

# Embedded Web Server (EWS)

The embedded web server (EWS) is a factory installed option for the IGC100. The EWS provides an ethernet connection between the IGC100 and a network. The EWS allows monitoring and control of the IGC100 (and vacuum system) from a local network or the world-wide web.

The EWS allows you to

- Monitor and control the IGC100 from virtually anywhere in the world.
- View vacuum system data using a standard web browser.
- Get log data from the IGC100 without writing a custom program.

## In This Application Note

<b>EWS Quick Start</b>	<b>3</b>	Process History	21
Connect the IGC100 to Your Network	3	Get Datalog	22
Set the Network Addresses	3	Get Userlog	23
Set the Security Level	3	E-Mail Status	23
Enable the EWS	3	Controlling the IGC100	24
Access the Web Page	4	Request Control	24
		Release Control	24
<b>Installing the EWS</b>	<b>5</b>	E-Mail Notices	24
Network Administration Concerns	5	Ion Gauge Power	27
Static IP	5	Change Relays	28
Port Number	6	<b>Networking Terms</b>	<b>29</b>
Setting Network Addresses	6		
Enable the EWS	7		
System Name	7		
MAC Address	8		
Choosing a Network Configuration	9		
Crossover Cable Configuration	9		
Internal LAN Configuration	10		
Conventional LAN Configuration	11		
Outside Firewall Configuration	12		
Testing with a Crossover Cable	13		
Testing Within a Network	14		
Configuring EWS Security	15		
Web Server Enable	15		
Web Control Enable	15		
Security Type	16		
IP Checking	16		
IP and Password Checking	16		
Password Checking Only	17		
<b>Using the EWS</b>	<b>18</b>		
Bookmarking the IGC100	19		
Monitoring the IGC100	19		
Get Readings	19		
Auto Monitor	19		



---

# EWS Quick Start

If you are comfortable with networking and wish to get your EWS up and going as quickly as possible, use the Quick Start instructions here. Please read the rest of this application note for a more complete description of the EWS features and capabilities.

---

## Connect the IGC100 to Your Network

### Warning!

- Connecting your vacuum system to the world-wide-web can expose it to unauthorized access, resulting in harm to personnel as well as equipment.
- Network security is a serious matter. Consult your network administrator for more information about using web-enabled instruments in your lab.

Use a CAT5 ethernet cable to connect your hub or switch to the ethernet connector on the back of the IGC100 (with EWS installed). *Do not use a crossover cable.*

Bring up the Web setup menu by pressing the [Menu] QuickKey (in the Pressure Display), choosing [Remote] and then [Web].

---

## Set the Network Addresses

For full use of the EWS, you will need a static IP (Internet Protocol) address, subnet mask, DNS (Domain Name Server) address, and gateway address. See your network administrator to obtain addresses appropriate for your network environment. If you already know the IP address you will be using, you may be able to find your subnet mask and gateway by typing "ipconfig" from your workstation's command line prompt.

Enter these values in the Main/Remote/Web menu of the IGC100.

---

## Set the Security Level

To quickly allow access to all EWS features, go to the Main/Remote/Web/Control submenu and set Web Control to Enabled and Security Type to Password. The default password is "igc100".

Read the section 'Configuring EWS Security' later in this application note for a complete description of EWS security features.

---

## Enable the EWS

Return to Main/Remote/Web and set Web Server to Enabled. Your EWS stores the network addresses into non-volatile memory, then gathers data on your IGC100 setup (gauge and relay descriptions, etc.). Allow the EWS about 30 seconds before continuing.

To make sure the EWS is functioning, touch the [Web Queue] button. If commands are streaming across the display, the EWS is communicating with the IGC100.

## Access the Web Page

Start your web browser and in the location (URL) bar, type the IP address you assigned to the EWS. Make sure JavaScript is not disabled in your browser. You should see a web page similar to below. Relay status is displayed only if Option 03 (Process Control) is installed in the IGC100.

