deviceIndex  INTEGER,
      slotIndex INTEGER,
      trapIndex GsmTraps,
      type   OCTET STRING,
      name   OCTET STRING,
      status GsmStatus
}
-- ************************************************
-- Each element of the status entry sequence has to be
-- specified individually.
-- ************************************************
deviceIndex OBJECT-TYPE
      SYNTAX  INTEGER
      ACCESS  read-only
      STATUS  mandatory
      DESCRIPTION "This is a unique device index in the table"
       ::= { statusEntry 1 }
slotIndex OBJECT-TYPE
      SYNTAX  INTEGER
      ACCESS  read-only
      STATUS  mandatory
      DESCRIPTION "This is a unique index defining the slot number.
       If the device has no slots, then ZERO is used"
```

```
       ::= { statusEntry 2 }
trapIndex OBJECT-TYPE
      SYNTAX  GsmTraps
      ACCESS  read-only
      STATUS  mandatory
      DESCRIPTION "This is a unique trap (alarm) index in the table"
      ::= { statusEntry 3 }
type OBJECT-TYPE
      SYNTAX  OCTET STRING
      ACCESS  read-only
      STATUS  mandatory
      DESCRIPTION "Device Type"
      ::= { statusEntry 4 }
name OBJECT-TYPE
      SYNTAX  OCTET STRING
      ACCESS  read-only
      STATUS  mandatory
      DESCRIPTION "Current Alarm Logical Name"
       ::= { statusEntry 5 }
status OBJECT-TYPE
      SYNTAX  GsmStatus
      ACCESS  read-only
      STATUS  mandatory
      DESCRIPTION "Current Alarm Status"
       ::= { statusEntry 6 }
```

Determining the OID for polling a specific status

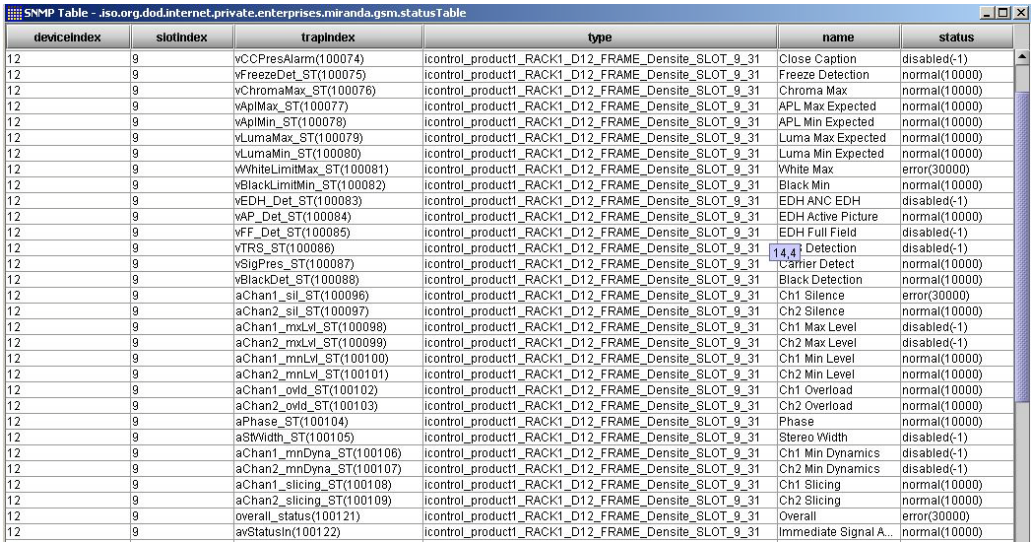
To obtain the current state for a specific status, a SNMP-GET can be performed using the following OID:

`.iso.org.dod.internet.private.enterprises.miranda.gsm.statusTable.statusEntry.status.deviceIndex.slotIndex.trapIndex`

This will return the variable binding of the status for the alarm type defined by the *trapIndex* number, for the card in the slot number matching the *slotIndex* of the frame identified by the *deviceIndex* number.

Example

Here's an example of the status table MIB object for a Grass Valley Densité SCP-1121 SDI probe card.



SNMP Table - .iso.org.dod.internet.private.enterprises.miranda.gsm.statusTable

deviceIndex	slotIndex	trapIndex	type	name	status
12	9	vCCPresAlarm(100074)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Close Caption	disabled(-1)
12	9	vFreezeDet_ST(100075)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Freeze Detection	normal(10000)
12	9	vChromaMax_ST(100076)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Chroma Max	normal(10000)
12	9	vAplMax_ST(100077)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	APL Max Expected	normal(10000)
12	9	vAplMin_ST(100078)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	APL Min Expected	normal(10000)
12	9	vLumaMax_ST(100079)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Luma Max Expected	normal(10000)
12	9	vLumaMin_ST(100080)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Luma Min Expected	normal(10000)
12	9	vWhiteLimitMax_ST(100081)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	White Max	error(30000)
12	9	vBlackLimitMin_ST(100082)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Black Min	normal(10000)
12	9	vEDH_Det_ST(100083)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	EDH ANC EDH	disabled(-1)
12	9	vAP_Det_ST(100084)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	EDH Active Picture	normal(10000)
12	9	vFF_Det_ST(100085)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	EDH Full Field	disabled(-1)
12	9	vTRS_ST(100086)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	[illegible] Detection	disabled(-1)
12	9	vSigPres_ST(100087)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Carrier Detect	normal(10000)
12	9	vBlackDet_ST(100088)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Black Detection	normal(10000)
12	9	aChan1_sil_ST(100096)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Silence	error(30000)
12	9	aChan2_sil_ST(100097)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Silence	normal(10000)
12	9	aChan1_mxLvl_ST(100098)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Max Level	disabled(-1)
12	9	aChan2_mxLvl_ST(100099)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Max Level	disabled(-1)
12	9	aChan1_mnLvl_ST(100100)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Min Level	normal(10000)
12	9	aChan2_mnLvl_ST(100101)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Min Level	normal(10000)
12	9	aChan1_ovld_ST(100102)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Overload	normal(10000)
12	9	aChan2_ovld_ST(100103)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Overload	normal(10000)
12	9	aPhase_ST(100104)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Phase	normal(10000)
12	9	aStWidth_ST(100105)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Stereo Width	disabled(-1)
12	9	aChan1_mnDyna_ST(100106)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Min Dynamics	disabled(-1)
12	9	aChan2_mnDyna_ST(100107)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Min Dynamics	disabled(-1)
12	9	aChan1_slicing_ST(100108)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch1 Slicing	normal(10000)
12	9	aChan2_slicing_ST(100109)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Ch2 Slicing	normal(10000)
12	9	overall_status(100121)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Overall	error(30000)
12	9	avStatusIn(100122)	icontrol_product1_RACK1_D12_FRAME_Densite_SLOT_9_31	Immediate Signal A...	normal(10000)

The device index for this particular frame is 12. The slot for the card of interest is 9. The table also shows all the supported alarm types (*trapIndex*) for this card. The type field is the long ID of the card:

`icontrol_product1_RACK1_D12_FRAME_Densité_SLOT_9_31`

This can be decomposed as follows:

`icontrol_product1`	the Application Server host name
`RACK1_D12_FRAME`	the Densité frame name as entered in Densité Manager,
`Densité_SLOT`	a static field
`9`	the slot number
`31`	the model number for the SCP-h1121 card

The polling process is initiated by sending a request to the GSM using an OID of this form:

`1.3.6.1.4.1.3872.11.1.1.6.deviceID.slotID.statusIndex`

where `deviceID` is the unique ID the Densité frame is given by the Application Server, `slotID` is the slot number of the card for which the current status is in question, and statusIndex is the number associated with a particular status (e.g., *black* = 100088, *freeze* =100075)

To obtain the *freeze detection* status of the signal that is feeding this SDI probe, the following OID should be polled:

Textual OID

`.iso.org.dod.internet.private.enterprises.miranda.gsm.statusTable.statusEntry.status.12.9.100075`

Numerical OID

`.1.3.6.1.4.1.3872.11.1.1.6.12.9.100075 (status OID)`

This would return the following variable binding:

```
status.12.9.100075:-->normal(10000)
```

Developer Tip

When developing code to interface with the iControl GSM agent, developers often ask how to determine a specific device index. A programming approach would be to poll the alarm status table using `SNMP GET-NEXT`, starting at the beginning of the table, and then to compare the returned `varBind` value (using `contains`) with the Densité or Imaging frame name. Once an entry in the table is found that matches the frame name, the device index can be determined from the OID.

GSM SNMP Traps

SNMP traps are GSM actions attached to GSM alarms. In order to configure a trap (see Configuring iControl to Send Traps, on page 499), the following information must be specified:

- the alarm transition(s) that will trigger the trap
- a trap target destination IP
- a trap SNMP version
- a trap number

The trap number, which is chosen arbitrarily from a predefined range, can be assigned to alarms that appear in the GSM browser, as well as to alarm transitions (e.g., from *normal* to *error*). The same trap number can be re-used for more than one alarm or alarm transition.

> **Note:** Values 1 to 99999 are reserved for user-defined virtual alarms and for third party SNMP devices. Values of 100000 and up are iControl alarms.

Once a trap number as been configured, a new user defined MIB entry is added for the trap.This is the form for the custom MIB entry for a v1 trap type:

```
User_defined_event TRAP-TYPE
      ENTERPRISE  miranda
      VARIABLES   { trapDevice, trapAlarm }
      DESCRIPTION
"User defined description"
::= user_defined_trap_number
```

This is the form for the custom MIB entry for a v2c trap type:

```
User_defined_event NOTIFICATION-TYPE
      OBJECTS { trapDevice, trapAlarm }
      STATUS  current
      DESCRIPTION
      "User traps sent after certain conditions"
 ::= { traps 0 3 }
```

Note: The v2c trap type currently does not include the configured trap number, making it necessary to repoll to determine the alarm that triggered the trap.

GSM-MIB

The following is an excerpt from the GSM-MIB file that relates to traps.

```
-- ****************************************
-- User Trap Events
-- ****************************************
traps OBJECT IDENTIFIER ::= { gsm 2 }
trapAlarm OBJECT-TYPE
      SYNTAX  OCTET STRING
      ACCESS  read-only
      STATUS  mandatory
      DESCRIPTION "The Alarm Identifier"
      ::= { traps 1 }
trapDevice OBJECT-TYPE
      SYNTAX  OCTET STRING
      ACCESS  read-only
      STATUS  mandatory
      DESCRIPTION "The service or transport stream that generated the alarm"
      ::= { traps 2 }
statusTrap NOTIFICATION-TYPE
      OBJECTS { trapDevice, trapAlarm }
      STATUS  current
      DESCRIPTION
      "User traps sent after certain conditions"
      ::= { traps 0 3 }
```

Example

In this example, a user has attached GSM trap actions to an SCP probe *freeze detection* alarm. The traps have been configured as follows:

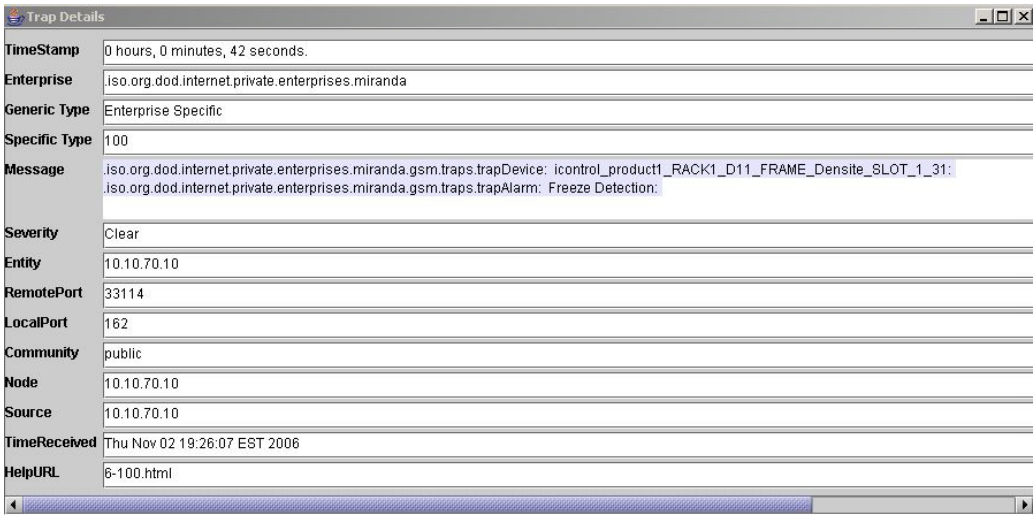
- if an alarm goes from normal (green) to error (red), trap number 100 is sent
- if an alarm goes from error (red) to normal (green), trap number 200 is sent

In order for these traps to be successfully parsed by a third party SNMP manager, the following custom MIB entries should be added to its GSM-MIB:

```
clear TRAP-TYPE
      ENTERPRISE  miranda
      VARIABLES   { trapDevice, trapAlarm }
      DESCRIPTION
      "A clear trap means that the alarm condition that existed has now been
      cleared."
      ::= 100
error TRAP-TYPE
      ENTERPRISE  miranda
```

```
        VARIABLES   { trapDevice, trapAlarm }
        DESCRIPTION
        "A error trap means that a error alarm condition is present"
        ::= 200
END
```

When the SCP probe *freeze detection* alarm goes from an error state to a normal state, a trap is sent to the specified trap target. Here's the output of a trap catcher application.



The trap number is shown in the **Specific Type** field. Variable bindings included in the trap are the `trapDevice` and the `trapAlarm` which are shown in the **Message** field. From the `trapDevice`, the SNMP manager can determine which card generated the trap. In this case it is the card with the following long ID:

`icontrol_product1_RACK_D11_FRAME_Densité_SLOT_1_31`

This long ID can be interpreted as follows:

`icontrol_product1`	Application server host name
`RACK_D11_FRAME`	Densité frame name (as entered in Densité Manager)
`1`	Slot number
`9`	the slot number
`31`	the model number for the SCP-1121 card

Application Server Health Monitoring

Health monitoring in iControl is accomplished in two ways:

- Third party SNMP managers can poll an Application Server directly via its Net-SNMP agent.
- iControl can monitor itself via the *AppServer Health Monitoring* plug-in.

Net-SNMP Agent

Third party SNMP managers can monitor the health of an iControl Application Server and its services using iControl's customized version of the open source Net-SNMP package (www.net-snmp.org), which is installed on all iControl Application Servers. The Net-SNMP agent can be polled (using UDP port 1161) for health monitoring data based on the following MIBs (also part of the Net-SNMP package):

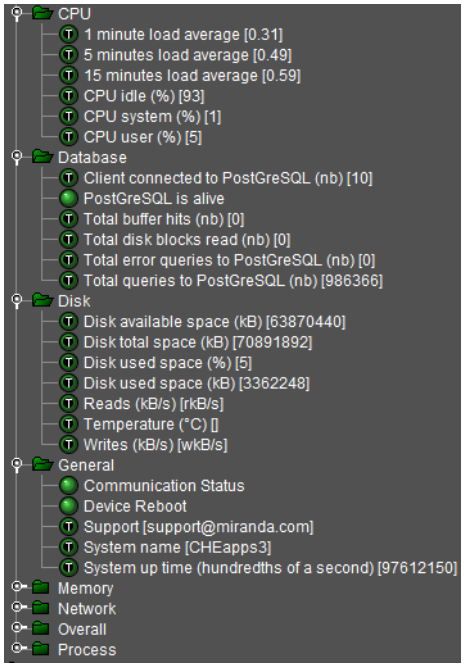
UCD-SNMP-MIB			
ssCPUidle	laLoad.2	memTotalReal	dskTotal
ssCPUuser	laLoad.3	memAvailableReal	dskAvail
ssCPUsystem	memTotalSwap	memBuffer	dskUsed
laLoad.1	memAvailableSwap	memCached	dskPercent
HOST-RESOURCE-MIB			
hrSystemNumUsers	hrSystemProcesses		
IF-MIB			
ifDescr	ifSpeed	ifInDiscards	ifOutDiscards
ifInErrors	ifOutErrors	ifInOctets.	ifOutOctets
SNMPv2-MIB			
sysUpTime	sysContact	sysName	

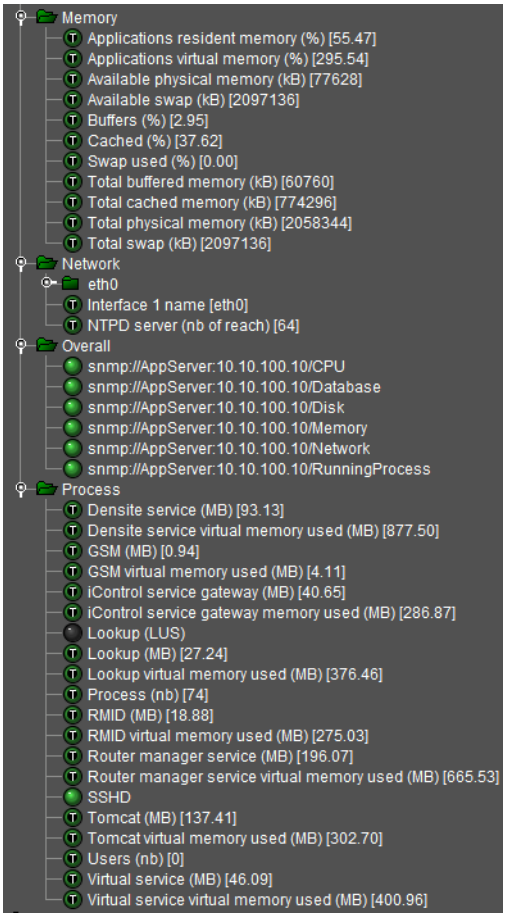
The Net-SNMP agent is running by default. There is no configuration necessary on the iControl side. You will need to compile the Net-SNMP MIBs in the third party SNMP manager, specifying the Application Server's IP address and port 1161.

AppServer Health Monitoring Plug-in

The *AppServer Health Monitoring* plug-in is a custom SNMP driver created by Grass Valley that takes advantage of the Net-SNMP agent to monitor the health of an iControl Application Server and its services. This plug-in polls the Net-SNMP agent for health monitoring data, and reports the results within the GSM's Alarm Browser.

The following screens show typical alarms available via the GSM *AppServer Health Monitoring* plug-in.



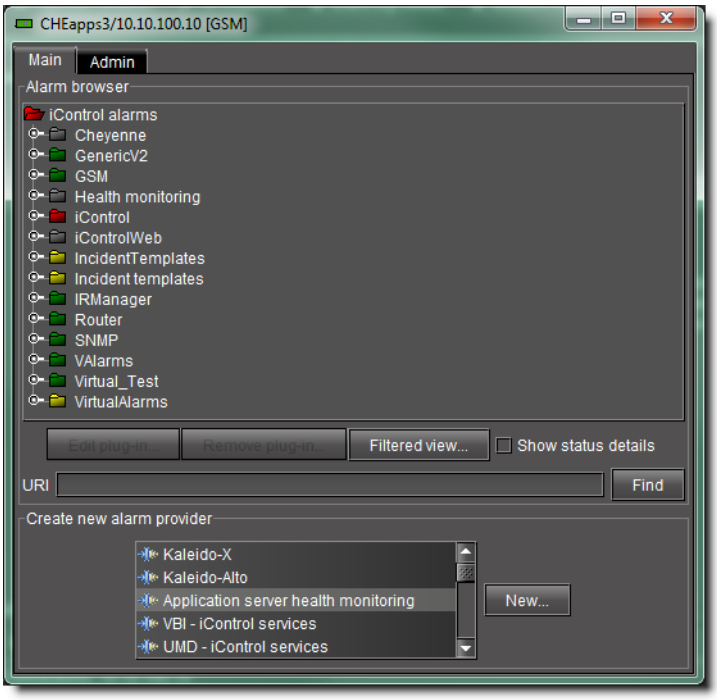


REQUIREMENT

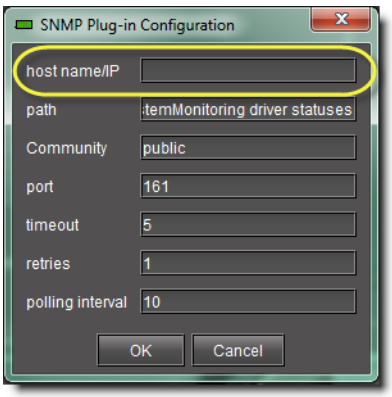
Before beginning this procedure, make sure you have opened the GSM Alarm Browser (see Opening the GSM Alarm Browser, on page 710).

To enable the GSM AppServer Health Monitoring plug-in

1. In the GSM Alarm Browser, in the list under **Create new alarm provider**, select **AppServer Health Monitoring**, and then click **New**.

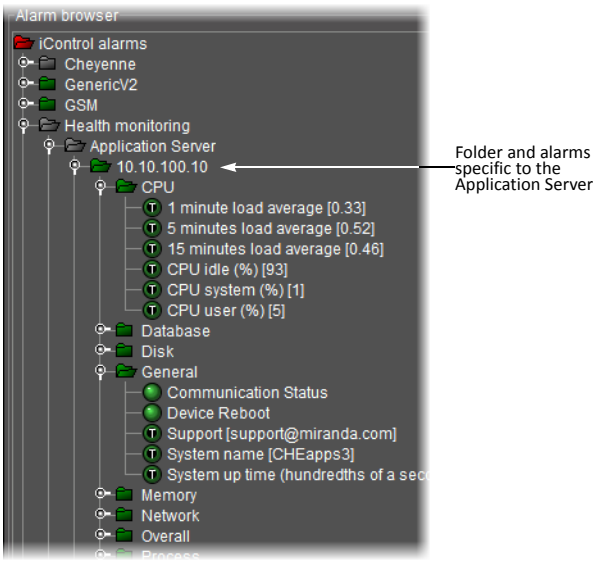


2. In the **Host** field of the **SNMP plug-in configuration** window, type the IP address of the Application Server whose health you wish to monitor, and then click **OK**.



IP address (circled) of the Application Server whose health you would like to monitor

3. In the **Alarm Browser** window, health monitoring alarms will appear in a folder whose name corresponds to the IP address of the Application Server.



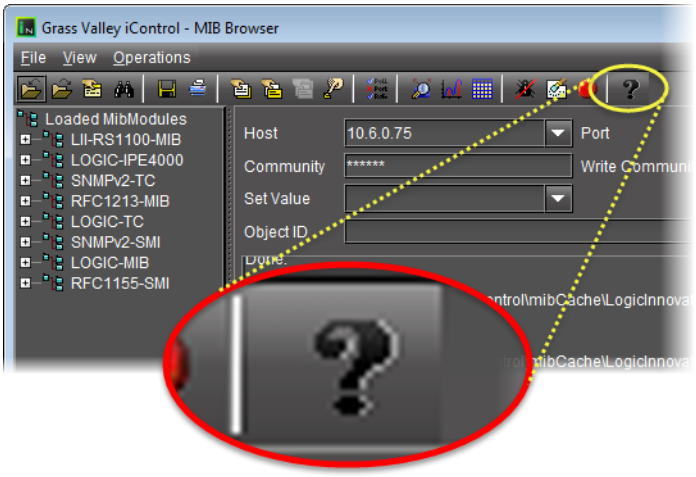
Accessing the MIB Browser Help Files

REQUIREMENT

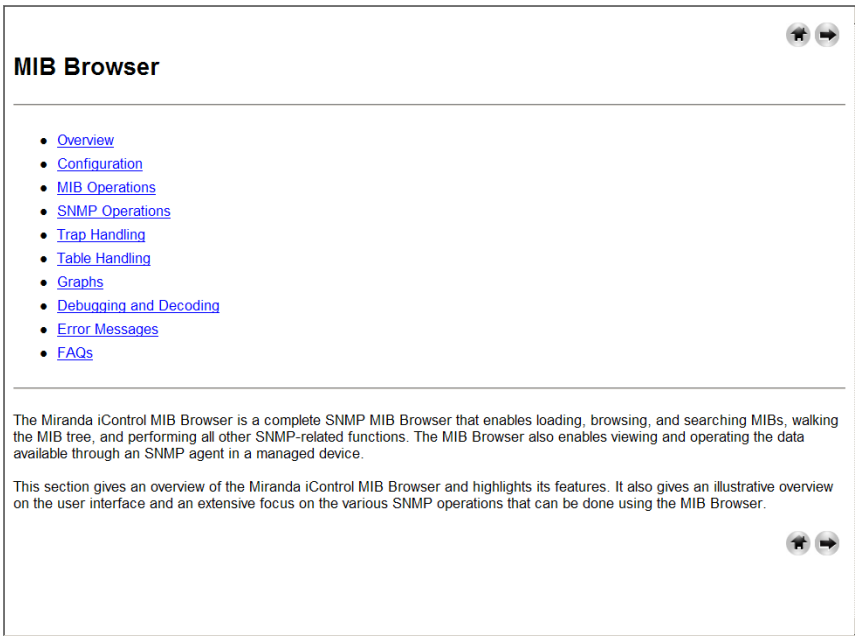
Before beginning this procedure, make sure you have opened the MIB Browser (see page 712).

To access the MIB Browser help files

- In MIB Browser, click the Help button ( ).



SYSTEM RESPONSE: The MIB Browser online help appears in your browser.



Adding a Third-Party SNMP Alarm Object to an iControl Web Page

iControl allows you to quickly integrate a third-party SNMP device into your monitoring configuration by adding alarm objects onto **iC Web** pages. You can select any SNMP OID from a MIB loaded in the iControl MIB Browser, and then drag it directly onto a Web page in **iC Creator**. With some minor adjustments, this new Web object establishes a direct link to a particular status on the third-party SNMP device.

The following procedures describe how to display the SNMP status of third party devices on **iC Web** pages. The first procedure applies in the case where the SNMP parameter is directly available in the MIB Browser. The second applies where the parameter is contained in an SNMP table.

> **Note:** Before beginning either procedure, make sure that the iControl Application Server you will be using has an active connection to the third-party SNMP device. You will also need the device's IP address, as well as a copy of its SNMP MIB.

Adding an Object from the MIB Browser

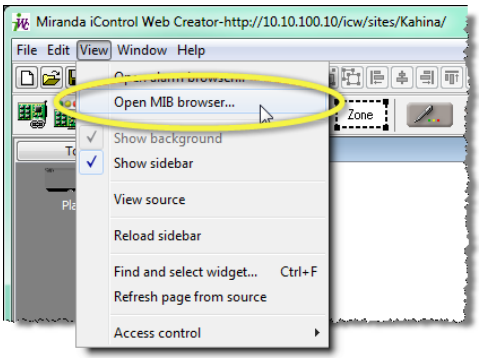
This procedure applies to MIB parameters that are not contained in an SNMP table.

REQUIREMENT

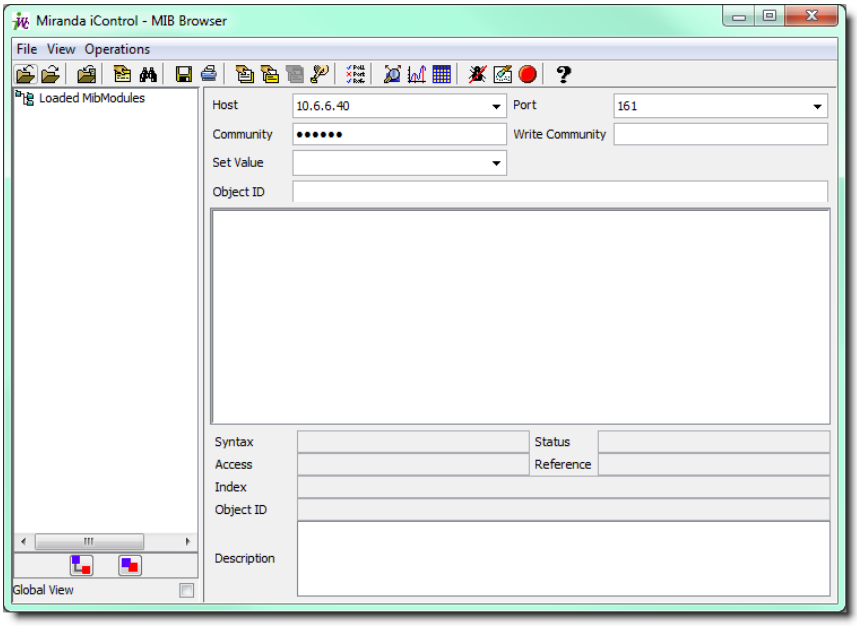
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To add a third-party SNMP alarm object to a Web page

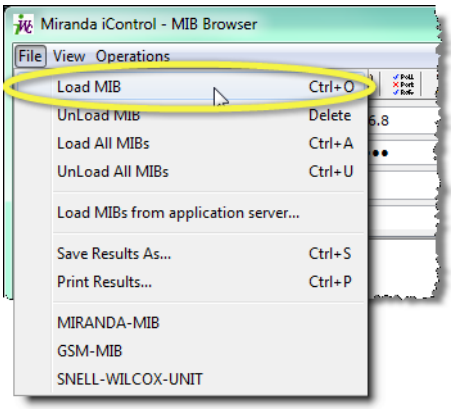
1. In **iC Creator**, on the **View** menu, click **Open MIB Browser**.



SYSTEM RESPONSE: The **MIB Browser** window opens.

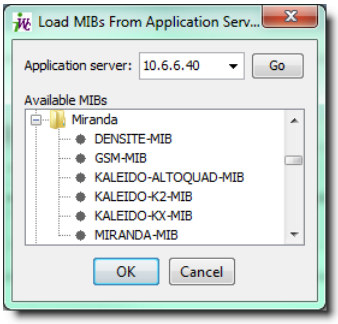


2. Choose **Load MIB from application server** from the MIB Browser's **File** menu.



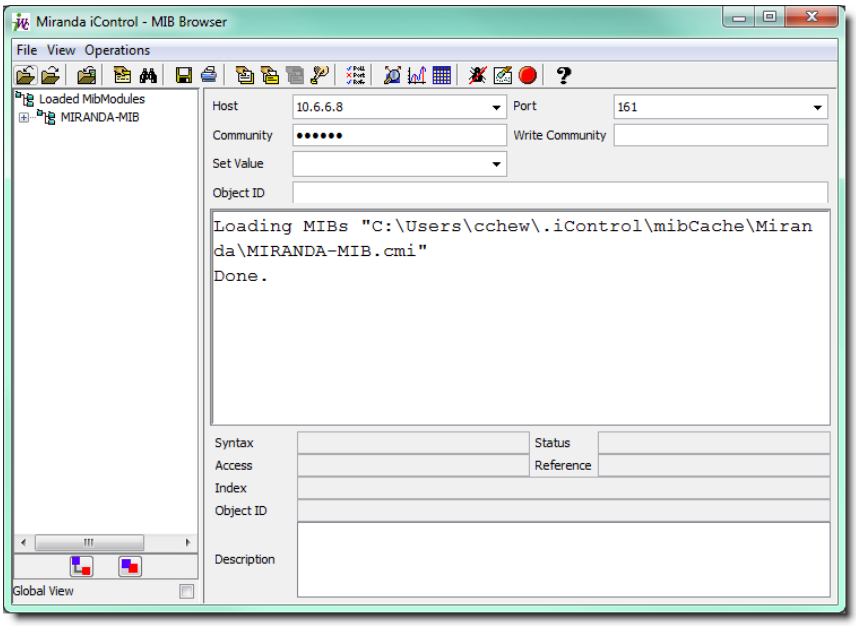
Note: If the MIB for the device you are working with is not on the Application Server, use the `Load MIB` command to locate and open the appropriate MIB.

3. In the list that appears, find and select the MIB for the device you are working with.

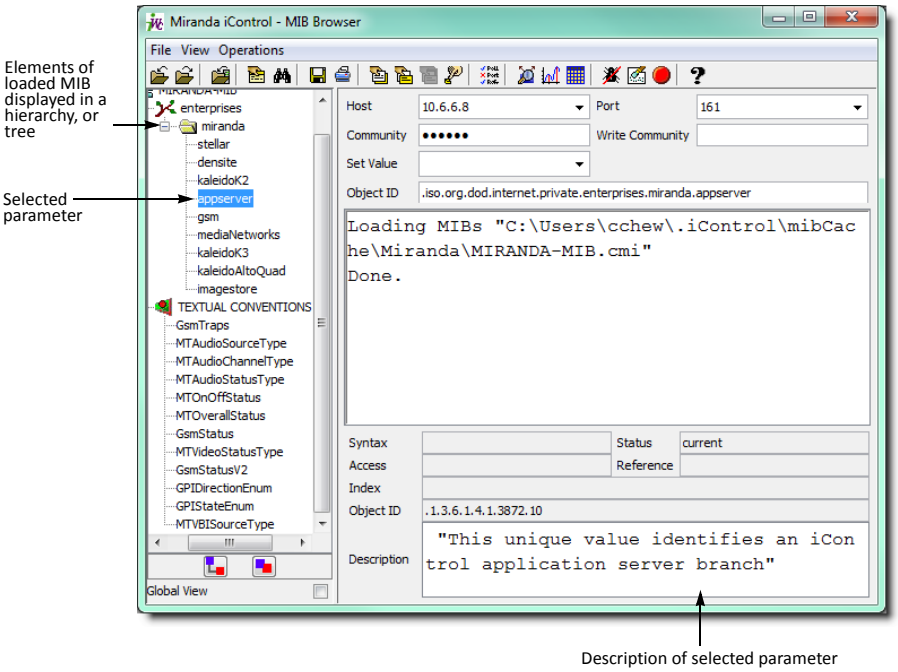


4. Click **OK**.

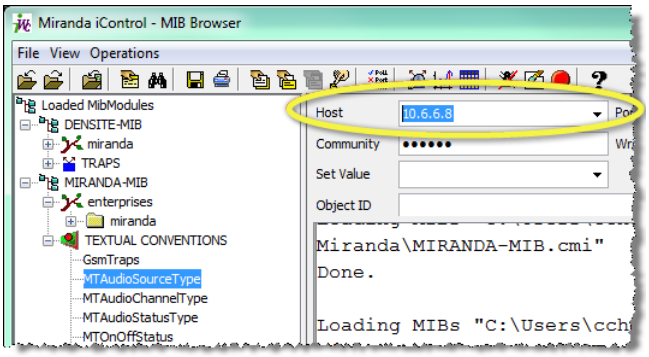
   SYSTEM RESPONSE: The selected MIB is loaded and appears in the left column of the MIB Browser.



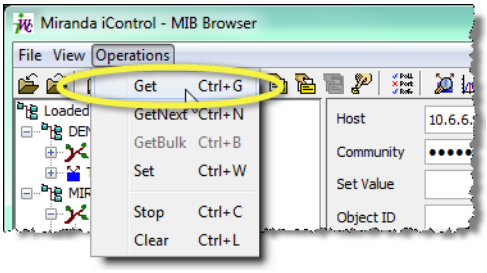
5. Click the Expand button ( ) to see the MIB's tree structure.
6. Find the parameter you wish to monitor in the hierarchy (tree) of the loaded MIB.



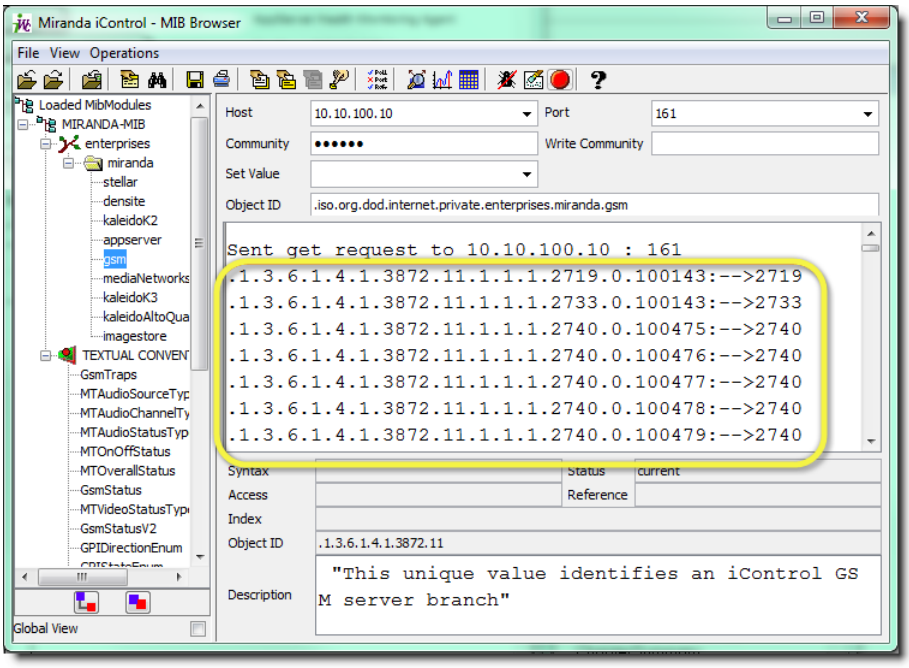
7. In the **Host** field, type the IP address of the third-party SNMP device you are working with.



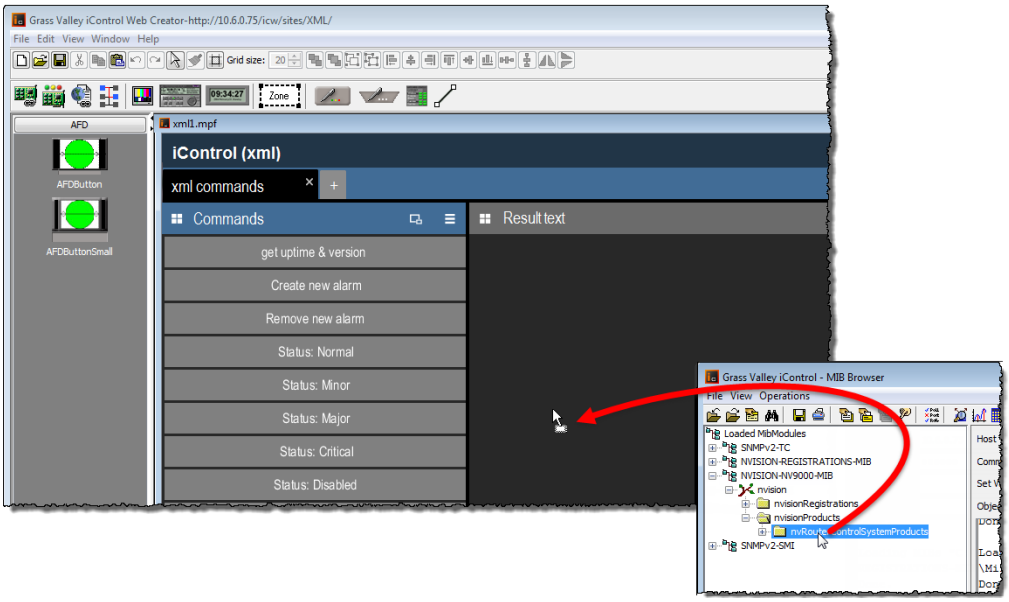
8. Choose **Get** from the **Operations** menu (or click the **SNMP Get** button in the toolbar).



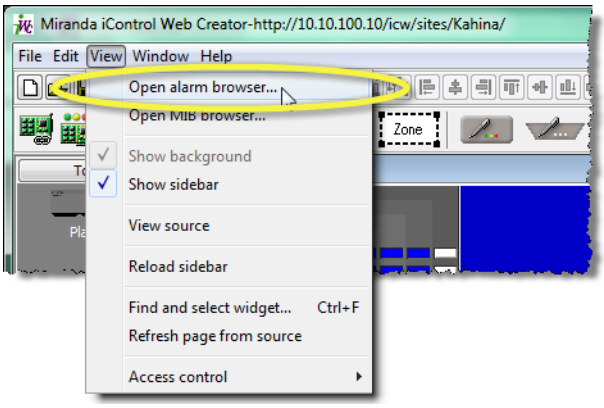
Make sure that the MIB Browser can communicate with the target device (the result of the `get` operation will appear in the message area).



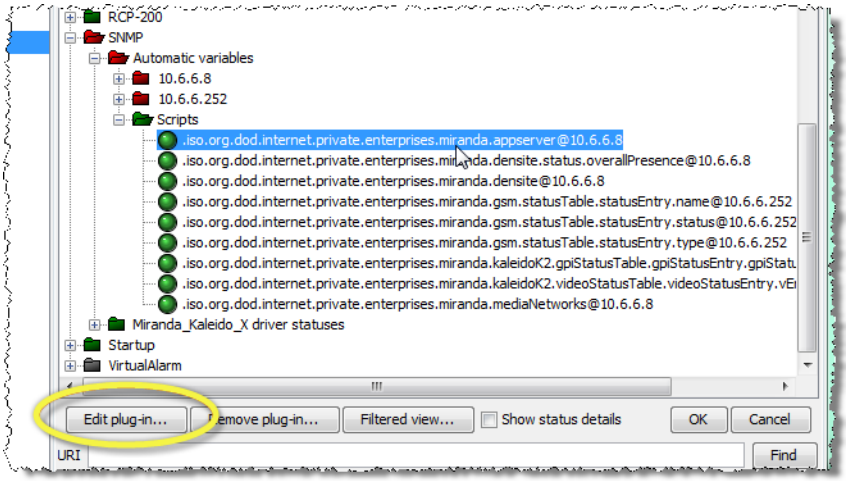
9. Click and drag the MIB parameter from the MIB Browser window onto the Web page.



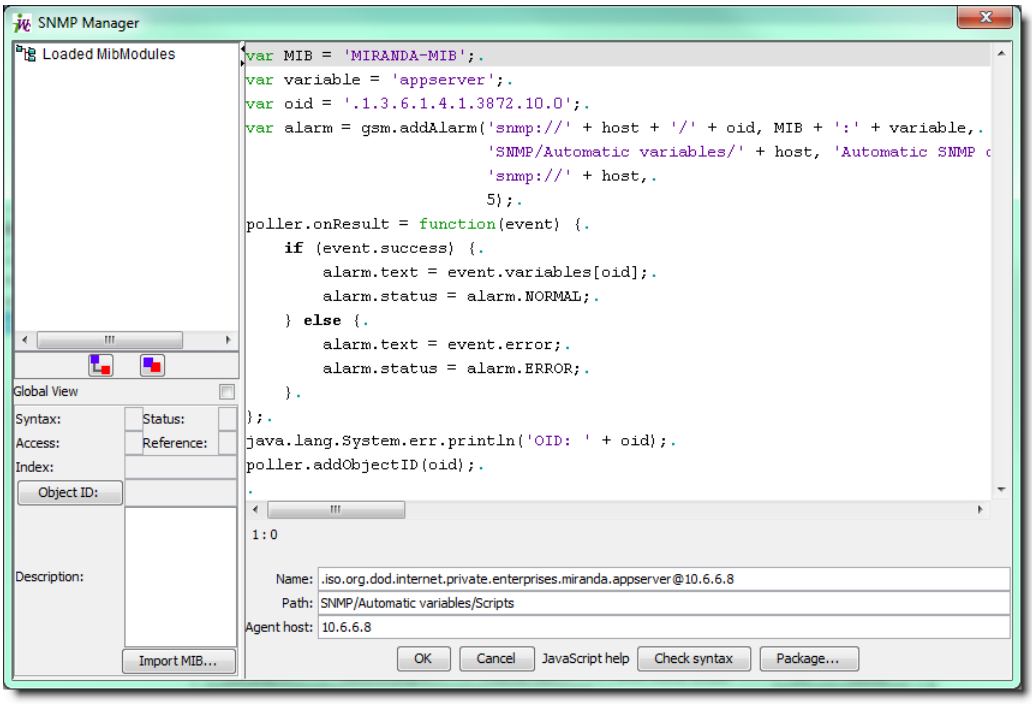
10. On **iC Creator**'s **View** menu, click **Open alarm browser**.



11. In the **Alarm browser** window, scroll down to the **SNMP** folder. Click to expand the folder contents until you find the alarm corresponding to the new Web page object (inside the **Scripts** folder). Select this object, and then click **Edit plug-in**.



SYSTEM RESPONSE: The **SNMP Manager** window opens, showing the default script generated for the new object.



12. Edit the script as needed, and then click **OK**.

    SYSTEM RESPONSE: The object on the Web page is updated to reflect any changes.

Adding an Object from an SNMP Table

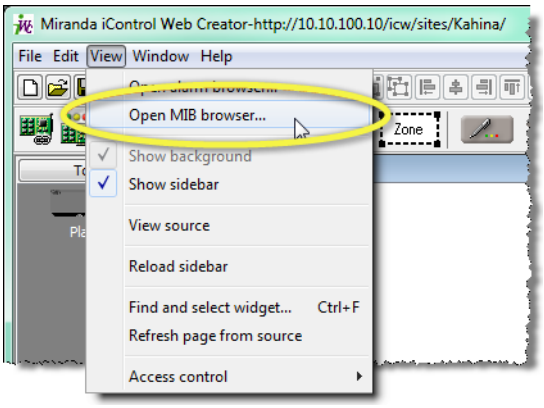
This procedure applies to MIB parameters that are contained in an SNMP table.

REQUIREMENT

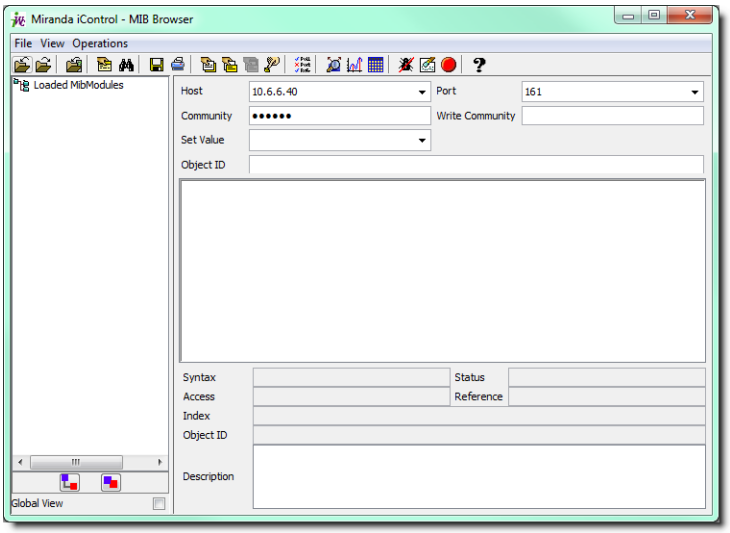
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To add a third-party SNMP alarm object to a Web page

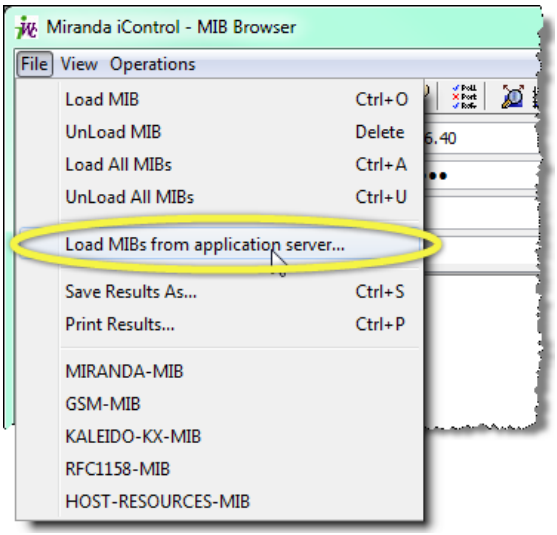
1. In **iC Creator**, open a Web page.
2. On the **View** menu, click **Open MIB Browser**.



SYSTEM RESPONSE: The **MIB Browser** window opens.

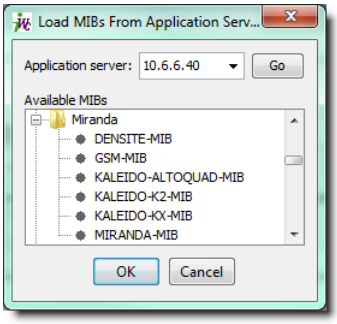


3. On the **File** menu, click **Load MIBs from application server**.



Note: If the MIB for the device you are working with is not on the Application Server, use the `Load MIB` command to browse elsewhere.

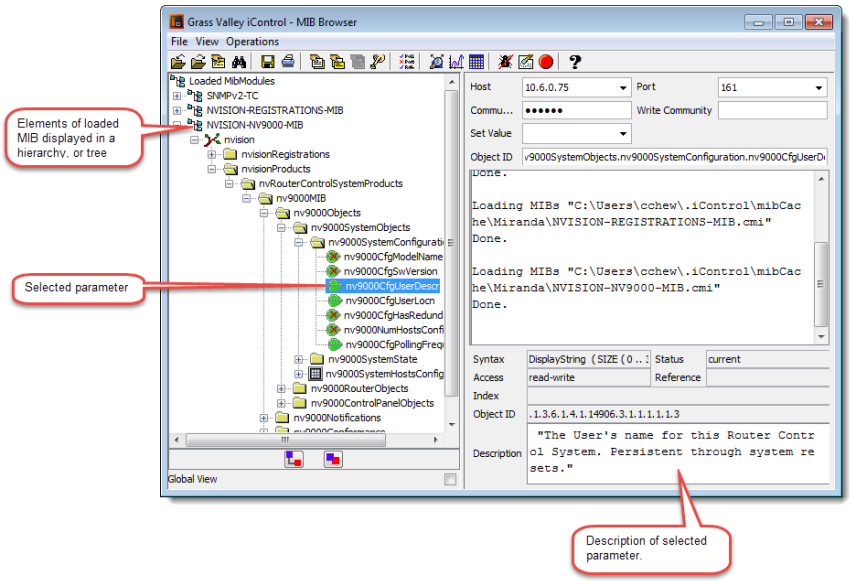
4. In the list that appears, find and select the MIB for the device you are working with.



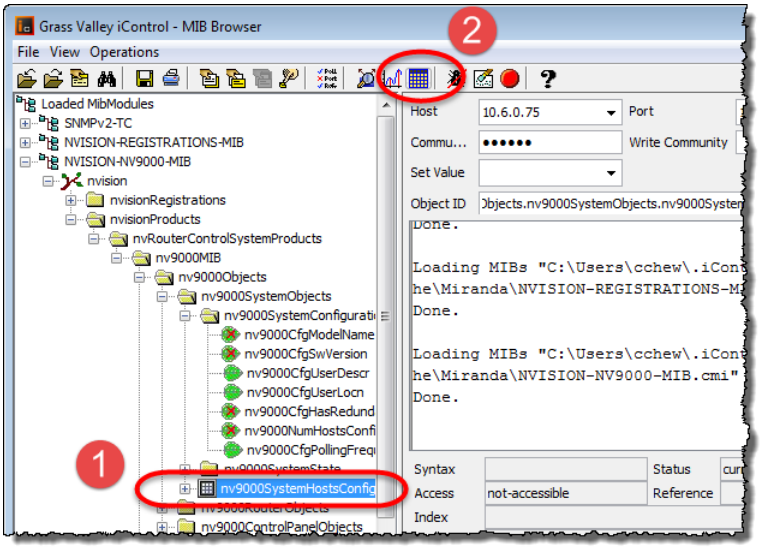
5. Click **OK**.

   SYSTEM RESPONSE: The selected MIB is loaded and appears in the left column of the MIB Browser.

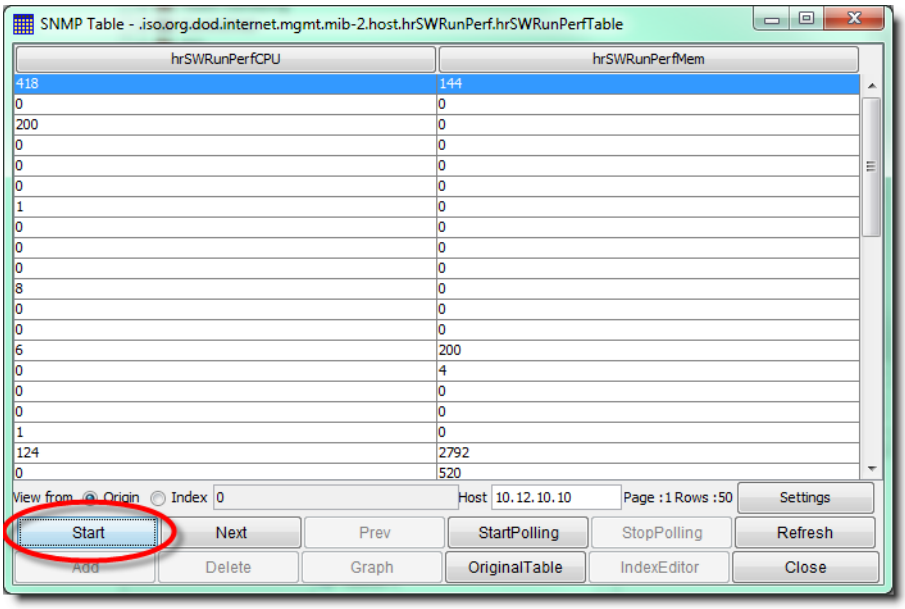
6. Find and select the parameter you wish to monitor in the hierarchy (tree) of the loaded MIB.



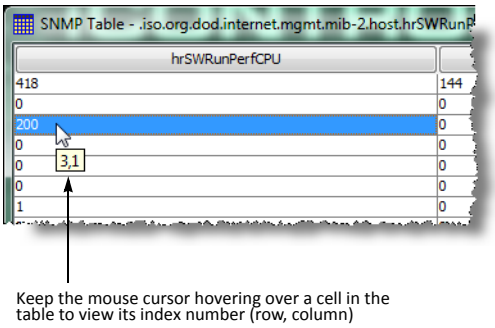
7. Select the table to which the object belongs, and then click the **View SNMP data table** button .



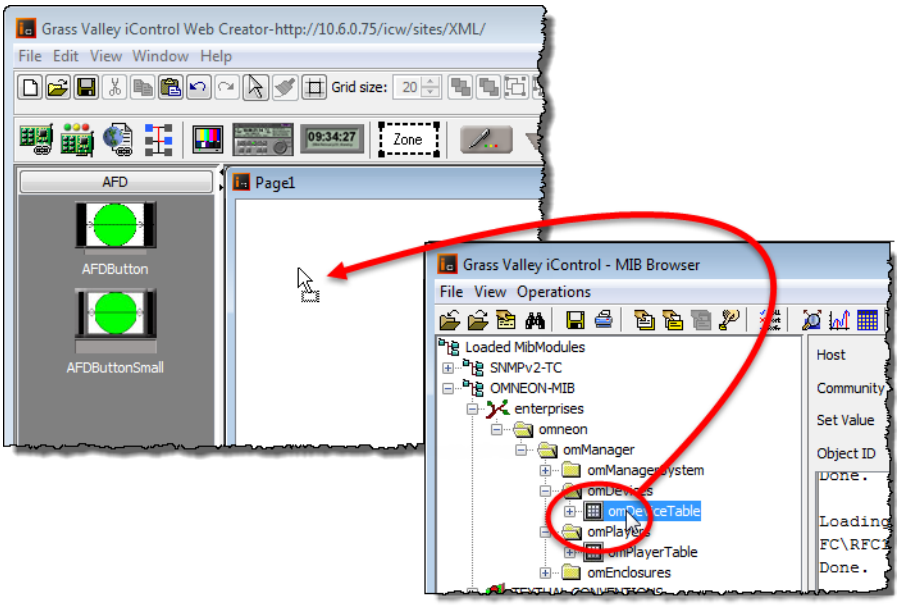
8. When the **SNMP Table** window appears, click **Start** to populate the table.



9. Select the parameter you are interested in.
10. Take note of the index number (row, column) that appears.



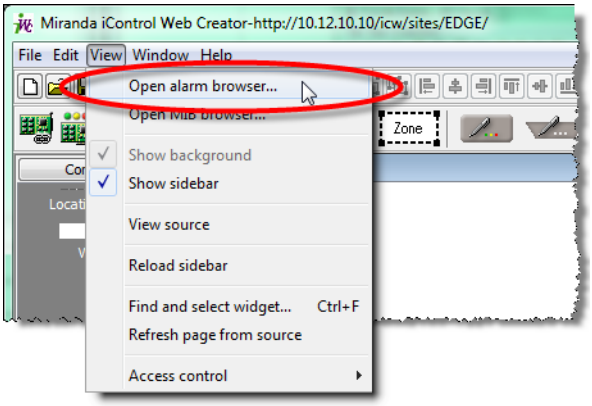
11. Close the **SNMP Table** window.
12. Click and drag the MIB parameter from the **MIB Browser** window onto the Web page.



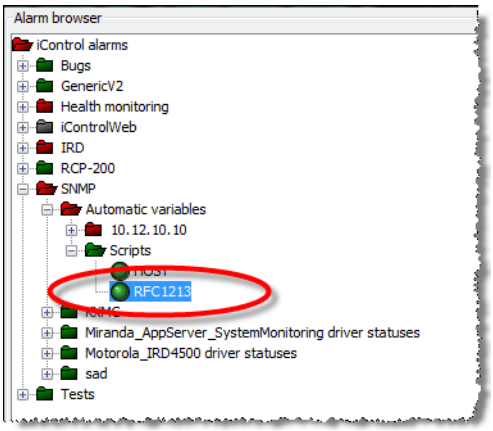
SYSTEM RESPONSE: The corresponding alarm object appears on the Web page, showing the actual status of the MIB parameter.

> **Note:** You may receive an error message. This is because the alarm object, by default, points to the index of the SNMP table, not the specific table entry.

13. On **iC Creator**'s **View** menu, click **Open alarm browser**.

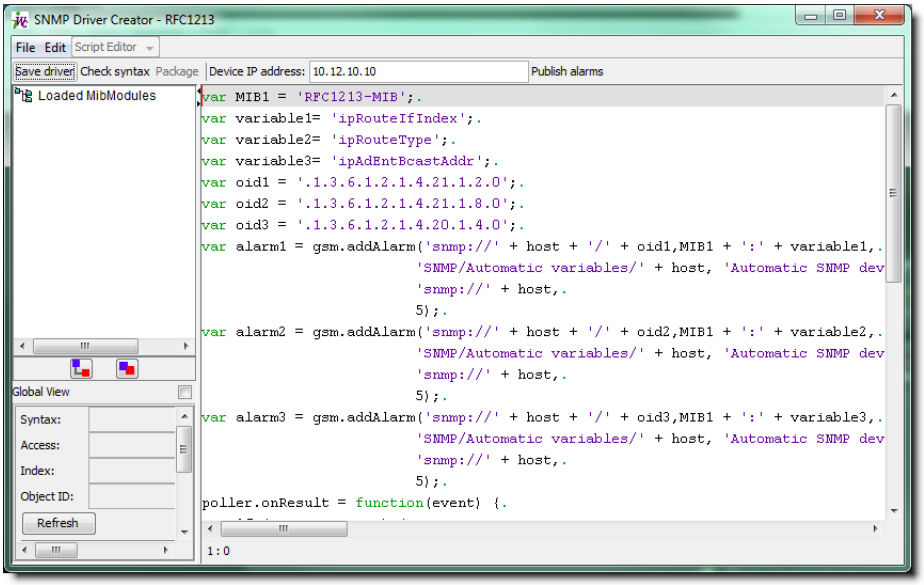


14. Scroll down to the **SNMP** folder. Click to expand its contents until you find the alarm corresponding to the new Web page object (in the **Scripts** folder). Select this object, and then click **Edit plug-in**.

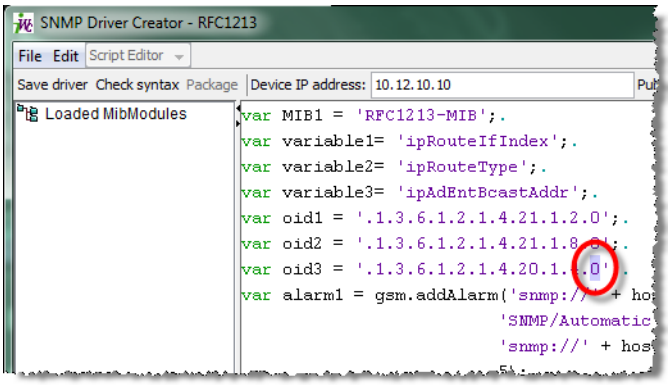


Alarm (circled) corresponding to new SNMP Web object

SYSTEM RESPONSE: The **SNMP Driver Creator** window opens.

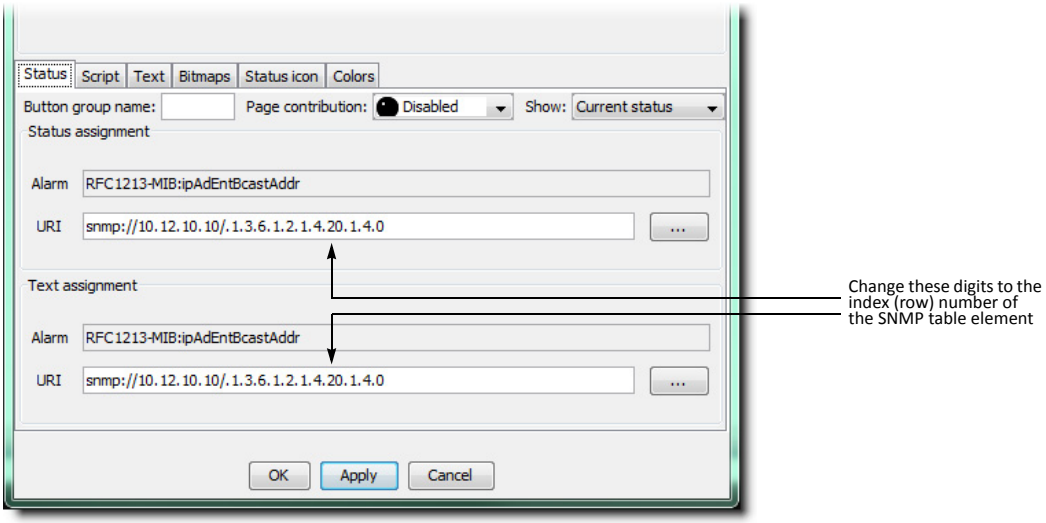


15. Change the last digit of the OID to the index number you determined in step 10.



Change this digit (circled) to the index (row) number of the SNMP table element

16. Edit the script as needed, and then click **OK**.
17. Double-click the alarm object on the Web page to open the **Status icon properties** window. Change the last digit of both URIs to the index number you determined in step 9.
18. Click **OK**.



SYSTEM RESPONSE: The object on the Web page is updated to reflect the changes.

