iControl Edge Version 1.20
Installation & Setup Guide

Miranda

Copyright Notice

Copyright © 2009 Miranda Technologies Inc. All rights reserved.

ATTENTION: please read the following terms and conditions carefully. By using iControl Edge documentation, you agree to the following terms and conditions:

Miranda Technologies Inc. hereby grants permission and license to owners of iControl Edge to use their product manuals for their own internal business use. Manuals for Miranda Technologies Inc. products may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose unless specifically authorized in writing by Miranda Technologies Inc.

A Miranda Technologies Inc. manual may have been revised to reflect changes made to the product during its manufacturing life. Thus, different versions of a manual may exist for any given product. Care should be taken to ensure that one obtains the proper manual version for a specific product serial number.

Information in this document is subject to change without notice and does not represent a commitment on the part of Miranda Technologies Inc.

Warranty Policies

Warranty information is available in the Support section of the Miranda Web site (www.miranda.com).

Title	iControl Edge Version 1.20 Installation & Setup Guide
Part Number	M867-0602-101
Revision	November 18, 2009 4:21 pm

toc

Table of Contents

Appendix A: Troubleshooting   89

Appendix B: Using PuTTY   93

Appendix C: Using WinSCP   97

Contact Us!   105

Introduction to iControl Edge

iControl Edge enables television service providers to cost-effectively monitor hundreds of television signals spread across multiple remote locations, using remotely controlled set-top boxes and receiver/decoders. It consists of a suite of existing Miranda products that have been specifically packaged into an "off-the-shelf" monitoring solution.

Summary

Overview

An iControl Edge system is a combination of various quantities and models of Miranda iControl, Allégro (optional), and Densité products as well as third-party set-top box infrared interface units. At each remote head-end, the set-top box signals are fed into Densité control probes or to an Allégro-1 Analog encoder/server. The signals are then streamed back to the Network Operations Center's iControl Edge monitoring system. The iControl Edge system can be easily expanded to offer set-top box monitoring of up to 16 head ends from a central Network Operations Center.

Combining the flexibility of iControl Web and the advanced processing and alarm capabilities of Densité probes, iControl Edge allows any television service provider to perform comprehensive *monitoring by exception* of all its important video and audio signals. Using LAN and WAN connectivity, iControl Edge allows complete monitoring of multiple signals, across wide geographical areas.

The system can include one or more Allégro encoders for streaming remote signals in the form of full-motion video and audible audio. This allows operators, from their desktop, to listen to audio programs and to view high-quality video streams featuring multiple video images, closed captioning, audio level meters and metadata.
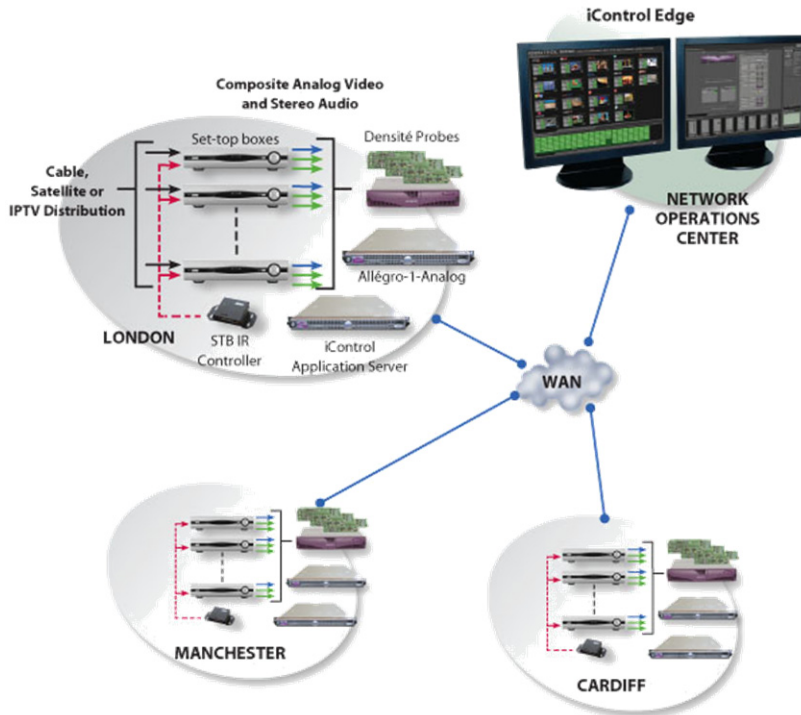
As a multi-signal monitoring system, iControl Edge performs simultaneous verification on multiple remote, multi-format video, audio and ancillary signals from set-top boxes, while cycling through channels. The system provides signal probing on an extensive set of signal parameters, including:

- video signal loss
- video black
- video freeze
- video luma
- macroblocking (optional)
- audio silence
- audio overload

In the event of a signal fault, the system generates alarms and provides telemetry information, which is automatically logged for reports.

Customizable elements (e.g. station names, signal paths) are stored in spreadsheets that can be edited using the Microsoft® Excel® spreadsheet software. By adding elements to (or removing them from) a spreadsheet, you can dynamically update your monitoring system.

Operational Overview

The diagram below shows the relationship between the elements of an iControl Edge system, and how they work together to provide real-time monitoring of signals.
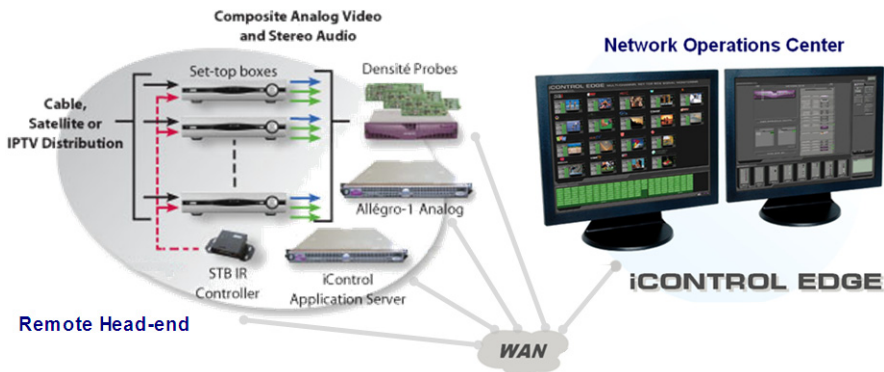
User Interface

Once the iControl Edge system is up and running, monitoring data and live audio/video streams are automatically presented to operators within a Web page. The operator has easy access to current and historical information on every device and signal being monitored.
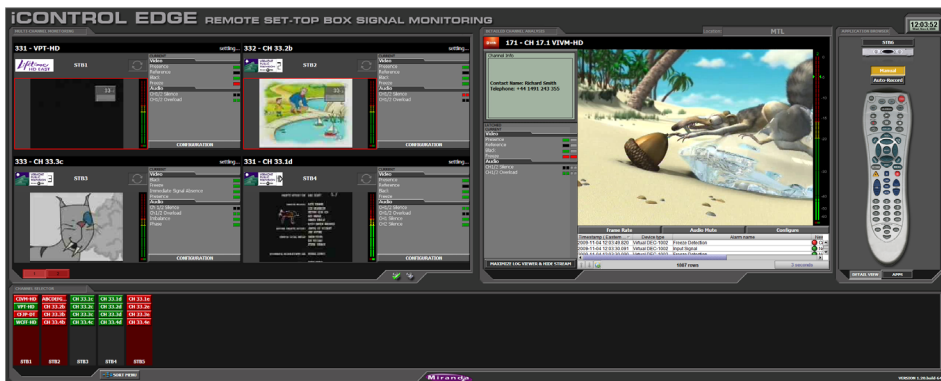
iControl Edge user interface (initial view)
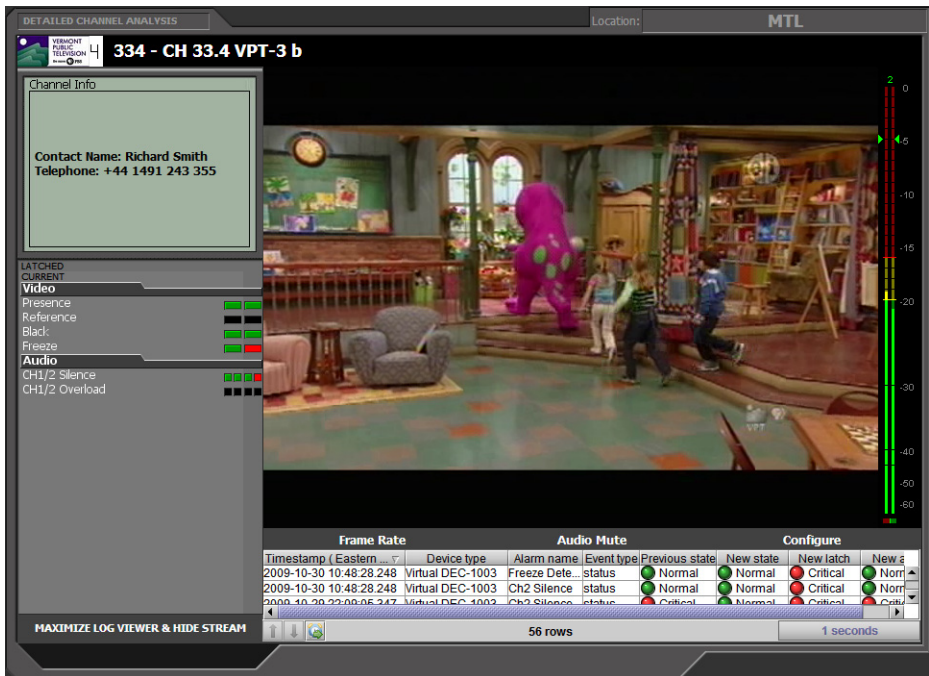
iControl Edge user interface (Detailed Channel Analysis area)
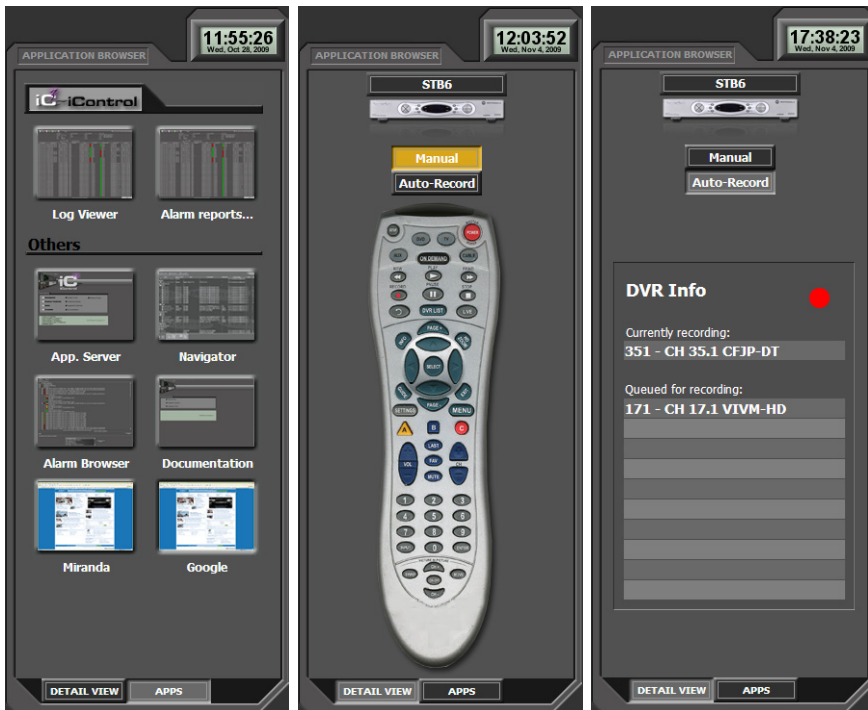
iControl Edge user interface (Application Browser area: Application Selector, Soft Remote, and DVR Info)
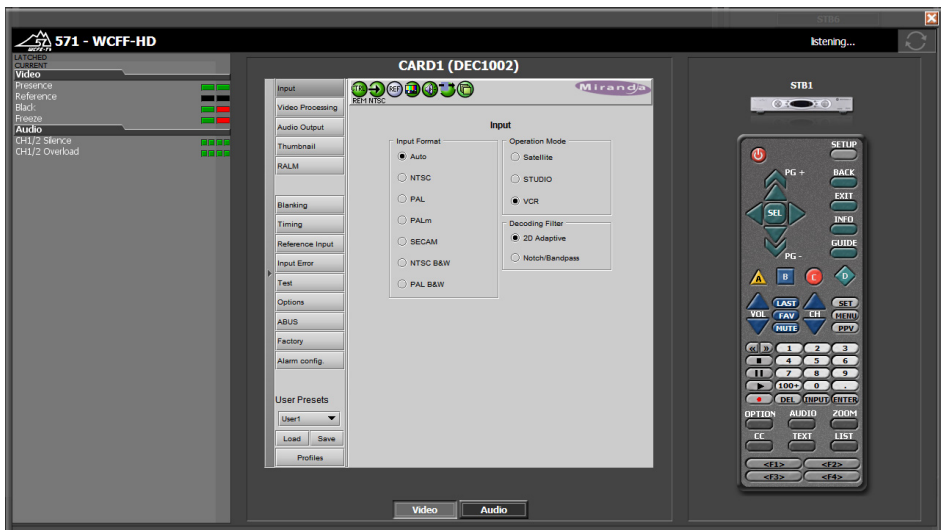
iControl Edge user interface (probe configuration window, with detailed alarm panel and soft remote)

Reference Material

The table below contains a list of some of the documentation available with your iControl Edge system. Each device also ships with a set of release notes that contain important information.

Part number	Description
M867-0602-101	iControl Edge Installation & Setup Guide
M867-0700-101	iControl Edge Operator's Overview
M659-9900-100	Densité CPU-ETH2 Enhanced Ethernet Controller Card Guide to Installation and Operation
M262-9900-101 -OR- M844-9900-100	Densité Housing Frame Guide to Installation and Operation Densité3 Housing Frame Guide to Installation and Operation
—	Global Caché GC-IRL IR Learner Quick Start Guide[1]
—	Global Caché GC-100-12 Network Adapter Quick Start Guide[1]
M226-9900-270	iControl User's Guide (available by clicking the Documentation link on the iControl Startup Page)
—	iControl v3.X User's Guide [PRELIMINARY] (available by clicking the Documentation link on the iControl Startup Page)
M719-9900-280	Miranda Allégro-1 User Guide (available from the Allégro Startup page)

1. Available from the "Support Documents and Files" section of Global Caché's Web site
   (see http://www.globalcache.com/support/support_docs.html)

You may also need to refer to the documentation received with the set of Densité probes you ordered for your monitoring purposes.

Video probe		Audio probe	
Part number	Description	Part number	Description
M667-9900-100	VCP-1021 Composite Video Control Probe Guide to Installation and Operation	M649-9900-104	ACP-1721 Digital Audio Control Probe Guide to Installation and Operation
...or any of the following:		...with any of the following:	
M761-9300-102	DEC-1002 10-Bit Composite to SDI Decoder Guide to Installation and Operation	M768-9900-101	UAP-1781 –Eight Channel Universal Audio Processor Installation and Operation Manual
M761-9400-100	DEC-1003 10-Bit Composite to SDI Decoder Guide to Installation and Operation	M768-8900-101	UAP-1783 Eight Channel Universal Audio Processor Guide to Installation and Operation
M761-9900-101	DEC-1021 12-Bit Composite to SDI Decoder Guide to Installation and Operation	M768-8200-100	AAP-1741 Four Channel Analog Audio Processor Guide to Installation and Operation
M761-9500-100	DEC-1023 12-Bit Composite to SDI Decoder Guide to Installation and Operation		
...or the following probe:		...with the following converter:	
M813-9900-110	HCP-1801HD/SD SDI Control Probe Guide to Installation and Operation	M822-9900-101	ADC-800 CAM HDV Camera HD/SD A-to-D Converter Guide to Installation and Operation
M666-9900-100	SCP-1121 Digital Video Control Probe w. Embedded Audio Guide to Installation and Operation		

Note: When referring to the documents listed above, keep in mind that the constituent products of an iControl Edge system may have features that are not supported in the context of iControl Edge.

System Requirements 2

This section lists the iControl Edge system requirements.

Hardware Requirements

iControl Edge Clients

Client platforms must meet the following system requirements:

Processor	Intel Pentium 4 or equivalent
Operating System	Windows XP Professional
Memory	2 GB RAM
Graphics Card	Optimized for nVidia GeFORCE 6600GT (PCI Express, 128 MB DDR3, 1 GHz)
Sound Card	For monitoring audio signals streamed from the Allégro, if applicable

Software Requirements

You can connect to an iControl Edge Application Server from any client PC or laptop on your network. The first step is to obtain the host name or IP address of the Application Server. Once you connect to an Application Server, you can download iControl Edge software to your PC or laptop. Once launched, this

software will continue to run on your PC or laptop, communicating with distributed network applications that may or may not reside on the Application Server where the initial connection was made.

The components of your iControl Edge system must meet the following requirements:

Device	Software Version
Application Server	3.30 or later
Allégro-1 Analog	3.00 or later

To run any application in the iControl Edge suite, you must have the following software installed on your PC or laptop:

- a Web browser (e.g. Internet Explorer 6.0 or later, Mozilla Firefox 1.5 or later)
- Java 2 Runtime Environment (JRE) version 1.5.0_07). The installer file for JRE version 1.5.0_07 (which includes Java Web Start) can be downloaded by following the **Useful Downloads** link on the iControl Startup page.

> **Note:** If the Java Web Start application reports errors regarding the inability to find files, it is important to clear both the Internet Explorer cache and the Java Application cache.

To modify the Configuration Spreadsheets used to define the iControl Edge monitoring layout, you will need a PC or laptop with the Microsoft® Excel spreadsheet software.

Installation and Network Requirements

Network Capacity

We recommend that you install all iControl Edge devices, as well as any associated equipment, on a dedicated LAN. The quality of service of your iControl Edge system (including streaming bit rate, frame rate, and the number of concurrent users possible) is directly related to the capacity of your network.

Network Clients

Users can access the iControl Edge Application Server using a Web browser (Microsoft Internet Explorer or Mozilla Firefox) on a client PC or laptop running Windows®. When a user logs on and launches an iControl module (e.g. iC Web), the software is automatically downloaded from the Application Server and runs on the client PC or laptop.

Note: On the client PC or laptop, the firewall must be disabled. Only one network interface card (NIC) should be enabled. It is recommended to use a wired network connection and disable any wireless adapter.

Security

iControl Edge can be incorporated into your existing security infrastructure. A qualified system administrator should verify that the setup follows your organization's security standards.

Network Configuration

Each device in your iControl Edge system arrives pre-configured with default IP Address, Subnet Mask and Gateway. Instructions for changing these settings to conform to your network are provided further on in this document. The first table below provides an overview of the default settings. The second table can be used as a worksheet for recording your new network settings.

Default Network Settings:

Device	#	IP Address	Subnet Mask	Gateway
Application Server	—	10.0.3.6	255.255.0.0	10.0.3.6
Densité frame	—	192.168.3.1	255.255.255.0	—
Global Caché GC-100 network adapter	—	192.168.1.70	255.255.255.0	—
Allégro-1 Analog	—	10.0.3.7	255.255.0.0	—

Note: iControl Edge devices may be shipped with a sticker, usually located on the top of the enclosure, identifying the default network settings.

Your Network Settings:

Device	#	IP Address	Subnet Mask	Gateway
Application Server	01			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				

Your Network Settings:

Device	#	IP Address	Subnet Mask	Gateway
Application Server	02			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	03			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	04			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	05			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	06			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	07			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				

Your Network Settings:

Device	#	IP Address	Subnet Mask	Gateway
Application Server	08			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	09			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	10			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	11			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	12			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	13			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				

Your Network Settings:

Device	#	IP Address	Subnet Mask	Gateway
Application Server	14			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	15			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				
Application Server	16			
Densité frame				
GC-100 network adapter				
Allégro-1 Analog				

Installation & Setup

3

iControl Edge is a distributed system, which may entail installing hardware at more than one location. An iControl Edge Application Server is usually installed at each head end, with a number of set-tops and IR network adapters, Densité probes, and an Allégro. This section describes the physical setup of the iControl Edge hardware, as well as the configuration of network settings and other software parameters.

Summary

Key Concepts

Channel	TV or radio service that is addressable by a channel number on a set-top box (see "Services Worksheet" on page 70).

Input	A set-top box output that is used as an input to the iControl Edge system.
DVR	A set-top box that is also a digital video recorder.
Cycling set-top box	Within the iControl Edge system, a cycling set-top box (or DVR) is used to automatically cycle through a pre-determined channel list (see "Services Worksheet" on page 70). Video and audio probing is usually available on this input through the use of a pair of probes (one for the video signal and one for the audio), or of a single HCP-1801 video control probe with embedded audio (in conjunction with an ADC-800 CAM converter).
Manual set-top box	Within the iControl Edge system, a manual set-top box (or DVR) is not used for cycling. It can be controlled via the Remote Control area of the iControl Edge Web site. If the output of this set-top box is fed to an Allégro then it can be monitored from the Detailed Channel Analysis view. Streaming is usually available on this input. Probing is usually not available on this input.

Step 1: Preparing to Install an iControl Edge System

The components of an iControl Edge system are usually shipped separately. One Application Server may be sent to the Network Operations Center. One Application Server, the appropriate number of Densité frames and Global Caché GC-100 network adapters (IC -STB-CTL), and one Allégro-1 Analog system are typically sent to each peripheral site where remote monitoring will be taking place.

You should inspect the shipping containers at each location to make sure that the equipment arrived undamaged, and that all materials are included. If any items are missing or damaged, contact your distributor or Miranda Technologies Inc.

