# iControl

Signal and facility monitoring

# **Quick Start Guide**

M226-0700-343

1 February 2013



A BELDEN BRAND

# **Copyright Notice**

Copyright © 2001 - 2013 Miranda Technologies Inc. All rights reserved.

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

Miranda Technologies Inc. hereby grants permission and license to owners of iControl 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 (http://www.miranda.com).

Title	iControl Quick Start Guide	
Part Number	M226-0700-343	
Revision Date	1 February 2013 2:29 pm	

# Table of Contents

1	Introduction to iControl	. 1
	Overview	1
	Operational Overview	2
	User Interface	3
	How iControl Works	4
	Components of iControl	5
2	Getting Started	. 7
	Getting Organized	7
	New Installation	7
	Upgrade	7
	Installation and Network Requirements	8
	Hardware Requirements	8
	Software Requirements	9
	Running Java in Windows2000 Compatibility Mode	. 10
	Installation and Network Requirements	. 12
	Software Component Compatibility	. 12
	Task 1 — Installing the iControl Application Server	13
	Task 2 — Preparing a PC for Configuring the Application Server	15
	Task 3 — Configuring the iControl Application Server	20
	Task 4 — Configuring Client Workstations	33
	Task 5 — Configuring the Application Server on the Network	35
	Task 6 — Configuring GPI Outputs on a GPI-1501	43
	Task 7 — Connecting & Configuring Devices	48
	Task 8 — Configuring System Time	53
<b>C</b> -	antact IIcl	67
	///////////////////////////////////////	37

toc

# Introduction to iControl

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

## **Summary**

Overview	1
How iControl Works	4

# **Overview**

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

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

Features of the iControl system include:

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

iControl represents video networks with rich, interactive graphics that are immediately understandable and easy to operate. The system is geared towards simplifying operations so that a single user can control more channels, or a broader range of monitoring and control tasks.

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

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



# **Operational Overview**

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



#### iControl Monitoring Workstation

# User Interface

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

HSIM REMOTE STATION MONITORING		Miranga 12021
And and a second		
Desire on the second seco		(MINAN)
	A series and a series and a series of the se	Hermitian Constraints     Hermitian Constraints     Hermitian Constraints     Hermitian Constraints     Hermitian     Hermitian     Hermitian     Hermitian     Hermitian     Hermitian
WEAVEN] WH	🖉 🦌 IC- total	N0000 (144)

Example 1: customized iControl User Interface



Example 2: customized iControl User Interface

CONTROL GC ADVANCED INCOMING FEED GUALITY CON	VTROL	1330244
		RECEIPT
	INIComputer         Factor         NonComputer           207 2014         State Office         T	-
		HU 1.1 Control Color Color 1.1 C Market Color Color Color Market Color Color Color Market Color Color Market Color Color Market Color Color Market Color Color Market Color Mar

Example 3: customized iControl User Interface

# **How iControl Works**

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

iControl runs in a distributed network environment. Devices to be monitored or controlled are either directly connected to the iControl Application Server, or accessible over a TCP/IP

connection. Each iControl Application Server runs several device control services, as well as a lookup service.

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

# Components of iControl

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

- iC Navigator
- iC Router Control
- iC Website Creator
- iC Web

Each of these core components is a Java application, stored on the iControl Application Server. When a user points a Web browser to the IP address of the Application Server, a Startup page appears, with links for each application. If the user clicks on one of these links, the Java code is downloaded to their PC, and the application launches.

There are two other core iControl components, important for system administration, and the smooth, integrated operation of iControl as a whole:

- iControl Webmin
- iControl Services

For a more in-depth overview of iControl's features, please refer to Chapter1: "Introduction to iControl" in the *iControl User Guide*.

# **Getting Started**

This Quick Start Guide is designed to help you get iControl up and running for the first time. Follow the steps outlined in this chapter in sequence. When you are finished, your iControl system will be configured and operational.

# **Getting Organized**

Getting an iControl system up and running involves installing, connecting and configuring a variety of hardware and software components. This manual provides a guide to successfully installing and activating your iControl system in nine tasks:

- "Task 1: Installing the iControl Application Server", on page 13
- "Task 2: Preparing a PC for Configuring the Application Server", on page 15
- "Task 3: Configuring the iControl Application Server", on page 20
- "Task 4: Configuring Client Workstations", on page 33
- "Task 5: Configuring the Application Server on the Network", on page 35
- "Task 6: Configuring GPI Outputs on a GPI-1501", on page 43
- "Task 7: Connecting & Configuring Devices", on page 48
- "Task 8: Configuring System Time", on page 53

#### **New Installation**

A new iControl system, as shipped, includes one or more iControl Application Servers and related hardware accessories. It also ships with a document folder containing this Quick Start Guide, Release Notes, as well as a Welcome letter with Setup & Configuration checklists that provide a summary of the main steps that must be completed to properly set up and configure an iControl System.

## Upgrade

The latest version of iControl is pre-installed on all new systems. If you are planning to upgrade an existing iControl system to the latest version, you will need to contact the Miranda Technical Support team (support@miranda.com) to request an upgrade package.

#### **Upgrading from iControl 1.xx**

Previous versions (1.xx) of iControl are not compatible with release versions 2.00 and higher. Not all configuration files can be reused. User configurations such as iControl Navigator aliases, error log configuration and proc amps must be regenerated. We recommend you record all values before proceeding with an upgrade. Old iControl Web sites will be converted, but the links will need to be reassigned.

An upgrade from version 1.xx involves a platform change. Please contact the Miranda Technical Support team for more information

#### Upgrading from 2.xx

In order to update your system from version 2.xx releases, you must obtain an upgrade package from the Miranda Technical Support team. This package consists of the files and instructions you will need, which may vary according to the system to be upgraded.

When planning an upgrade, consider the following:

- If you are upgrading an existing Application Server, review "Hardware Requirements", on page 8. Some version 4.00 features (e.g. streaming and probes), if used, may require a hardware upgrade.
- Check compatibility with other Miranda and third-party software components (see the Release Notes). You may have to upgrade some applications.
- Review configuration guidelines (see the Release Notes) to properly set up your installation.
- Check the hardware compatibility of Imaging or Densité cards with this release (see the Release Notes). Firmware upgrades may be requested from the Miranda Technical Support team.

**Note:** The iControl Maintenance Form of the Application Server Web administration tool (Webmin) cannot be used to update from 2.xx. The update has to be performed through an SSH command line interface.