9 Fingerprint Comparison and Analysis

Summary

Key Concepts

Fingerprint Comparison and Analysis

iControl's *fingerprint comparison and analysis* feature allows you to perform any of the following functions across potentially broad signal distribution networks:

- **detect and measure lip sync errors**
- **compare video content**
- **compare audio content**

In conjunction with Densité cards, iControl allows you to monitor conditions where the synchronization between audio and video has been severed (lip sync detection). Alternatively, you may choose to compare strictly video content or audio content between two or more sources (video-video/audio-audio content comparison).

Input signals required for fingerprint comparison

Fingerprint comparison mode	Minimum # of inputs required	Description of input
Lip sync error detection	1 *REFERENCE* source	a fingerprinting point where the audio/video synchronization is known to be good upstream of probe points
	1 *PROBED* source	a fingerprinting point where the audio/video sync is to be compared with the reference
Video content comparison	1 *REFERENCE* source	a video fingerprinting point against which a probed video source is to be compared for content integrity (match or mismatch).
	1 *PROBED* source	a fingerprinting point where the video sync is to be compared with the reference
Audio content comparison	1 *REFERENCE* source	an audio fingerprinting point against which a probed audio source is to be compared for content integrity (match or mismatch)
	1 *PROBED* source	a fingerprinting point where the audio/video sync is to be compared with the reference

iControl allows you to designate groupings of input sources. These *Comparison Groups* are comprised of those signals being compared to one another. Each comparison group is a subset of the overall pool of available input sources.

Regardless of the fingerprint comparison mode you choose (*lip sync*, *video*, or *audio*), one of the sources in each comparison group must be designated as the *Reference source*. The *Reference source* is the source each *Probed source* is compared to.

In the case of lip sync error detection, the *Reference source* is a point where the audio/video synchronization is known to be good and that is upstream to all the *Probed sources*. In the cases of both the video content and audio content comparisons, the *Reference source* is the baseline each of the *Probed sources* is compared to.

Notes

- A fingerprinting point can be re-used in multiple comparison groups as a reference or a probed point.
- Fingerprinting Densité cards can be distributed among multiple Densité frames, managed by multiple Application Servers as long as there is network connectivity between the Applications Servers and the Densité frames.
- A maximum delay of +/- 4 seconds between the reference and probed signal is tolerated.

An Application Server, equipped with a *Fingerprint Analyzer Service*, can read the fingerprints of simultaneous input feeds and compare them to the reference. iControl uses the fingerprints to perform a comparison and analysis, and provides a real-time view of the results on its **Status** tab, in the GSM Alarm Browser, as well as in alarm widgets in iC Web, if applicable.

The maximum number of fingerprint channels recommended is a value that is hardware-dependent, specifically upon the Application Server model type and the allocated memory of the server, as follows:

Maximum recommended fingerprint channels

Application Server model	Memory allocation	Maximum recommended number of fingerprint channels
Dell PowerEdge R200	512MB	150
	1GB	250
Dell PowerEdge R320	512MB	150
	1GB	250
	2GB	450

This feature supports the following Densité cards as both probed and referenced input sources:

- **ADX-3981** *(3Gbps/HD/SD 8 AES audio and Metadata de-embedder)*

- **AMX-3981** *(3Gbps/HD/SD 8 AES audio and Metadata embedder)*
- **EAP-3901** *(3Gbps/HD/SD embedded audio and Metadata processor)*
- **EAP-3101** *(SD embedded audio and Metadata processor)*
- **HCO-1822** *(HD/SD/ASI change-over with clean switch and ALC)*
- **HLP-1801** *(HD/SD lip-sync probe)*
- **XVP-3901** *(3Gbps/HD/SD up, down, and cross converter with audio processor)*
- **EdgeVision**

IMPORTANT: In iControl installations, the following parameters and limitations currently apply:

- If you have a Dell PowerEdge R200 Application Server, iControl supports a maximum of 40 fingerprint comparisons
- If you have a Dell PowerEdge R210 Application Server, iControl supports a maximum of 60 fingerprint comparisons
- If you have a Dell PowerEdge R310 Application Server, iControl supports a maximum of 120 fingerprint comparisons.
- If you have a Dell PowerEdge R320, or R330 Application Server, iControl supports a maximum of 200 fingerprint comparisons.
- A group is composed of a reference source and 1 or more probe sources. For the purposes of counting comparisons, the reference source is not counted.
- Application Servers used for comparison should be dedicated (i.e. they should not run other resource-intensive services).

See also

For more information about:

- Administrator tasks of the Fingerprint Analysis feature, see page 552.
- Operator tasks of the Fingerprint Analysis feature, see page 566.
- Relevant iControl user interface elements, see User Interface of Fingerprint Analysis Feature, on page 534.
- the **ADX-3981 card**, see the *ADX-3981 3Gbps/HD/SD 8 AES Audio & Metadata De-Embedder Guide to Installation and Operation*.
- the **AMX-3981 card**, see the *AMX-3981 3Gbps/HD/SD 8 AES Audio & Metadata Embedder Guide to Installation and Operations*.
- the **EAP-3101 card**, see the *EAP-3101 SD Embedded Audio and Metadata Processor Guide to Installation and Operations*.
- the **EAP-3901 card**, see the *EAP-3901 3Gbps/HD/SD Embedded Audio & Metadata Processor Guide to Installation and Operations*.
- the **HCO-1822 card**, see the *HCO-1822 HD/SD/ASI Change Over with Clean Switch and ALC Guide to Installation and Operations*.

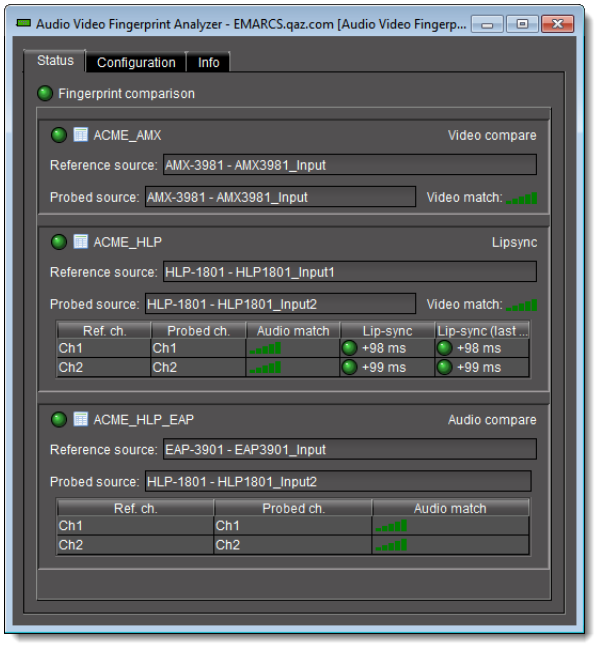
See also (*Continued*)

For more information about:

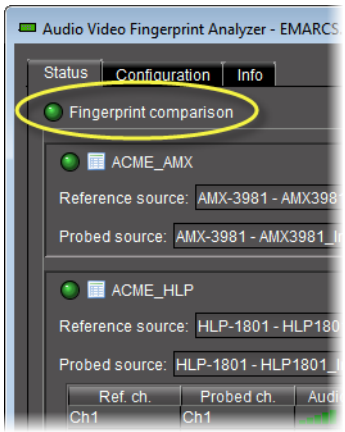
- the **XVP-3901 card**, see the *XVP-3901 3Gbps/HD/SD Up, Down & Cross Converter with Audio Processor Guide to Installation and Operations*.

User Interface of Fingerprint Analysis Feature

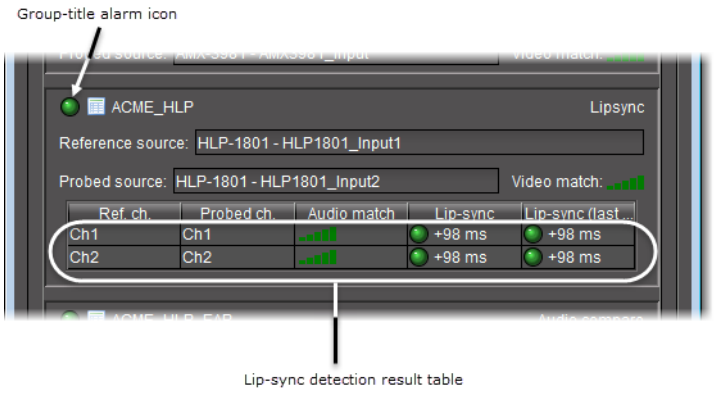
Audio Video Fingerprint Analyzer—Status Tab



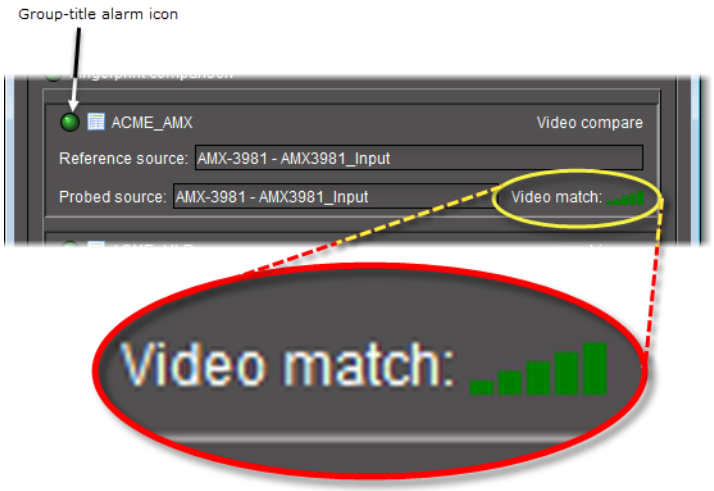
When a comparison of probed sources to a reference is underway, you can observe the real-time results of the fingerprint analysis on the **Status** tab of **Audio Video Fingerprint Analyzer**. The results are organized by comparison group. Each comparison group area has a results table for each probed source.



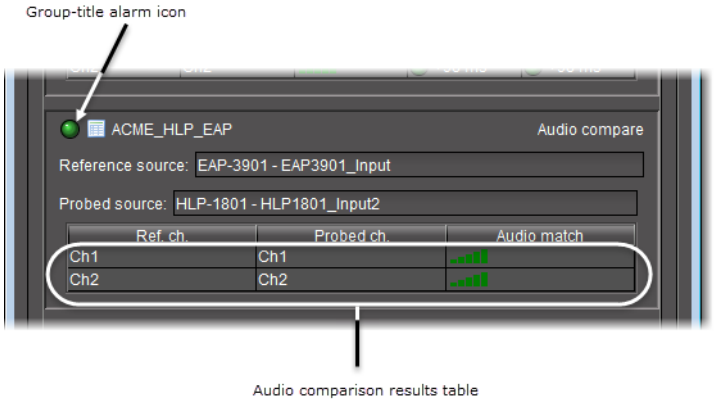
Page-title icon (circled) on Status tab



Lip-sync detection results

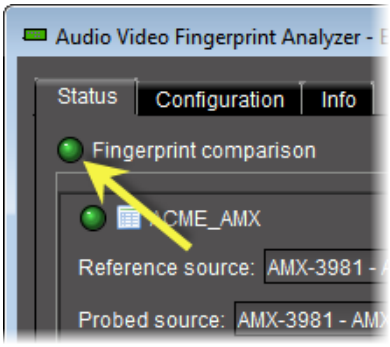
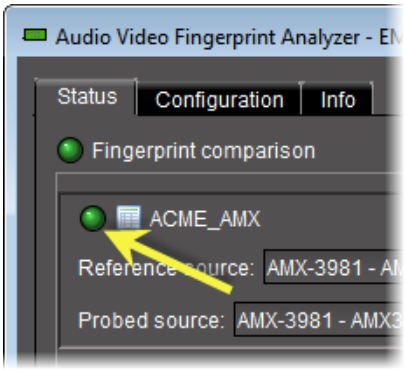
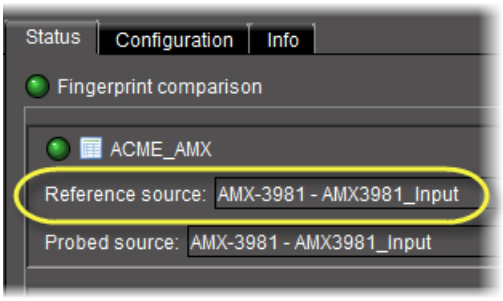


Video comparison results

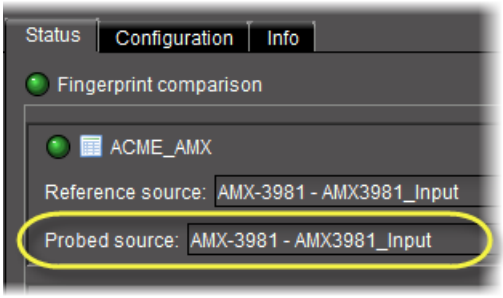
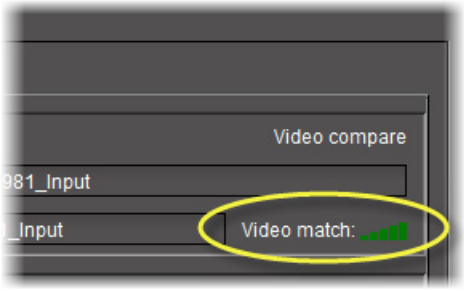
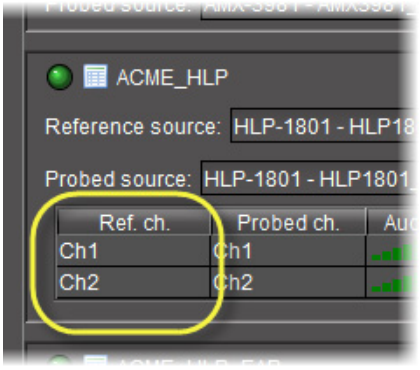


Audio comparison results

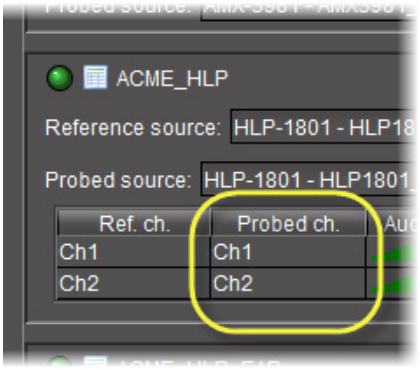
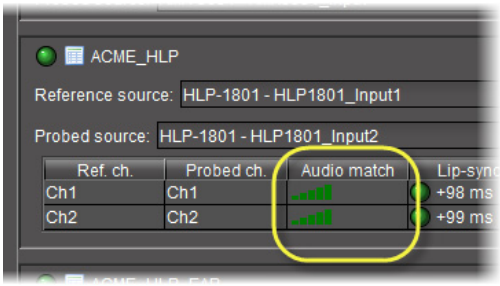
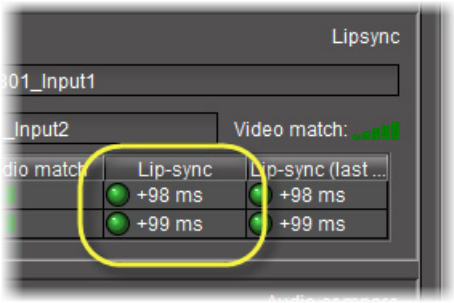
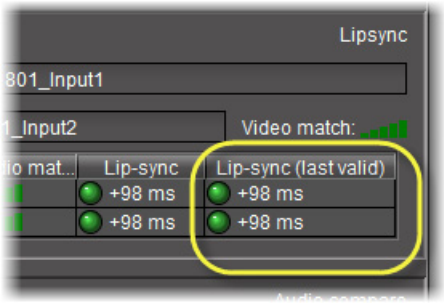
UI elements of the Status tab (Audio Video Fingerprint Analyzer)

UI Element	Description
Lip-sync detection results LED 	This icon indicates the overall status of all alarms about lip-sync detection and content comparison.
Group title alarm LED 	This icon indicates the overall status of all alarms for each comparison group.
Reference source name 	The name of the reference source within each comparison group.

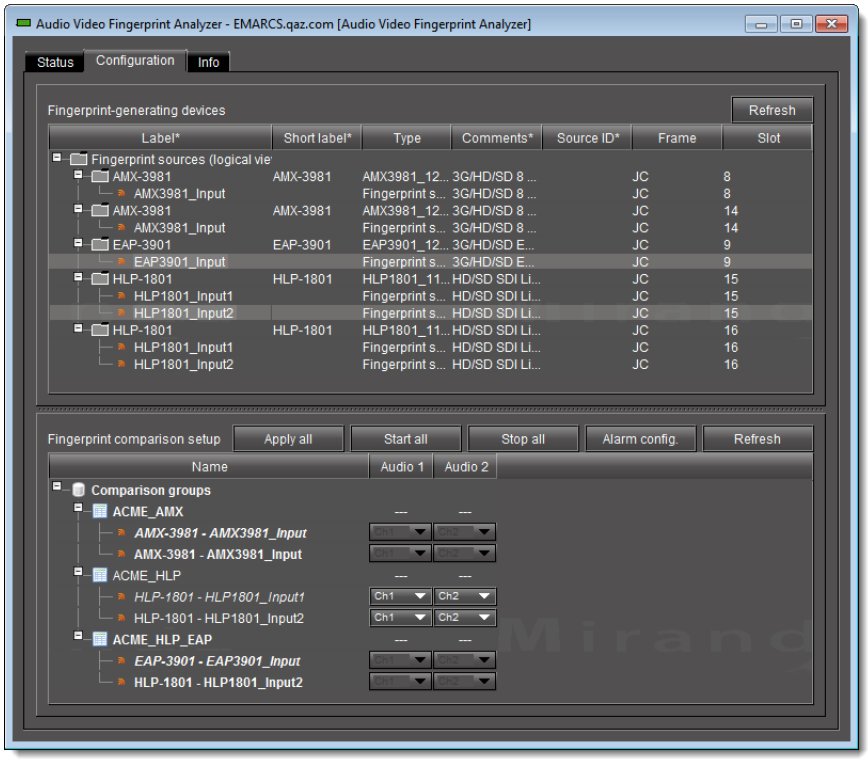
UI elements of the Status tab (Audio Video Fingerprint Analyzer) (*Continued*)

UI Element	Description
Probed source name 	The name of the probed source with each comparison group.
Video match 	This bar graph represents the degree to which there is a match between the reference video signal and the probed video signal. • 3-5 bars: good match • 2 bars: marginal match • 1 bar: poor match or no match
Reference channel 	Reference audio signal channel number for this audio comparison.

UI elements of the Status tab (Audio Video Fingerprint Analyzer) (*Continued*)

UI Element	Description
Probed channel 	Probed audio channel number for this audio comparison.
Audio match 	This bar graph represents the degree to which there is a match between the reference audio signal and the probed audio signal. • 3-5 bars: good match • 2 bars: marginal match • 1 bar: poor match or no match
Lip-sync 	Current measurement (in milliseconds): • if the signal match is normal, • if silence or low motion is not detected on probed or reference signal, and • if updates to this measurement are uninterrupted The precision of the lip-sync delay measurement is +/ 1 ms. A positive value (+) indicates that audio is late with respect to the video (lagging). A negative value (-) indicates that the audio leads the video.
Lip-sync (last valid) 	Last valid measurement (in milliseconds)—latched when one of the sources is interrupted or else in an error condition if a lip-sync cannot be measured. Differently put, the data in this column reflects the last lip-sync value the system was able to measure.

Audio Video Fingerprint Analyzer—Configuration Tab



The **Configuration** tab of **Audio Video Fingerprint Analyzer** has two areas: **Fingerprint-generating devices** and **Fingerprint comparison setup**. All devices producing fingerprints that are discovered by iControl's Fingerprint Analyzer Service are listed in the **Fingerprint-generating devices** area. Each device's discovered input is listed under the device name with an icon to indicate a viable fingerprint ( ).

By contrast, what is currently configured is represented in the **Fingerprint comparison setup** area and listed by comparison group. Each comparison group shows its configured inputs (*Probed* and *Reference*) with either the viable fingerprint icon ( ) or else a caution icon ( ) to indicate the signal is no longer available.

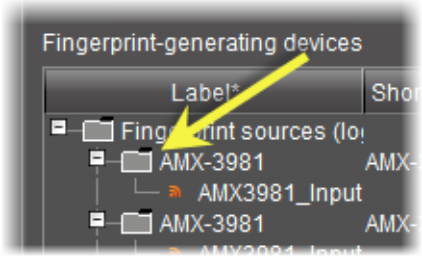
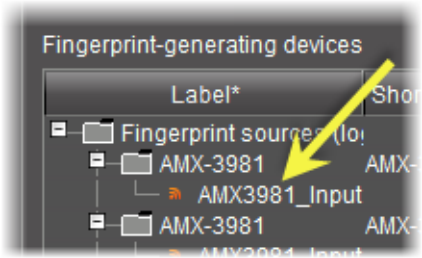
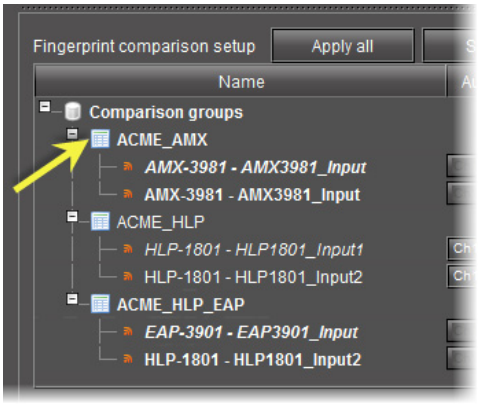
> **Note:** In the **Fingerprint comparison setup** area, the reference source label is indicated with italicized text.

The list of comparison groups allows you to select audio channels, and, at a glance, detect the following:

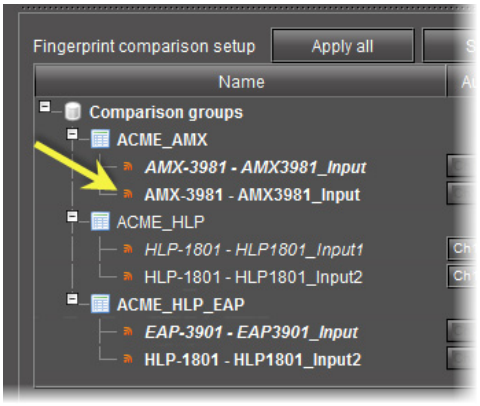
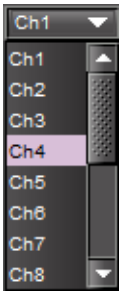
- whether a group's configuration data has been saved (it is **not** saved if there is an asterisk next to the comparison group name)
- whether a comparison is underway (a comparison **is** underway if the text of the comparison group and its inputs is bolded)

Several buttons at the top of the **Fingerprint comparison setup** area allow you to perform actions on all the listed comparison groups at once.

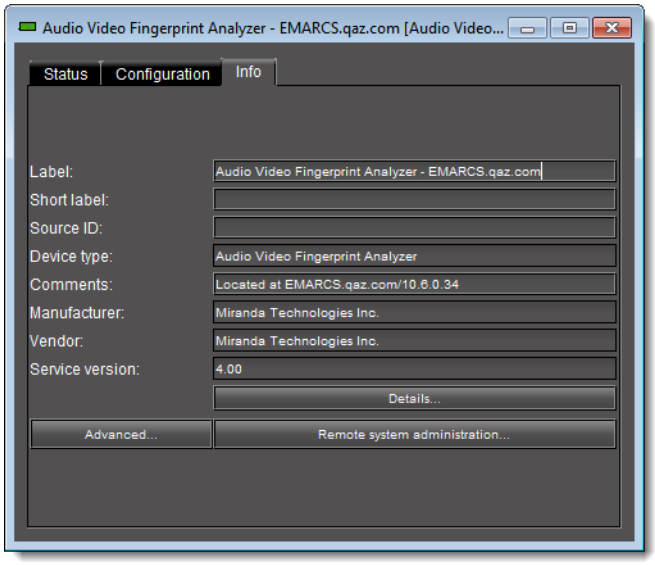
UI elements of the Configuration tab (Audio Video Fingerprint Analyzer)

UI Element	Description
--- ***Fingerprint-generating devices area*** ---	
Discovered device folder 	A folder representing the device whose input signal signals have been discovered by iControl's Fingerprint Analyzer Service.
Discovered input source 	A discovered signal from a supported device that produces a fingerprint. The viability of the signal is indicated by the viability icon ( ).
Refresh	Click to refresh the list of input sources visible to iControl's Fingerprint Analyzer Service.
--- ***Fingerprint comparison setup area*** ---	
Comparison group folder 	A folder representing the logical grouping of assigned sources, including probed sources as well as one reference source.

UI elements of the Configuration tab (Audio Video Fingerprint Analyzer) (*Continued*)

UI Element	Description
Assigned source 	An input source configured as belonging to a comparison group. An assigned source may be a probed source (one that is analyzed) or the reference source (one against which a probed source is compared). In addition, an assigned source may currently be a viable signal ( ) or a non-viable or absent signal ( ).
Channel lists 	Select channels from these lists.
Apply all	Click to save configuration changes to the comparison groups and their component inputs.
Start all	Click to begin all listed comparisons simultaneously.
Stop all	Click to stop all currently ongoing comparisons.
Alarm config	Click to open Fingerprint Analyzer's **Alarm Configuration** window.
Refresh	Click to refresh the list and statuses of the configured comparison groups and their component inputs.

Audio Video Fingerprint Analyzer—Info Tab

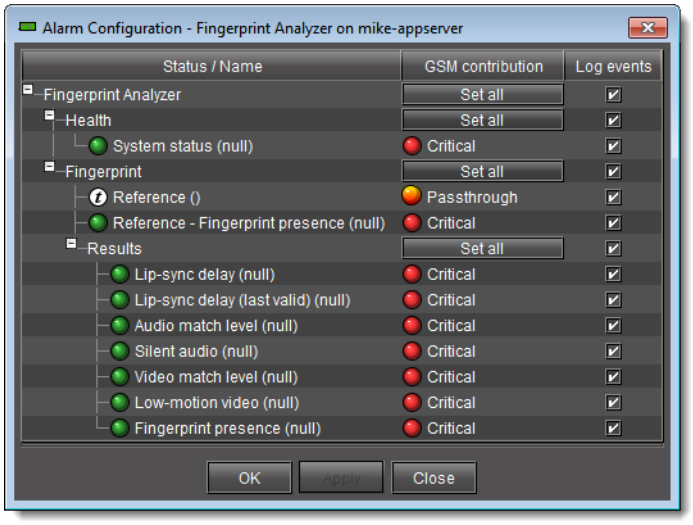


The **Info** tab of **Audio Video Fingerprint Analyzer** displays information about the Analyzer virtual device itself. The nature of the information is described in the following table:

UI elements of the Info tab (Audio Video Fingerprint Analyzer)

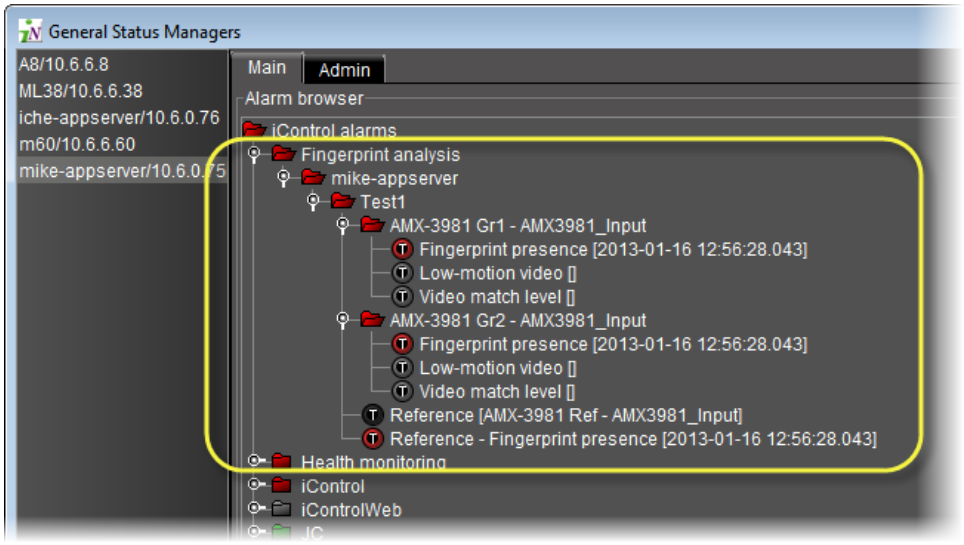
UI Element	Description
Label	*Human-friendly* description of this particular Fingerprint Analyzer virtual device.
Short label	A more compact version of the *Label* parameter
Source ID	*[Not a pertinent parameter for the Fingerprint Analyzer. You may disregard this value]*
Device type	The type of the virtual device. *[This is a read-only parameter which does not change value.]*
Comments	Descriptive text used to provide device-specific comments
Manufacturer	Name of the manufacturer
Vendor	Name of the vendor
Service version	Version of Fingerprint Analyzer
Details	Click to open a window displaying more details about Fingerprint Analyzer.
Advanced	Click to display the long ID of this Fingerprint Analyzer.
Remote system administration	*<Reserved for future use>*

Alarm Configuration Window



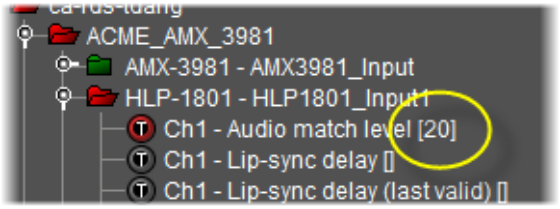
You can configure how the fingerprint analysis alarms are sent to the GSM and whether state changes are logged as events.

GSM Alarm Browser—Fingerprint Analysis Alarms



Fingerprint analysis alarms (circled) in the GSM Alarm Browser

When a comparison is underway, you can monitor the results of the comparison and analysis through the GSM's view of the fingerprint analysis alarms. How alarms are reported depends upon how you initially configured them in the **Alarm Configuration** window. The analysis results governing the statuses of individual alarms are shown as alarm text. In the example, the channel 1 audio match level is at 20%.



The *Fingerprint analysis* alarms are as follows:

Fingerprint analysis alarms

Alarm name	Relation	Applicability (based on comparison mode)			Alarm state	Description
		Lipsync detect	Video comp	Audio comp		
Audio match level	For each audio channel	**YES**	**NO**	**YES**	`Normal` Match is locked [*i.e.* Result is conclusive and match level is not below minimum threshold. Text shows match level.]	Audio match level for this channel.
					`Fault` Match is unlocked [*i.e.* Result is conclusive and match level is below minimum threshold. Text shows 0.]	
					`Unknown` Match cannot be determined. Check fingerprint presence.	
Audio delay[1]	For each audio channel	**YES**	**NO**	**YES**	`Normal` Match is locked and delay is not above the configured maximum threshold (default is no maximum). Text shows delay in ms.	Audio delay for this channel.
					`Fault` Match is locked and delay is above the configured maximum threshold (default is no maximum). Text shows delay in ms.	
					`Unknown` Delay cannot be determined due to match fault.	

Fingerprint analysis alarms (*Continued*)

Alarm name	Relation	Applicability (based on comparison mode)			Alarm state	Description
		Lipsync detect	Video comp	Audio comp		
Weak correlation for audio	For each audio channel	**YES**	**NO**	**YES**	`Normal` No weak correlation when comparing the Probe's ChX audio content with the Reference's.	Status of weak correlation for the compared channels.
					`Fault` Weak correlation when comparing the Probe's ChX audio content with the Reference's.	
					`Unknown` Weak correlation not applicable. Check fingerprint presence.	
Silent audio	For each audio channel	**YES**	**NO**	**YES**	`Normal` The audio content on the Probe's ChX is not completely silent.	Audio silence status for this channel on the Probe.
					`Fault` The audio content on the Probe's ChX is completely silent. Text shows fault's start time.	
					`Unknown` Silence cannot be determined on the Probe's ChX. Check fingerprint presence.	
Silent audio on reference	For each audio channel	**YES**	**NO**	**YES**	`Normal` The audio content on the respective Reference channel is not completely silent.	Audio silence status for the respective channel on the Reference.
					`Fault` The audio content on the respective Reference channel is completely silent. Text shows fault's start time.	
					`Unknown` Silence cannot be determined on the respective Reference channel. Check fingerprint presence.	

Fingerprint analysis alarms (*Continued*)

Alarm name	Relation	Applicability (based on comparison mode)			Alarm state	Description
		Lipsync detect	Video comp	Audio comp		
Lip-sync delay	For each audio channel	**YES**	**NO**	**NO**	`Normal` The lip-sync delay computed from video and audio delays is not above the maximum allowed. Text shows delay in ms.	Current lip-sync delay for this channel.
					`Fault` The lip-sync delay computed from video and audio delays is above the maximum allowed. Text shows delay in ms.	
					`Unknown` Lip-sync delay cannot be determined unless both match alarms are Normal.	
Lip-sync delay (last valid)	For each audio channel	**YES**	**NO**	**NO**	`Normal` The lip-sync delay computed from video and audio delays is not above the maximum allowed. Text shows delay in ms.	Last valid lip-sync delay for this channel.
					`Fault` The lip-sync delay computed from video and audio delays is above the maximum allowed. Text shows delay in ms.	
Video match level	For each probe input	**YES**	**YES**	**NO**	`Normal` Match is locked, i.e. result is conclusive and match level is not below minimum threshold (default is 50%). Text shows match level.	Video match level for this source.
					`Fault` Match is unlocked, i.e. result is conclusive and match level is below minimum threshold (default is 50%). Text shows 0.	
					`Unknown` Match cannot be determined. Check fingerprint presence.	

Fingerprint analysis alarms (*Continued*)

Alarm name	Relation	Applicability (based on comparison mode)			Alarm state	Description
		Lipsync detect	Video comp	Audio comp		
Video delay[1]	For each probe input	**YES**	**YES**	**NO**	`Normal` Match is locked and delay is not above the configured maximum threshold (default is no maximum). Text shows delay in ms.	Video delay for this source.
					`Fault` Match is locked and delay is above the configured maximum threshold (default is no maximum). Text shows delay in ms.	
					`Unknown` Delay cannot be determined due to match fault.	
Weak correlation for video	For each probe input	**YES**	**YES**	**NO**	`Normal` No weak correlation when comparing the Probe's video content with the Reference's.	Status of weak correlation for the compared video contents.
					`Fault` Weak correlation when comparing the Probe's video content with the Reference's. Text shows fault's start time.	
					`Unknown` Weak correlation not applicable. Check fingerprint presence.	
Low-motion video	For each probe input	**YES**	**YES**	**NO**	`Normal` The video content on the Probe is not completely in low motion.	Low motion video status for the Probe content.
					`Fault` The video content on the Probe is completely in low motion. Text shows fault's start time.	
					`Unknown` Low motion cannot be determined. Check fingerprint presence.	

Fingerprint analysis alarms (*Continued*)

Alarm name	Relation	Applicability (based on comparison mode)			Alarm state	Description
		Lipsync detect	Video comp	Audio comp		
Low-motion video on reference	For each probe input	**YES**	**YES**	**NO**	`Normal` The video content on the Reference is not completely in low motion.	Low motion video status for the Reference content.
					`Fault` The video content on the Reference is completely in low motion. Text shows fault's start time.	
					`Unknown` Low motion cannot be determined. Check fingerprint presence.	
Fingerprint presence	For each probe input	**YES**	**YES**	**YES**	`Normal` Fingerprints are received for the Probe input.	Status of the fingerprint presence on this probed input.
					`Fault` Fingerprints are still not received for the Probe input after at least 5 seconds. Text shows fault's start time.	
Reference - Fingerprint presence	For each group	**YES**	**YES**	**YES**	`Normal` Fingerprints are received for the Reference input.	Status of the fingerprint presence on this reference input.
					`Fault` Fingerprints are still not received for the Reference input after at least 5 seconds. Text shows fault's start time.	
Reference [<probed source in a comparison>]	For each group	**YES**	**YES**	**YES**	Text only. Shows the name of the Reference input.	Name of the reference input within this group.
System status[2]	For each server	**YES**	**YES**	**YES**	`Normal` The Fingerprint Analyzer is running and operational.	Status of the Fingerprint Analyzer service.
					`Fault` The Fingerprint Analyzer is not operational.	

Fingerprint analysis alarms (*Continued*)

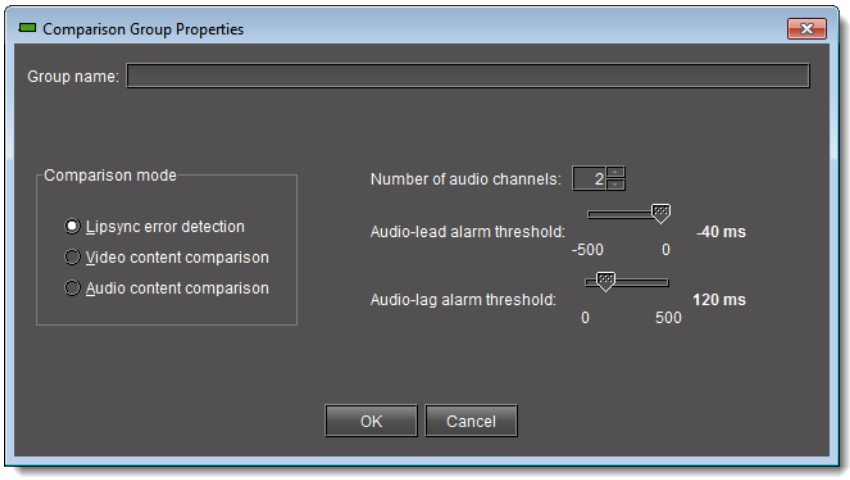
Alarm name	Relation	Applicability (based on comparison mode)			Alarm state	Description
		Lipsync detect	Video comp	Audio comp		
Fingerprint analysis configuration status[2]	For each server	**YES**	**YES**	**YES**	Always `Normal`. Text shows last modification time.	Status of the fingerprint analysis configuration data (update time, etc)

1. The "program delay" alarms (Audio delay and Video delay) are hidden by default because the delay values may not reflect the actual delays due to the lack of a centralized time source.
2. The **System status** and **Lip-sync configuration status** alarms are displayed under **Health monitoring/Fingerprint analyzer** in the alarm tree.

Note: An alarm in a comparison group remains in a *Disabled* state while the following two conditions are both true:

- a comparison operation is not in progress
- a first conclusive result has not yet been reached

Comparison Group Properties Window (Context: Creating or Editing a Comparison Group)



When first creating a comparison group or when viewing or modifying the properties of an existing one, the **Comparison Group Properties** window displays the group entity's properties.

UI elements of the Comparison Group Properties window

Context	UI element	Description
	Group name	User-defined name of the comparison group.

UI elements of the Comparison Group Properties window (*Continued*)

Context	UI element	Description
Comparison mode area	**Lipsync error detection**	Select to configure a comparison group for lipsync error detection.
	Video content comparison	Select to configure a comparison group for video comparison.
	Audio content comparison	Select to configure a comparison group for audio comparison.
Lipsync error detection mode selected	**Number of audio channels**	Number of audio channels to be analyzed for lip-sync delay in this comparison group (1-16).
	Audio-lead alarm threshold	Threshold for which the lip-sync delay is considered normal or not-in-error. The lead threshold represents audio leading video at the probed point.
	Audio-lag alarm threshold	Threshold for which the lip-sync delay is considered normal or not-in-error. The lag threshold is for audio lagging the video at the probed point.
Audio content comparison mode selected	**Number of audio channels**	Number of audio channels in each input source.

Sample Workflows

[Workflow]: Initial Setup—Administrator

iControl allows you to configure settings for the fingerprint analysis feature. This feature relies upon the generation of signal fingerprints by supported Densité cards. A probed or referenced Densité card's service subsequently sends the fingerprint to interested system entities.

IMPORTANT: Who performs these tasks?

This section contains procedures typically performed by an administrator. These procedures are generally configuration tasks that must be completed before an operator can begin a fingerprint comparison (see the sample configuration workflow, below). However, several configuration tasks are possible during and after the operator performs a comparison.

IMPORTANT: Maximum recommended number of fingerprint channels

Make sure your system does not exceed the maximum recommended number of fingerprint channels according to your hardware specifications (see Maximum recommended fingerprint channels, on page 532).

See also

For more information about fingerprint comparison and analysis, see page 531.

A sample workflow of initial configuration tasks is as follows:

Sample workflow: Initial configuration tasks

1.	Enable the Audio/Video Fingerprint Analyzer Service on your Application Server (see Starting & Stopping iControl Services, on page 678).
2.	Open **Audio Video Fingerprint Analyzer** (see page 715).
3.	Configure Fingerprint Analyzer Service alarms according to your individual needs (see page 552).
4.	Create a comparison group of input sources, including a reference source (see page 553).
5.	Assign all desired input sources (including the reference source) to your comparison group (see page 556).
6.	Designate one of the assigned sources as the *Reference* (see Configuring a Source as the Reference Source in a Comparison Group, on page 560).
7.	Configure each assigned source's channel assignments, as required (see Changing a Source's Channel Assignments, on page 562).

[Workflow]: On-Going Operations—Operator

iControl allows you to initiate a comparison between signals of probed sources and one from the reference source, as well as monitor and analyze comparison data. This feature relies upon the generation of signal fingerprints by supported Densité cards. A probed or referenced Densité card's service subsequently sends the fingerprint to interested system entities.

IMPORTANT: Who performs these tasks?

This section contains procedures typically performed by an operator. Before beginning these procedures, the initial configuration tasks must be completed—typically done by an administrator (see Configuring Fingerprint Analysis through iControl, on page 552).

IMPORTANT: Maximum recommended number of fingerprint channels

Make sure your system does not exceed the maximum recommended number of fingerprint channels according to your hardware specifications (see Maximum recommended fingerprint channels, on page 532).

See also

For more information about fingerprint comparison and analysis, including an overall workflow, see page 531.

A sample monitoring and analysis workflow is as follows:

Sample workflow: Monitoring and analysis tasks

1.	Start a fingerprint comparison for your comparison group (see page 566).
2.	Monitor fingerprint comparison data in real-time (see page 567).
3.	If desired, and when the required amount of time has passed, stop the fingerprint comparison (see page 567).

Detailed Directions

Configuring Fingerprint Analysis through iControl

Configuring Fingerprint Analyzer Service Alarms

The Fingerprint Analysis feature uses alarms to communicate comparison data to a user in real-time. You can configure the following parameters of Fingerprint Analyzer Service alarms:

- Alarm severity sent to the GSM (GSM contribution)
- Whether to log events

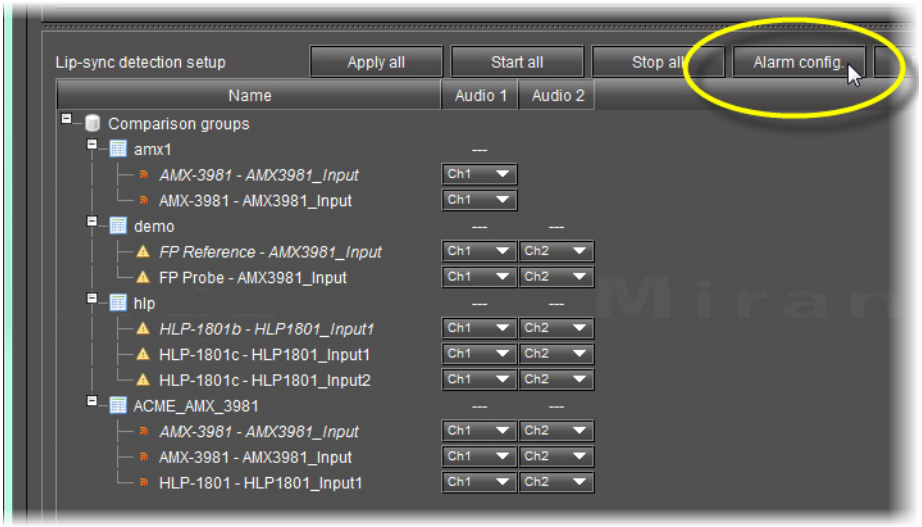
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

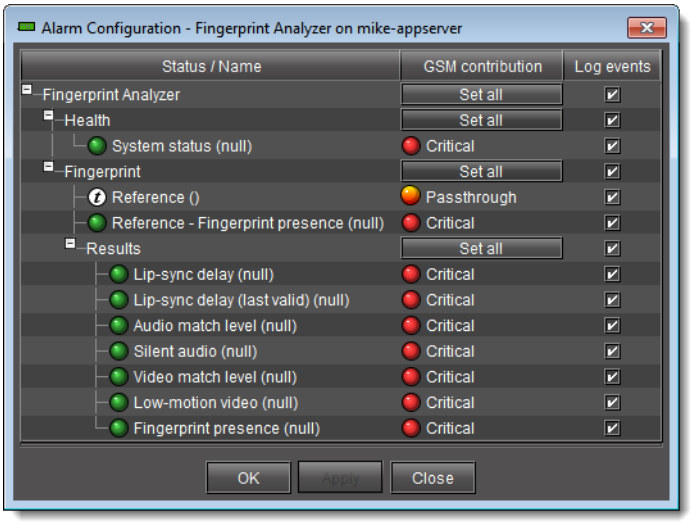
- You have opened **Audio Video Fingerprint Analyzer** (see page 715).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see Sample Workflows, on page 550).

To configure Service alarms

1. On the **Configuration** tab, in the **Fingerprint comparison setup** area, click **Alarm config**.



SYSTEM RESPONSE: The **Alarm Configuration** window appears.



2. Configure the GSM contribution and enable or disable event logging as required.
3. Click **OK**.

Creating a New Comparison Group

Create a new comparison group if you would like to initiate a lip-sync or motion detection comparison between the reference source and another probed source.

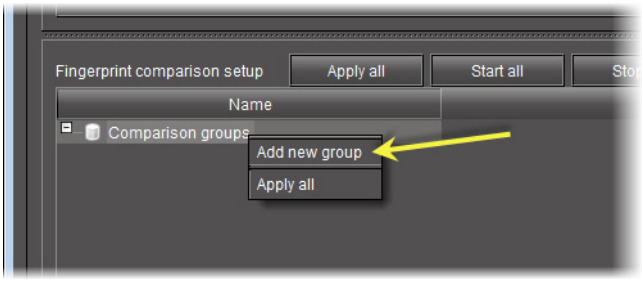
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **Audio Video Fingerprint Analyzer** (see page 715).
- **[RECOMMENDED]:** You are performing this procedure as a task within the context of an approved workflow (see Sample Workflows, on page 550).

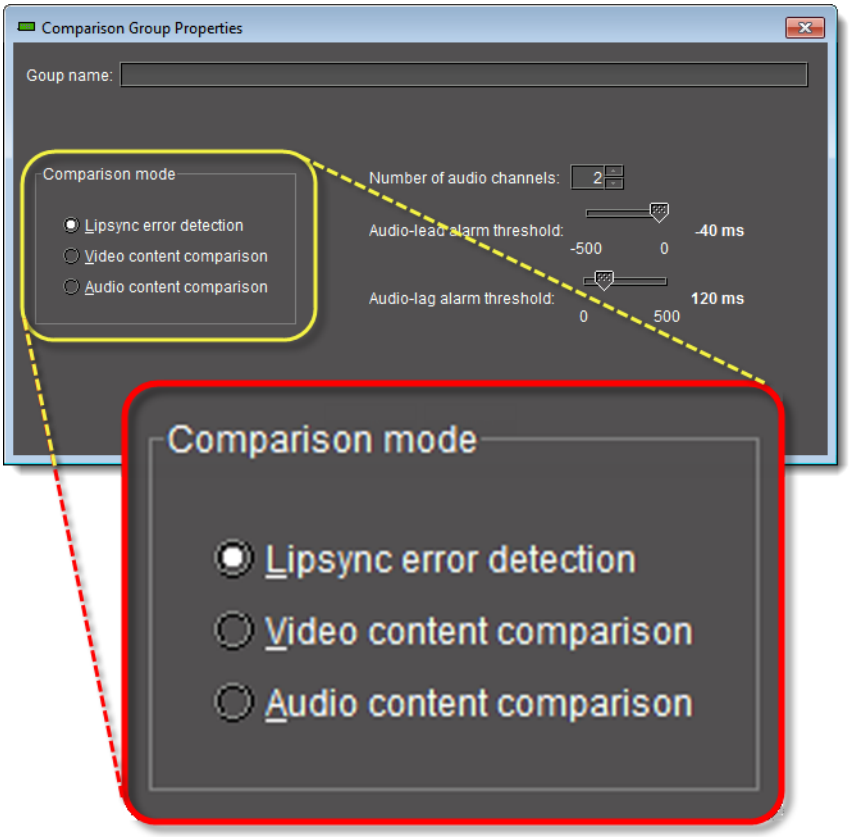
To create a new comparison group

1. On the Configuration tab, in the **Fingerprint comparison setup** area, right-click **Comparison groups**, and then click **Add new group**.



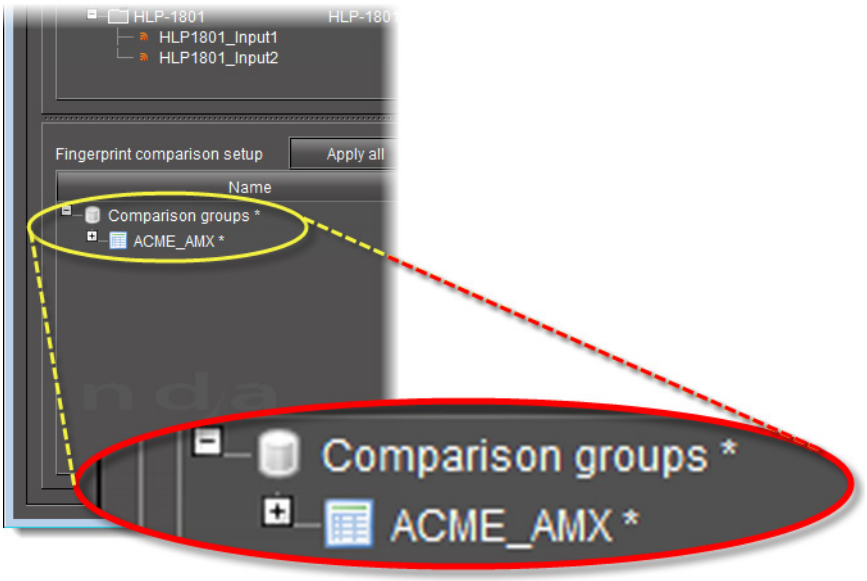
SYSTEM RESPONSE: The **Comparison group properties** window appears.

2. In the **Group name** box, type the name you would like to give to your new comparison group.
3. Select a comparison mode.



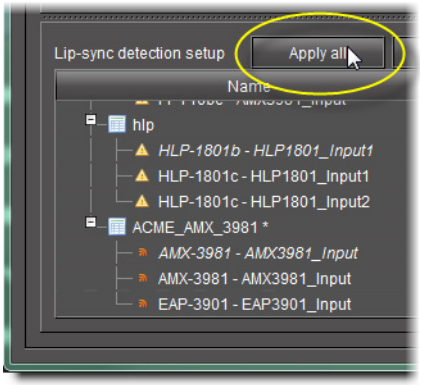
4. Adjust the comparison group properties as required, and then click **OK**.

   SYSTEM RESPONSE: In **Audio Video Fingerprint Analyzer**, the new comparison group appears in the **Fingerprint comparison setup** area.



Note: Your new comparison group does not yet exist as a configured entity until you assign at least two sources to it and then click **Apply all**. A comparison group that has not yet been accepted by the system as a configured entity appears with an asterisk (*) beside its name.

5. Assign at least two sources to the new comparison group (see Assigning Sources to a Comparison Group, on page 556).
6. Click **Apply all**.



System Response: The asterisk following the name of the new comparison group in the **Fingerprint comparison setup** area disappears, indicating the group is configured.

7. Make sure your desired reference source is configured as the reference (see Configuring a Source as the Reference Source in a Comparison Group, on page 560).

Assigning Sources to a Comparison Group

Assign sources to a comparison group when you would like to increase the number of probed sources in a comparison.

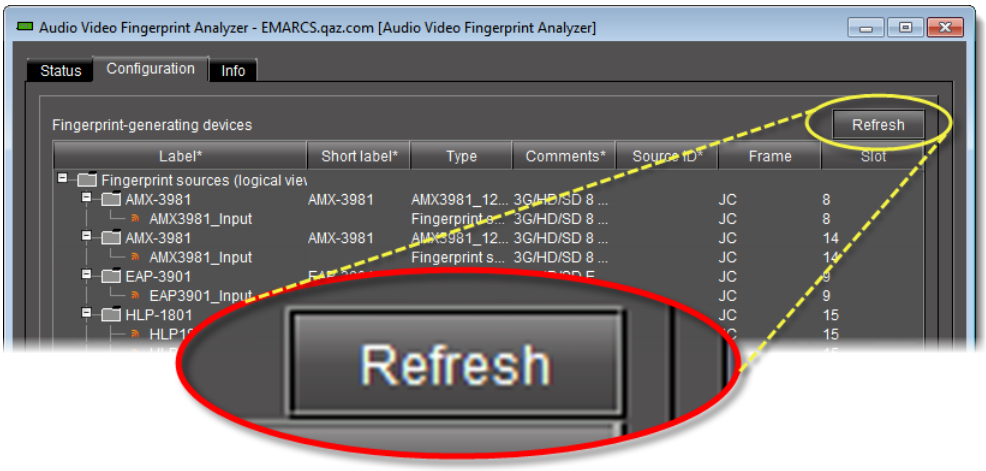
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **Audio Video Fingerprint Analyzer** (see page 715).
- There are currently no comparisons underway for the comparison group you would like to edit.
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see Sample Workflows, on page 550).

To assign a source to a comparison group

1. On the **Configuration** tab, in the **Fingerprint-generating devices** area, click **Refresh** to update the list of available devices.

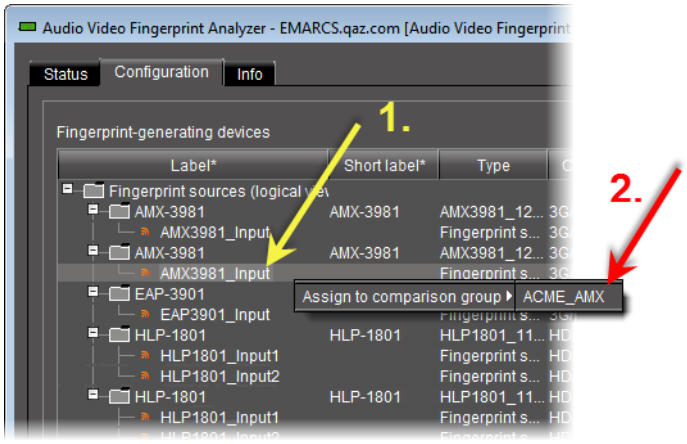


SYSTEM RESPONSE: The list of available fingerprint-generating devices refreshes.

2. If the folders representing the source cards are not expanded, expand them (by clicking the appropriate *plus* (⊞) symbols) in order to display the individual sources.
3. To assign a single source (at a time) to a comparison group, do **one** of the following:
   - Click once on a source to select it, and then click, hold, and drag the source to the desired comparison group in the **Fingerprint comparison setup** area.

OR,

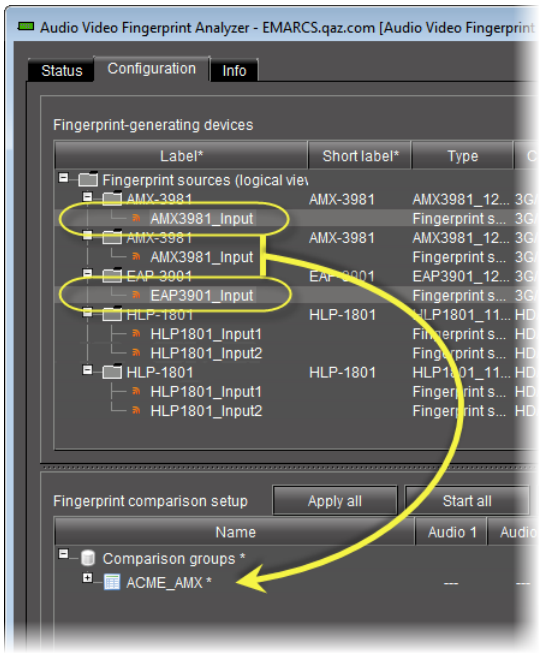
- Right-click once on a source, point to **Add to comparison group**, and then click the name representing the comparison group to which you would like to assign this source.



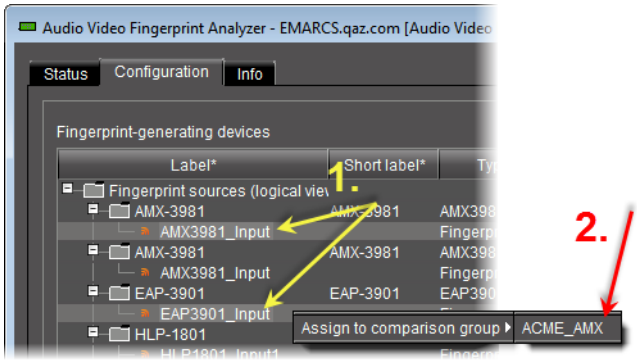
SYSTEM RESPONSE: The source appears under the comparison group in the **Fingerprint comparison setup** area.

SYSTEM RESPONSE: An asterisk (*) appears next to the comparison group, indicating changes have been made that have not yet been saved.

4. To assign non-consecutive (as listed in the **Fingerprint-generating devices** area), multiple sources to a comparison group, do **one** of the following:
   - Click once on a source to select it, **Ctrl**-**<click>** each additional source you would like to add, and then click and hold any of the selected sources and drag the entire selection to the desired comparison group in the **Fingerprint comparison setup** area.



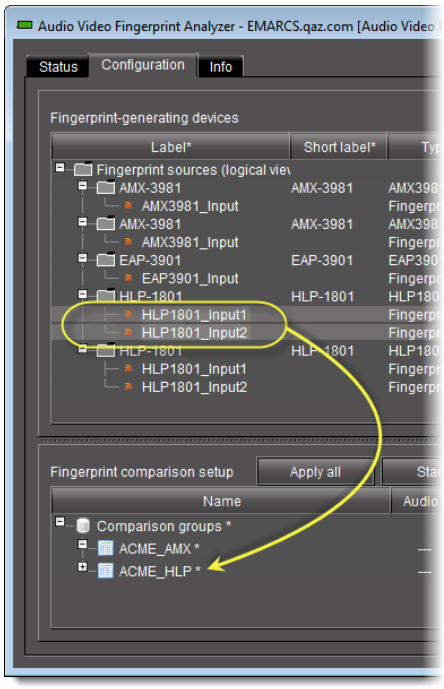
- Click once on a source to select it, **Ctrl**-**<click>** each additional source you would like to add, right-click any of the selected sources, point to **Add to comparison group**, and then click the name representing the comparison group to which you would like to assign this selection of sources.



System Response: The sources appear under the comparison group in the **Fingerprint comparison setup** area.

System Response: An asterisk (*) appears next to the comparison group, indicating changes have been made that have not yet been saved.

5. To assign consecutive (as listed in the **Fingerprint-generating devices** area) multiple sources to a comparison group, do **one** of the following:
   - Click once on the top-most source you would like to add to the comparison group, **Shift**-**<click>** the bottom-most source you would like to add, and then click and hold any of the selected sources and drag the entire selection to the desired comparison group in the **Fingerprint comparison setup** area.

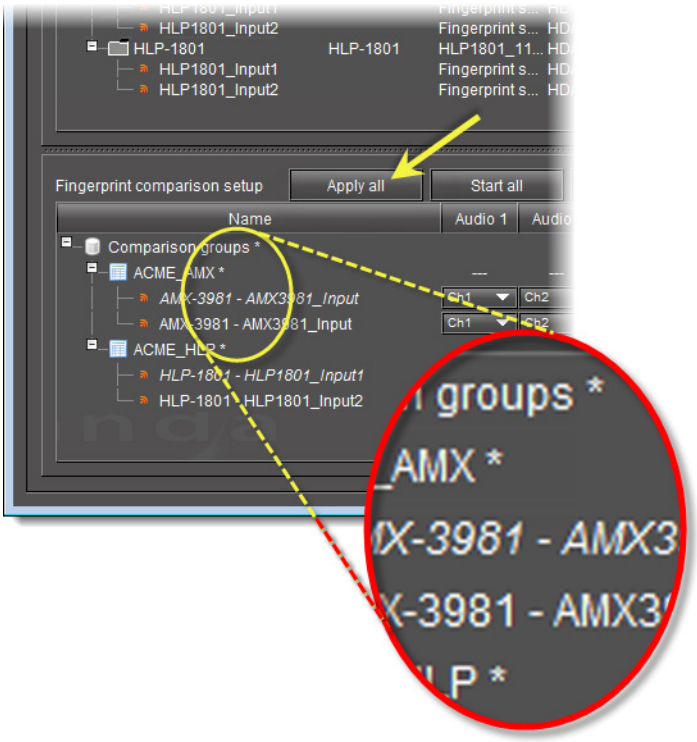


- Click once on the top-most source you would like to add to the comparison group, **Shift**-**<click>** the bottom-most source you would like to add, right-click somewhere in the selection, point to **Add to comparison group**, and then click the name representing the comparison group to which you would like to assign this selection of sources.

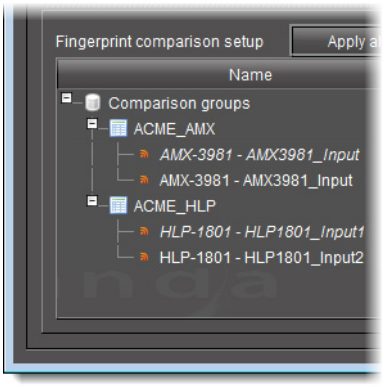
SYSTEM RESPONSE: The sources appear under the comparison group in the **Fingerprint comparison setup** area.

SYSTEM RESPONSE: An asterisk (*) appears next to the comparison group, indicating changes have been made that have not yet been saved.

6. Configure the desired audio channels on the new source as required (see Changing a Source's Channel Assignments, on page 562).