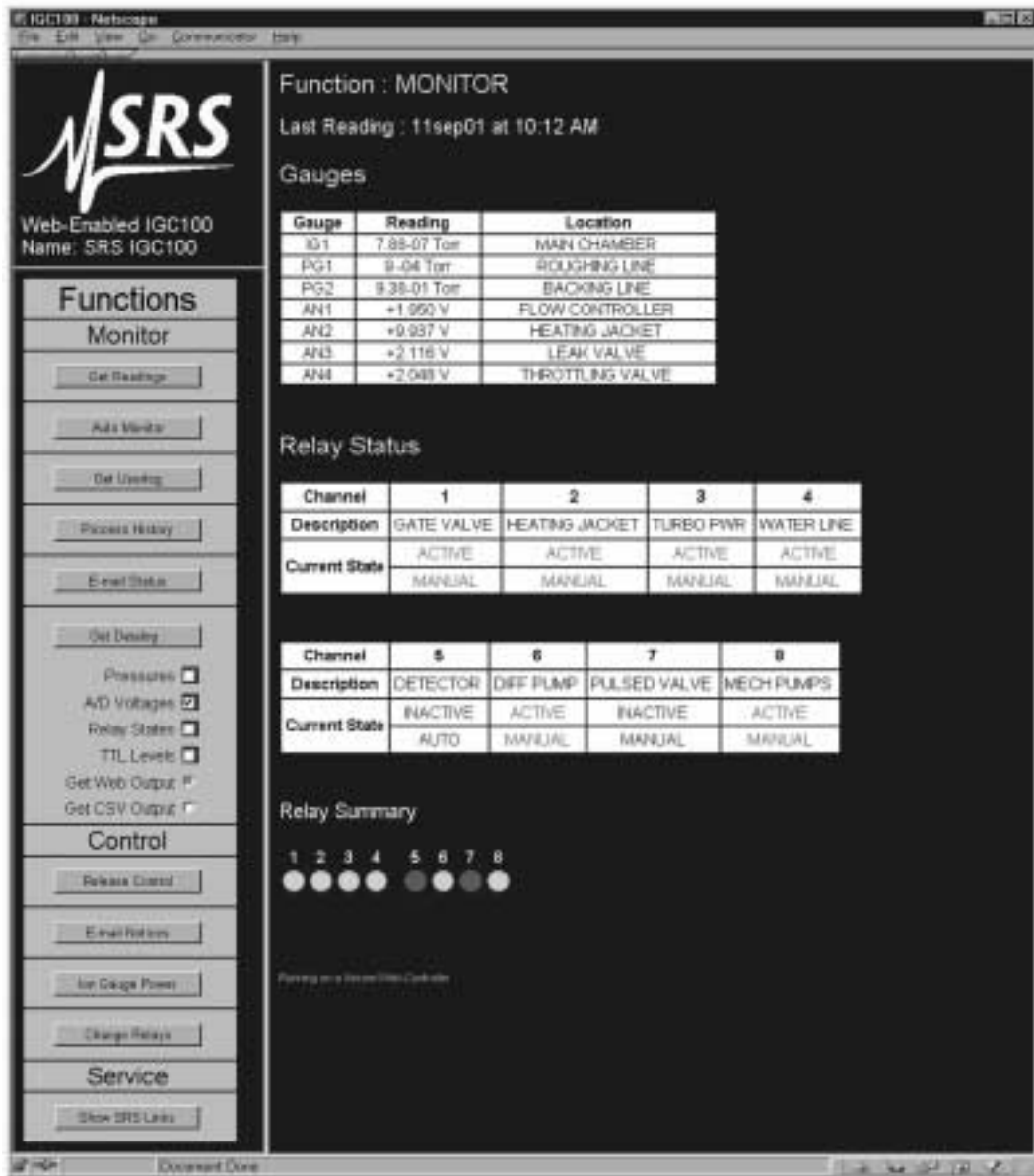


Figure 8-1. EWS web page.

---

# Installing the EWS

This section covers the network installation and configuration of the Embedded Web Server option. While this option adds powerful functionality to the IGC100, *connecting your vacuum system to the world-wide-web can expose it to unauthorized access, resulting in harm to personnel as well as equipment.*

## **Warning!**

Network security is a serious matter. Consult your network administrator for more information about using web-enabled instruments in your lab.

---

## Network Administration Concerns

Your network administrator has a difficult job. In addition to making sure your network is always running smoothly, she also needs to keep track of which IP addresses are assigned to which machines. This prevents IP address collisions (where more than one computer has the same IP address), as well as maintains the security of the network.

Your administrator may have a limited number of free IP addresses, and may show concern about having an instrument on the network in the first place.

Some of the first questions she may ask include:

- Why does an instrument need an IP address?
- Why does it need a static IP address?
- What happens if everyone in the department wants instruments with IP addresses?
- What is the MAC address for this instrument?
- What kind of security measures are in place?

These are all very valid concerns. You will need to explain what you want to do, and allow your administrator enough leeway to accomplish your goals while still satisfying theirs. Some of the information in this application note may help you both.

---

## Static IP

The reason your instrument needs a static IP address is because it is a *server*. You need your server to be at the *same* address all the time, so you always know where to point your browser. The server does not use a conventional file system. It is likely that once your instrument is running, it will remain on 24 hours a day, 7 days a week. This makes using a dynamic IP address (one that changes with each power up sequence) somewhat infeasible.

## Port Number

The default port is 80 and should **NOT** be changed except in the following situations.

1. If IP addresses are scarce in your network environment, consider using a network address translation (NAT) router. With such a device, several IGC100's can 'share' a single IP address. Each IGC100 is assigned a 'fictitious' IP address and the router presents a single IP address to the rest of the world. In this case, all of the IGC100's will appear at the same IP address to the outside world (they will have different IP addresses on the local network). Each IGC100 needs to be on a different port and the router must be configured to forward port requests to the correct IGC100. From the outside, each IGC100 is accessed at its own port number (but the same IP address).
2. If you are experiencing attacks on port 80 that block access to the IGC100. In this case, change the port to something else (like 8080). You will need to specify this port in your browser address window as 208.123.123.32:8080 where 208.123.123.32 is the IP address of the IGC100 and 8080 is the port number.

For more information about NAT routers and ports, see your network administrator.

## Setting Network Addresses

To enter network addresses into the IGC100, press the [Menu] QuickKey from the Pressure Display, then choose [Remote] from the Main Menu. Finally, choose [Web] in the Remote Menu.

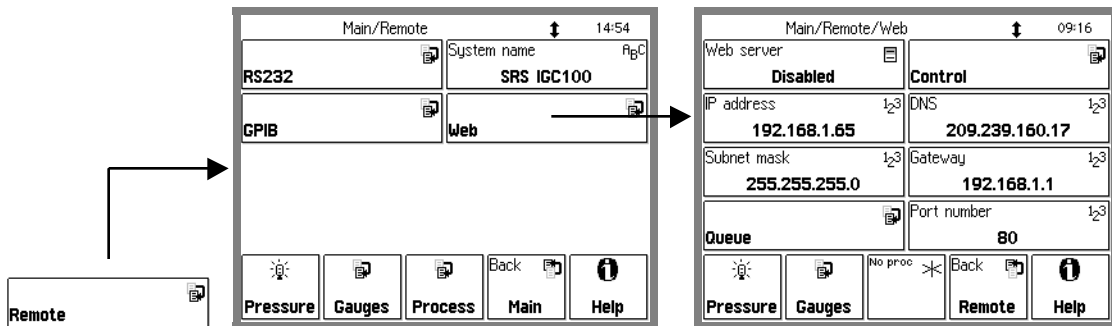


Figure 8-2. Getting to the Web menu.

In order to use the EWS option, you will need to have a connection to the internet and some information about your network environment.

The best source of information about your network environment is your network administrator. Here is a list of information you will need from that person:

- 1) An IP (Internet Protocol) address for the instrument
- 2) The IP address of a domain name server (DNS)
- 3) The IP address of the gateway
- 4) The IP address of a simple mail transfer protocol (SMTP) server
- 5) The Subnet mask

An IP address is made up of four bytes. It is often expressed as a set of three digit numbers separated by a '.' such as 209.239.160.084. The Internet protocol maps each machine's individual media access control (MAC) address to an IP address. Every page you are served from the world wide web is actually from a machine with a particular IP address.