# **Installation and Network Requirements**

## Hardware Requirements

#### **iControl Clients**

The client platform must meet the following system requirements to qualify for this release:

iControl Client Platforms	Memory	Processor	Operating System
Minimum requirements for general usage (excluding iControl Web)	2 GB RAM	Intel Core i3 or better	Windows XP Professional or
Minimum requirement for streaming video and using iC Web	4 GB RAM		Windows 7'

1. On the Windows 7 platform, it is recommended to use the Java 1.6 runtime environment (update 21).

**Note:** On Windows 7 platforms, it is recommended to use the Java 1.6 runtime environment.

#### **Graphics Card**

Optimized for nVidia GeFORCE 6600GT (PCI Express, 128 MB DDR3, 1 GHz)

The Miranda Application Server must meet the following system requirements to qualify for this release:

Application Server Platforms	Memory	Processor
Recommended requirements for general usage with hosting of small Web sites, with streaming support and limited number of services	2 GB RAM	Intel Core i3 or better
Minimum requirements for a large configuration (e.g. 8 ports used for Symphonie frames, multiple Densité frames, RCP-100 or RCP-200 Client Gateway, proc amps, Router Control, and extensive iC Web sites	4 GB RAM	

#### **Supported Servers**

The latest version of iControl is supported on the following Application Servers:

- Dell PowerEdge 850
- Dell PowerEdge 860
- Dell PowerEdge R200
- Dell PowerEdge R210
- Dell PowerEdge R310

# Software Requirements

You can connect to an iControl Application Server from any client PC on your network using a standard Web browser. Once you connect to a valid Application Server IP address, you can download iControl applications to your client PC. Consequently, no other application software is needed, which greatly simplifies installation and system maintenance.

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

To run any application in the iControl suite, you need to have the following software installed on your PC:

• a Web browser (Internet Explorer 8.0 or Mozilla Firefox 1.5 or higher)

• Java 2 Runtime Environment (JRE) version 1.5.0\_07 or higher). A Java update (which includes Java Web Start) can be downloaded from the iControl Application Server (see "Installing Java", on page 33 for more information)

**IMPORTANT:** If the Java Web Start application reports errors regarding an inability to find files, it is important to clear the Internet Explorer cache.

IMPORTANT:	Recommendation to run Java in Windows 2000 Compatibility mode
------------	---

Miranda highly recommends you switch your Java 2 JRE to Windows 2000 Compatibility mode (see "Running Java in Windows2000 Compatibility Mode", on page 10).

# Running Java in Windows2000 Compatibility Mode

#### To switch your client PC's Java JRE to Windows2000 Compatibility mode

- 1. In Windows Explorer, navigate to the location of the following Java \*.exe files:
  - java.exe
  - javacpl.exe
  - javaw.exe
  - javaws.exe

Typically, you would find these files in a location such as the following:

C:\Program Files\Java\jre6\bin

- 2. Perform the following sub-steps for each of the above-mentioned files:
  - a) Right-click the file, and then click **Properties**.

م دوم المار والمار وم مراجع المراجع	والمستعمر والمعالي والمتعارية والمستعر والمستعر والمستعر	X
j2pcsc.dll		201
j2pkcs11.dll		201
🖇 jaas_nt.dll		201
java dl		201
👌 🤇 🏄 java.exe		201
java cow de	Open	101
javacrexe	Run as administrator Troubleshoot compatibility	101
) java-mi.exe	Scan with Sophos Anti-Virus	201
🍰 javaw.ex	Restore previous versions	101,
javaws.exe	Send to	▶ 201
🚳 jawt.dll	Cut	201
jbroker.exe	Сору	101
JdbcOdbc.dl	reate shortcut	201
} jdwp.dll	🛞 tete	201
kernel dlass	Rename	105
Contract (1)	Properties	

The **Properties** window appears.

🔮 java.exe Pro	operties	×
Security General	Details Previous Versions Compatibility Digital Signatures	
	java.exe	
Type of file:	Application (.exe)	
Description:	Java(TM) Platform SE binary	
Location:	C:\Program Files\Java\jre6\bin	
Size:	141 KB (145,184 bytes)	
Size on disk:	144 KB (147,456 bytes)	
Created:	Tuesday, December 21, 2010, 11:25:30	
Modified:	Tuesday, December 21, 2010, 11:25:30	
Accessed:	Tuesday, December 21, 2010, 11:25:30	
Attributes:	Read-only Hidden Advanced	
	OK Cancel Apply	

b) Click the **Compatibility** tab.



The **Compatibility** tab appears in focus.

Security	Details	Previous Versions
General	Compatibility	Digital Signatures
vou have problem earlier version of atches that earlier eap me choose the Compatibility mode	s with this program and it w Windows, select the comp version. : <u>settings</u> ; gram in compatibility mode:	vorked correctly on batibility mode that
Windows XP (S	ervice Pack 3)	
E Durings	-less	
Hun in 256 c	olors	
E Hun in 640 x	480 screen resolution	
Disable visual themes		
Disable desk	top composition	
Disable displ	ay scaling on high DPI set	tings
Privilege Level		
Run this prog	gram as an administrator	
😗 Change settir	ngs for all users	

- c) Select Run this program in compatibility mode for.
- d) From the list, click **Windows 2000**.

🕌 java.exe Propert	ies		
Security General	Details Compatibility	Previous Version Digital Signatur	
If you have problems with this program and it worked correctly on an earlier version of Windows, select the compatibility mode that matches that earlier version. <u>Help me choose the settings</u> Comparative mode			
Windows XP (S Windows 95/ Windows 95/ Windows 98/V Windows 2000 Windows XP (S Windows XP (S Windows Serve Windows Vista Windows Vista Windows Vista	Vindows Me U (Service Pack 5) ervice Pack 5) ervice Pack 3) r 2003 (Service Pack 1) r 2008 (Service Pack 1) (Service Pack 1) (Service Pack 2)		
Privilege Level	gram as an administrator		

e) Click **OK**.



# Installation and Network Requirements

We recommend that you install the iControl Application Server (as well as the associated equipment it controls) on a dedicated LAN, using the existing security infrastructure. A qualified system administrator should verify that the setup follows your organization's security standards.

# Software Component Compatibility

iControl is compatible with the following Miranda software components:

- iControl Router/Router Configuration Manager and Router Service version 3.00 (or later).
- RCP-100 Remote Control Panel firmware version 1.80 (or higher)
- RCP-200 Remote Control Panel firmware version 1.1.0 and later (version 1.3.0 or later recommended)

- iC Web version 3.00 (or later)
- Kaleido-K2 version 5.30 (or later refer to the Kaleido-K2 release notes)
- Kaleido-X version 2.0 (or later)
- Kaleido-IP version 6.0.0 and later (version 6.5.0 recommended for best performance and maximum functionality)
- Densité CPU ETH controller version 3.00 (or later)
- Densité CPU-ETH2 version 1.0.5 or later (version 2.0.4 or later recommended)
- EdgeVision version 1.0.0 or later (version 1.2.0 recommended for best performance and maximum functionality)
- NV9000 version 6.1.0.1538 and later (version 6.2.0.1674 and later recommended for best performance and maximum functionality)
- SEUtilities version 6.0.28 and later (version 6.2.2 build 125 and later recommended for best performance and maximum functionality)

# Task 1: Installing the iControl Application Server

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

#### Notes

- As of the release of iControl version 4.00, all Application Servers configured with new systems are Dell PowerEdge models R210 or R310. The older Dell PowerEdge 850/860 servers are still supported but may require hardware/firmware upgrades in order to run iControl version 4.40.
- If your Application Server is a Dell PowerEdge model, install the faceplate after the server is placed in a rack. If your Application Server is an older Supermicro model, install the faceplate before the server is placed in a rack.