Make sure the following items have been shipped with your Application Servers:

☐ Application Server unit (Dell PowerEdge 850, 860, or R200 server)

☐ Rack mounting kit (rails, screws and washers)

☐ Power cord

Make sure the following items have been shipped with your GC-100 network adapters:

☐ Global Caché GC-100 network adapters (one for each set of 6 set-top boxes to be controlled)

☐ One AC power supply unit and AC cord

☐ Six IR emitter cables

Make sure the following items have been shipped with your Densité frames:

☐ Densité housing frame with one controller card

☐ The Densité series devices you ordered:

Video probes	Audio probes
VCP-1021 Composite Video Control Probe	ACP-1721 Digital Audio Control Probe
...or any of the following:	**...with any of the following**
DEC-1002 10-Bit Composite to SDI Decoder	UAP-1781 Eight-Channel Universal Audio Processor
DEC-1003 10-Bit Composite to SDI Decoder	UAP-1783 Eight-Channel Universal Audio Processor
DEC-1021 12-Bit Composite to SDI Decoder	AAP-1741 Four-Channel Analog Audio Processor
DEC-1023 12-Bit Composite to SDI Decoder	
...or the following probe:	**...with the following converter:**
HCP-1801HD/SD SDI Control Probe	ADC-800 CAM HDV Camera HD/SD A-to-D Converter

- ☐ One ADC-800 CAM HDV camera HD/SD A to D converter, for each HCP-1801 module you ordered
- ☐ Blank rear panels (for empty slots)
- ☐ One AC power supply unit and AC cord
- ☐ A second power supply and AC cord (optional)

Make sure the following items have been shipped with your Allégro systems:

- ☐ Allégro unit (Dell PowerEdge 850, 860, or R200 server)
- ☐ Rack mounting kit (rails, screws and washers)
- ☐ AC power cord

Once the hardware components are all in place, each device must be configured to work on a common TCP/IP network. Other operational parameters, such as which alarm conditions are to be monitored, should also be configured.

> **Note:** Densité devices ship with some pre-configured alarm settings that must be changed for proper operation of your iControl Edge system. See "Configuring the Probing Features" on page 36. Before making any such changes, please refer to the documentation specific to each device (see "Reference Material" on page 6).

You will need a PC or laptop that can connect to certain iControl Edge devices using a crossover Ethernet cable or via a network switch. The PC or laptop will need to have its network settings temporarily changed to ones that are compatible with the device.

Configuring a Client PC or Laptop

You will use a client PC or laptop to configure the various devices in your iControl Edge system. This client must have network configuration settings that will allow it to communicate with each device in its default state.

To configure the TCP/IP network settings of a client PC or laptop:

1. Open your PC's **Network Connections** control panel (on the Windows XP **Start** menu, point to **Control Panel**, and then click **Network Connections**).

2. Right-click the currently active **Local Area Connection**, and then click **Properties** on the shortcut menu.

3. In the **Local Area Connection Properties** window, select **Internet Protocol (TCP/IP)**, and then click **Properties**:
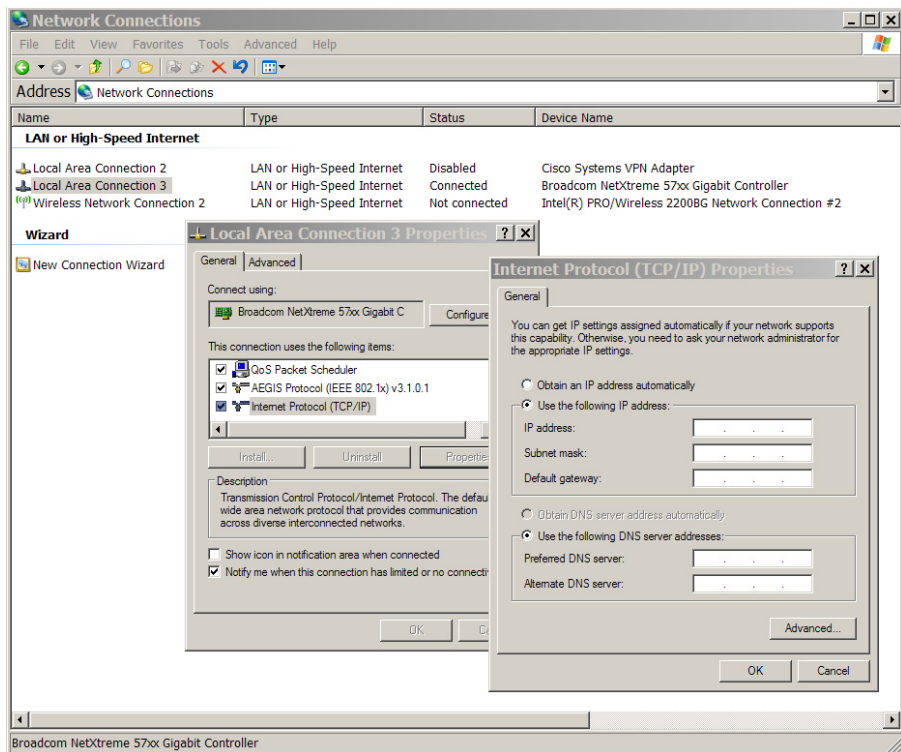
Configuring TCP/IP settings on a PC running Windows XP.

4. In the **Internet Protocol (TCP/IP) Properties** window, click **Use the following IP address**.

5. Type an IP address in the same range as the default IP address of the targeted device. For example, if the device is using the default address **10.0.3.6**, type **10.0.3.10** (refer to "Network Configuration" on

page 11, for the default addresses of the Application Servers, Densité frames, GC-100 network adapter, and Allégro systems).

6. Type a subnet mask in the same range as that of the targeted device.

7. Click **OK** to apply these settings.

8. Click **OK** again, to close the **Local Area Connection Properties** window.

9. Close the **Network Connections** control panel.

> **Note:** Remember to return the PC to its original network settings once you have finished configuring the devices.

Step 2: Installing & Configuring the Application Server

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

Physically Installing the Application Server

To install the Application Server:

1. Place the Application Server in a standard 19-inch rack, using the rails, screws and washers provided. Make sure that the unit has adequate ventilation.

2. To configure and operate the Application Server, you must be able to access it from a client PC or laptop over an Ethernet connection. Use the *eth0* port on the rear panel of the Application Server.

> **Note:** The 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. During the initial configuration process described in this document, you may find it more convenient, or even necessary, to connect your client workstation directly to the eth0 port using a crossover cable (not supplied).

3. Connect power cords, and then turn the server on. The power switch is located on the front panel.

4. Install the Miranda faceplate onto the front of the Application Server by sliding it onto the guide blocks on the side handles, and then pushing it in until it clicks into place.

> **Note:** Hardware documentation for the PowerEdge 850, 860 and R200 is available from the Dell Web site:
> http://support.dell.com/support/edocs/systems/pe850/
> http://support.us.dell.com/support/edocs/systems/pe860/
> http://support.dell.com/support/edocs/systems/per200/

Configuring the Application Server

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

- connect to the Application Server from a client PC or laptop
- ensure that the client PC or laptop has the correct version of the Java Runtime Environment installed
- log on to the Application Server's Webmin utility
- configure the Application Server's Ethernet interface settings
- configure the Application Server's Domain Name Service settings
- configure the Application Server's host name and IP address
- apply your changes and perform a readiness check

Connecting to the Application Server

To connect to the Application Server:

1. Set the IP address of your client PC or laptop to **10.0.3.10** with subnet **255.255.0.0** (see "Configuring a Client PC or Laptop" on page 18).

> **Note:** Record your PC's existing settings so you can return to them later.

2. Open a browser window on the client PC or laptop.

3. In the address bar, type **10.0.3.6** (this the default IP address of the Application Server).

> **Note:**   The default IP address and subnet mask settings for the Application Server are shown on a sticker on the top cover of the chassis.

The iControl Startup Page appears:

Installing Java

In the course of using iControl Edge, certain software modules (e.g. iC Web) may be downloaded from the Application Server to your client PC or laptop. To run any of these iControl applications, you must have the Java 2 Runtime Environment (JRE) installed on your PC or laptop. The installer is available from the Application Server itself.

To install the Java 2 Runtime Environment on your PC or laptop:

1. Click **Useful downloads** on the iControl Startup page.

2. Click **JRE for Windows**. When prompted, save the installer file (the file name should be similar to `jre-1_5_07-windows-i586-p.exe`).

3. Open the installer file. The installation process takes several seconds.

   Once completed, a confirmation message appears.

Logging on to Webmin

Webmin is the Application Server's built-in Web management utility. Logging on to Webmin is the starting point for accomplishing many tasks, including configuring the Application Server.

To log on to the Webmin utility:

1. Click **System Tools** on the iControl Startup page.

   The System Tools page appears:
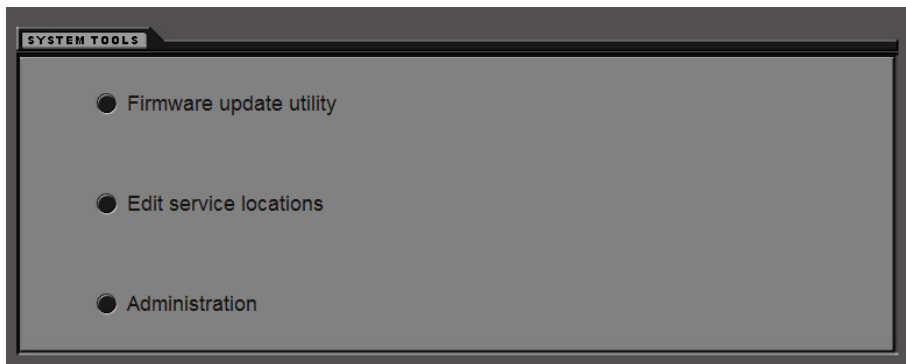
2. Click **Administration**.

   The **Login to Webmin** window appears:

   Type your user name and password. By default, these are:
   Username: *miranda*
   Password: *icontrol*

3. Click **Login**.

   The iControl Webmin home page appears:

The Webmin home page.

Configuring the Network

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

To configure the network:

1. Specify the DNS settings to be used by your Application Server (see "Specifying DNS Client Settings" on page 24).

2. Configure your host addresses (see "Configuring Host Addresses" on page 26).

3. Specify a network gateway to be used by your Application Server (see "Specifying a Network Gateway" on page 27).

4. Configure the Ethernet interface (see "Configuring the Ethernet Interface" on page 29).

5. Restart the system and verify the configuration (see "Restarting the System and Verifying the Configuration" on page 31).

Navigating to the Network Configuration Page

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

•   You you have launched iControl (see "Connecting to the Application Server" on page 20).

•   You are logged on to iControl Webmin (see "Logging on to Webmin" on page 22).

To navigate to the Network Configuration page:

•   On the Webmin home page, click **Network Configuration**:
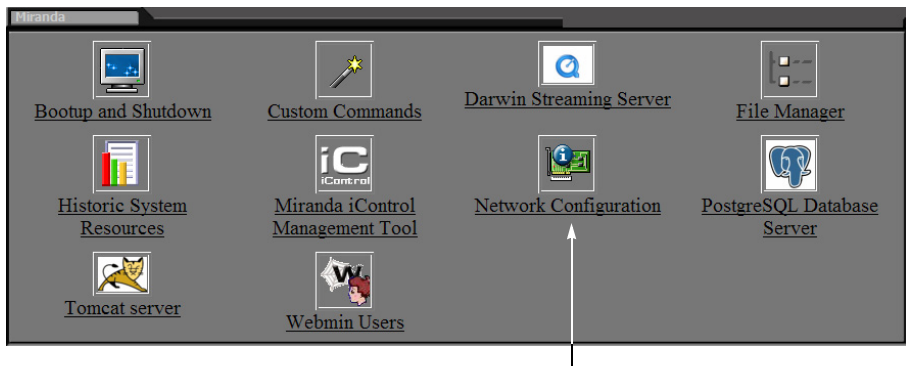
The Network Configuration page appears:
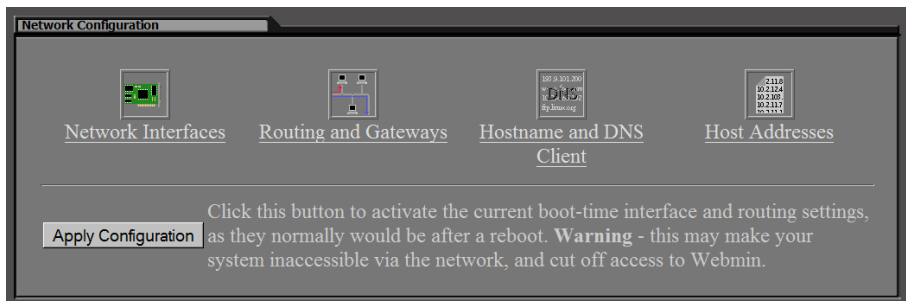
Specifying DNS Client Settings

The Domain Name Service (DNS) is a type of directory service that translates host names to IP addresses and vice versa. For the most part, Application Servers and other devices on an iControl network rely on IP addresses, and so DNS is not usually needed. There are, however, circumstances where DNS is required, such

as when an Application Server needs to have access to the Internet in order to display a Web page from some external source (e.g. www.weather.com).

Before beginning this procedure, make sure you have navigated to the Network Configuration page of Webmin (see "Navigating to the Network Configuration Page" on page 24).

To specify the DNS settings to be used by this Application Server:

1. On the Network Configuration page, click **Hostname and DNS Client**.

   The Hostname and DNS Client page appears:

2. In the **Hostname** box, type the host name by which you would like this Application Server to be known on your network.

3. Select the **Update hostname in host addresses if changed** check box.

   Note: This function ensures the host name in the Host Addresses page is the same as the host name in the Hostname and DNS Client page.

4. Configure the other parameters as required:

Resolution Order	Do not change the values in these six boxes unless your system administrator advises otherwise.
DNS Servers	The IP address 127.0.0.1, corresponding to localhost, appears by default. Do not change this address. You may type the addresses of other DNS servers in the lines below. Consult your system administrator.
Search Domains	Click the Listed radio button, and then type a list of all the domains where you wish to have the Application Server look for DNS services (one line per domain). You should type at least your own local domain name (e.g. miranda.com).

5. Click **Save**.

> **Note:** Clicking **Save** does not update the Application Server with the new configuration. To apply your changes, you still need to click **Apply Configuration** on the Network Configuration page or restart the system through Webmin (see "Restarting the System and Verifying the Configuration" on page 31).

6. Return to the Network Configuration page by clicking the Return arrow at the bottom of the Hostname and DNS Client page.

> **Note:** Do not click **Apply Configuration** on the Network Configuration page.

Configuring Host Addresses

Before beginning this procedure, make sure you have navigated to the Network Configuration page of Webmin (see "Navigating to the Network Configuration Page" on page 24).

To configure host addresses:

1. On the Network Configuration page, click **Host Addresses**.

   The Host Addresses page appears. The currently defined hosts are listed, showing the IP address and host name of each:
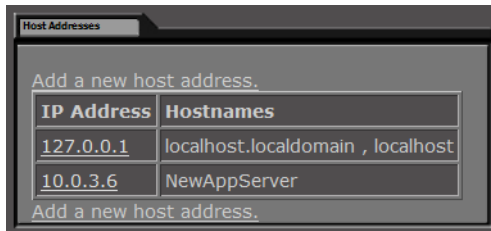
   Notes
   - The first entry (IP Address: 127.0.0.1, Hostname: localhost.localdomain, localhost) is predefined and should be left as found.
   - The host name you defined in step 2 of "Specifying DNS Client Settings" on page 24 should be listed here. However, you will need to assign an appropriate IP address to this Application Server.

2. Click the IP address of the Application Server (10.0.3.6 in the example screen shown above).

   The Edit Host Address page appears:

3. In the **IP Address** box, type the IP address you would like to give to this Application Server.

4. In the **Hostnames** box, make sure the listed host name is the correct one, and then (if required) type one or more other names that will refer to this IP address.

    Note: If the host name you entered on the Host Name and DNS Client page is not accurately listed here, correct this name in the Edit Host Address page, now.

5. Click **Save**.

    The Host Addresses page reappears. The saved host names will appear in the list.

    Note: Clicking **Save** does not update the Application Server with the new configuration. To apply your changes, you still need to click **Apply Configuration** on the Network Configuration page or restart the system through Webmin (see "Restarting the System and Verifying the Configuration" on page 31).

6. Return to the Network Configuration page by clicking the Return arrow at the bottom of the Host Addresses page.

    Note: Do not click **Apply Configuration** on the Network Configuration page.

Specifying a Network Gateway

In order for an Application Server to be able to send to (or receive data from) devices outside its own subnet, it must use a network gateway.

Before beginning this procedure, make sure you have navigated to the Network Configuration page of Webmin (see "Navigating to the Network Configuration Page" on page 24).

To specify a network gateway to be used by the Application Server:

1. On the Network Configuration page, click **Routing and Gateways**.

The Routing and Gateways page appears:

Routing and Gateways

Routing configuration activated at *boot time*

	Interface	Gateway
Default routes	eth0 ▾	10.10.80.1
	Any	
	lo	
Act as router?	eth1	○ No
Static routes	eth0	Network	Netmask	Gateway

	Interface	Network	Netmask
Local routes	eth0	224.0.0.0	255.255.255.255

[Save]

Active Routes

Destinaton	Gateway	Netmask	Interface
192.168.3.0	None	255.255.255.0	eth1
10.10.80.0	None	255.255.255.0	eth0
169.254.0.0	None	255.255.0.0	eth1
127.0.0.0	None	255.0.0.0	lo
Default Route	10.10.80.1		eth0

2. Select **eth0** from the **Interface** list in the **Default routes** area.

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

4. Click **No** beside **Act as Router**.

5. Leave the **Static routes** boxes blank.

6. In the **Local routes** boxes, do not change the value that appears for the eth0 interface unless your system administrator advises it.

7. Click **Save**.

> **Note:** Clicking **Save** does not update the Application Server with the new configuration. To apply your changes, you still need to click **Apply Configuration** on the Network Configuration page or restart the system through Webmin (see "Restarting the System and Verifying the Configuration" on page 31).

8. Return to the Network Configuration page by clicking the Return arrow at the bottom of the Routing and Gateways page.

> **Note:** Do not click **Apply Configuration** on the Network Configuration page.

Configuring the Ethernet Interface

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 section describes how to reconfigure eth0 to meet your local network requirements.

> **Note:** You must use *eth0* as your main network interface. Client applications (e.g. iC Navigator, iC Web, etc.) must be started via the Application Server's eth0 IP address. The other Ethernet port (*eth1*) is also configurable, but is intended for specialized use, such as connecting Miranda Densité frames and some third-party devices. As of iControl version 3.31, new Application Servers have the eth1 network interface disabled by default.

Before beginning this procedure, make sure you have navigated to the Network Configuration page of Webmin (see "Navigating to the Network Configuration Page" on page 24).

To configure the Ethernet interface:

1. On the Network Configuration page, click **Network Interfaces**.

   The Network Interfaces page appears. This page shows all Ethernet interfaces currently active, and lists those that will be activated any time the system starts:

2. Click **eth0** in the **Name** column.

   The Edit Bootup Interface page appears:

> **Note:** This page shows the current settings for the eth0 interface, which are the factory default values if you are configuring this port for the first time.

3. Click **Static**, and then type the fixed IP address you would like to use for this Application Server:

Notes

- Make sure you type the IP address exactly as it is on the Edit Host Address page (see step 3 of "Configuring Host Addresses" on page 26).

- 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.

4. Type addresses in the **Netmask** and **Broadcast** boxes that correspond to your desired network configuration.

   The values you type should be based on the IP address and the desired network configuration. In the above example (10.10.80.10), the corresponding netmask has been configured as 255.255.255.0, with a resulting broadcast address of 10.10.80.255. You should always verify these values with your network administrator.

5. Leave the **MTU** box blank.

6. Click the **Yes** option button, next to **Activate at boot**.

   > **Note:** If you do not click **Yes**, the eth0 interface will return to its previous configuration the next time the system restarts.

7. Click **Save**.

Notes

- Clicking **Save** does not update the Application Server with the new configuration. To apply your changes, you still need to click **Apply Configuration** on the Network Configuration page or restart the system through Webmin (see "Restarting the System and Verifying the Configuration" on page 31).

- The Application Server's eth0 port is set to auto-negotiate, full duplex mode by default. This setting should not be changed. The network switch to which the Application Server is connected should also be set to auto-negotiate to avoid data packet loss.

Restarting the System and Verifying the Configuration

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.

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

- You are logged on to iControl Webmin (see "Logging on to Webmin" on page 22).
- You have performed step 2 through step 4 of "Configuring the Network" on page 23.

To restart the system and verify the configuration:

1. On the Webmin home page, click **Bootup and Shutdown**:

   The Bootup and Shutdown page appears.
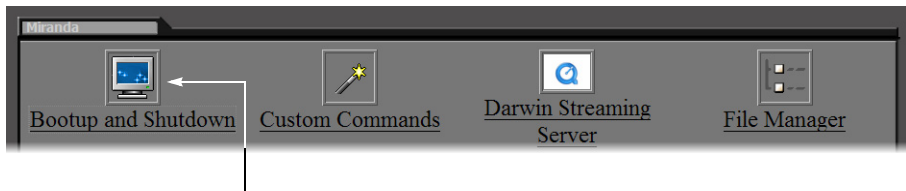
2. At the bottom of the Bootup and Shutdown page, click **Reboot System**:
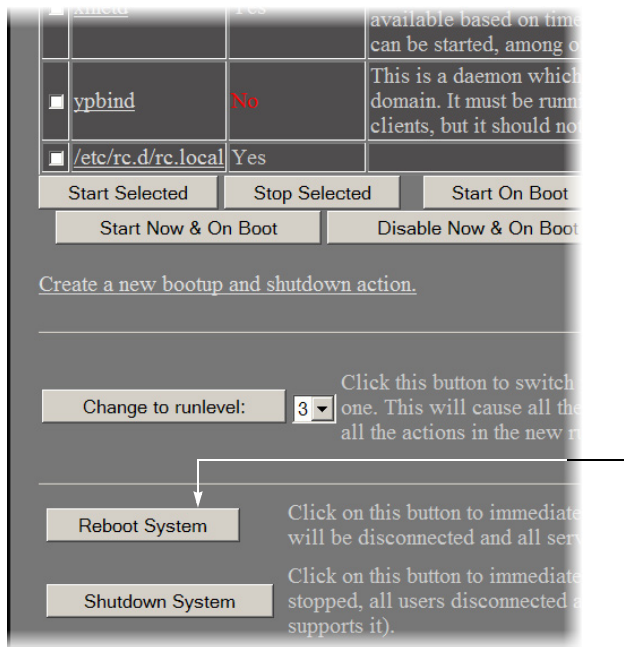
The Application Server restarts with the network parameters you have established.