7. Click **Apply all** to save comparison group changes.



SYSTEM RESPONSE: The asterisk (*) next to the comparison group name disappears, indicating the change to the comparison group configuration is saved.



Configuring a Source as the Reference Source in a Comparison Group

IMPORTANT: The reference source you select should come from a point in the signal path where the fingerprint is known to be acceptable. In addition, the reference source should be upstream of the probed source(s) in the signal path.

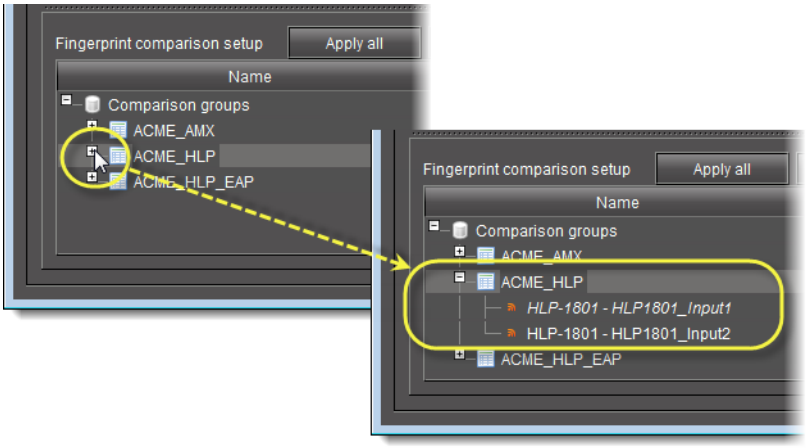
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

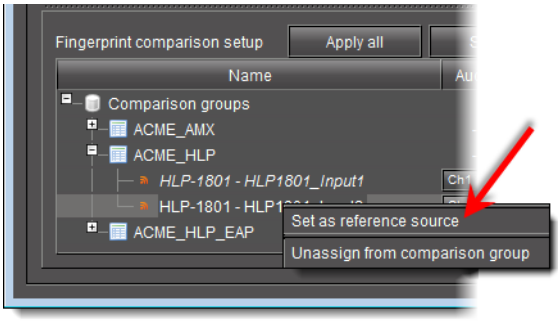
- You have opened **Audio Video Fingerprint Analyzer** (see page 715).
- There are currently no comparisons underway for the comparison group you would like to edit.
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see Sample Workflows, on page 550).

To configure a source as the reference source in a comparison group

1. On the **Configuration** tab, in the **Fingerprint comparison setup** area, expand the comparison group folder representing the group whose source you would like to configure as the reference.



2. Right-click the source you would like to configure as the reference, and then click **Set as reference source**.



SYSTEM RESPONSE: The desired new reference source's name becomes italicized and the former reference source's name is no longer italicized.

Note: An italicized source name indicates a source is configured as the reference.

System Response: An asterisk (*) appears next to the name of the comparison group indicating pending changes.

3. Click **Apply all** to save changes to the comparison group.

   System Response: The asterisk next to the comparison group name disappears indicating all changes are now saved and saved to the group.

Changing a Source's Channel Assignments

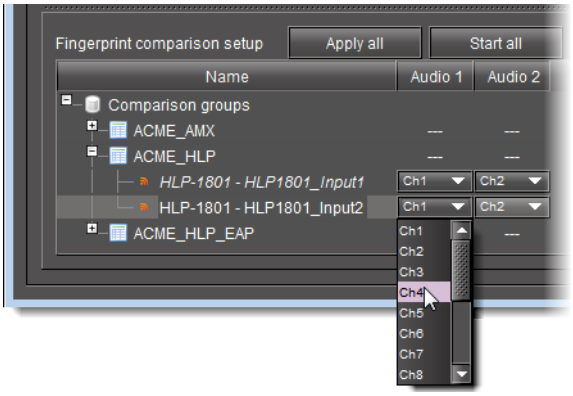
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **Audio Video Fingerprint Analyzer** (see page 715).
- There are currently no comparisons underway for the comparison group you would like to edit.
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see Sample Workflows, on page 550).

To change a source's channel assignments

1. On the **Configuration** tab, in the **Fingerprint comparison setup** area, expand the comparison group folder representing the group whose source's channels you would like to configure.
2. In the **Audio 1** channel list of the source whose configuration you are changing, select the desired channel.



3. Perform step 2 for all visible Audio channel list for this source (e.g., **Audio 2** list and **Audio 3** list).
4. Click **Apply all** to save all changes to the comparison group.

   System Response: The asterisk next to the comparison group disappears.

Miscellaneous Fingerprint Comparison Configuration Tasks

Editing a Comparison Group's Properties

Edit a comparison group's properties when you would like to change any of the following settings of an existing comparison group:

- Name (of the comparison group)

- Number of audio channels
- Audio-lead alarm threshold (time in milliseconds)
- Audio-lag alarm threshold (time in milliseconds)

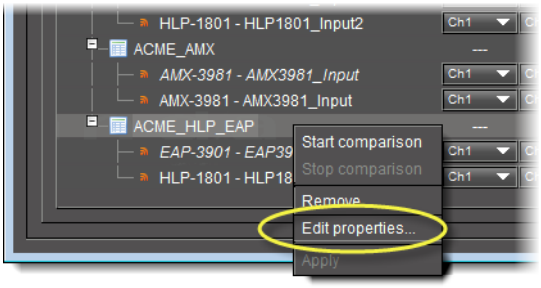
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

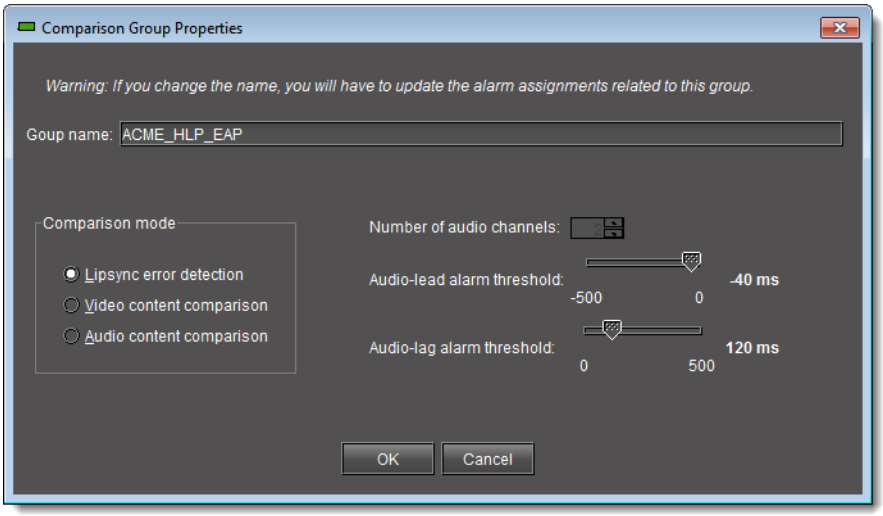
- You have opened **Audio Video Fingerprint Analyzer** (see page 715).
- There are currently no comparisons underway for the comparison group you would like to edit.

To edit a comparison group's properties

1. On the **Configuration** tab, in the **Fingerprint comparison setup** area, right-click the comparison group whose properties you would like to edit, and then click **Edit properties**.



SYSTEM RESPONSE: The **Comparison group properties** window appears.

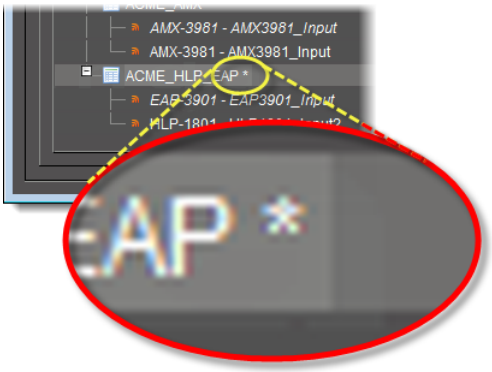


Note: When editing the properties of an existing comparison group, the **Comparison group properties** window does not allow you to alter the number of audio channels configured for the group. This parameter may only be set when the group is initially configured.

2. Edit the comparison group properties as required, and then click **OK**.

   IMPORTANT: If you change the name of your comparison group, make sure you also update the alarm assignments to the group.

   SYSTEM RESPONSE: The **Comparison group properties** window disappears and an asterisk (*) appears beside the name of this group in the **Fingerprint comparison setup** area of **Audio Video Fingerprint Analyzer**.



3. Click **Apply all** to save configuration changes to the comparison group.

   SYSTEM RESPONSE: The asterisk following the name of your comparison group disappears, indicating the configuration changes have been saved.

Unassigning Sources from a Comparison Group

Unassign sources from a comparison group to remove one or more probed sources being compared.

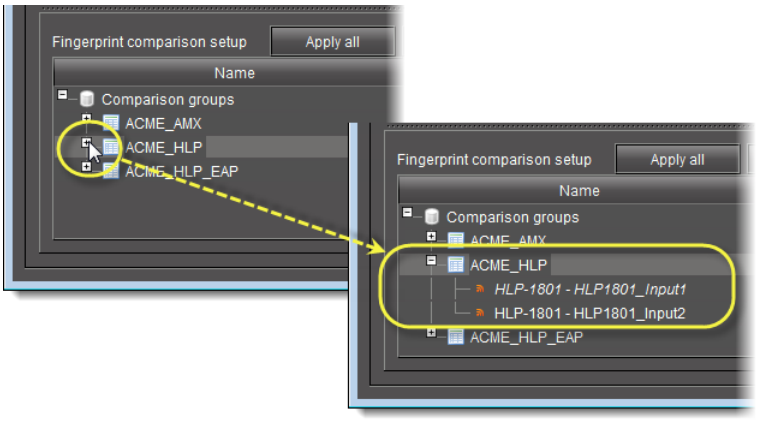
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **Audio Video Fingerprint Analyzer** (see page 715).
- There are currently no comparisons underway for the comparison group you would like to edit.

To unassign a source from a comparison group

1. On the **Configuration** tab, in the **Fingerprint comparison setup** area, expand the comparison group folder representing the group the source you would like to remove belongs to.



2. Right-click the source you would like to remove, and then click **Remove**.

> **Note:** If the **Remove** option is unavailable (grayed out), there is most likely a comparison underway. Stop the current comparison before continuing (see Stopping a Fingerprint Comparison, on page 567).

3. Click **Apply all** to save the change to the comparison group.

   System Response: The asterisk (*) next to the comparison group name disappears, indicating the change to the comparison group configuration is saved.

Deleting a Comparison Group

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened **Audio Video Fingerprint Analyzer** (see page 715).
- There are currently no comparisons underway for the comparison group you would like to delete (see Stopping a Fingerprint Comparison, on page 567 to stop a comparison).

To delete a comparison group

1. On the **Configuration** tab, in the **Fingerprint comparison setup** area, expand the comparison group folder representing the group the source you would like to remove belongs to.
2. Right-click the source you would like to remove, and then click **Remove**.

> **Note:** If the **Remove** option is unavailable (grayed out), there is most likely a comparison underway. Stop the current comparison before continuing (see Stopping a Fingerprint Comparison, on page 567).

3. Click **Apply all** to save the change to the comparison group.

   System Response: The asterisk (*) next to the comparison group name disappears, indicating the change to the comparison group configuration is saved.

Monitoring and Analyzing Comparison Data

Starting a Fingerprint Comparison

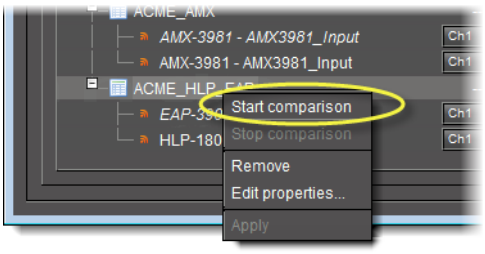
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

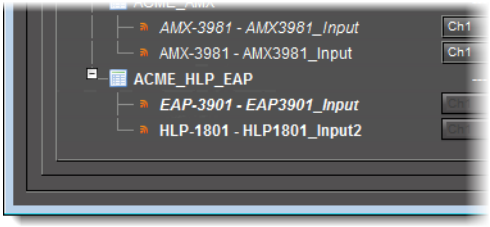
- You have opened **Audio Video Fingerprint Analyzer** (see page 715).
- You can see all of your comparison group's sources in the group folder.
- There is no asterisk (*) next to the name of your comparison group.
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see Sample Workflows, on page 550).

To start a lip-sync comparison

1. On the **Configuration** tab, in the **Fingerprint comparison setup** area, identify the comparison group on which you would like to perform a fingerprint comparison.
2. Right-click the comparison group and then click **Start comparison**.



SYSTEM RESPONSE: The names of the comparison group and its sources become bolded, indicating that a comparison is underway.



Note: The Audio channel lists for sources being compared are not editable during a comparison.

Stopping a Fingerprint Comparison

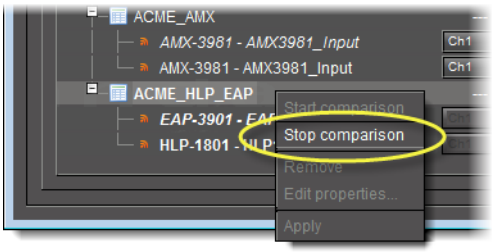
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- you have opened **Audio Video Fingerprint Analyzer** (see page 715).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see Sample Workflows, on page 550).

To stop a fingerprint comparison

1. On the **Configuration** tab, in the **Fingerprint comparison setup** area, identify the group whose comparison you would like to stop.
2. Right-click the comparison group and then click **Stop comparison**.



System Response: The names of the comparison group and its sources are no longer bolded, indicating that the comparison has ended.

Monitoring Fingerprint Comparison Data

Once a lip-sync or motion detection comparison has been initiated, you can monitor the analysis results in real-time, either as status alarms in the GSM Alarm Browser or on the **Status** tab of **Audio Video Fingerprint Analyzer**. You can also view events in **Event Log Viewer**:

Note: If the signal format changes on any of the compared cards during a comparison, there may be a delay of 15 to 20 seconds before comparison data resume updating. This applies to status updates on both the GSM Alarm Browser and **Audio Video Fingerprint Analyzer**.

Monitoring Comparison Data with Audio Video Fingerprint Analyzer

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- Your comparison group already exists and is configured (see Creating a New Comparison Group, on page 553).

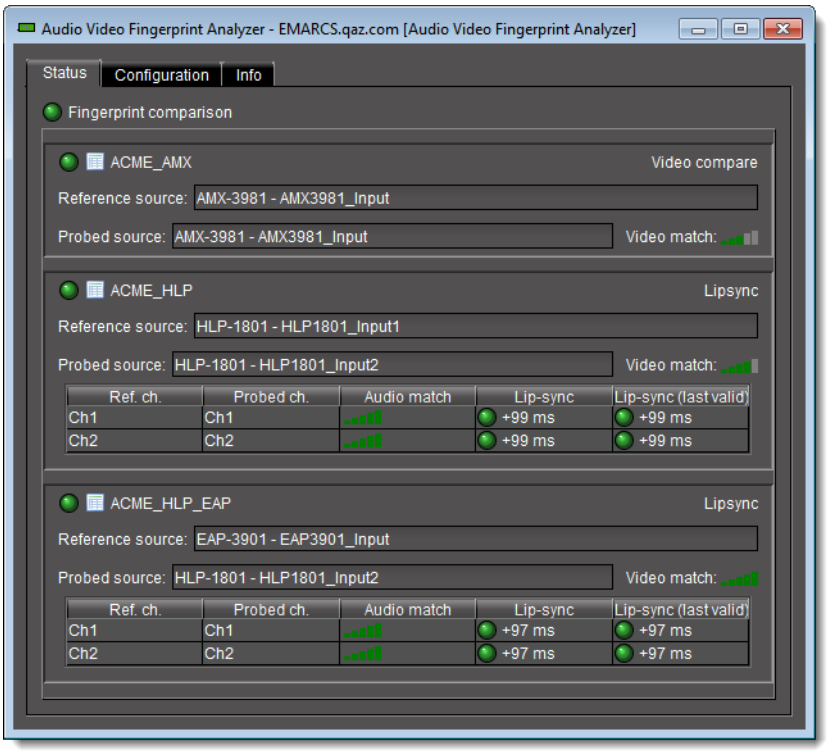
REQUIREMENTS (*Continued*)

Make sure you meet the following conditions before beginning this procedure:

- You have initiated a comparison between the reference source and one or more probed sources (see Starting a Fingerprint Comparison, on page 566).
- You have opened **Audio Video Fingerprint Analyzer** (see page 715).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see Sample Workflows, on page 550).

To monitor comparison data with Audio Video Fingerprint Analyzer

1. In **Audio Video Fingerprint Analyzer**, click on the **Status** tab.
2. Use the vertical scroll bar (if there is one) to scroll down to the area corresponding to the comparison group whose data you would like to view.



See also

For more information about the **Status** tab of **Audio Video Fingerprint Analyzer**, see Audio Video Fingerprint Analyzer—Status Tab, on page 534.

Monitoring Comparison Data in the GSM Alarm Browser

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

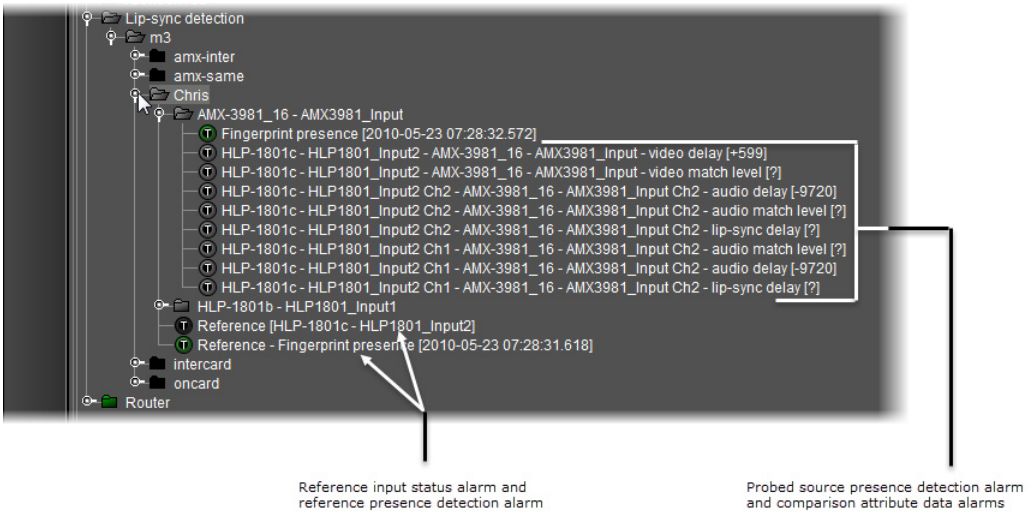
- Your comparison group already exists and is configured (see Creating a New Comparison Group, on page 553).
- You have initiated a comparison between the reference source and one or more probed sources (see Starting a Fingerprint Comparison, on page 566).
- You have opened the GSM Alarm Browser (see Opening the GSM Alarm Browser, on page 710).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see Sample Workflows, on page 550).

To monitor comparison data in the GSM Alarm Browser

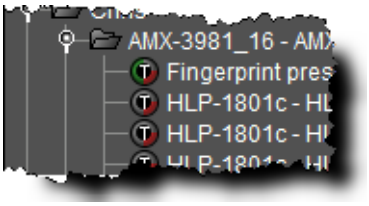
- On the **Main** tab of the GSM Alarm Browser, expand the **Lip-sync detection** folder and the sub-folders representing your comparison group and probed inputs.

  SYSTEM RESPONSE: The comparison attributes are displayed as alarms under a folder representing each respective probed input.

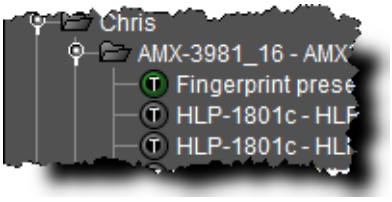
  Note: Reference input status and reference presence detection are displayed as two alarms, respectively, at the same level as the probed input folder:



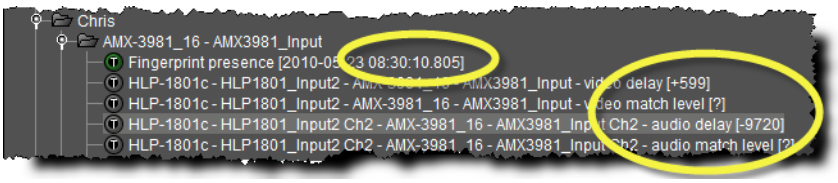
SYSTEM RESPONSE: When the comparison is underway, the alarm component icons are updated in real-time in the GSM Alarm Browser alarm to indicate the status (as well as latched status and acknowledged status, if you have selected the **Show status details** check box).



Alarm component icons showing status details



SYSTEM RESPONSE: The comparison data appears and is updated in real-time in the GSM Alarm Browser window as well as individual **Alarm Properties** windows.



Real-time comparison data in the GSM Alarm Browser window

See also

For more information about alarm component status details, see Alarm Components, on page 348.

Troubleshooting procedures for Fingerprint Analysis

Scenario 1

[PROBLEM]—Fingerprint devices are displayed but the fingerprint sources are grayed out.

[SOLUTION]—Devices are visible to iC Navigator (client-side), but they are **NOT** visible to the *Fingerprint Analyzer* service (server-side), which is probably in a different subnet. To resolve this, you must configure the service locations so that those devices are visible to the *Fingerprint Analyzer* service.

1. Open the *Startup* page of the Application Server on which the Fingerprint Analyzer is hosted, and navigate to the *iControl admin* page.
2. Open the *Lookup locations* page by using the link under the **iControl services** section.
3. Add the lookup service where the fingerprint generating devices are registered by entering the IP address and optionally a name.
4. Restart the *Fingerprint Analyzer* service using the *Service Management* page.

5. Go back to iC Navigator, open the *Fingerprint Analyzer* control panel and click **Refresh** in the upper panel.

Scenario 2

[PROBLEM]—The match alarms are green when the two input sources are identical. However, they still remain green a long time after one of the sources has changed to a different content.

[SOLUTION]—Make sure the silence, low-motion, and weak correlation alarms for those respective sources are not currently red. Due to the way the fingerprints are generated, silence and still images are not currently supported for comparison. In addition, some contents are more difficult for the Fingerprint Analyzer to compare one with the other. Examples of such contents are: end-of-program credits, repetitive tones (weather summaries), talking heads, etc. In that case, the *weak correlation* alarms should indicate that the current contents cannot be produce conclusive results, which will come when the contents change to something that can be compared conclusively.

1. In iC Navigator, open the GSM control panel and select the **Main** tab.
2. Expand the *Fingerprint analysis* branch of the alarm tree until you reach the folder associated with the comparison group.
3. Check the status of the alarms listed above.

10 Backup and Redundancy

Summary

Key Concepts

Application Server Auto-failovers and Manual Takeovers

Application Servers actively working in the iControl system are known as *Main* Application Servers. Application Servers on which copies of configuration data from the Main Application Servers reside are known as *Backup* Application Servers. If one of the Main Application Servers fails, an operator can manually switch service to a Backup Application Server, or else the system can automatically fail over to a Backup Application Server if configured to do so.

A necessary condition for a successful Auto-failover or Manual Takeover is for the Main Application Server's iControl software and Web sites, configuration data, and IP address configuration data to be replicated and up-to-date on the Backup Application Server. *Replication* is the automatic scheduled copying of Application Servers on the network. Configuration of the replication function is done through *iControl admin*. After a failover, the Backup Application Server assumes the exact same configuration profile as the original Main at the time of its last replication (that is, operational status, IP addresses, configuration data are identical to the replication *snapshot*).

Redundancy Groups

Only when Application Servers are configured to belong to a *Redundancy Group* can Auto-failovers and Manual Takeovers occur. A Redundancy Group defines the pool of Application Servers in the role of Main, and the one Application Server serving as standby in the role of Backup (protecting the Mains). Operators can choose to perform Manual Takeovers (from any online Main to the standby Backup) and Reverse Takeovers.

> **IMPORTANT: System behavior**
>
> You must configure one Application Server in every Redundancy Group in the role of Backup and in a standby state in order for Auto-failovers and Manual Takeovers to succeed.

Manual Takeovers

Manual Takeovers have an **n+1** redundancy scheme. That is, iControl doesn't limit the number of *Main* Application Servers. iControl limits the number of Application Servers acting in a

Backup capacity to one within a single Redundancy Group. If more than one Backup server is required, they should be put into separate N+1 Redundancy Groups.

For example, consider two Main (online) Application Servers plus one Backup Application Server. The Backup is in a standby state and doesn't run any processes used in normal operation. To address the GSM as a single point-of-failure problem or GSM load balancing, we may want to run two GSMs. GSM duties are thus load-balanced between the two Mains. When an operator initiates a Manual Takeover from one of the Mains to the Backup, that portion of the GSM duties being handled by the taken-over Main is switched to the Backup along with all other services of this Application Server and its identity.

The Backup Application Server replicates the configuration data and identities of the **n** Application Servers. The default replication frequency is every 24 hours. This means that in the case of an Application Server failure, any changes performed to the Application Server profile in the previous 24 hours could be lost.

See also

For more information about:

- Manual Takeovers, see Configuring and Managing Application Server Redundancy, on page 584.
- Redundancy Groups, see page 573.

Auto-failovers

Auto-failovers have an **n+1** redundancy scheme. That is, iControl doesn't limit the number of *Main* Application Servers. However, iControl does limit the number of Application Servers acting in a Backup capacity to only one. When two or more Application Servers are configured as a *Redundancy Group* on the *Redundancy configuration* page, any one of several conditions can trigger an Auto-failover of service from a *Main* Application Server to the *Backup* Application Server. In such cases, the Backup assumes the full role and identity of the original (including its IP address if the **Take over the main IP address after failover** check box is selected), and becomes the new *Main*. This process does not require user intervention except in the initial Redundancy Group configuration and when performing failover recovery tasks such as Reverse Takeovers or Replace operations.

IMPORTANT: If you configure your Redundancy Group **NOT** to take over the *Main*'s IP address upon failover or takeover, make sure you keep the *Backup* Application Server's IP address configured in **System tools** | **Edit service locations** | **Service and alarm discovery** on all Application Servers that belong to the Redundancy Group.

In a Redundancy Group topology configured for Auto-failover, there may be multiple *Main* Application Servers but only one *Backup* in an **n+1** redundancy scheme.

To enable the Auto-failover feature, you must first configure your Redundancy Group on the *Redundancy configuration* page and manually enable Auto-failover on one or more *Main* Application Servers.

The *Backup* Application Server monitors the health of the *Main* Application Server and its connection to devices and the network, through the use of a *heartbeat* trigger. As long as both of the following conditions are met, no Auto-failover will occur:

- There is a heartbeat from the *Main* to the *Backup*.
- The *Main* can communicate with other devices (besides the *Backup* Application Server) over its **eth0** interface.

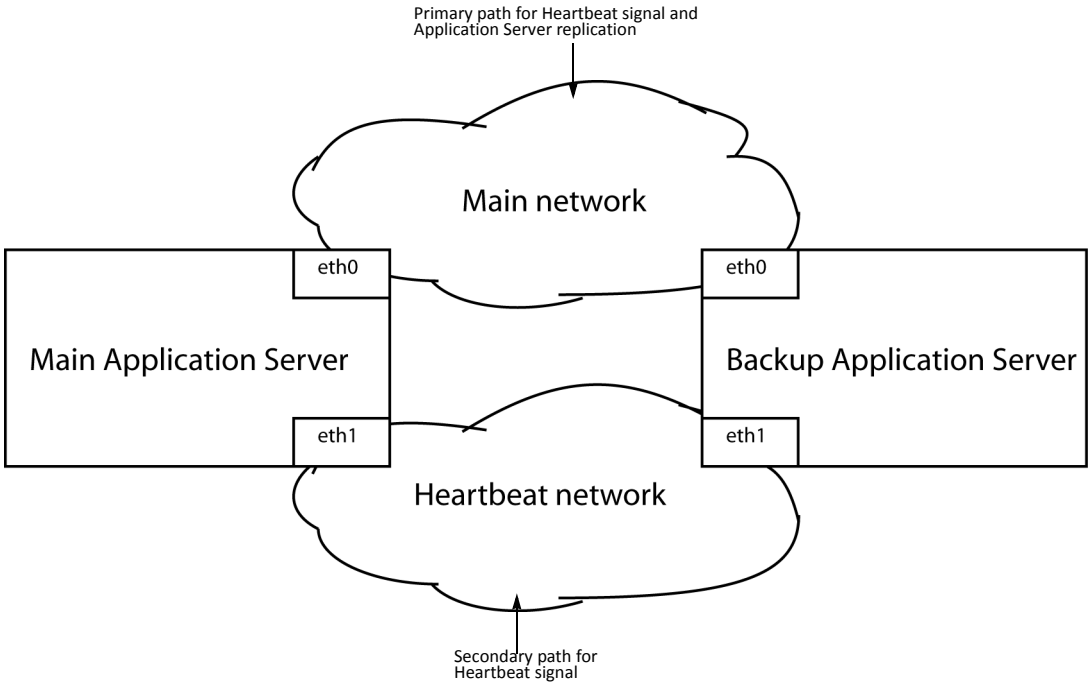
IMPORTANT: Ethernet Port Label Considerations

Please read the section regarding Ethernet port labels (see Ethernet Port Labels on Dell PowerEdge Application Servers, on page 48).

The heartbeat is carried on a *Main network cable* which connects all *Main* Application Servers in a Redundancy Group to the *Backup* Application Server.

The heartbeat cabling between the *Main* and the *Backup* has two cable paths: the Main network and the Heartbeat network. The *Backup* Application Server uses the Main network but switches to using the Heartbeat network if the Main network is unresponsive.

IMPORTANT: The Heartbeat network and the Main network use cables and equipment that are distinct from one another to avoid single points of failure.



*Auto-failover heartbeat topology example (1 Main Application Server; Main network on **eth0** port)*

The Main network serves as the medium through which replication occurs between the *Main* Application Server and the *Backup,* as well as being the primary path the *Backup* Application Server uses to test the heartbeat of the *Main*. Only if the *Backup* does not receive the *Main*

Application Server's heartbeat signal through the Main network will the Backup resort to the Heartbeat network to listen for the Main Application Server's heartbeat.

> **Note:** When connecting your Application Servers to the networks, use the **eth0** port to connect to the Main network. Use **eth1** to connect to the Heartbeat network.

When a Redundancy Group is configured and online, any one of the following conditions can cause a Main Application Server to automatically fail over to its Backup:

Condition	Details
The Main Application Server loses network connectivity on the Main network.	The Main Application Server loses its network connection and is unable to service its clients.
The Backup Application Server loses network connectivity with the Main Application Server via both the Main and the Heartbeat network (and the Backup Application Server has connectivity on the Main network).	In this case, the Backup Application Server has no way of knowing if the Main server has connectivity on the Main network. It therefore takes over the Main's responsibilities.
The Main Application Server stops responding or is too overloaded to answer the Heartbeat request quickly enough.	In this case, pinging between the Backup and the Main Application Servers is still possible but not quick enough.
The Main Application Server loses power.	The Main Application Server shuts down because of a power loss to that Application Server.

IMPORTANT: Make sure the Main Application Server's resource usage is within acceptable parameters

Prior to enabling the Auto-failover feature, the operator should make sure that the Application resource usage on the *Main* Application Server (e.g., CPU usage, RAM usage) is within acceptable limits so that it can respond to Heartbeat requests from the *Backup* Application Server monitoring it.

IMPORTANT: When configuring a Redundancy Group, make sure virtual machines are not mixed with physical machines. Additionally, if both *Main* and *Backup* devices are virtual machines, ensure they are running operating systems at the same bit-processing level (i.e., *Main* and *Backup* should have operating systems that are either **BOTH** 32-bit or **BOTH** 64-bit).

The *Redundancy configuration* page contains the following information about the Redundancy Group and its Application Servers.

Parameter	Description	Parameter range	User editable?	Visible on Main Application Server?	Visible on Backup Application Server?
Role	The redundancy role of an Application Server	Main, Backup	Yes	Yes	Yes
Host name	Host name of the Application Server	Alphanumeric	Yes, from elsewhere in iControl	Yes	Yes
Configured IP	Configured IP address of the Application Server (retained after an Auto-failover or Manual Takeover has changed the current IP)	IPv4 address (`xxx.xxx.xxx.xxx`)	Yes, from elsewhere in iControl	Yes	Yes
Current IP	Current IP address of the Application Server	IPv4 address (`xxx.xxx.xxx.xxx`) (or Unknown if Application Server unreachable)	No	Yes	Yes
Operational state	The operational state of an Application Server	Main: Offline, Online Backup: Standby, Online	No	Yes	Yes
Auto-failover function state	If enabled, the corresponding *Main* Application Server shall be monitored by *Backup* Application Server through heartbeat mechanism. If disabled, an Application server will not Auto-failover to a Backup Application Server.	Enabled, Disabled	Yes	Yes	Yes
Take over the main IP address after failover	A function that, when selected, causes the Backup Application Server to take on the IP address of the Main during a failover or takeover. When disabled, the Backup keeps its own configured IP address.[1]	Enabled, Disabled	Yes	Yes	Yes
Auto-failover status	Running status message indicating the current Auto-failover status	Manual[2], Automatic[3], Takeover[4]	No	Yes	Yes
Extra IP	This IP address will be given to a Main Application Server, when it comes back online after a failover (since its configured IP address would not be available while the Backup Application Server uses it).[5]	IPv4 address (`xxx.xxx.xxx.xxx`)	Yes	Yes	Yes

(*Continued*)

Parameter	Description	Parameter range	User editable?	Visible on Main Application Server?	Visible on Backup Application Server?
Last replication result	Timestamp for the most recent replication of each Main Application Server	N/A	No	No	Yes
Backup used for Auto-failover	Backup Application Server displaying the server currently assigned as the Auto-failover Backup	Host name and MAC address (alphanumeric)	Selectable list	No	Yes
Replication frequency	List of preset replication frequencies	• never • every 5 min • every 15 min • every 30 min • every 1 hour • every 2 hours • every 3 hours • every 6 hours • every day **(default)**	Selectable list	No	Yes

1. Grass Valley recommends you enable this function.
2. Manual: The heartbeat mechanism is disabled (therefore, not in *Automatic* or *Takeover* state).
3. Automatic: A valid Redundancy Group exists and an Auto-failover *Backup* is in Standby mode.
4. Takeover: A failover or a switchover is in progress. While this is occurring, no additional switchover or failover can be triggered.
5. If you have not provided this Extra IP address, when a Main Application Server comes back online after a failover, the Main will fall back to the factory default IP address: 10.0.3.6 (see Troubleshooting an Auto-failover or Manual Takeover Operation, on page 586).

All the information on the *Redundancy configuration* page of a *Main* Application Server is visible from that of a *Backup* Application Server. However, the *Redundancy configuration* page on the *Backup* Application Server also displays the following:

- Timestamps for the most recent replication of each Main Application Server
- A list allowing operators to choose which Main Application Server to perform a Manual Takeover on
- The name of the Backup Application Server designated as the Auto-failover Backup, and the option of putting this Backup in Auto-failover Backup mode.
- A list allowing operators to choose the replication frequency

In addition, only from a Backup Application Server can the following operations be done:

- Trigger a Manual Takeover
- Perform a Reverse Takeover
- Perform a Replace Takeover

See also

For more information about:

- Auto-failovers, see Configuring and Managing Application Server Redundancy, on page 584.
- Redundancy Groups, see page 573.

Backup and Restore

Backup File

In the iControl documentation and iControl system a backup refers to creation of one backup file that contains all iControl related services and their configurations, Web sites, GSM, and scripts. Backups can be restored on the Application Server where the backup was originally created OR on another Application Server that you want to have configured in the same way.

Note: It is possible to set a schedule for an Application Server to perform automatic backups.

See also

For more information, see:

- Manually Backing Up an Application Server on page 581
- Scheduling Automatic Backups of an Application Server on page 583

Restore

Restore refers to the replacement of a backup file on an Application Server which restores all iControl related services, Web sites, GSM, and scripts can also be restored.

IMPORTANT: Restoring a backup file must be done on an Application Server running the same software version as the server from which the backup file was created.

See also

For more information, see Restoring Configuration Data to an Application Server on page 584.

Sample Workflows

[Workflow]: Configuring and Managing a Redundancy Group

REQUIREMENTS

Make sure you meet the following conditions before beginning this workflow:

- Upon failover or takeover, if you would like your *Backup* to take over the IP address of the *Main* Application Server, then all Application Servers you would like to assign to a Redundancy Group are on the same subnet.
- None of your Application Servers currently belong to a Redundancy Group.
- Each Application Server's **eth0** and **eth1** interfaces are connected.
- All **eth1** interfaces are connected together on the Heartbeat network (and can successfully ping other **eth1** IP addresses).
- All **eth0** interfaces are connected together on the Main network (and can successfully ping other **eth0** IP addresses).
- Your network is properly configured on both **eth0** and **eth1**, specifically:
  - Make sure the Broadcast IP (used by the Heartbeat mechanism) is correct.
  - Make sure both **eth0** and **eth1** are activated on boot.
  - Make sure the *Backup* Application Server has enough hard drive space left to replicate the *Main* Application Servers.

Sample workflow: Configuring and managing a Redundancy Group

1.	Create a Redundancy Group (see page 587).
2.	Add an Application Server to your Redundancy Group (see page 590). Repeat this step if you wish to add more *Main* Application Servers to your Redundancy Group.

IMPORTANT: Application Server Installation / Commissioning Notice

After configuring a Redundancy Group for the first time, it is highly recommended that you perform **ONE** of the following tests, as required:

- For every *Main* Application Server whose Auto-failover function is disabled, perform a Manual Takeover followed by a Reverse Takeover to ensure that everything is properly configured.
- For every *Main* Application Server whose Auto-failover function is enabled, disconnect that Application Server's **eth0** port from *Main* Application Server followed by a Reverse Takeover.

IMPORTANT: If you configure your Redundancy Group **NOT** to take over the *Main*'s IP address upon failover or takeover, make sure you keep the *Backup* Application Server's IP address configured in **System tools** | **Edit service locations** | **Service and alarm discovery** on all Application Servers that belong to the Redundancy Group.

[Workflow]: Recovering from a Manual Takeover or Auto-failover

REQUIREMENTS

Make sure you meet the following conditions before beginning this workflow:

- You have already configured your Redundancy Group and all required Application Servers are associated with it (see [Workflow]: Configuring and Managing a Redundancy Group, on page 580).
- If you are not performing a Manual Takeover, then an Auto-failover has already occurred.

Sample workflow: Recovering from a manual takeover or auto-failover

1.	If you are performing a Manual Takeover from a *Main* Application Server to a *Backup* Application Server, do so now (see Initiating a Manual Takeover to a Backup Application Server, on page 595).
2.	Perform any required maintenance work on the configured Main Application Server (currently offline).
3.	If you had not specified an Extra IP address, or the Extra IP address is in a different subnet, see Troubleshooting an Auto-failover or Manual Takeover Operation, on page 586.
4.	If you would like to return the configured Main Application Server to an active Main role, see Restoring an Offline, Configured Main Application Server to Online Status, on page 597.
5.	If you would like to reconfigure the configured Main Application Server in a Backup role, see Reconfiguring an Offline, Configured Main Application Server in a Backup Role, on page 599.
6.	If you would like to replace a failed Main Application Server, see Replacing an Application Server in a Redundancy Group, on page 602.

Detailed Directions

Manually Backing Up an Application Server

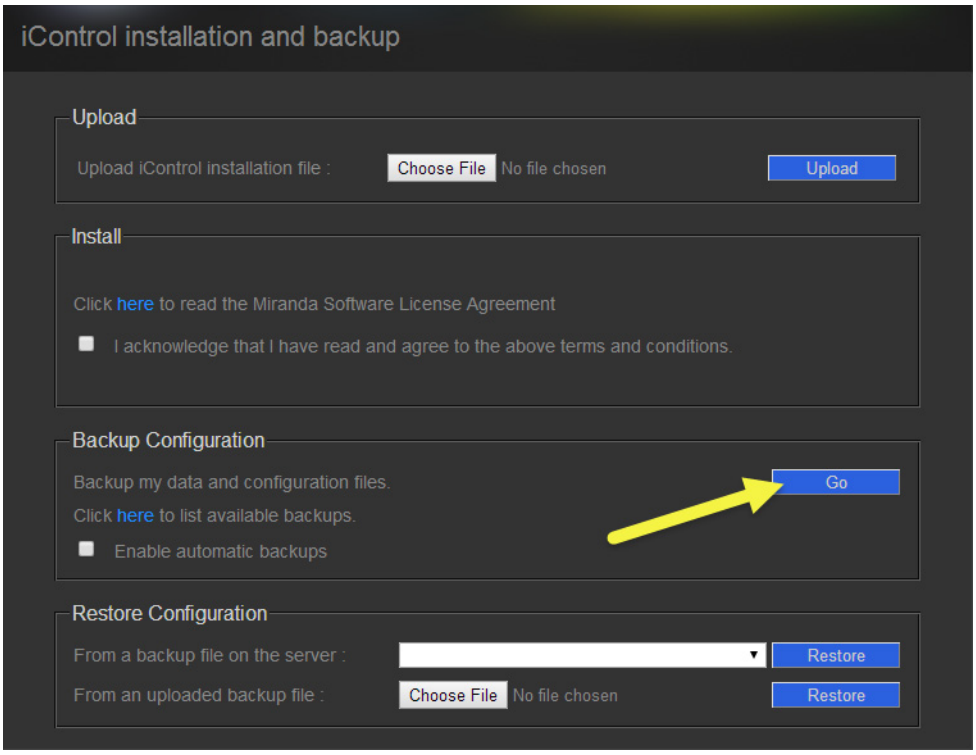
IMPORTANT: All iControl services, Web sites, GSM, and scripts must be backed up for restorations to be possible.

REQUIREMENT

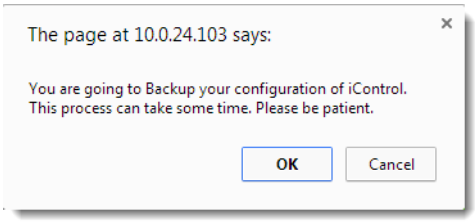
Before beginning this procedure, make sure you have opened the *Installation and backup* page for the Application Server on which you would like to perform a backup (see page 689).

To perform a backup

1. On the *Installation and backup* page, in the **Backup Configuration** area, click **Go**.

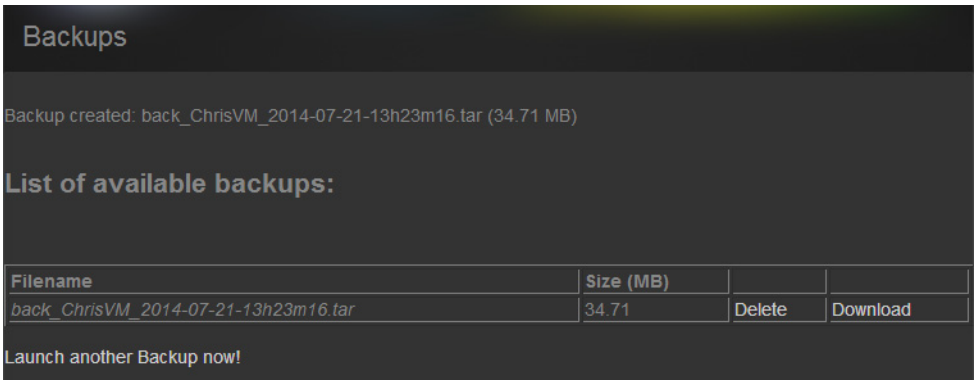


SYSTEM RESPONSE: A verification window appears.



2. Click **OK**.

SYSTEM RESPONSE: The backup proceeds.



SYSTEM RESPONSE: The backup file is saved on the Application Server.

IMPORTANT: It is highly recommended that you copy backup files to a separate PC in case of an Application Server failure that may prevent recovery of the backup file.

See also

For more information about backing up an Application Server, see Backup and Restore, on page 579.

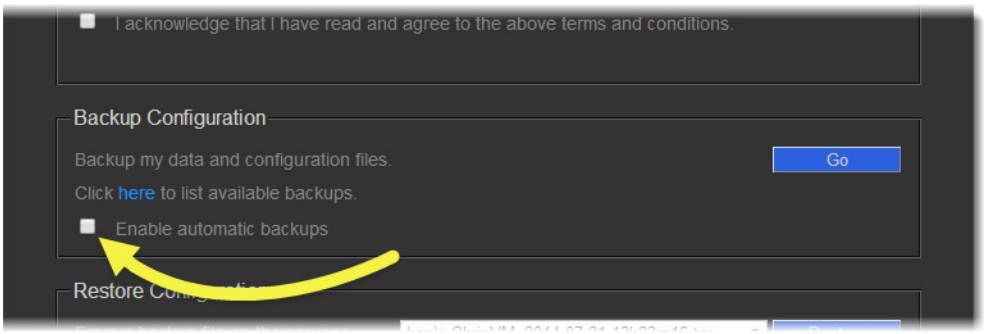
Scheduling Automatic Backups of an Application Server

REQUIREMENT

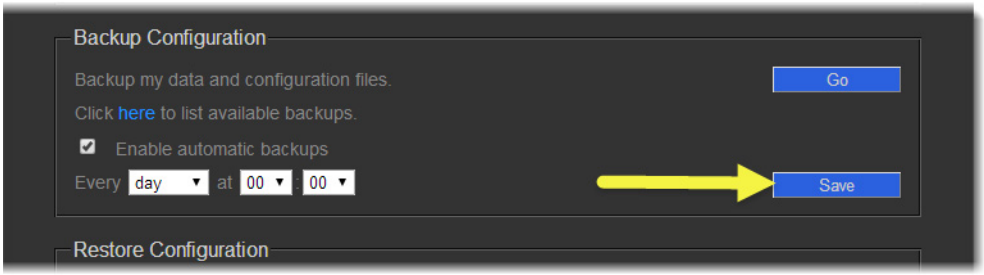
Before beginning this procedure, make sure you have opened the *Installation and backup* page.

To schedule automatic backups on an Application Server

1. On the *Installation and backup* page, in the **Backup Configuration** area, select **Enable automatic backups**.



2. Enter the desired time and frequency, and then click **Save**.



Restoring Configuration Data to an Application Server

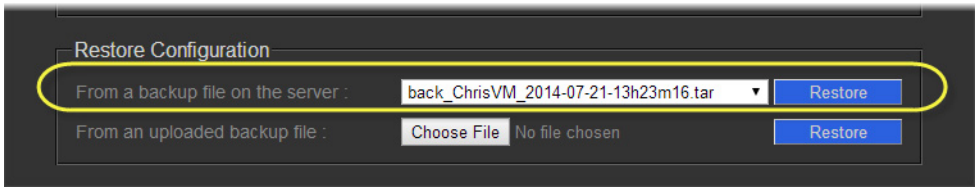
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- Backups currently exist of the files intended for restoration.
- You have opened the *Installation and backup* page for the Application Server on which you would like to perform a restore (see page 689).
- The backup file to restore was done for an Application Server running the same software version.

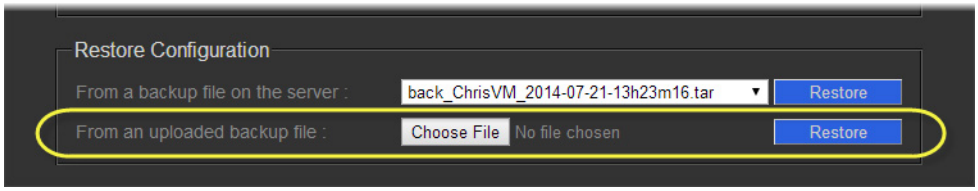
To perform a restore

1. On the *Installation and backup* page, in the **Restore Configuration** area, specify the file that you would like to use to perform the restore operation by one of the following two methods:
   - Browse for a backup file on the server,



   OR,

   - Upload a backup file from your local file system.



2. Click **Go**

   System Response: A message appears, prompting you to confirm your intention.

3. Click **OK**.

   System Response: The restore proceeds.

See also

For more information about restoring configuration data to an Application Server, see Backup and Restore, on page 579.

Configuring and Managing Application Server Redundancy

There are two ways the role and function of a *Main* Application Server can switch to its designated *Backup*: through an automatic failover (Auto-failover) or through a Manual Takeover. In either case, you must create a Redundancy Group on the *Redundancy*

configuration page of any Application Server you would like to assign to your group. After the group's creation, any further configuration, including adding and removing of Application Servers, can be accomplished from the *Redundancy configuration* page of any Application Server belonging to this Redundancy Group.

You can enable or disable the Auto-failover function of individual Application Servers in a Redundancy Group. With this function enabled, as long as there is a valid, *standby* Application Server, configured in a Backup role, a Main Application Server meeting failover criteria switches automatically to the Backup.

In addition, as long as the Backup Application Server is in *standby* mode, operators can perform a Manual Takeover from any Main in the Redundancy Group to the Backup.

Note: To perform Manual Takeovers, you do not need to disable Auto-failover on the Main Application Server.

As there are two independent switching mechanisms (Auto-failover and Manual Takeover), there are system behaviors you should take note of regarding potential conflicts between them, as follows.

IMPORTANT: System behavior

In the scenario where two or more Application Servers are configured as a Redundancy Group for Auto-failover and there is a condition present that, when detected, will cause an Auto-failover to the Backup, the following system behaviors result:

- If a user initiates a Manual Takeover and this is already in progress before the Backup Heartbeat function triggers an Auto-failover, then the Manual Takeover occurs and the Auto-failover is suspended.
- If an Auto-failover is already in progress when a Manual Takeover is attempted, then the Auto-failover occurs and the Manual Takeover command is ignored.

Considerations when Configuring Application Server Redundancy

There are several things we recommend you consider before and during the act of configuring your Application Server redundancy:

- If there is a performance difference among the Application Server hardware in your Redundancy Group, make sure the best performing Application Server is the *Backup*.
- If you would like your *Backup* to take on the IP address of your *Main*, make sure that all Application Servers are in the same subnet.
- It is important that the Broadcast IP address is configured correctly, since this is used by the heartbeat mechanism.
- If the **NTP synchronization** in your *Main* is set to **Disabled**, the time settings will need to be set manually in the *Backup* after an Auto-failover or Manual Takeover occurs. If you want your time settings to automatically be set and synchronized in the *Backup*, **NTP synchronization** must be set to **Enabled**. For more information, see Configuring an Application Server's Date and Time, on page 66.

- It is important that you activate both **eth0** and **eth1** at start-up and that they are both operational. A Redundancy Group assumes two working network interfaces.
- It is important that the *Main* network is over the **eth0** interface.
- It is important the *Heartbeat* network is over the **eth1** interface.

> **IMPORTANT: Ethernet Port Label Considerations**
>
> Please read the section regarding Ethernet port labels (see Ethernet Port Labels on Dell PowerEdge Application Servers, on page 48).

- In order for redundancy to be fully functional, **ALL** the Application Servers within the Redundancy Group must be running the same version of iControl software.

Troubleshooting an Auto-failover or Manual Takeover Operation

If an Auto-failover or Manual Takeover event occurs when there is no Extra IP address configured, when the *Main* Application Server comes back online, its IP address will fall back to the factory default IP address (10.0.3.6). The factory default is most likely not on the same subnet as the Application Servers in your Redundancy Group, in which case you will not be able to access this Application Server through the network. The procedure below explains how to repair a redundancy group, after a Main Application Servers' IP address reverted to 10.0.3.6.

To restore communications with a Main when its IP address reverted to 10.0.3.6

1. Navigate to the *Redundancy configuration* page of the **Backup** Application Server (see Opening the Redundancy Configuration Page, on page 685).

   This is the Application Server that took the Main's configured IP address.

2. Type a valid IP address, from the pool of free IP addresses on your network, in the **Extra IP** box.

   The configured Main Application Server will take this IP address (instead of the default 10.0.3.6).

3. Make sure the **Enabled** check box is *not* selected, in the **Auto-failover** column for the configured Main Application Server.
4. Click the **Apply** button near the bottom of the page.
5. Configure your client PC or laptop with network settings that will allow it to communicate with the configured **Main** Application Server, whose IP address fell back to 10.0.3.6 (see Preparing a PC for Configuring the Application Server, on page 45).
6. Log in to your configured **Main** Application Server with a PuTTY secure shell (see page 674).
7. In your PuTTY secure shell, enter

   `vi /usr/local/iControl/conf/cluster/cluster.conf`

8. Press `i` on your keyboard, to switch to vi's insert mode.
9. Locate the line that starts with `freeip =` and replace the IP address with the **Extra IP** address you configured at step 2.
10. Change any occurence of `auto_failover = on` to `auto_failover = off`.
11. Press Esc on your keyboard, to switch back to vi's command mode.

12. Type `:wq`, and then press Enter to save your changes and quit vi.
13. Type `reboot`.
14. Wait until your Main Application Server has restarted.

    You can verify whether it has restarted, by checking if *iControl admin* is available (enter the **Extra IP** address you configured at step 2 in your browser's address bar).
15. Navigate to the *Redundancy configuration* page of this Application Server (see page 685).

    The **Reverse** button should now be available to press (instead of **Replace**).

Creating a Redundancy Group

You can create a Redundancy Group either by starting with a Main Application Server or the Backup Application Server. Grass Valley recommends starting with the Backup Application Server because only the Backup server displays all redundancy information.

Creating a Redundancy Group starting with the Backup Application Server

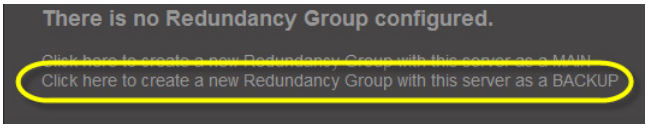
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

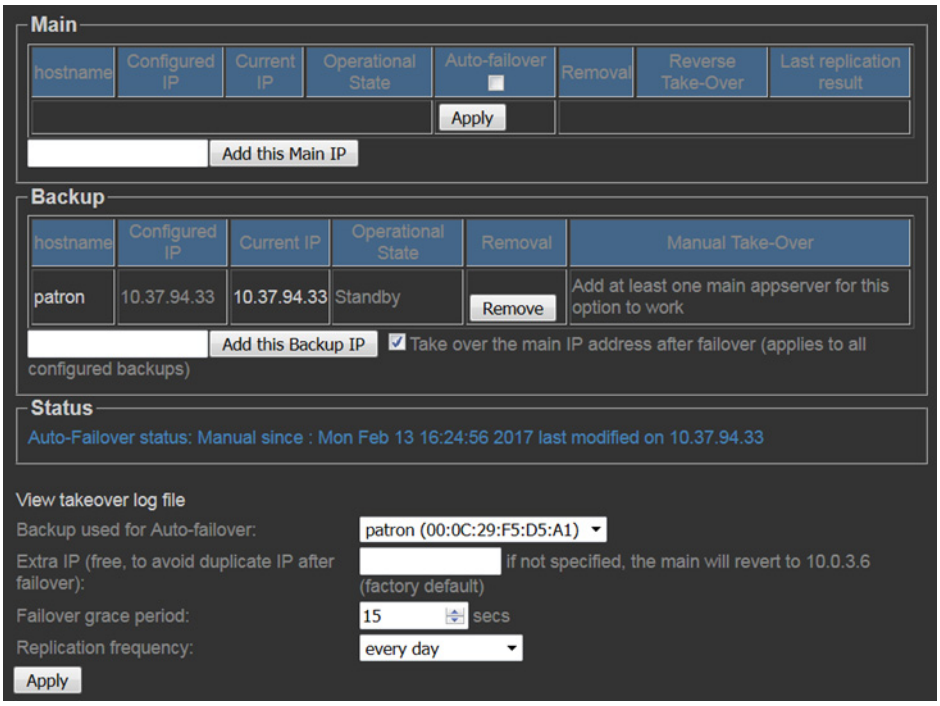
- You have navigated to the *Redundancy configuration* page of this Application Server (see page 685).
- Cabling for the **eth0** and **eth1** interfaces is properly connected.
- Network settings for **eth0** and **eth1** have been properly configured on each Application Server you would like to add to the Redundancy Group (e.g., IP broadcast, Netmask, IP address, Host name).

To create a Redundancy Group starting with the Backup Application Server

1. On the *Redundancy configuration* page, click **Click here to create a new Redundancy Group with this server as a BACKUP**.



SYSTEM RESPONSE: The *Redundancy configuration* page refreshes with the Application Server displayed in the **Backup** area.



2. Near the bottom of the Web page, type the desired **Extra IP** address.
3. Click **Apply**.

IMPORTANT: Make sure your Extra IP is in the same subnet as your Redundancy Group servers

- If you configure an Extra IP address that is not in the same subnet as the Application Servers in your Redundancy Group, subsequent tasks like a Reverse Takeover can only be done on a laptop connected by a crossover cable directly to the Main.
- If you do not configure an Extra IP address, and the factory default 10.0.3.6 is not in the same subnet as the other Application Servers, the same behavior as that stated above occurs.

IMPORTANT: No redundancy if Main Application Server is not configured

Even if a Backup Application Server has been added to a Redundancy Group, there is no redundancy if a Main has not yet been added to the group. That is, without a Main Application Server, there is no Application Server to backup. To add a Main Application Server to your group, see Adding an Application Server to a Redundancy Group, on page 590.

Creating a Redundancy Group starting with the Main Application Server

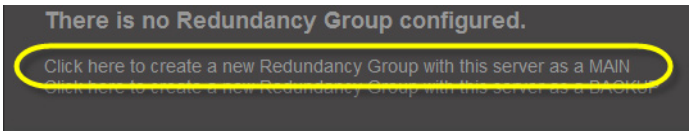
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

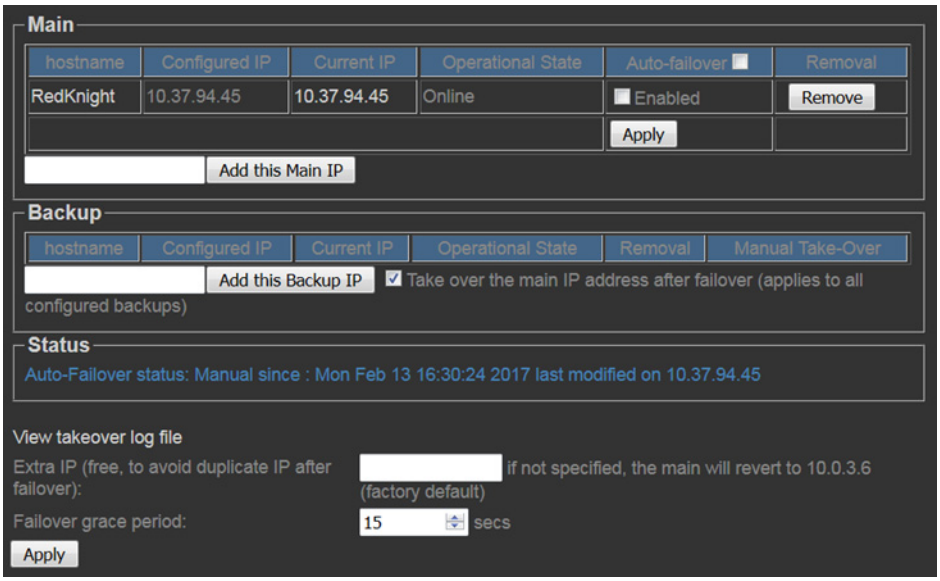
- You have navigated to the *Redundancy configuration* page of one of the Application Servers you would like to add to the Redundancy Group (see page 685).
- Cabling for the **eth0** and **eth1** interfaces is properly connected.
- Network settings for **eth0** and **eth1** have been properly configured on each Application Server you would like to add to the Redundancy Group (e.g., IP broadcast, Netmask, IP address, Host name).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Configuring and Managing a Redundancy Group, on page 580).

To create a Redundancy Group starting with the Main Application Server

1. On the *Redundancy configuration* page, click **Click here to create a new Redundancy Group with this server as a MAIN**.



SYSTEM RESPONSE: The *Redundancy configuration* page refreshes with the added Application Server displayed in the **Main** area.

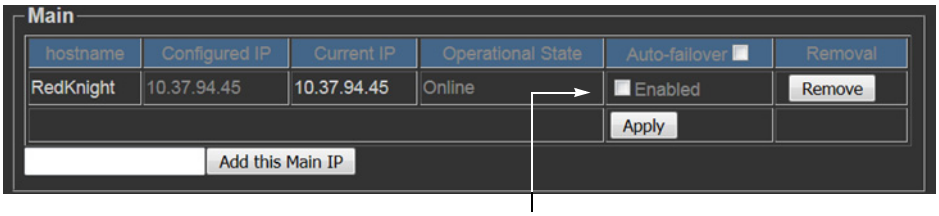


2. Near the bottom of the Web page, type the desired **Extra IP** address.
3. Click **Apply**.

IMPORTANT: Make sure your Extra IP is in the same subnet as your Redundancy Group servers

- If you configure an Extra IP address that is *not* in the same subnet as the Application Servers in your Redundancy Group, subsequent tasks like a Reverse Takeover can only be done on a laptop connected by a crossover cable directly to the Main.
- If you do not configure an Extra IP address, and the factory default 10.0.3.6 is not in the same subnet as the other Application Servers, the same behavior as that stated above occurs.

4. If you would like to enable this Application Server's Auto-failover function, in the **Auto-failover** column, select **Enabled** in the row associated with this Application Server, and then click **Apply**.



Note: If you would like the Auto-failover function to remain disabled for this Application Server, clear the **Enabled** check box, and then click **Apply**.

IMPORTANT: No redundancy if Backup Application Server is not configured

Even if the Auto-failover function is enabled on a Main Application Server, there is still no redundancy until a Backup Application Server belongs to your Redundancy Group and is in standby mode. To add a Backup Application Server to your group, see Adding an Application Server to a Redundancy Group, on page 590.