#### To install the iControl Application Server

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

#### Notes

- An unexpected power disruption, such as might occur during a power failure, can damage the file system on an iControl Application Server. It is strongly recommended that all Application Servers be connected to a standby power source, such as a UPS (Uninterruptible Power Supply), as a preventive measure.
- Hardware documentation for the PowerEdge 850, 860, R200, R210, and R310 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/
  - http://support.dell.com/support/edocs/systems/peR210/
  - http://support.dell.com/support/edocs/systems/peR310/

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

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

#### To connect the 8-port breakout box

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

**Note:** It is important to assign serial ports on both the iControl Application Server and any routers that will be participating in the iControl system to avoid conflicts that might negatively affect system performance. Refer to "Task 7: Connecting & Configuring Devices", on page 48 of this guide for more information.

#### **RS-422 Pinout Assignments**

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



RS-422 connector pinout

# Task 2: Preparing a PC for Configuring the Application Server

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

Perform one of the following procedures depending upon your client PC's operating system:

- "Configuring TCP/IP Settings of a Client PC Running Windows 7", on page 15
- "Configuring TCP/IP Settings of a Client PC Running Windows XP", on page 18

# Configuring TCP/IP Settings of a Client PC Running Windows 7

#### To configure TCP/IP settings of a client PC running Windows 7

1. From the Windows 7 Start menu, click Control Panel.



The Control Panel appears.

2. Click Network and Sharing Center.

Programs	Dell ControlPoint
Manager	B Devices and Printers
Access Center	F Folder Options
Started	🍓 HomeGroup
g Options	🐱 Intel(R) GMA Driver for Mobile
¢ Options	🕌 Java
n and Other Sensors	C Meil
{	🚆 Network and Sharing Center
nance Information and Tools	Personalization
Options	🔄 Programs and Features
V-	👷 🔗 Region and Language

The Network and Sharing Center appears.

3. In the **Access type** area, click the link that corresponds to your LAN Internet connection (**Local Area Connection** in the example shown).



The Local Area Connection Status window appears.

🎍 Local Area Connecti	on Status 🗮	x
General		
Connection IPv4 Connectivity:	Internet	
IPv6 Connectivity:	No Internet access	
Media State:	Enabled	
Duration:	00:50:54	
Speed:	100.0 Mbps	
Details		
Activity		.
	Sent — 🦣 — Received	
Bytes:	7,851,575 202,483,747	
Properties	Disable Diagnose	
	Close	

4. Click Properties.

The Local Area Connection Properties window appears.

Local Area Connection Properties
Networking Sharing
Connect using:
Intel(R) 82567LM Gigabit Network Connection
Configure
Install Uninstal Properties
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK Cancel

5. Select Internet Protocol Version 4 (TCP/IPv4), and then click Properties. The Internet Protocol Version 4 (TCP/IPv4) Properties window appears.

Internet Protocol Version 4 (TCP/IPv4)	Properties	? <b>×</b>	
General Alternate Configuration			
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.			
Obtain an IP address automatical	у		
Use the following IP address:			
IP address:			
Subnet mask:			
Default gateway:			
Obtain DNS server address auton	atically		
Use the following DNS server add	esses:		
Preferred DNS server:			
Alternate DNS server:	• • •		
Validate settings upon exit	Ac	dvanced	
	ОК	Cancel	

- 6. Take note of the PC's current settings.
- 7. Click Use the following IP address.
- 8. The default IP address of each new iControl Application Server is 10.0.3.6. On the client PC, type an address in the same range (e.g. 10.0.3.10) in the **IP address** field.
- 9. The default subnet mask of each new iControl Application Server is 255.255.0.0. On the client PC, type 255.255.0.0 in the **Subnet mask** field.

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

General							
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.							
O Us	e the following IP	address:					4
© Us IP ad	e the following IP dress:	address: —	10 .	0.3	. 10		Ĭ
IP ad Subn	e the following IP dress: et mask:	address: —	10 . 255 . 2	0.3 255.0	. 10 . 0	1	

- 10. Click **OK** to apply these settings.
- 11. In the Local Area Connection Properties window, click OK.
- 12. Close the Network and Sharing Center control panel.

**Note:** Remember to return the PC to its original network settings once you have finished configuring the iControl Application Server.

# Configuring TCP/IP Settings of a Client PC Running Windows XP

#### To configure TCP/IP settings of a client PC running Windows XP

- 1. From the Windows XP Start menu, select Settings | Control Panel | Network Connections.
- 2. Select the currently active Local Area Connection, and then right-click and click Properties.
- 3. In the Local Area Connection Properties window, select Internet Protocol (TCP/IP), and then click Properties.
- 4. In the Internet Protocol (TCP/IP) Properties window, click Use the following IP address.

Network Connections				
File Edit View Favorites Tools Advanced Help				
3 • 0 • ♪ ♪ ▷ ☆ ♪ × ♥   ■•				
Address 🗞 Network Connections				
Name	Туре	Status	Device Name	
LAN or High-Speed Internet	t			
Local Area Connection 2 Local Area Connection 3 Wireless Network Connection	LAN or High-Speed Inter LAN or High-Speed Inte 2 LAN or High-Speed Inte Local Area Connectio	net Disabled Internet Protocol (TCI General	Cisco Systems VPN Adapter P/IP) Properties	<u>?</u> ×
New Connection Wizard	General Advanced   Connect using: ■ Broadcom NetXtreme 57xx Gig This connection uses the following ite ■ GoS Packet Scheduler ■ GoS Packet Scheduler ■ Transmission Cortrol (TCP/IP) ■ Internet Protocol (TCP/IP) ■ Instell Uninste Description Transmission Cortrol Protocol/Intel wide area network protocol (Intel privide) Transmission Cortrol Protocol/Intel wide area network protocol/Intel Notify me when this connection h:	You can get IP setting capability. Otherwise, appropriate IP setting: Obtain an IP add Use the following IP address: Subnet mask: Default gateway: Obtain DNS sen Obtain DNS sen Alternate DNS sen	s assigned automatically if your network supports this you need to ask your network administrator for the s. tress automatically g IP address: 10 0 3 10 255 255 0 0 0 255 - 255 0 0 0 255 - 255 - 0 255 - 255 - 0 0 255 - 255 - 0 255 - 255 - 0 0 255 - 255 - 0 255 - 255	
•				
roadcom NetXtreme 57xx Gigabi	it Controller			

Configuring TCP/IP settings on a PC running Windows XP.

- 5. Take note of the PC's current settings.
- 6. The default IP address of each new iControl Application Server is 10.0.3.6. On the client PC, type an address in the same range (e.g. 10.0.3.10) in the **IP address** field.
- 7. The default subnet mask of each new iControl Application Server is 255.255.0.0. On the client PC, type 255.255.0.0 in the **Subnet mask** field.

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

- 8. Click **OK** to apply these settings.
- 9. In the Local Area Connection Properties window, click OK.
- 10. Close the Network Connections control panel.

**Note:** Remember to return the PC to its original network settings once you have finished configuring the iControl Application Server.

# Task 3: Configuring the iControl Application Server

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

- Connect to the Application Server from a Client PC
- Log on to the Application Server's Webmin utility and configure the Application Server's:
  - Ethernet interface
  - Network gateway
  - Domain Name Service settings
  - Host name and IP address
- Apply your changes and perform a readiness check

# Connecting to a New iControl Application Server

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

#### IMPORTANT: Ethernet Port Labels on the PowerEdge R210 and R310

If your Application Server is a Dell PowerEdge R210 or R310, please read the section regarding Ethernet port labels (see page 22).