3. Verify that the Application Server is connected to your local LAN via an Ethernet cable plugged into the eth0 port.

4. Restore the previous network settings on the PC or laptop that was used to configure the Application Server (see "Configuring a Client PC or Laptop" on page 18).

5. Verify that the Application Server is available on your network. From a workstation on the same subnet, open a browser window and type the IP address of the newly-configured Application Server. You should see the iControl Startup page.

6. Alternatively, you can use the **ping** command. Open the DOS command line window on the client PC or laptop (on the **Start** menu, click **Run)**, and then 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

> **Note:** If this is a workstation that will be used to operate iControl Edge, make sure that the Java Runtime Environment is installed (refer to "Installing Java" on page 21).

Step 3: Installing & Configuring Densité Systems

Densité modules housed in your Densité frames process video and audio signals from set-top boxes and relay all relevant monitoring data and alarms to the iControl Edge Application Server.

Installing Densité Frames

To install a Densité frame:

1. Install the housing frame directly into a standard 19-inch rack using 4 standard rack-mounting screws.

2. Fit all received Densité series cards and rear panels into the frame, referring to the *Densité Housing Frame Guide to Installation and Operation* for detailed instructions (see "Reference Material" on page 6).

3. Make the appropriate video, audio and network connections, referring to the *Densité CPU-ETH2 Enhanced Ethernet Controller Card Guide to Installation and Operation,* to learn how to connect your Densité system to the network, and to the documentation included with each card (see "Reference Material" on page 6).

4. Connect the supplied AC power cord to the rear-panel AC receptacle, and secure it with the retainer clip attached to the receptacle.

5. Plug the power cord into an AC outlet to turn the unit on.

Configuring Densité Services

Before you can begin operations, you must configure Densité Manager and Densité Communicator services to make your Densité frames and the associated Densité modules available on your local network. Specifically, you may have to:
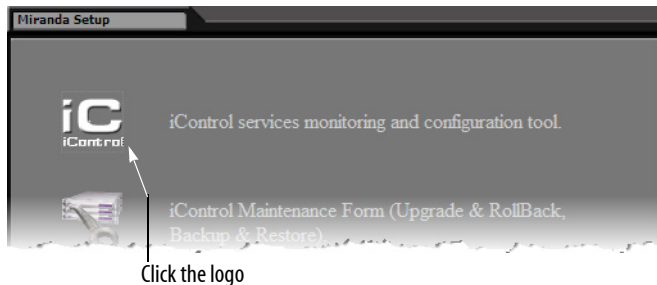
- enable at least one Densité Manager service on the Application Server

- access the appropriate Densité Manager control panel and add a Densité Communicator service for each Densité frame included in your system

- access your Densité card's control panels to enable thumbnails and audio level meters, and to configure video and audio alarms.

Enabling Densité Manager Services
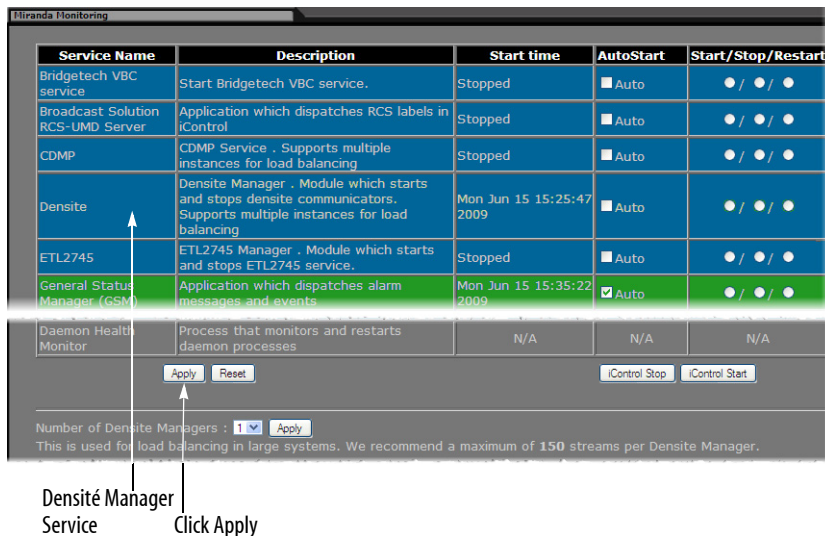
To enable a Densité Manager Service:

1. Log on to Webmin (see "Logging on to Webmin" on page 22).

2. Click **Miranda iControl Management Tool**.

   The Miranda Setup page appears:

Click the logo

3. Click the iControl logo next to **iControl services monitoring and configuration tool**.

The Miranda Monitoring page appears:
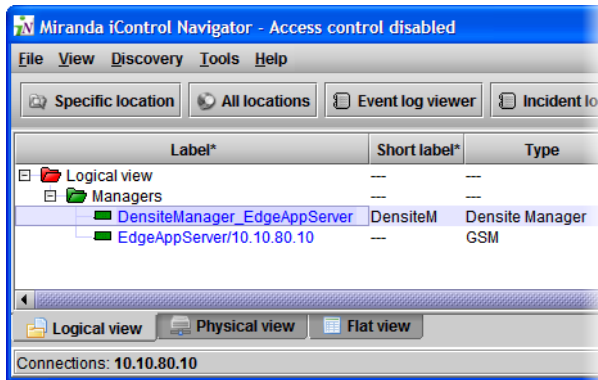

Densité Manager
Service   Click Apply

4. Find the row corresponding to the Densité Manager service.

5. In the **Start/Stop/Restart** column, select the **Auto** check box, click the **Start** option button, and then click **Apply** at the bottom of the page.

> **Note:** If you need to increase the number of Densité Managers, select the appropriate number for your purposes from the list at the bottom of the page, before clicking the **Apply** button next to it.

Adding Densité Communicator Services

To add a Densité Communicator service:

1. Open iControl Navigator, and double-click **DensiteManager** in the logical view.

2. In the **Densite Manager** window, click **Add**.

Click **Add**
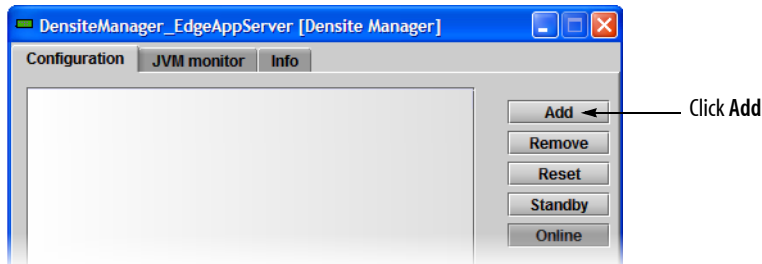
3. In **Target Information**, type the Densité frame's IP address and a descriptive name for the new Densité Communicator service, and then click **OK**.

Type the Densité frame's IP address

Type a name for the new Densité Communicator
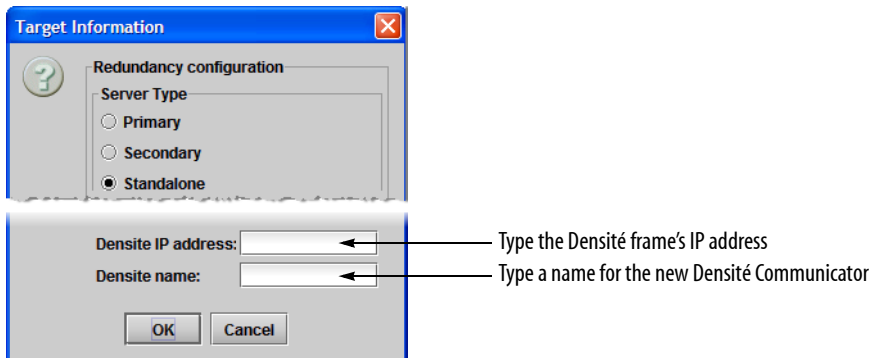
The new Densité Communicator will be started and added to the list. The Application Server will query the corresponding Densité frame, and any devices (e.g. cards) it discovers will be displayed in the iControl Navigator window.

Communicator service
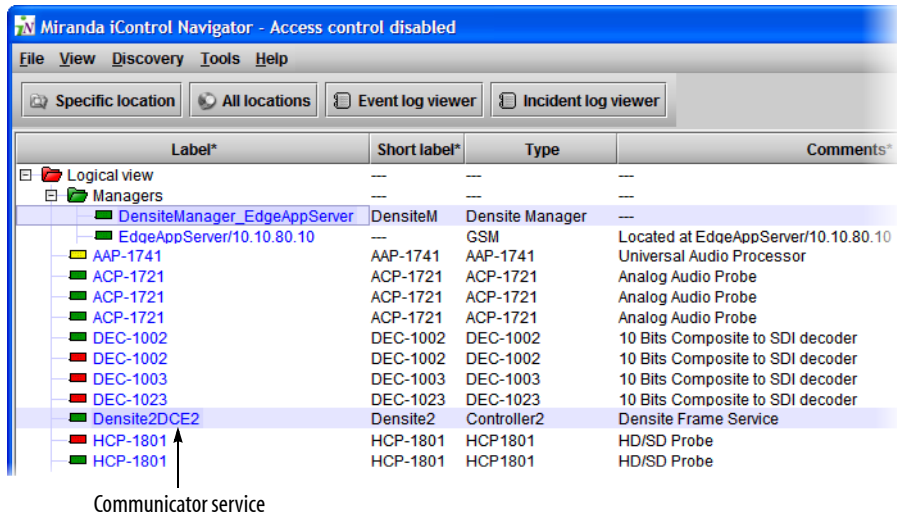
4. Repeat this procedure until you have added Communicator services for every Densité frame in your iControl Edge configuration.

> **See also:** *For more information about Densité Communicator services (also called Densité Frame services), refer to the "Configuring Devices & Services" chapter in the iControl User Guide (see "Reference Material" on page 6).*

Configuring the Probing Features

For each Densité module in your iControl Edge configuration, you need to enable thumbnail streaming and/or audio level meters. You must also configure the appropriate video and audio alarms for your monitoring purposes, and disable all logging to avoid filling the system logs with irrelevant entries.

Enabling Thumbnail Streaming

To enable thumbnail streaming on a video probe:

1. In iControl Navigator, select the Densité card you wish to configure.
2. On the **View** menu, click **Show control panel**, to open the card's control panel.
3. Click the control panel's **Thumbnail** tab.
4. Under **Enable**, click **Video**.
5. Under **Size**, click **Large**.
6. Select **Fast** from the **Rate** list.
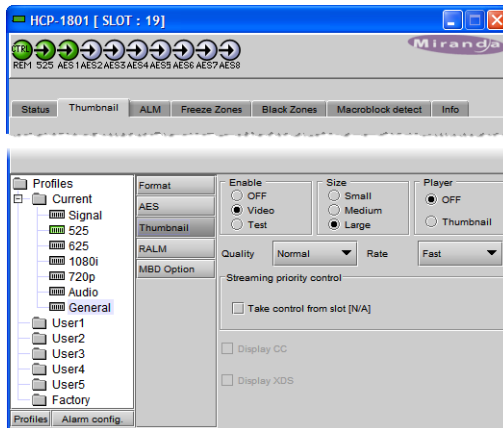
Example of a control panel showing Thumbnail settings

Enabling Audio Level Meters

The procedure below is an example showing how to enable the appropriate audio level meter on HCP-1801 cards. Some steps may vary, depending on your actual card model. Refer to the documentation that shipped with the card you wish to configure (see "Reference Material" on page 6).

To enable audio level meters:

1. In iControl Navigator, select the Densité card you wish to configure.

2. On the **View** menu, click **Show control panel**, to open the card's control panel.

3. Click the control panel's **RALM** tab.

4. Under **RALM remote control**, select the **AES1** check box.

5. Select **Fast** from the **Speed** list.
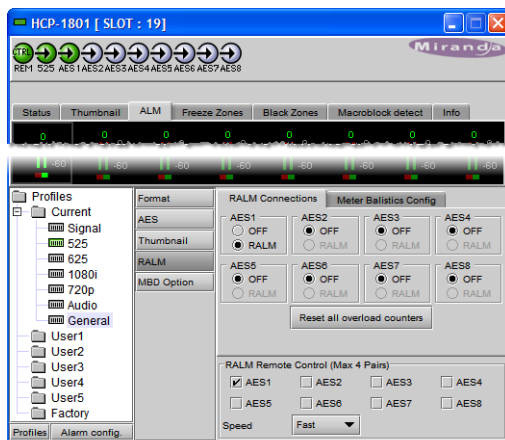
Example of a control panel showing RALM settings
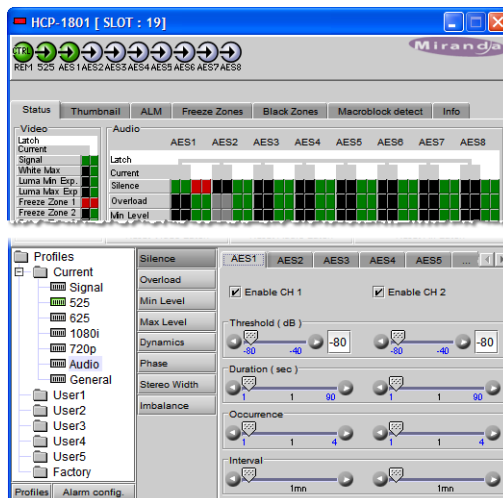
Configuring Alarm Settings

To configure relevant alarms on a Densité probe:

1. In iControl Navigator, select the Densité card you wish to configure.

2. On the **View** menu, click **Show control panel**, to open the card's control panel.

3. Enable and configure all relevant alarms (e.g. video black and freeze, audio silence and overload).

> **Note:** Make sure to set the alarm duration to the lowest value (typically **1 second**) and the number of occurrences to **1**.
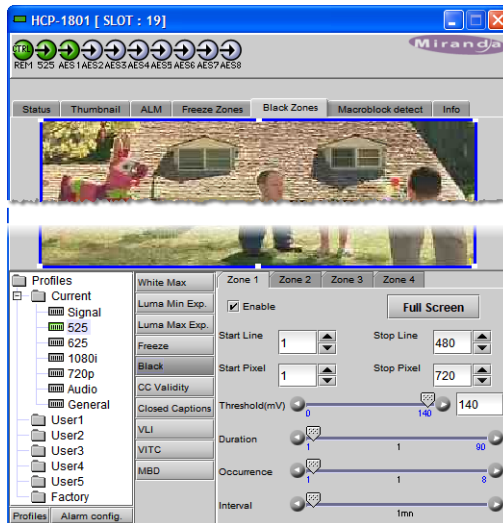
Example of a control panel showing enabled video black alarm settings

Example of a control panel showing enabled audio silence alarm settings

4. Click the **Alarm config.** button.

    The **Alarm Configuration** window for this Densité probe opens.

5. In the **Log events** column, clear the first check box to disable all event logging for this probe.

    This will avoid filling the event log with irrelevant entries.

6. For each alarm you enabled for this card, set the appropriate overall and GSM contribution.
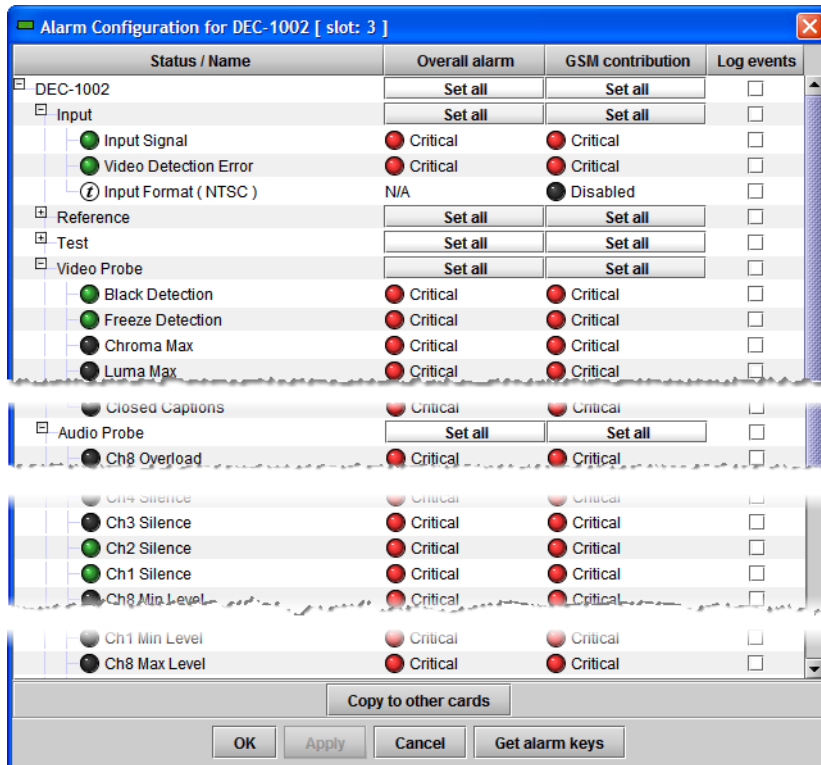
Alarm configuration example

See also:	For more information about alarm configuration, refer to "Virtual Alarms" in the "Alarms in iControl" chapter of the iControl User Guide (see "Reference Material" on page 6).

7. Once all relevant alarms are enabled and configured for this card, click **Copy to other cards**.

   The **Copy to other cards** window appears, displaying a list of all cards of the same type.

8. For each card to which you wish to copy the current alarm configuration, select the corresponding check box. Select the **All** check box at the top of the column to select all the available cards. Select the **All** check box again to remove all check marks.

9. Click **Copy**.

   A successful copy is indicated for each card by the appearance of the word "Succeeded" in the **Transfer status** column.

10. Click **Close** to close the **Copy to other cards** window.

11. Click **Profiles** at the bottom left of the control panel.

The **Profile copy for card** window appears, with the current card identified under **Copy profile from**. All other cards of the same type are listed under **Copy profile to**.

12. For each card to which you wish to copy the current profile, select the corresponding check box in the Select column.

13. Select **Select All** at the top of the column to select all the available cards.

> **Note:** 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.

14. Click **Copy**.

    A successful copy is indicated for each card by the appearance of the word "Succeeded" in the **Transfer Status** column.

15. Click **Exit** to close the **Profile Copy for Card** window.

16. Close the iControl Navigator window.

    This will also close any control panels that were left open, and other secondary windows.

Step 4: Installing & Configuring GC-100 Network Adapters

Install and configure your GC-100 units to make them available on your local network. You also need to configure the appropriate number of *IR or Sensor* connectors on each unit as **IR output.** Refer to the *Global Caché GC-100-12 Network Adapter Quick Start Guide* (see "Reference Material" on page 6) for details.

Configuring the GC-100 IR Service

Once your GC-100 units are connected to your local network you must enable the GC-100 IR service on the Application Server.

To enable the GC-100 Service:

1. Log on to Webmin (see "Logging on to Webmin" on page 22).

2. Click **Miranda iControl Management Tool**.

    The Miranda Setup page appears.

3. Click the iControl logo next to **iControl services monitoring and configuration tool**.

    The Miranda Monitoring page appears.

4. Find the row corresponding to the GC-100 IR service.

	balancing			
Densite3	Densite Manager 3. Module which starts and stops densite communicators. Supports multiple instances for load balancing	Mon Jun 15 11:58:08 2009	☑ Auto	● / ● / ●
ETL2745	ETL2745 Manager . Module which starts and stops ETL2745 service.	Stopped	☐ Auto	● / ● / ●
General Status Manager (GSM)	Application which dispatches alarm messages and events	Mon Jun 15 11:57:50 2009	☑ Auto	● / ● / ●
GlobalCache GC100 IR service	Start GlobalCache GC100 IR services.	Stopped	☐ Auto	● / ● / ●
Harmonic NMX				● / ● / ●

GC-100 IR service

Select Auto   Click Start

5. In the **Start/Stop/Restart** column, select the **Auto** check box, click the **Start** option button, and then click **Apply** at the bottom of the page.

Step 5: Installing Set-Top Boxes

A number of set-top boxes will typically be controlled from cycler services on the Application Server via GC-100 network adapters. If your system includes an Allégro streaming encoder/server, then one set-top box will be manually controlled, either from the associated remote control unit, or from the soft remote in the Application Browser area of the iControl Edge's Web site.

To connect a GC-100 network adapter to a cycling set-top box:

•   Plug one end of an IR emitter cable to an IR output on the GC-100, and position the other end against the IR receiver on the set-top box front panel.

> **Note:** You may want to shield the link between the IR emitter cable and the IR receiver on the set-top box by using protective adhesive tape (e.g. duct tape), to prevent adjacent set-top boxes from picking up IR commands that are not targeted at them.

To connect a set-top box to an HCP-1801 video control probe with embedded audio:

•   If using an HCP-1801 video control probe with embedded audio, then you need to insert an ADC-800 CAM converter between the set-top box and the HCP-1801 probe (refer to the documentation that shipped with these devices).

To connect a set-top box to a pair of Densité probes:

1. Using appropriate cables, connect the composite video output on your set-top box to a BNC input at the back of the appropriate video probe in your Densité frame (refer to the documentation for your specific set-top box model and Densité probe).

2. Connect an RCA cable to the appropriate audio connectors from the back of your set-top box to the back of the appropriate audio probe in your Densité frame (refer to the documentation for your specific set-top box model and Densité probe).

Step 6: Installing & Configuring Allégro Systems

The Allégro is the component of the iControl Edge system that provides a streaming solution for remote monitoring. The Allégro encodes and transmits video and audio streams in real time with low latency, making them available to multiple clients simultaneously via IP. It is designed for continuous, autonomous operation, and is entirely integrated into the iControl Edge environment.

The Allégro-1 Analog is a one-channel streaming encoder server with composite video input and analog stereo audio input. It allows video encoding (in aspect ratios of both 4:3 and 16:9) to resolutions that range between 80×64 and 640×480, using Miranda's proprietary MVC-1, MVC-2 and MVC-3 video codecs.