People have a difficult time remembering and using long strings of numbers, so domain name servers (DNS) are in use. You can think of these machines as a kind of telephone book; they associate a particular IP address (209.239.160.084) with a string of characters (www.thinksrs.com). A DNS is not required to use the EWS, but it can make your life a little easier.

Next we need to consider the gateway. The gateway is simply the machine that connects your network to the outside world. It is the link between two networks, routing data traffic between those networks. For this reason, a gateway is sometimes referred to as a router. Its IP address is required for you to be able to send email from the EWS. If you will not be using the email notices feature of the EWS, and you will always be contacting the EWS from a machine on the same network, this IP address is not required.

A simple mail transfer protocol (SMTP) server often has one purpose in life: to relay email from one machine to another. It follows some simple rules for how the information that makes up the email is exchanged between the machine sending the email and the machine that will relay the message to its destination. This address is not required if you will not be using the email feature of the EWS.

Lastly, the subnet mask is required. In a network, there are quite often sub-networks. The subnet mask is required to let the EWS know which subnet it will be on.

---

## Enable the EWS

After entering network addresses, set the Web Server to Enabled. Your EWS stores the network addresses into non-volatile memory, then gathers data on your IGC100 setup (gauge and relay descriptions, etc.). Allow the EWS about 30 seconds before continuing.

To make sure the EWS is functioning, touch the [Web Queue] button. If commands are streaming across the display, the EWS is communicating with the IGC100.

### Important

Whenever network setup information is changed, you must wait at least 5 seconds for the changes to take effect.

---

## System Name

The System Name (Menu/Remote/System Name) identifies this IGC100 on the web. This is important if your setup includes multiple web-enabled IGC100's. The system name is displayed in the web pages to identify the source of the data.

---

## **MAC Address**

Your administrator may want to know the media access control (MAC) address of your instrument. The MAC is a unique address used at a lower layer of the internet protocol. Each IP address is mapped to a unique MAC address. Administrators often like to know this address as a crosscheck for the IP address (both should be unique). Knowing the MAC address also provides some extra security; if the administrator finds a MAC address that isn't listed in their directory, it could be an unauthorized user. When you put a server on a network, you are essentially inviting people to come and get information. Your administrator will want to make sure that this server doesn't create a security risk for the rest of the network.

To find the MAC address of your IGC100 from a networked PC (which can access the IGC100 via the web) :

Type in the IGC100's IP address (and port if not 80) in your browser's address window. This should bring up the IGC100 web page. Click on "Get Userlog" on the left. This displays the network settings of the IGC100 including its MAC address.



## Choosing a Network Configuration

This section illustrates some possible network configurations for the EWS. This may help in choosing the best network configuration for your EWS.

### Crossover Cable Configuration

This setup uses a crossover ethernet cable that allows the EWS to connect to a single computer without a network. A crossover cable is wired differently than regular network cables. A normal ethernet cable is wired 'straight through' (Tx to Tx, Rx to Rx), while a crossover cable is connects transmit to receive (Tx to Rx, Rx to Tx). *To use this configuration, make sure you use a crossover cable!*

This configuration will **NOT** allow email, use of a DNS, or access from more than one computer. It will **NOT** allow the computer connected to the IGC to connect to the internet. However, it does allow you to use a standard web browser to monitor, control and receive data from the IGC100.

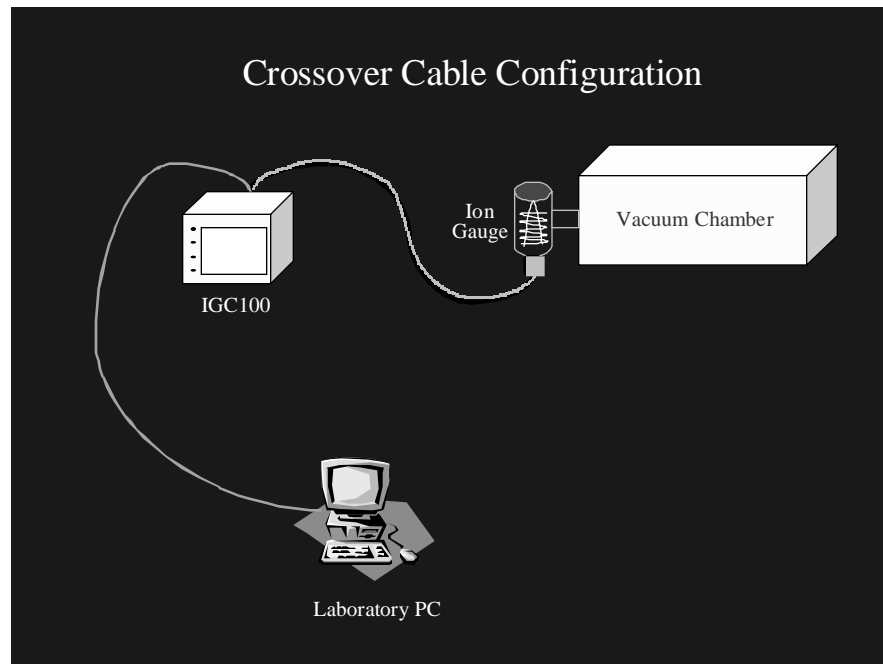


Figure 8-3. Crossover Cable Configuration

This configuration does **NOT** allow access to the IGC100 from the outside world. However, if security is a concern, this limitation is a strong reason for its use. The only security question to ask is "who will have access to this computer?". Since there is no intermediate connection, or dependence on outside hardware, this is also a very reliable connection. Furthermore, since the EWS will not actually be on the internet, you do not need a 'real' IP address. You can simply choose your own IP (on the same subnet as the PC).

## Internal LAN Configuration

You can retain the security of the crossover connection and still allow more than one computer to access the IGC100. An ethernet hub will allow you to make a local area network (LAN) that can use fictitious IP addresses in order to access the instrument (as well as other computers on the LAN). The figure below shows a conceptual diagram of this configuration. While the IP addresses are fictitious, other networking parameters are still required and your network administrator can help you set up this type of LAN.