Adding an Application Server to a Redundancy Group

Adding a Main Application Server to a Redundancy Group

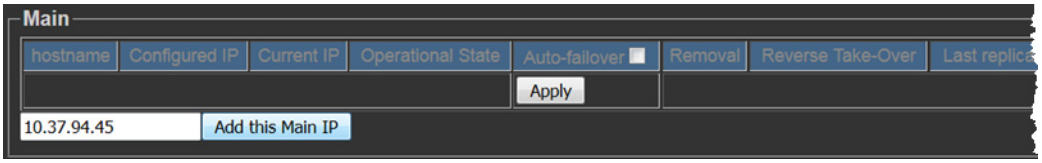
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

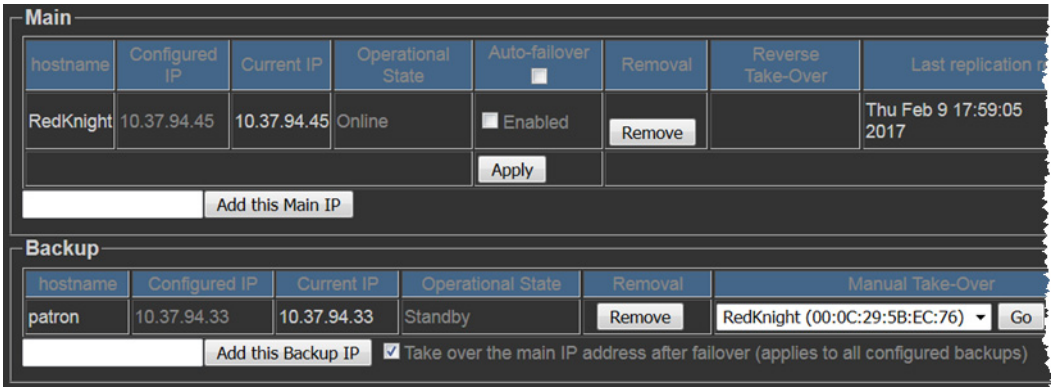
- A Redundancy Group already exists. If it does not, create the Redundancy Group (see page 587).
- You have navigated to the *Redundancy configuration* page of one of the Application Servers already belonging to this Redundancy Group (see page 685).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Configuring and Managing a Redundancy Group, on page 580).

To add a Main Application Server to a Redundancy Group

1. Type the IP address of the new Application Server in the box within the **Main** area.
2. Click **Add this Main IP** (next to the text box).



SYSTEM RESPONSE: The *Redundancy configuration* page refreshes with the added Application Server listed in the **Main** area.



3. If you would like to enable this Application Server's Auto-failover function, in the **Auto-failover** column, select **Enabled** in the row associated with this Application Server, and then click **Apply**.

Notes

- If you would like the Auto-failover function to remain disabled for this Application Server, clear the **Enabled** check box, and then click **Apply**.
- If you would like to enable the Auto-failover function for all Main Application Servers, select the check box in the **Auto-failover** column's header row, and then click **Apply**.
- If you would like the Auto-failover function to remain disabled for all Main Application Servers, clear the check box in the header row of the **Auto-failover** column, and then click **Apply**.

IMPORTANT: No redundancy if Backup Application Server is not configured

Even if the Auto-failover function is enabled on a Main Application Server, there is still no redundancy until a Backup Application Server belongs to your Redundancy Group and is in standby mode.

Adding a Backup Application Server to a Redundancy Group

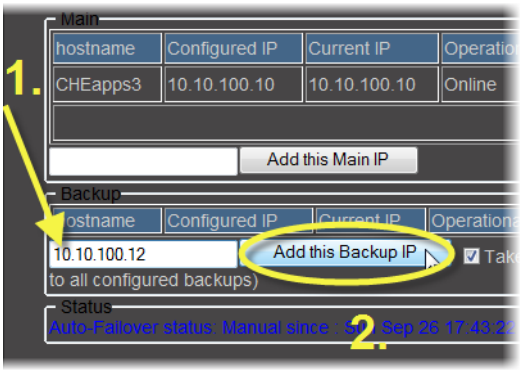
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- A Redundancy Group already exists. If it does not, create the Redundancy Group (see page 587).
- You have navigated to the *Redundancy configuration* page of one of the Application Servers already belonging to this Redundancy Group (see page 685).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Configuring and Managing a Redundancy Group, on page 580).

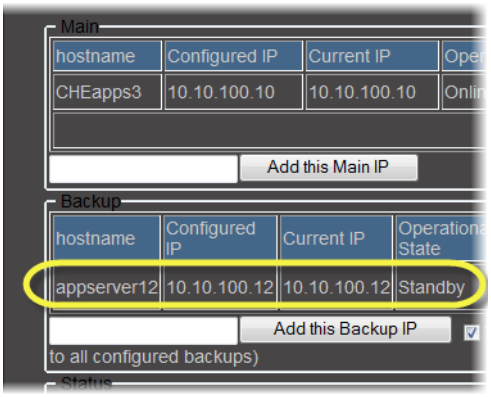
To add a Backup Application Server to a Redundancy Group

1. Type the IP address of the new Application Server in the box in the **Backup** area.



2. Click **Add this Backup IP** (next to the text field).

   SYSTEM RESPONSE: The Redundancy configuration page refreshes with the added Application Server listed in the **Backup** area.



IMPORTANT: System behavior

Your Redundancy Group offers no redundancy until you have configured one Application Server in the role of Backup.

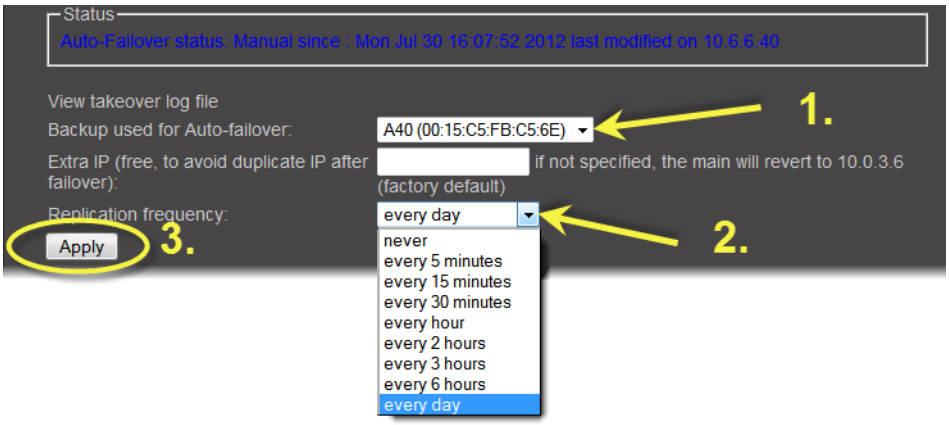
3. Perform only **ONE** of the following two actions:

- Click the host name of the newly added *Backup* Application Server.

  OR,

- In another browser window or tab, type the IP address of the newly added *Backup* Application Server.

4. Navigate to the *Redundancy configuration* page for this Application Server (see page 685).
5. Near the bottom of the Web page, in the **Backup used for Auto-failover** list, select the *Backup* Application Server that will be used in the Auto-failover.
6. Select the desired replication frequency from the list.



> **Note:** You can view the last time the *Main* Application Server was replicated on the *Redundancy configuration* page of the *Backup* Application Server, in the **Last replication result** column. Initially, there will be no timestamp because the *Backup* initiates its first replication after the *Main* has been added. If a replication is in progress, then *Running* will be displayed.

7. Click **Apply**.

   SYSTEM RESPONSE: The *Redundancy configuration* page refreshes displaying the new replication frequency.

> **IMPORTANT: System behavior**
>
> Regardless of the configured replication frequency, the system performs a replication immediately following any change in the *Redundancy configuration* page.

Removing an Application Server from a Redundancy Group

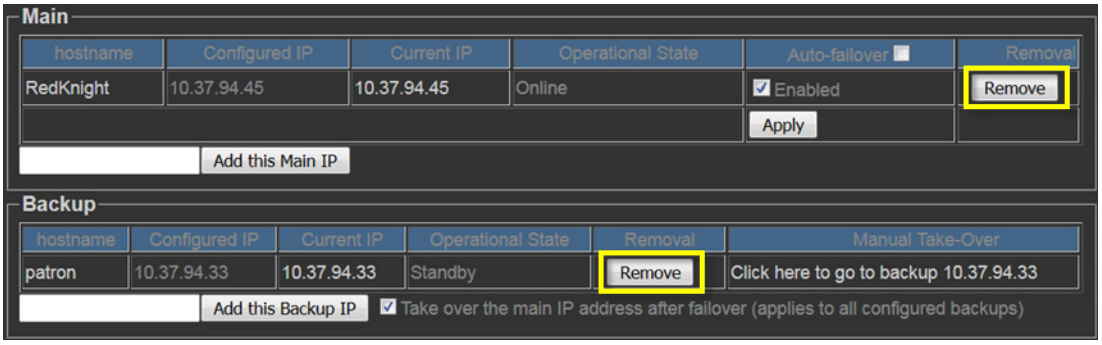
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

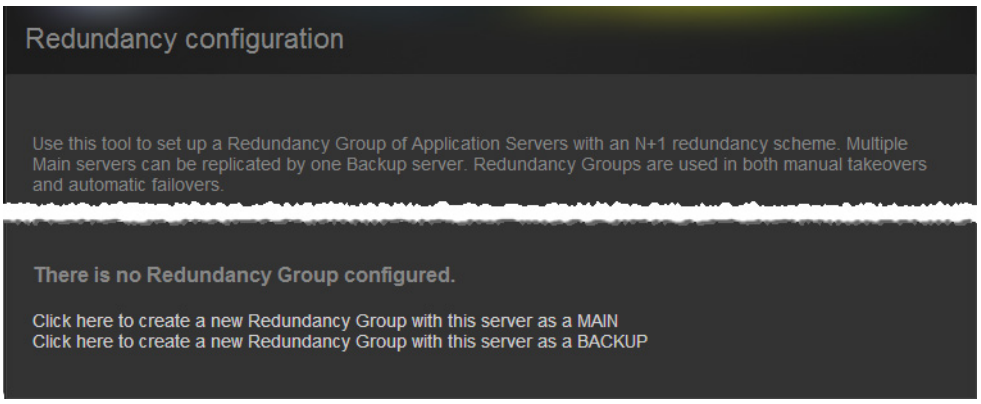
- A Redundancy Group already exists with associated Application Servers.
- You have navigated to the *Redundancy configuration* page of one of the Application Servers already belonging to this Redundancy Group (see page 685).

To remove an Application Server from a Redundancy Group

1. On the *Redundancy configuration* page identify the Application Server you would like to remove in either the **Main** area or the **Backup** area.
2. Click **Remove** in the **Removal** column of the row corresponding to the Application Server you are removing.



SYSTEM RESPONSE: If you performed this procedure from the Application Server you just removed, the Redundancy configuration page refreshes as follows.



SYSTEM RESPONSE: If you performed this procedure from an Application Server still in the Redundancy Group, the list of Application Servers on the *Redundancy configuration* page refreshes, excluding the removed server.

Initiating a Manual Takeover to a Backup Application Server

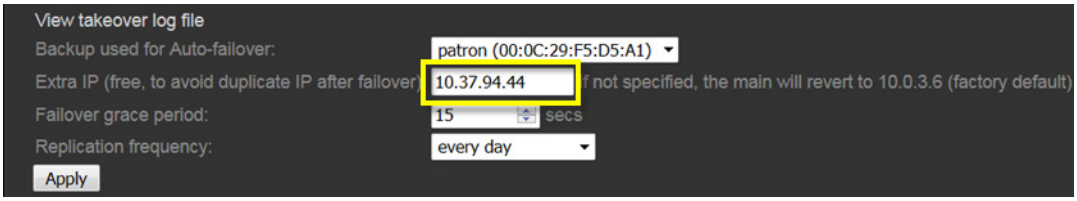
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have confirmed that the external devices connected to the target *Backup* Application Server are functional and compatible to the devices connected to the *Main* Application Server you will be taking over.
- There is at least one Application Server in the Redundancy Group with a configured role of Backup and whose state is *Standby*.
- You have navigated to the *Redundancy configuration* page of the target Backup Application Server (see page 685).
- The *Backup* Application Server has replicated the *Main* Application Server at least once (check in the **Last replication result** column of the *Backup*'s *Redundancy configuration* page for a time stamp).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Recovering from a Manual Takeover or Auto-failover, on page 581).

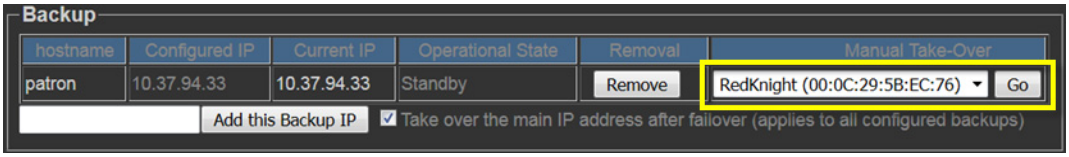
To initiate a Manual Takeover to a Backup Application Server

1. On the *Redundancy configuration* page of the *Backup* Application Server, near the bottom of the page, take note of the **Extra IP** address.



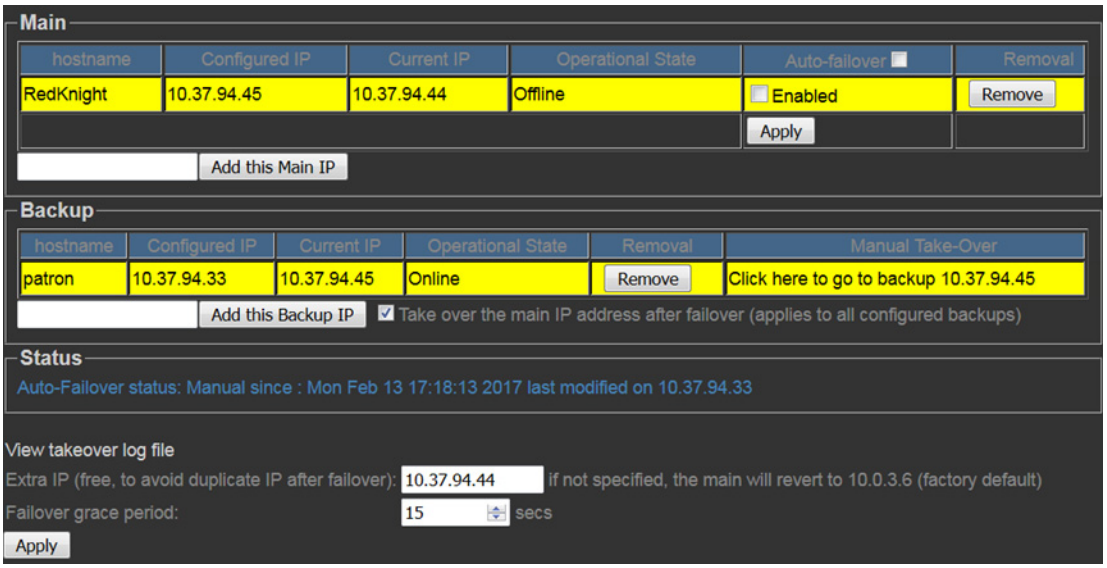
Extra IP address on the Redundancy configuration page (as seen from the Backup)

2. In the **Backup** area, use the list in the **Manual Take-Over** column to select the *Main* whose services, role, and identity you would like to take over, and then click **Go**.



SYSTEM RESPONSE: When the page next attempts to refresh (or when you manually click the Refresh button) it will be unable to retrieve data because the configured IP address for the Backup is no longer current.

3. Wait about 1 minute.
4. In your browser's address bar, type the Extra IP address (noted in step 1) to connect to the taken-over configured Main (now Offline).
5. Navigate to the *Redundancy configuration* page (see page 685).



6. If you observe the following, the manual takeover was a success:

   In the row corresponding to the taken-over configured Main (now Offline):

   - the color of the row is yellow
   - the **Current IP** is the same as the configured **Extra IP** (or the factory default IP 10.0.3.6, if no Extra IP address was configured)
   - the **Operational State** is *Offline*
   - the Auto-failover function is disabled

   In the row corresponding to the configured *Backup* (now Online*)*:

   - the color of the row is yellow (indicating a Manual Takeover or Failover has occurred)
   - the **Current IP** is the IP of the *Main* Application Server that was taken over
   - the **Operational State** is *Online*

   Note: If the NTP synchronization in your Main was set to Disabled, the time settings will need to be set manually in the Backup after the Manual Takeover occurs. For more information, see Configuring an Application Server's Date and Time, on page 66.

IMPORTANT: System behavior

Immediately following a Manual Takeover or an Auto-failover event, there is no longer any redundancy as the configured Backup is currently in the active role of a Main Application Server. In order to restore your system to full redundancy, you must do one of the following:

- **[Recommended option]:** Fix any issues with the configured Main Application Server that failed over or upon which you performed a Manual Takeover. Then perform a Reverse Takeover to revert Application Servers to their configured roles.
- Fix any issues with the configured Main. Then reconfigure this Application Server in the role of Backup and the configured Backup in the role of Main.
- Replace the defective Application Server. Then perform a Replace Takeover to revert the Backup Application Server to its Backup role and to use the Application Server to take over the role of the defective Main Application Server.

Restoring an Offline, Configured Main Application Server to Online Status

This procedure assumes the following:

- A *Main* Application Server Autofailed to, or was manually taken over by, its *Backup*.
- All required maintenance and troubleshooting work on the configured Main Application Server is complete.
- You would like the configured Main Application Server to be returned to *online* status as a Main Application Server (with its original IP address and host name).

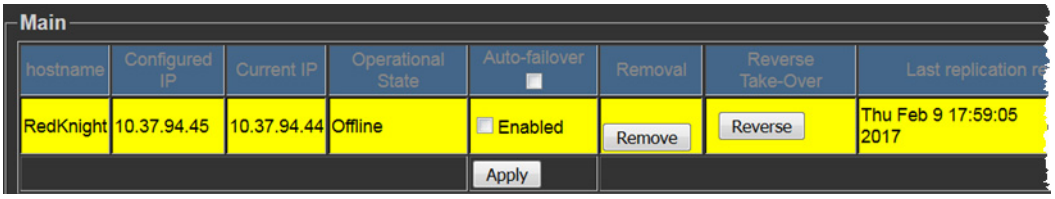
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have navigated to the *Redundancy configuration* page of the Backup Application Server (see page 685).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Recovering from a Manual Takeover or Auto-failover, on page 581).

To restore an offline, configured Main Application Server to online status

1. In the **Main** area of the *Redundancy configuration* page, use the **Configured IP** column to identify the Application Server that failed over or was manually taken over.



> **Note:** The row for the Application Server that failed over (or was taken over) should be yellow and the operational state should be *Offline*.

2. In the row corresponding to the Application Server you would like to restore to an *Online* status, click **Reverse** in the **Reverse Take-Over** column.

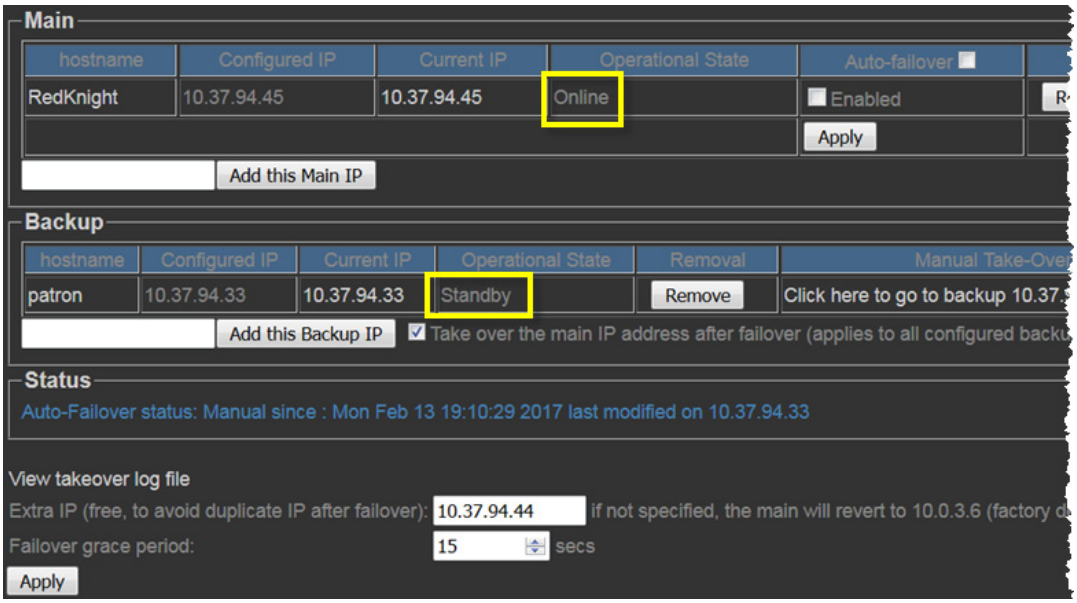
   SYSTEM RESPONSE: The system performs a Reverse Takeover on the Application Server.

> **Note:** Because this operation changes the physical hardware corresponding to the Main's IP address, the *Redundancy configuration* page is no longer able to refresh.

3. In your browser's address bar, enter the configured IP address of the Main Application Server you are restoring to online status.

> **Note:** The Reverse Takeover operation can take several seconds before completing.

4. Navigate to the *Redundancy configuration* page (see page 685).
5. On the *Redundancy configuration* page, verify that the operation completed successfully.



An online configured Main and a standby configured Backup: successful operation

6. Navigate to the *Redundancy configuration* page for the configured Backup Application Server (see page 685).
7. In the **Main** area, select the check box in the column header of the **Auto-failover** column, and then click **Apply**.

SYSTEM RESPONSE: The Auto-failover function is re-enabled on all Main Application Servers in the Redundancy Group.

Reconfiguring an Offline, Configured Main Application Server in a Backup Role

This procedure assumes the following:

- A Main Application Server Autofailed to, or was manually taken over by, a Backup Application Server.
- There are more than one configured Main Application Servers in the Redundancy Group.
- All required maintenance and troubleshooting work on the configured Main Application Server is complete.
- You would like the configured Main Application Server to be returned to the Network, but reconfigured in the role of a Backup Application Server.
- You would like the online, configured Backup Application Server to be reconfigured as the online Main Application Server.

IMPORTANT: This procedure uses the following naming conventions:

- The configured Main Application Server (currently offline) is Application Server **A1**.
- The configured Backup Application Server (currently online) is Application Server **A2**.

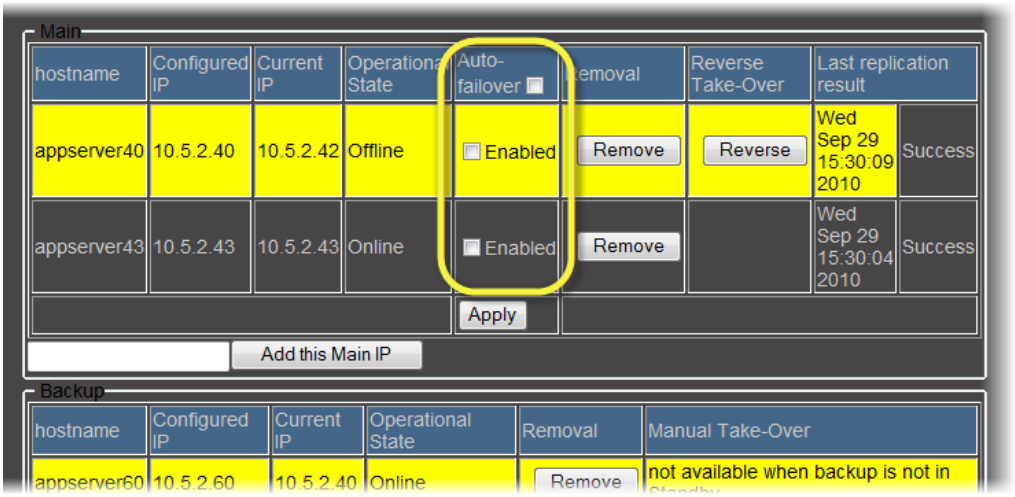
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have navigated to the *Redundancy configuration* page of the **A2** Application Server (see page 685).
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Recovering from a Manual Takeover or Auto-failover, on page 581).

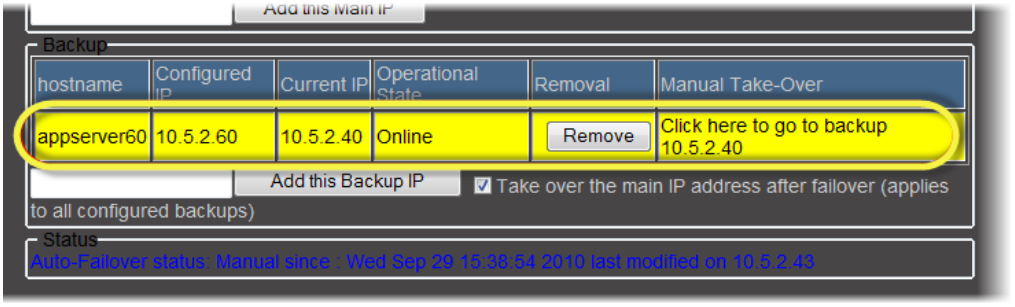
To reconfigure an offline, configured Main Application Server in a Backup role

1. In the **Main** area of the *Redundancy configuration* page, make sure the Auto-failover function for all Application Servers is disabled by clearing all **Enabled** check boxes.



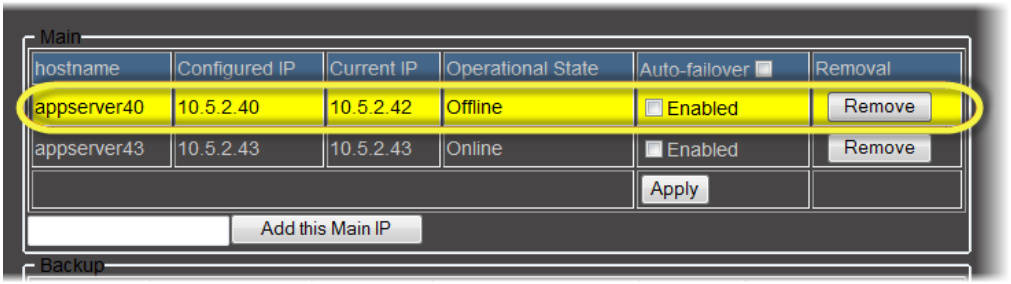
Note: You can disable Auto-failover for all Application Servers at once by clearing the check box in the **Auto-failover** column header.

2. Click **Apply**.
3. In another browser window, log in to iControl for the other **Main** Application Server (that is, neither **A1** nor **A2**) (see Starting iControl, on page 677).
4. Navigate to the *Redundancy configuration* page on the Application Server mentioned in step 3.
5. Identify **A2** in the **Backup** area.



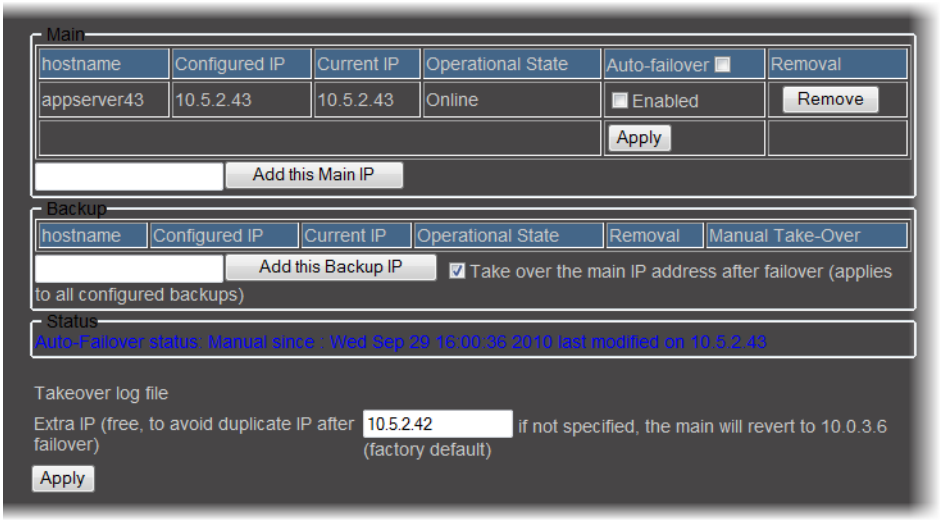
6. In the row corresponding to **A2**, click **Remove** in the **Removal** column.
7. Click **OK** in the confirmation window.

   SYSTEM RESPONSE: Once the *Redundancy configuration* page has refreshed, note that **A2** is not listed among the Application Servers in the Redundancy Group.
8. Identify **A1** in the **Main** area.



9. In the row corresponding to **A1**, click **Remove** in the **Removal** column.
10. Click **OK** in the confirmation window.

    SYSTEM RESPONSE: Once the Redundancy configuration page has refreshed, note that **A1** is no longer listed among the Application Servers in the Redundancy Group.



11. If you are performing this procedure with only one configured Main and one configured Backup, (that is, only **A1** and **A2** in the Redundancy Group), perform the following steps:
    a) In your browser's address bar, type the IP address of **A2**.
    b) Navigate to the *Redundancy configuration* page (see page 685).
    c) Click **Click here to create a new Redundancy Group with this server as a MAIN**.

       SYSTEM RESPONSE: The *Redundancy configuration* page refreshes, displaying **A2** in the **Main** area.
    d) In the **Backup** area, type the IP address of **A1**.
    e) Click **Add this Backup** (next to the IP address you just typed).

       SYSTEM RESPONSE: The *Redundancy configuration* page refreshes, displaying **A1** has been added to the **Backup** area.

12. If your Redundancy Group has more Application Servers than just **A1** and **A2**, perform the following steps:
    a) In your browser's address bar, type the IP address of one of the Application Servers (neither **A1** nor **A2**) still remaining in the Redundancy Group.
    b) Navigate to the *Redundancy configuration* page (see page 685).
    c) In the **Main** area, type the IP address of **A2**.
    d) Click **Add this Main** (next to the IP address you just typed).

    SYSTEM RESPONSE: The *Redundancy configuration* page refreshes, displaying **A2** has been added to the **Main** area.
    e) In the **Backup** area, type the IP address of **A1**.
    f) Click **Add this Backup** (next to the IP address you just typed).

    SYSTEM RESPONSE: The *Redundancy configuration* page refreshes, displaying **A1** has been added to the **Backup** area.

Replacing an Application Server in a Redundancy Group

Note: This procedure is applicable only if the **Take over the main IP address after failover** check box is selected (on the *Redundancy configuration* page). If this check box was cleared when an Auto-failover or Manual Takeover occurred, you will need to restore old Application Server's configuration data, to the new Application Server, from a backup (see Restoring Configuration Data to an Application Server, on page 584).

When the current IP is unknown and the operation state is *Offline*, you may choose to replace the Application Server. The *Replace* function replaces the online, Main Application Server with another Application Server outside the Redundancy Group.

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- An Auto-failover or Manual Takeover has occurred and the **Replace** button is visible in the *Redundancy configuration* page for the server you would like to replace.
- You have navigated to the *Redundancy configuration* page of the Backup Application Server (see page 685).
- Cabling for the **eth0** and **eth1** interfaces on the replacing Application Server is properly connected.
- Network settings for **eth0** and **eth1** have been properly configured for the replacing Application Server (e.g., IP broadcast, Netmask, IP address, Host name).

REQUIREMENTS (*Continued*)

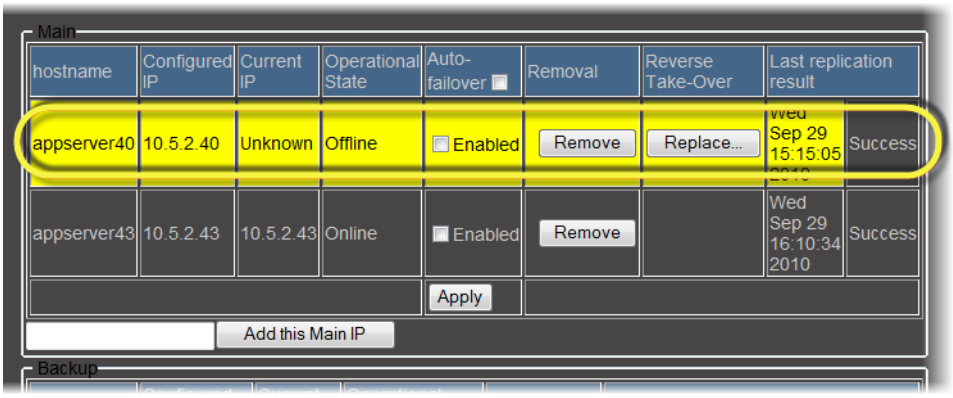
Make sure you meet the following conditions before beginning this procedure:

- The replacing Application Server is running and on the same subnet as the Application Server you would like to replace.
- The defective Application Server (the one being replaced) must be shut down or physically unplugged from the network.
- **[RECOMMENDED]**: You are performing this procedure as a task within the context of an approved workflow (see [Workflow]: Recovering from a Manual Takeover or Auto-failover, on page 581).

To replace an Application Server in a Redundancy Group

1. On the *Redundancy configuration* page, in the **Main** area, identify the row associated with the Application Server you would like to replace.

   Note: The row should be yellow, the Application Server should be Offline, and there should be a **Replace** button visible in the **Reverse Take-Over** column.



2. You may select or clear the **Take over the main IP address after failover** check box as required.
3. Click **Replace**.

   SYSTEM RESPONSE: The system prompts you for the IP address of the Application Server (not currently in the Redundancy Group) that you would like to assign as a replacement.
4. Type the IP address, and then click **OK**.

   SYSTEM RESPONSE: The following behaviors occur:

   - The *Redundancy configuration* page refreshes displaying the new Application Server as the replacement.
   - The *Backup* Application Server will rsync the new Application Server with the configuration of the *Main* it is supposed to replace.
   - The network setting of the new Application Server will be modified.
   - A Reverse Takeover will be initiated.

- The new Application Server will become the *online Main*.
- The *Backup* Application Server will go back to *standby* status.

5. If, in step 2, you selected the **Take over the main IP address after failover** check box, perform the following steps:
   a) Change the IP addresses of **eth0** and **eth1** on the new Application Server to the old *Main*'s **eth0** and **eth1** IP addresses (see Changing an Application Server's IP Address, on page 604).
   b) Restart iControl services on the new Application Server (see Starting & Stopping iControl Services, on page 678).
   c) If you are using **iC Web**, refresh the interface.

Changing an Application Server's IP Address

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened the *Network interfaces* page of the Application Server whose IP address you would like to change (see page 688).
- You have removed this Application Server from the Redundancy Group (see page 594).

To change the IP address of an Application Server

1. On the *Network interfaces* page, under **Eth0**, type a new IP address in the **IP Address** box.
2. Click **Apply**.
3. If required, add this Application Server to the Redundancy Group (see page 590).

Engaging a Failover of an External Device

IMPORTANT: The following failover procedure is applicable only if your **iC Web** site offers failover functionality.

iControl detects an error on a main device and when *Engage Failover* is active the router changes crosspoints for the backup device to feed both the main and the backup outputs.

Engaging Failover

To engage failover

- Select **Engage Failover** from the **Remote Control Monitoring and Pilot Control** area (lower right area of the Web page).

  System Response: The button becomes grayed out to indicate that it is active.

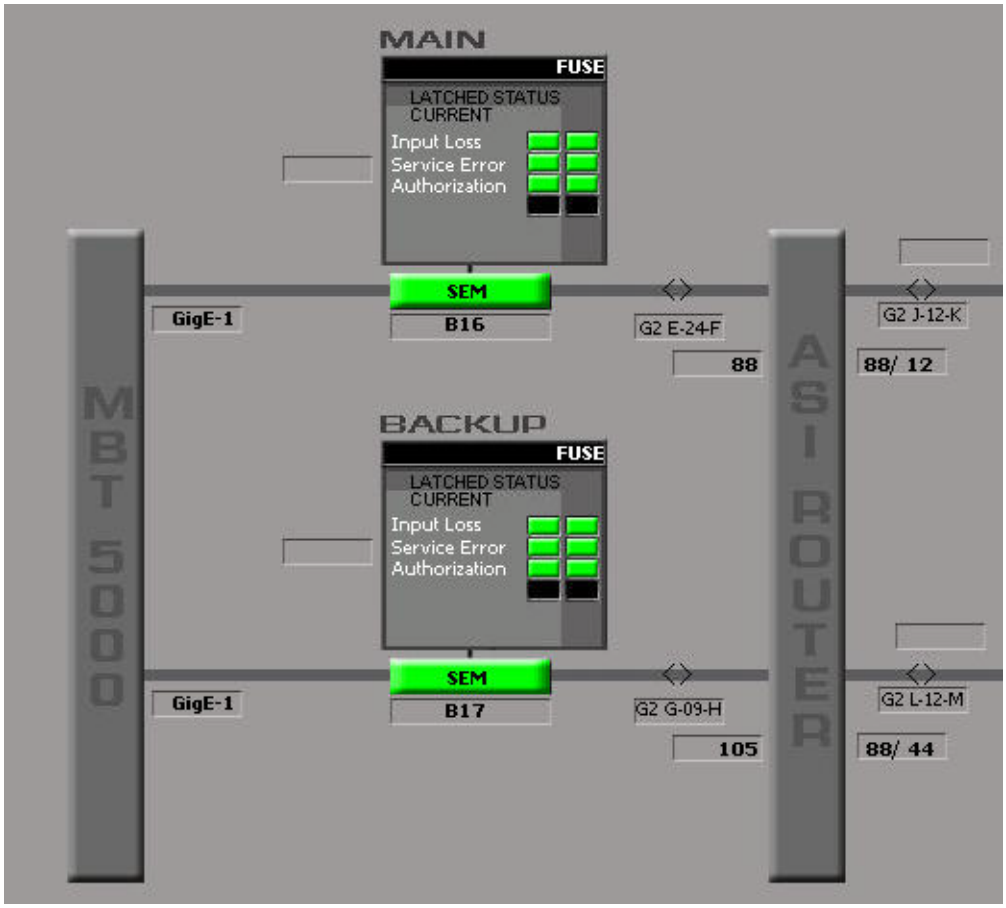
Changing the Signal Path from the Backup to the Main using the Matrix Application

After completion of an Engage Failover, the following procedure explains how to return the signal path from the backup to the main.

> **Note:** The following procedure includes steps that use iControl Router. For details about iControl Router configuration, refer to the *iControl Router Quick Start Guide*.

> **IMPORTANT:** The following Failover procedure is applicable only if your **iC Web** site offers Failover functionality.

The following image shows the signal path from the main to the backup as it should be after completion of the procedure.



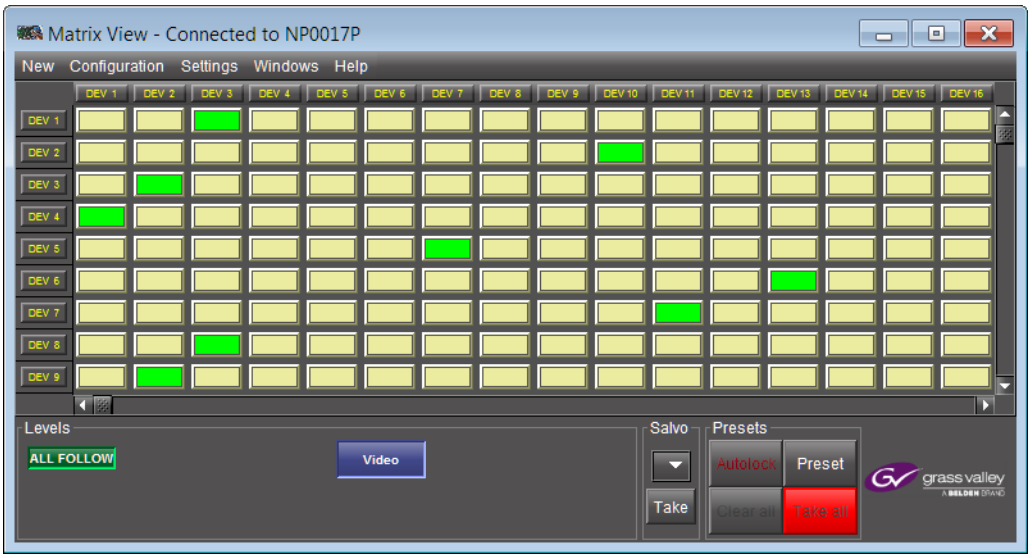
REQUIREMENT

Before beginning this procedure, make sure you have opened iControl Router (see page 728), and that it is connected to the Application Server running the router service.

To change the signal path from the backup to the main using the Matrix application

1. In iControl Router, select the router requiring configuration, and then click **Open**.

   SYSTEM RESPONSE: The **Matrix View** window appears.



Note: *Single Bus* is more practical if the matrix has an abundance of rows and columns. To open a Single Bus panel, on the **New** menu, click **Single bus**.

2. Select the desired router matrix point that will replace the currently active matrix point and close the window.

Note: Crosspoint changes are live.

Changing the Signal Path from the Backup to the Main using the Single Bus Application

After completion of an Engage Failover, the following procedure explains how to return the signal path from the backup to the main.

Note: The following procedure includes steps that use iControl Router. For details about iControl Router configuration, refer to the *iControl Router Quick Start Guide*.

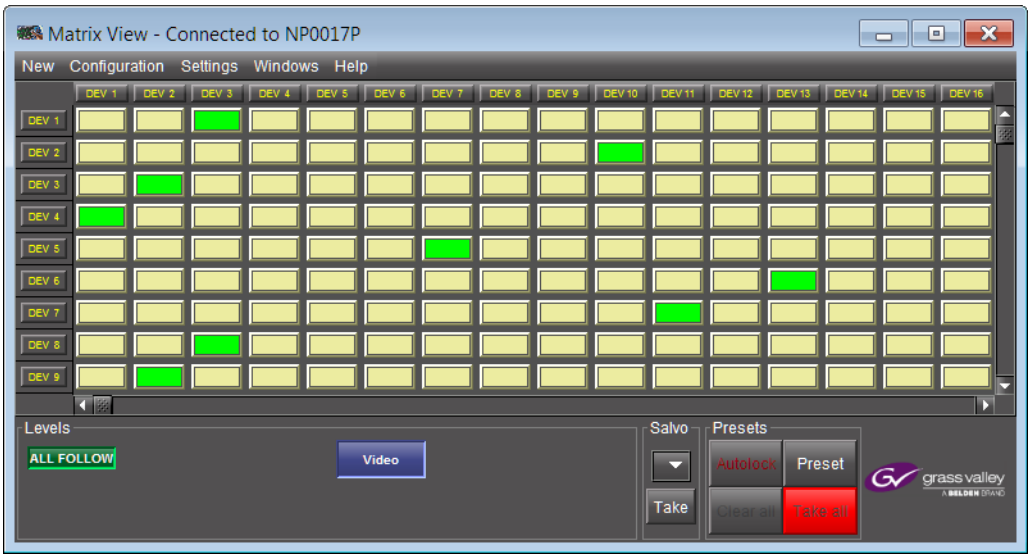
REQUIREMENT

Before beginning this procedure, make sure you have opened iControl Router (see page 728), and that it is connected to the Application Server running the router service.

To change the signal path from the backup to the main using the Single Bus application

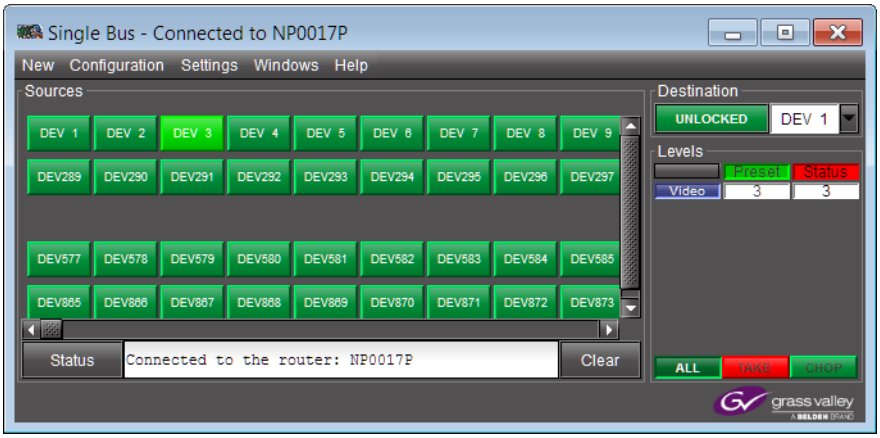
1. In iControl Router, select the router requiring configuration, and then click **Open**.

   SYSTEM RESPONSE: The **Matrix View** window appears.



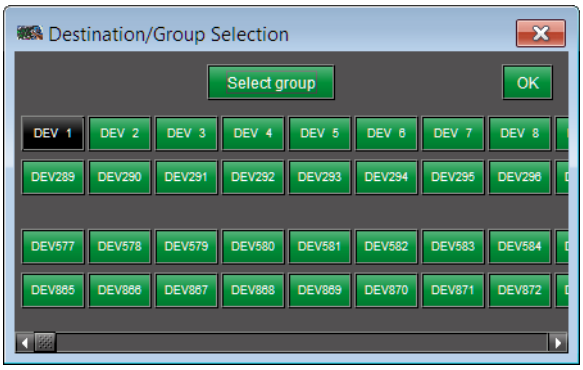
2. On the **New** menu, click **Single bus**.

   SYSTEM RESPONSE: The **Single Bus** window appears.



3. Click the arrow button in the **Destination** area.

   SYSTEM RESPONSE: The **Destination/Group** window appears.



4. Select an output/destination, and then click **OK**.

   SYSTEM RESPONSE: The **Single Bus** window re-appears.

5. Select a source, and then close the window.

> **Note:** Crosspoint changes are live.

11 iControl Web

Summary

Key Concepts

iC Web

iC Web is a Web-based device-monitoring module made up of two applications: iControl Web Creator (also known as **iC Creator**) allows users to create Web pages to control and monitor devices, while iControl Web is used to view and access Web sites available on the iControl Application Server

Web Sites

A Web site is a logical grouping of directories containing pages, page backgrounds, and graphic images. iControl sites can only be built using **iC Creator** and viewed with **iC Web**.

An iControl site can be either local or remote:

A local Web site is stored locally on your client PC or laptop. Sites must be initially created as local sites. A local site can later be published to the iControl Application Server to make it a remote site, accessible by any user with IP access to the Application Server on the network.

A remote Web site is stored on the iControl Application Server. Any modification to this site is available on the network.

With **iC Creator**, you can create sites, open existing sites, save sites locally, and publish sites to the Application Server.

Pages

A page is a customized display consisting of an optional background and one or more graphical objects or components placed on the background. With **iC Creator**, you can create pages, edit pages, set and size a background on a page, and place interactive graphical components on the background to create device and page links, control a router, and display streaming video.

Once a Web site has been created and is open on your computer, you can begin to create pages within the site.

Home Page

When you open a site in **iC Creator**, the home page automatically displays. When a home page is not defined, you will see no change to the main window, except the site address (remote sites) or path (local sites) which displays in the title bar. Creating a home page is optional.

Components

The components that appear on the pages of an **iC Web** site are the workhorses of the system. Each component type has specific functions in the runtime environment of **iC Web** sites and each individual implementation of a component type can be configured specifically for its intended application.

Components can perform a variety of functions. Each component type implements one or more of these functions:

- Report the status for a specific device, a page within the site, a virtual alarm, etc.
- Perform an action such as send an e-mail, change a router crosspoint, etc. if the status changes
- Jump to another page in the site
- Operate a device such as to set a router crosspoint or open a control panel on command
- Display or monitor program content

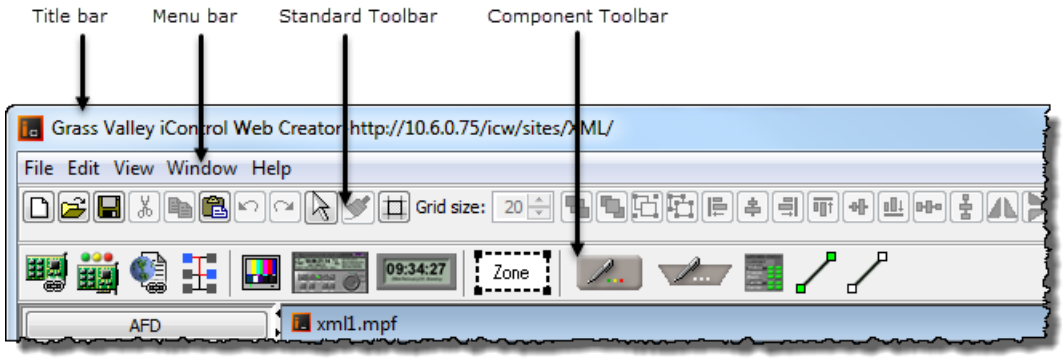
The following table summarizes the various types of components available with **iC Creator**.

Component Name	Description
Link to Device	• links to any device • reports GSM overall status • provides access to **iC Navigator** control panel • For example, if a card is malfunctioning, the device link will display the Error status image.
Status Inspector	• links to a device, a page or any defined group of items that uses alarms. Any linked object can trigger an external application when its status goes to Error. • reports any GSM status that appears in the alarm browser (the bitmap is the same as 'link to device') • shows image/bitmap changes with no user action • Only Status Inspectors can respond to virtual alarms. • Actions that are supported by **iC Web** include sending an e-mail to a defined address advising of the detected status change, activating a router crosspoint, setting a GPI output on a device, or sending an SNMP trap.
Link to Page	• links to another page within the same site • reports page status of the linked page (the bitmap is the same as 'link to device') • jumps to the linked page • For example, if a card is malfunctioning, the page link will display the Error status image. In a multiple-page link scenario, operators can use *Power Drill* to go directly to the page with the Error status. Clicking on a Page Link in runtime mode jumps to that page.

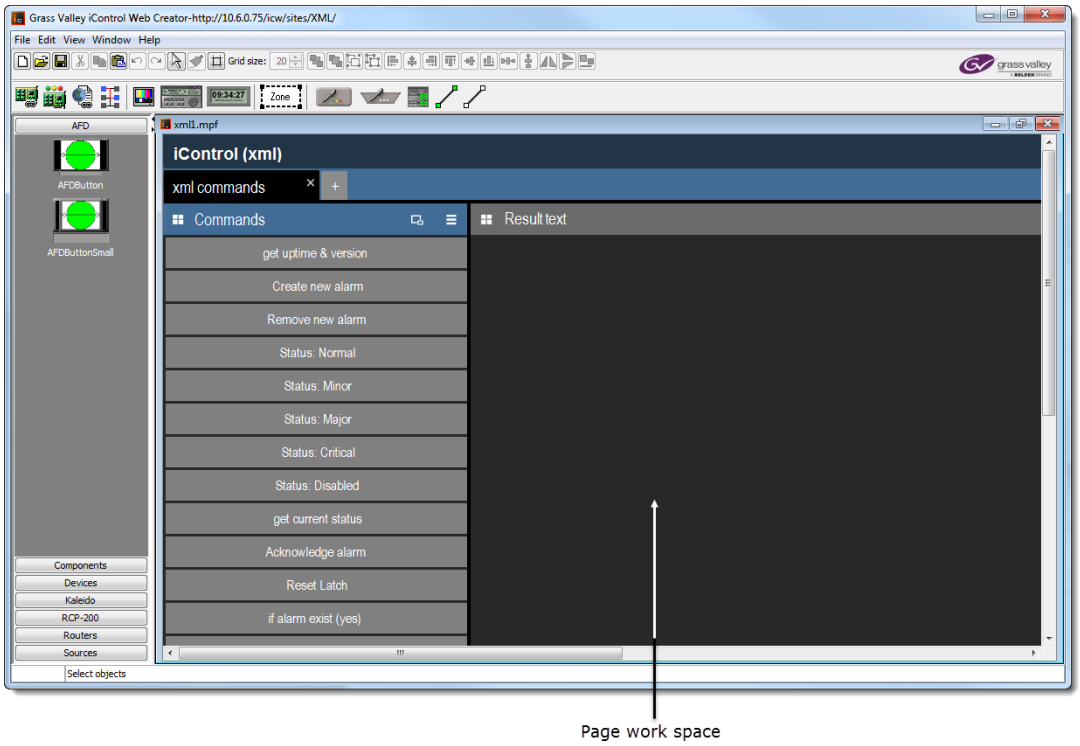
(*Continued*)

Component Name	Description
Crosspoint Selector	• links to a set of router crosspoints • activates router crosspoints • reports the status of the set of selected crosspoints
Player	• displays video, audio meters, and waveform/vectorscope • displays from streaming sources
VTR Player	displays the VTR control panel with standard controls on the page
Digital Clock	displays the current date and time
Zone	Similar to a HTML frame where a placeholder displays embedded components such as a service panel, page global log viewer, **iC Navigator**, VNC viewer, and a Web browser.
Status Icon	• The icon is a combination of a color and image where the image changes depending on whether or not the icon is selected and the color changes according to the current status. The status icon performs the same actions as link to device, link to page, crosspoint selector, status inspector and more. • reports any GSM status and any GSM static or dynamic text from a GSM text alarm • can execute a JavaScript program in accordance with a user click and/or a status change • works only with scripts since there is no GUI for its use
UMD	• displays different icon colors to represent status changes • reports any GSM status and any GSM static or dynamic text from a GSM text alarm • can execute a JavaScript program in accordance with a user click and/or a status change

iControl Web Creator Main Window



iControl Web Creator main window (Menu and toolbar detail)



iControl Web Creator main window (Work space view detail)

Background Properties Window

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

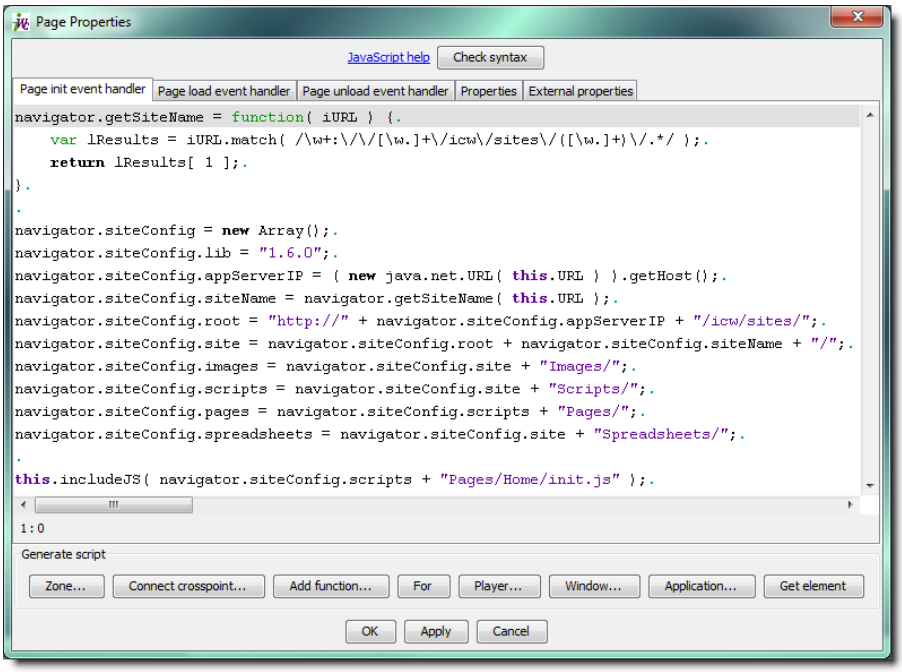
- You have opened iControl (see page 677).
- You have opened **iC Creator** (see page 722).

To open the Background Properties window

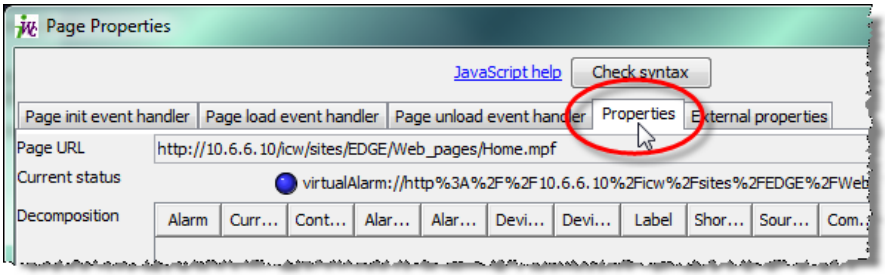
1. In **iC Creator**, load a page (see Opening Pages, on page 629).
2. Perform only **ONE** of the following two actions:
   - Right-click anywhere on the page's background (that is, not on a widget) and then click **Properties**.

     OR,
   - On the **File** menu, click **Page properties**.

   SYSTEM RESPONSE: The **Page properties** window appears.

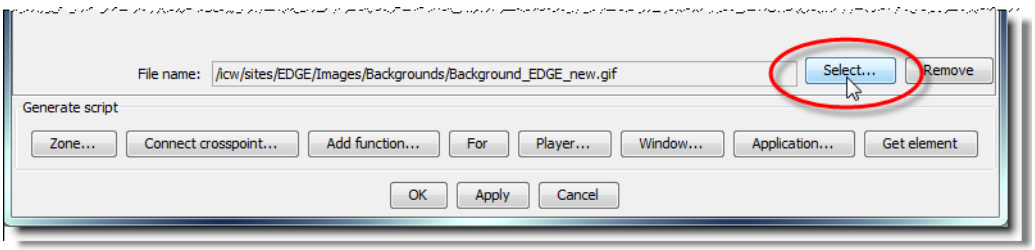


3. Select the **Properties** tab at the top of the **Page properties** window.

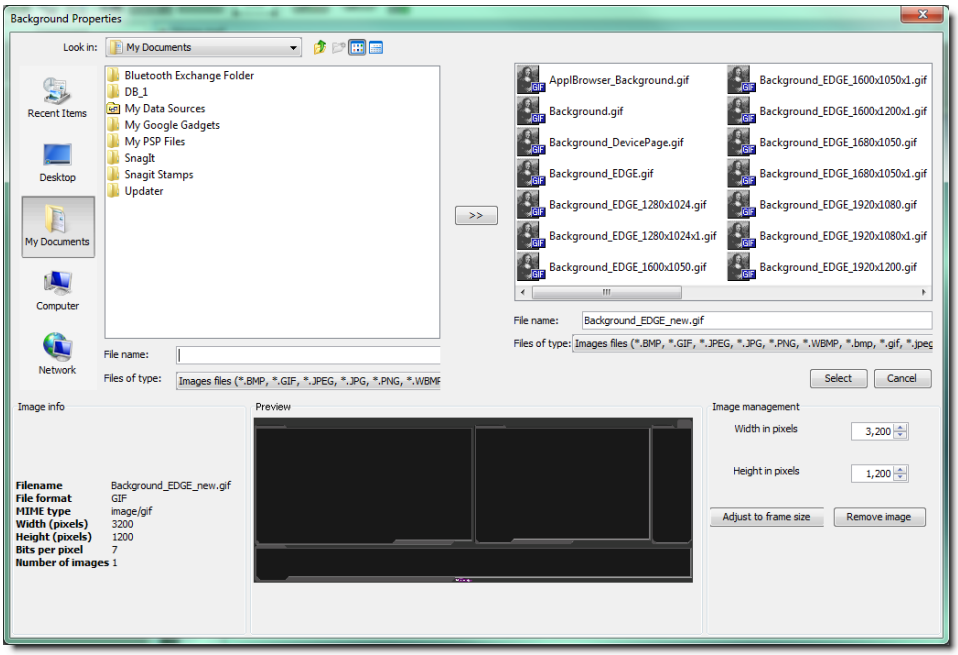


SYSTEM RESPONSE: The properties are displayed on the bottom half of the window.

4. Click **Select** beside the **File name** text box.



SYSTEM RESPONSE: The **Background Properties** window appears.



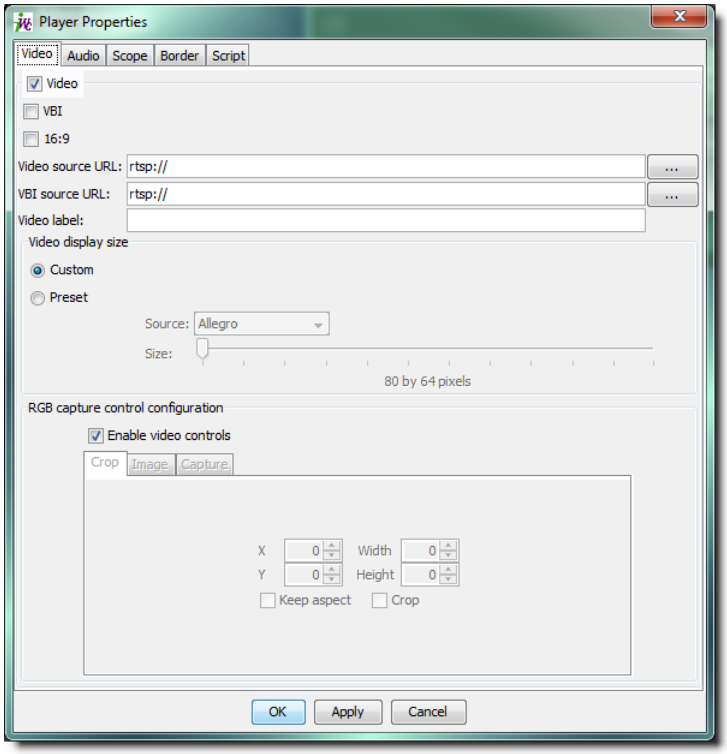
The **Background Properties** window contains five sections:

Name	Location	Description
Search	Top-left corner of the window	Use this window to search for image files that can be used as backgrounds.
Background images	Top-right corner of the window	Shows all the images which have been imported into the current site for use as backgrounds.
Image Info	Bottom-left corner of the window	Gives information about the image currently selected in either the Search window or the Background images window.
Preview	Bottom-center of the window	Shows a preview of the image currently selected in either the Search Window or the Background images window.
Image management	Bottom-right of the window	Allows an image selected in the Background images window to be resized or removed from the window.

Status Icon Properties Window

When adding a graphical component to a page, you specify the component parameters via its **Object properties** window. Properties vary according to the type of component.

In each properties window, there are tabs that correspond to different groups of parameters for the component. For example, the **Player** component has the object property tabs **Video**, **Audio**, **Scope**, **Border**, and **Script**.