> **Note:** Allégro is designed to work in a secure private network with a bandwidth that is proportional to the desired audio and video streaming quality as well as the number of simultaneous users. Due to performance considerations, a maximum of 16 simultaneous users can be connected to the streaming source from an Allégro.

Installing Allégro Systems

In a basic configuration, one Allégro system is installed at each site to be monitored.

To install an Allégro system:

1. Install the Allégro in a standard 19-inch rack, using the rails, screws and washers provided. Make sure that the unit has adequate ventilation.

2. Make the appropriate video, audio and network connections.

3. Connect the supplied AC power cord to the rear-panel AC receptacle, and secure it with the retainer clip attached to the receptacle.

4. Plug the power cord into an AC outlet to turn the unit on.

Configuring Allégro systems

Before you can begin operations, you must configure each Allégro and make it available on your local network. Specifically, you may have to:

• access the Allégro

• configure network and other settings

• set up streaming relays

• apply your changes and perform a readiness check

Accessing the Allégro

The Allégro has a built-in Web-based management utility. This utility is available as soon as the system is powered up, and can be used to configure the system using a Web browser on any PC or laptop, provided the PC or laptop can reach the Allégro's IP address.

To access the Allégro system:

1. Configure your Client PC or laptop with an IP address in the same range as the IP address of the Allégro. See "Configuring a Client PC or Laptop" on page 18.

2. Open a Web browser and type the Allégro's default IP address (see "Network Configuration" on page 11), specifying a connection on port 8080:

   `http://10.3.0.7:8080/`

   The Allégro Startup Page appears:

Configuring the Allégro

To configure the Allégro system:

1. Click **Administration page** on the Allégro Startup page.

2. When prompted, type "admin" in the **User Name** box, type "16streams" in the **Password** box, and then press Enter.
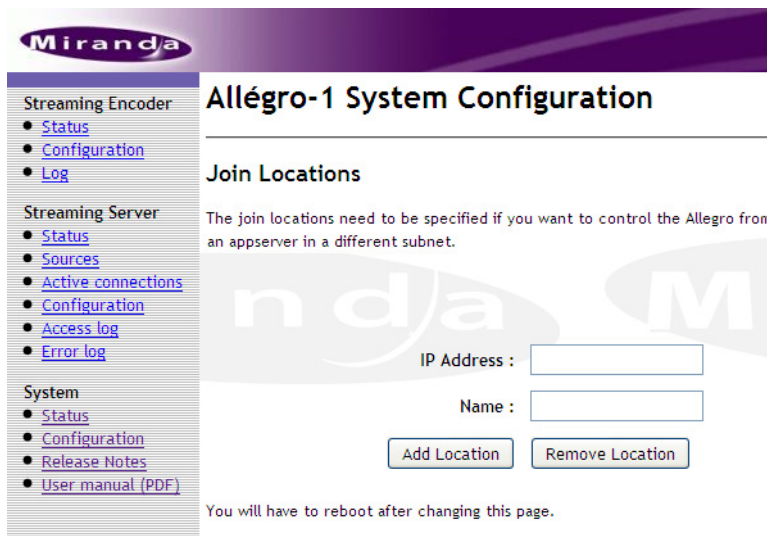
   The System Status page appears:

Allégro System Status page

3. Click the **Configuration** link under the **System** heading in the bottom part of the navigation bar.

   The System Configuration page appears:
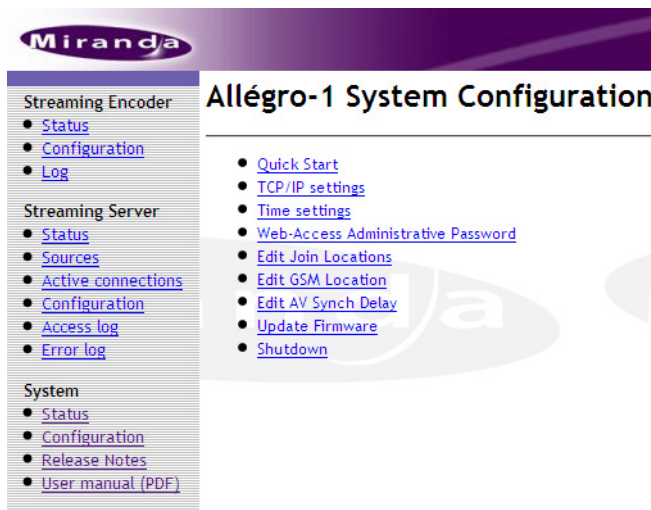
4. Click **Edit Join Locations**.

   The Join Locations page appears:

5. Type the new IP address and host name of the Application Server, and then click **Add Location**.

6. Click **Configuration** under the **System** heading in the navigation pane, and then click **Edit GSM Locations** in the main pane.

   The GSM Location page appears:

7. Type the new IP address and host name of the Application Server, and then click **Add GSM**.

8. Click **Configuration** under the **Streaming Encoder** heading in the left pane.

   The Streaming Encoder Configuration page appears:

Streaming Encoder Configuration page (Video/Audio)

9. In the **Video** section, make sure **Enabled** is set to "Yes".

10. In the **Video** section, select the encoding, frame rate, and video quality as follows:

Parameter	Recommended value
Encoding	MVC3 -- 640x480
Framerate	15 (or less)
Video quality	9.0

11. In the **Audio** section, make sure the **Enabled** setting is "Yes".

12. In the **Audio** section, set **Encoding** to "MAC2 - 44100 samp./sec, 16 bit, stereo"

13. Click **Apply**.

14. Click the **Compression** link in the navigation bar near the top of the Streaming Encoder Configuration page.

15. In the **Encoding** section, make sure the **Deinterlace** setting is "No".

16. Click **Apply**.

17. Click on **TCP/IP settings** in the right panel.

The **TCP/IP settings** page appears:
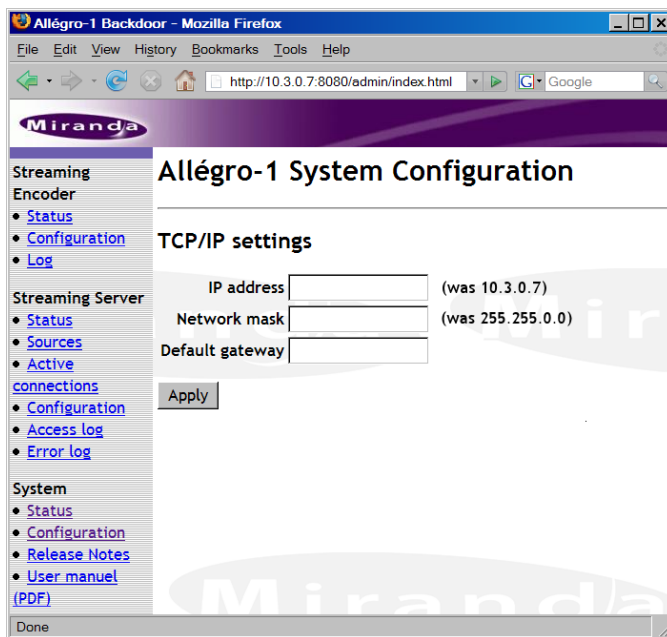
18. Type the new IP address, network mask, and default gateway address in the corresponding boxes, and then click **Apply**.

Configuring Allégro Streaming Relays

In an iControl Edge configuration, operators typically monitor audio/video streams from several remote locations at once. Having each remote Allégro send a stream to multiple operators over a WAN can result in performance problems. The recommended alternative is to have each remote Allégro send its stream to the Application Server, and then have these streams relayed over the local network to the operators' client workstations.

To configure streaming relays:

On the Application Server, for each Allégro in the configuration, you will need to create a file that provides some important parameters.

1. Launch WinSCP. If you do not have WinSCP installed on your PC or laptop, see "Using WinSCP" on page 97.

2. Log on to the Application Server (see "Logging on to an Application Server from WinSCP" on page 103).

> **Note:** Only user **root** is allowed to add or modify files in the specific directory where the streaming relay configuration files must be located. Be sure to log on as user **root** (default password is **icontrol**).
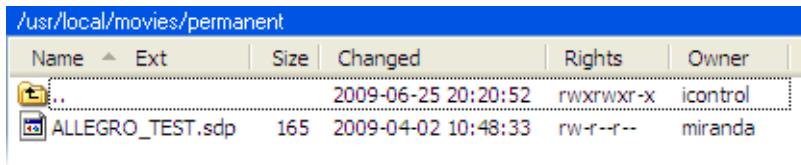
The main WinSCP window opens, showing the files on your PC in the left panel, and the files on the Application Server in the right panel:

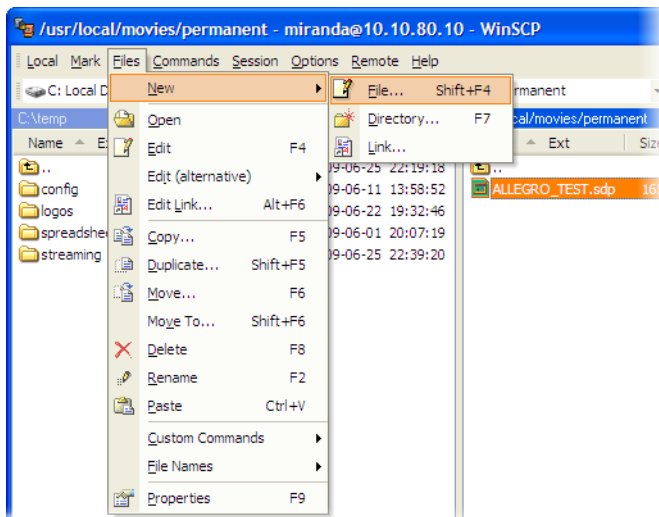You can access the top level of your PC's file system from this menu

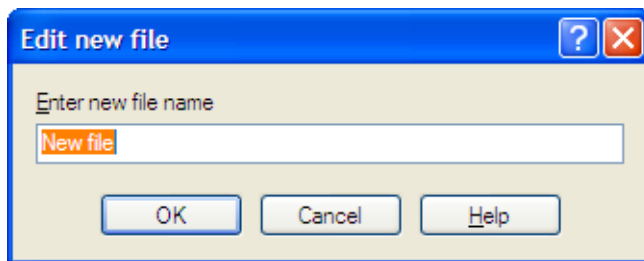You can access the root level of the Application Server's file system from this menu
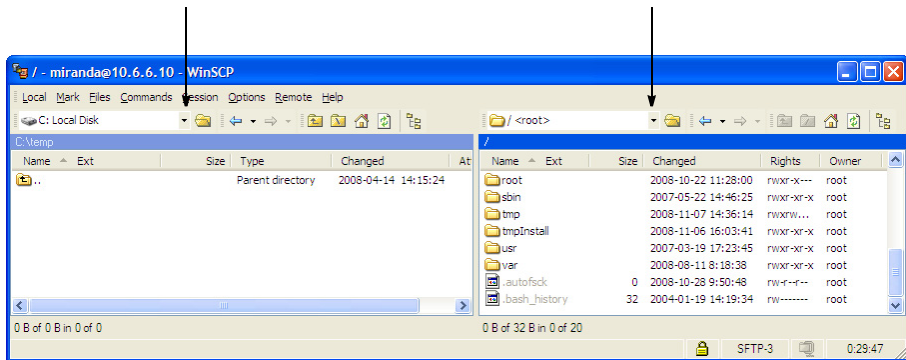
3. On the Application Server side, navigate to `/usr/local/movies/permanent`:

4. On the **Files** menu, point to **New**, and then click **File**:

A window appears, prompting you for a file name:

5. Type a name, and then click **OK**.

> **Note:** The file name must match one of the names specified in the *Devices* tab of the
> configuration spreadsheet (see "Devices Worksheet" on page 64). For example, if this streaming
> relay corresponds to the device "Allegro1" in the spreadsheet, the file should be named
> `ALLEGRO1.sdp`.

6. Type (or copy and paste) the following into the new file:

```
v=0
c=IN IP4 127.0.0.1
m=video 46010 RTP/AVP 96
a=rtpmap:96 MVC3/90000
a=control:trackID=6
m=audio 46012 RTP/AVP 1
a=rtpmap:1 MAC2/44100
a=control:trackID=7
```

7. Change the port number in the third line ("46010" in the sample above) to a port number that is unique
    to this Allégro; this is the port that will be used for the video component of the streaming relay.

8. Change the port number in the sixth line ("46012" in the sample above) to a port number that is unique
    to this Allégro—usually the video component port number plus two; this is the port that will be used
    for the audio component of the streaming relay.

> **Note:** The port numbers for the video and audio streaming components must be unique for
> each Allégro. As you create additional SDP files, increment the previously assigned port number
> by 4. For example, if the port numbers used in `ALLEGRO1.sdp` are 460**10** and 460**12**, then the
> port numbers used in `ALLEGRO2.sdp` should be 460**14** and 460**16**, and so on.

9. Save and close the file.

10. Repeat step 4 to step 9 for each Allégro in your configuration.

Next, you must configure each Allégro so that it streams to the Application Server.

11. In your Web browser's address bar, type the Allégro's IP address and specify port 8080 (e.g. `http://10.44.34.25:8080`).

12. Under **Streaming Encoder**, click **Configuration**:
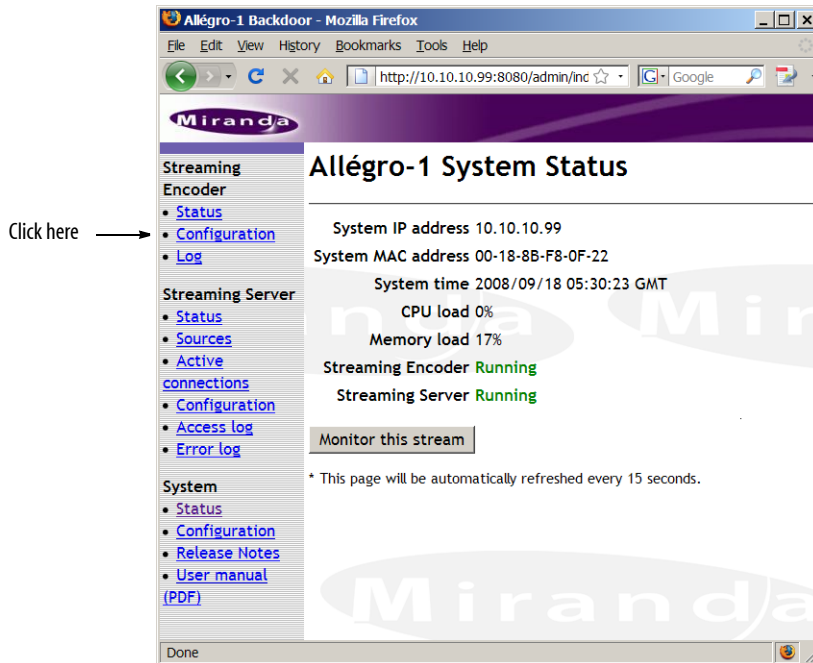
13. On the Streaming Encoder Configuration page, click **Network**:

53
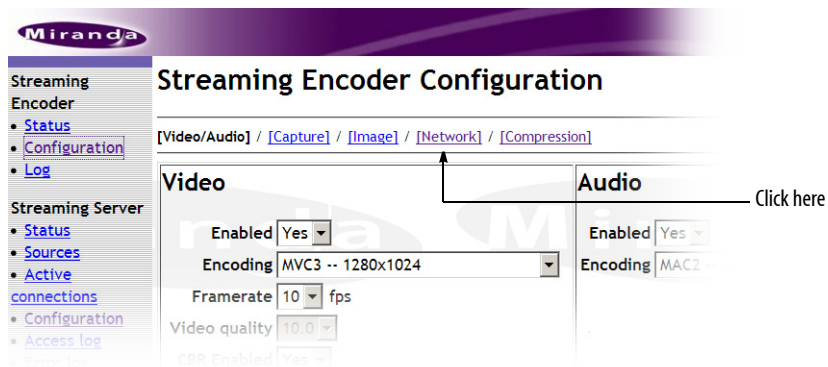
14. On the Network page, type the Application Server's IP address in the **Destination host** box. Type the appropriate port number in the **Destination port base** box (this number must match what is specified in the `ALLEGRO.sdp` file for this Allégro frame):
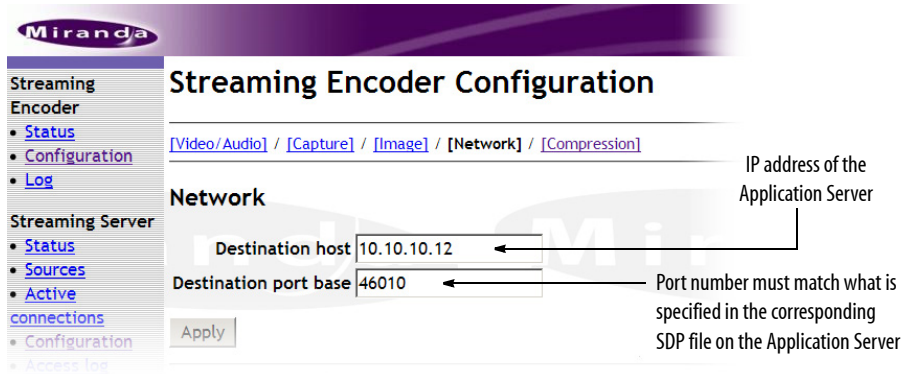
15. Click **Apply**.

16. Restart the Allégro.

17. Repeat steps step 11 to step 16 for each Allégro in the iControl Edge configuration.

18. Restart iControl on the Application Server.

Step 7: Verification & Readiness Check

When you finish configuring all devices, use an SSH client such as PuTTY to ping them from the Application Server to make sure that the devices recognize each other on your network.

> **Note:** PuTTY is available from your Application Server's Useful Downloads page. If you do not have PuTTY installed on your PC or laptop, see "Using PuTTY" on page 93.

To verify that all devices are properly connected to your system:

1. Launch PuTTY and log on to the Application Server (see "Establishing an SSH Connection with an Application Server" on page 94).

2. In the PuTTY command line window, type the following:

```
ping -s 32 AAA.BBB.CCC.DDD
```

where `AAA.BBB.CCC.DDD` is the new IP address of a Global Caché GC-100 Network Adapter. A series of messages similar to the following should appear:

```
PING 10.10.120.50 (10.10.120.50) 32(60) bytes of data.
40 bytes from 10.10.120.50: icmp_seq=1 ttl=99 time=3.43 ms
```

```
40 bytes from 10.10.120.50: icmp_seq=2 ttl=99 time=6.57 ms
40 bytes from 10.10.120.50: icmp_seq=3 ttl=99 time=3.10 ms
```

- If the ping command is successful, stop the ping by pressing Ctrl+C.
- If you see the message "`Destination Host Unreachable`", stop the ping by pressing Ctrl+C, and then verify that the device is powered up, properly cabled, and that its IP address is correctly configured.

3. Repeat the previous step for every network device in your iControl Edge system (e.g. other GC-100 network adapters at this location, an Allégro system if one was installed at this location, other Application Servers if applicable).

- For a GC-100 Network Adapter, type: `ping -s 32 AAA.BBB.CCC.DDD`
- For any other device, type: `ping AAA.BBB.CCC.DDD` (without the "`-s 32`" option)

4. Type `exit`, and then press Enter to close the PuTTY command line window.

Step 8: Managing the iControl Edge Configuration Files

Two or more configuration spreadsheets are used to specify the network, audio channel, video channel and associated information for your iControl Edge network. The first spreadsheet, `Locations.xls`, is used to specify the physical locations (i.e. head ends) in your network. Each physical location corresponds to a separate spreadsheet containing multiple signal IDs that map to actual monitored channels. The signals, in turn, correspond to multiple signal paths that map to the physical path of the signal among different devices. In addition, you may need to create configuration files to define the commands that will be used by the Global Caché GC-100 Network Adapter to control your set-top boxes. A separate configuration file is needed for each specific set-top box model.

Creating Configuration files for the Global Caché GC-100 Network Adapter

Each Global Caché GC-100 Network Adapter that shipped with your system can control up to six different set-top boxes. Depending on the set-top box model, the set of supported IR signals may vary and follow different standards.

Your iControl Edge system includes a set of predefined configuration files for the following set-top box models:

Company	STB model	File name
ARION Technology	DVB STB model for Cablevision SA	ARION
Channel Master	CM-7000	ChannelMaster
Cisco (Scientific Atlanta)	Explorer 3250HD	Explorer3250HD
	Explorer 8240HDC	Explorer8240HDC
	Explorer 8550HDC	Explorer8550HDC
Echostar	Echostar 4100	Echostar4100
Kaon Media	Kaon DVB STB models for Cablevision SA	KAON_PAIDING, KAON_TC
Motorola	DCH3200	MotorolaDCH3200
	DCT700	MotorolaDCT700
	DCT3412, and DCT6416	MotorolaDCT3412
	DCT6412	MotorolaDCT6412
	DSR205	MotorolaDSR205
Philips	DTR 220	PhilipsDTR220
Scientific Atlanta	See *Cisco (Scientific Atlanta)*.	
Winegard	RC-1010	WinegardRC1010

If you have other models of set-top boxes, you will need to create custom configuration files based on a template that is also located on the application server.