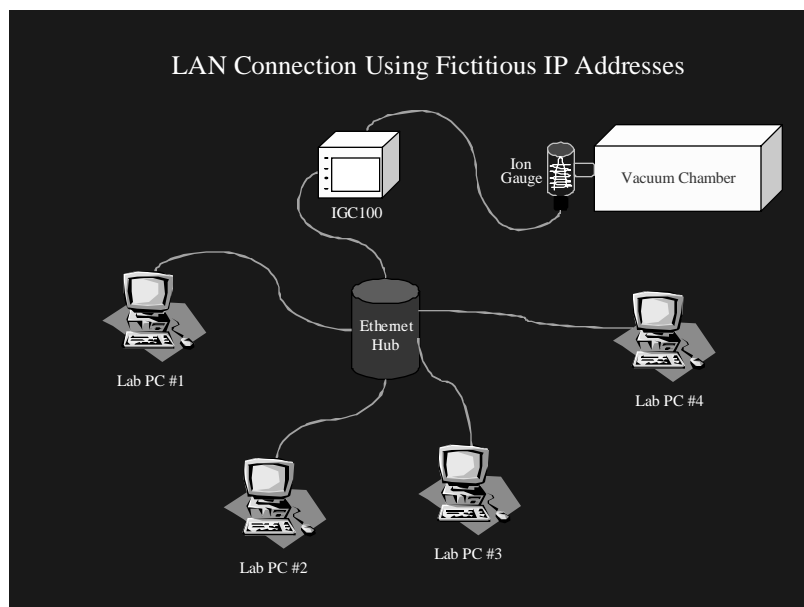


Figure 8-4. Internal LAN Configuration

Note that no connection to the internet is made in this LAN. The network is completely within your laboratory or plant floor, so security from an outside attack on this LAN is not a concern. Of course this also means that *you* cannot access the LAN outside of the workplace. However, the IGC100 *can* be accessed from other computers on the same LAN.

## Conventional LAN Configuration

Chances are good that you are currently using a LAN with real IP addresses that is also connected to the internet through a firewall. A firewall is a piece of hardware designed to exclude unwanted data traffic coming from the outside world. A gateway is often employed in order to allow data traffic from the LAN to reach the outside world. Within a LAN that is using real IP addresses, you need to contact your network administrator in order to set up your EWS. For details, see the section 'Network Administration Concerns'.

This configuration allows anyone on your LAN to use the EWS. With a gateway in place, it also allows the EWS to send out email to a computer which is outside the LAN. However, this configuration may not allow you to monitor or control your vacuum system from outside your workplace. Talk with your network administrator for their advice on setting up this configuration to allow outside access to the IGC100. To maintain the security of the LAN, your administrator may wish to place the IGC100 outside the firewall, as described in the next section.

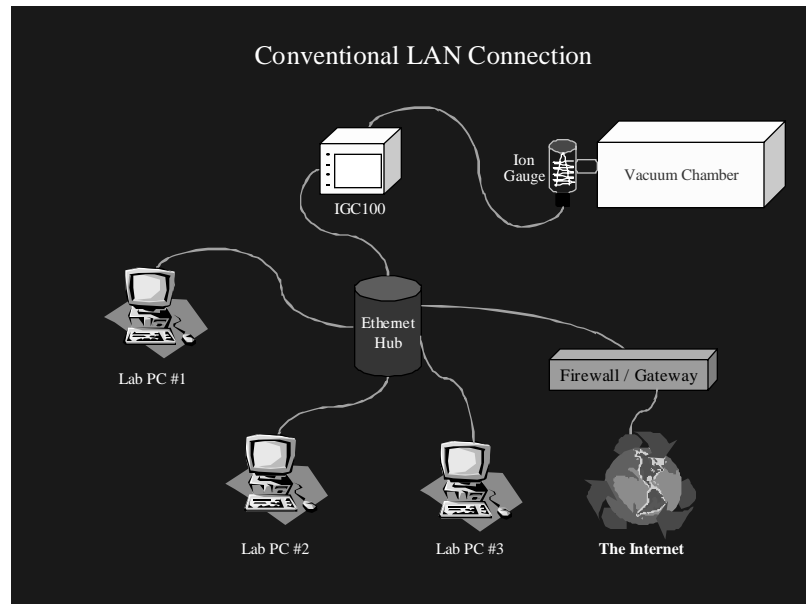


Figure 8-5. Conventional LAN Configuration

## Outside Firewall Configuration

Here, the IGC100 is connected to the world wide web via a router outside the workplace firewall. This connection requires setting up real network parameters (as discussed in the previous sections) and your network administrator should work with you to set this type of connection. This configuration allows you to interact with your instrument from any computer, anywhere on the internet, via a standard browser. You can monitor your data, control relay states, and even receive email notification about relay state changes, from any location. There is a trade-off for all this flexibility and power. Once your instrument is accessible throughout the world, security issues must be addressed. See 'Configuring EWS Security' later in this application note.

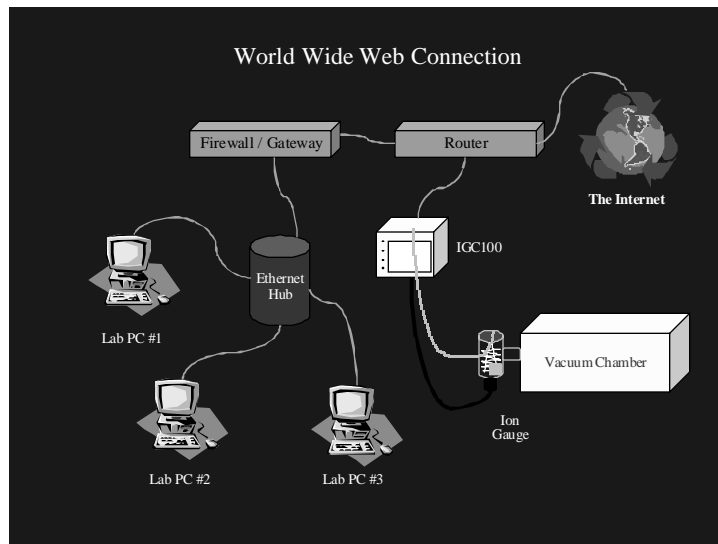


Figure 8-6. Outside Firewall Configuration

---

## Testing with a Crossover Cable

Before putting your instrument on the web, it is best to test it via a direct PC to instrument connection. You will need an ethernet crossover cable, and a computer with a network card, already configured with network parameters. If you need to set up a computer for networking, contact your network administrator. Please do not contact SRS for support of your network. A workstation attached to the same network you wish to use the EWS with is ideal for this test. If the computer is already hooked up to a network, make sure disconnecting it will not cause problems for others on that network.