Component window

Notable Line-Drawing Behaviors

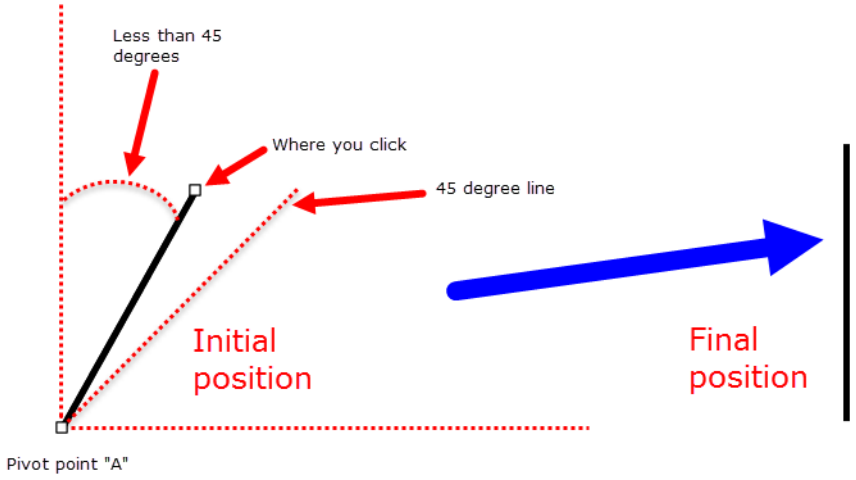
Change of Line-Segment Orientation

When using the line tool to draw lines in iC Creator, you may at some point decide you would like a line to rotate until its orientation is either vertical or horizontal. The line tool allows you to do this.

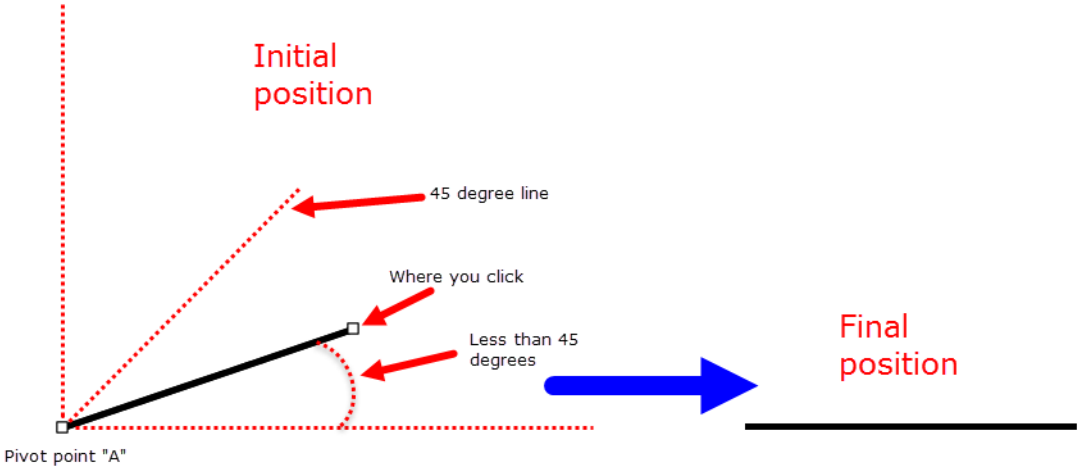
There are four important behaviors to keep in mind when performing this function of the line tool:

- The point on the line (whether an end-point or a middle-point) that you last click will be the point that moves. That is, the point that is *next* to the last-clicked point is the point the line segment will pivot around.
- Performing this function of the line tool will cause your line to become vertical only if the angle between the line and the vertical axis is less than 45 degrees. If the angle is greater than 45 degrees, the line will become horizontal.
- If your line has more than two points, using this function of the line tool will rotate only a single segment of the line and not the whole line.
- The point around which the line segment pivots is one of the two immediate neighbors (adjacent points) to the point last-clicked. Exactly which of these two points will be the pivot point is the one which is closest to the first end-point created on the line.

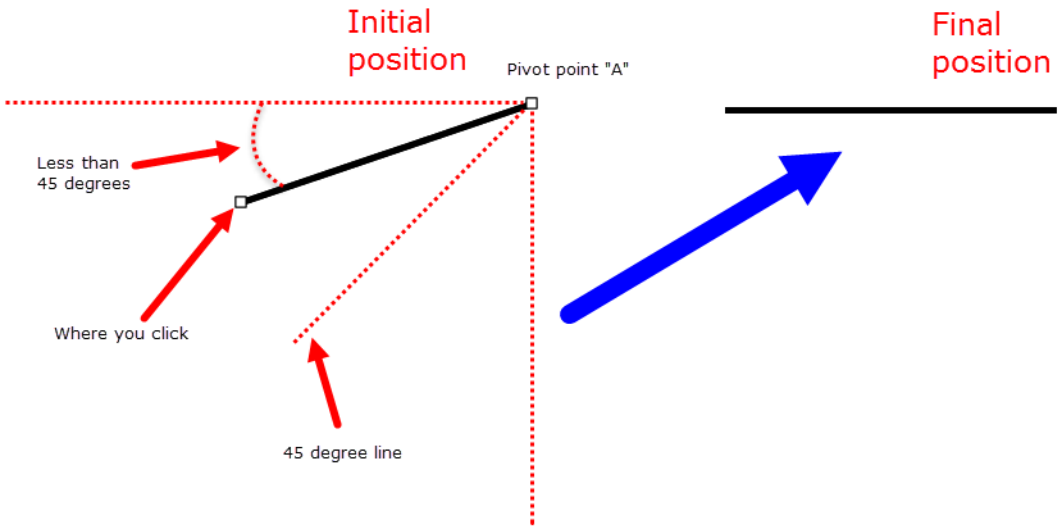
See the scenarios pictured, below, for a graphical representation of the different possible scenarios.



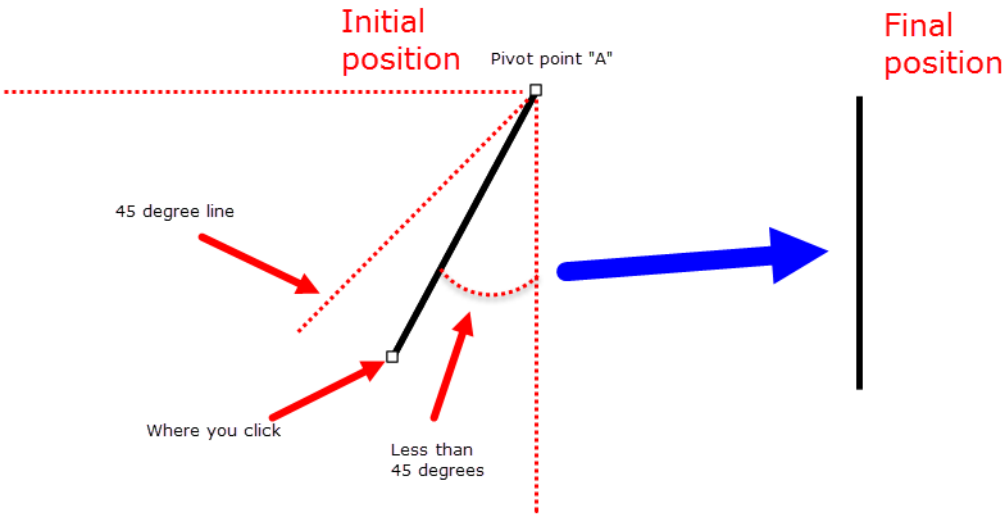
Scenario 1: Two-point line; line initially oriented closer to vertical orientation; click right-most point



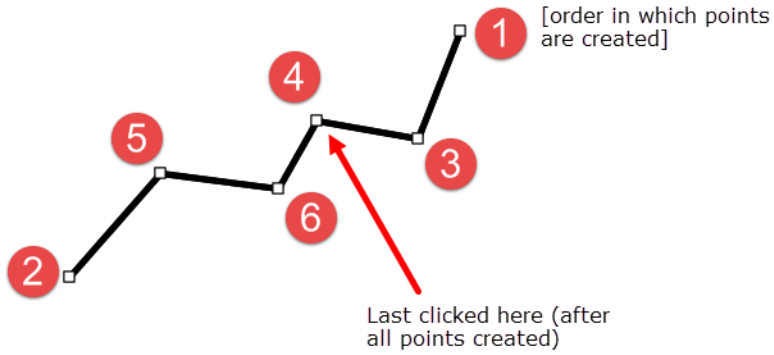
Scenario 2: Two-point line; line initially oriented closer to horizontal orientation; click right-most point



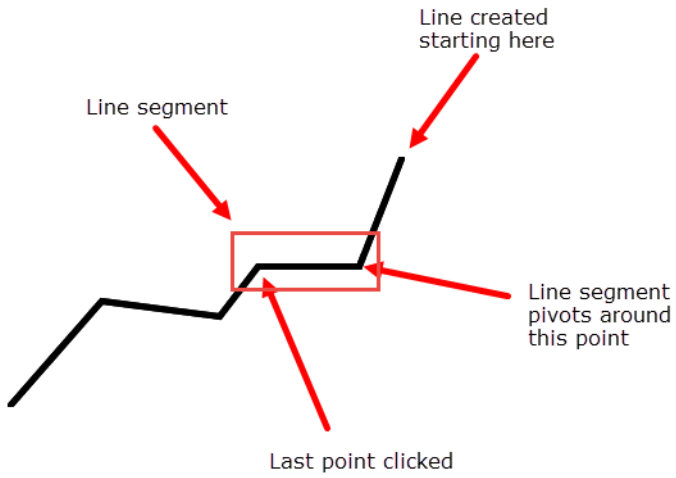
Scenario 3: Two-point line; line initially oriented closer to horizontal orientation; click left-most point



Scenario 4: Two-point line; line initially oriented closer to vertical orientation; click left-most point



Scenario 5 [part 1]: Multi-point line; determination of pivot point



Scenario 5 [part 2]: Multi-point line; determination of pivot point

Sample Workflow

The following steps summarize the tasks required to get started using **iC Web**:

Quick start task list:

1.	Start **iC Creator** (see page 722).
2.	Create a new local site or open an existing site (see Creating a New Local Site and Opening an Existing Site on page 622).
3.	Publish the site to the remote Application Server (see page 625).
4.	Create a page (see page 626).
5.	**[OPTIONAL]** Customize the dimensions of the *total full screen* window of your new page (see page 627).
6.	Import and set a background for the page (see Setting a Background for a Page, on page 630).
7.	Ensure that the GSM service is running on the same subnet as the Web site.
8.	Add zones to the page.
9.	Add components to the page.
10.	Save the page (see page 628).
11.	Create other pages within the site.
12.	Save each page immediately after changes (see page 628).
13.	Open the newly published remote site. Open **iC Web** to view and access your Web site in *Webpage* mode.

Quick start task list: (*Continued*)

14.	If you have not already done so, publish the site to the remote Application Server (see page 625).
15.	**[OPTIONAL]** Return to **iC Creator** and edit pages in the site.
16.	**[OPTIONAL]** Remove a remote site (see page 626).

Detailed Directions

Creating a New Local Site

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To create a new local site

1. In the **iControl Web Creator Welcome** window, select **Create a new local site**, and then click **Next**.

   SYSTEM RESPONSE: The **Create New Site** window appears.

2. Browse to locate the folder where you want to store the new site.

   SYSTEM RESPONSE: The folder containing the site will be created in the folder shown in the **Look in** box at the top of the screen.

3. Type the Web site name in the **File name** box, and then click **Create site folder**.

   SYSTEM RESPONSE: The new local Web site is created with your specified name and location. The **iC Creator** main window appears.

   SYSTEM RESPONSE: The site is now created. You may choose to either publish it to the Application Server, or work on the local site. In either case, the site is now ready for you to begin creating pages.

System Response: **iC Creator** saves the site when you create it. The site will be automatically updated each time you save a page or save all pages.

Opening an Existing Site

You can open an existing local or remote site to view or modify it. You can only open one site at a time.

IMPORTANT: If you have one site open and you want to open another site, make sure you save all your modifications (i.e., save all your pages) before opening the second site. When you open a new site, all operations (such as saving pages or importing graphics) will refer to that site.

If you chose to open an existing site, the procedure varies depending on whether it's a local or a remote site.

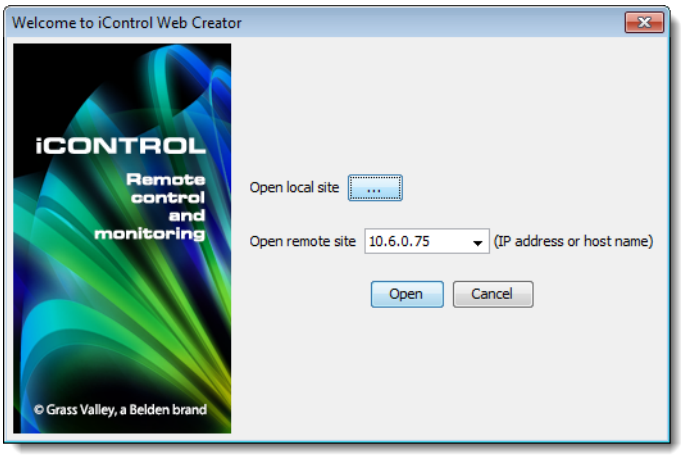
Opening an Existing Local Site

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To open an existing local site:

1. In the **iC Creator** welcome window, select **Open an existing site**, and then click **Next**.
   System Response: The 2nd iControl Web Creator welcome window appears.



2. Click the ellipsis button (...) beside **Open local site**.
   System Response: The **Open site** window appears.
3. Browse to locate the folder, and then click **Open site folder**.
   System Response: The selected site opens.

Opening an Existing Remote Site

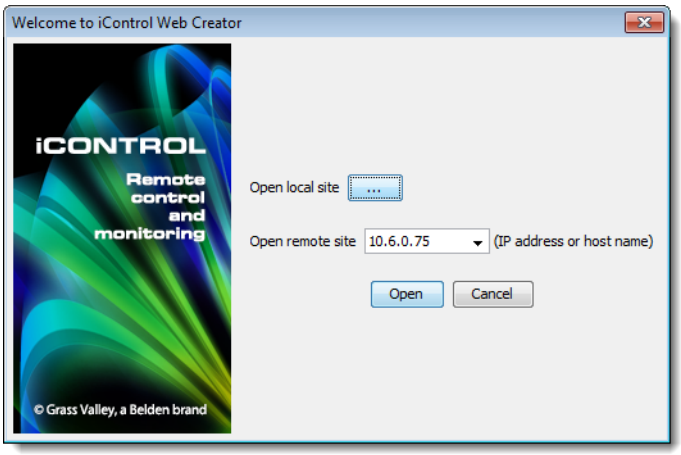
REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To open an existing remote site:

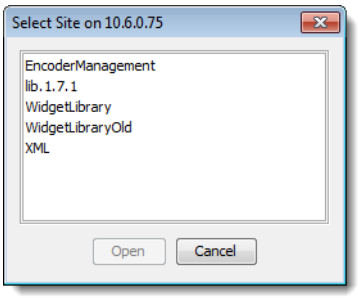
1. In the **iC Creator** welcome window, select **Open an existing site**, and then click **Next**.

   SYSTEM RESPONSE: The 2nd window appears iControl Web Creator welcome window appears.



2. Select the IP address of the remote site's Application Server in the **Open remote site** list, or type the IP address.

   SYSTEM RESPONSE: The **Select site on** window appears.



3. Select the remote site, and then click **Open**.

   SYSTEM RESPONSE: The selected site opens and the **iC Creator** main window appears.

   At this point, you can continue to work on this site and all your modifications will be public. If you want to work offline, save the site on the local disk and re-open it as a local site.

> **Note:** It may take some time to download a site. If an incorrect IP address is entered, the system will only display an error message after the internal time-out expires.

Saving a Remote Site Locally

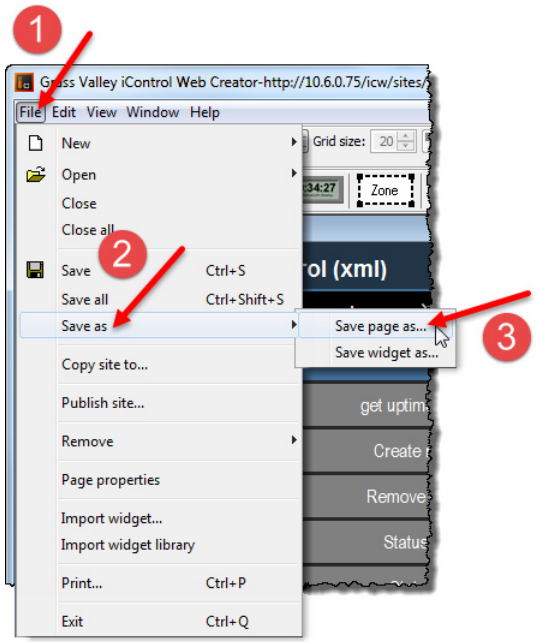
When you create a site, it is automatically saved locally. To transfer a remote site from an Application Server to your client hard disk, you need to open it and save it to your hard drive. When you save a site, all the pages associated with the site are also saved automatically.

REQUIREMENT

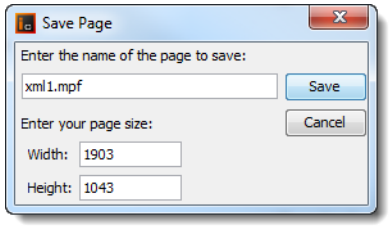
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To save an open site on a local hard drive

1. In **iC Creator**, on the **File** menu, point to **Save as**, and then click **Save page as**.



SYSTEM RESPONSE: The **Save page** window appears.



2. Type the file name under which the site will be saved, and click **Save**.

   SYSTEM RESPONSE: The **Saving page as** window displays the progress of the saving operation. This operation may take a while depending on the pages to be downloaded.

Publishing a Site

Publishing a site is the process of transferring a local site that has been saved on the hard disk to an iControl Application Server.

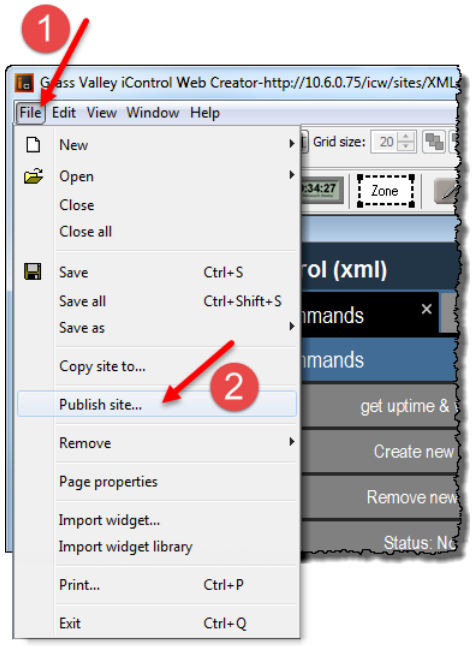
You can only publish open sites.

REQUIREMENT

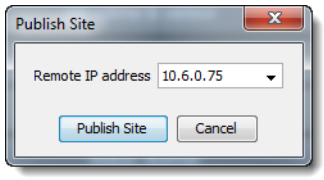
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To publish a local site

1. In **iC Creator**, on the **File** menu, click **Publish site**.



SYSTEM RESPONSE: The **Publish site** window appears.



2. Type the IP address of the Application Server on which the site is to be published (e.g., `192.128.01.16`).
3. Click **Publish Site**.

Removing a Site

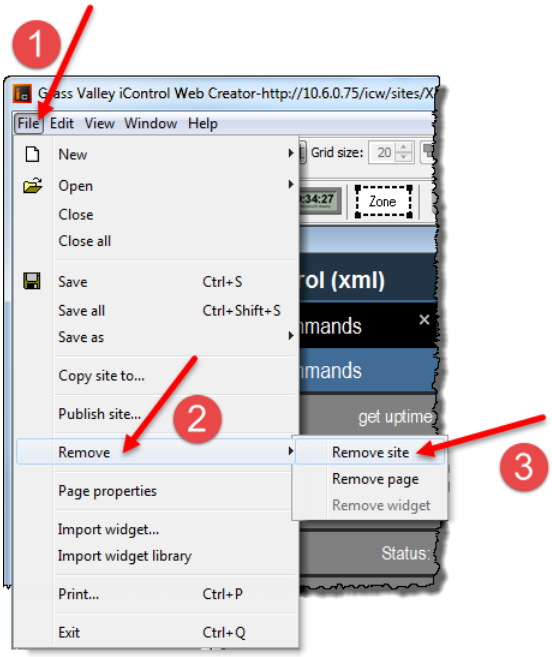
Removing a Remote Site from an Application Server

REQUIREMENT

Before beginning this procedure, make sure you have opened the existing remote site in **iC Creator** (see page 722).

To remove a remote site from an Application Server

- In **iC Creator**, on the **File** menu, point to **Remove**, and then click **Remove site**.



Note: When you remove a remote site, all the pages, images, and backgrounds associated with the site are automatically removed.

Removing a Local Site from a Client

To remove a local site from a client

- In Windows Explorer on your local PC or laptop, remove all the directories associated with the local Web site.

Creating a Page

REQUIREMENT

Before beginning this procedure, make sure you have opened the site to which you would like to add pages in **iC Creator** (see page 722).

To create a page

- In **iC Creator**, on the **File** menu, point to **New**, and then click **New page**.

  SYSTEM RESPONSE: A new, untitled page appears in the work space.

> **Note:** A *home* page is the first page retrieved when users access a site. In **iC Web**, the home page typically provides links to the rest of the pages on the site. Creating a home page is optional. To create a home page, create and save a page using the filename `home`, paying attention to type all lower-case letters as shown. The newly saved home page will be displayed automatically whenever the site is opened in **iC Creator**.

Customizing the Dimensions of the Total Full Screen Mode

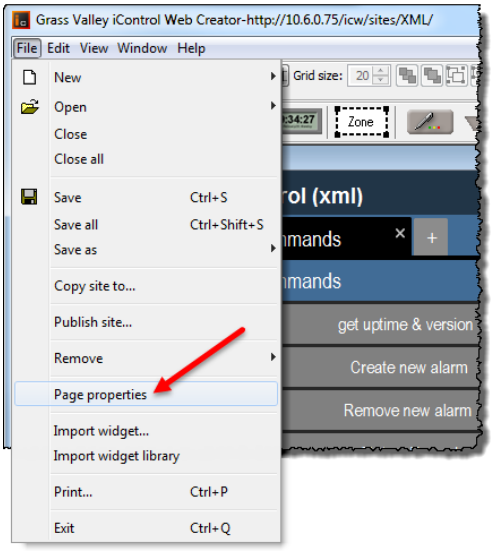
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

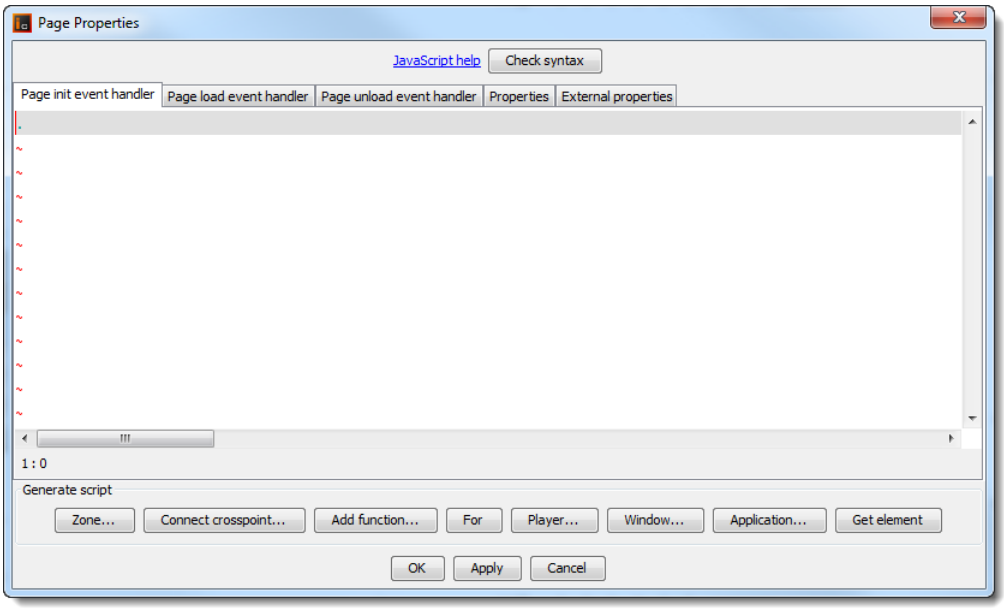
- You have opened **iC Creator** (see page 722).
- The page - whose *total full screen* dimensions you would like to edit - is in focus in **iC Creator**.

To customize the total full screen mode dimensions

1. In **iC Creator**, on the **File** menu, click **Page properties**.



SYSTEM RESPONSE: The **Page Properties** window appears.



2. Click on the **Page init event handler** tab.
3. Add the following line:

   `window.customFullscreen = "x,y,width,height";`

   where:

   - `x` is the x-coordinate of the upper-left corner
   - `y` is the y-coordinate of the upper-left corner
   - `width` is the number of pixels defining the overall width of the *total full screen* window
   - `height` is the number of pixels defining the overall height of the *total full screen* window
4. Click **OK**.

Saving Pages

Saving an Open Page

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To save an open page

- In **iC Creator**, on the **File** menu, click **Save**.

  SYSTEM RESPONSE: The open page is saved in the currently open site.

Saving an Open Page with a New Name

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To save an open page with a new name

- In **iC Creator**, on the **File** menu, point to **Save as**, and then click **Save page as**.

  System Response: The open page is saved in the currently open site.

Saving Several Open Pages

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To save several open pages

- In **iC Creator**, on the **File** menu, click **Save all**.

  System Response: The open pages are saved in the currently open site.

Opening Pages

Note: You can open as many pages as you wish in the same site.

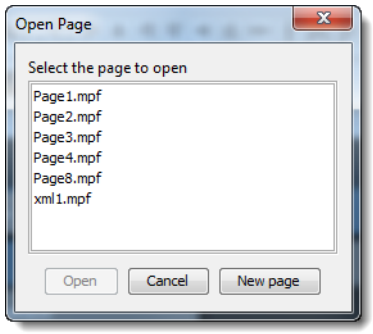
REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To open an existing page

1. In **iC Creator**, on the **File** menu, point to **Open**, and then click **Open page**.

   System Response: The **Open pages** window appears.



2. Select one of the pages that has already been created and click **Open**.

   System Response: The selected page opens in the work space.

Setting a Background for a Page

The first step in adding content to a new page is placing a background in the page. A background is a graphic file whose contents cannot be modified in **iC Creator**. The background provides an image that covers the entire page over which you can place dynamic components.

iC Creator supports the following graphic file formats for page backgrounds: GIF, JPG, and PNG.

iC Creator provides sample background image files which you may download for use in your site's pages.

IMPORTANT: If you import your own background images, do not include blank spaces or special characters in their file names.

Downloading Background Samples

REQUIREMENT

Before beginning this procedure, make sure you are logged in to iControl (see page 677).

To download background samples

1. From the *Startup* page, click **Useful Downloads**, and then click **iControl Web images**.

   SYSTEM RESPONSE: The **File Download** window appears.

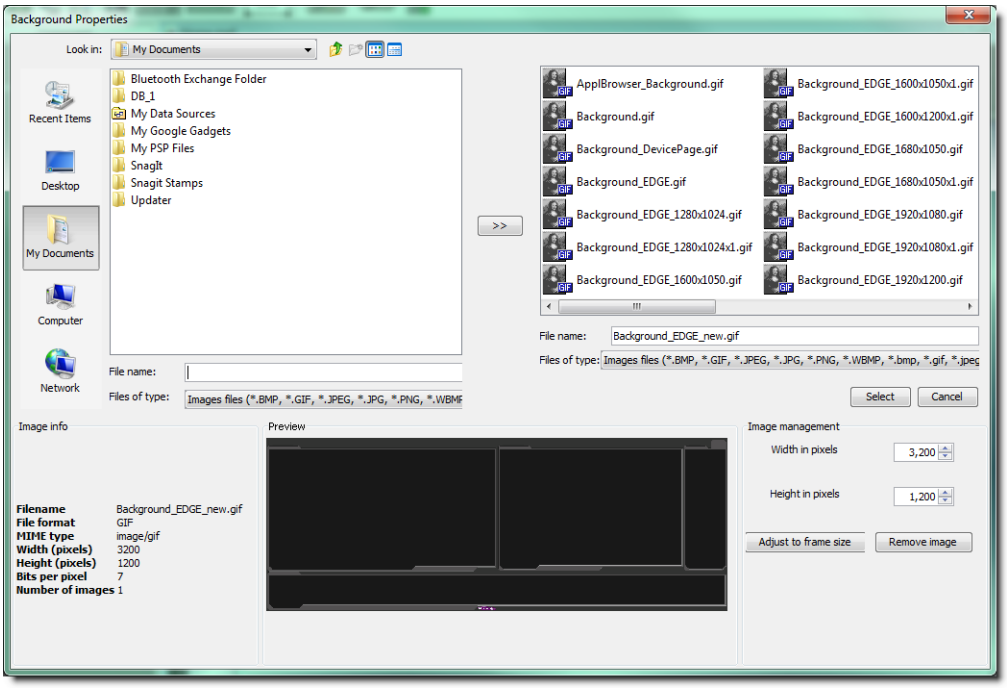
2. Save the files on your hard disk.

   Note: You will need WinZip to decompress the file.

   SYSTEM RESPONSE: When you download the background samples, the status samples for links and cross-point selectors are downloaded at the same time.

   All functions pertaining to backgrounds are handled from the **Background Properties** window.

   Note: To open the **Background Properties** window, see page 614).



Background properties window

Importing an Image File for Use as a Page Background

Once you have created a site, you will need to import graphic files to be available as backgrounds for the site. These files can be imported from other folders and directories on your hard drive, or from other computers accessible through your network connection. Your graphic arts department can create appropriate images for your site.

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To import an image file for use as a page background

1. In **iC Creator**, from the **Background images** window, use the **Search** window to navigate through your local computer and network connections to locate image files.

   SYSTEM RESPONSE: Only file types appropriate for use as a background image (i.e. GIF, JPG or PNG) will appear.

2. Select a file.

   SYSTEM RESPONSE: The **Preview** and **Image info** panels display file information.

3. Click the Double-arrow button between the **Search** and **Background Images** windows.

   SYSTEM RESPONSE: The selected image imports into the site, and will now appear in the **Background Images** window.

Adding a Page Background

The image as imported may not be sized to display at the proper scale on the page. Two sizing options are provided in the Background Size area.

To add a page background

1. In **iC Creator**, manually scale the image by resetting the height and width, expressed in pixels, using the data boxes. Scroll the value using the up and down arrows, or type a new value directly into the data box.
2. Scale the image to fit exactly onto the current page by clicking the **Adjust to frame size** button.
3. Select an image from the **Background Images** window, and then click **Select**.

   System Response: The selected image installs as the background for the current page.

Removing a Page Background

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To remove a page background

1. In **iC Creator**, open the page (see page 629).
2. Right-click anywhere in the page background (that is, not on a widget), and click **Properties**.

   System Response: The **Page properties** window appears.
3. Select the **Properties** tab near the top of the page.
4. Click **Remove** near the **File name** text box.

   System Response: The background is removed from the current page.

Using an Image in a Project

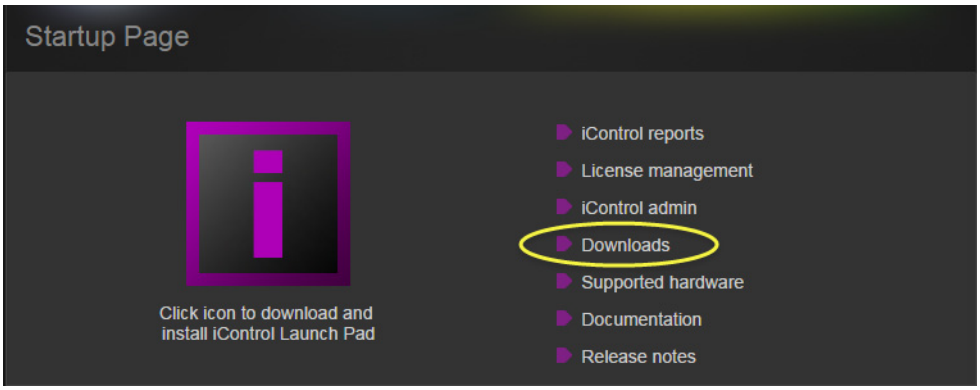
Importing iC Web Images into a Project

REQUIREMENT

Before beginning this procedure, make sure you have opened iControl (see page 677).

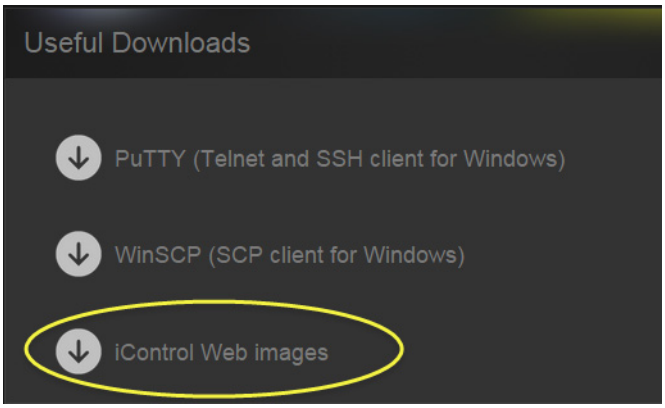
To import an iC Web image into a project

1. On the *Startup* page, click **Useful downloads**.

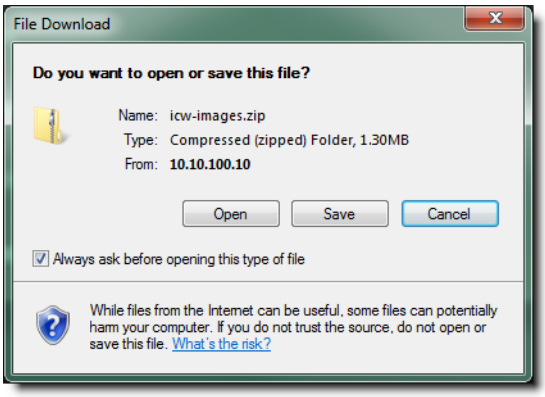


SYSTEM RESPONSE: The Useful Downloads page appears.

2. Click **iControl Web images**.

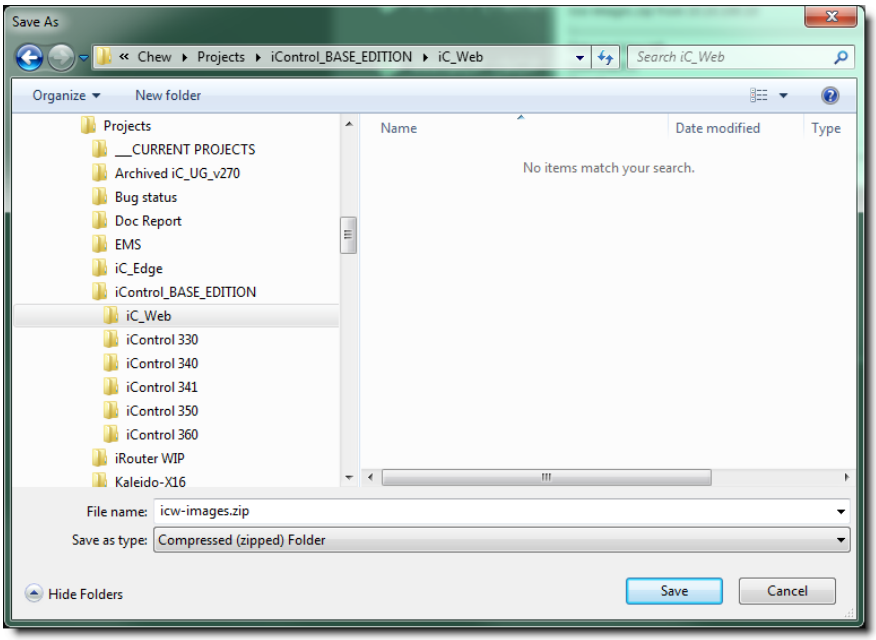


SYSTEM RESPONSE: A **File Download** confirmation window appears.



3. Click **Save**.

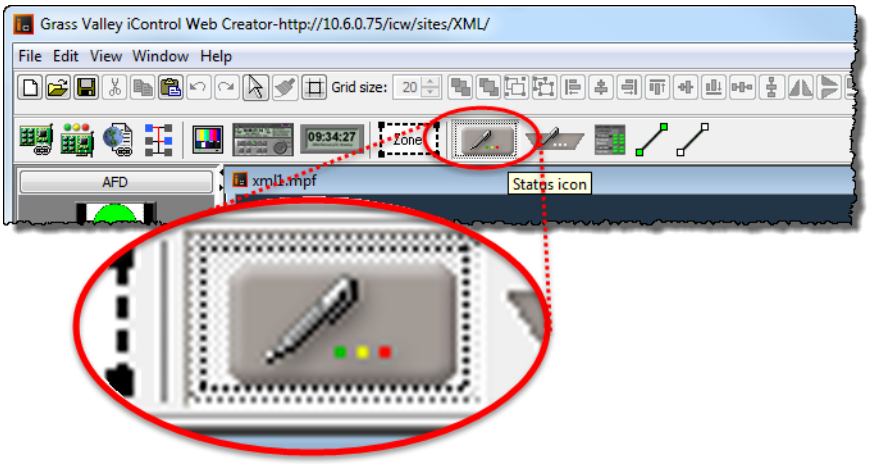
SYSTEM RESPONSE: A **Save As** window appears.



4. Browse and select an appropriate location to which you would like to save the ZIP file.
5. Click **Save**.

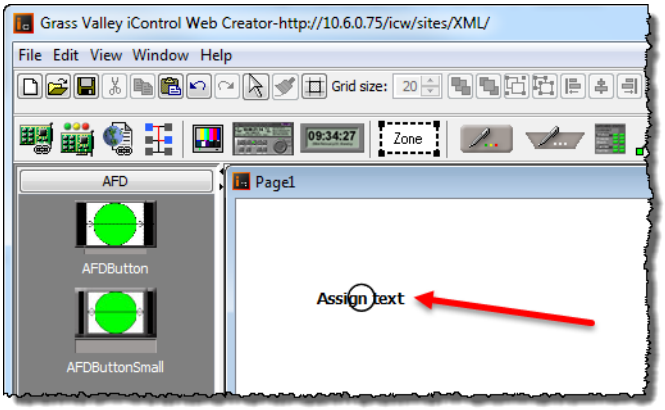
   SYSTEM RESPONSE: The file is saved to the designated location on your local computer.
6. Decompress the ZIP file.

   IMPORTANT: The ZIP file can contain many files. Make sure you decompress the `*.ZIP` file into the desired folder.
7. Open **iC Creator** (see page 722).
8. Open your project (see page 622).
9. Create a new page (see page 626).
10. In **iC Creator**, click **Status** on the toolbar.



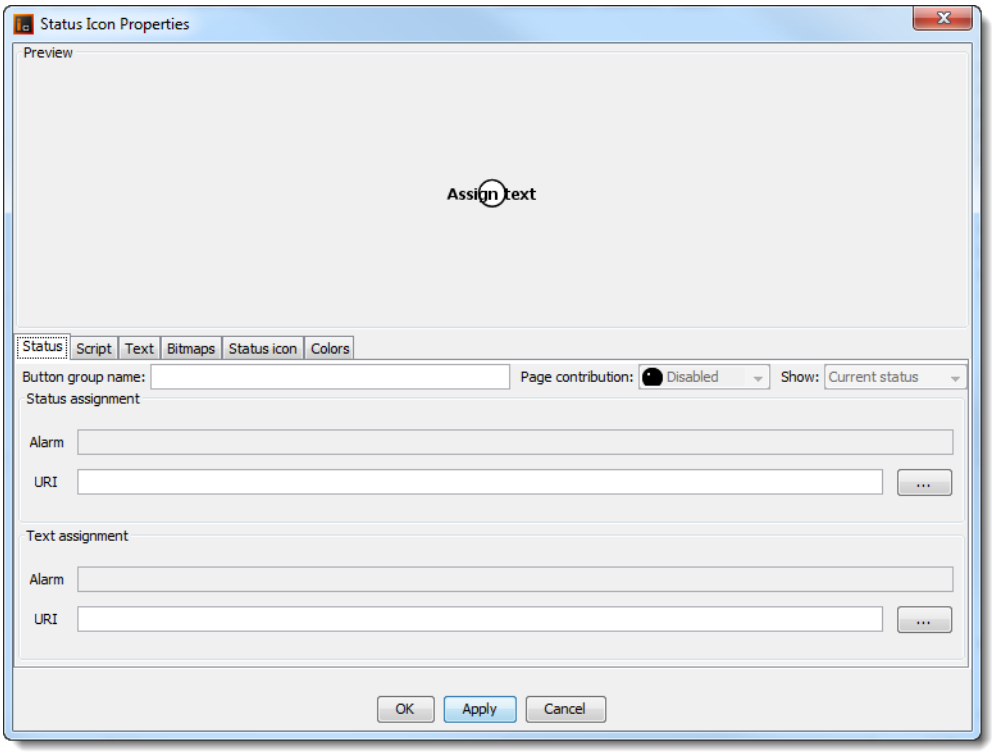
11. Click anywhere in the new page to add the icon to the page.

    SYSTEM RESPONSE: The icon appears on the page.

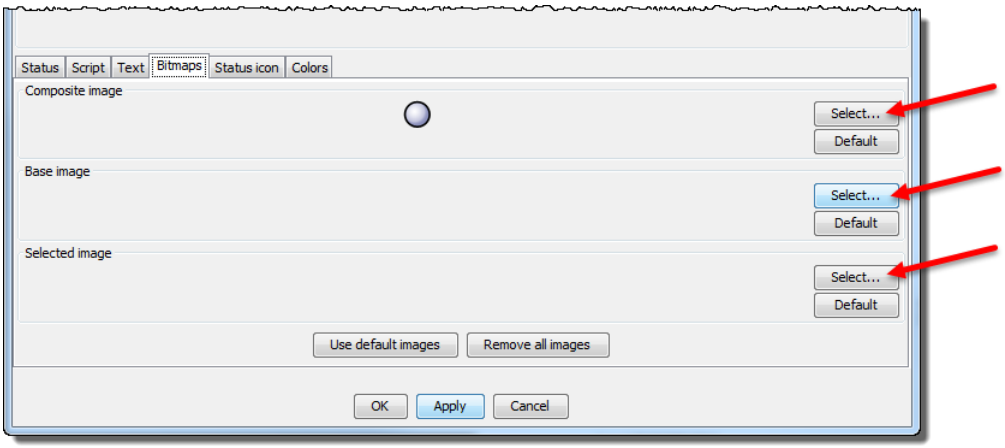


12. Double-click the icon.

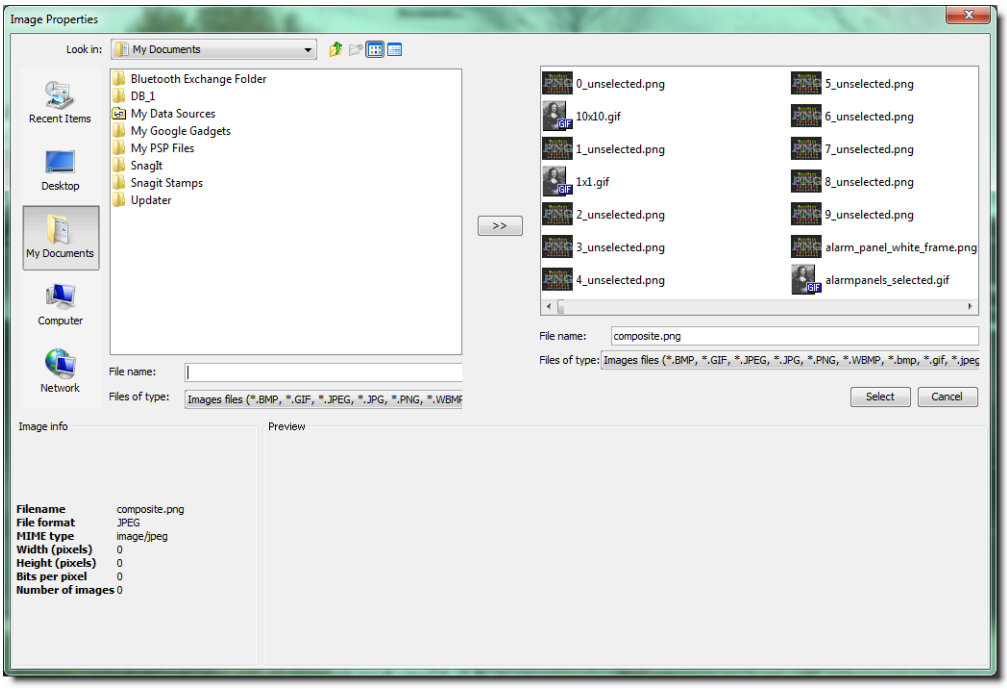
    SYSTEM RESPONSE: The **Status Icon Properties** window appears.



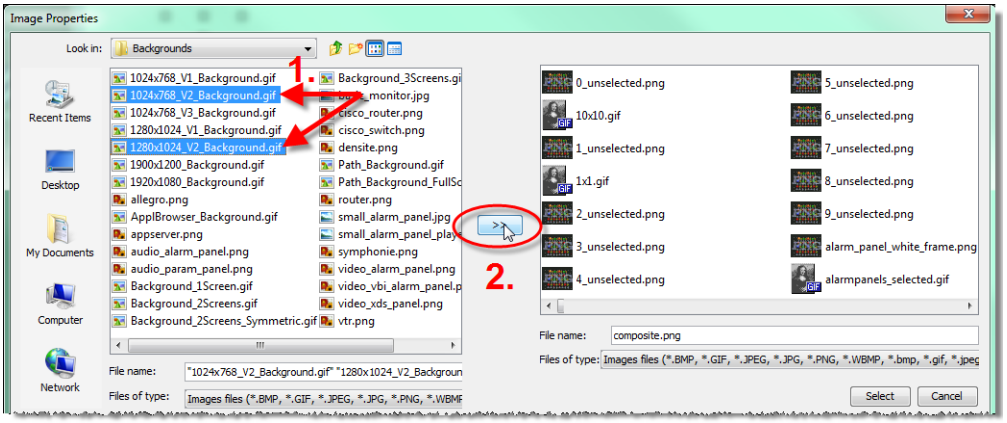
13. Select the **Bitmaps** tab.
14. Click any one of the **Select** buttons.



SYSTEM RESPONSE: The **Image Properties** window appears.



15. In the top-left box, browse to the location of the `images/link` folder you decompressed in step 6 and double-click the folder to display its contents.
16. In the images folder, select the image files you would like to import by performing **one** of the following steps, as required:
    a) If you would like to import only one image file, click on the image file.
    b) If you would like to import several image files, press (and hold) the **Ctrl** key while clicking once on each of the image files you would like to import.
    c) If you would like to import all image files in the folder, click on any one image file, and then type **Ctrl**+**A**.
17. Click the double arrow button (near the middle of the window).



SYSTEM RESPONSE: All the imported images are now part of the project and can be used at any time as needed.

> **Note:** Image files are saved inside the current project only and once imported can no longer be deleted.

The page can be now closed without saving.

Ensuring Proper GSM Operation

It is essential that the GSM is running on the same subnet as the Web site for successful operation of component links.

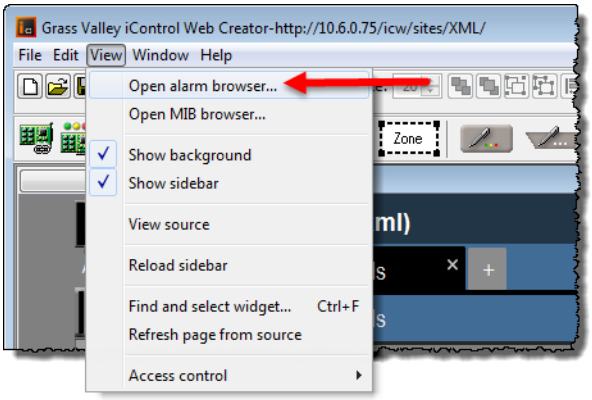
Using iC Creator to Verify GSM is Running on the Same Subnet as the Web Page

REQUIREMENT

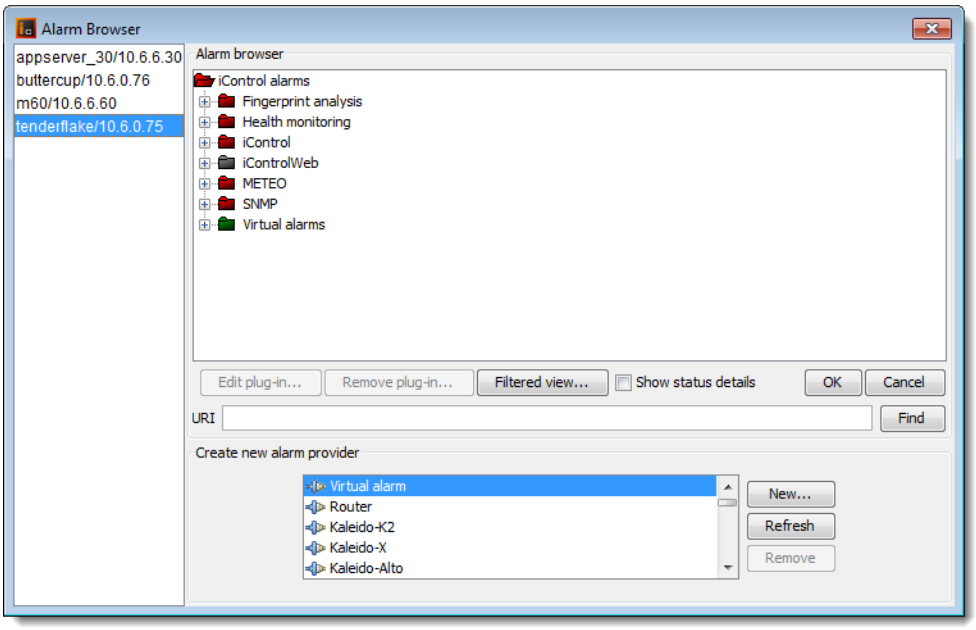
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To verify the GSM is running on the same subnet as the Web page

- In **iC Creator**, on the **View** menu, click **Open alarm browser**.



SYSTEM RESPONSE: The **Alarm Browser** window appears.



Note: As components are assigned they can be seen as additions to the tree structure.

Using iControl to Verify GSM is Running on the Same Subnet as the Web Page

REQUIREMENT

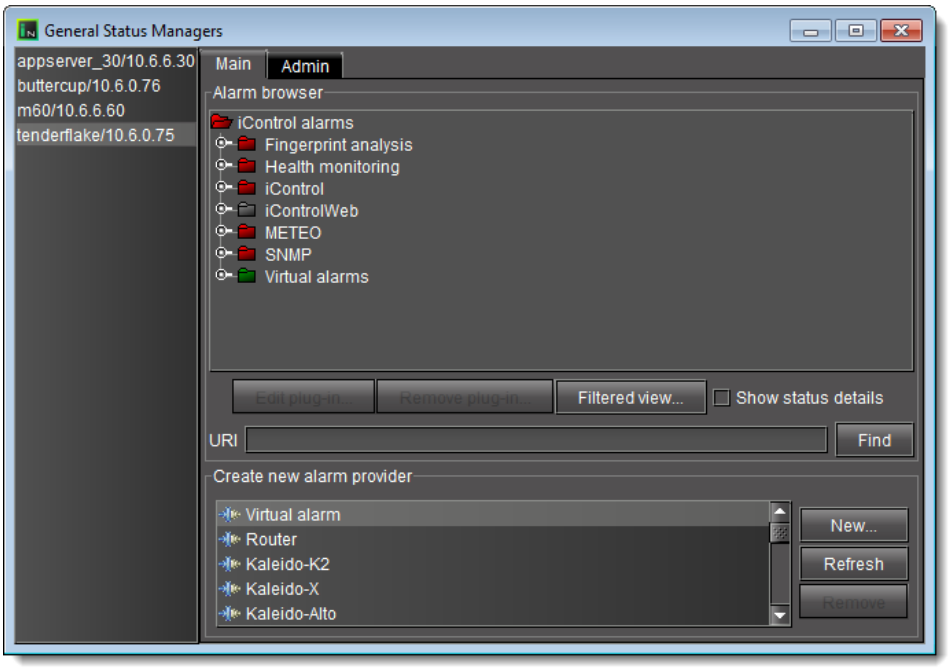
Before beginning this procedure, make sure you have opened **iC Navigator** (see page 697).

To verify the GSM is running on the same subnet as the Web page

- In **iC Navigator**, on the **View** menu, click **General status managers**.

  SYSTEM RESPONSE: The **General Status Managers** window appears.

Note: There should **NOT** be a message indicating that the GSM is not running.



Configuring Zones on a Web Page

Adding a Zone to a Web Page

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To add a zone to a Web page

1. In **iC Creator**, from the toolbar, click the **Zone** button and then from the Web page, click on the location for the zone.
2. Double-click on the zone.

   System Response: The **Property** window appears.
3. Specify the size, zone name, and initial value (content) of the zone.

   System Response: The zone appears empty.

Note: At run time, the zone appears with the initial content as specified in the zone properties: a service panel, page global log viewer, **iC Navigator**, VNC viewer, or a Web browser.

Defining Zone Properties

To define zone properties

- Consult the table, below.

Zone	fields to complete
Object Properties Tabs	description and explanation
Size	Size: Width, Height Position: X, Y
Initial value	content of the zone
Zone name	the ID used in the scripts to refer to the zone

Adding a Component to a Web Page

The following components are only available to maintain compatibility with version 1.7:

- Link to device
- Status inspector
- Link to page
- Crosspoint Selector.

The same functionality is available within the *Status* Icon component.

Adding a Graphical Element to a Web Page

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To add a graphical element to a Web page

1. In **iC Creator**, on the main window, click on a component icon and then from the Web page, click on the location for the component.

   SYSTEM RESPONSE: The new graphical element appears at the specified location.

   Note: Some of the device's properties will automatically be set when using this method.

2. Resize the graphical element with the image handles.

Resizing a Web Page's Graphical Object

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To resize a Web page's graphical object

1. In **iC Creator**, click the graphical element.
2. From the Web page, click on the location for the component.

3. Drag and drop the selected component to a specific position on the Web page.

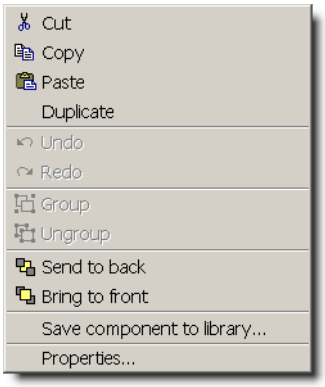
   SYSTEM RESPONSE: The graphical element for the new component appears at the specified location.

Shortcuts to Positioning a Web Page's Graphical Object

Shortcuts to positioning a Web page's graphical object

- In **iC Creator**, right-click the graphical element for a component.

  SYSTEM RESPONSE: A menu appears.



To do this...	...do this...
Erase all selected items in a page.	In **iC Creator**'s main menu, point to **Edit**, and then click **Cut**.
	In **iC Creator**'s standard toolbar, click **Cut**.
	In **iC Creator**'s standard toolbar, click **Delete**.
Copy all selected items.[1]	In the main menu, point to **Edit**, and then click **Copy**.
	In the standard toolbar, click **Copy**.
Paste all previously copied or cut items.[2]	In the main menu, point to **Edit**, and then click **Paste**.
	In the standard toolbar, click **Paste**.
Duplicate and paste all selected items.	In the main menu, point to **Edit**, and then click **Duplicate**.
Group all selected items.	In the main menu, click and drag over the area containing the items for the group, point to **Edit**, and then click **Group**.
Ungroup all previously grouped items.	In the main menu, point to **Edit**, and then click **Ungroup**.
Copy the graphic attributes from one item to another item.	In the standard toolbar, click **Copy Attribute (Brush)**.
Position a selected item behind all other items.	On the main menu, point to **Edit**, and then click **Send to back**.
	On the standard toolbar, click **Send to back**.

(*Continued*)

To do this...	...do this...
Position a selected item in front of all other items.	On the main menu, point to **Edit**, and then click **Bring to front**.
	On the standard toolbar, click **Bring to front**.
Resize a graphical object located on a page.	On **iC Creator**'s main pane, click and drag the sizing handle of the component until the desired object size is achieved.

1. Copied components exactly replicate the originating component where the new graphical object and object properties are identical to the original.
2. This is useful when copying and pasting from one page to the next.

Setting the Properties for a Web Page Graphical Component

Note: The **Object properties** window is different for each type of component.

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To set the properties for a Web page graphical component

- In **iC Creator**, double-click the graphical element.

  SYSTEM RESPONSE: The left-most tab of the component's **Object properties** window appears.

Creating lines in iC Creator

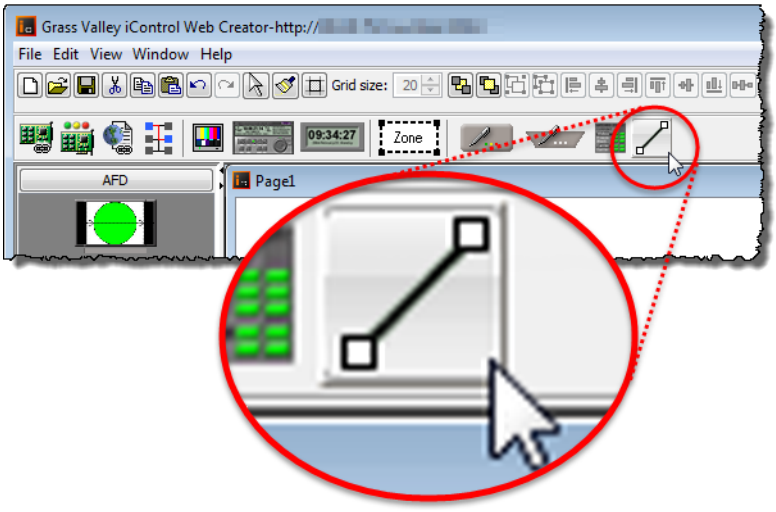
Creating a simple line

REQUIREMENT

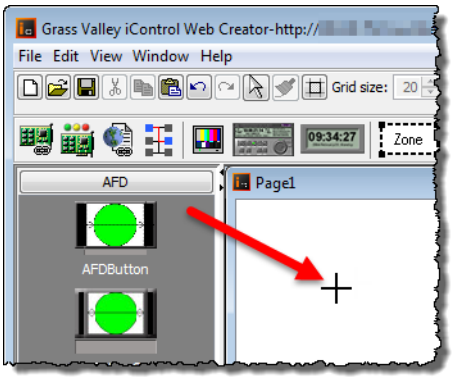
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To create a line in iC Creator

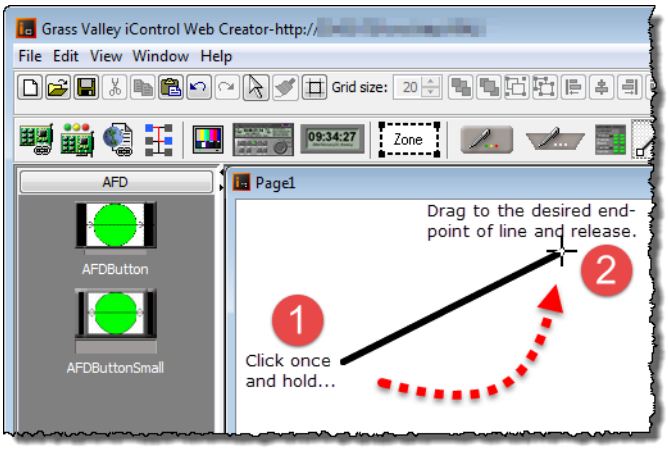
1. In **iC Creator**, click the line tool icon.



2. Position the cursor at the location on your page where you would like to start drawing a line.



3. Click and hold while dragging the mouse to the desired end-location of the line, and then release.



Creating Control Points on a Line

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have iC Creator open (see page 722).
- You have a line.

To create a control point on a line

- Press and hold the **Shift** key while clicking the point along the length of your line where you would like to create a control point.

Making a Line Vertical or Horizontal

REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have iC Creator open (see page 722).
- You have a line.
- You understand the behavior of the line tool rotation feature (see Change of Line-Segment Orientation, on page 617).

To make a line vertical or horizontal

1. In **iC Creator**, move the cursor to the end of the line you would like to move.
2. Press and hold the **Ctrl** key while clicking the end point.

   System Response: The line (or line segment) pivots around an adjacent point to either a vertical or horizontal orientation (whichever rotation requires the least rotational movement).

12 Alarm Panel Templates

Detailed Directions

Creating an Alarm Panel Template

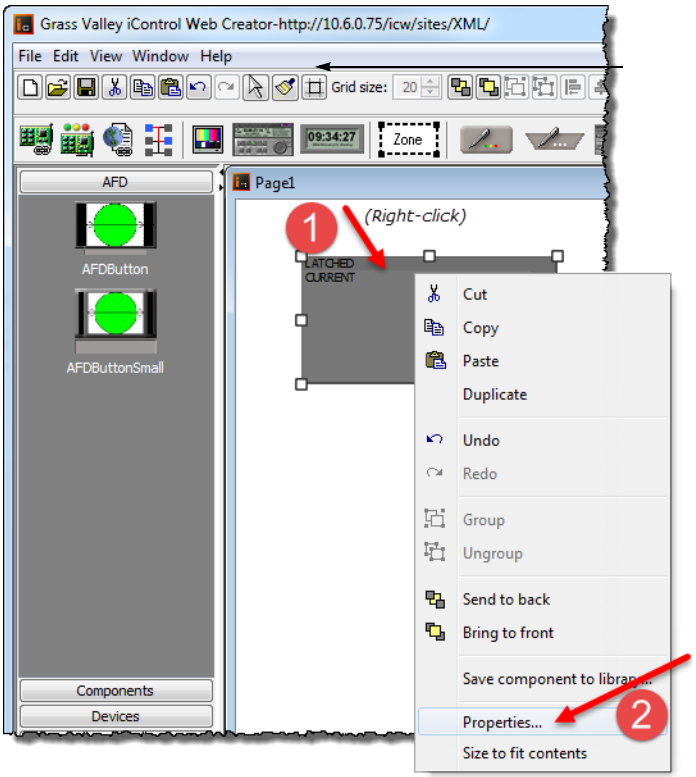
The following procedures demonstrate how to create an alarm panel template, how to save the template as a widget, and how to use the widget to build Web pages with multiple alarm panels.