> **Note:** Predefined configuration files for the GC-100 have a `.conf` file extension, and are located on the Application Server (under `var/tomcat4/webapps/icw/sites/EDGE/Config`). Customized configuration files must be uploaded to `/usr/local/iControl/bin/conf/GC100`. In the *Devices* worksheet, you must specify only the file name, but not the `.conf` extension (see "Devices Worksheet" on page 64).
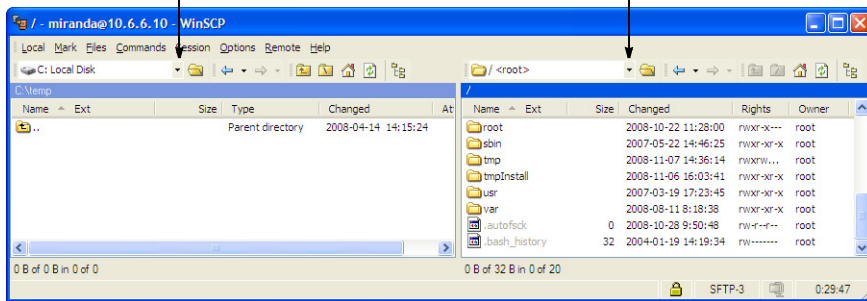
Downloading the Configuration File Template from the Application Server

To download the configuration file template to your workstation:

1. Launch WinSCP. If you do not have WinSCP installed on your PC, see "Installing WinSCP" on page 97.

2. Log on to the Application Server (see "Logging on to an Application Server from WinSCP" on page 103).

   The main WinSCP window opens, showing the files on your PC in the left panel, and the files on the Application Server in the right panel:

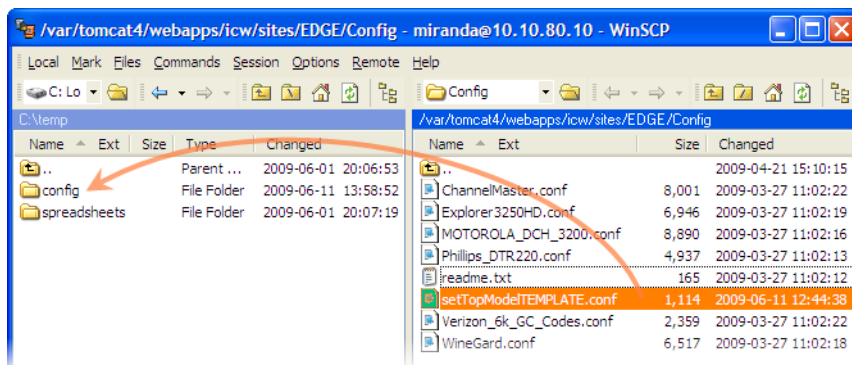   You can access the top level of your PC's file system from this menu

   You can access the root level of the Application Server's file system from this menu

3. On the Application Server side, navigate to `/var/tomcat4/webapps/icw/sites/EDGE/Config`:
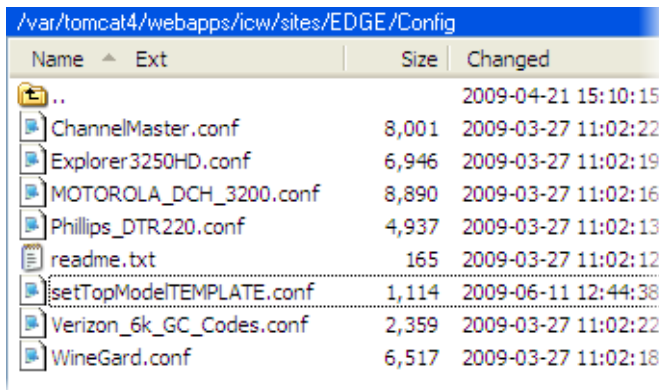
4. Select the configuration file template (`setTopModelTEMPLATE.conf`), and then drag it to a convenient location on your PC:

5. A confirmation window may appear. Click **Copy** to continue.

6. Once the download has completed, close the main WinSCP window. If prompted, click **OK** to close the application.

   You have successfully downloaded a copy of the configuration file template. You can now proceed with populating this file with the required information, as described below (see "Capturing IR Codes from Remote Control Units").

   > **Note:**   If you have more than one custom file to create, you may want to set aside a read-only copy of the template file on your hard drive to avoid having to download the clean template from the server again.

Capturing IR Codes from Remote Control Units

To capture the information required to recreate the IR signals that correspond to your specific set-top box models, you will need to use *Global Caché - IR Learner Utility* with the *GC-IRL IR Learner* serial device from Global Caché (see http://www.globalcache.com/products/ir-index.html).

> **Note:**   The IR Learner Utility and more information are available from the "Support Documents and Files" section of Global Caché's Web site
> (see http://www.globalcache.com/support/support_docs.html).

To capture IR signals from the remote control unit associated with a specific set-top box model:

1. Open a copy of the configuration file template in a text editor (e.g. Notepad).

2. Connect the GC-IRL IR Learner serial device to a serial port on your PC or laptop.

3. Launch the IR Learner Utility application (on the **Start** menu, point to **All Programs**, and then click **GC-IRL IR Learner Utility**).

4. In the **IR Learner Utility** window, select the following options:

Option	Value
End Timeout	100 ms
GC-100 Output	Selected
Repeat count	1
Module	2
Connector	1

5. Click **Connect** to connect the device to the PC application.

6. Use the set-top box remote control unit to point to the GC-IRL device, and the press one of the buttons on the remote (e.g. press **1**).

   The IR signal from the remote is converted to a string of characters placed on the clipboard.

7. Paste the content of the clipboard into the template file on the line whose header corresponds to the button your pressed (e.g. "`BUTTON_1`").

   The result will be something like the following:

   `BUTTON_1 sendir,2:1,17,38000,1,1,341,171,21,63...`

8. Repeat the same operation for every button on the remote control unit.

9. Save the text file, and name it after the set-top box model, with a `.conf` extension.

   > **Note:** The file name must not include spaces.

10. Close the text editor.

When you are done with editing configuration files and spreadsheets, you will need to upload them to the appropriate location on the server (see "Uploading and Applying the iControl Edge Configuration Files" on page 77).

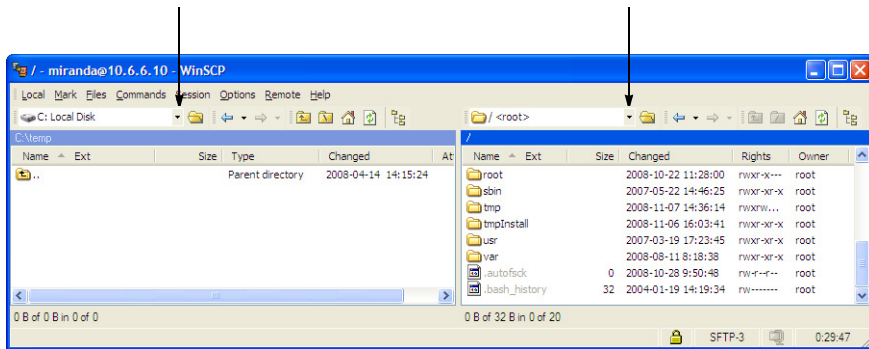## Downloading the iControl Edge Configuration Spreadsheets

The iControl Edge configuration spreadsheets reside on the Application Server. They can be downloaded for editing to a client PC or laptop with the Microsoft® Excel® spreadsheet software installed. You can use any suitable file transfer application (WinSCP, for instance) to download the spreadsheets.

To download the iControl Edge configuration spreadsheets to your workstation:

1. Launch WinSCP. If you do not have WinSCP installed on your PC or laptop, see "Installing WinSCP" on page 97.

2. Log on to the Application Server (see "Logging on to an Application Server from WinSCP" on page 103).

   The main WinSCP window opens, showing the files on your PC or laptop in the left panel, and the files on the Application Server in the right panel:

   You can access the top level of your PC's file system from this menu
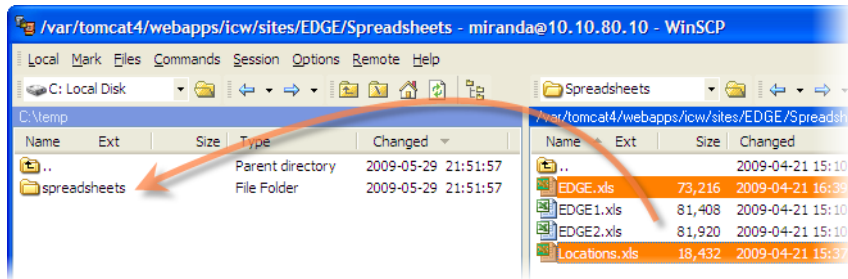
   You can access the root level of the Application Server's file system from this menu

3. On the Application Server side, navigate to `/var/tomcat4/webapps/icw/sites/EDGE/Spreadsheets/`:

4. Select the spreadsheet files (typically: `Locations.xls` and `EDGE.xls`), and drag them to a convenient location on your PC or laptop:

5. A confirmation window may appear. Click **Copy** to continue.

6. When you are done, close the main WinSCP window. If prompted, click **OK** to close the application.

    You have successfully downloaded a copy of the configuration spreadsheets. Refer to "Modifying the iControl Edge Configuration Spreadsheets" on page 61 for information on how to edit these files.

Modifying the iControl Edge Configuration Spreadsheets

You can edit the configuration spreadsheets on any client PC or laptop with the Microsoft® Excel® spreadsheet software installed. Once the files have been edited, you will transfer them back to the Application Server as described on page 77.

> **Note:** Before editing a configuration spreadsheet, make a backup copy that can be used to restore the system to its previous state.

Locations Spreadsheet

When you open the `Locations.xls` file, you will see that it contains two worksheets, corresponding to the **Locations** and **Version** tabs at the bottom of the Excel window. The Locations worksheet contains data describing each of the remote locations that are part of your iControl Edge system. The Version worksheet determines how the Devices spreadsheets will be parsed throughout the system.

	A	B	C
1	Version		
2	**	KEY	VALUE
3		Project	EDGE
4		Model	1.20
5			

Locations Worksheet

To define the locations monitored in your iControl Edge configuration:

1. Open the Locations Spreadsheet in Excel, and then click the **Locations** tab.

The *Locations* worksheet specifies the name of each location and associated Devices spreadsheet:

LOCATIONS							
**	**ID**	**TYPE**	**ENABLE**	**SHORT NAME**	**LONG NAME**	**IP**	**HOSTNAME**	**SPREADSHEET**
	LOCATION1	EDGE	YES	MTL	Montreal	10.10.80.10	EdgeAppServer	EDGE.xls
	LOCATION2	EDGE	YES	NY	New York	10.12.100.5	EdgeAppServNY	EDGE_NY.xls

The table below describes the worksheet contents:

Column	Description
**	Two asterisks (**), with no spaces, positioned in the first column indicate rows to be ignored, such as rows containing column headers, or intended for future use. Note that rows you wish to leave empty must include the two asterisks in this column.
ID	The unique ID of the iControl Edge location. **Mandatory**. **Note:** The current version of iControl Edge supports up to 12 locations.
TYPE	Must be "EDGE".
ENABLE	Type "YES" to enable a location, "NO" to disable it for troubleshooting or maintenance. A disabled location remains defined in the system, but does not participate in monitoring/control operations. In the corresponding Web page, alarms associated with a disabled location will appear in black (i.e. their state will be considered unknown).
SHORT NAME	The short name of the location. Will be displayed at the bottom of the Channel Selector area (see "Channel Selector" in the Web Monitoring chapter of the iControl Edge Operator's Overview). Optional. **Note:** On a typical system, the Location buttons can fit approximately 10 characters (or up to 16 characters, in the iControl Edge Web pages designed for a 1280 × 1024 display resolution). Longer names may appear truncated.
LONG NAME	The full name of the location. Will be displayed above the Detailed Channel Analysis area, and as a tooltip. Optional.
IP	IP Address of the Application Server at this location. **Mandatory**.
HOSTNAME	Host name of the Application Server at this location. Must match the name specified under HOSTNAME for the Application Server, in the *Devices* worksheet for this location. Case sensitive. **Mandatory**.
SPREADSHEET	Name of the file that defines the monitoring devices available at this location. **Mandatory**. **Note:** The names of the Devices spreadsheet files should be unique across the entire iControl Edge configuration (e.g. EDGE1.xls, EDGE2.xls, etc.).

2. Add rows until there are enough to describe each location in your iControl Edge configuration.

3. For each row, specify an ID, a short name, a long name, the Application Server's IP address, its host name and the name of the corresponding spreadsheet file.

> **Note:** The short names appear on the Location buttons. On a typical system, the Location buttons can fit approximately 10 characters (or up to 16 characters, in the iControl Edge Web pages designed for a 1280 × 1024 display resolution). Longer names may appear truncated.

Version Worksheet

The iControl Edge configuration spreadsheets included with your initial purchase of an iControl Edge Application Server match the current version of the iControl Edge package. The set of spreadsheets provided with the next software release could have a different structure. However, when upgrading your iControl Edge system, you do not need to start over, and port all your existing data to the new spreadsheets. The **Model** attribute ensures that legacy spreadsheets can still be parsed with a new version of the package.

Version		
**	KEY	VALUE
	Project	EDGE
	Model	1.20

When you are ready to use the new features introduced with the most recent version of the package, then all you need to do is to add the necessary columns and rows to your existing spreadsheets, and populate them based on your actual system configuration. Once you have completed adding the new data, you must update the Version worksheet accordingly.

> **Note:** With the current version of the iControl Edge package, all locations within a distributed system must have configuration spreadsheets based on the same iControl Edge version.

To update the Model attribute in the Version worksheet:

1. Open the Locations spreadsheet in Excel, and then click the Version worksheet.

2. On the **Tools** menu, point to **Protection**, and then click **Unprotect Sheet** to make the worksheet editable. (By default, there is no password.)

3. Update the Model value to the corresponding iControl Edge version number.

4. On the **Tools** menu, point to **Protection**, and then click **Protect Sheet** to make this worksheet read-only again.
   The **Protect Sheet** window appears.

5. Click **OK** to close it.

Devices Spreadsheet

When you open the XLS file that defines the monitoring devices available at a given location, you will see that it contains five worksheets—**Devices**, **Paths**, **Services**, **Alarms**, and **Config**—corresponding to tabs at the bottom of the Excel window:
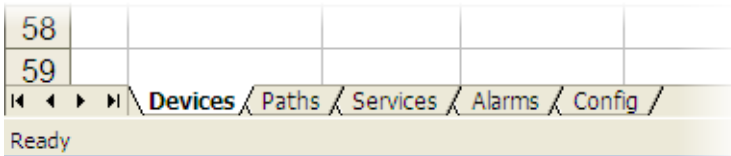
Each worksheet contains data on various aspects of the iControl Edge configuration at this location. By editing the data, you can control the way your system operates.

Devices Worksheet

To define the devices at this location:

1. Click the **Devices** tab.

   The *Devices* worksheet contains a list of the iControl Edge devices associated with a given location: an Application Server, at least one Densité frame and all the Densité probes, the Global Caché GC-100 network adapters, set-top boxes and DVRs, and one Allégro:

Devices worksheet (part 1– Physical Devices: Application Server, Densité frame and probes)

**	GC100						
**	**ID**	**TYPE**	**ENABLE**	**IP**	**PORT**	**APP SERVER ID**	
	GC1001	GC100	YES	10.0.9.119	4998	APPSERVER1	
**	STB						
**	**ID**	**TYPE**	**ENABLE**	**GC100 ID**	**GC100 PORT**	**STB**	**REMOTE CONTROL**
	STB1	STB	YES	GC1001	1	Explorer3250HD	
	STB2	STB	YES	GC1001	2	MotorolaDCT3412	
	STB3	STB	YES	GC1001	3	Explorer3250HD	
	STB4	STB	YES	GC1001	4	MotorolaDCT3412	
	STB5	STB	YES	GC1001	5	MotorolaDCT3412	
**	STB6	STB	YES	GC1001	6	MotorolaDCT3412	
**	DVR						
**	**ID**	**TYPE**	**ENABLE**	**GC100 ID**	**GC100 PORT**	**STB**	**REMOTE CONTROL**	**RECORD DURATION**
	DVR1	DVR	YES	GC1001	6	MotorolaDCT3412		60

Devices worksheet (part 2 – Physical Devices: GC-100 controller, set-top boxes, and DVRs)

This worksheet also includes a section where virtual devices are defined. A virtual device is an abstract concept, that associates a physical Densité card to a cycler profile.

**	**VIRTUAL DEVICE**				
**	**ID**	**TYPE**	**ENABLE**	**REAL DEVICE ID**	**CYCLER ID**
	VIRTUAL1	VIRTUAL	YES	CARD1	CYCLER1
	VIRTUAL2	VIRTUAL	YES	CARD2	CYCLER1
	VIRTUAL3	VIRTUAL	YES	CARD3	CYCLER2
	VIRTUAL4	VIRTUAL	YES	CARD4	CYCLER2
	VIRTUAL5	VIRTUAL	YES	CARD5	CYCLER3
	VIRTUAL6	VIRTUAL	YES	CARD6	CYCLER3

Devices worksheet (part 3: Virtual Devices)

The last section at the bottom of this worksheet is the Cycler section where the necessary cycler profiles are configured.

**	**CYCLER**						
**	**ID**	**TYPE**	**ENABLE**	**POLLING PERIOD**	**SETTLING TIME**	**DURATION**	**OCCURRENCES**
	CYCLER1	CYCLER	YES	45000	5000	30000	1
	CYCLER2	CYCLER	YES	45000	5000	30000	1
	CYCLER3	CYCLER	YES	45000	5000	30000	1
	CYCLER4	CYCLER	YES	45000	5000	30000	1
	CYCLER5	CYCLER	YES	45000	5000	30000	1

Devices worksheet (part 4: cyclers and associated alarm debouncing parameters)

The table below describes the worksheet contents:

Column	Description
**	Two asterisks (**), with no spaces, are positioned in the first column to indicate rows to be ignored, such as rows containing column headers, or intended for future use. Note that rows you wish to leave empty must include the two asterisks in this column.
ID	The unique indentifier for the device. This ID is used to reference the device within and between spreadsheets. **Mandatory**.

Column	Description
TYPE	The device type. **Mandatory**. Choices are: AS = Application Server DENSITE = Densité Housing Frame ALLEGRO = Allégro Streaming Encoder/Server ACP1721 = ACP-1721 Digital Audio Control Probe VCP1021 = VCP-1021 Composite Control Probe DEC1002 = DEC-1002 10-Bit Composite to SDI Decoder UAP1781 = UAP-1781 8-Channel Universal Audio Processor DEC1003 = DEC-1003 10-Bit Composite to SDI Decoder with Probing Option UAP1783 = UAP-1783 8-Channel Universal Audio Processor DEC1023 = DEC-1023 12-Bit 3D Composite to SDI Decoder with Probing AAP1741 = AAP-1741 4-Channel Analog Audio Processor HCP1801 = HCP-1801 HD/SD Video Control Probe with Embedded Audio SCP-1121 = SDI Control Probe with Embedded Audio GC100 = Global Caché GC-100 Network Adapter STB = Set-Top Box DVR = Digital Video Recorder VIRTUAL = Represents a Densité probe and the associated cycling profiles CYCLER = Defines a cycling profile and associated alarm debouncing parameters
ENABLE	Type "YES" to enable a device, "NO" to disable it for troubleshooting or maintenance. A disabled device remains defined in the system, but does not participate in monitoring/control operations. In the corresponding Web page, alarms associated with a disabled device will appear in black (i.e. their state will be considered unknown).
IP	Unique IP address of the device. **Mandatory**.
HOSTNAME	Host name of the Application Server (default value is "Show"). Case sensitive. **Mandatory**.
NAME	The name of a Densité frame.
APP SERVER ID	ID of the associated Application Server (e.g. "APPSERVER1"). Case sensitive. **Mandatory**.
DENSITE ID	ID of the associated Densité frame (e.g. "DENSITE1").
SLOT	Slot number (1-20) where the card is located inside the associated Densité frame.
PORT	Active port number on a GC-100 network adapter. Must be "4998".
GC100 ID	ID of the GC-100 network adapter associated with a specific set-top box.

Column	Description
CG100 PORT	IR output port number (1-6) on the GC-100 from which commands are sent to a specific set-top box.
STB	Name of the configuration file associated with a specific set-top box (or DVR) model (see "Creating Configuration files for the Global Caché GC-100 Network Adapter" on page 55). **Note:** Do not specify the **.conf** extension.
REMOTE CONTROL	Path to an iC Web page (MPF file) that represents the remote control used with a specific set-top box (or DVR) model, relative to EDGE/Web_pages. A set of default MPF files is provided matching the remotes commonly used with the set-top models for which a predefined configuration file (for the GC-100) exists. If left blank, a generic remote control image will be used.
RECORD DURATION	Maximum time during which the associated DVR will record a video stream after an error is detected. Default value is **60 seconds**.
REAL DEVICE ID	ID of the Densité probe associated with a specific virtual service.
CYCLER ID	ID of the cycler associated with a specific probe. **Note:** Specify the same cycler ID for each pair of audio and video probes: a pair of probes that are meant to process video and audio signals from the same channel must be associated with the same cycler ID.
POLLING PERIOD	Total length, in milliseconds, of the period allowed for monitoring each channel during a cycle, including the settling phase, and the listening phase. Default value is **45000 ms**, i.e. 45 seconds.
SETTLING TIME	Time allowed, in milliseconds, at the beginning of each polling period for properly tuning a channel. Alarms are not actively monitored during this period. Default value is **5000 ms**, i.e. 5 seconds.
DURATION	Determines the amount of time, in milliseconds, required before an error condition is considered as an alarm occurrence. Default value is **30000 ms**, i.e. 30 seconds. **Note:** This value should be less than the length of the polling period minus the settling time.
OCCURRENCES	Number of alarm occurrences required before an alarm is triggered (default value is **1**).

2. Specify the Application Server's IP address (see "Configuring the Ethernet Interface" on page 29) and host name (see "Specifying DNS Client Settings" on page 24).

3. In the DENSITE section, specify an ID.

The ID for each Densité frame across the entire iControl Edge configuration should be unique (e.g. **Densite1, Densite2**, etc.). Specify each Densité frame's host name (see "Configuring Densité Services" on page 33). Do not change the default values for TYPE (**DENSITE**), or ENABLED (**YES**).

4. In the ALLEGRO section, specify an ID.

The ID for each Allégro across the entire iControl Edge configuration should be unique (e.g. **Allegro1, Allegro2**, etc.). Specify the Allégro's IP address. Do not change the default values for TYPE (**ALLEGRO**), or ENABLED (**YES**)

> **Note:** If the Application Server is configured to relay for the Allégro stream (see "Configuring Allégro Streaming Relays" on page 50), you must put the Application Server's ID in the APP SERVER ID column, beside the Allégro's IP Address.