In this crossover configuration, real networking parameters (Subnet mask, DNS, Gateway) are not required.

- 1) Make sure the IGC100 is powered up and running normally.
- 2) Disconnect the computer from its ethernet network.
- 3) Connect the IGC100 EWS to the computer using a crossover cable.
- 4) From the command line prompt of your workstation, enter the command 'ipconfig'. This command will report the workstation's IP address.
- 5) On the IGC100, go to the Main/Remote/Web menu. Make sure the EWS is Disabled.
- 6) For this test, the IP address can be 'fictitious'. Set the EWS to use a fictitious address by subtracting one from the IP address of your workstation. For example, if your workstation IP address was reported as 111.111.111.111, use 111.111.111.110 for your fictitious EWS IP address. This is the only networking parameter required for this crossover test.
- 7) In the IGC100 Main/Remote/Web menu, set EWS to Enabled. This sets the IP addresses in the EWS and starts the EWS.
- 8) Under Main/Remote/Web, touch [Web Queue]. This screen should show web server activity as it queries the IGC for information. Allow the web server to gather information from the IGC for several seconds.
- 9) Run a web browser on your workstation. At the browser's "http://" prompt, type the fictitious IP address you set on the IGC100 front panel and hit the return key. In a moment, you should see the opening screen of the web page.

If you did not see the opening screen within a few seconds, make sure of the following:

- The web server is enabled. Check Main/Remote/Web/Web Queue (see above) for activity.
- When the cable is plugged in and the server is enabled, a green activity light on the ethernet connector on the rear panel should be illuminated. Verify this light is on. If it does not light, there may be a hardware problem with the crossover cable or your PC network card.
- The IP address on the front panel of the IGC100 matches the IP address you typed in on your browser.
- The crossover cable is connected directly from the PC to the IGC (no hub or switch is in the path).

- The cable is wired as a crossover cable.
- If the web page display seems garbled or if parts are incomplete, try waiting a few seconds and reloading the page in your browser. The most likely cause for this problem is that the web server has not had time to initialize.

---

### Testing Within a Network

In order to test your EWS with a real network, you will need an IP address from your network administrator. You will also need the subnet mask, and IP address of the default gateway machine. You can get these addresses from the administrator. If you wish to use electronic mail, you may also wish to obtain the address of a domain name server (DNS).

- 1) Make sure the EWS is Disabled (Go to the Main/Remote/Web menu on the IGC100 if necessary).
- 2) Set the IP address.
- 3) Set the gateway address and subnet mask.
- 4) Connect the IGC100 EWS to a hub (or other network connection) with a standard ethernet network cable. *Do not use a crossover cable.*
- 5) In the IGC100 Main/Remote/Web menu, set EWS to Enabled. This sets the IP addresses in the EWS and starts the EWS.
- 6) Under Main/Remote/Web, touch [Web Queue]. This screen should show web server activity as it queries the IGC for information. Allow the web server to gather information from the IGC for several seconds.
- 7) Run a web browser on your computer. At the browser's "http://" prompt, type the IP address you entered on the IGC100 front panel and hit the return key.

If you did not see the opening screen within a few seconds, make sure of the following:

- The web server is enabled. Check Main/Remote/Web/Web Queue (see above) for activity.
- When the cable is plugged in and the server is enabled, a green activity light on the ethernet connector on the rear panel should be illuminated. Verify this light is on. If it does not light, there may be a hardware problem with the crossover cable or your PC network card.
- The IP address on the front panel of the IGC100 matches the IP address you typed in on your browser.
- The ethernet cable is connected from the IGC100 to a hub or other ethernet port (not directly to a PC).
- The cable is *NOT* a crossover cable.
- If the web page display seems garbled or if parts are incomplete, try waiting a few seconds and reloading the page in your browser. The most likely cause for this problem is that the web server has not had time to initialize.

**Note**

Your local network environment may prohibit your ability to get web pages from the EWS from outside your facility. See the section below entitled 'Network Configurations' and consult your network administrator for possible solutions.

---

## Configuring EWS Security

You must decide if the IGC100/EWS offers enough security for your application. The EWS employs a number of security measures, however, *no network can be made entirely secure!* All security measures are implemented from the front panel of the IGC100 and cannot be changed via the web interface. This ensures that only authorized users set security levels.

Monitoring of the IGC100 through the EWS is allowed from all users. The security measures are designed to prevent unauthorized users from making changes to the IGC100 settings.

---

### Web Server Enable

If you use your EWS only during certain hours, simply disable it when not in use. No web monitoring or control of the IGC100 is possible when the EWS is disabled. This setting can only be changed from the front panel.

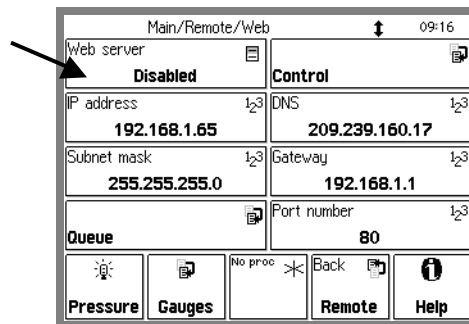


Figure 8-7. Web server enable/disable.

**Important**

Whenever network setup information is changed, you must wait at least 5 seconds for the changes to take effect.

---

### Web Control Enable

If you only wish to monitor your vacuum system from the web, you should disable Web Control. Web Control of the IGC100 includes setting relay states and turning ion gauges on and off. When control is disabled, the EWS does not allow changes to the IGC100 settings. If you allow web control, make sure that the security features below are enabled.

Touch [Control] in the Main/Remote/Web menu to access the control and security features of the EWS.