REQUIREMENT

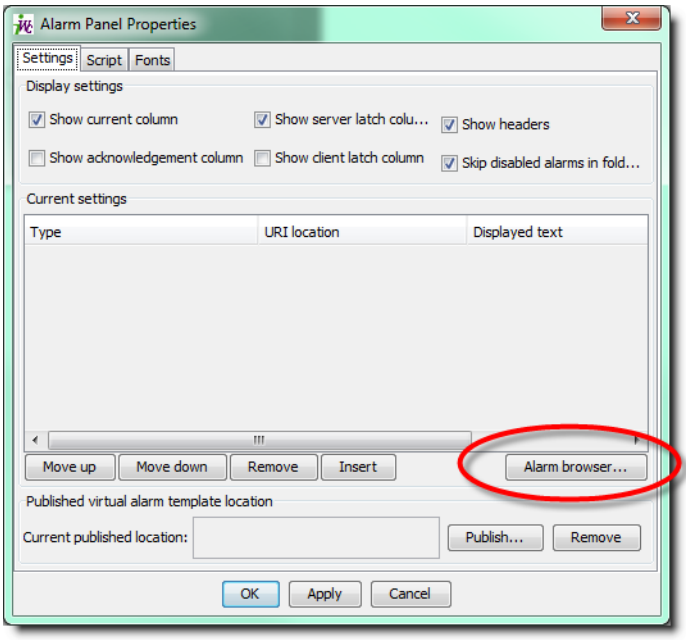
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To create an alarm panel template

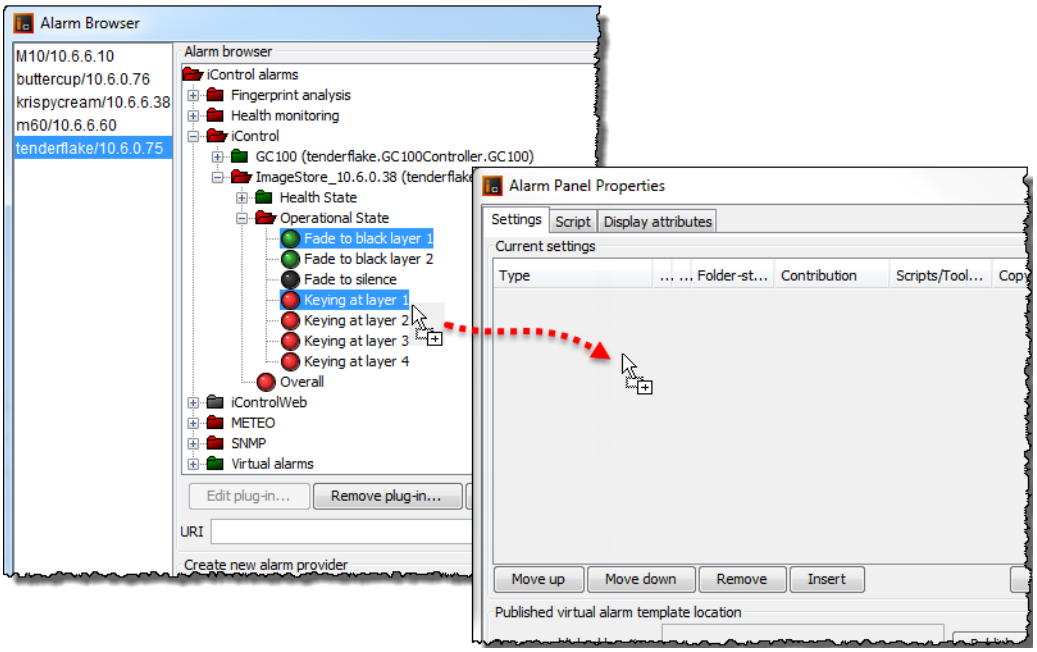
1. In **iC Creator**, draw an alarm panel.
2. Right-click the panel and click **Properties**.

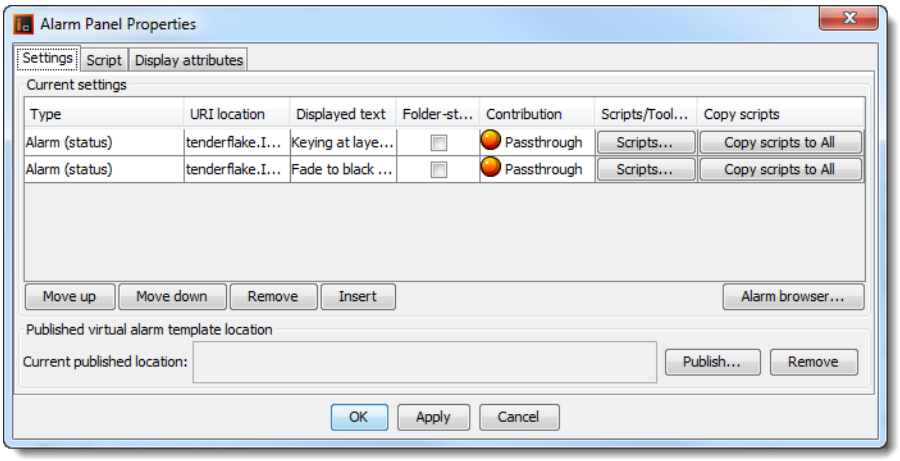


3. In the **Alarm panel properties** window, click **Alarm browser**.



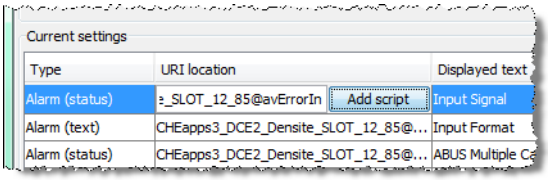
4. In the **Alarm browser** window, find a group of cards or devices for which you wish to create an alarm panel template.
5. Select the alarms of interest (individually, or an entire folder) from one card or device in the targeted group.
6. Drag the alarms from the Alarm browser window into the **Alarm panel properties** window.





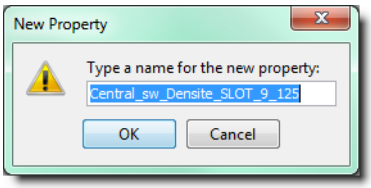
Note: Drag a folder to copy its alarms to the **Properties** panel. Hold down the **Ctrl** key as you are dragging a folder to copy the alarms into all of its sub-folders as well.

7. Click the URI location of one of the alarms.



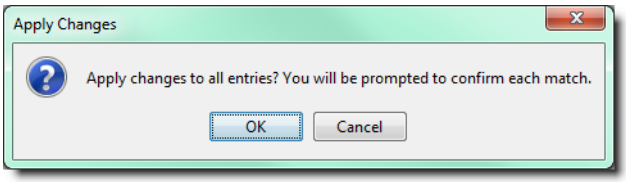
System Response: The URI becomes editable.

8. Select the portion of the URI location that you wish to use as a template pattern, and then click **Add script**.
9. In the **Enter new property name** window, type a descriptive name, and then click **OK**.

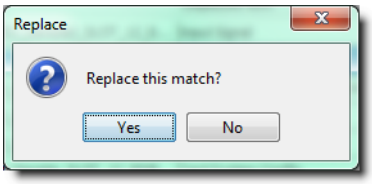


System Response: The Apply Changes window appears.

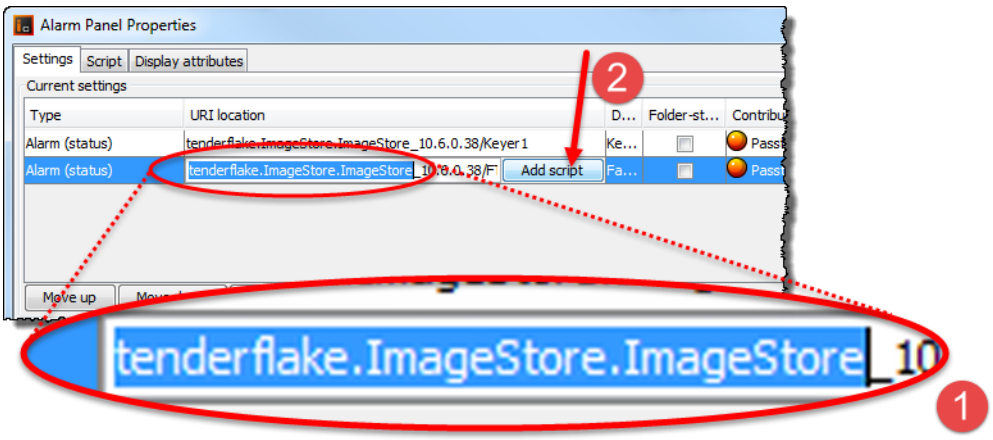
10. In the **Apply changes** window, click **OK**.



11. For each alarm, click **Yes** when prompted to replace the match.

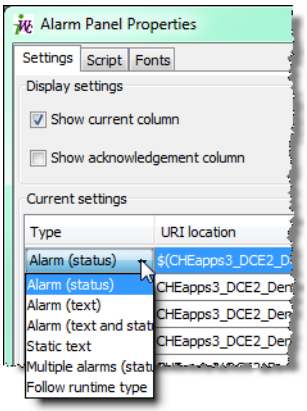


SYSTEM RESPONSE: In the **Alarm properties** window, the variable name you typed in step 9 replaces the corresponding portion of the URI location.



The portion of the URI you selected is replaced by a variable based on the name you provided.

12. You can refine the appearance of the alarm panel by clicking on the **Type** for each URI, and choosing a value (described in the table below) from the drop-down menu.

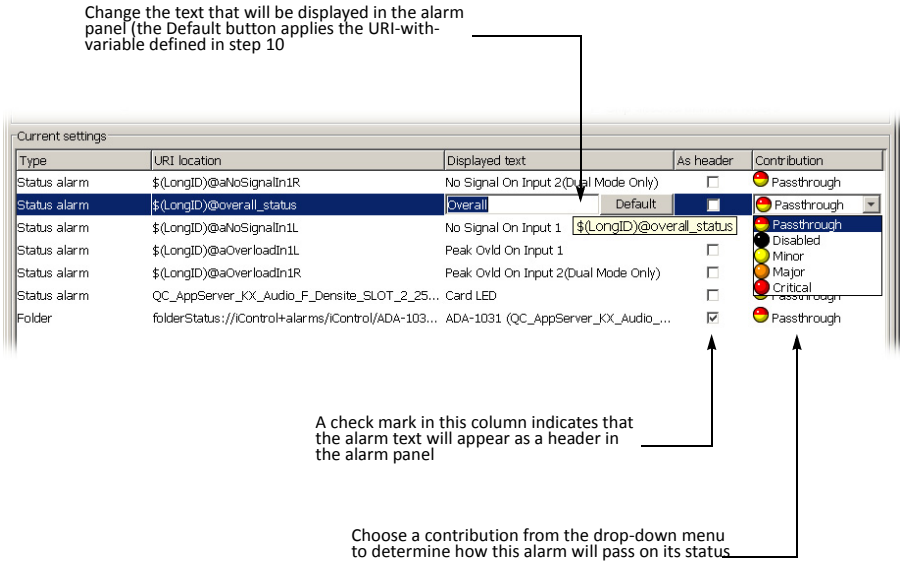


Status alarm	displays the status of a URI

(*Continued*)

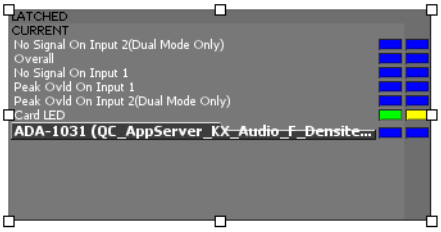
Folder	displays the status of a folder, and any alarms within the folder (in the runtime panel only —not in the properties window)
Folder as text	same as Folder without the status LEDs
Text alarm	displays the text value of a URI
Text and status alarm	displays both text and alarm values of a URI
Follow runtime type	attempts to determine the type of the URI at runtime, and create the appropriate entry
As title text	useful for typing lines of text for titles
Compressed alarms	displays multiple URIs (up to 4) side by side with smaller LEDs (useful for audio alarms)

You can also change the alarm's text, how it appears, and its contribution to higher-level alarms.



13. Click **OK** in the **Alarm properties** window.

    SYSTEM RESPONSE: The alarm panel in **iC Creator** is updated to display the selected alarms.



SYSTEM RESPONSE: At first, **iC Creator** assumes the value of the URI location variable to be the default (i.e., the text string you selected and replaced in step 7 to step 10). If you publish and view this page, the alarm statuses will be based on the default URI.

Working with Alarm Panel Templates & Widgets

While an alarm panel template, once created, can simply be copied and pasted into various Web pages, a better way to use such as template is to convert it to a widget.

Converting an Alarm Panel Template into a Widget

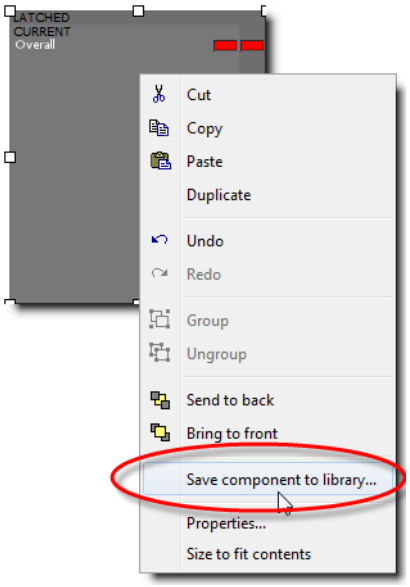
Alarm panel templates can be reused, any number of times, on any **iC Web** page. In **iC Creator**, you can convert an alarm panel template into a component, or *widget,* to provide convenient access.

REQUIREMENT

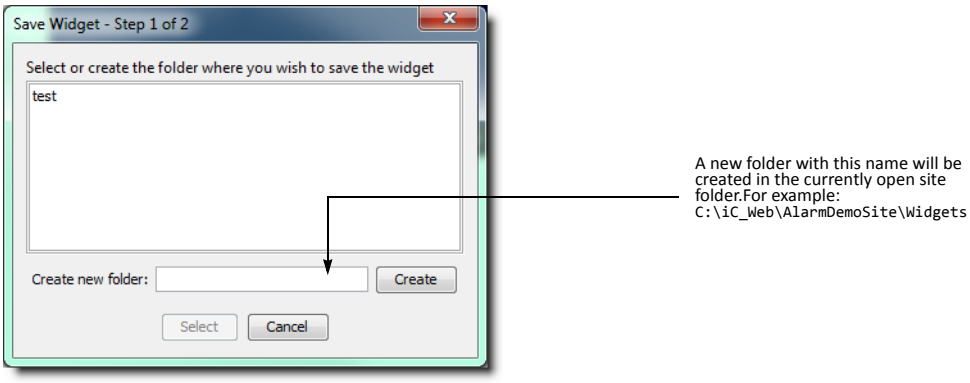
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To turn your alarm panel template into a widget

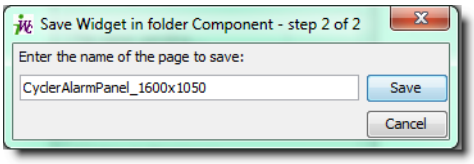
1. Right click the alarm panel template, and click **Save component to library**.



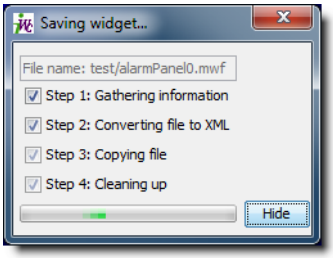
2. Select an existing folder, or create a new one, into which to save the new widget.



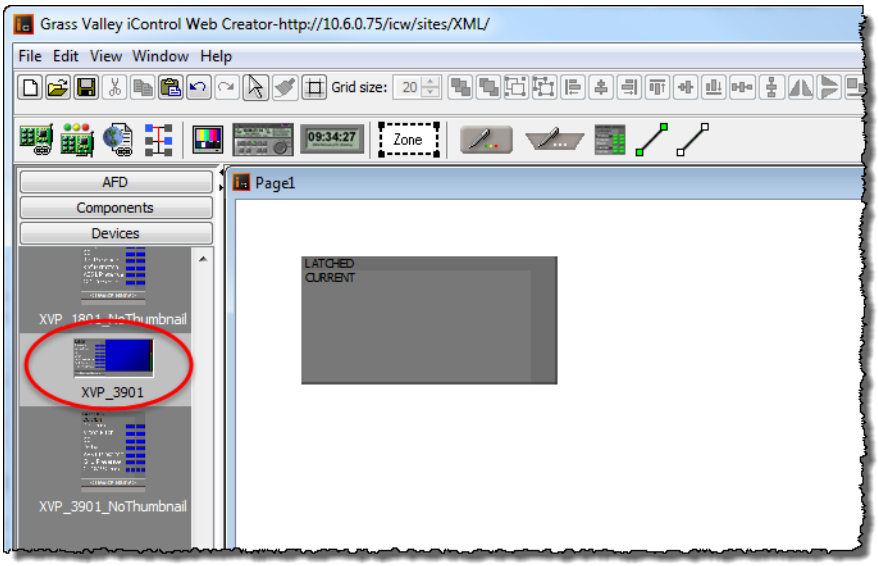
3. Type a descriptive name for the widget, and then click **Save**.



SYSTEM RESPONSE: A progress window appears.



SYSTEM RESPONSE: A button with a thumbnail and the name of the new widget appears in the sidebar of **iC Creator**.



Using an Alarm Panel Template Widget

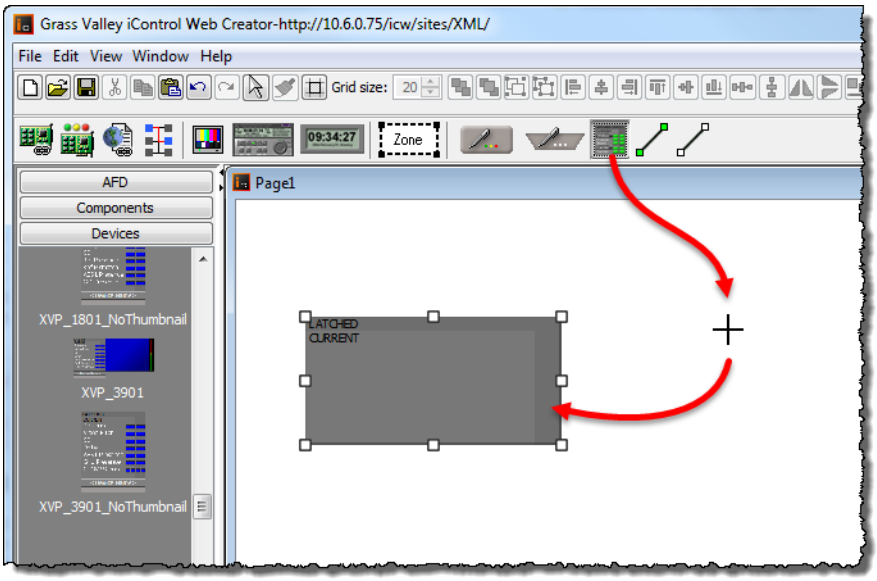
Once saved as a widget, alarm panel templates are readily available any time you open **iC Creator**, and can be used to quickly create Web layouts with many similar but unique alarm panels.

REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To use your alarm panel template widget on a Web page

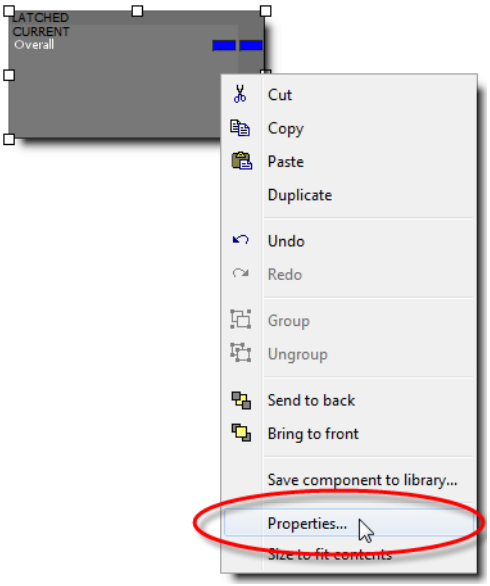
1. Open an existing Web page or create a new one.
2. Click the alarm panel template widget.



SYSTEM RESPONSE: The cursor changes to a crosshair.

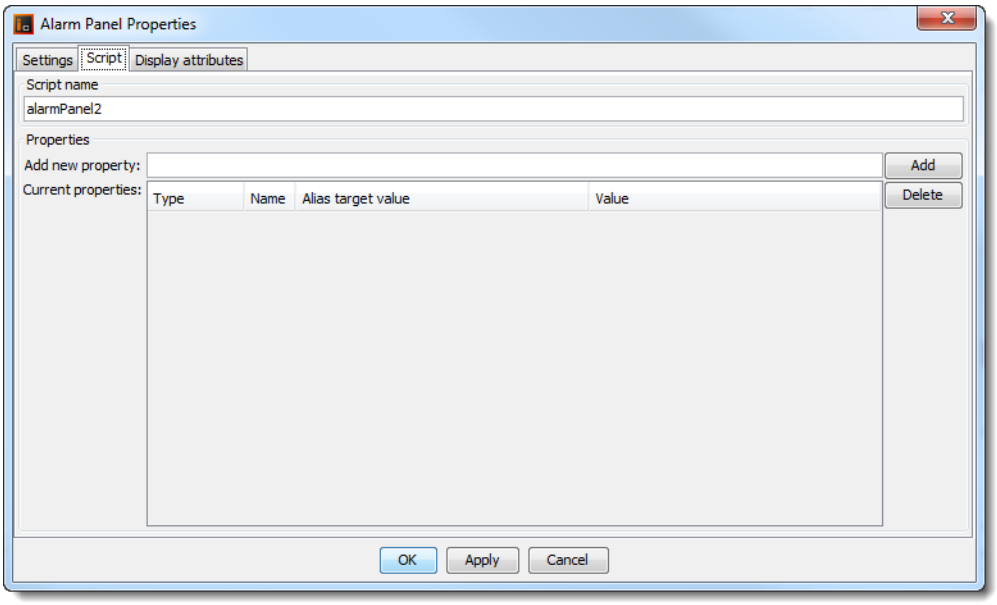
3. Draw as many new alarm panels as you need to complete your design.

   Each of the panels you draw has the same properties as the original widget. To customize a panel, right-click on it and select **Properties**.



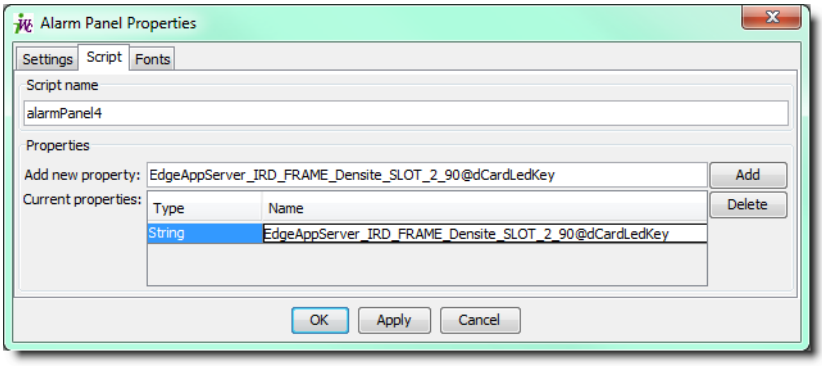
4. In the **Alarm panel properties** window, click the **Script** tab

> **Note:** The panel has the same variable name(s) and default value(s) as the original widget.

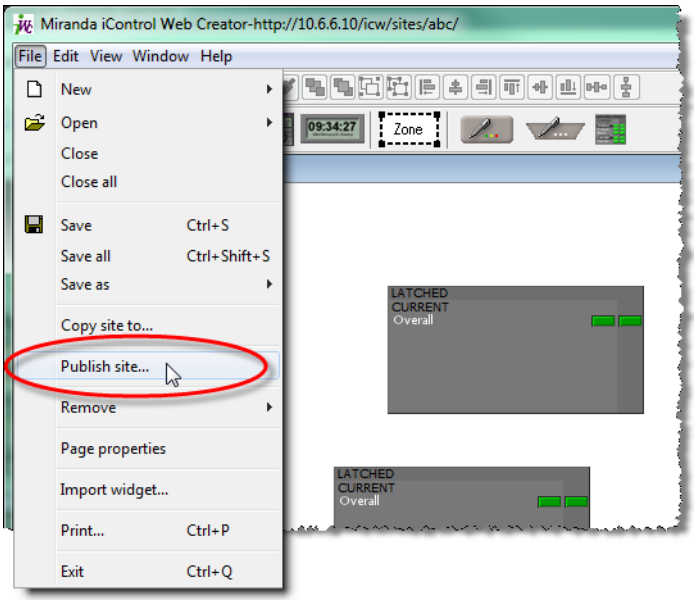


5. Change all or part of the default value.

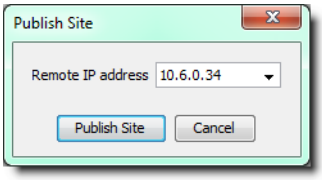
> **Note:** This new value will be applied to all of the alarms associated with the panel (i.e. the variable portion of each alarm URI will take on the new default value).



6. Continue drawing panels and modifying their properties as needed. When you have finished, save the page, and then choose **Publish site** from the **File** menu.

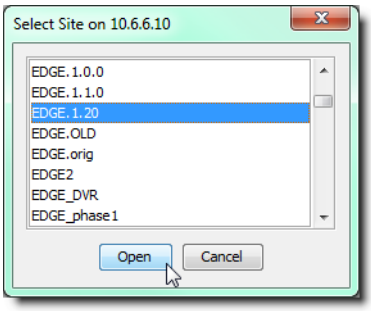


7. When prompted, type the IP address of the Application Server to which you would like to publish your **iC Web** site (including the page with the new alarm panels).

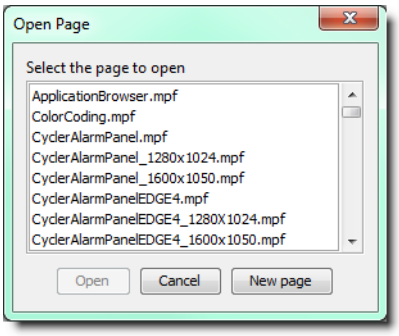


To view the Web page with the new alarms panels

1. Open **iC Web** from the *Startup* page of the Application Server to which you published the site (see page 718).
2. On the **File** menu, click **Open site**.
3. Select the site that contains the new alarm panel page, and then click **Open**.



4. Select the page that contains the new alarm panels, and then click **Open**.



SYSTEM RESPONSE: The selected Web page appears, with the new alarm panels displaying their current alarm statuses.

Modifying an Alarm Panel Widget

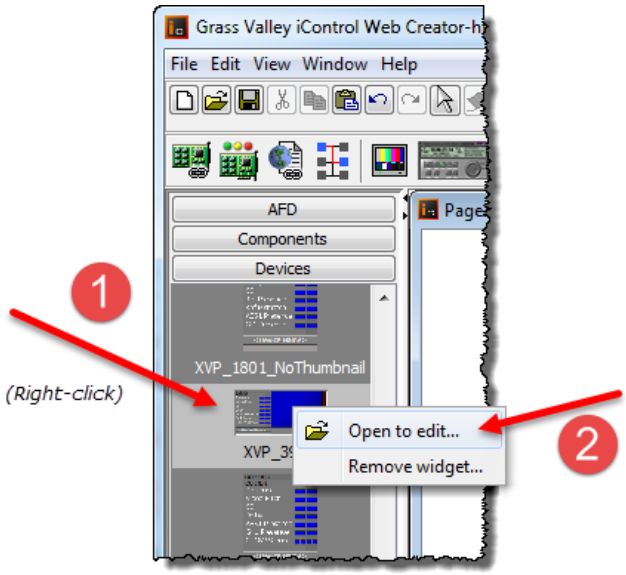
Another useful characteristic of alarm panel (or any other) widgets is that they can be modified at any time, and the modifications can be applied to all the alarm panels on a Web page derived from that widget.

REQUIREMENT

Before beginning this procedure, make sure you have opened iC Creator (see page 722).

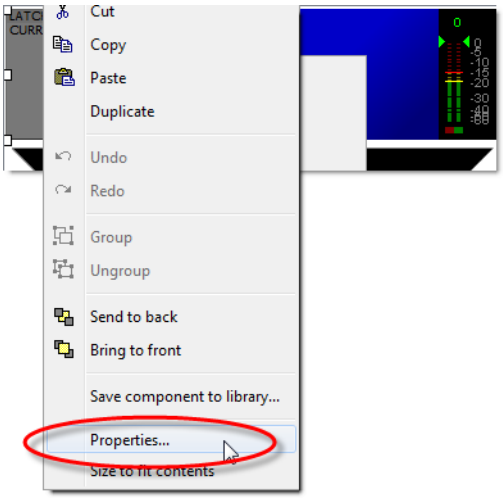
To modify the properties of an alarm panel widget, and apply the modifications to a Web page

1. Open a Web page containing alarm panels that were created using the widget you wish to modify. Right-click the alarm panel widget, and click **Open to edit**.

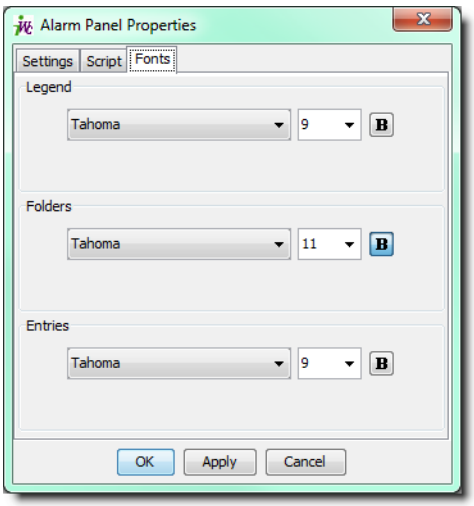


SYSTEM RESPONSE: The page saved with the original alarm panel widget appears.

2. Right-click the alarm panel template, and then click **Properties**.



3. Modify the properties of the alarm panel template as needed.



4. When you have finished modifying the properties, click **OK**.
   SYSTEM RESPONSE: The changes you made will appear in the alarm panel template.
5. On the **File** menu, click **Save**.
6. If prompted, click **Yes** to save the changes to the alarm panel widget.

13 Widget Library

Overview

Widgets are graphical elements that are used on an **iC Web** page to represent devices, alarm panels, sources, routers and other parts of a signal path or site layout.

A collection of widgets resides on the Application Server (as of iControl 3.20) in a special **iC Web** site folder named `WidgetsLibrary`. The library is divided into folders that group the widgets by type. You can browse the library and import any number of widgets into another Web site.

For a complete list of widgets in the library, as well as a description of their properties, please refer to the iControl Widget User Guide, available from the Documentation page of any Application Server (iControl 3.20 or later).

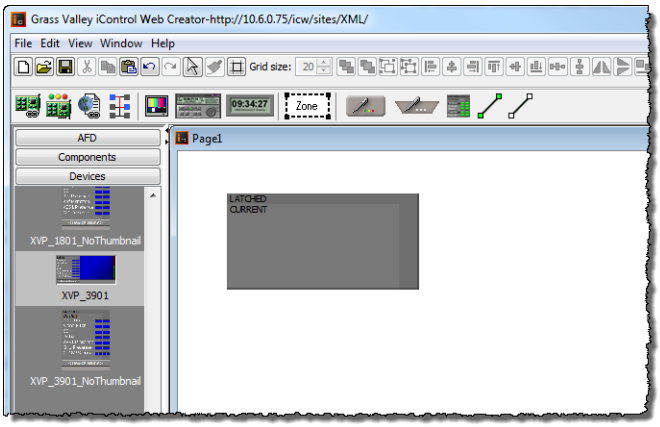
> **Note:** Even though *WidgetsLibrary* is an **iC Web** site, we recommend that you do not open and edit this site in **iC Creator**. Instead, use the procedure described below to import copies of widgets into other sites

Importing Widgets into an iC Web Site

> **REQUIREMENT**
>
> Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

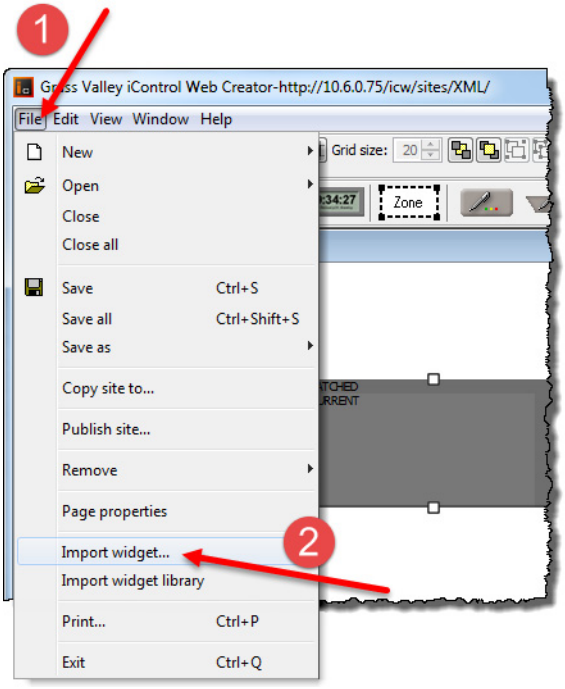
To import one or more widgets into an iControl Web site

1. In **iC Creator**, open an existing site, or create a new one.

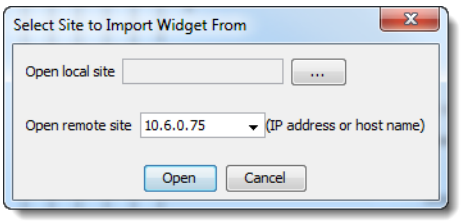


Note: You can import widgets into a site at any time.

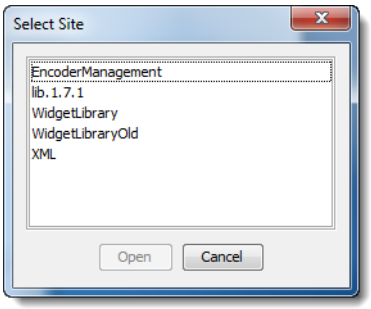
2. On the **File** menu, click **Import widget**.



3. In the **Select site to import widget from** window, type the IP address of an Application Server running iControl 3.20 or later.



4. Select **WidgetLibrary** from the list, and then click **Open**.

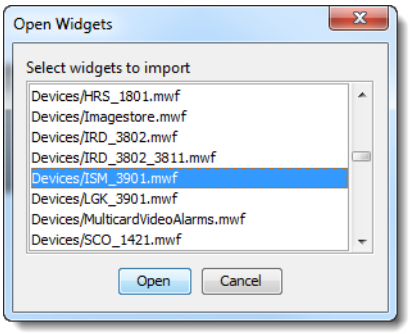


5. In the **Open widgets** window, select the widget(s) you wish to import.

   TIP: Hold down the **Shift** key and click to select multiple widgets. Hold down the **Ctrl** key and click to make a non-contiguous selection.

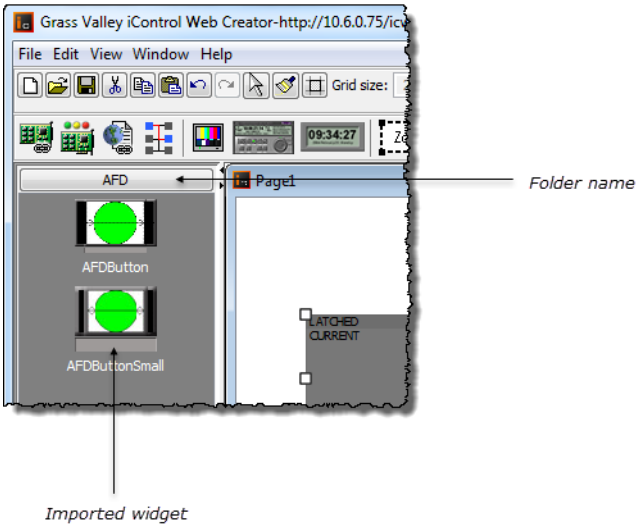
6. Click **Open**.

7. Choose an existing folder into which to import the selected widget(s), and then click **Open**. Alternatively, create a new folder by typing a name in the field provided, and then clicking **Create**.



If this list is empty, you must create a new folder in order to import the selected widget(s).

SYSTEM RESPONSE: Thumbnails of the imported widgets appear in the sidebar of **iC Creator**, grouped according to the folders into which they were imported.



Note: When a widget is imported from the WidgetsLibrary site, the source folder is not automatically created in the target Web site.

Listing and Locating Widgets in Use on a Web Page

You can find the widgets currently being used on a page by listing them and selecting them.

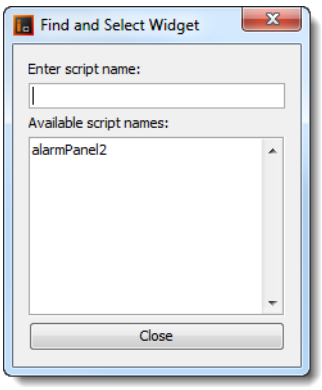
REQUIREMENT

Before beginning this procedure, make sure a page is open in **iC Creator** (see page 722).

To find and list widgets currently in use on a page

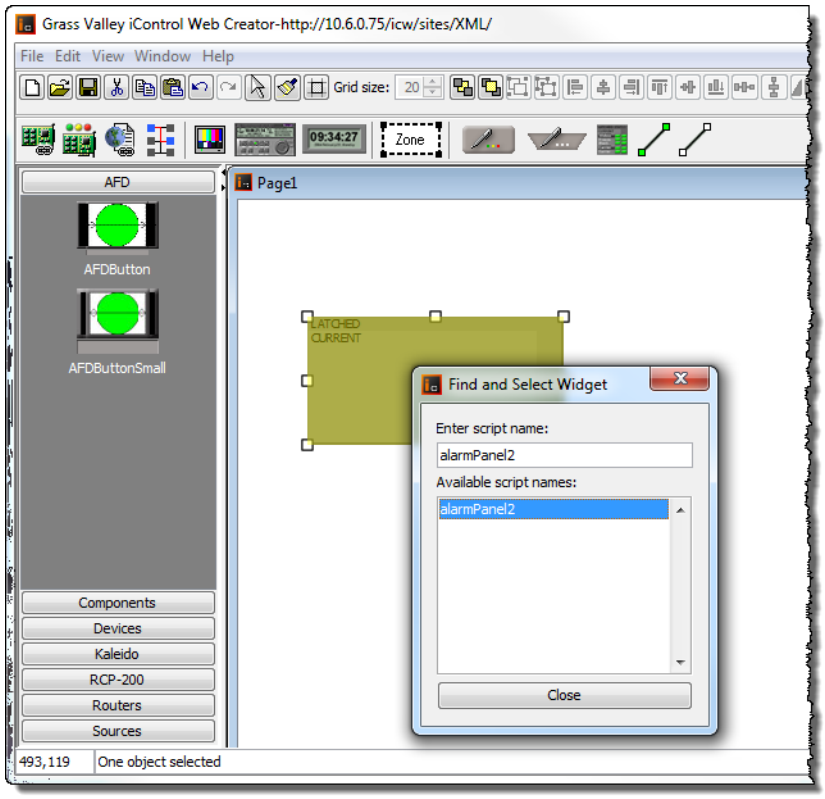
1. With **iC Creator** in focus, type **Ctrl**+**F**.

   SYSTEM RESPONSE: The **Find and Select Widget** window appears, listing alphabetically the widgets currently in use on the page.



2. To locate a particular widget on the page by name, find the widget in the list and then select it.

   SYSTEM RESPONSE: The selected widget becomes highlighted in yellow.



3. To locate several widgets on the page by name, find the widgets in the list and then **Ctrl**-select each widget individually.

> **Note:** Alternatively, if you would like to select several widgets listed contiguously, select the first in the series and then **Shift**-select the last in the series.

SYSTEM RESPONSE: The selected widgets become highlighted in yellow.

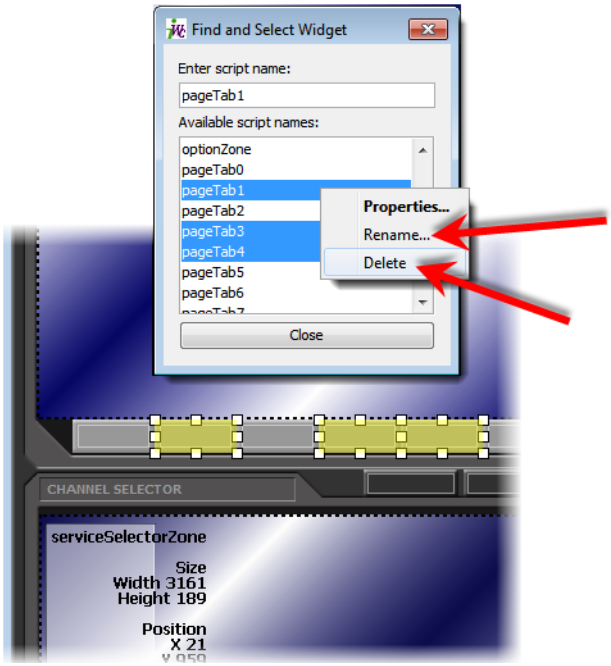
Deleting or Renaming One or More Widgets on a Web Page

REQUIREMENT

Before beginning this procedure, make sure you have selected the widgets you would like to delete or rename in **iC Creator**'s **Find and Select Widget** window (see Listing and Locating Widgets in Use on a Web Page, on page 663).

To delete or rename one or more widgets on a Web page

1. With the **Find and Select Widget** window in focus, make sure the widgets you would like to delete (or rename) are selected.
2. Right-click one of the selected widgets in the list, and then click either **Rename** or **Delete**, as required.



Using a Widget on a Web Page

Note: For illustrative purposes, this procedure describes how to use an alarm panel widget for a specific card type. Keep in mind that while the procedure applies to all widget types, in practice properties vary from one widget to another.

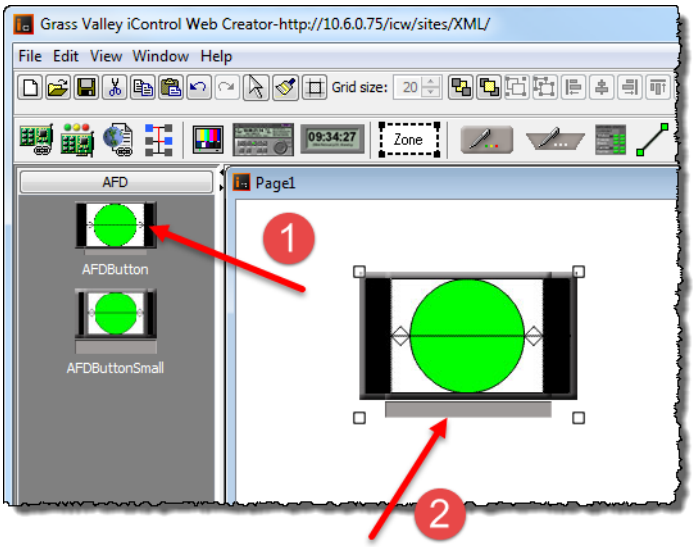
REQUIREMENT

Before beginning this procedure, make sure you have opened **iC Creator** (see page 722).

To use a widget on a Web page

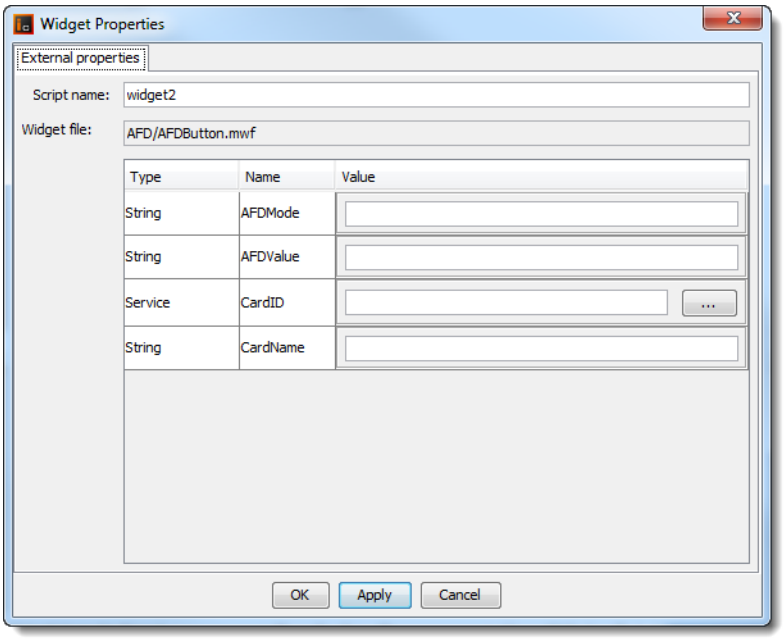
1. In **iC Creator**, click on a widget in the sidebar, and then click the Web page.

   SYSTEM RESPONSE: A copy of the widget appears.

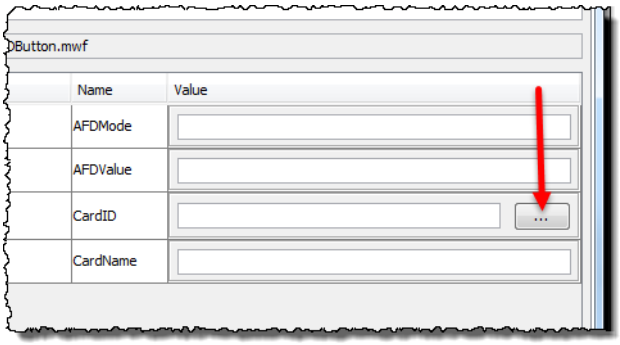


2. Double-click the widget.

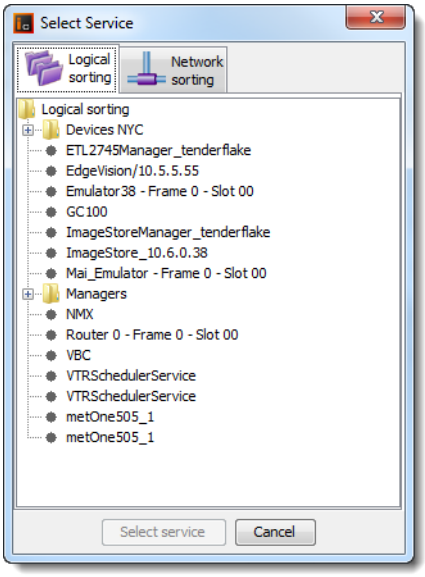
   SYSTEM RESPONSE: The **Widget Properties** window appears.



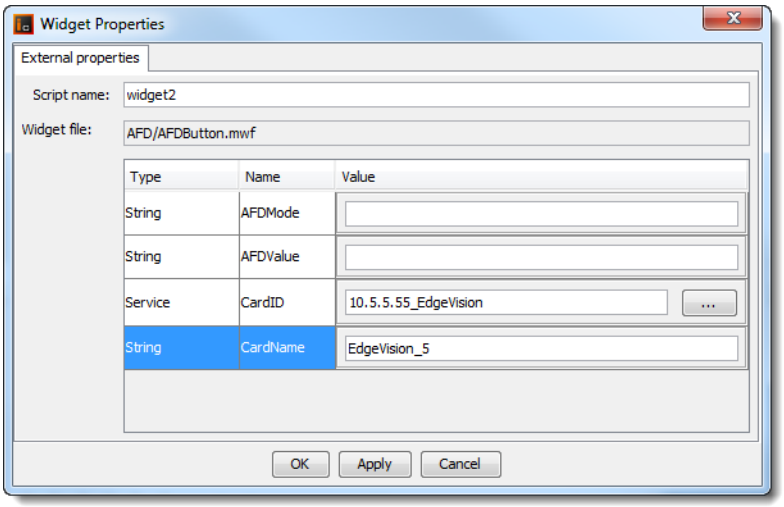
3. Click **Browse** beside the **CardID** field.



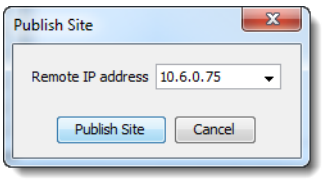
4. In the **Select service** window, click a service to assign to the widget, and then click **Select service**.



5. Type a name for the service in the **CardName** field, and then, if available, type a name for the channel associated with the card in the **ChannelName** field.



6. Click **OK**.
7. On the **File** menu, click **Save**, and then click **Publish site**.
8. In the **Publish site** window, type the IP address of an Application Server, and then click **Publish site**.



9. Open **iC Web** (see page 718).
10. Open the page you published in step 7.

    SYSTEM RESPONSE: The widget displays the live alarm statuses for the card you assigned to it in step 4.

A Common Tasks

Summary

Reaching Technical Support

If ever you need to contact Grass Valley Technical Support, you can navigate to the *Contacts and snapshots* page in iControl. Frequently, Grass Valley Technical Support will request a system snapshot of your Application Server in order to better troubleshoot any problems you may have. The *Contacts and snapshots* page allows you to do this.

- Opening the Contacts and snapshots Page on page 671
- Creating a System Snapshot on page 673

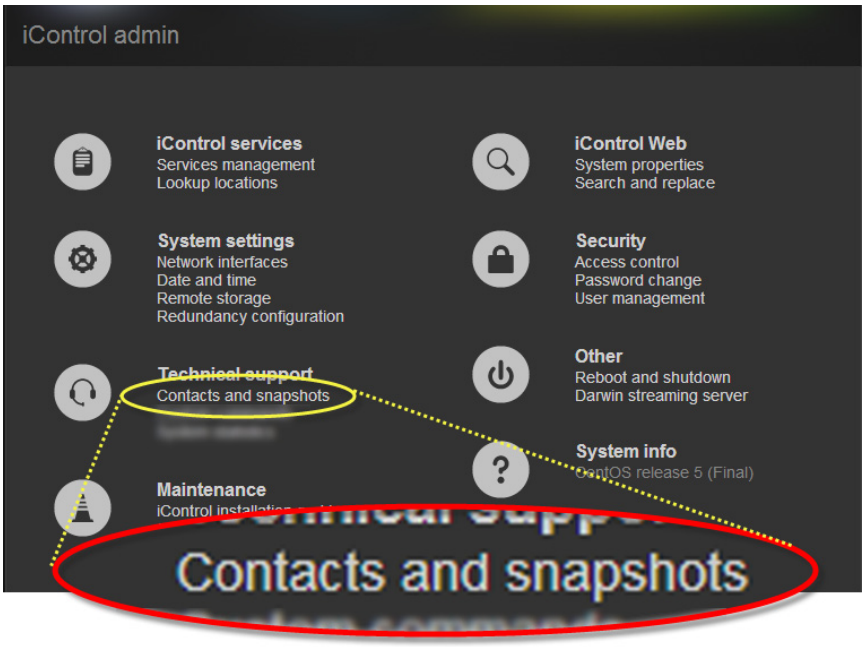
Opening the Contacts and snapshots Page

REQUIREMENT

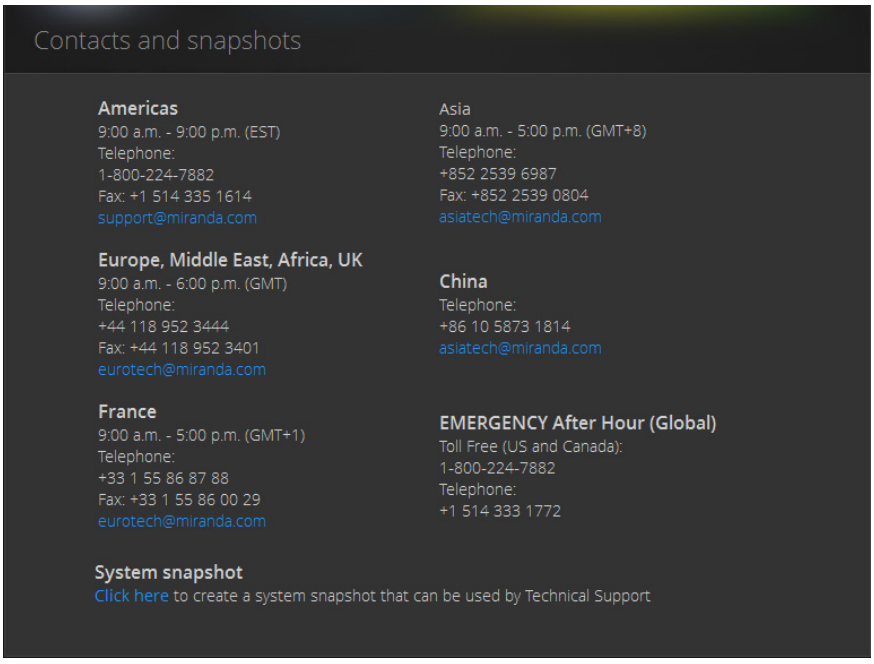
Before beginning this procedure, make sure you have opened the *iControl admin* page on your Application Server (see page 681).

To open the Contacts and snapshots page

- On the *iControl admin* page, click **Contacts and snapshots**, under **Technical support**.



SYSTEM RESPONSE: The *Contacts and snapshots* page appears.



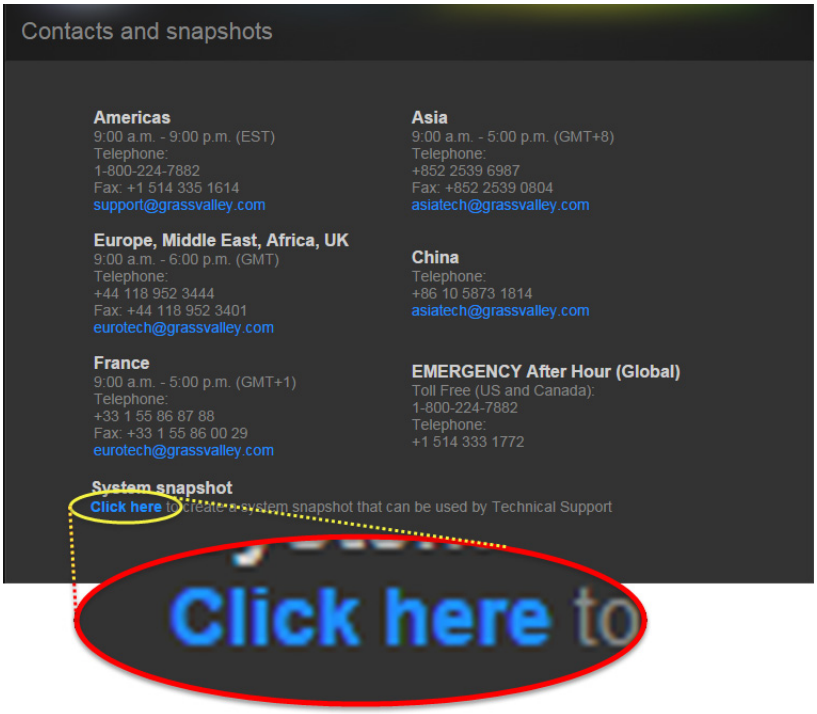
Creating a System Snapshot

REQUIREMENT

Before beginning this procedure, make sure you have navigated to the *Contacts and snapshots* page of iControl (see page 671).

To create a system snapshot

1. On the *Contacts and snapshots* page, click the link at the bottom of the page to begin a system snapshot.



SYSTEM RESPONSE: iControl displays a message indicating when the snapshot is complete. The data listed above this message comprise the snapshot information.

2. Click the link in the message to download the file to your local file system.

3. Send the file to Grass Valley Technical Support.

Logging in to an Application Server with PuTTY

REQUIREMENTS

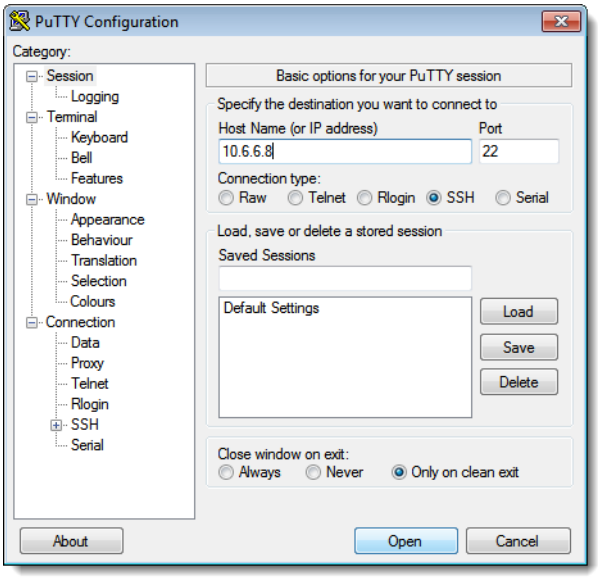
Make sure you meet the following conditions before beginning this procedure:

- You have the PuTTY client application on your client PC. PuTTY is downloadable from the *Downloads* link on iControl's *Startup* page.
- Your client PC has connectivity with the Application Server.

To log in to an Application Server with PuTTY

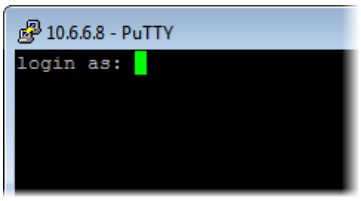
1. Open the PuTTY application.

   SYSTEM RESPONSE: The PuTTY Configuration window appears.



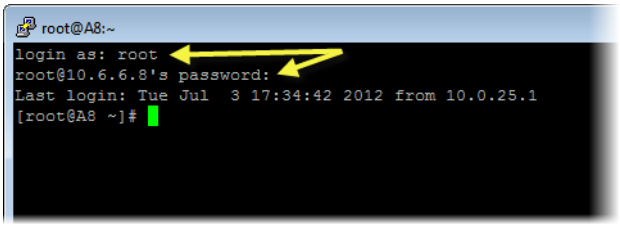
2. Make sure the PuTTY Configuration window reflects the following settings:
   - **Host Name**: `<host name or IP address of Application Server>`
   - **Port**: 22
   - **Connection type**: SSH
3. Click **Open**.

   SYSTEM RESPONSE: A secure shell appears with a login prompt.



PuTTY SSH shell displaying Application Server login prompt

4. Login to the Application Server using the *root* profile:
   - userid: `root`
   - password: `icontrol`



Logging in to Application Server with PuTTY

Creating a Local Shortcut to an iC Web Page

Web Browser Shortcut Keys

Shortcut Keys	Description
Alt+**left arrow**	Back a page
Alt+**right arrow**	Forward a page
F5	Reload current page/frame
F11	Display the current Web Site in full screen mode. Pressing **F11** again will exit this mode
Ctrl+**F11**	Display ALL the Web Site in full screen mode. Pressing **Ctrl**+**F11** again will exit this mode[1]
Esc	Stop page or download from loading
Ctrl+**Enter**	Quickly complete an address. For example type `computerhope` in the address bar and press **Ctrl**+**Enter** to get `http://www.computerhope.com`

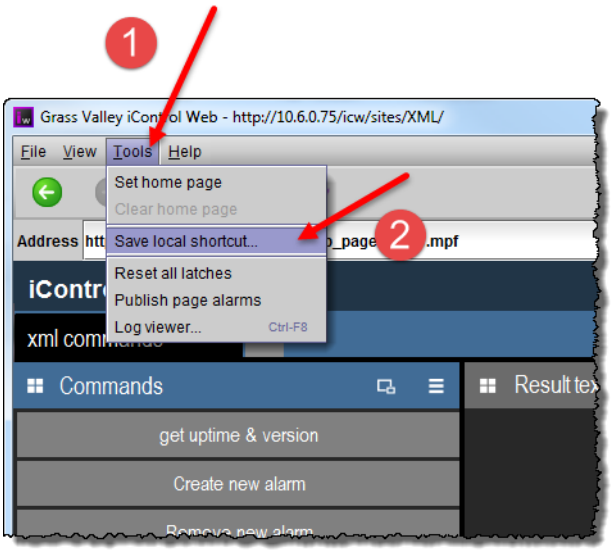
1. You can customize the dimensions of the *total full screen* window (**Ctrl**+**F11**) in **iC Creator**. For more information, see page 627.

REQUIREMENT

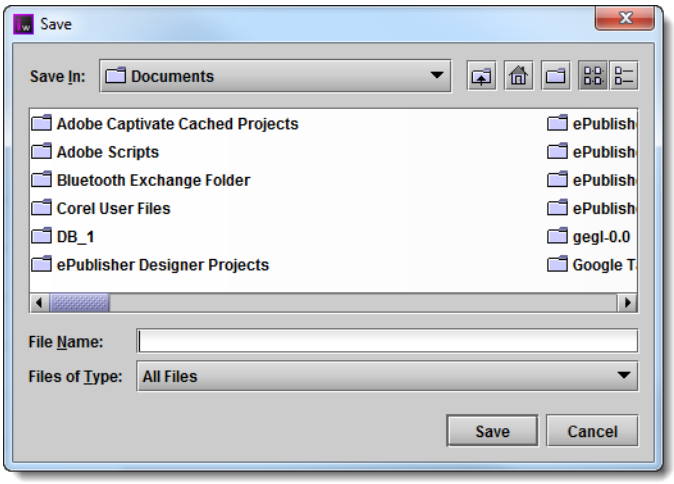
Before beginning this procedure, make sure you have opened the desired iC Web page (see page 718).

To create a local shortcut to an iC Web page

1. In iC Web, open the page for which you wish to save a local shortcut.
2. On the **Tools** menu, click **Save local shortcut**.



3. In the **Save** window that appears, specify a name and location for the shortcut.



4. Click **Save**.

   System Response: The local shortcut for the currently open page appears in the specified location on your PC.