5. In the CARD section, specify an ID, and a card type, for every card at this location.

The ID for each Densité card across the entire iControl Edge configuration should be unique (e.g. **Card1, Card2**, etc.). Specify the Densité frame's ID (see "Configuring Densité Services" on page 33). Do not change the default values for TYPE (**DENSITE**), or ENABLED (**YES**).

6. In the GC100 section, specify an ID for every GC-100 network adapter at this location.

The ID for each GC-100 network adapter across the entire iControl Edge configuration should be unique (e.g. **GC1001, GC1002**, etc.). Specify the GC-100 network adapter's IP address. Specify the Application Server's ID. Do not change the default values for TYPE (**GC100**), ENABLED (**YES**), or PORT (**4998**).

7. In the STB section, specify an ID.

The ID for each set-top box across the entire iControl Edge configuration should be unique (e.g. **STB1, STB2**, etc.). For each set-top box, specify the associated GC-100 ID (in the GC100 ID column) and IR output port number (in the GC100 PORT column). In the CCF FILE NAME column, specify the name of the configuration file associated with each set-top box model. Do not specify the `.conf` file extension (see "Creating Configuration files for the Global Caché GC-100 Network Adapter" on page 55). Do not change the default values for TYPE (**STB**), or ENABLED (**YES**).

8. Complete the DVR section in the same fashion, with the appropriate information for your DVR devices. Do not change the default values for TYPE (**DVR**). Specify the appropriate RECORD DURATION.

9. In the VIRTUAL DEVICE section, specify an ID to represent a Densité card that will probe signals from a cycling set-top box.

The ID for each virtual device across the entire iControl Edge configuration should be unique (e.g. **VIRTUAL1, VIRTUAL2**, etc.). Specify the associated card ID (in the REAL DEVICE ID column), and specify a common cycler ID for each pair of audio and video probes (i.e. a pair of probes that are meant to process video and audio signals from the same channel must be associated with the same cycler ID).

10. In the CYCLER section, list the cycler IDs you specified in the VIRTUAL DEVICE section (see step 9). For each cycler, specify the appropriate polling period and settling time (in seconds) for the channel lineup

that will be associated with a given cycling set-top box. Also specify appropriate alarm debouncing parameters for each cycler (DURATION, OCCURRENCES).

> **Note:** A cycle comprises two phases: the settling phase, and the listening phase (polling period). Alarms are actively monitored during the listening phase only. When an alarm condition is detected, if it lasts at least for the duration specified, then it is counted as one occurrence. The specified duration should be less than the polling period minus the settling time. The number of occurrences can span more than one cycle.

Paths Worksheet

To define the signal paths for this site:

1. Click the **Paths** tab

   For a given location, the *Paths* worksheet specifies which set-top box feeds which Densité modules (usually a pair of audio/video probes represented as virtual devices associated with a common cycling profile; see "Devices Worksheet", step 9 on page 68), and whether an Allégro is used for streaming signals from a designated set-top box:

**				STB	VIDEO	AUDIO
**	ID	TYPE	ENABLE	ID	ID	ID
	C_PATH1	STB_CYCLING	YES	STB1	VIRTUAL1	VIRTUAL2
	C_PATH2	STB_CYCLING	YES	STB2	VIRTUAL3	VIRTUAL4
	C_PATH3	STB_CYCLING	YES	STB3	VIRTUAL5	VIRTUAL6
	C_PATH4	STB_CYCLING	YES	STB4	VIRTUAL7	VIRTUAL8
	C_PATH5	STB_CYCLING	YES	STB5	VIRTUAL9	VIRTUAL10
**				STB	ALLEGRO	
**	ID	TYPE	ENABLE	ID	ID	
	M_PATH1	STB_MANUAL	YES	STB6	ALLEGRO1	

The table below describes the *Paths* worksheet contents:

Column	Description
**	Two asterisks (**), with no spaces, are positioned in the first column to indicate rows to be ignored, such as rows containing column headers, or intended for future use. Note that rows you wish to leave empty must include the two asterisks in this column.
ID	The unique indentifier for the Path. This ID is used to reference the device within and between spreadsheets. **Mandatory**.
TYPE	The device type. **Mandatory**. Choices are: STB_CYCLING = Set-top box (or DVR) controlled by a cycler service STB_MANUAL = manually-controlled set-top box (or DVR)

Column	Description
ENABLE	Type "YES" to enable a Path, "NO" to disable it for troubleshooting or maintenance.
STB ID	Unique ID of a set-top box (or DVR), as specified on the *Devices* worksheet. Case sensitive. **Mandatory**.
VIDEO ID	Unique ID of a video probe, as specified on the *Devices* worksheet. Case sensitive. **Mandatory in cycling paths**. Optional in manual paths.
AUDIO ID	Unique ID of an audio probe, as specified on the *Devices* worksheet. Case sensitive. **Mandatory in cycling paths**. Optional in manual paths.
ALLEGRO ID	Unique ID of the Allégro, as specified on the *Devices* worksheet. Case sensitive. **Mandatory**.

2. For each Path, specify a unique ID, and the TYPE of set-top box being used in the path (**STB-CYCLING** or **STB-MANUAL**). Specify the associated set-top box ID.

• For a *cycling* path, specify the *virtual device* IDs representing the associated pair of video and audio probes.

• For a *manual* path, specify the *card* IDs representing the associated pair of video and audio probes, if present.

> **Note:** In the case of HCP-1801 HD/SD video control probes with embedded audio, both VIDEO ID and AUDIO ID should refer to the same virtual device ID (in cycling paths) or card ID (in manual paths).

Services Worksheet

To define the services at this location:

1. Click the **Services** tab.

The *Services* worksheet is used to define the services or channels assigned to a path:

ID	TYPE	ENABLE	CH NUMBER	SHORT NAME	LONG NAME	DESCRIPTION	LOGO FILE NAME	G
FOXESP	STB	YES	125	FOXESP	Fox Sports Espanol	<HTML>Contact Name: Jes	fox_sports_espanol.gif	SD
REELZ	STB	YES	131	REELZ	REELZ	<HTML>Contact Name: Mid	reelz_channel.gif	SD
FUSE	STB	YES	132	FUSE	FUSE	<HTML>Contact Name: Ric	fuse.gif	SD
CBSHD	STB	YES	702	CBSHD	CBS HD	<HTML>Contact Name: Jes	cbs_hd.gif	HD
TNTHD	STB	YES	703	TNTHD	TNT HD	<HTML>Contact Name: Mid	tnt_hd.gif	HD
NBCHD	STB	YES	704	NBCHD	NBC HD	<HTML>Contact Name: Ric	nbc_hd.gif	HD
ABCHD	STB	YES	707	ABCHD	ABC HD	<HTML>Contact Name: Jes	abc_hd.gif	HD

Services worksheet (part 1, description and configuration of the Channel Selector area)

LOGICAL GROUP	ALTERNATE GROUP ID	OFFLINE	RECORDABLE	CYCLING PATH ID	MANUAL PATH ID
SD	TS_004	NO	NO	C_PATH3	M_PATH1
SD	TS_004	NO	YES	C_PATH3	M_PATH1
SD	TS_004	NO	NO	C_PATH3	M_PATH1
HD	TS_005	NO	YES	C_PATH4	M_PATH1
HD	TS_005	NO	NO	C_PATH4	M_PATH1
HD	TS_005	NO	YES	C_PATH4	M_PATH1
HD	TS_005	NO	NO	C_PATH4	M_PATH1

Services worksheet (part 2, groups and paths)

The table below describes the worksheet contents:

Column	Description
**	Two asterisks (**), with no spaces, are positioned in the first column to indicate rows to be ignored, such as rows containing column headers, or intended for future use. Note that rows you wish to leave empty must include the two asterisks in this column.
ID	The unique indentifier for the service. This ID is used to reference the service within and between spreadsheets. **Mandatory**.
TYPE	Must be "STB".
ENABLE	Type "YES" to enable a service, "NO" to disable it for troubleshooting or maintenance. The corresponding Channel Selector button will then be hidden (i.e. replaced with an unlabeled unavailable button).
CH NUMBER	The channel number associated with the service. Used by the CG-100 service and in the remote control area for tuning set-top boxes to this channel.
SHORT NAME	The short name of the service (e.g. call letters). Will be displayed as a heading above the thumbnail showing video from this service in the Multi-Channel Monitoring view, on Channel Selector buttons, and in logs of DVR recordings (see "Channel Selector" in the Web Monitoring chapter of the iControl Edge Operator's Overview. Optional. **Note:** On a typical system, the Channel Selector buttons can fit approximately 8 characters. Longer names may appear truncated.
LONG NAME	The full name of the service. Will be displayed as a title, in the Detailed Channel Analysis view, and as a tooltip when the pointer is over a Channel Selector button. The long name also appears along with the channel number in the DVR recording area. Optional.
DESCRIPTION	Description of the service that appears in the message box at the top left of the Detailed Channel Analysis view. Format the text by enclosing it between valid HTML tags. Optional

Column	Description
LOGO FILE NAME	The name of the file containing the logo associated with this service. If present, this logo will appear at the top of the corresponding player in the Multi-Channel Monitoring area or Detailed Channel Analysis view.
LOGICAL GROUP	Organize the Channel Selector area, by creating logical groups of related services identified by a meaningful name. The logical group name is displayed at the bottom of the Channel Selector area, under the associated service buttons. **Note:** The current version of iControl Edge support a maximum of 25 groups.
ALTERNATE GROUP ID	Define another set of logical groups to organize the Channel Selector area to suit your monitoring purposes. A meaningful name for the alternative grouping can be specified in the *Config* worksheet (see "Config Worksheet" on page 75). **Note:** The current version of iControl Edge support a maximum of 25 groups.
OFFLINE	Type "YES" to designate a service as offline. The service will appear on the monitoring application Web pages, but will not contribute to overall alarms.
RECORDABLE	Type "YES" to designate a service you wish to record for a certain amount of time when an error condition is detected. The recording duration (60 seconds by default) is a configurable attribute of the DVR device specified in the manual path for this service (see "Devices Worksheet" on page 64).
CYCLING PATH ID	ID of the cycling path associated with a service. This ID determines which cycling set-top box (or DVR) and which Densité probe (or pair of probes) process signals for this service.
MANUAL PATH ID	ID of the manual path associated with a service. This ID determines which manual set-top box or DVR, and which Allégro (if any) process signals for this service.

2. For each Service, specify a unique ID, the associated channel number, a short name, and a long name.

> **Note:** The short names appear on the Channel Selector buttons. On a typical system, the Channel Selector buttons can fit approximately 8 characters. Longer names may appear truncated.

Do not change the default value for TYPE (**STB**), ENABLED (**YES**), or OFFLINE (**NO**). Insert a description (using HTML tags where appropriate), and specify the logo file name. Specify a cycling path and a manual path for this service, and identify a recordable service by typing YES in the RECORDABLE column.

Note: Custom logo files can be uploaded to `/var/tomcat4/webapps/icw/sites/EDGE/images/Logo` on the Application Server (see "Uploading Custom Logo Files" on page 78). The logo images provided with the package are 52 pixels wide × 32 pixels high, but other dimensions up to 104 pixels × 64 pixels are also supported. A 13:8 ratio will best fit the space available for the logos in the iControl Edge user interface.

3. Adjust the positioning of the Channel Selector buttons by changing the LOGICAL GROUP value.

4. Define an alternative grouping of the Channel Selector buttons by typing the desired group names under ALTERNATE GROUP ID.

Alarms Worksheet

iControl Edge shows current alarm statuses in different ways: in the Channel Selector area, the color of a Channel Selector button represents the corresponding service's overall alarm status; the alarm panel for a service displays more detailed alarm status information.

To define the alarms covered by your iControl Edge configuration:

1. Click the **Alarms** tab.

The *Alarms* worksheet defines which alarms will be monitored by your system:

	A	B	C	D	E	F	G
1	**ALARMS**						
2	**	DEVICE TYPE	ALARM GROUP	ALARM URI	ALARM NAME	ALARM TYPE	LEVEL
3		ACP1721	Audio	{baseuri}aChan1_ovld_ST	Ch. 1/2 Silence	COMPRESSED	SERVICE
4		ACP1721	Audio	{baseuri}aChan1_sil_ST	Ch. 1/2 Silence	COMPRESSED	SERVICE
5		ACP1721	Audio	{baseuri}aChan2_ovld_ST	Ch. 1/2 Overload	COMPRESSED	SERVICE
6		ACP1721	Audio	{baseuri}aChan2_sil_ST	Ch. 1/2 Overload	COMPRESSED	SERVICE
7		ACP1721	Audio	{baseuri}aImbalance_ST	Imbalance	STATUS	SERVICE
8		ACP1721	Audio	{baseuri}aPhase_ST	Phase	STATUS	SERVICE
9	**						
10		VCP1021	Video	{baseuri}vBlackDet_ST	Black	STATUS	SERVICE
11		VCP1021	Video	{baseuri}vFreezeDet_ST	Freeze	STATUS	SERVICE
19		DEC1002	Video	{baseuri}vBlackDet_ST	Black	STATUS	SERVICE
20		DEC1002	Video	{baseuri}vFreezeDet_ST	Freeze	STATUS	SERVICE
21	**						
22		UAP1781	Audio	{baseuri}aNoSigCh1	Ch. 1/2 Silence	COMPRESSED	SERVICE
23		UAP1781	Audio	{baseuri}aNoSigCh2	Ch. 1/2 Silence	COMPRESSED	SERVICE
24	**						
25		DENSITE	Health	{baseuri}dCPUStatus	CPU Critical Load	STATUS	DEVICE
26		DENSITE	Health	{baseuri}dFan1Status	Left Fan	STATUS	DEVICE
27		DENSITE	Health	{baseuri}dPs1Status	Left Power Supply	STATUS	DEVICE
28		DENSITE	Health	{baseuri}dFanPs1Status	Left Power Supply Fan	STATUS	DEVICE
38		AS	CPU	{baseuri}CPUUser	CPU User %	TEXT	DEVICE
39		AS	Health	{baseuri}commStatus	Communication Status	STATUS	DEVICE
40		AS	Health	{baseuri}powerCycle	Device Reboot	STATUS	DEVICE
41	**						
42		HCP1801	Video	{baseuri}vBlackDet1_ST	Zone 1 Black	STATUS	SERVICE
43		HCP1801	Video	{baseuri}vFreezeDet1_ST	Zone 1 Freeze	STATUS	SERVICE

The table below describes the worksheet contents:

Column	Description
**	Two asterisks (**), with no spaces, are positioned in the first column to indicate rows to be ignored, such as rows containing column headers, or intended for future use. Note that rows you wish to leave empty must include the two asterisks in this column.
DEVICE TYPE	The device type to which this alarm applies: DENSITE = Densité 3 Housing Frame AS = Application Server ACP1721 = ACP-1721 Digital Audio Control Probe VCP1021 = VCP-1021 Composite Control Probe DEC1002 = DEC-1002 10-Bit Composite to SDI Decoder DEC1003 = DEC-1003 10-Bit Composite to SDI Decoder with Probing Option DEC1023 = DEC-1023 12-Bit 3D Composite to SDI Decoder with Probing UAP1781 = UAP-1781 8-Channel Universal Audio Processor UAP1783 = UAP-1783 8-Channel Universal Audio Processor AAP1741 = AAP-1741 4-Channel Analog Audio Processor HCP1801 = HCP-1801 HD/SD Video Control Probe with Embedded Audio
ALARM GROUP	The group to which this alarm belongs. Will be displayed as a header in the alarm panel.
ALARM URI	The alarm's Uniform Resource Identifier.
ALARM NAME	The name of the alarm that appears in the Detailed Channel Analysis views (see "Alarm Browser" in the Web Monitoring chapter of the iControl Edge Operator's Overview).

Column	Description
ALARM TYPE	The type of alarms ("TEXT", "STATUS", or "COMPRESSED").
LEVEL	Specifies whether the alarm belongs to the Device or Service category. An alarm set to the "SERVICE" level is visible in the service's alarm panel, and its state contributes to the overall alarm status for this service. The service's button color in the Channel Selector area represents this overall alarm status. An alarm set to the "DEVICE" level is also visible in the service's alarm panel, but its state does not contribute to the alarm status for this service (and thus does not affect the color of the corresponding Channel Selector button).

2. If desired, change the ALARM NAME—this will change the text displayed in the monitoring application.

> **Note:** Do not edit the ALARM URI.

3. If you wish to discontinue monitoring for a specific alarm, insert two asterisk in the first column of the corresponding row, or delete the entire row. The alarm will be removed from all Alarm Panels and will no longer be calculated or displayed.

Config Worksheet

To define the alarm behavior and other options for your iControl Edge configuration:

• Click the **Config** tab, and specify the appropriate values for the attributes described in the table below. The *Config* worksheet defines alarm behavior, and other options:

Key	Description
blinkWhenUnacknowledged	Default value is "NO." Setting this value to "YES" causes new Alarms to blink in the monitoring application page. Operator has to acknowledge individual alarms to stop the blinking. If ackAudibleAlarm is enabled, the operator can click the **Acknowledge** button to acknowledge all alarms at once.
ackAudibleAlarm	Default "YES" value causes an audible alarm (chime) to activate when a new alarm comes in, and allows operators to temporarily mute the chime, by clicking the **Acknowledge** button. When another alarm comes in, the audible alarm will be re-activated. Click the **Mute sound** button to mute the audible alarm and prevent it from being re-activated automatically (until you decide otherwise by clicking **Unmute sound**). Set ackAudibleAlarm to "NO" to disable the audible alarm, and hide both the **Acknowledge** and **Mute/unmute sound** buttons.
alternateGroupLabel	The Channel Selector can be sorted on the basis of some criteria, including logical groups defined in the Services worksheet and referred to as *Logical group* in the context of the Channel Selector's sort menu. The alternate label you can provide here will appear in the Channel Selector's sort menu to designate an additional set of groups, also defined in the Services worksheet (see "Services Worksheet" on page 70). The default value is "TS" (i.e. "transport stream").
EMBEDDED WEB PAGES	In the Embedded Web Pages section, you can define and configure up to two custom Application Selector buttons linked to Web pages or iC Web pages. To configure a button, remove the asterisks at the beginning of the corresponding rows (the set of four rows that start with either "browserButton0" or "browserButton1"), and type the desired values for the four parameters (the parameters for the first button are described below; the other button is configured in the same fashion). **Note:** A custom button is added to the application Selector, only if the associated URL or MPF file path is specified.
browserButton0_url	The address of a Web page (URL) or iC Web page (path to MPF file, relative to EDGE/Web_pages). Default value is "http://www.miranda.com".

Key	Description
browserButton0_title	The label of the button ("Miranda" by default).
browserButton0_image	Unselected button image (URL, or path to image file, relative to EDGE/Web_pages).
browserButton0_selectedImage	Selected button image (URL, or path to image file, relative to EDGE/Web_pages).

Note: Remember to save the configuration spreadsheet once you have made the necessary changes.

Step 9: Uploading and Applying the iControl Edge Configuration Files

Once you have finished modifying the configuration spreadsheets, and creating the required configuration files for the Global Caché GC-100 Network Adapter, you must transfer them to the Application Server and restart the GSM services (see "Restarting the General Status Manager (GSM) Services" on page 80) for the changes to take effect.

Uploading the GC-100 Network Adapter Configuration Files

You can use any suitable file transfer application—WinSCP, for instance, or the upload function of the Application Server's File Manager utility—to transfer new or updated configuration files from your client PC or laptop to the Application Server.

To upload the configuration files to the Application Server:

1. Launch WinSCP, log on to the Application Server and navigate to `/usr/local/iControl/bin/conf/GC100`:

2. Select the new or modified configuration files (`.conf`) on your PC or laptop, and then drag them to the `GC100` directory on the Application Server:
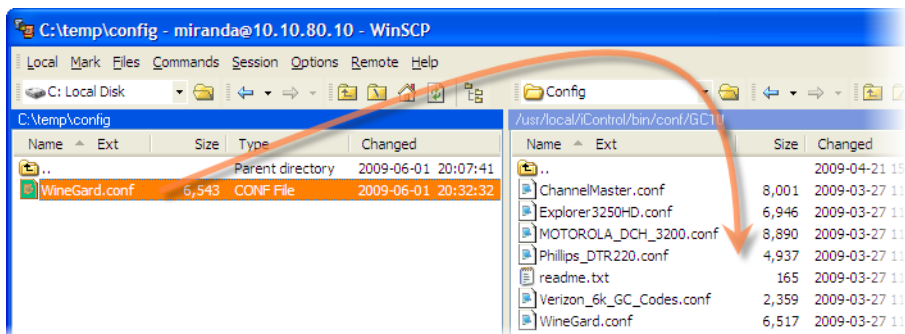
3. Close WinSCP.

   You have successfully uploaded the configuration files for your GC-100 Network Adapter.

Uploading Custom Logo Files

Your iControl Edge system ships with a set of predefined logo files located under `/var/tomcat4/webapps/icw/sites/EDGE/images/Logo` on the Application Server. You can add custom logo files to this directory.

> **Note:** When you update your system with a new version of the iControl Edge package, any existing logo file that is not part of the default logo set, or that is more recent than a logo file with the same name within the default set, will be carried forward. Nevertheless, it is always advisable to keep a backup copy of your custom logo files (e.g. on your hard drive).

To upload custom logo files to the Application Server:

1. Launch WinSCP, log on to the Application Server and navigate to `/var/tomcat4/webapps/icw/sites/EDGE/images/Logo`:
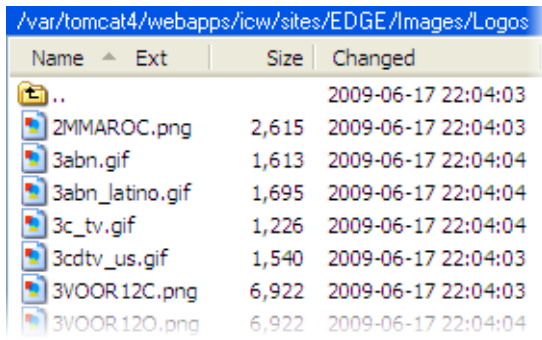
2. Select the custom logo files (GIF or PNG) on your PC or laptop, and then drag them to the `Logos` directory on the Application Server:
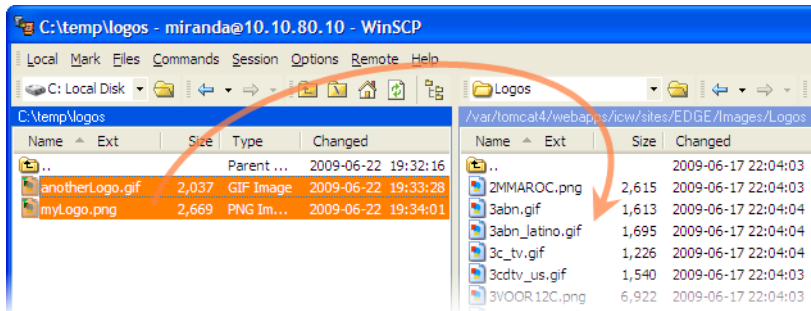
3. Close WinSCP.