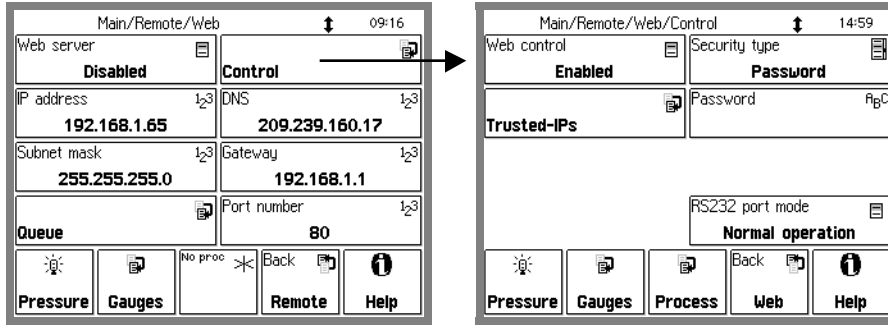


Figure 8-8. Web Control menu.

## Security Type

The IGC100 offers a choice of security options when web control is enabled.

## IP Checking

Within a networking environment in which the IP addresses do not change (the IP addresses are static), you can limit who has access to the instrument by checking the IP address of users asking for data.

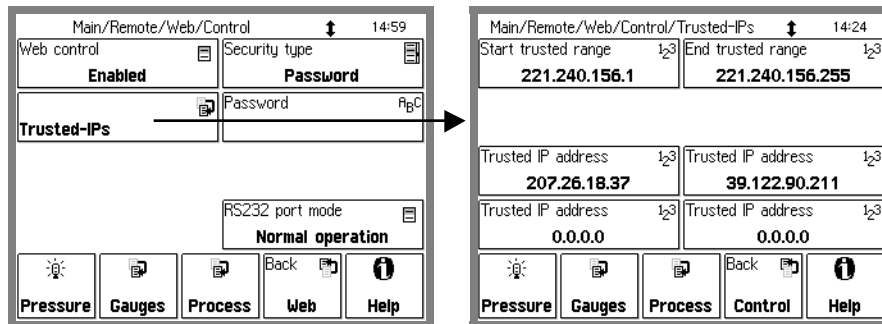


Figure 8-9. Trusted-IP setup menu.

The IGC100 allows you to specify the IP addresses that will be allowed to access the instrument over the web. You may specify a range of addresses as well as four addresses that are outside that range. The addresses outside the range are for trusted users outside the local network with static IP addresses. If your network uses dynamic IP addresses, but they always fall in the same range, you can still use IP checking security. If you do not require access to the EWS via a dial-up connection, this is the security measure to use.

Note that no password is required - if the IP address is trusted, control access is granted.

## IP and Password Checking

As an extra measure of security in addition to IP checking, you can also assign a password to gain access to control of the IGC100. If you have set special parameters that are to remain unchanged even by in-house personnel, this is this measure to use.



## Password Checking Only

This is the lowest level of security for the IGC100's control functions. However, if you require access to the control functions over a dial-up connection to the instrument, this is the method to use. A dial-up connection almost always assigns a different IP address to your connection each time you log on to your internet service provider (ISP). This means IP checking is not a feasible option.

### Note

*The password exchange is not encrypted.* This means that if someone is monitoring your communication with the EWS, they will see your password.

# Using the EWS

To view the EWS web pages, simply type the IP address of the EWS into your web browser.



Figure 8-10. Enter the IGC100's IP address into your browser.

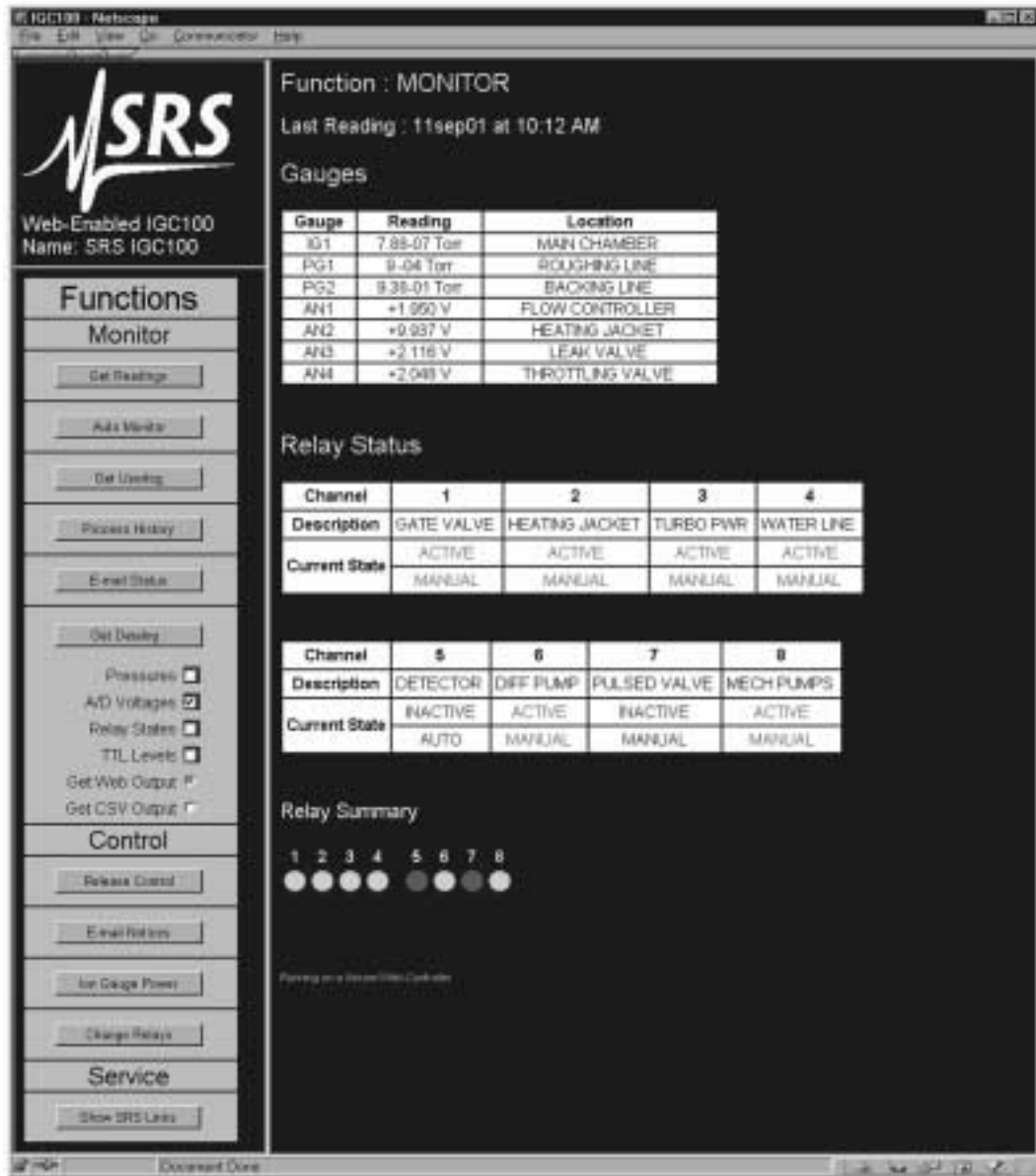


Figure 8-11. Main EWS web page.