#### To connect to a new Application Server

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



Connection between client PC and Application Server



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

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



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

The iControl Startup page appears.

icont Startup page	ROL
iC Navigator	
iC Router Control	License management
iC Web	♂ System tools
	Useful downloads
iC Creator	Supported hardware
iC Data Management	A Documentation
	◆ Release notes
iC Reports	
	in. Go here to make a license download request.

#### Notes

- iC Router Control, iC Web and iC Creator are optional, and will only appear on the iControl Startup Page if you purchased the corresponding options.
- If your Web browser cannot find the Application Server, make sure the PC's network settings are correct (see "Preparing a PC for Configuring the Application Server", on page 15).

#### Ethernet Port Labeling on the R210 and R310 Application Servers

The physical Ethernet ports on the backs of the Dell PowerEdge R210 and R310 are labeled as **Gb1** and **Gb2**. The physical (cabling) port called **Gb1** corresponds to logical (Webmin) port **eth0**. Likewise, the physical port called **Gb2** corresponds to logical port **eth1**. Throughout this document, when speaking of cabling and physical ports, the physical port numbers will match the logical port numbers, which is true for all types of Application Servers except the R200, R210, and R310. In the case of the R200, R210, and R310, you must map according to the table below. For example, if a procedure instructs you to connect a cable to an Application Server's **eth0** port, you must connect the cable to the R210's physical port labeled **Gb1**.

Physical Label on R200, R210, R310	Logical (Webmin) Name
Gb1	eth0
Gb2	eth1

Ethernet Port Mapping on the R200, R210, and R310 Application Servers

# Using Webmin to Configure the Application Server

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

#### Logging on to Webmin

**REQUIREMENT** Before beginning this procedure, make sure you have opened iControl.

#### To log on to iControl's Webmin utility

- Click System Tools on the iControl Startup page. The System Tools page appears.
- 2. Click Administration.



The Login to Webmin window appears.

Login to Webmin		
You must enter a userna		n to the Webmin server on
Username	miranda	
Password	•••••	
	Login Clear	
	Remember login perman	ently?

3. Type your user name and password. By default, these are:

- Username: miranda
- Password: icontrol
- 4. Click Login.

The iControl Webmin home page appears.

Miranda	a		
ሳ	Bootup and Shutdown		Custom Commands
Ø	Darwin Streaming Server		File Manager
<u>.</u>	Historic System Resources		Miranda iControl Management Tool
	Network Configuration	Ø	PostgreSQL Database Server
<b>.</b> •	Remote Storage Configuration		System Settings
O	Technical Support	$\swarrow$	Tomcat server
Ж	Webmin Users		

#### **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 page 25.
- 2. Configure your host addresses (see page 27).
- 3. Specify a network Gateway to be used by your Application Server (see page 28).
- 4. Configure the Ethernet interface (see page 29).
- 5. Restart and verify the configuration (see "Restarting the Application Server", on page 31).

Navigating to the Network Configuration Page

#### REQUIREMENT

Before beginning this procedure, make sure you are logged on to iControl Webmin (see page 23).

#### To navigate to the Network Configuration page

• On the Webmin 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).

#### REQUIREMENT

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

#### To specify the DNS settings to be used by the iControl Application Server

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

The Hostname and DNS Client page appears.

Hostna	me and DNS	5 Client		
DNS Client (	Options			
Hostname	pdev1	Resolution order	Hosts VIS+ DNS V	• •
	🗹 Update hostnam			
DNS	127.0.0.1	Search	None O Listed	.
servers		domains	miranda.com	• •
Save				

- 2. In the **Hostname** field, 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:

Parameter	Detailed instruction
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 option 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. www.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 Application Server", 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.

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

#### **Configuring Host Addresses**

#### REQUIREMENT

Before beginning this procedure, make sure you have navigated to the Network Configuration page of Webmin (see 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 is internally-generated and should be left as found:
  - IP Address: 127.0.0.1
  - Hostname: localhost.localdomain, localhost
- The host name you defined in step 2 of "Specifying DNS Client Settings", on page 25 should be listed here. However, you will need to configure the proper IP address for this Application Server.
- 2. Click the IP address of the iControl Application Server whose IP address you will change. The Edit Host Address page appears.

Edit Host	Addres	S	
Host and Addre	sses		
IP Address 10.0	0.3.6		
Hostnames <sub>Nev</sub>	wAppServer		^
			-
		Save	Delete

- 3. In the IP Address field, type the IP address you would like to give to this Application Server.
- 4. In the **Hostnames** field, 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 Application Server", on page 31).

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

**IMPORTANT:** 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.

#### REQUIREMENT

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

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

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

The Routing and Gateways page appears.

Routing a	and G	atewa	ys			
Routing config	juration a	ctivated a	t boot tim	е		
Default routes	eth0 -	e Gatewa 10.6.0.1	ý 			
Act as router?	) 🕥 Yes 🤇	No No				
Static routes	Interfac	Network	ς	Netmask	Gateway	
Local routes	Interfac	Network	(	Netmask	]	
	eth0	224.0.0.0		255.255.255.255		
Save						
Active Routes	5			=		
Destinaton G	ateway N	etmask	Interface	2		
10.6.0.0 N	lone 2	55.255.0.0	eth0			
169.254.0.0 N	lone 2	55.255.0.0	eth0			
127.0.0.0 N	lone 2	55.0.0.0	10			
Default Route 1	0.6.0.1		eth0			

2. Select eth0 from the Interface list in the Default Routes area.

#### IMPORTANT: Ethernet Port Labels on the R210 and R310 Application Servers

If your Application Server is a Dell PowerEdge R210 or R310, please read the section regarding Ethernet port labels (see page 22).

- 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 field. If a gateway is not being used, then leave the **Gateway** field empty.
- 4. Click No beside Act as Router.
- 5. Leave the fields associated with Static Routes blank.
- 6. In the fields associated with **Local Routes**, 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 Application Server", on page 31).

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

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

#### **Configuring the Ethernet Interface**

The iControl 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.

#### IMPORTANT: Ethernet Port Labels on the R210 and R310 Application Servers

If your Application Server is a Dell PowerEdge R210 or R310, please read the section regarding Ethernet port labels (see page 22).

**Note:** You must use **eth0** as your main network interface. The other Ethernet port (**eth1**) is also configurable, but is intended for specialized use, such as connecting 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.

#### REQUIREMENT

Before beginning this procedure, make sure you have navigated to the Network Configuration page of Webmin (see 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 is booted.

Network Interfaces						
Add a new interfa	ce. Add a new address	range.	Netmask	Activate at boot?		
eth0	Ethernet	10.6.6.252	255.255.0.0	Yes		
eth1	Ethernet	192.168.3.6	255.255.0.0	No		
lo	Loopback	127.0.0.1	255.0.0.0	Yes		
Add a new interfa	ce. Add a new address	s range.				

2. Click eth0 in the Name column.

The Edit Bootup Interface page appears.