> **See also:** For more information about logo files, see "Services Worksheet" on page 70.

Uploading the iControl Edge Configuration Spreadsheets

You can use any suitable file transfer application—WinSCP, for instance, or the upload function of the Application Server's File Manager utility—to transfer updated spreadsheets from your client PC or laptop back to the Application Server.

To upload the configuration spreadsheets to the Application Server:

1. Launch WinSCP, log on to the Application Server and navigate to `/var/tomcat4/webapps/icw/sites/EDGE/Spreadsheets/` (see "Downloading the iControl Edge Configuration Spreadsheets" on page 59).

2. Select the modified spreadsheet (`.xls`) files on your PC or laptop, and then drag them to the `Spreadsheets` directory on the Application Server:
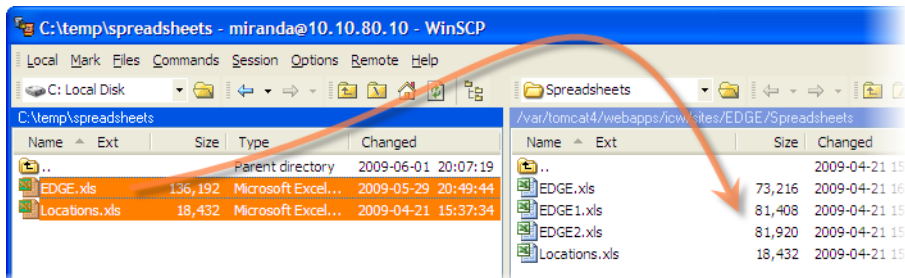
3. Close WinSCP.

You have successfully uploaded your modified configuration spreadsheets.

Restarting the General Status Manager (GSM) Services

Once you have uploaded the modified iControl Edge Configuration Spreadsheets, you must restart iControl's General Status Manager (GSM) services, and refresh the iControl Edge Web page for the changes to take effect.

To restart iControl's GSM services:

1. Log on to Webmin (see "Logging on to Webmin" on page 22).

2. Click **Miranda iControl Management Tool**.
   The Miranda Setup page appears:

3. Click the iControl logo next to **iControl services monitoring and configuration tool**.

The Miranda Monitoring page appears.

4. In the **Start/Stop/Restart** column, select the **Restart** option button, for all General Status Manager (GSM) services listed on the page, and then click **Apply** at the bottom of the page.

b. Click Apply

a. Select Restart

You have successfully restarted the GSM services and applied the settings contained in your modified Configuration Spreadsheets.

Step 10: Launching the iControl Edge Web Site

The iControl Edge system is designed to be ready for operation from the moment the initial setup is completed. When the Application Server at the central monitoring location, and all remote Application Servers, Densité frames, GC-100 network adapters and Allégro systems are configured and online, an operator with network access can get started simply by launching the iControl Edge Web site.

> **Note:**   The iControl Edge Web site can be accessed from any PC or laptop on the same network as the Application Server. iControl Edge offers several pre-configured versions of its main Web page. Choose either a dual-screen or a single-screen layout, with the appropriate resolution for your client PC or laptop.

To launch the iControl Edge Web site:

1. From a client PC or laptop on the same network as the Application Server, open a Web browser and type the Application Server's IP address in the address bar.

    The iControl Startup Page appears:

2. Click **iC Web**.

The Java Web Start window opens, and the iControl Web application is downloaded to your PC or laptop. When the download is completed, the iControl Web splash screen appears:

A few seconds later, the iControl Web browser window appears:
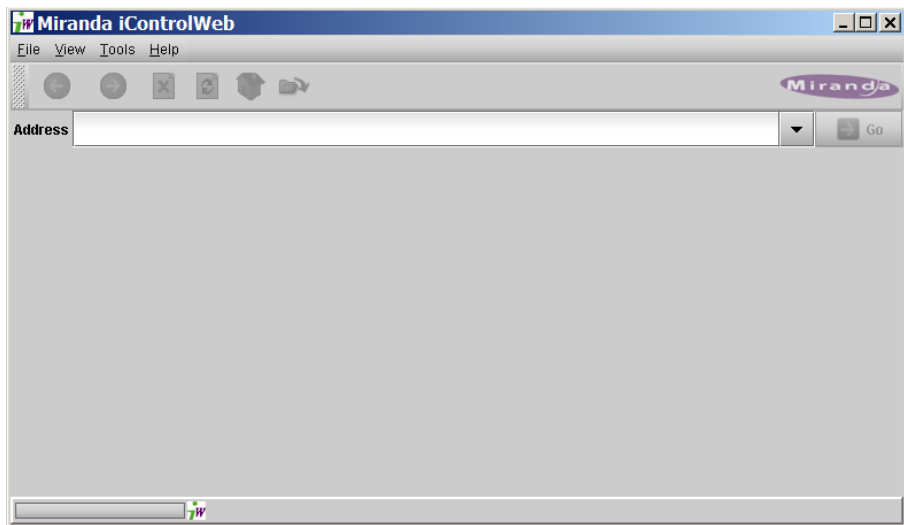
3. On the **File** menu, click **Open Site**.

4. In the **Open site** window that appears, type the Application Server's IP address:
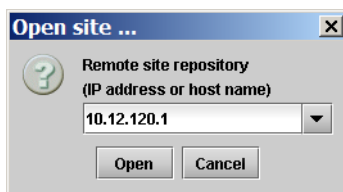
5. In the **Select site** window, double-click **EDGE:**
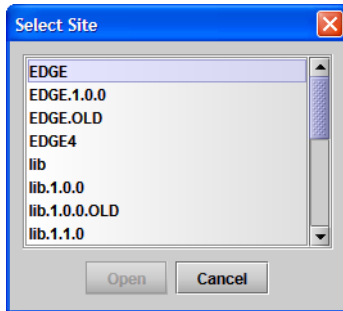
> **Note:** You may see other versions of the EDGE Web site. These are backups of previous versions that were saved when updating the Web site, and could be useful should you need to revert to an older version.

6. In the **Select page** window, double-click the desired home page.

For instance:

- **Home.mpf**, if you have two 1600×1200 monitor

- **HomeEDGE4.mpf**, if you have a 4-input head-end and two 1600×1200 monitor

- **Home1280x1024.mpf**, for a single monitor with a resolution of 1280×1024

- **Home_1600x1050x2.mpf**, if you have two 1600×1050 monitors in *Multiple Monitor*[1] mode

- **HomeEDGE4_1600x1050x2.mpf**, if you have a 4-input head-end and two 1600×1050 monitors in *Multiple Monitor* mode
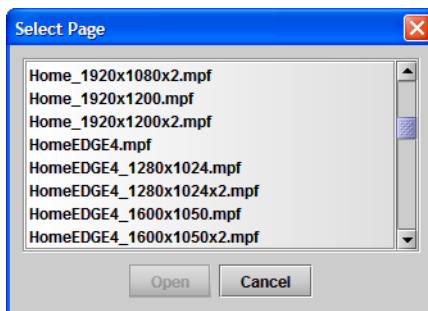
The current version of iControl Edge includes three sets of pre-configured single-screen and double-screen home pages: one set for systems with typically 4 set-top boxes, another one for systems

---

1. *Multiple Monitor* mode is when you have two monitors connected to one PC and you expand your primary display to the second monitor.

with 8 set-top boxes, and the default set for system with 16 set-top boxes. The table below shows the supported monitor resolutions:

Resolution	Single/ dual	16-player monitoring area	8-player monitoring area	4-player monitoring area
1280 × 1024	1 screen	Home_1280x1024	HomeEDGE8_1280x1024	HomeEDGE4_1280x1024
	2 screens	Home_1280x1024x2	HomeEDGE8_1280x1024x2	HomeEDGE4_1280x1024x2
1600 × 1050	1 screen	Home_1600x1050	HomeEDGE8_1600x1050	HomeEDGE4_1600x1050
	2 screens	Home_1600x1050x2	HomeEDGE8_1600x1050x2	HomeEDGE4_1600x1050x2
1600 × 1200	1 screen	Home_1600x1200	HomeEDGE8_1600x1200	HomeEDGE4_1600x1200
	2 screens	Home	HomeEDGE8	HomeEDGE4
1680 × 1050	1 screen	Home_1680x1050	HomeEDGE8_1680x1050	HomeEDGE4_1680x1050
	2 screens	Home_1680x1050x2	HomeEDGE8_1680x1050x2	HomeEDGE4_1680x1050x2
1920 × 1080	1 screen	Home_1920x1080	HomeEDGE8_1920x1080	HomeEDGE4_1920x1080
	2 screens	Home_1920x1080x2	HomeEDGE8_1920x1080x2	HomeEDGE4_1920x1080x2
1920 × 1200	1 screen	Home_1920x1200	HomeEDGE8_1920x1200	HomeEDGE4_1920x1200
	2 screens	Home_1920x1200x2	HomeEDGE8_1920x1200x2	HomeEDGE4_1920x1200x2

In a few moments, the iControl Edge Web interface appears:

7. On the **View** menu, click **Total full screen** (or press Ctrl+F11) to display the full screen over dual monitors if you chose a dual-screen layout. Click **Full screen** (or press F11) if you chose a single-screen layout.

> **Note:** Press F11 or Ctrl+F11 again to restore the iC Web window.
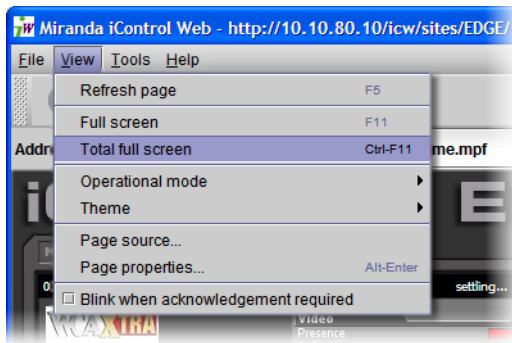
Alternatively, right-click in a blank area between elements on the Web page (e.g. between thumbnails, or between the banner and the monitoring area), and then click **Toggle total full screen** (or **Toggle full screen**) on the shortcut menu.
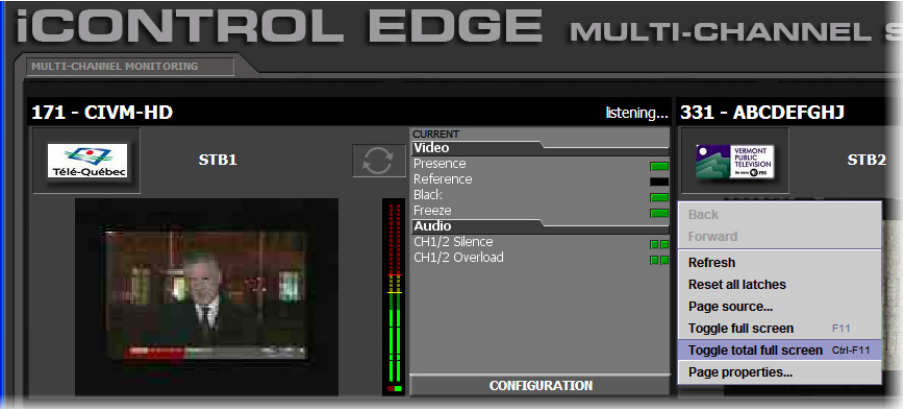
The complete monitoring Web page appears in full screen mode:
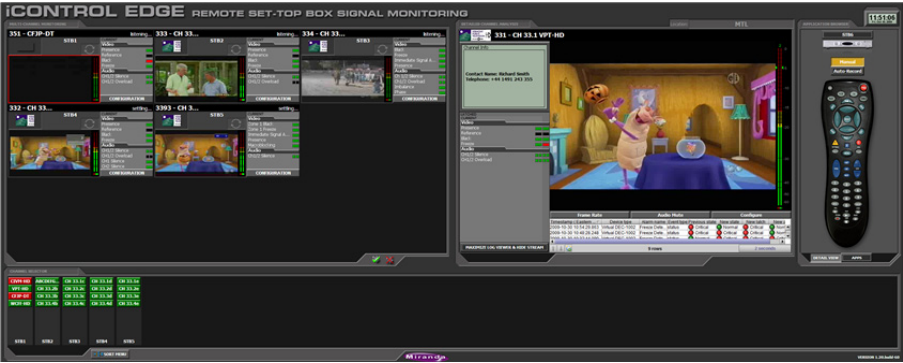
iControl Edge dual-screen Web page in total full screen mode (over two monitors)
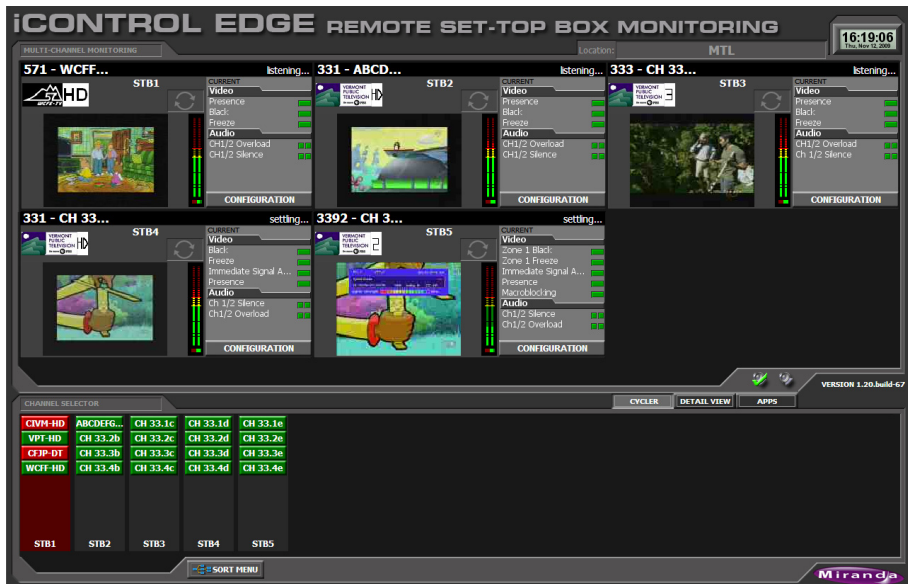
iControl Edge single-screen Web page in full screen mode

8. If you set this site as your home page, you will not need to go through the selection steps described above any more.

> **Note:** To set this site to open by default, click **Set home page** on the **Tools** menu.
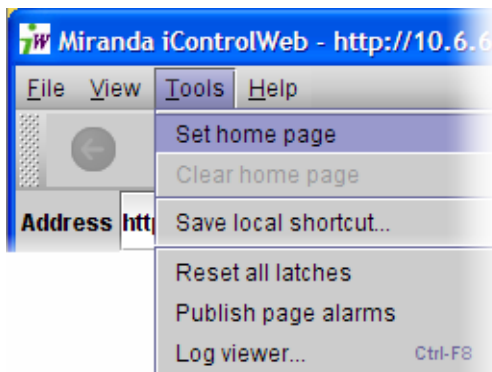
The next time you open iControl Web, this iControl Edge Web page will appear by default.

Congratulations—your iControl Edge system is now ready for operation! For a more complete description of the monitoring application, please refer to the iControl Edge Operator's Overview.

Troubleshooting A

If you encounter problems with your iControl Edge system, you should begin your

troubleshooting by verifying that the client PC and the Application Server are networked

correctly to the other devices that are part of your system.

Verifying Device Connectivity

One way of verifying that the client PC and the Application Server are networked correctly to the other devices that are part of your system is to use an SSH client such as PuTTY to ping them from the Application Server. If you do not have PuTTY installed on your PC, see "Using PuTTY" on page 93.

To verify that a device is properly connected to your system:

1. Launch PuTTY and log on to the Application Server (see "Establishing an SSH Connection with an Application Server" on page 94).

2. In the PuTTY command line window, type the following:

   ping AAA.BBB.CCC.DDD

   where AAA.BBB.CCC.DDD is the IP address of a Global Caché GC-100 Network Adapter. A message similar to the following should appear:

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

   • If the ping command is successful, stop the ping by pressing Ctrl+C.

   • If the message does not appear within a second, stop the ping by pressing Ctrl+C, and then verify that the device is powered up, properly cabled, and that its IP address is correctly configured.

3. For each Global Caché GC-100 Network Adapter, type the following command:

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

where `AAA.BBB.CCC.DDD` is the GC-100's IP address (e.g. 192.168.1.70). A message similar to the following should appear:

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

• If the ping command is successful, stop the ping by pressing Ctrl+C.

• If the message does not appear within a second, stop the ping by pressing Ctrl+C, and then verify that the device is powered up, properly cabled, and that its IP address is correctly configured.

4. For each Allégro system in your configuration, type the following command:

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

where `AAA.BBB.CCC.DDD` is the Allégro system's IP address (e.g. 10.0.3.7). A message similar to the following should appear:

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

• If the ping command is successful, stop the ping by pressing Ctrl+C.

• If the message does not appear within a second, stop the ping by pressing Ctrl+C, and then verify that the device is powered up, properly cabled, and that its IP address is correctly configured.

5. Type `exit`, and then press Enter to close the PuTTY command line window.

6. If your problem persists, consult the troubleshooting chart below.

Troubleshooting Chart

Symptom	Action
iControl Edge Web monitoring interface does not load	Verify that the IP addresses of the various devices that are part of your system are set correctly in the configuration spreadsheet for the selected location (see "Devices Spreadsheet" on page 64). If a device is not detected on the network, attempts to load the iControl Edge Web interface may continue for several minutes, until a communication timeout occurs.
All alarms in the Alarm Panels are blue	Verify that the **GSM** and **Densité Manager** services are active on the Application Server (see "Restarting the General Status Manager (GSM) Services" on page 80).
No video in a player	Open the control panel for the video probe associated with the player and enable thumbnail streaming (see "Enabling Thumbnail Streaming" on page 36).

Symptom	Action
No audio at the client PC	• Verify that the **Audio Mute** button in the monitoring page is not in the **Mute** position. Mute is ON any time a new stream is selected. • Click **Monitor this stream** on the Allégro System Status page (see "Allégro System Status page" on page 45). When the **Miranda Streaming Player** window opens, check to see if the audio level meter indicates any activity. If there is no activity, then it is likely that the Allégro is not receiving audio input. • On the Allégro Streaming Encoder Configuration page (see "Streaming Encoder Configuration page (Video/Audio)" on page 47), verify that Audio is set to: (i) Enabled=Yes, (ii) MAC2 - 44100 samp./sec, 16 bit, and (iii) stereo.
No video at the client PC	• Verify that the RCA composite video input cable is connected to port 1 (right-hand side) of the video capture card on the back of the Allégro. • Verify that the video encoder is running on the Allégro Streaming Encoder Status page (from the Allégro Web interface, under **Streaming Encoder** in the left navigation bar, click **Status**).
Java Web Start application reports errors	If the Java Web Start application reports errors regarding the inability to find files, it is important to clear the Internet Explorer cache. Open the client PC's Java Control Panel. Click the **Java** tab, and then click **View** under **Java Application Runtime Settings**. Verify that the **User** version numbers under **Platform** and **Product** are the same as what was installed with iControl. Disable any newer versions (by clicking the corresponding check boxes).
Allégro stream not available	Verify that DHCP has **not** been used to allocate the Allégro TCP/IP address.
iControl Edge Web interface does not load	• If this is a new client, verify that Java Runtime Environment (JRE for Windows) has been installed. See "Software Requirements" on page 9. • Verify that the default page has been set. See "Step 10: Launching the iControl Edge Web Site" on page 82.

Using PuTTY

PuTTY is an open source terminal emulator application that supports the SSH protocol. It

can be used to establish an SSH connection with iControl Application Servers.
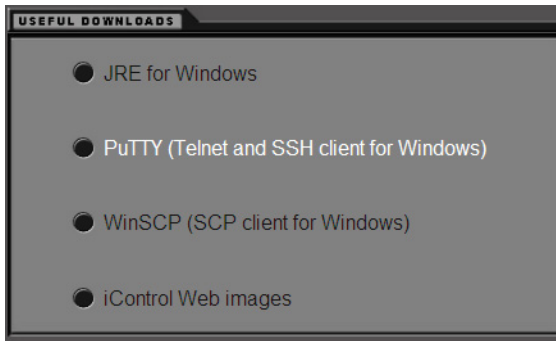
Installing PuTTY

PuTTY is available from your Application Server's Useful Downloads page.

To install PuTTY on your client PC or laptop:

1. Open an Application Server's Startup Page in a Web browser.

2. On the iControl Startup page, click **Useful Downloads**.
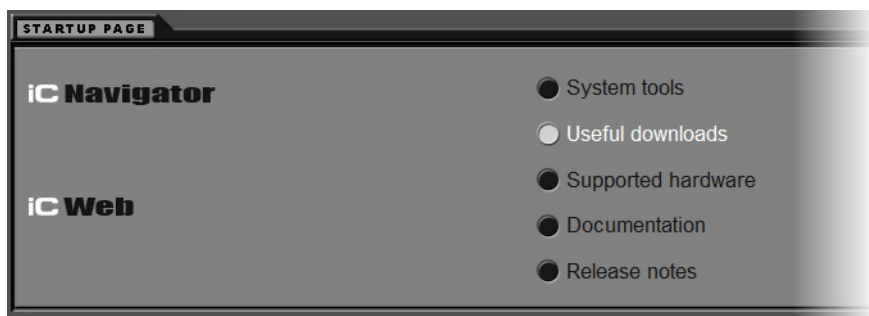
3. On the Useful Downloads page, click **PuTTY** to download the PuTTY executable file (`putty.exe`).