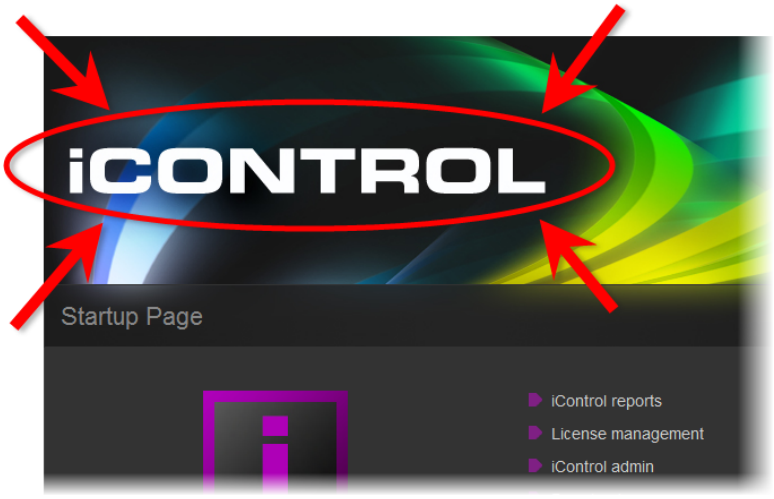
iControl Common Tasks

Starting iControl

To start an iControl session

- Open a Web browser and type an Application Server's IP address or host name.
  SYSTEM RESPONSE: The *Startup* page appears.

> **Note:** Click the iControl logo—visible on **all** iControl pages and identified, below—at any time to return to the *Startup* page.



Note: As you navigate to other Web pages on the Application Server, you can quickly return to the startup page by clicking the iControl logo in the header area.

Starting & Stopping iControl Services

An Application Server runs a number of programs (services) in support of various iControl operations. You may, at times, need to start, stop, or restart one or more of these services.

- Opening the Services management page on page 678
- Stopping, Starting, or Restarting a Service on page 680
- Stopping all iControl Services on page 680
- Restarting all iControl Services on page 680

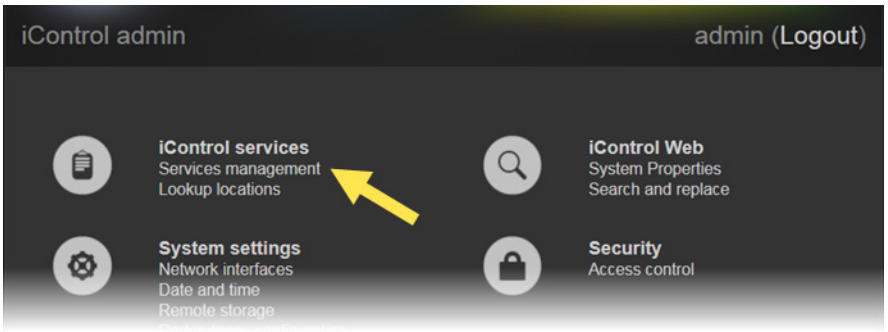
Opening the Services management page

REQUIREMENT

Before beginning this procedure, make sure you have logged in to the *iControl admin* page (see page 681).

To open the Services management page

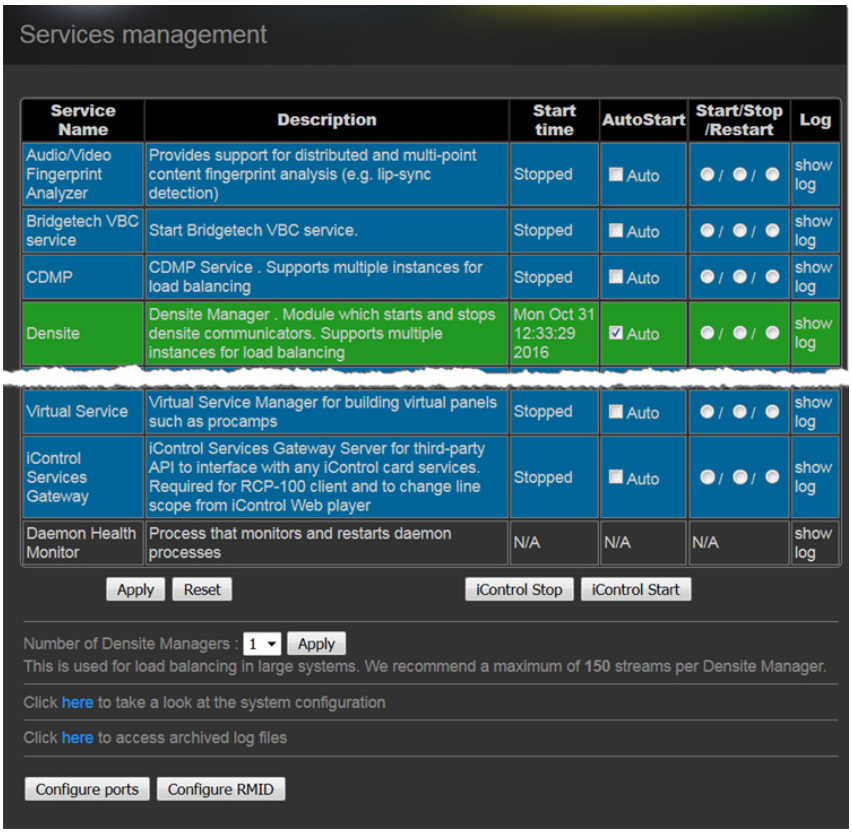
- On the *iControl admin* page, click **Services management**, under **iControl services**.



SYSTEM RESPONSE: The *Services management* page appears.

All iControl services available on the current Application Server are listed in a table, one service per row. A row's background color indicates the service state:

- Green indicates an active service
- Blue indicates an inactive service
- Red indicates a problem with the service.



Stopping, Starting, or Restarting a Service

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Services management* page (see page 678).

To stop, start, or restart a service

1. On the *Services management* page, find the row corresponding to the service you wish to stop, start, or restart.
2. In the **Start/Stop/Restart** column, click the button corresponding to the action you would like to take.
3. In the **Autostart** column, click to put a check mark in the **Auto** box if you want the service to always start when the Application Server is rebooted.
4. Click **Apply**.

Stopping all iControl Services

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Services management* page (see page 678).

To stop all iControl services

- Near the bottom of the *Services management* page, click **iControl Stop**.

  The page reloads, with a blue background for all services.

Restarting all iControl Services

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Services management* page (see page 678).

To restart all iControl services

1. On the *Services management* page, in the **Autostart** column, click to put a check mark in the **Auto** box corresponding to the services you wish to start or restart when the Application Server is rebooted.
2. Click **Apply**.
3. Click **iControl Stop**.

   System Response: The page reloads, with a blue background for all services.
4. Click **iControl Start**.

   System Response: The page reloads with a green background for all services that have a check mark in the **Autostart** column.

Starting the iControl Launch Pad

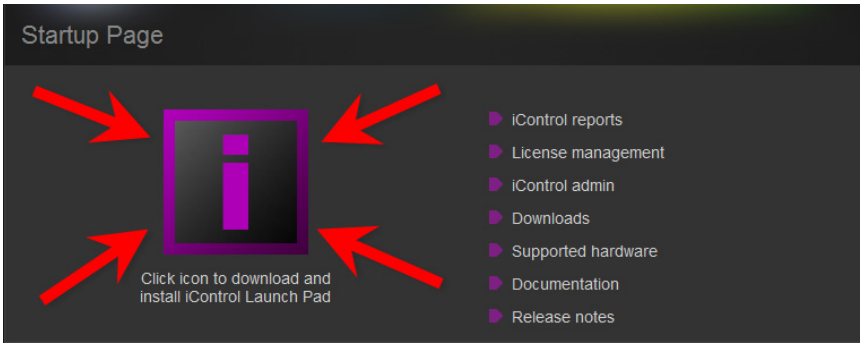
To open any of the iControl client-side applications, you must do so from the *iControl Launch Pad*.

REQUIREMENT

Before beginning this procedure, make sure you have started iControl (see page 677).

To launch iControl Launch Pad

1. On the *Startup* page, click the massive **i** icon.



SYSTEM RESPONSE: The *iControl Launch Pad* executable file is downloaded to your local file system.

2. Double-click the executable file.

Opening the iControl admin Page

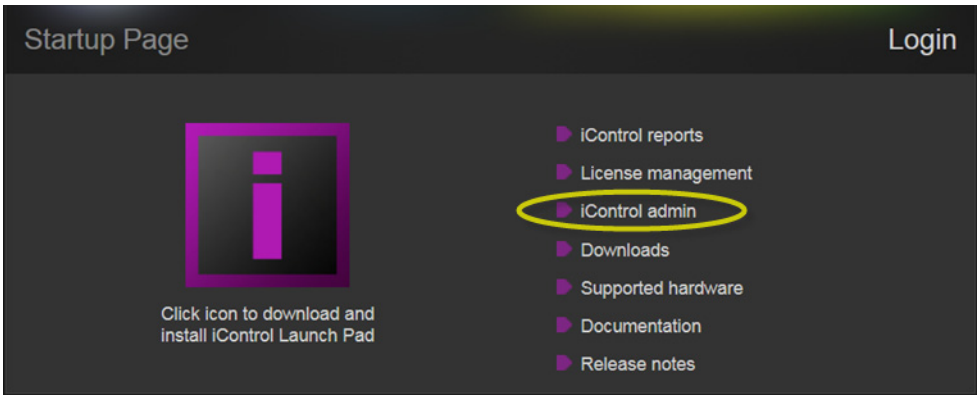
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have started iControl (see page 677).
- You know if you need *administrator,* or *super* privileges for the task you would like to perform, and you know the required user credentials.

To open the iControl admin page

1. On the *Startup* page, click **iControl admin**.



2. If you have not yet logged in to iControl, the system prompts you for credentials. Type the required user name, and password, select the appropriate domain (if your system has LDAP services enabled), and then click **Log In**.

IMPORTANT: **iControl admin's default users (and users created in iControl admin) do not have access to LDAP (or AD) sub-domains:** If your system has LDAP services enabled, and the task you wish to perform requires *administrator* (or *super*) privileges, log in with the appropriate domain's ***admin*** user profile (default password: `admin`), or a user with the required permissions for the selected domain.

Default profiles for iControl admin

	Super user	Administrator
User name	`admin`	`miranda`
Password	`icontrol`	`icontrol`

SYSTEM RESPONSE: The *iControl admin* page appears. The set of tasks available from this page depends on the current user's role.

Opening the Access control Page

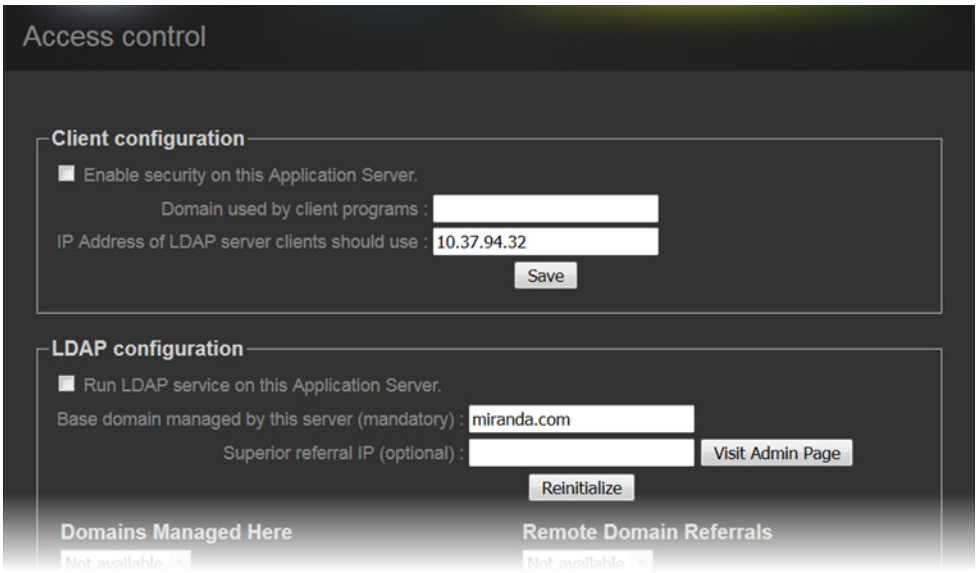
REQUIREMENT

Before beginning this procedure, make sure you have logged in to iControl admin, as a user associated with the *super,* or *administrator* role (see page 681).

To open the Access control page

- On the *iControl admin* page, click **Access control**, under **Security**.

  SYSTEM RESPONSE: The *Access control* page appears. The set of tasks available from this page depends on the current user's role.



Opening the User management Page

REQUIREMENT

Before beginning this procedure, make sure you have opened your Application Server's *iControl admin* page (see page 681), after having logged in to iControl admin, as a user associated with the *super* role.

To open the User management page

- On the *iControl admin* page, click **User management**, under **Security**.

  SYSTEM RESPONSE: The *User management* page appears.

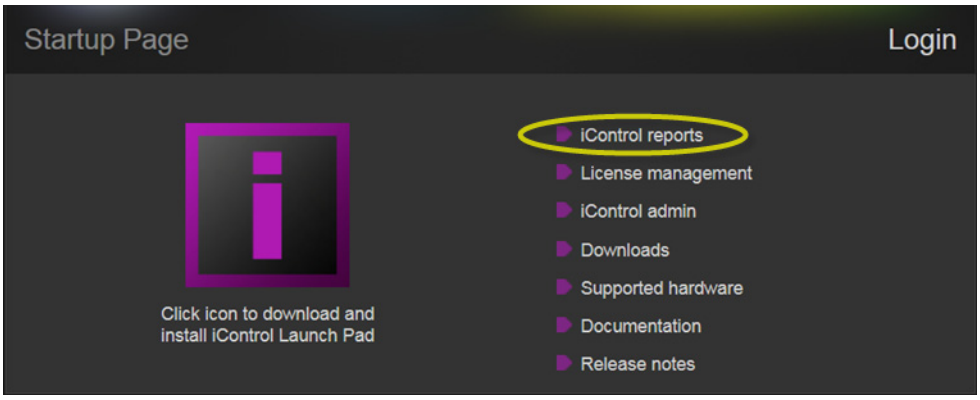
Opening the Reports Page

REQUIREMENT

Before beginning this procedure, make sure you have started iControl on the desired Application Server (see page 677).

To open the Reports page

- On the *Startup* page, click **iControl reports**.



SYSTEM RESPONSE: The *Reports* page appears.

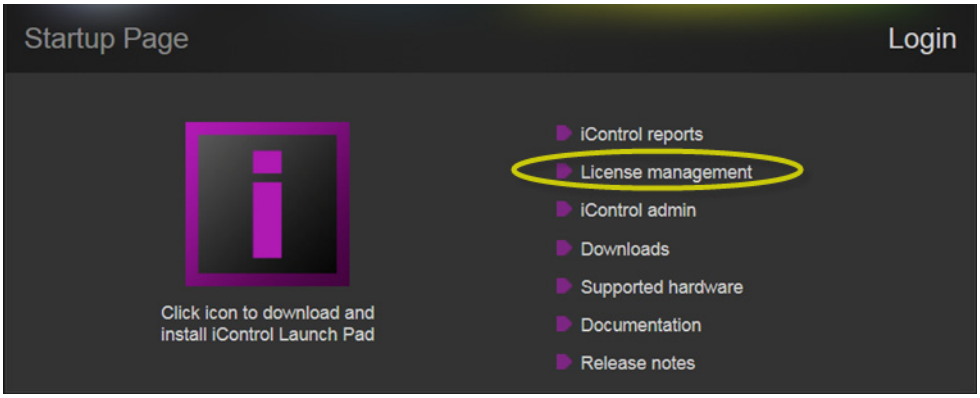
Opening the License Management Page

REQUIREMENT

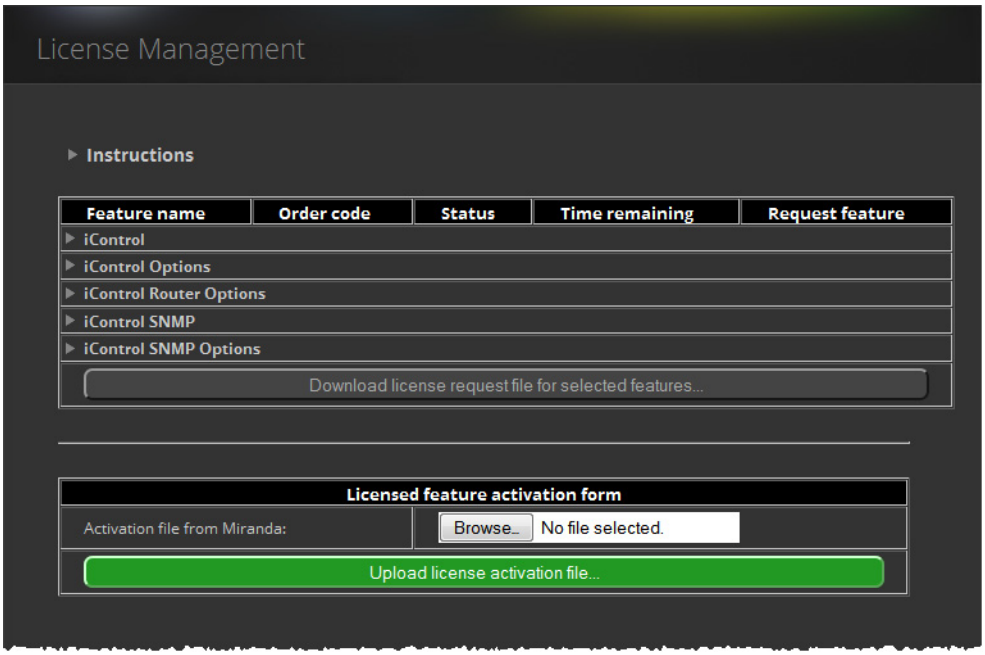
Before beginning this procedure, make sure you have started iControl (see page 677).

To open the License management page

- On the *Startup* page, click **License management**.



SYSTEM RESPONSE: The *License management* page appears.



Note: If you have not yet activated any licenses through iControl's *License Management* feature, you will see a notice on the *Startup* page indicating there are options or drivers whose licenses are pending activation. This notice will disappear after the first time you activate a license.

Opening the Redundancy Configuration Page

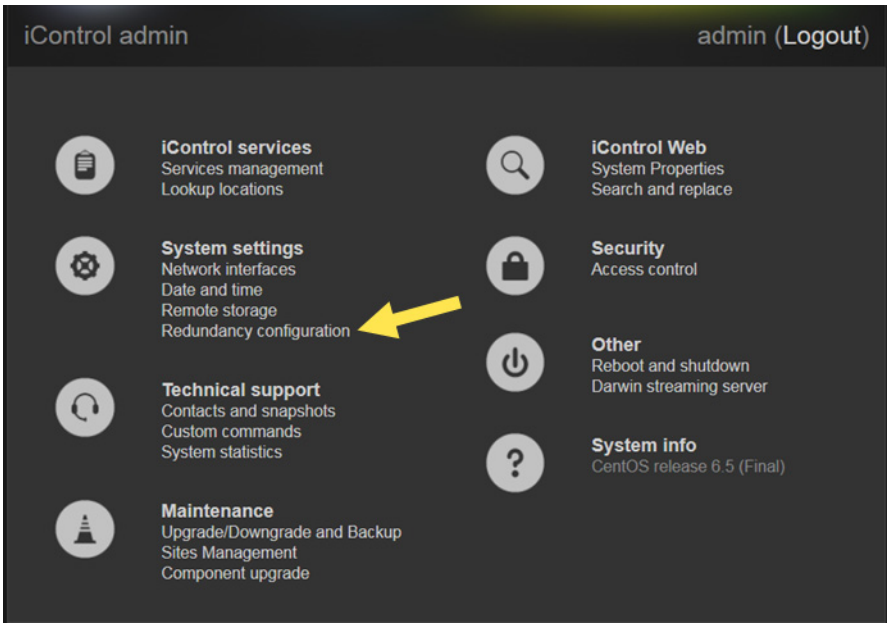
Use this procedure to display and configure Application Server redundancy settings.

REQUIREMENT

Before beginning this procedure, make sure you have opened the *iControl admin* page on the Application Server for which you would like to configure redundancy (see page 681).

To open the Redundancy configuration page

- On the *iControl admin* page, click **Redundancy configuration**, under **System settings**.



SYSTEM RESPONSE: The *Redundancy configuration* page appears.

If your Application Server is not yet part of a Redundancy Group, links on the page allow you to create one. If your Application Server is part of a Redundancy Group, the amount of information available on the page depends on the server's role (i.e., Main, or Backup) in the group.

Opening the Lookup Location Page

The need for specifying lookup locations depends on several factors (see Lookup Services, on page 27). In general, we recommend the following:

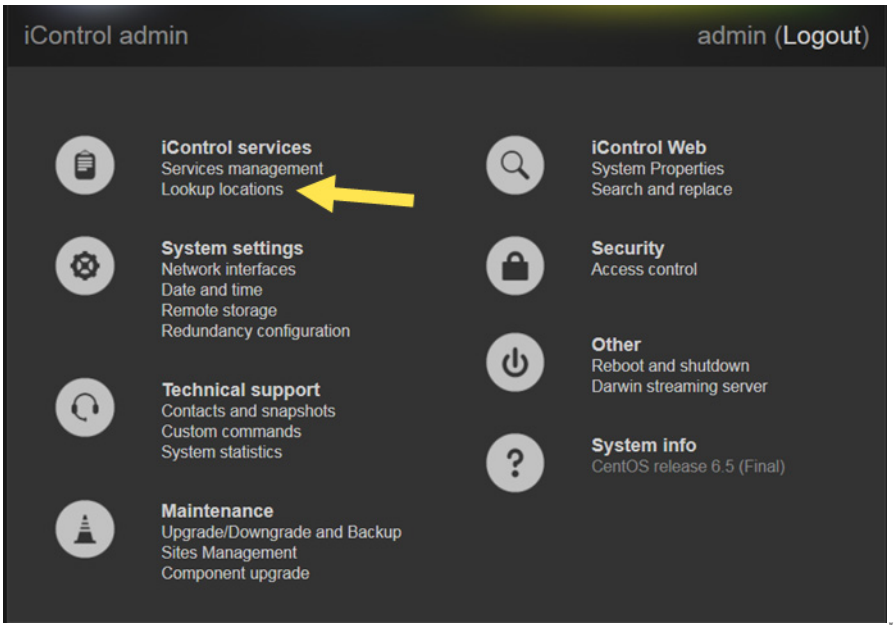
- If an Application Server is **not** running a lookup service, you should type the locations of all Application Servers running the lookup service on its own subnet, as well as those on external subnets.
- If an Application Server **is** running a lookup service, you should type the locations of all Application Servers running the lookup service on external subnets.

REQUIREMENT

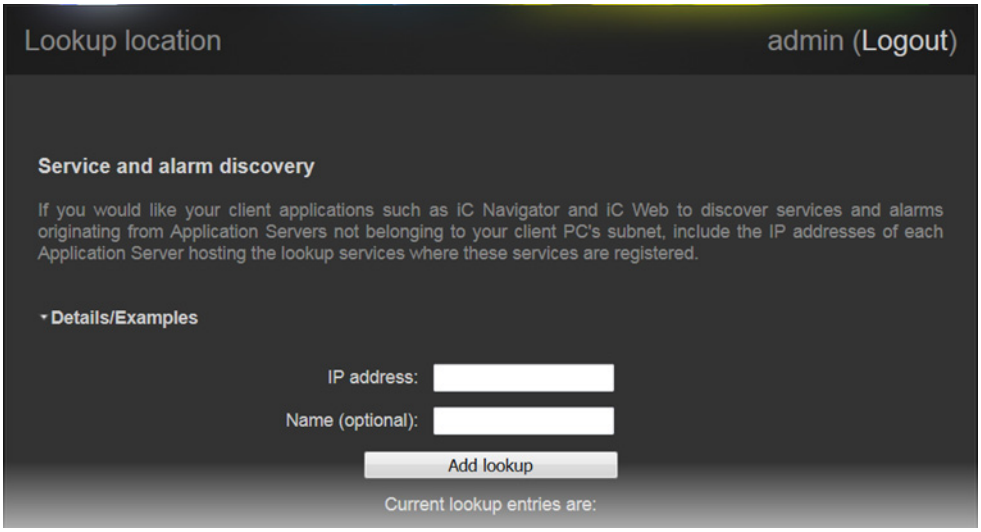
Before beginning this procedure, make sure you have opened the *iControl admin* page (see page 681).

To open the Lookup location page

- On the *iControl admin* page, click **Lookup locations**, under **iControl services**.



SYSTEM RESPONSE: The *Lookup location* page appears.



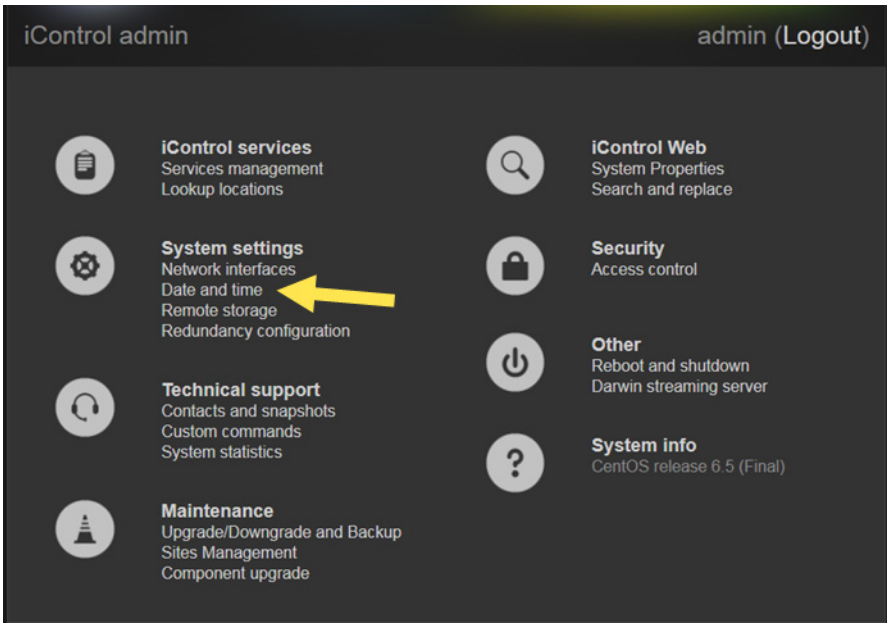
Opening the Date and Time Page

REQUIREMENT

Before beginning this procedure, make sure you have opened the *iControl admin* page (see page 681).

To open the Date and Time page

- On the *iControl admin* page, click **Date and time**, under **System settings**.



SYSTEM RESPONSE: The Date and Time page appears.

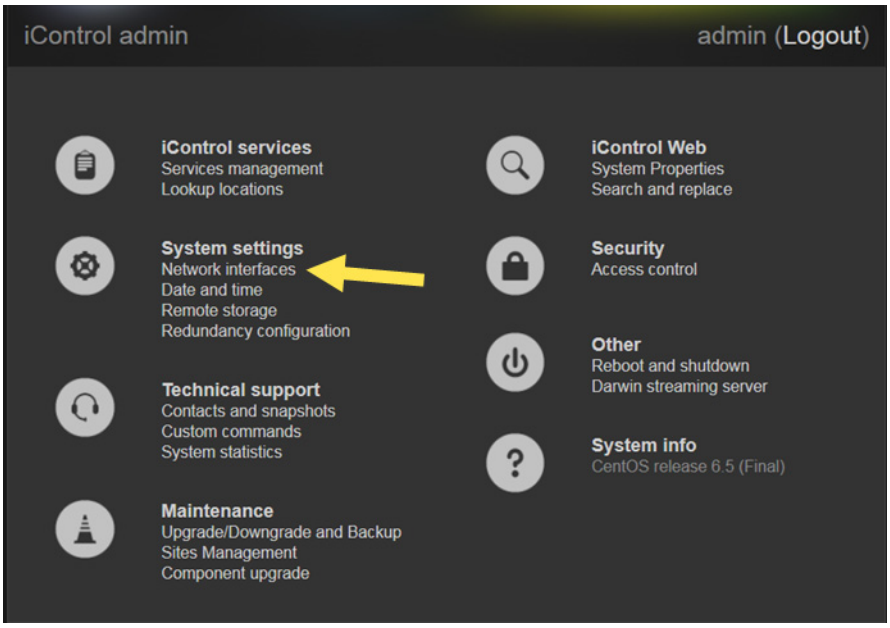
Opening the Network Interfaces Page

REQUIREMENT

Before beginning this procedure, make sure you have opened the *iControl admin* page (see page 681).

To open the Network interfaces page

- On the *iControl admin* page, under **System settings**, click **Network interfaces**.



SYSTEM RESPONSE: The *Network interfaces* page appears.

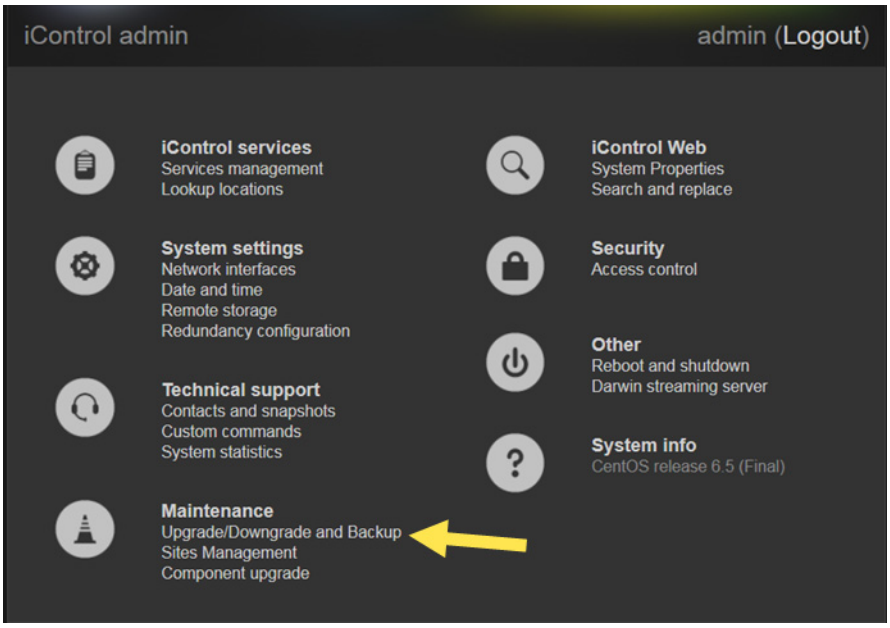
Opening the Installation and Backup Page

REQUIREMENT

Before beginning this procedure, make sure you have opened the *iControl admin* page (see page 681).

To open the Installation and backup page

- On the *iControl admin* page, under **Maintenance**, click **Upgrade/Downgrade and Backup**.



SYSTEM RESPONSE: The Upgrade/Downgrade and Backup page appears.

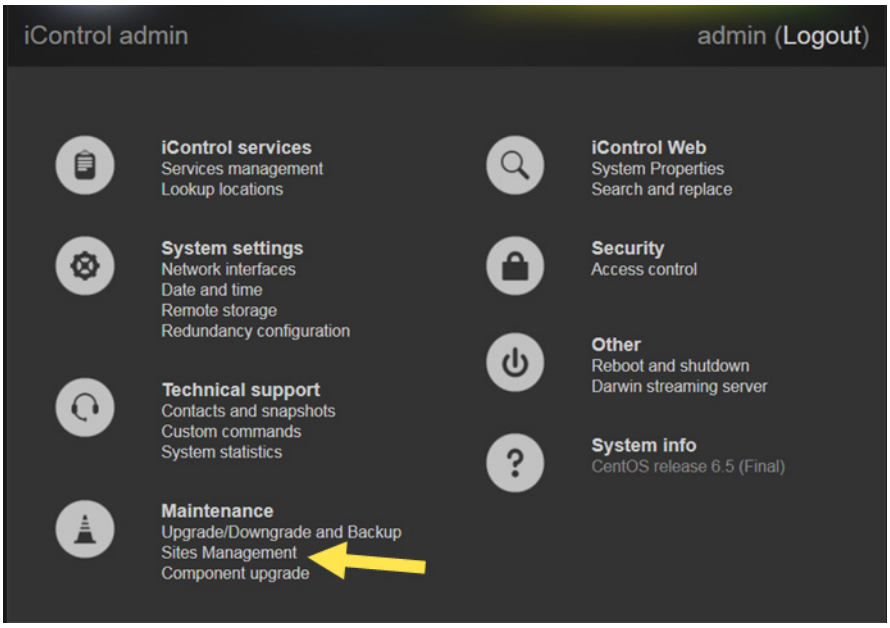
Opening the Sites Management Page

REQUIREMENT

Before beginning this procedure, make sure you have opened the *iControl admin* page (see page 681).

To open the Sites Management page

- On the *iControl admin* page, under **Maintenance**, click **Sites Management**.



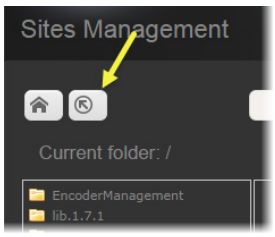
SYSTEM RESPONSE: The *Sites Management* page appears.

Working with the Sites Management Page

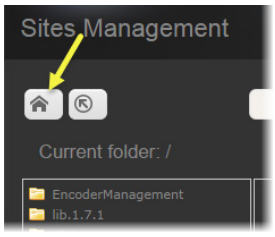
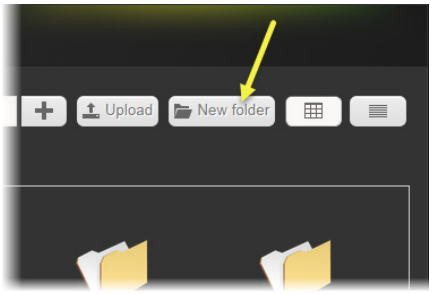
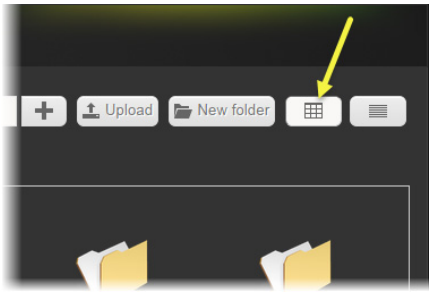
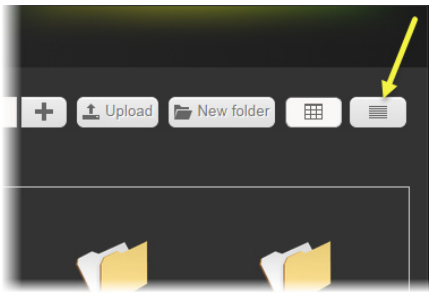
Sites Management Page (Various Tasks)

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Sites Management* page (see page 690).

To do this...	...do this...
Display the contents of the parent folder in the main pane.	On the *Sites Management* page, click the *Navigate Up* button. 

(*Continued*)

To do this...	**...do this...**
Display the contents of the root folder in the main pane.	On the *Sites Management* page, click the *Home* button. 
Create a new folder (at the level displayed in the main pane).	On the *Sites Management* page, click **New folder**. 
Switch the main pane to *Grid* view.	On the *Sites Management* page, click the *Grid view* button. 
Switch the main pane to *List* view.	On the *Sites Management* page, click the *List view* button. 
Upload a spreadsheet to an Application Server.	See Uploading a Spreadsheet to an Application Server on page 693.

(*Continued*)

To do this...	...do this...
Perform operations involving spreadsheets already on the Application Server.	See Managing Existing Spreadsheets on page 693.

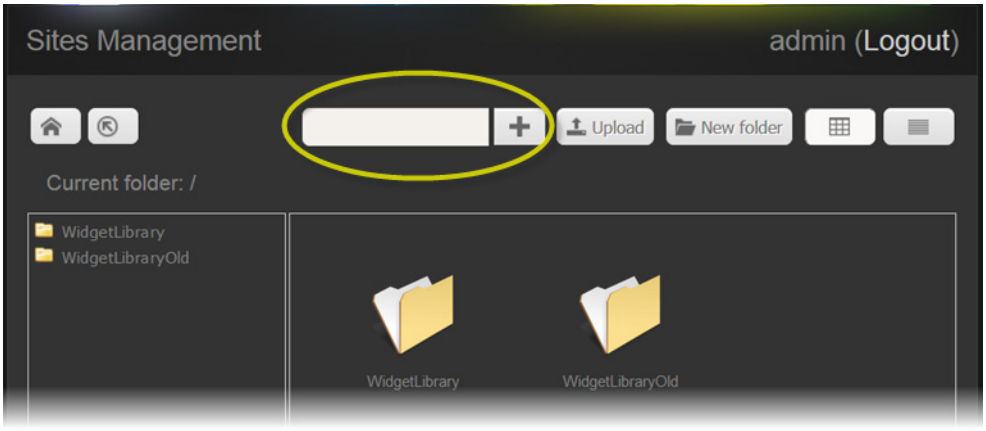
Uploading a Spreadsheet to an Application Server

REQUIREMENT

Before beginning this procedure, make sure you have opened the *Sites Management page* (see page 690).

To upload a spreadsheet to an Application Server

1. On the Sites Management page, perform step 1 to step 2 of the task Renaming a Spreadsheet File on an Application Server on page 694, to navigate to the folder where you would like to upload your spreadsheet.
2. Click anywhere in the Browse field to select a spreadsheet from your local file system.



3. Navigate to the spreadsheet you wish to upload, select it, and then click **Upload**.
   SYSTEM RESPONSE: A message appears, indicating the spreadsheet has been uploaded.
4. Click **OK**.

Managing Existing Spreadsheets

- Renaming a Spreadsheet File on an Application Server on page 694
- Downloading a Spreadsheet from an Application Server on page 695
- Deleting a Spreadsheet File on an Application Server on page 695

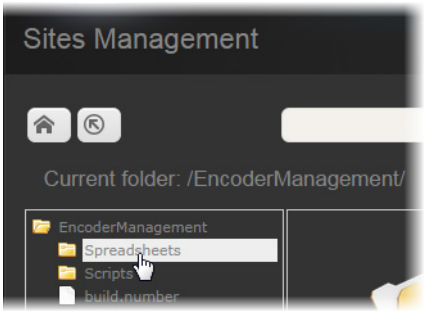
Renaming a Spreadsheet File on an Application Server

REQUIREMENT

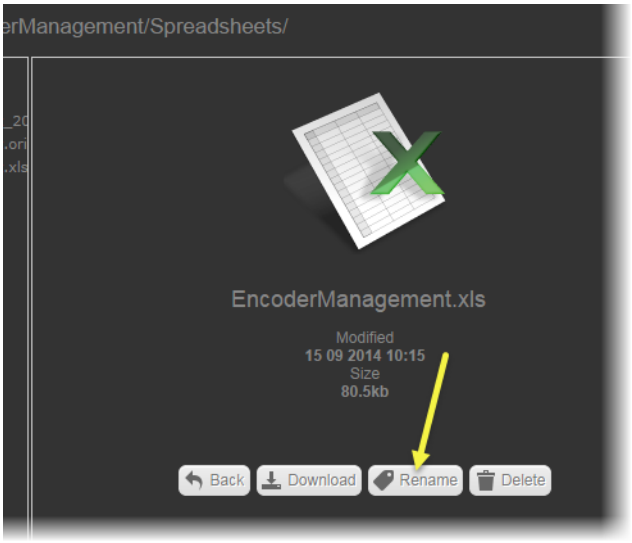
Before beginning this procedure, make sure the *Sites Management* page is open (see page 690).

To rename a spreadsheet file

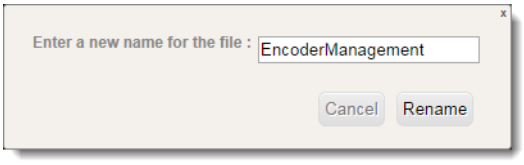
1. On the *Sites Management* page, use the navigation pane to locate—and select—the folder where your spreadsheet is located.



2. In the main pane, click the spreadsheet file.
3. Click **Rename**.



4. Type a new name and then click **Rename**.



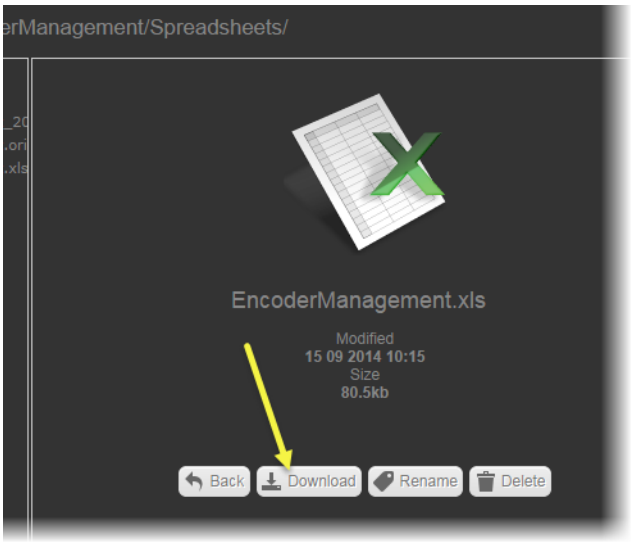
Downloading a Spreadsheet from an Application Server

REQUIREMENT

Before beginning this procedure, make sure the *Sites Management* page is open (see page 690).

To download a spreadsheet from the server

1. Perform step 1 to step 2 of Renaming a Spreadsheet File on an Application Server on page 694 to navigate to the location of the spreadsheet you would like to download.
2. Click **Download**.



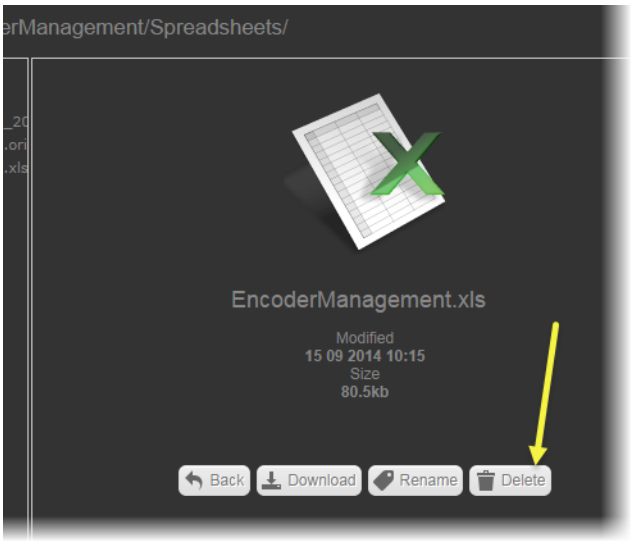
Deleting a Spreadsheet File on an Application Server

REQUIREMENT

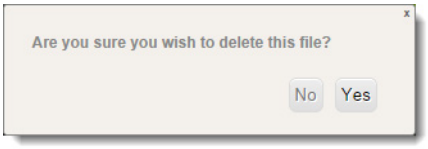
Before beginning this procedure, make sure the *Sites Management* page is open (see page 690).

To delete a spreadsheet file

1. Perform step 1 to step 2 of Renaming a Spreadsheet File on an Application Server on page 694 to navigate to the location of the spreadsheet you would like to delete.
2. Click **Delete**.



SYSTEM RESPONSE: A confirmation message appears.



3. Click **Yes**.

iC Navigator Common Tasks

- Opening iC Navigator on page 697
- Opening Log Viewers and Analyzers on page 697
- Opening Device Profile Manager on page 707
- Opening Densité Manager on page 707
- Opening Densité Upgrade Manager on page 709
- Opening the Privilege Management Window on page 709
- Opening the GSM Alarm Browser on page 710
- Opening the MIB Browser on page 712
- Opening the SNMP Driver Creator Window on page 713
- Opening Audio Video Fingerprint Analyzer on page 715
- Opening GV Node Manager on page 716

Opening iC Navigator

REQUIREMENT

Before beginning this procedure, make sure you have started **iControl Launch Pad** (see page 681).

To start iC Navigator

1. On **iControl Launch Pad**, type in the IP address of your Application Server, or select it from the list of available IP addresses.

2. Click the iC Navigator icon.

3. If access control is enabled for this Application Server's client applications, iC Navigator prompts you for credentials. Type the required user name, and password, select the appropriate domain (if required), and then click **OK**.

   System Response: The iC Navigator splash screen appears followed by the main iC Navigator window.

Opening Log Viewers and Analyzers

There are three different types of log viewers in iControl. They are *Event Log Viewer*, *Incident Log Viewer*, and *Audio Loudness Analyzer*. Additionally, there is a *Loudness Logger* tool which is used to start and stop the logging of loudness data.

Opening Event Log Viewer

You can open **Event Log Viewer** in three contexts:

- In network environments with a **single GSM**, see Opening Event Log Viewer in a Single GSM Environment.

- In network environments with **multiple GSMs**, see Opening Event Log Viewer in a Multi-GSM Environment.
- When you would like to display logs for a specific device, see Displaying a Device-Specific Event Log Viewer.

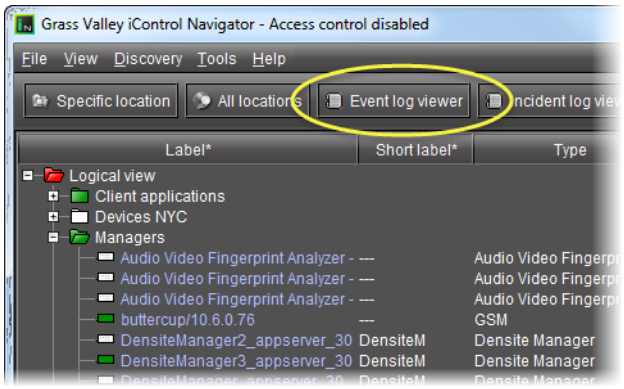
Opening Event Log Viewer in a Single GSM Environment

REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

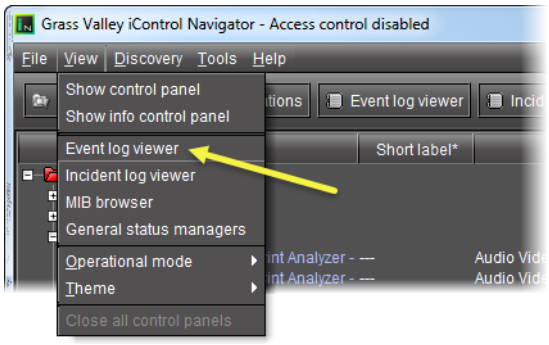
To open Event Log Viewer

- In iC Navigator, perform only **ONE** of the following two actions:
  - Click **Event Log Viewer**.

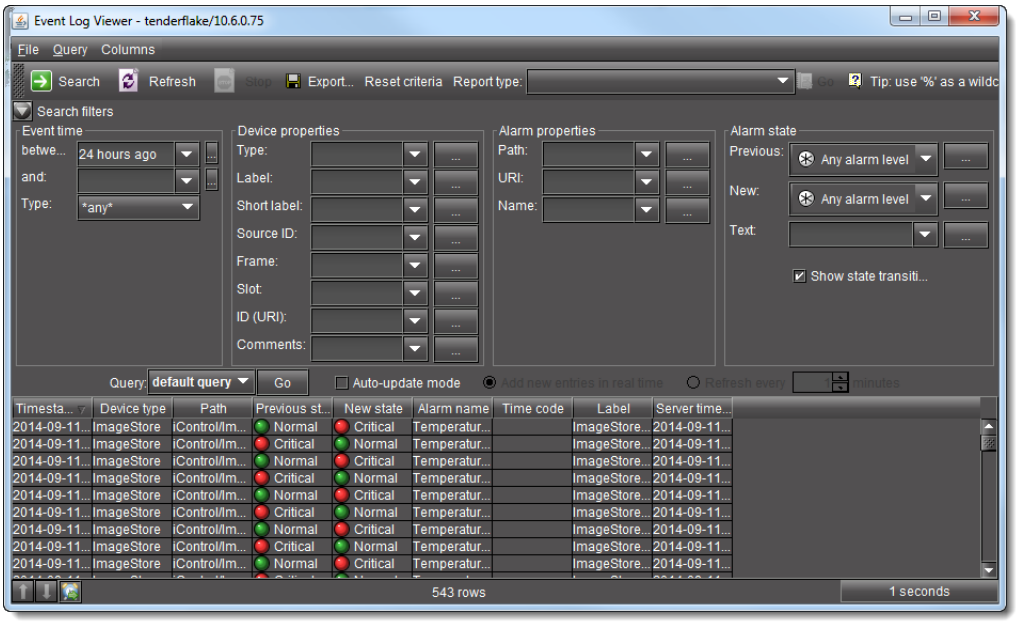


OR,

  - On the **View** menu, click **Event log viewer**.



SYSTEM RESPONSE: **Event Log Viewer** appears.



Event Log Viewer

Opening Event Log Viewer in a Multi-GSM Environment

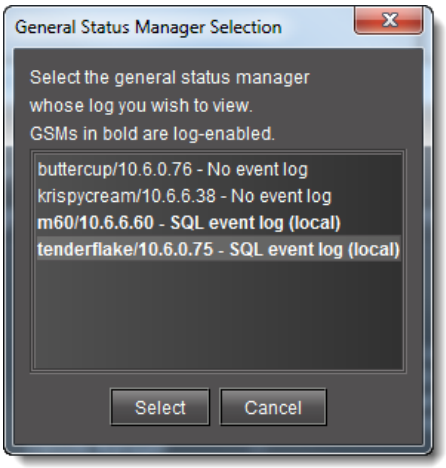
REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To open Event Log Viewer in a multi-GSM environment

1. In iC Navigator, open **Event Log Viewer** as you would according to the procedure Opening Event Log Viewer in a Single GSM Environment on page 698.

   SYSTEM RESPONSE: Given that this is a multi-GSM environment, the **Log Selection** window appears.



2. Select a GSM event log, and then click **Select**.

   System Response: **Event Log Viewer** for the selected GSM event log appears.

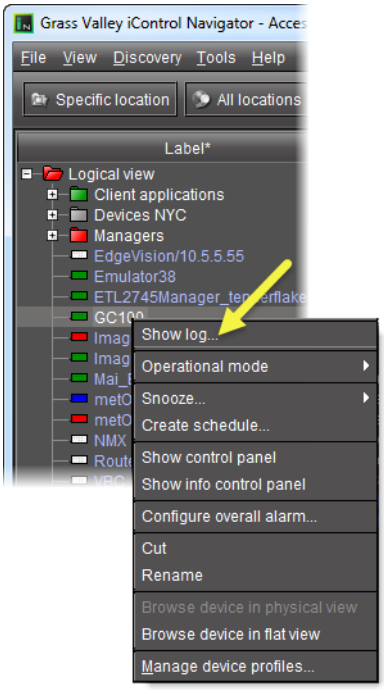
Displaying a Device-Specific Event Log Viewer

REQUIREMENT

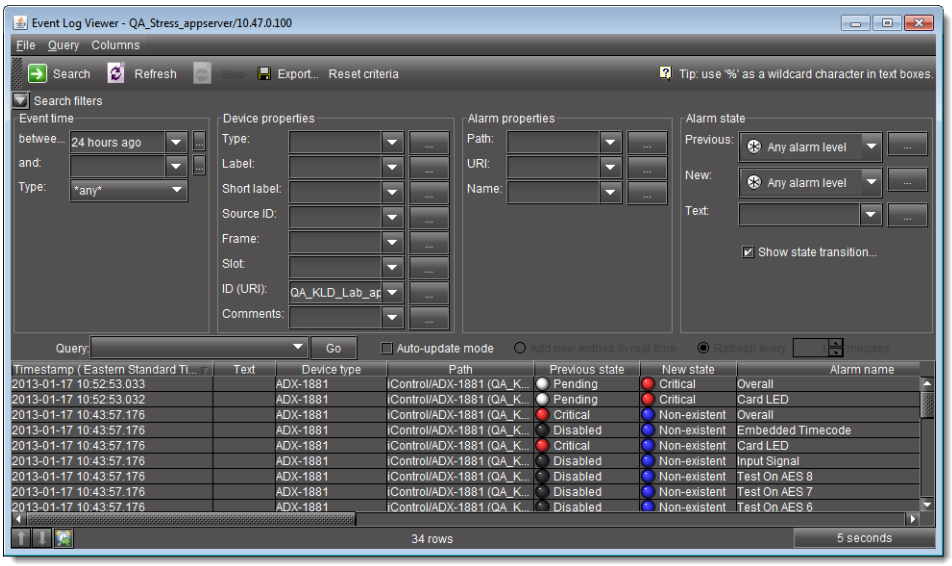
Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To display a device-specific Event Log Viewer

- In iC Navigator, right-click a device, and then click **Show log**.



System Response: The In-context Log Viewer appears, showing entries for the specified device.



The entries displayed are based on the latest search criteria settings in the main **Event Log Viewer** window.

Opening Incident Log Viewer

You can open **Incident Log Viewer** in two contexts:

- In network environments with a **single GSM**, see Opening Incident Log Viewer in a Single-GSM Environment.
- In network environments with **multiple GSMs**, see Opening Incident Log Viewer in a Multi-GSM Environment.

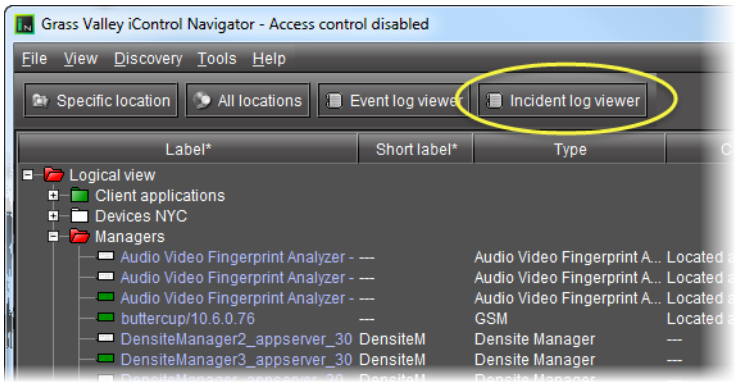
Opening Incident Log Viewer in a Single-GSM Environment

REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

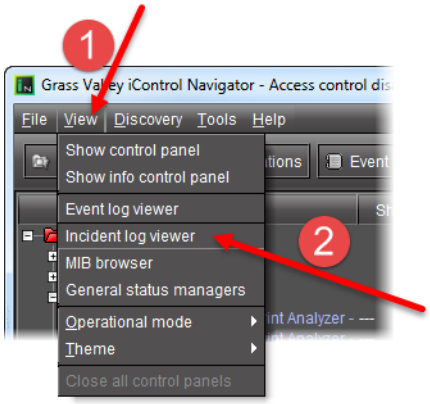
To open Incident Log Viewer

- In iC Navigator, perform only **ONE** of the following two actions:
  - Click **Incident log viewer**,

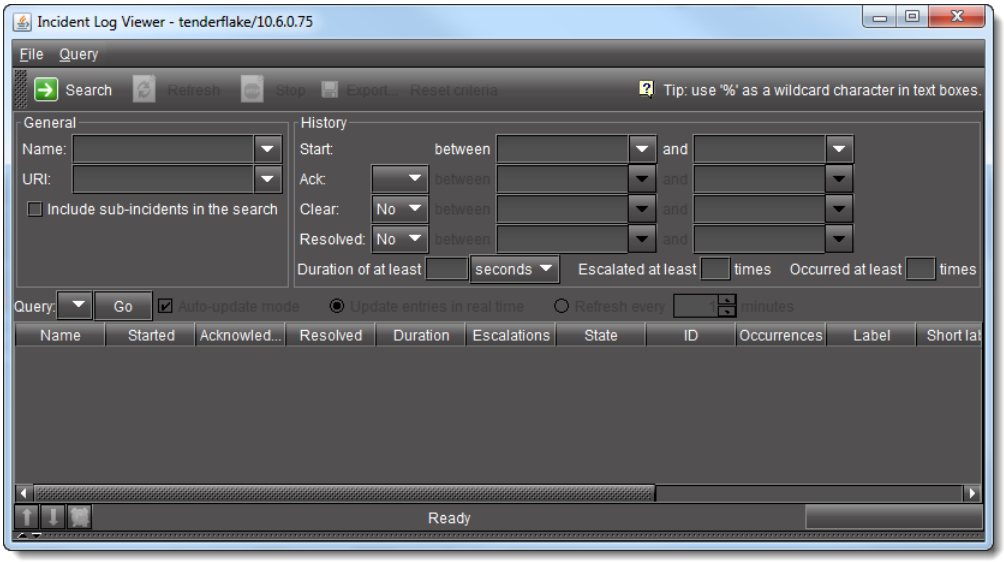


OR,

- On the **View** menu, click **Incident Log Viewer**.

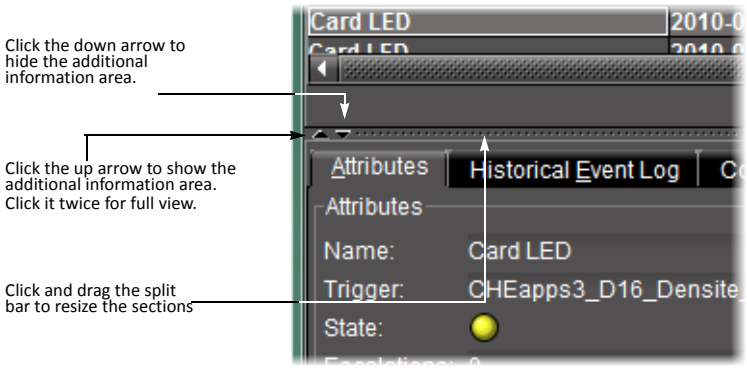


SYSTEM RESPONSE: **Incident Log Viewer** appears.



Incident Log Viewer

TIP: You can hide, show and resize an additional incident information area using the *split bar*.



Opening Incident Log Viewer in a Multi-GSM Environment

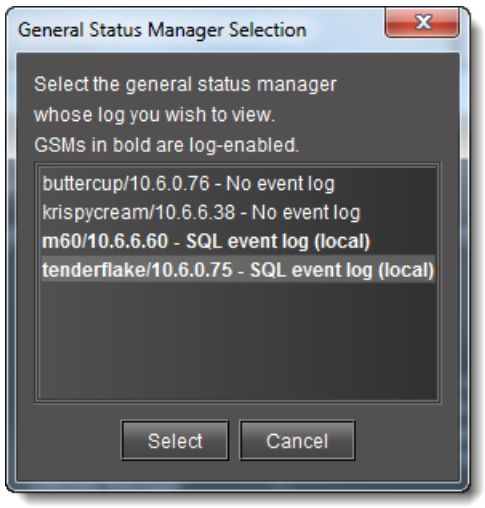
REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To open Incident Log Viewer in a multi-GSM environment

1. In iC Navigator, on the **View** menu, click **Incident Log Viewer**.

   SYSTEM RESPONSE: The **Log Selection** window appears.



2. Click a GSM event log, and then click **Select**.

   SYSTEM RESPONSE: **Incident Log Viewer** for the selected GSM event log appears.

Opening Loudness Logger

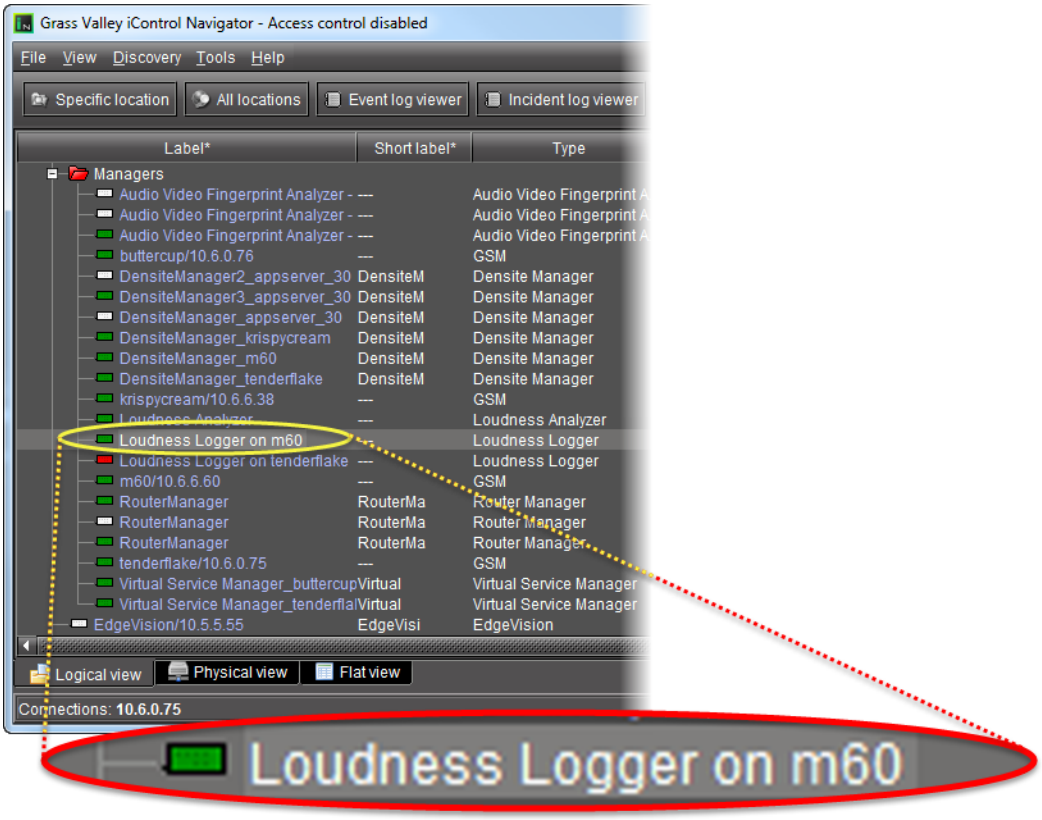
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

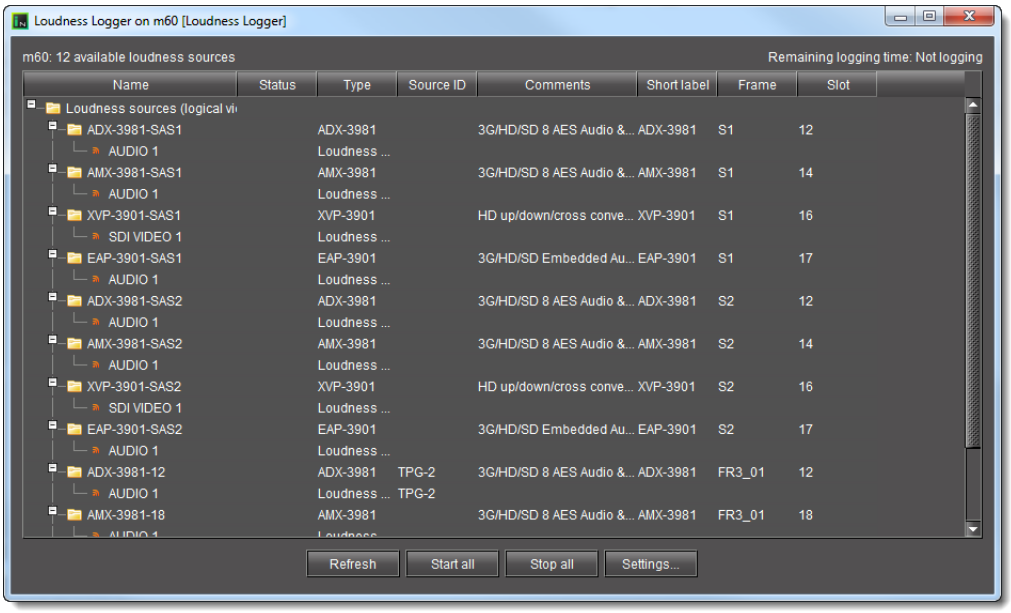
- Your Application Server is connected to a device that is streaming loudness values, such as a Kaleido-Solo.