Edit B	ootup Inte	erface					
Boot Time	e Interface Param	eters					
Name		IP Address	From DHCP	From BOOTP	<ul> <li>Static</li> </ul>	10.6.6.252	
Netmask	255.255.0.0	Broadcast	10.6.255.255				
мти		Activate at boot?	🗿 Yes 💿 No				
		Virtual interfaces	0 (Add virtual int	erface)			
Save						Dele	ete

**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. Select Static.

4. In the field to the right of the **Static** option button, type the fixed IP address you would like to use for this iControl Application Server.

**IMPORTANT:** 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 27).

**Note:** 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.

5. Type addresses in the **Netmask** and **Broadcast** fields 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 a network administrator.

- 6. Leave the **MTU** field blank.
- 7. Select Yes next to Activate at boot.

**Note:** If you do not select **Yes**, the **eth0** interface resets to its previous values the next time the system restarts.

#### 8. 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 Application Server", 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.
- 9. Return to the Network Configuration page by clicking the Return arrow at the bottom of the Network Interfaces page.

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

#### **Restarting the Application Server**

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

#### REQUIREMENTS

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

- You are logged on to iControl Webmin (see page 23).
- You have performed step 1 through step 4 of "Configuring the Network", on page 24.

#### To restart the Application Server

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



The Bootup and Shutdown page appears.

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

2. At the bottom of the Bootup and Shutdown page, click Reboot System.

	xinetd	Yes		machanisms, available bas can be starte	
	ypbind	No		This is domaii but it s	a dae n. It mu should
	/etc/rc.d/rc.local	Yes			
S	Start Selected	Stop S	elected		Start
	Start Now & On	Boot		Disable	Now &
Crea	ate a new bootup	and shut	Clic Clic Clic the	ction. ck this l e. This action	button will cau s in the
	<b>▼</b> Reboot System	Ci	lick on t e discor	his but	ton to i d and a
	Shutdown System	n Ci al	lick on t I users	this but discon	ton to nected

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

3. Disconnect the client PC that was used to configure the Application Server. Remember to restore the previous network settings on the PC (see "Preparing a PC for Configuring the

#### Application Server", on page 15).

 Connect the Application Server to its designated network. Use a standard Ethernet cable plugged into the Application Server's **eth0** port (see "Installing the iControl Application Server", on page 13).

#### IMPORTANT: Ethernet Port Labels on the R210 and R310 Application Servers

If your Application Server is a Dell PowerEdge R210 or R310, please read the section regarding Ethernet port labels (see page 22).

# **Task 4: Configuring Client Workstations**

Any Linux or Windows workstation with access to an Application Server can be used to operate iControl, without the need for special client-side software. There are, however, two considerations in preparing them to work with iControl: the version of Java installed on the workstation, and its local DNS settings.

#### Installing Java

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

#### To install the Java 2 Runtime Environment on your PC

- 1. Click Useful downloads on the iControl Startup page.
- 2. Click **JRE for Windows**. When prompted, save the download. The filename should be similar to jre-1\_5\_07-windows-i586-p.exe.
- 3. Open the downloaded EXE file. The installation process takes several seconds. Once completed, a confirmation message appears.

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

# **Configuring DNS Settings**

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

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

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

#### To configure DNS settings

- 1. On the client PC, open the hosts file (no extension) in a text editor. In Windows XP, the hosts file is located in C:\WINDOWS\system32\drivers\etc. In Linux, the hosts file is located in /etc
- 2. For each Application Server and Allégro-1 that the PC will be accessing, add a line of the form:

AAA.BB.CC.DDHostName.yourDomain.com

where AAA.BBB.CC.DD is the IP address of the Application Server or Allégro-1.



3. Save and close the hosts file.

# Connecting to the Application Server

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

#### To connect to the Application Server

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

ping AAA.BBB.CCC.DDD

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

<sup>1.</sup> Return to the Network Configuration page by clicking the Return arrow at the bottom of the Routing and Gateways page.

A small window should briefly appear with a message similar to the following: Reply from AAA.BBB.CCC.DDD: bytes=32 time<1ms TTL=62

# Task 5: Configuring the Application Server on the Network

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

# **Configuring Lookup Services**

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

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

#### **Enabling or Disabling the Lookup Service**

#### REQUIREMENTS

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

- You have opened iControl.
- You have logged onto Webmin (see page 23).

#### To turn a lookup service on or off

- On the Webmin main page, click Miranda iControl Management Tool. The iControl Management Tools page appears.
- Click the icon beside iControl services monitoring and configuration tool. The Miranda Monitoring page appears.
- 3. Click Configure RMID.

iControl Services Gateway	Control Services Gateway Server for third-party API to interface with any iCont card services. Required for RCP-100 client and to change line scope from iControl We player				
Daemon Health Monitor	Process that monitors and restarts daemon processes				
Number of Densite Managers : 1 💽 Apply					
(Click here) to Take a look at the system's configuration					
Configure port	Configure port				

The RMID page appears. By default, the Lookup Service is configured to start automatically when the RMI (Remote Method Invocation) daemon is activated.

RMID
RMID configuration
Select if you want the Lookup Service to start after the RMI Daemon.
● Start Lookup Service with RMID
Do not start Lookup Service with RMID
Accept

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

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

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

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

#### **Opening the iControl Lookup Locations Page**

The need for specifying Lookup Locations depends on several factors. In general, we recommend the following:

- If an Application Server is **not** running a lookup service, you should type the locations of all Application Servers running the lookup service on its own subnet, as well as those on external subnets.
- If an Application Server **is** running a lookup service, you should type the locations of all Application Servers running the lookup service on external subnets.

#### See also

For more information, see the "Lookup Services" section of the "Getting Started" chapter in the *iControl User Guide* (**M226-9900-278**).

#### REQUIREMENT

Before beginning this procedure, make sure you have opened iControl.

#### To open the iControl Lookup locations page

1. On the iControl main page, click **System tools**.



The System tools page appears.

2. Click Edit service locations.



# The iControl Lookup locations page appears.

Service and alarm discovery
If you would like your client applications such as iC Navigator and iC Web to discover services and alarms originating from Application Servers not belonging to your client PC's subnet, include the IP addresses of each Application Server hosting the lookup services where these services are registered.
- Details/Examples
IP address:
Name (optional):
Add lookup
Current lookup entries are:
IP address Name
10.6.6.68 m68 Delete
Alarm publication
For services such as Densite Managers to publish their alarms in other GSMs that are <u>NOT</u> located in the same subnet, include the IP addresses of the Analyzation Servers begins the lockup services where these GSMs are registered.
Details/Examples
IP address:
Name (optional):
Add lookup
Current lookup entries are:
IP address Name
10.4.4.50 m50 Delete
NOTE: You must restart iControl to apply GSM location changes.
Click here to access the Administration web page in order to restart (Control.
Dack to system tools page

#### **Specifying Service and Alarm Discovery Locations**

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

Service and alarm discovery				
If you would like your client applica Application Servers not belonging to lookup services where these service	tions such as iC Navi your client PC's subr s are registered.	igator and iC net, include th	Web to discover set e IP addresses of ea	vices and alarms originating from ach Application Server hosting the
• Details/Examples				
	IP address:		$\neg$	
Na	ime (optional):			
	A	dd lookup		
	Current I	lookup entries	are:	
	IP address	Name		
	106620	m20	Delete	
	10.0.0.20			
	10.6.6.68	m68	Delete	

#### REQUIREMENT

Before performing any of the following tasks, make sure you have opened the iControl Lookup locations page (see page 36).