## Bookmarking the IGC100

You can add a bookmark to the IGC100 in your browser. Be sure to rename the bookmark to something meaningful. If you are accessing multiple IGC100's, make sure each bookmark is unique.

## Monitoring the IGC100

The simplest use of the EWS is to monitor your data. The EWS offers three distinct ways to monitor.

- Display a page with all active gauges and current relay states
- Monitor selected parameters in an automatically updated window
- Display the data log to see how your system is behaving over time.

## Get Readings

Get Readings reports the value of all inputs that are not in an error state as well as the process control relay states. If a gauge reading does not appear, use the Auto Monitor function described below to display the error state of the gauge. Note that all analog ports which can be converted to capacitance manometer readings are listed twice, as the analog voltage and the corresponding pressure value.

The system name (default "SRS IGC100") can be changed in the Main/Remote menu of the IGC100. This is important if you are monitoring multiple units.

This screen only updates when you click Get Readings. For continuous updates, use Auto Monitor.

## Auto Monitor

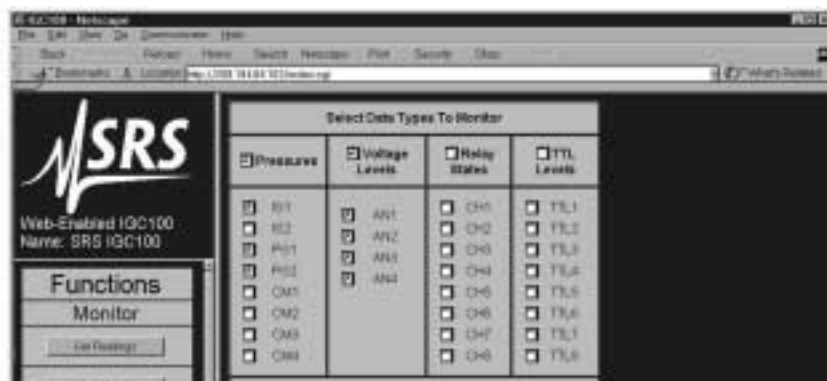


Figure 8-12. Auto Monitor menu.

This function allows automatic monitoring of specific inputs or values. Select the quantities you wish to monitor from the menu and how often you wish the display to update. A new browser window will be created displaying only the selected data. This

window will refresh every 20 seconds (depending upon network availability). The auto monitor function will show the status of a gauge that cannot report a value.

The auto monitoring window can be on your desktop while you work, allowing you to keep tabs on critical parameters (see below). You can create multiple windows to group critical parameters by type, or use a single window and look at several types of data at once. This feature can be especially useful when a relay state is tied to a pressure reading; you can make absolutely sure that the relays are functioning correctly with the given pressure input. These same ideas can be applied to the analog inputs to monitor parameters such as temperature.

Gauge Type	Gauge Reading	Gauge Location
IG1	7.87-07 Torr	MAIN CHAMBER
PG1	9.04 Torr	ROUGHING LINE
PG2	9.40-01 Torr	BACKING LINE
AN1	+1.950 V	FLOW CONTROLLER
AN2	+9.934 V	HEATING JACKET
AN3	+9.934 V	HEATING JACKET
AN4	+2.116 V	LEAK VALVE

*Figure 8-13. Auto Monitor window.*

## Process History

If your IGC100 is equipped with a Process Control option, this function will return up to the last 20 events in the process history. Each entry of the history has a timestamp, a listing of what relays were active at that moment, a listing of what relays were under automatic control at that moment, and what change took place at that moment. By examining the process history, you can trace how your vacuum system arrived in its current state. Often, you can quickly diagnose a problem in your vacuum system when you learn which interlocks were activated and the order in which they were activated.

Process Control History						
Timestamp	Active Relays	Automatic Relays	Channel	Name	Change	
11sep01 10:12:56	11110101	00001000	8	MECH PUMPS	State Active	
11sep01 10:12:56	11110100	00001000	6	DIFF PUMP	State Active	
11sep01 10:12:56	11110000	00001000	4	WATER LINE	State Active	
11sep01 10:12:56	11100000	00001000	4	WATER LINE	Mode Manual	
11sep01 10:12:55	11100000	00011000	3	TURBO PWR	State Active	
11sep01 10:12:55	11000000	00011000	1	GATE VALVE	State Active	
11sep01 24:00:00	01000000	00011000	5	DETECTOR	State Inactive	
11sep01 24:00:00	01001000	00011000	4	WATER LINE	State Inactive	
10sep01 17:00:00	01011000	00011000	5	DETECTOR	State Active	
10sep01 16:00:00	01010000	00011000	4	WATER LINE	State Active	
10sep01 15:53:44	01000000	00011000	2	HEATING JACKET	State Active	
10sep01 24:00:00	00000000	00011000	5	DETECTOR	State Inactive	