4. When prompted, save the file to your desktop, or some other location on your PC or laptop.

Establishing an SSH Connection with an Application Server

To establish an SSH connection with the Application Server:

1. Browse to the PuTTY executable file on your PC or laptop, and then open it.

> **Note:** If Windows prompt you about the application's signature, click **Yes**.

The **PuTTY Configuration** window appears:
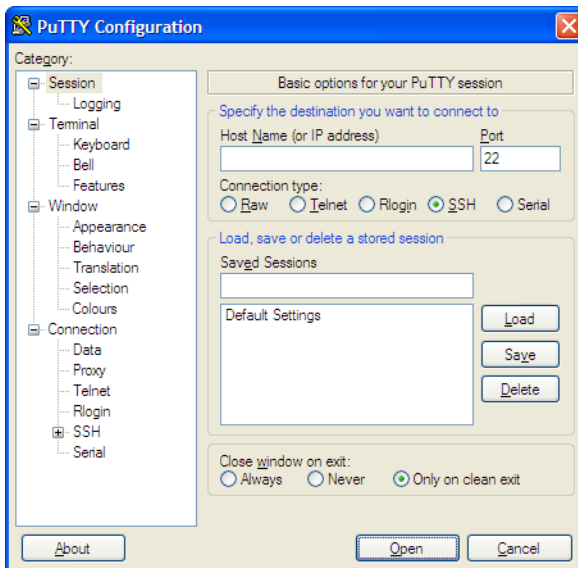
2. In the **Session** panel, specify your Application Server's IP address or host name, make sure that **SSH** is the selected connection type, and then click **Open**.
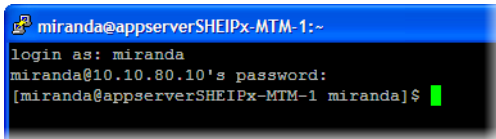
> **Note:** If the **PuTTY Security Alert** window appears, click **Yes** to close it.

A command line window appears, prompting you for a user name.

> **Note:** Application Servers are configured by default with the user name **miranda** and the password **icontrol**, but these may have been changed by your system administrator.

3. Type **miranda**, and then press Enter.
4. When prompted for a password, type **icontrol**, and then press Enter.

You are now connected to the Application Server.

Ending a PuTTY Session

To end the SSH session:

- Type `exit`, and then press Enter to close the PuTTY command line window.

Using WinSCP

WinSCP (Windows Secure copy) is an open source SFTP and FTP client for Microsoft

Windows. Its main function is secure file transfer between a local and a remote computer.

As of iControl 3.21, it can be used (in place of the Webmin File Manager) to copy files to and

from iControl Application Servers.

Installing WinSCP

To install WinSCP on your PC:

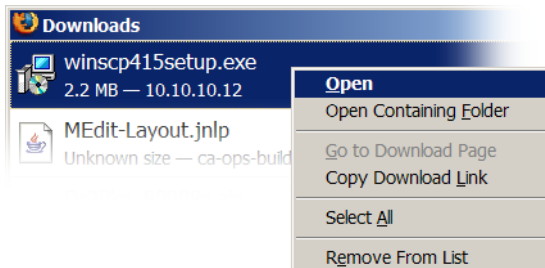1. Open an Application Server's Startup Page in a Web browser.

2. Click **Useful Downloads**:
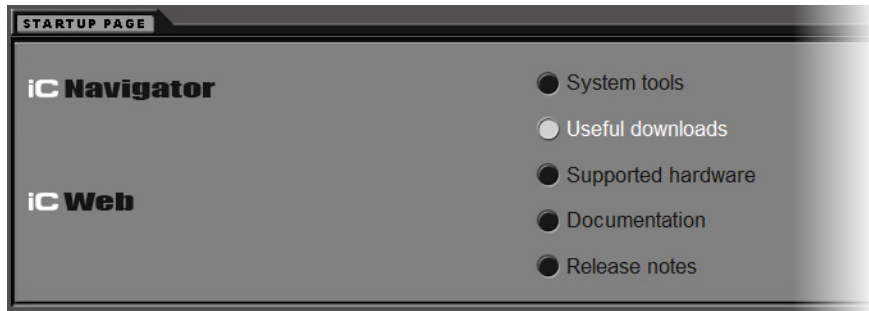
3. Click **WinSCP**:
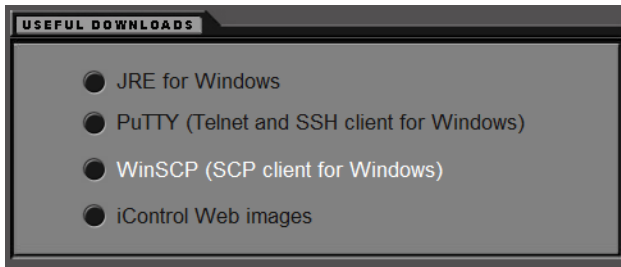
4. When prompted, click **Save File** to save the WinSCP installer to your PC:
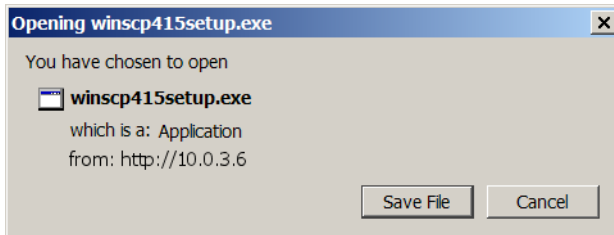
5. When the download is complete, open your browser's Downloads window:
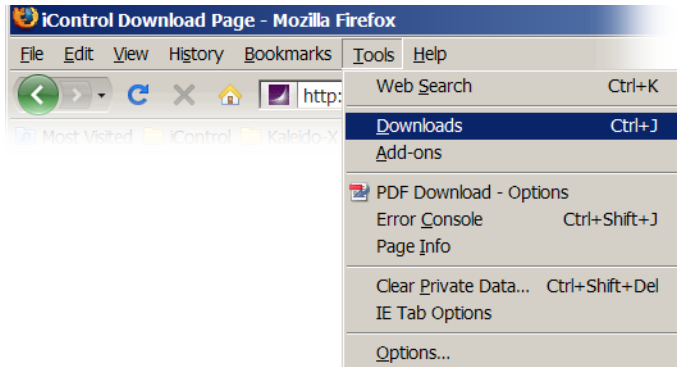
6. Right-click the WinSCP Installer, and then click **Open** on the shortcut menu:

7. If a security warning appears, click **Run**:
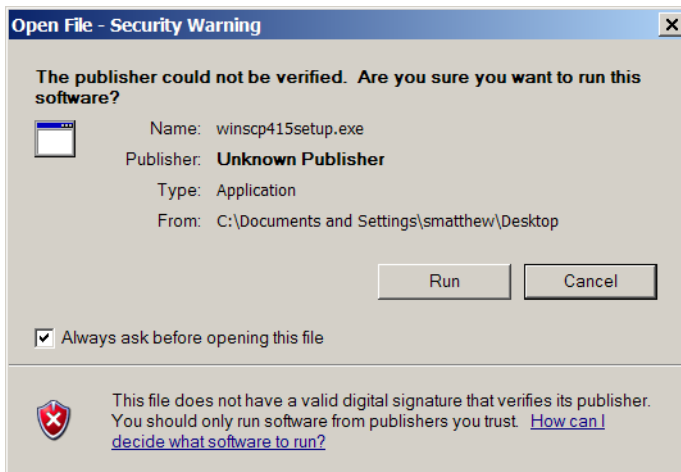
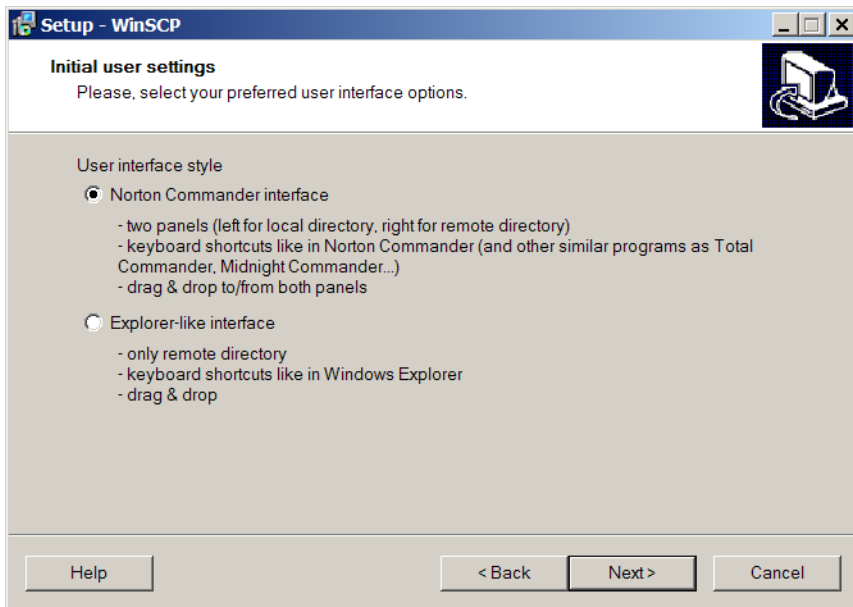8. When prompted, select a language, and then click **OK**:
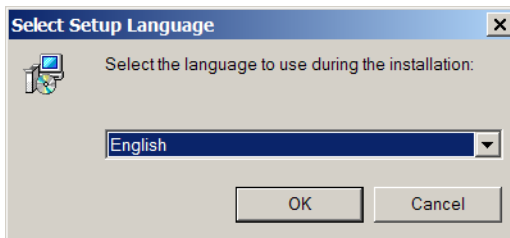
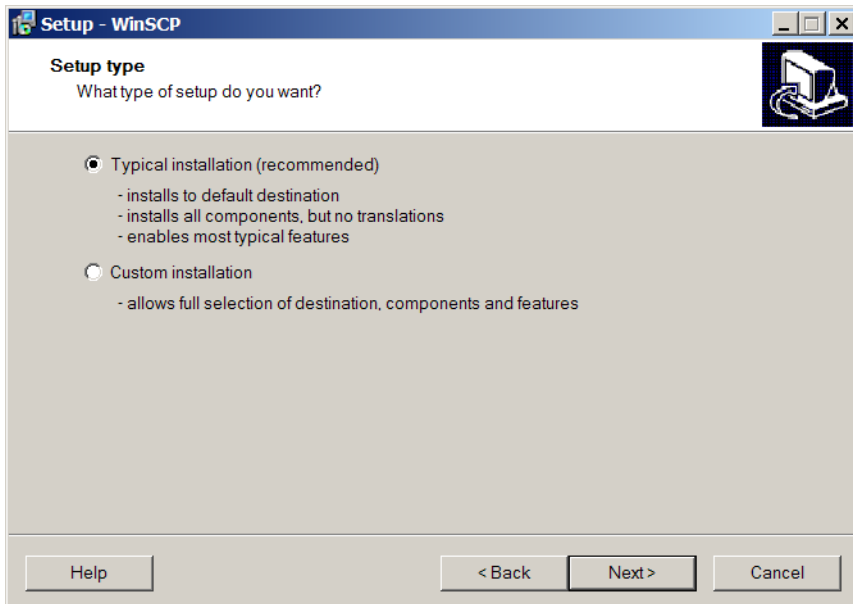
9. When the WinSCP Setup Wizard appears, click **Next**:

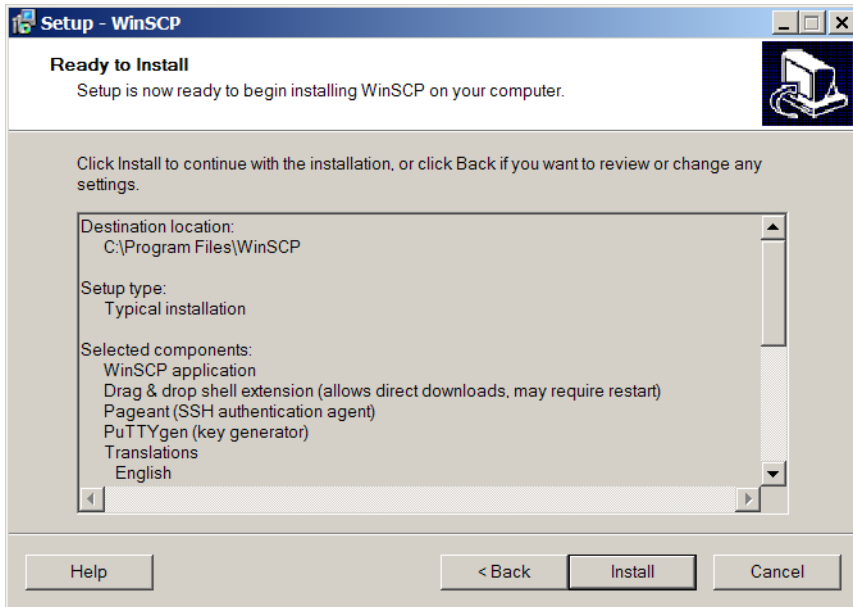10. When the License Agreement appears, click **Next** to continue:
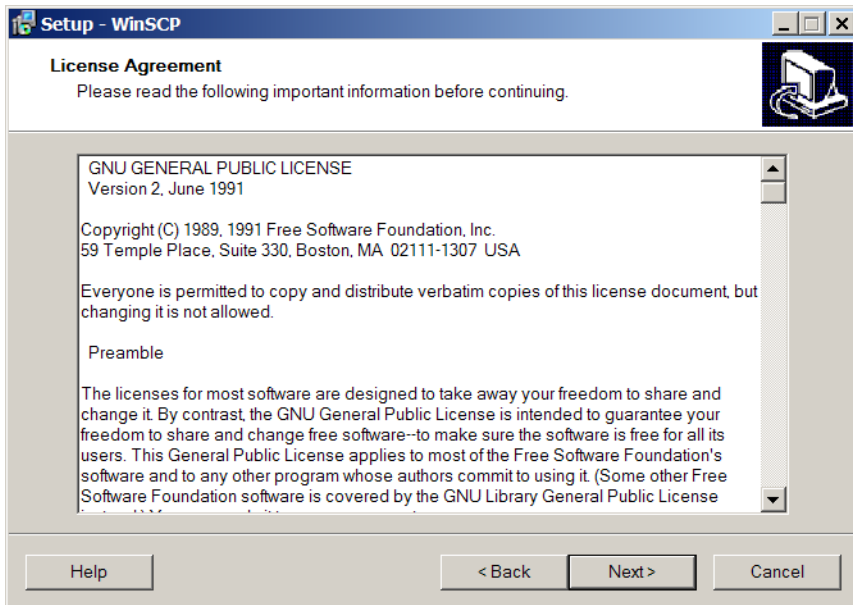
11. In the **Initial user settings** window, choose **Norton Commander interface**, and then click **Next** to
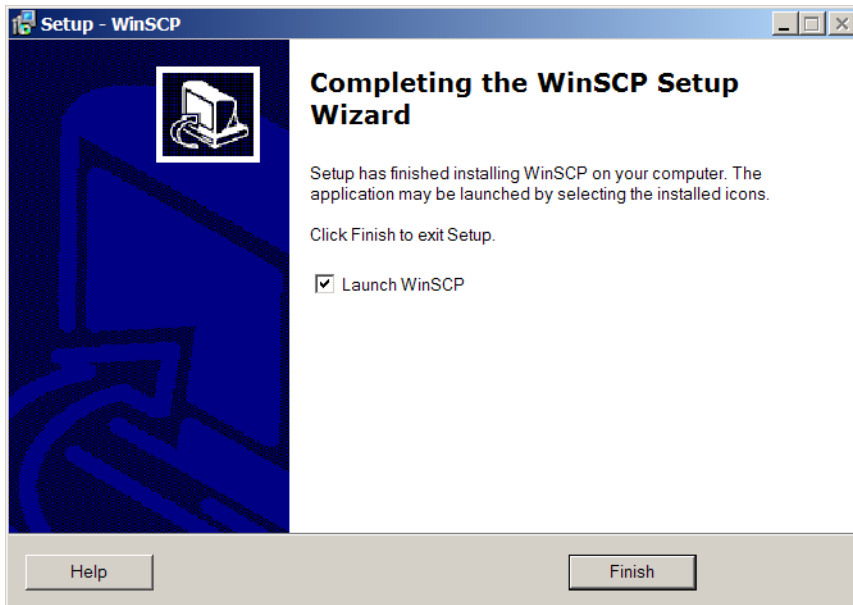continue:

12. In the **Setup type** window, choose **Typical installation**, and then click **Next** to continue:

13. When the **Ready to install** window appears, click **Install** to continue:

14. Click **Finish** to exit the WinSCP Setup Wizard:

# Logging on to an Application Server from WinSCP

To log on to the Application Server:

1. Launch WinSCP (on the **Start** menu, point to **All Program**, then to **WinSCP**, and then click **WinSCP**). The WinSCP Login window appears.

2. Type the Application Server's IP address in the **Host name** box, and specify your user name and password.

> **Note:**   The default IP address is **10.0.3.6**, default user names are **miranda** and **root**, and the default password (for both) is **icontrol**. The **miranda** user account has suitable permissions for most applications. However for some specific purposes such as configuring streaming relays for an Allégro (see "Configuring Allégro Streaming Relays" on page 50), you will need to be logged on as user **root**.
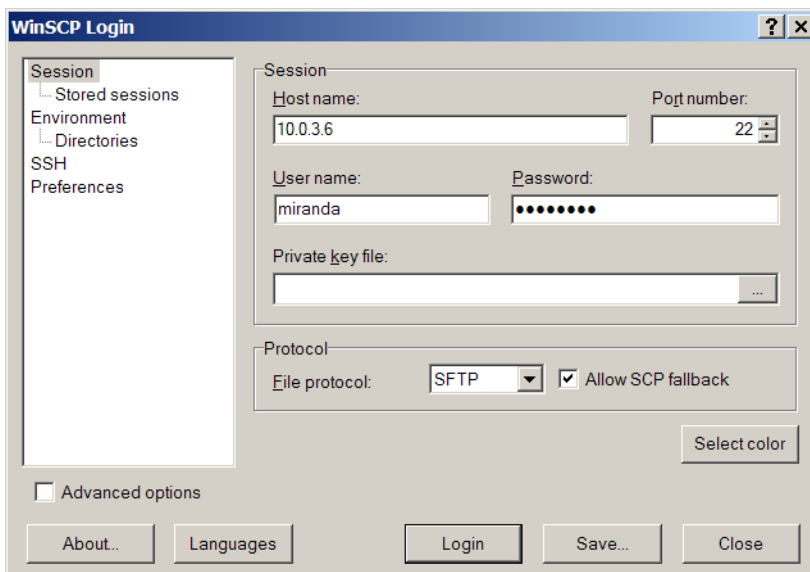
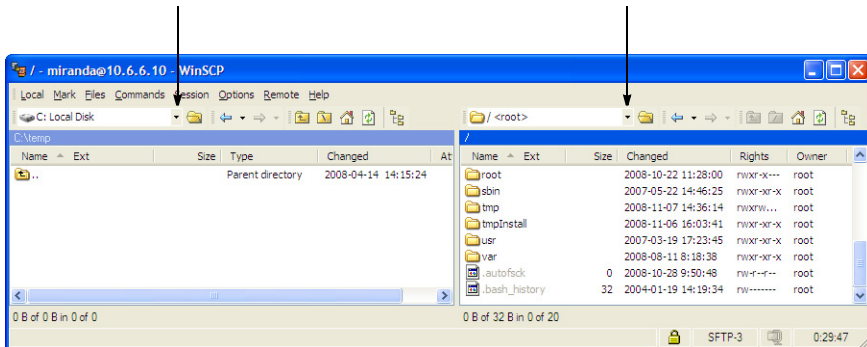A message concerning the server's host key may appear:
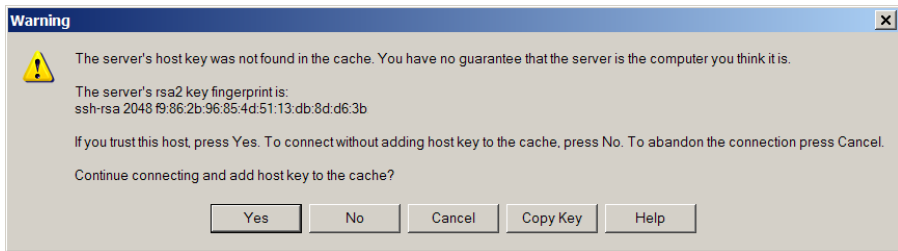
3. Click **Yes** to continue.

   The main WinSCP window opens, showing the files on your PC in the left panel, and the files on the Application Server in the right panel:

   You can access the top level of your PC's file system from this menu

   You can access the root level of the Application Server's file system from this menu

Contact Us!

Miranda Technical Support

For technical assistance, please contact the Miranda Technical Support centre nearest you:

Americas

Office hours: 9:00 a.m. – 9:00 p.m. (EST)
Telephone: +1-800-224-7882
Fax: +1-514-335-1614
E-mail: *techsupp@miranda.com*

Europe, Middle East, Africa, UK

Office hours: 9:00 a.m. – 6:00 p.m. (GMT)
Telephone: +44 (0) 1491 820222
Fax: +44 (0) 1491 820002
E-mail: *eurotech@miranda.com*

France

Office hours: 9:00 a.m. – 5:00 p.m. (GMT+1)
Telephone: +33 1 55 86 87 88
Fax: +33 1 55 86 00 29
E-mail: *eurotech@miranda.com*

Asia

Office hours: 9:00 a.m. – 5:00 p.m. (GMT+8)
Telephone: +852-2539-6987
Fax: +852-2539-0804
E-mail: *asiatech@miranda.com*

China

Telephone: +86-10-5873-1814
E-mail: *asiatech@miranda.com*

Corporate Head Office

Miranda Technologies Inc.

3499 Douglas-B.-Floreani, St-Laurent, Quebec, Canada H4S 1Y6
Telephone: 514-333-1772
Fax: 514-333-9828
Web: *www.miranda.com*