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

#### **Specifying Alarm Publication Lookup Locations**

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

If, however, you wish to have these services connect to GSMs running on Application Servers on other subnets, you must explicitly specify the GSM locations. You do this by typing the

IP address of the target Application Server (on the remote subnet) in the iControl Lookup locations page of the Application Server running the Densité, Imagestore, or other service on the local subnet.

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

#### **Adding an Alarm Publication Lookup Location**

#### REQUIREMENT

Before beginning this procedure, make sure you have opened the iControl Lookup locations page for the Application Server that is running the Densité, Imagestore, or other service you wish to publish to remote GSMs (see page 36).

#### To add an Alarm publication lookup location

1. On the iControl Lookup locations page, type one of the following:

- the IP address of an Application Server on a remote subnet that is running a GSM
- the IP address of an Application Server on a remote subnet that is running a lookup service

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

#### 2. Click Add lookup.

The address appears in the Alarm publication lookup table.



3. Restart the specific service (e.g. Densité Manager) that you wish to publish to the remote GSM, or restart iControl to publish all services to the remote GSM (see "Starting & Stopping iControl Services", on page 666).

## **Deleting an Alarm Publication Lookup Location Entry**

#### REQUIREMENT

Before beginning this procedure, make sure you have opened the iControl Lookup locations page on the Application Server hosting the Densité or ImageStore services you no longer wish to be visible outside the subnet (see page 36).

#### To delete an Alarm publication lookup location entry

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

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

## Configuring the iControl Services Gateway

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

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

**Note:** The iControl Services Gateway is not related to the Network Gateway function, although the latter may need to be active to allow the iControl Services Gateway to operate between different subnets (see "Specifying a Network Gateway", on page 28).

#### REQUIREMENT

Before beginning this procedure, make sure you have logged on to iControl Webmin (see page 23).

#### To activate the iControl Services Gateway

- From the Webmin main page, click Miranda iControl Management Tool. The Miranda Setup page appears.
- 2. Click the icon beside iControl services monitoring and configuration tool.



The Miranda Monitoring page appears.

All iControl services available on the current Application Server are listed in a table, one service per row. A row's background color indicates the service state:

- Green indicates an active service
- Blue indicates an inactive service
- Red indicates a problem with the service.
- 3. On the Miranda Monitoring page, locate the **iControl Services Gateway** row in the list of services on the Miranda Monitoring page.

Service Name	Description	Start time	AutoStart	Start/Stop/Restart	Log
Audio/Video Fingerprint Analyzer	Provides support for distributed and multi-point content fingerprint analysis (e.g. lip-sync detection)	Mon Jun 21 10:49:25 2010	Z Auto	•/•/•	Show log
Bridgetech VBC service	Start Bridgetech VBC service.	Stopped	🗖 Auto	• / • / •	Show log
	CDMP Service . Supports multiple instances for load balancing	Stopped	Auto	•/•/•	Show log
Densite	Densite Manager , Module which starts and stops densite communicators. Supports multiple instances for load	Mon Jun 21 10:49:23 2010	🗹 Auto	•/.•/.•	Show log
Virtual Service	building virtual panels such as procamps	Stopped	🗖 Auto	● / ● / ●	Show log
iControl Services Gateway	IControl Services Gateway Server for third-party API to interface with any IControl card services. Required for RCP-100 client and to change line scope from IControl Web player	Stopped	🗖 Auto	• / • / •	Show log
Daemon Health Monitor	Process that monitors and restarts daemon processes	N/A	N/A	N/A	Show Log
Apply	Reset	iCont	rol Stop	iControl Start	
Number of Densi	te Managers : 1 - Apply				
i his is used for l	oad balancing in large systems. W	re recommend a	maximum of	150 streams per De	nsite Manager
	ake a look at the evetemic configu	ration			

4. In the Auto Start column, select the Auto check box.

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

- 5. In the Start/Stop/Restart column, click the left-most button (corresponding to Start).
- 6. Click Apply.

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

# Task 6: Configuring GPI Outputs on a GPI-1501

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

#### REQUIREMENT

Before beginning this procedure, make sure you have opened iC Navigator.

#### To configure GPI outputs on a GPI-1501

1. In iC Navigator, on the View menu, click General status managers.



The General Satus Managers window appears.

ᇌ General Status Manag	ers
CHEapps3/10.10.100.10	Main       Admin         Alarm browser       -         IControl alarms       -         Cheyenne       -         CenericV2       -         Control alarms       -         Incident templates       -         Incident templates       -         Indent emplates       -         NMP       -         Virtual_Test       -         Virtual/Alarms       -
	Edit plug-in Remove plug-in Filtered view Show status details URI Create new alarm provider  Kaleido-K2 Kaleido-K2 Kaleido-Alto Kaleido-Alto Kaleido-Alto Kaleido-Alto

2. Select one of the GSMs from the list in the left pane of the window.

The Alarm Browser (under the **Main** tab) displays the devices and services associated with the selected GSM in a hierarchy of folders, subfolders, and alarms.

**Note:** You can, alternatively, open the Alarm Browser for a specific GSM by doubleclicking its name in the iC Navigator window. This opens the Alarm Browser in a smaller window.

👬 Miranda iControl Navigator - Access control	disabled	
<u>F</u> ile <u>V</u> iew <u>D</u> iscovery <u>T</u> ools <u>H</u> elp		
Specific location 🦻 All locations 🔳	Event log view	er
Label*	Short label*	
💷 🗁 Logical view		
CompositeServices		
DCE2		
DECs		
🗖 🗁 Managers		
AudioA/ideo Fingerprint Analyze		Audi
CHEanos3/10.10.100.10		GSM
DensiteManager_CHEapps3	DensiteM	Den
📃 👘 🖵 Virtual Service Manager_CHEar	Virtual	Virtu
UAPs		