- You have mounted an external drive to the designated Loudness folder on your Application Server (see Mounting a Remote Shared Drive in your Application Server, on page 184).
- You have opened iC Navigator (see page 697).

To open Loudness Logger

- In iC Navigator, double-click the desired Loudness Logger.



SYSTEM RESPONSE: **Loudness Logger** appears.



Opening Audio Loudness Analyzer

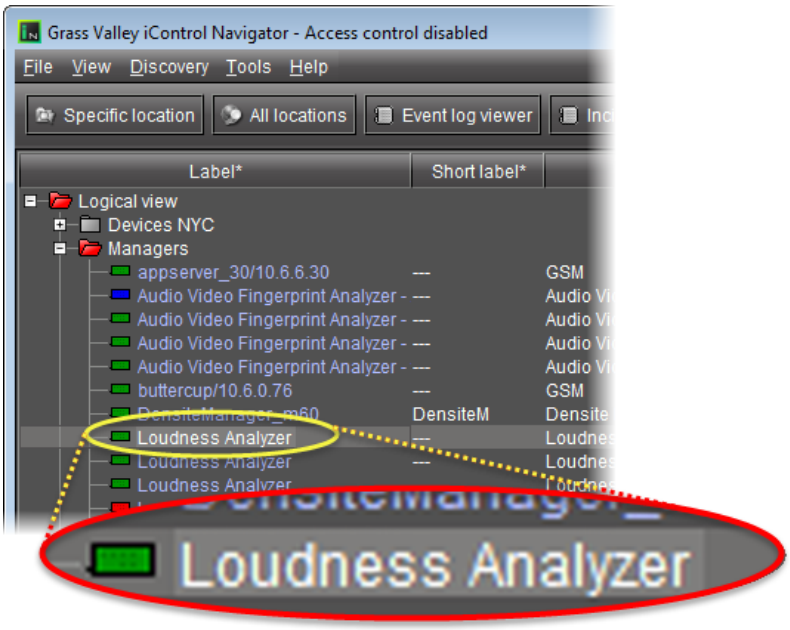
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

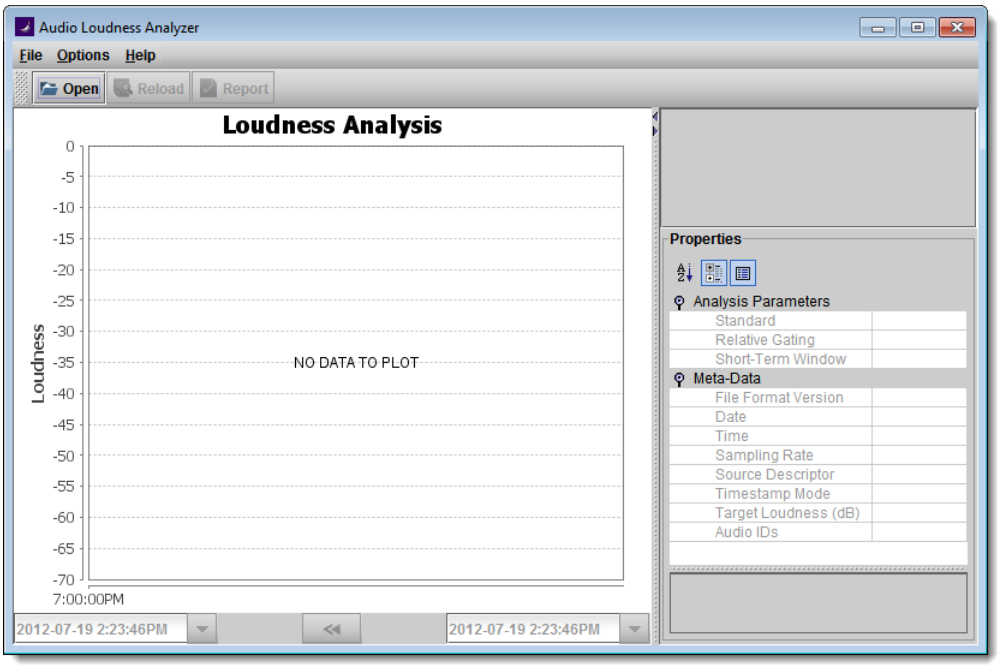
- Your Application Server is connected to a device which is streaming loudness values, such as a Kaleido-Solo.
- You have already logged loudness data (see Logging an Audio Stream's Loudness Data, on page 188).
- You have opened iC Navigator (see page 697).

To open Audio Loudness Analyzer

- In iC Navigator, double-click **Loudness Analyzer**.



SYSTEM RESPONSE: **Audio Loudness Analyzer** appears.



Note: **Audio Loudness Analyzer** is time zone-agnostic, meaning it displays a data plot's time code as UTC (coordinated universal time). When you configure your general **Audio Loudness Analyzer** settings, make sure you set the time zone to that of the signal being analyzed.

Opening Device Profile Manager

REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To open the Device Profile Manager

1. In iC Navigator, select the devices whose profiles you would like to compare, export from or import to.
2. On the **Tools** menu, click **Manage device profiles**,

   OR,

   Right-click one of the selected device rows, and then click **Manage device profiles**.

   System Response: The Device Profile Manager appears, displaying (by default) the **Export** tab in the **Logical view** of the selected devices.

   Note: You can select **Show all devices** to display all discovered devices.

3. Near the top of the window, click the **Export** tab, **Import** tab, **Presets** tab, or **Compare** tab, as required.
4. Near the bottom of the window, click the **Logical view** tab, **Physical view** tab, or **Flat view** tab as required.

   Notes

   - If you are in the **Import** tab, you must select a view for both **Source devices** and **Target devices**.
   - If you are in the **Compare** tab, you must select a view for both **Master card selection** and **Compare cards selection**.
   - The **Logical view**, **Physical view**, and **Flat view** tabs behave in the same way in **Device Profile Manager** as in iC Navigator. For more information about these tabs, see Devices and Services Views in iC Navigator, on page 228.

Opening Densité Manager

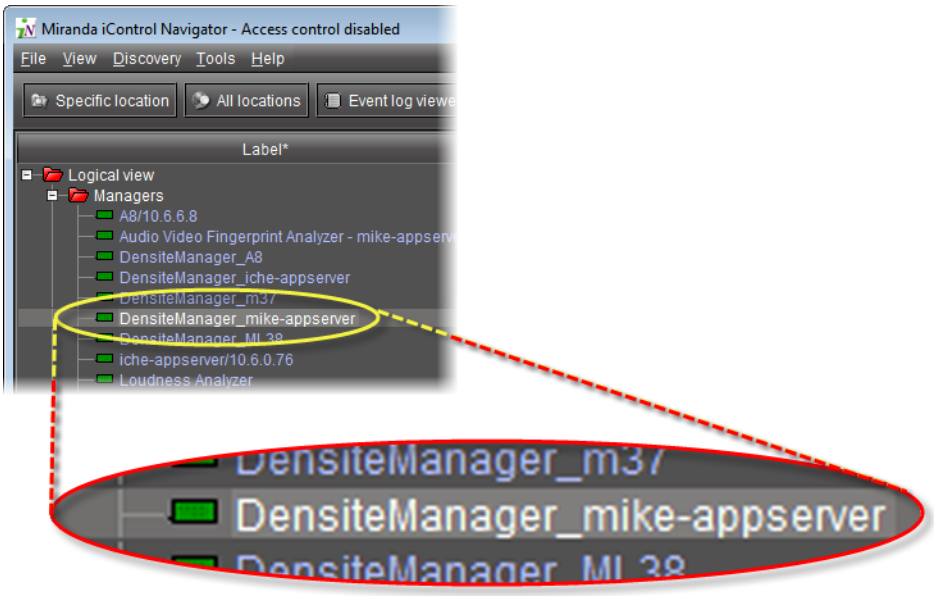
REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see Opening iC Navigator, on page 697).

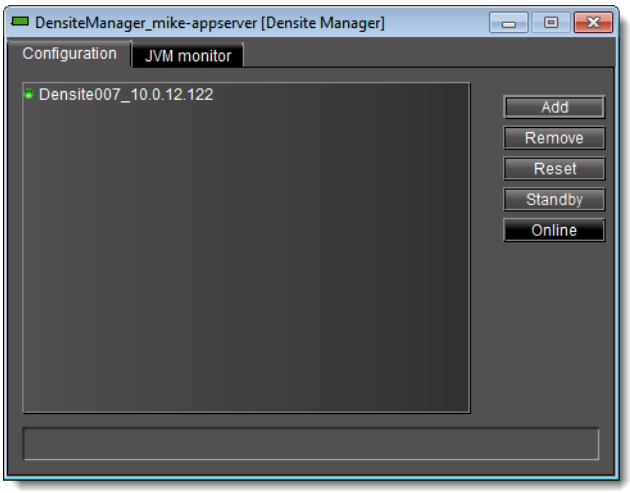
To open Densité Manager

- In iC Navigator, in the *Logical* view, expand the *Managers* folder and then double-click the Densité Manager you would like to open.

Note: Although each Application Server has only one Densité Manager, you may see *several* different Densité Managers in the *Managers* folder. Each Application Server has visibility of the Densité Managers — and other services — belonging to all other Application Servers connected to it by way of the network of Lookup Tables (see Opening the Lookup Location Page, on page 686).



SYSTEM RESPONSE: **Densité Manager** appears.



Opening Densité Upgrade Manager

REQUIREMENTS

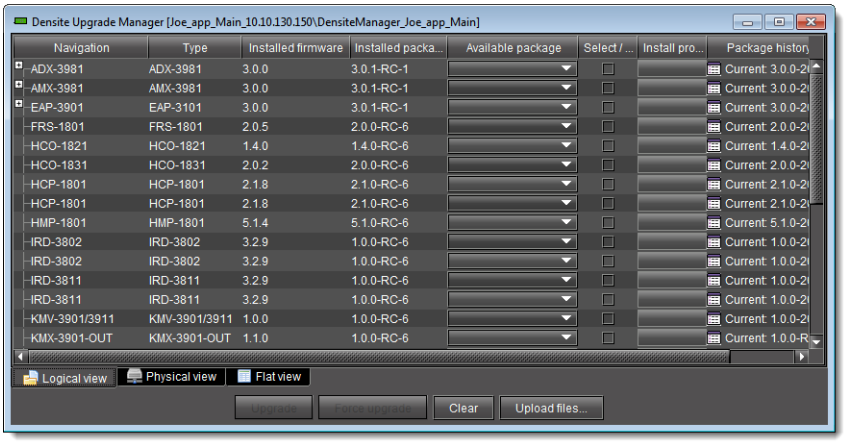
Make sure you meet the following conditions before beginning this procedure:

- Your Application Server's *Densité* service is active (see Stopping, Starting, or Restarting a Service, on page 680).
- The Densité frame housing the card whose upgrade package you would like to change is visible in the **Densité Manager** of your Application Server (see Opening Densité Manager, on page 707).

To open Densité Upgrade Manager

- In iC Navigator, on the **Tools** menu, click **Densité Upgrade Manager**.

  SYSTEM RESPONSE: **Densité Upgrade Manager** appears.



Opening the Privilege Management Window

REQUIREMENT

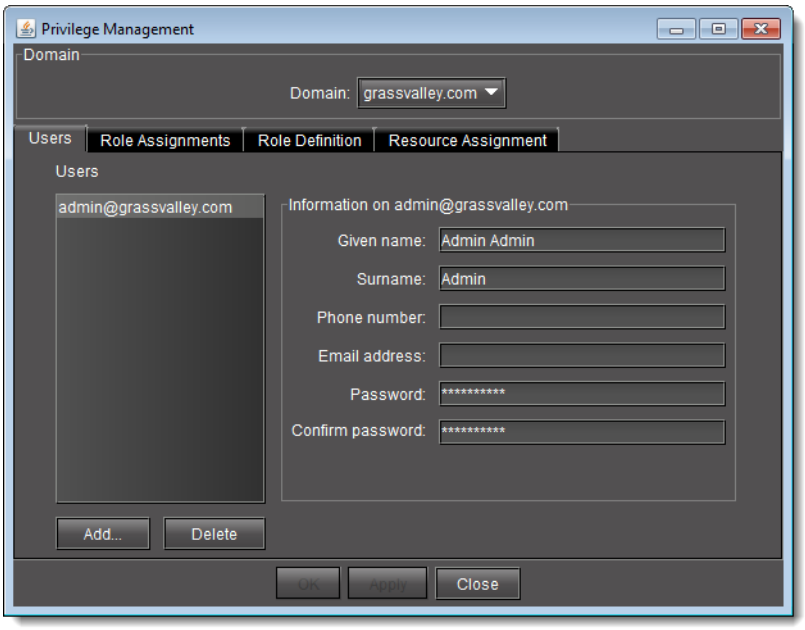
Before beginning this procedure, make sure you have opened iC Navigator (see page 697), and logged in as a user with an appropriate role. The default credentials associated with the *super* role are:

- User: `admin`
- Password: `admin`

To open the Privilege Management window

- On the **Tools** menu, point to **Access control**, and then click **Manage users and roles**.

  SYSTEM RESPONSE: The **Privilege Management** window appears. It contains four tabs: **Users**, **Role Assignments**, **Role Definition**, and **Resource Assignment**.



Note: In order to be able to modify user privileges, you must have the appropriate permissions (i.e., the role associated with your user name must have permission to manage privileges). The *super* role has this permission by default. If you logged in as a user that does not have permission to manage privileges, you only see the **Users** tab.

Opening the GSM Alarm Browser

REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

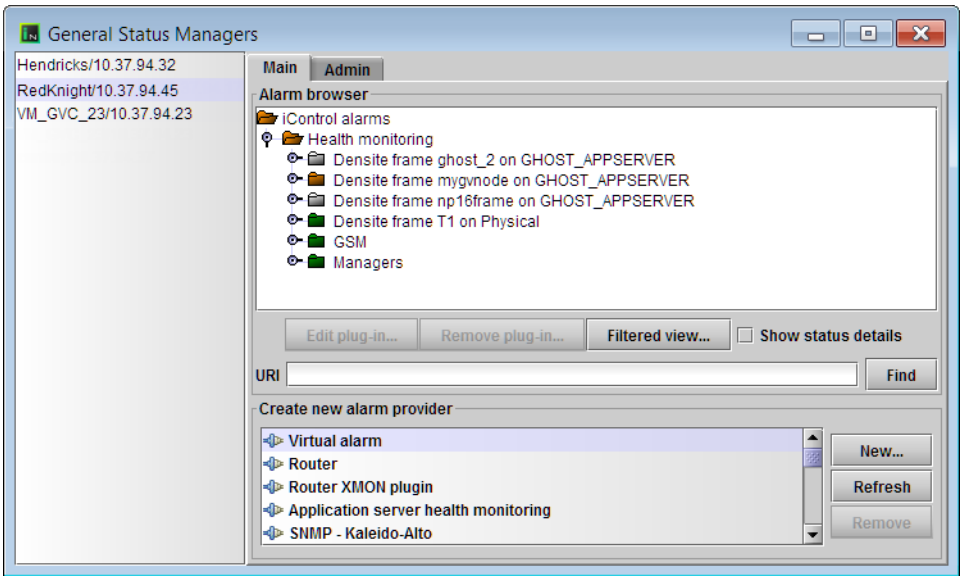
To open the GSM Alarm Browser

1. In iC Navigator, on the **View** menu, click **General status managers**.

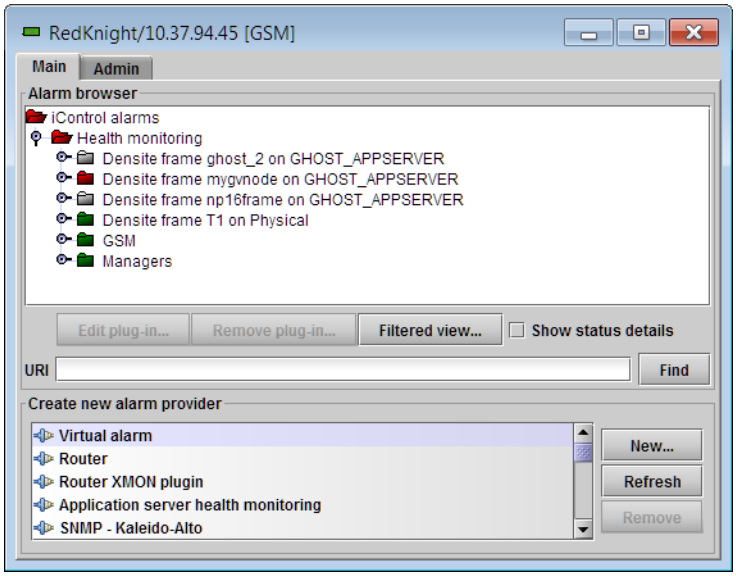
   SYSTEM RESPONSE: The **General Status Managers** window appears.

2. Select one of the GSMs from the list in the left pane of the window.

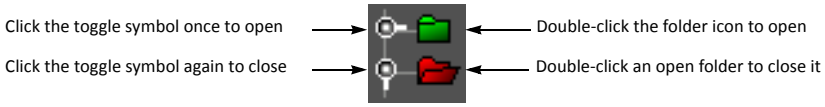
   SYSTEM RESPONSE: The Alarm Browser (under the **Main** tab) displays the devices and services associated with the selected GSM in a hierarchy of folders, subfolders, and alarms.



Note: Alternatively, you can open the Alarm Browser for a specific GSM by double-clicking its name in the iC Navigator window. This opens the Alarm Browser in a smaller window.



3. Open and close folders by clicking on the toggle symbol, or by double-clicking on the folder icons.



Opening the MIB Browser

The MIB Browser is made up of four major areas:

- a toolbar with images that act as shortcuts to the menu options
- a Loaded MibModules area (left side of window) that displays all the loaded MIBs
- a detailed information pane that has three different versions: Result Display, MIB Description, and Multi-Varbind (right side of window). To change the display, select **View** | **Display** and then select the desired view.
- menus (**File**, **View**, **Operations**)

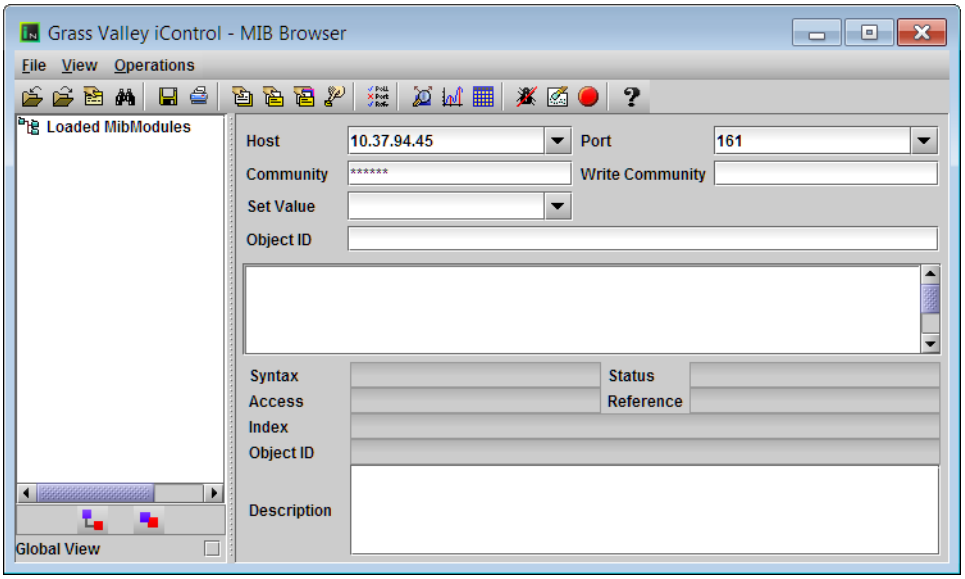
REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator (see page 697).

To access the MIB Browser

1. In iC Navigator, on the **View** menu, click **MIB browser**.

   SYSTEM RESPONSE: The MIB browser appears.



2. Load a MIB module by doing ONE of the following:
   - Click the Open button ( ) on the toolbar.

     OR,
   - On the **File** menu, click **Load MIB**.

   SYSTEM RESPONSE: The **Load a MIB File** window appears.
3. In **Load a MIB File**, use the **Open** tab, or the **Recent** tab, to navigate to the MIB file you wish to load, and then click **Open**.

   The selected MIB appears in the MIB browser's **Loaded MibModules** area.
4. Click on a MIB element to see its description.

Note: For more information, click the **Help** button ( ) on the MIB Browser menu (see Accessing the MIB Browser Help Files, on page 515).

See also

For more information about the MIB Browser, see page 712.

Opening the SNMP Driver Creator Window

You can open the **SNMP Driver Creator** window in iC Navigator or in iC Creator. The steps to do so differ only in how you open the Alarm Browser. Other than this, functionality remains the same and the user interface layout is consistent.

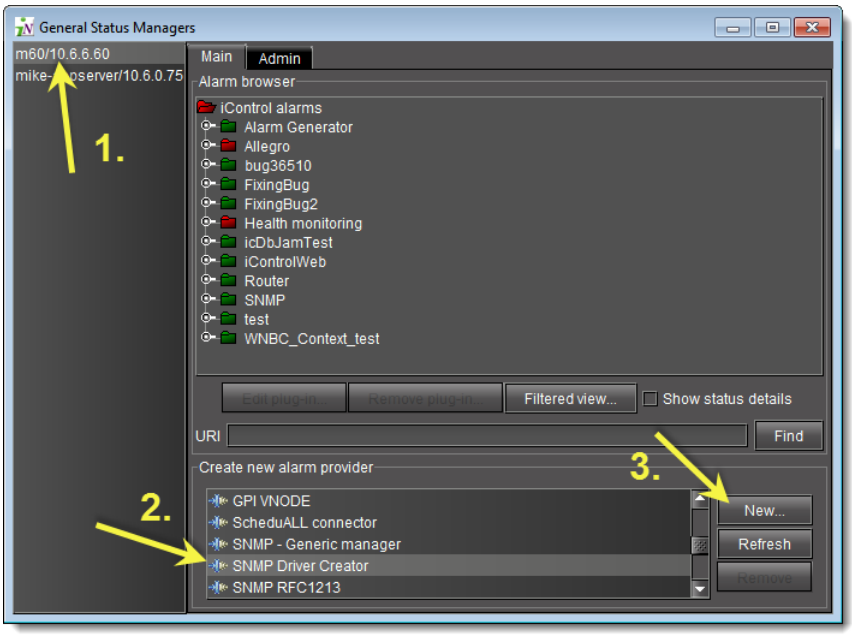
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

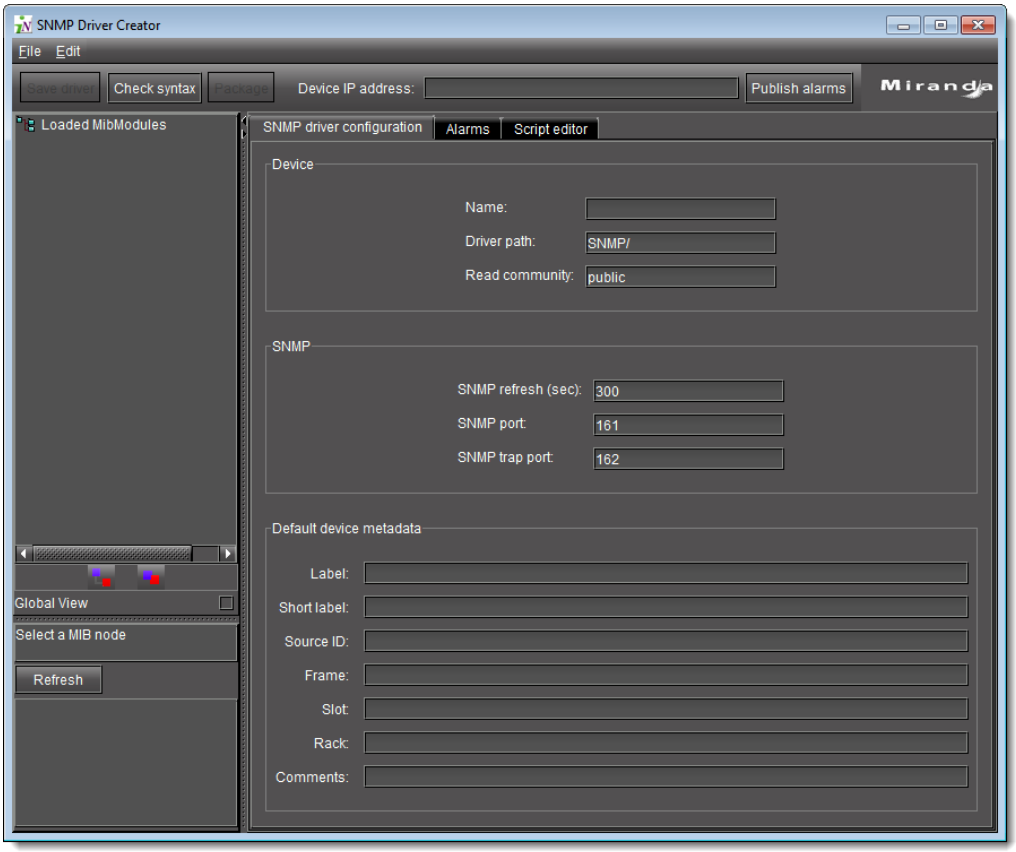
- If you are opening the **SNMP Driver Creator** window from iC Navigator, you have first:
  - started iControl on the Application Server hosting your GSM (see page 677).
  - opened iC Navigator (see page 697).
  - opened the GSM Alarm Browser (see Opening the GSM Alarm Browser, on page 710).
- If you are opening the **SNMP Driver Creator** window from iC Creator, you have first:
  - opened iC Creator from the Application Server hosting your GSM (see Working with iC Creator, on page 722).
  - opened the iC Creator Alarm Browser (see Using iC Creator to Verify GSM is Running on the Same Subnet as the Web Page, on page 638).

To open the SNMP Driver Creator window in iC Navigator

1. In the GSM Alarm Browser, in the left pane, select the Application Server hosting the GSM.



2. In the **Create new alarm provider** area, click **SNMP Driver Creator**, and then click **New**.
   SYSTEM RESPONSE: The **SNMP Driver Creator** window appears.



Opening Audio Video Fingerprint Analyzer

In order to configure, perform, and monitor lip-sync detection and comparison in iControl, you must first open **Audio Video Fingerprint Analyzer**.

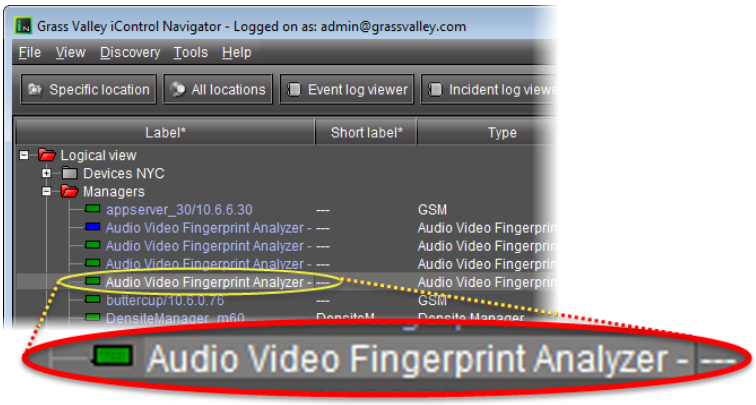
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

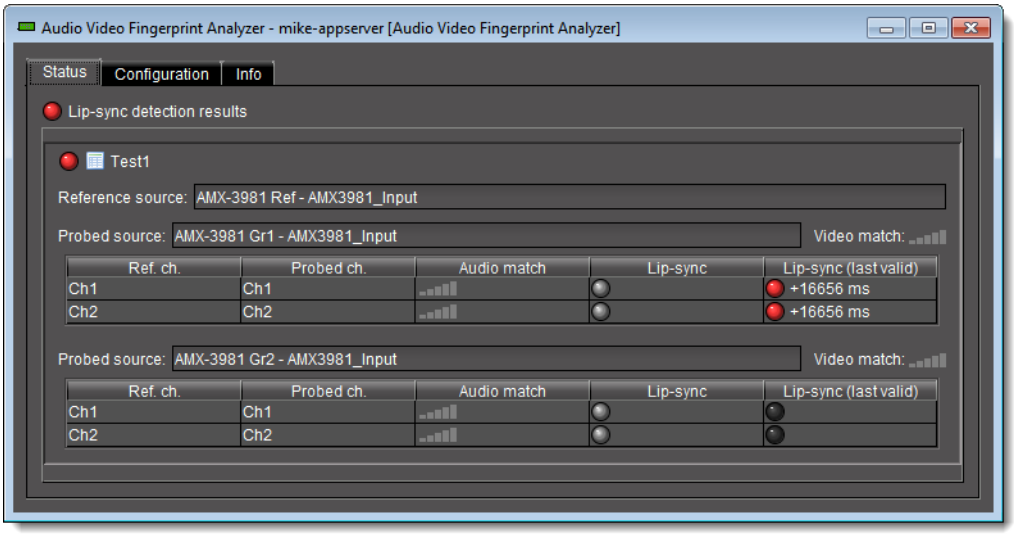
- You have opened iC Navigator (see page 697).
- Your Fingerprint Analyzer Service, intended probed sources and reference source are all visible in iC Navigator.

To open Audio Video Fingerprint Analyzer

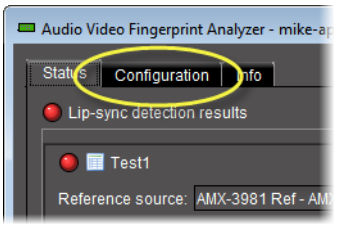
1. In iC Navigator, in the **Logical view**, expand the **Managers** folder, and then double-click **Audio Video Fingerprint Analyzer** (the link corresponding to the desired Application Server).



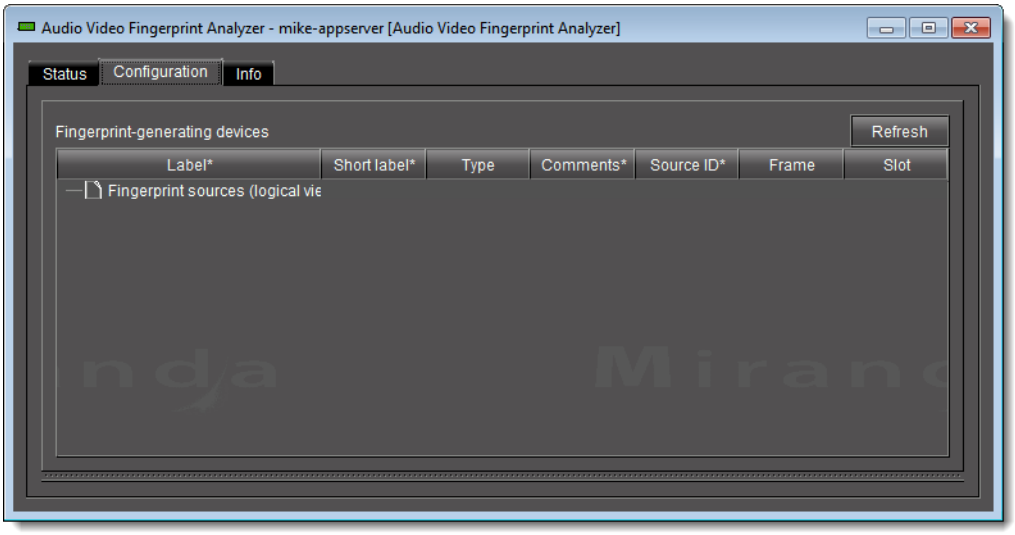
SYSTEM RESPONSE: The **Fingerprint Analyzer Service** window appears.



2. Click the **Configuration** tab to configure comparison groups.



SYSTEM RESPONSE: The fingerprint-generating devices appear in a list.



Opening GV Node Manager

Along with the other elements that represent a GV Node frame in iControl, which typically include service panels for the IFM-2T fabric module, Frame Controller module, and Frame Reference modules, GV Node Manager is available from iC Navigator.

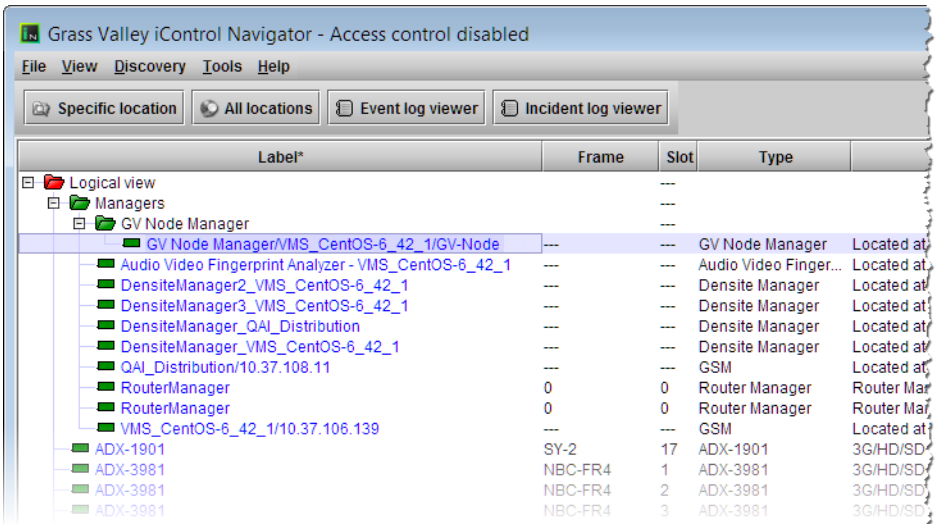
REQUIREMENTS

Make sure you meet the following conditions before beginning this procedure:

- You have opened iC Navigator (see page 697).
- You have added your GV Node frame to a Densité manager (see page 247).

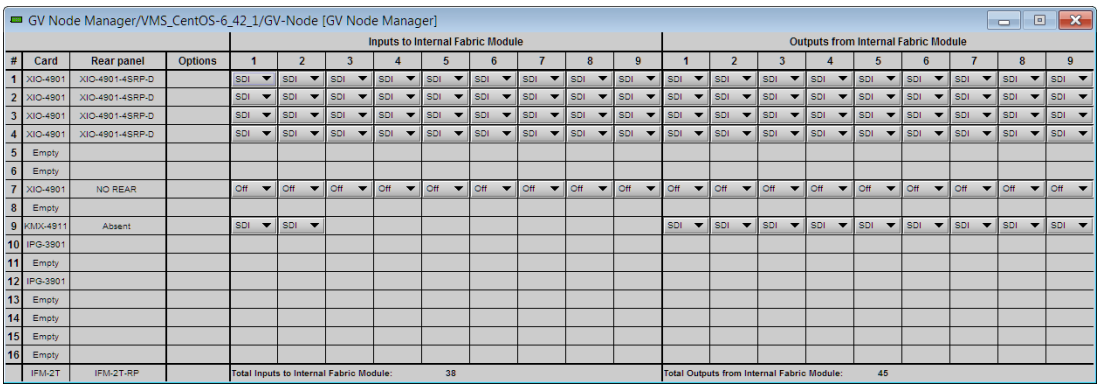
To open GV Node Manager

1. In iC Navigator's *Logical view,* open the *Managers* folder, and then the *GV Node Manager* folder.



Alternatively, locate your GV Node Manager in the *Physical,* or in the *Flat* view.

2. Double-click the GV Node Manager you would like to open.
   The **GV Node Manager** window opens.



iC Web Common Tasks

- Working with iC Web on page 717
- Exiting iC Web on page 722

Working with iC Web

- Opening iC Web on page 718
- Opening an iControl Web Site on page 719
- iC Web Shortcuts on page 721

Opening iC Web

REQUIREMENT

Before beginning this procedure, make sure you have started **iControl Launch Pad** (see page 681).

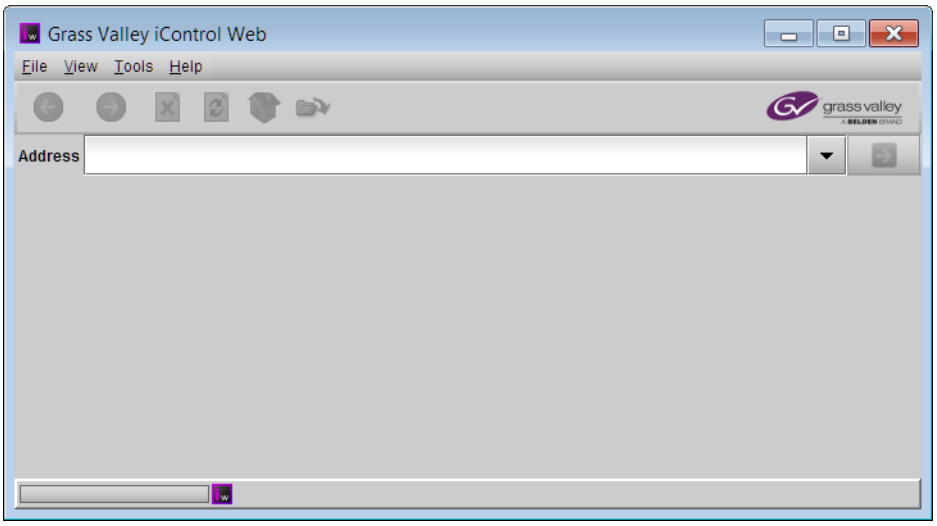
To open iC Web

1. On **iControl Launch Pad**, type the IP address of your Application Server, or select it from the list of available IP addresses.

2. Click the iC Web icon.

3. If access control is enabled for this Application Server's client applications, iC Web prompts you for credentials. Type the required user name, and password, select the appropriate domain (if required), and then click **OK**.

   SYSTEM RESPONSE: The iC Web splash screen appears, followed by a blank iC Web window.



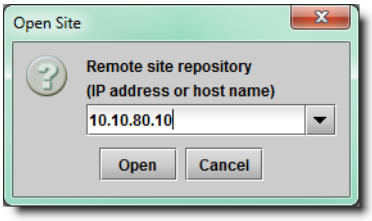
Opening an iControl Web Site

REQUIREMENT

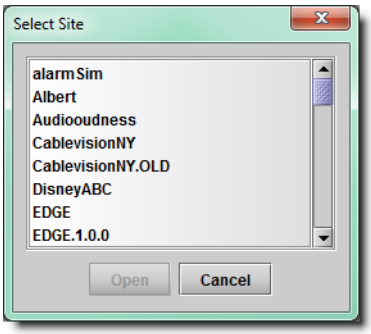
Before beginning this procedure, make sure you have started iC Web (see page 718).

To open an iC Web site

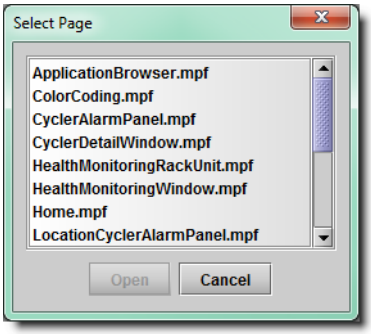
1. In the iC Web window, on the **File** menu, click **Open site**.
2. In the **Open Site** window, type the IP address or host name of the Application Server to which the site you wish to open has been published. You can, alternatively, choose an Application Server from the drop down menu, which contains a list of the most recently used servers. Click **Open**.



3. In the **Select Site** window, select a Web site from the list, and then click **Open**.

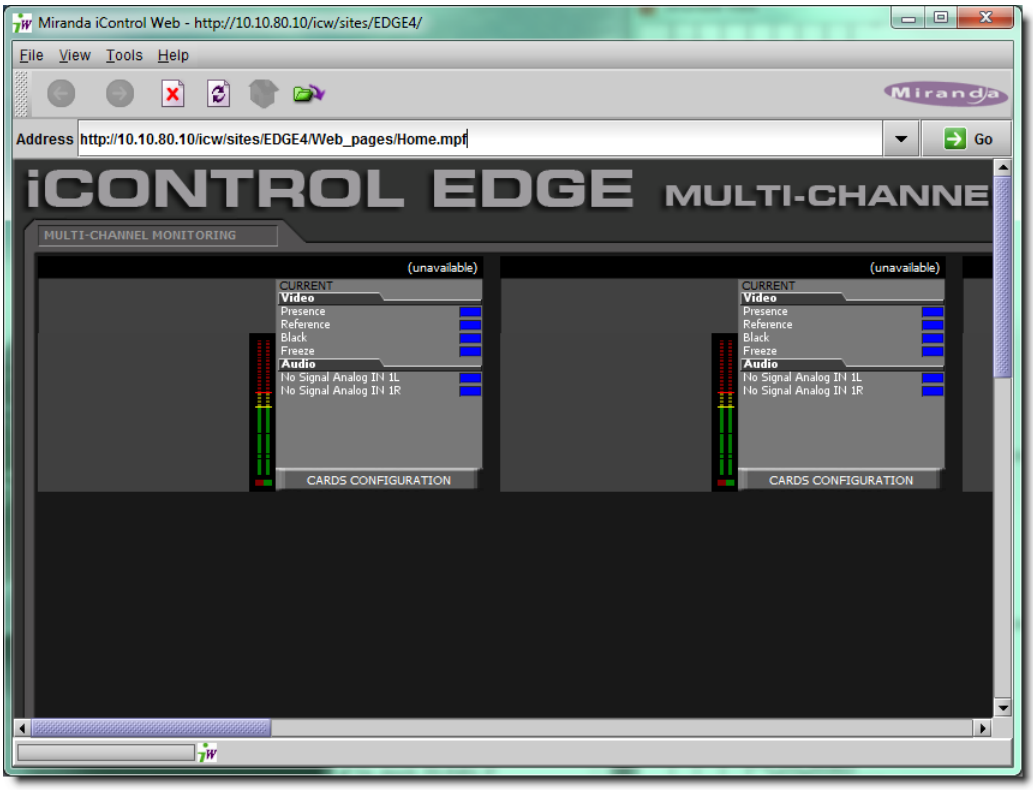


4. In the **Select Page** window, select a Web page from the list, and then click **Open**.

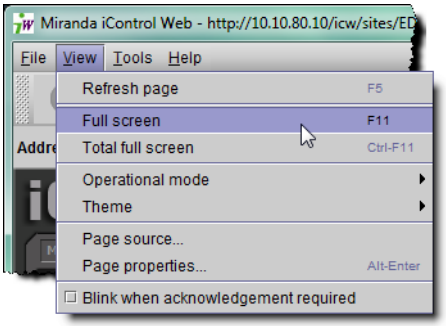


SYSTEM RESPONSE: A progress bar and message appear at the bottom of the iC Web window.

SYSTEM RESPONSE: In a few moments, the Web page appears.



5. To expand the iC Web window to accommodate large Web pages, choose **Full screen** or **Total full screen** from the **View** menu.



iC Web Shortcuts

The following shortcuts can be helpful in iC Web's full screen mode when there is no access to the menu:

Shortcuts	Description
Alt+left arrow	Back a page
Alt+right arrow	Forward a page

(*Continued*)

Shortcuts	Description
F5	Reload current page / frame
F11	Display the current Web Site in full screen mode. Pressing **F11** again will exit this mode
Ctrl+**F11**	Display ALL the Web Site in full screen mode. Pressing **Ctrl**+**F11** again will exit this mode
Esc	Stop page or download from loading
Ctrl+**Enter**	Quickly complete an address. For example, type `computerhope` in the address bar and press Ctrl+Enter to get `http://www.computerhope.com`.

Exiting iC Web

To end an iC Web session

- Close all iC Web windows.

iC Creator Common Tasks

Working with iC Creator

Opening iC Creator

REQUIREMENT

Before beginning this procedure, make sure you have started **iControl Launch Pad** (see page 681).

To start iC Creator

1. On **iControl Launch Pad**, type in the IP address of your Application Server, or select it from the list of available IP addresses.

2. Click the **iC Creator** icon.

3. If access control is enabled for this Application Server's client applications, iC Creator prompts you for credentials. Type the required user name, and password, select the appropriate domain (if required), and then click **OK**.

   SYSTEM RESPONSE: The iC Creator splash screen appears, followed by the iC Creator welcome screen.

Creating a New Site

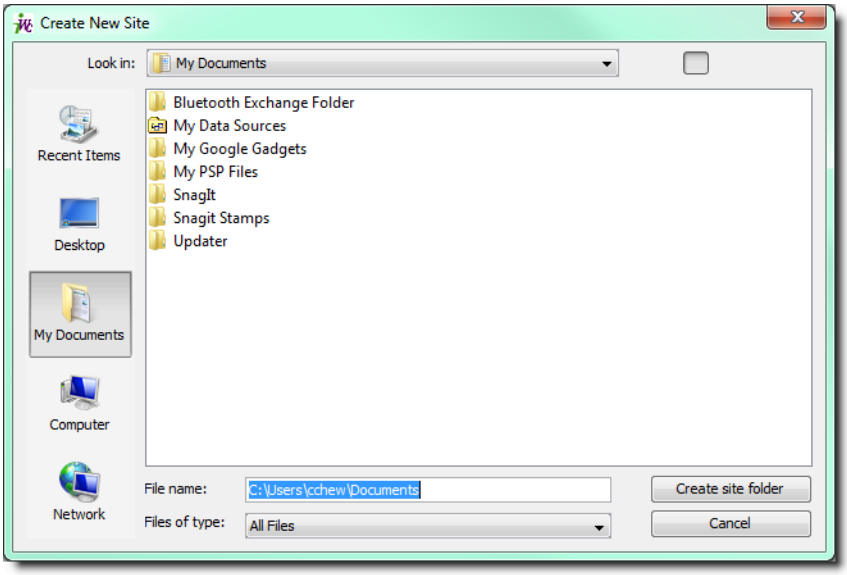
REQUIREMENT

Before beginning this procedure, make sure you have started **iC Creator** (see page 722).

To create a new site

1. In the **iC Creator Welcome** window, select **Create a new local site**, and then click **Next**.

   SYSTEM RESPONSE: The **Create New Site** window appears.



2. Browse to the location you wish to save your new site. Type a file name (do *not* use spaces), and then click **Create site folder**.

   SYSTEM RESPONSE: The **iC Creator** main window appears.

Opening an Existing Site

REQUIREMENT

Before beginning this procedure, make sure you have started **iC Creator** (see page 722).

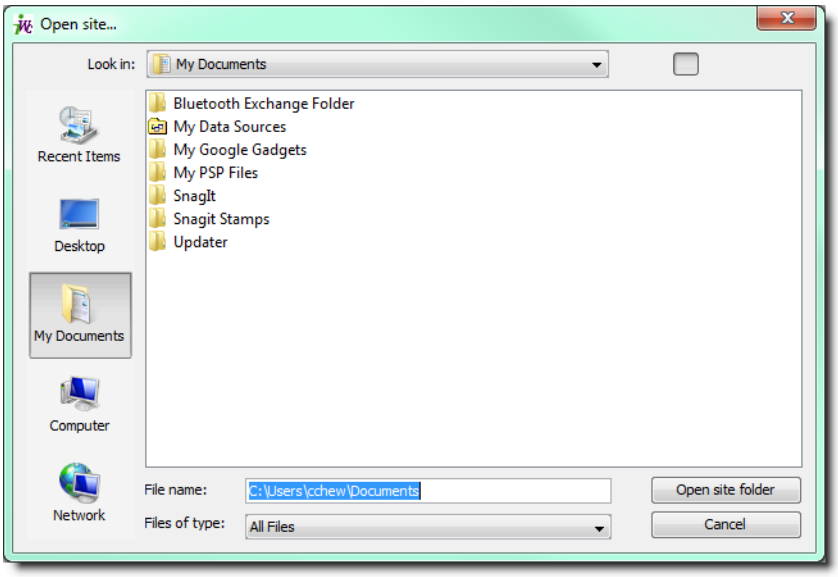
To open an existing (locally stored) site

1. In the **iC Creator Welcome** window, select **Open an existing site**, and then click **Next**.

   SYSTEM RESPONSE: The **Welcome to iControl Web Creator** window appears, showing options for opening a local or remote site.

2. Click **Browse** (...) beside the **Open local site** field.

   SYSTEM RESPONSE: The **Open site** window appears.



3. Locate and select the folder that has the Web site name you want to open, and then click **Open site folder**.

   SYSTEM RESPONSE: The **iC Creator** main window appears.

Opening an Existing Remote Site

REQUIREMENT

Before beginning this procedure, make sure you have started **iC Creator** (see page 722).

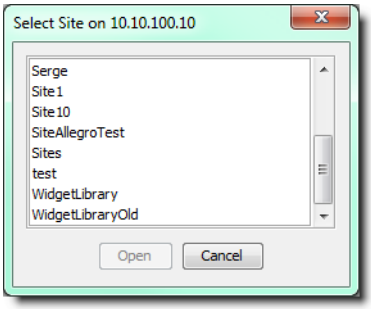
To open an existing remote site

1. In the **iC Creator Welcome** window, select **Open an existing site**, and then click **Next**.

SYSTEM RESPONSE: The **Welcome to iControl Web Creator** window appears, showing options for opening a local or remote site.

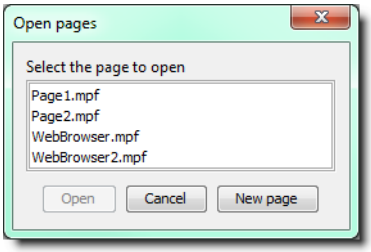
2. In the **Open remote site** combo box, select or type an IP address for the Application Server to which the site has been published.
3. Click **Open**.

   SYSTEM RESPONSE: The **Select site** window appears, showing all sites published to that Application Server.



4. Select a site, and then click **Open**.

   SYSTEM RESPONSE: The **Open pages** window appears, showing all pages in the site you are opening.



5. Select a page, and then click **Open**.

Note: By convention, the initial page for an iC Web site is called `home.mpf`.

Opening the Pages Privilege Management Window

REQUIREMENT

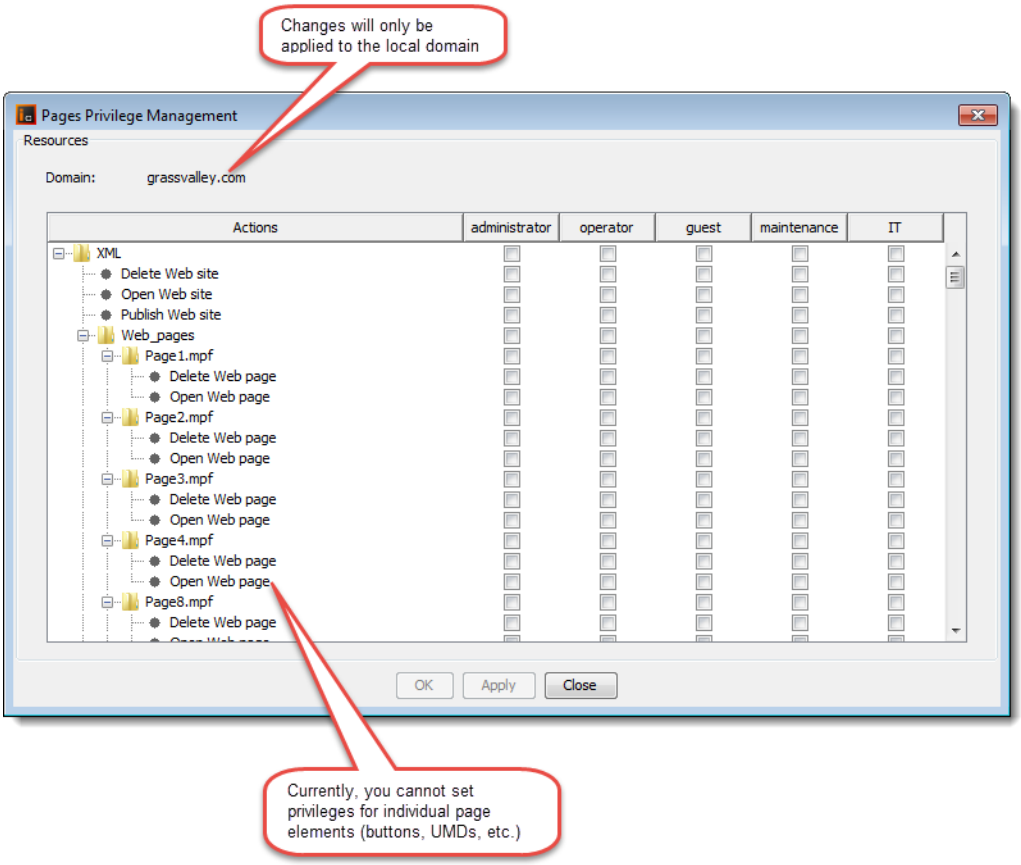
Before beginning this procedure, make sure you have opened **iC Creator** (see page 722), and logged in as a user with an appropriate role. The default credentials associated with the *super* role are:

- User: `admin`
- Password: `admin`

To open the Pages Privilege Management window

- On the **View** menu, point to **Access control**, and then click **Configure resources**.

  SYSTEM RESPONSE: The **Pages Privilege Management** window appears.



Note: In order to be able to modify user privileges, you must have the appropriate permissions (i.e., the role associated with your user name must have permission to manage privileges). The *super* role has this permission by default.

Exiting iC Creator

To end an iC Creator session

- Close all iC Creator windows.

  System Response: You will be prompted to save any pending changes.

iC Router Common Tasks

Opening iC Router

REQUIREMENT

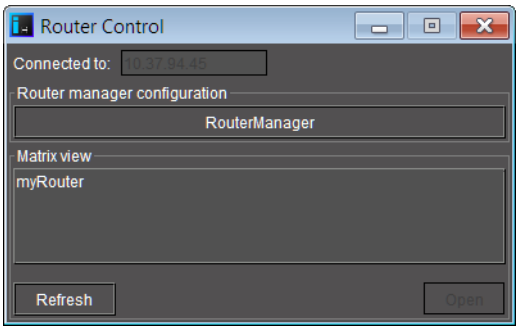
Before beginning this procedure, make sure you have started **iControl Launch Pad** (see page 681).

To open iC Router

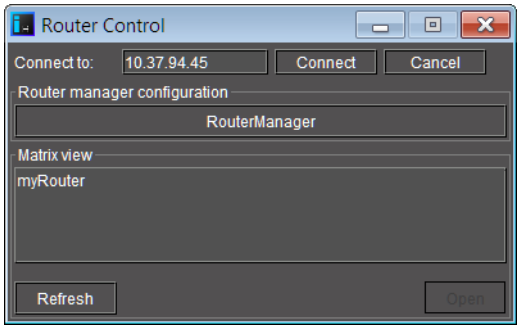
1. On **iControl Launch Pad**, either type in the IP address of your Application Server or select from the list of available IP addresses.

2. Click the **iC Router** icon.

System Response: The **Router Control** window appears.



3. Perform the following tasks in the **Router Control** window, as required:

To do this...	...do this...
Connect to a different Router Manager's IP address (*other than the one currently displayed*)	1. Click within the **Connected to** box. 2. Delete the existing IP address. 3. Type the new Router Manager's IP address. 4. Click **Connect**. 
Open **Router Manager Configurator**	• Click **RouterManager**. If access control is enabled for this Application Server's client applications, iC Router prompts you for credentials. Type the required user name, and password, select the appropriate domain (if required), and then click **OK**.
Start router control software.	1. Select the desired item under **Matrix view**. 2. Click **Open**. If access control is enabled for this Application Server's client applications, iC Router prompts you for credentials. Type the required user name, and password, select the appropriate domain (if required), and then click **OK**.

See also

For more information about iC Router, refer to the *iControl Router Quick Start Guide,* and *iControl Router User Guide.*

B Glossary

Term	Definition
Alarm	Alarms are the central feature of monitoring in iControl. There are three types of alarms in the General Status Manager (GSM): events, statuses, and text alarms. Each alarm is a status report on a specific condition within a site, triggered by equipment interfaced with the iControl system, or by scripts. Alarms can appear on an **iC Web** page, in the Alarm Browser, in **iC Navigator**, and in system logs.
Allégro	Grass Valley's Allégro is a line of 1 RU streaming encoders/servers that enables real-time confidence monitoring of remote signals by using low latency streaming of video, audio and data over a standard IP network. Allégro combines encoder and server functions to allow streaming audio, video and data to be sent over standard IP networks for monitoring of critical broadcast signals. It integrates telemetry such as signal presence, VBI extraction and audio level metering. Allégro encoders can be remotely managed from a central location, and numerous local and remote player clients can monitor the same signal. Streaming video for Allégro can be fully integrated into Grass Valley's iControl or Kaleido products.
Application Server	The iControl Application Server is a compact server that interfaces to audio, video, and other hardware through a variety of configurable ports (RS-232, RS-422, Ethernet). The Application Server hosts the various software modules that make up iControl. Users connect to an Application Server from any desktop or portable computer, using a Web browser.
GSM	General Status Manager is an iControl service responsible for central management of all alarm conditions and error logging.
iC Navigator	**iC Navigator** is an application that lets operators view, control and monitor devices on an iControl network. It gives operators direct access to the control windows of both Grass Valley Technologies and third-party equipment. It shows the status of devices and services in a hierarchical view, so that a system problem can quickly be pinpointed. It also supports administrative tasks such as status reporting and logging.
iC Router	iControl Router is a flexible graphical user interface that provides advanced router control and status monitoring. With protocol drivers for many router models, iControl Router software may be configured to control multiple routers from multiple vendors from a single user interface. This enables operators to simultaneously manage routers from different vendors without having to deal with differences in functionality and user interface. iControl Router is controlled over regular IP networks and multiple users can use it to monitor and control several routers, either locally or from remote locations.
iC Web	**iC Web** is a Web-based device-monitoring module made up of two applications: **iC Creator** is a tool for creating sites to provide a user-friendly interface for operators to control and monitor devices connected throughout the iControl environment. **iC Web** Site allows you to view and access sites available on the iControl Application Server. You may see **iC Web** Site referred to as the "runtime mode" of **iC Web**.
iControl	Grass Valley's iControl is a high level Element Management System which operates with sophisticated telemetry probes to provide advanced facility monitoring over IP. The system leverages industry standard SNMP protocols, and can fully integrate third party control applications to create a complete facility monitoring environment. With automated reactions to failures, and guided operator response, the system can deliver dramatically reduced down times.

(*Continued*)

Term	Definition
Kaleido	Grass Valley's Kaleido line of multi-image display processors features auto-sensing HD-SDI, SDI, and/or analog composite video inputs, and a high quality DVI output with a resolution of up to 1920 x 1080 pixels. The Kaleido offers advanced video and audio probing, including the following alarms: signal black, freeze and luminance too high, audio presence, overload, mono and out-of-phase. The feature-rich display can also include audio level metering (embedded, AES and analog), along with Source IDs, tallies, aspect ratio markers, and clocks/timers.
M-Audio Transit USB	Third party audio transcoder, USB-based. Enables an Allégro-1-RGB to receive analog audio output from a Kaleido-Alto/Quad.
RMI daemon	Remote Method Invocation daemon, a service that enables Java objects to communicate with each other remotely. This service is necessary for iControl applications.
URI	A Uniform Resource Identifier is string of characters used to identify a resource. In iControl, URIs are used to identify each and every element of a network—from hardware devices, such as cards and frames, to logical resources, such as services, alarms, Web pages and user interface elements.
Virtual Alarm	A virtual alarm is a special type of alarm that allows a logical combination of multiple arbitrary alarms. A virtual alarm is made up of one or more sub-alarms. Technically a virtual alarm is an alarm provider that provides a single alarm. Any alarms in iControl—including other virtual alarms—can be combined together to form a new, higher-level alarm (provided the new virtual alarm does not create a cyclical dependency).
XEdit	XEdit is the Kaleido-X layout editor, a software intended to be run on a remote computer. Its purpose is to create and apply the necessary configuration for layouts, rooms, system, channels, and RCP user definitions as required for successful operation of the Kaleido-X.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X

Contact Us

Grass Valley Technical Support

For technical assistance, contact our international support center, at 1-800-547-8949 (US and Canada) or +1 530 478 4148.

To obtain a local phone number for the support center nearest you, please consult the *Contact Us* section of Grass Valley's website (`www.grassvalley.com`).

An online form for e-mail contact is also available from the website.

Corporate Head Office

Grass Valley
3499 Douglas-B.-Floreani, St-Laurent, Québec H4S 2C6, Canada

Telephone: +1 514 333 1772
Fax: +1 514 333 9828
Web: `www.grassvalley.com`