Main       Admin         Alarm browser       Alarm browser <ul> <li>Control alarms</li> <li>Cheyenne</li> <li>GenericV2</li> <li>GenericV2</li> <li>GenericV2</li> <li>Control Web</li> <li>Incident Templates</li> <li>Incident Templates</li> <li>Incident Templates</li> <li>Incident Templates</li> <li>Incident Templates</li> <li>Virtual_Test</li> <li>Virtual_Test</li> <li>VirtualAlarms</li> </ul> <li>Create new alarm provider</li> <li> <ul> <li>Witual alarm</li> <li>Kaleido-K2</li> <li>Kaleido-X</li> <li>Kaleido-Alto</li> <li>Application server health monitoring</li> </ul> </li>	CHEapps3/10.10.100.10 [GSM]
Alarm browser Control alarms Control alarms Cheyenne Cheyenne Cheyenne Cheyenne Cheyenne Cheyenne ControlWeb Control	Main Admin
Control alarms Cheyenne GenericV2 GSM Health monitoring Icontrol Web IncidentTemplates IncidentTemplates IncidentTemplates IncidentTemplates IncidentTemplates IRManager Router SNMP Virtual_Test Virtual_Test Virtual_Test Filtered view Show status details URI Find Create new alarm provider Kaleido-K2 Kaleido-X Kaleido-Atto Kaleido-Atto Kaleido-Atto Kaleido-Atto	Alarm browser
••       Cheyenne         ••       GenericV2         ••       GenericV2         ••       Ficontrol         ••       Iccontrol         ••       Iccontrol Web         ••       IncidentTemplates         ••       IncidentTemplates         ••       IncidentTemplates         ••       IncidentTemplates         ••       Incident templates         ••       Null         ••       Valarms         ••       Virtual_Test         ••       Virtual alarm         •*       Kaleido-K2         •*       Kaleido-X         •*       Kaleido-Atto         •*       Application server health monitoring	😂 iControl alarms
Generic/2     GSM     GSM     Generic/2     GSM     GSM     Generic/2     GSM     GSM     Generic/2     GSM     Generic/2     GSM     Generic/2     Gen	©- Cheyenne
Health monitoring Icontrol Icontrol Icontrol Incident templates Incident templates Incident templates IRManager IRManager IRManager IRManager IRManager IRManager IRManager IRManager IRManager Incident templates	Genericv2
iControl iControl iControlWeb IncidentTemplates IncidentTemplates IRManager Router SNMP Viltual_Test Viltual_Test ViltualAlarms Edit plugmee: Remove plugmee: Filtered view Show status details URI Find Create new alarm provider Kaleido-K2 Kaleido-K2 Kaleido-K2 Kaleido-Atto Mew	🗣 🗀 Health monitoring
Incident Templates Incident Templates Incident Templates IRManager Router SNMP Viltual_Test Viltual_Test ViltualAlarms Edit plughnee Remove plughnee Filtered view Show status details URI Find Create new alarm provider Kaleido-K2 Kaleido-K2 Kaleido-Alto Application server health monitoring New	
	or incontrolived or incidentTemplates
● ■ IRManager         ● ■ Router         ● ■ Router         ● ■ SMMP         ● ■ Valarms         ● ■ Virtual_Test         ● ■ Virtual_Test         ● ■ Virtual_Test         ● ■ Virtual_Test         ■ ■ Provider         Image: Virtual_Test         ■ ■ Now status details         URI       Find         Create new alarm provider         ■ ● ● Virtual_alarm         ● ● Note	👁 💼 Incident templates
Koller	Concerning and the second seco
Image: Second secon	©-☐ SNMP
Image: Second	O- C VAlarms
Edit plug-in Remove plug-in Filtered view Show status details URI Find Create new alarm provider *** Virtual alarm *** Kaleido-K2 *** Kaleido-X *** Kaleido-Atto *** Kaleido-Atto	on- Virtual_Test on- ProvidualAlarms
URI Find Create new alarm provider *** Virtual alarm *** Kaleido-K2 *** Kaleido-Atto *** Kaleido-Atto	
URI Find Create new alarm provider We Virtual alarm We Kaleido-K2 We Kaleido-X We Kaleido-Alto We Kaleido-Alto We Application server health monitoring	Edit plug-in Remove plug-in Filtered view
Create new alarm provider	URI Find
Image: Weight of the second secon	Create new alarm provider
Mer Kaleido-K2       Image: Constraint of the second	🐠 Virtual alarm
Mer Kaleido-X     New       Mer Kaleido-Alto     New       Mer Application server health monitoring     ▼	🔆 Kaleido-K2
Me Kaleido-Alto Me Application server health monitoring	Mew
	Me Application conver bealth manifering

3. Use the vertical scroll bar to find the alarm for which you would like to trigger a GPI output on a GPI-1501 card.

📊 General Status Managers			
CentralAppServer/10.10.10.13 appServerAPPS/10.12.10.10 Alarm browser DEC-1021 (KxRouterControl_Uideo_1S_Densite_SLOT_12_47) DEC-1023 (KxRouterControl_B5-UtilD3_Densite_SLOT_682) DEC-1023 (KxRouterControl_B5-UtilD3_Densite_SLOT_682) DEC-1023 (KxRouterControl_B5-UtilD3_Densite_SLOT_19_48) CentralAppServer_PietroDensite_Densite_SLOT_19_48) DEC-1821Central (CentralAppServer_PietroDensite_SLOT_14_105) Dec-1821Central (CentralAppServer_NTSCfeeds_Densite_SLOT_18_66) Dec-1021 (KxRouterControl_B5-UtilD3_Densite_SLOT_19_48) Dec-1021 (KxRouterControl_B5-UtilD3_Densite_SLOT_19_48) Dec-1021 (CentralAppServer_PietroDensite_SLOT_19_48) Dec-1021 (CentralAppServer_NTSCfeeds_Densite_SLOT_18_66) Dec-1021 (CentralAppServer_NTSCfeeds_Densite_SLOT_18_66) Dec-102 (CentralAppServer_NTSCfeeds_Densite_SLOT_18_66) Dec-102 (CentralAppServer_NTSCfeeds_Densite_SLOT_18_66) Dec-102 (CentralAppServer_NTSCfeeds_Densite_SLOT_18_66) Dec-102 (Centra			
	Edit plug-in Remove plug-in Filtered view Show status details		
	Create new alarm provider		
	Image: Maleido X     Image: Maleido X       Image: Method Relation     Image: Method Relation       Image: Method Relation     Imag		

4. Double-click the alarm.

The Alarm Properties window appears.

👬 Alarm Proper	ties		
Current status:	Show status details		
Name:	Input 2 Selected		
URI:	CentralAppServer_NTSCfeeds_Densite_SLOT_18_66@dlnput2Selected		
Path:	iControl/HCO-1821Central (CentralAppServer_NTSCfeeds_Densite_SLOT_18_66)		
Device URI:	CentralAppServer_NTSCfeeds_Densite_SLOT_18_66		
Device class:	HC0-1821		
Туре:	☑ Status  ☐ Text  ☐ Not logged  ☐ Logged only on status change  ☐ Incident		
Actions			
————— Global actions —————      SQL event log (local)			
Add	Add global Remove Edit Refresh		
	Edit plug-in		
	ОК		

5. Click Add.

The **New Action** window appears.

- 6. Click GPI-1501 relay to select it.
- 7. Click New.



The GPI-1501 Relay Configurator window appears.

ᇌ GPI 1	i01 Relay Configurator
GPI Card	Select Card 🗸 🗸
GPI IO0	State 💌
GPI IO1	State 💌
GPI IO2	State 👻
GPI 103	State 💌
GPI IO4	State 🗸
GPI 105	State 👻
GPI IO6	State 👻
GPI 107	State 💌
ОК	Cancel

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



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

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

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

🙀 GPI 1501 Relay Configurator			
GPI Card	CentralAp	oServer_PietroDensite_Densite_SLOT_14_105 ▼	
GPI IO1	State		
GPI IO2	State		
GPI IO3	State		
GPI IO4	State		
GPI IO5	State		
GPI IO6	State		
GPI 107	State		
GPI IO8	State	<b>~</b>	
ОК	Pressed		
	Released State		

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

- Pressed = high
- Released = low

#### Notes

- If you leave it at State, the GPI is not programmed to respond to this alarm, and can be assigned to a different alarm.
- You can use the labels to identify the alarm source once it is set.
- 10. Click OK when done, or Cancel to leave the status unchanged

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

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

#### See also

For more information, see the *Densité Series GPI-1501 General Purpose Interface I/O Module Guide to Installation and Operation* (**M906-9900-100**).

# Task 7: Connecting & Configuring Devices

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

# **Configuring Serial Ports**

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

Port Designation		Protocol
ттү	СОМ	
RO	3	RS-422
R1	4	
R2	5	
R3	6	
R4	7	
R5	8	
R6	9	
R7	10	

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



Dell PowerEdge R310 with optional 8-port serial expansion card



RocketPort 8-port serial breakout box

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

Configuring Serial Ports for a Specific Application Server

#### REQUIREMENTS

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

- You have opened iControl.
- You are logged on to iControl Webmin (see page 23).

#### To configure serial ports for an Application Server

- On iControl's Webmin page, click Miranda iControl Management Tool. The Miranda Setup page appears.
- 2. Click the icon beside iControl services monitoring and configuration tool.



The Miranda Monitoring page appears.

3. Click **Configure Ports**.



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

iCon	iControl port configuration page			
Seria	al ports configuration			
Port	Assignment			
ttyR0	None 🗸			
ttyR1	None 🗸			
ttyR2	None			
ttyR3	None -			
ttyR4	None Imaging Connection Manager			
ttyR5	Tandberg Alteia			
ttyR6	None 🗸			
ttyR7	None 🗸			
tty S0	None			
ttyS1	None			
Accep	t			

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

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

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

5. When you have finished assigning ports, click Accept.

The Miranda Monitoring page reappears, with new rows in the list of services for each of the newly assigned ports.

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

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

Existing serial port assignmer	nt Inactive	e service (blue)	Active service (gre	en)
Imaging Connection Manager ttyR1	communicator. Module which finds imaging services ar frames	nd Stopped		🗹 Auto
RMI daemon	RMI Server Daemon	Wed Jur	6 14:02:14 2007	Auto
Router Manager Service	Router Manager Service is responsible for all routers connected to a local machine	Wed Jur		🗹 Auto
Tandberg Alteia	Alteia	Wed Jur	6 14:02:19 2007	Auto
VTR Control Module ttyR2	VTR. Module which is used to control a VTR	Stopped		🗹 Auto
VTR Control Module ttyR3	VTR. Module which is used to control a VTR	Stopped		🗹 Auto
Daemon Health Monitor	Process that monitors and restarts daemon processe	s 🔤	N/A	N/A
	Apply Reset	iCon	trol Stop iControl Start	
New serial port Click to	apply any changes,	Click <b>Stop</b> , the	Start to activate r	new serial

New rows in list on iControl Services Monitoring and Configuration Tool page

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

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

- 7. In the **Start/Stop/Restart** column, click **Start** for each of the services corresponding to the newly assigned serial ports.
- 8. Click Apply.

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

# Task 8: Configuring System Time

Application Servers have both a *system time* and *hardware time*. The system time reflects the time set in the operating system. The hardware time reflects the time set in the Application Server's own BIOS.

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

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

#### REQUIREMENTS

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

- The remote Application Server whose system time you would like to synchronize to, is online and functioning.
- On the Application Server whose system time you would like to configure, you are logged into iControl and you have navigated to the System Time page.

#### To synchronize an Application Server's system time to that of another server

1. On the System Time page in iControl, in the **Time Server** area, type the host name or IP address of the remote NTP server in the **Timeserver hostnames or addresses** box.

Save				
Time Server				
Timeserver hostnames or address	es	10.6.6.60		
Synchronize on schedule?		<ul> <li>Set hardware time</li> <li>No</li> <li>Yes, at time</li> </ul>	e too les below	
Simple schedule Hourly	🗕 🔍 Tir	mes and dates selected	below	
Minutes	Hours	Days	Months	Week
<ul> <li>All</li> <li>Selected</li> <li>12 ^ 24 ^ 36 ^ 48 ^</li> <li>13 25 37 49</li> </ul>	<ul> <li>All</li> <li>Selected</li> <li>12 ^ 13</li> </ul>	All     Selected     All     Selected     All     A	<ul> <li>All</li> <li>Selected</li> <li>January</li> <li>February</li> </ul>	<ul> <li>All</li> <li>Se</li> <li>Sund</li> <li>Mond</li> </ul>

2. Select Set hardware time too.

**Note:** This check box should always be selected as Miranda recommends pegging hardware time to system time.



3. If you would like to synchronize just this one time and **NOT** perform scheduled synchronization sessions in future, select **No** next to **Synchronize on schedule**, and then proceed to step 7.



4. If you would like to schedule recurring synchronization sessions, select **Yes** next to **Synchronize on schedule**.



- 5. If you would like to configure a simple recurring schedule, perform the following sub-steps:
  - a) Select **Simple schedule**.

Synchronize on sche	ichronize on schedule?		
Simple schedule .	Daily (at midnight)	Times	
Minutes	Hourly Daily (at midnight) Weekly (on Sunday) Monthly (on the 1st) Yearly (on 1st Jan) When system boots	Da	

- b) In the list, select the desired synchronization frequency.
- 6. If you would like to configure specific times and dates for synchronizing, perform the following sub-steps:
  - a) Select Times and dates selected below.

	Synchronize on schedule?		<ul> <li>No O Yes, at times below</li> </ul>	
	Minutes	Hours	Days	Months
	O All	IA O	II AII	O All

b) In the **Minutes** area, select specific minutes (in conjunction with the **Ctrl** key) by first selecting **Selected**, or else select **All** to choose every minute.

Synchronize on schedule?	No O Yes, at tim	es below		
Simple schedule Hourly				
Minutes	Hours Days	Months Weekdays		
<ul> <li>All</li> <li>Selected</li> </ul>	<ul> <li>All</li> <li>Selected</li> <li>Selected</li> </ul>	All     All     Selected		
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	January A February Monday Monday Tuesday March Tuesday Monday Tuesday May Thursday June Friday July Saturday * August September October November December *		
Note: Ctrl-click (or command-click on the Mac) to select and de-select minutes, hours, days and months. Sync and Apply				

- c) In the **Hours** area, select specific hours or all hours, as required.
- d) In the **Days** area, select specific days or all days, as required.
- e) In the **Months** area, select specific months or all months, as required.

- f) In the Weekdays area, select specific days or all days, as required.
- 7. Click Sync and Apply.



# **Contact Us!**



# Miranda Technical Support

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

#### Americas

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

#### Europe, Middle East, Africa, UK

 Office hours:
 9:00 a.m. - 6:00 p.m. (GMT)

 Telephone:
 + 44 118 952 3444

 Fax:
 + 44 118 952 3401

 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

#### Office hours:

Asia

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

#### China

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

#### **EMERGENCY After Hours (Global)**

 Toll Free:
 1-800-224-7882 (US and Canada)

 Telephone:
 +1 514 333 1772

# **Corporate Head Office**

Miranda Technologies 3499 Douglas-B.-Floreani, St-Laurent, Québec, Canada H4S 2C6

Telephone:	+514 333 1772
Fax:	+514 333 9828
Web:	www.miranda.com