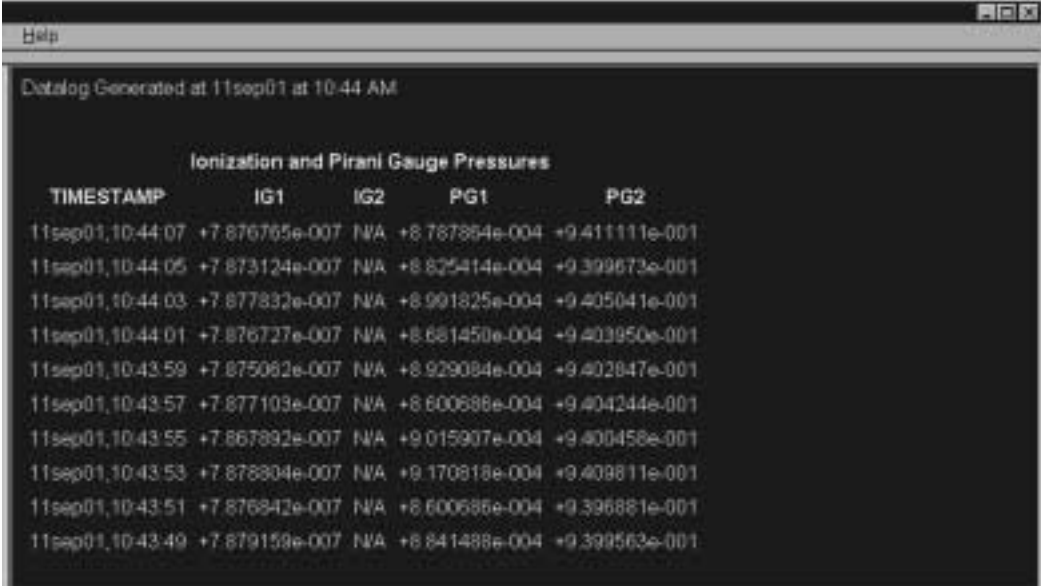
Figure 8-14. Process History.

## Get Datalog

The Get Datalog function downloads IGC100 log data to your computer, via the web. You can select data from four categories, pressures, analog port values, relay states, and TTL levels. The data is downloaded either as a web page or as a comma separated variable (.csv) file compatible with Microsoft Excel.

## Web Output

The number of log points in a web page is fixed at 10 points per data type.



Ionization and Pirani Gauge Pressures				
TIMESTAMP	IG1	IG2	PG1	PG2
11sep01,10:44:07	+7.876765e-007	N/A	+8.787884e-004	+9.411111e-001
11sep01,10:44:05	+7.873124e-007	N/A	+8.825414e-004	+9.399673e-001
11sep01,10:44:03	+7.877832e-007	N/A	+8.991825e-004	+9.405041e-001
11sep01,10:44:01	+7.876727e-007	N/A	+8.681450e-004	+9.403950e-001
11sep01,10:43:59	+7.875082e-007	N/A	+8.929084e-004	+9.402847e-001
11sep01,10:43:57	+7.877103e-007	N/A	+8.600686e-004	+9.404244e-001
11sep01,10:43:55	+7.867892e-007	N/A	+9.015907e-004	+9.400458e-001
11sep01,10:43:53	+7.878904e-007	N/A	+9.170818e-004	+9.409811e-001
11sep01,10:43:51	+7.876942e-007	N/A	+8.600686e-004	+9.396881e-001
11sep01,10:43:49	+7.879159e-007	N/A	+8.841488e-004	+9.399563e-001

Figure 8-15. Web Output of datalog.

## CSV Output

The CSV file is downloaded when you click Get Datalog. If the browser is not setup to automatically handle a .csv file, the data will be displayed in the browser. Users of Netscape Navigator can easily configure the browser to automatically launch Excel (or another graphing program) whenever a .csv file is downloaded.

In Navigator:

- 1) Go to Edit in the menu bar, and choose Preferences.
- 2) In the Category pane, double click on Navigator, then click on Applications.
- 3) Click on New Type. Enter the description "comma separated values", file extension ".csv", MIME type "text" and browse to your application. Do not type the quote symbols!
- 4) Click OK.
- 5) Download the CSV data and your chosen application should open.  
Remember, the application must be able to handle data in this format!

Internet Explorer uses the Windows file associations. Installing Excel usually associates .csv files to Excel. If you need to add the association, go to Windows Explorer or My Computer. Go to View in the menu bar, then choose Options. Click on the File Types tab. Either edit an existing entry or add a new one.

If Internet Explorer will not automatically open Excel, try saving the downloaded csv data to a file. To do this, right-click on the downloaded data frame and choose view source. This usually opens a Notepad window with the data in it. Save this file to disk. Either double-click on this file to launch Excel or open it from within Excel.

**Note**

The EWS is limited in how much data it can send out at a time. Selecting fewer quantities (for example, pressures only instead of pressures and relay states) will increase the number of log points you acquire in a single CSV download.

---

**Get Userlog**

This feature is simply for security purposes. It displays the recent activity on the EWS and it shows the IP address and files accessed.

The network settings of the IGC100 are also displayed, including the MAC address.

---

**E-Mail Status**

E-mail notification is available in units with the Process Control option.

This page displays information about e-mail notification including a summary of the e-mail setup and a list of e-mails which have been sent from the IGC100. In addition, the number of messages sent is shown along with the maximum number allowed.

For more information about setting up e-mail, see the next section 'Controlling the IGC100'.

---

## Controlling the IGC100

The world wide web allows the ultimate in remote control. You can change parameters of the instrument from virtually any location. For security purposes, the EWS only allows control of relay states, email configuration, and ion gauge power. All the control functions are under the security layer and require either the correct trusted IP address and/or password in order to gain access.

---

### Request Control

If web control is disabled from the front panel of the IGC100, the control functions do not appear on the EWS web pages. If control is disabled while someone is browsing the page, the control functions will still be in the web page, but any control operation is prevented.

*You must logon as the controller before any of the control functions can be accessed. Click this button to logon as the controller. Once you log in, the page reloads, and this button is re-drawn as 'Release Control'. Only one user can have control of the EWS at a time.*

The logon prompt depends upon the type of security selected on the IGC100. If you have selected password or both password and IP checking security, you will have to enter the password. If you are just using IP checking for security, no password is required. In both cases, you will need to enter a controller name for identification purposes.

If someone is already controlling the instrument, you will be informed of their logon name, their IP address, and how long it has been since that controller performed a control function (their idle time). If the current controller has been idle for hours, it is likely they simply forgot to logout by clicking 'Release Control'. For this reason, *you are allowed to take control from an idle user, provided you know the password and/or have a trusted IP.*

---

### Release Control

Click this button to logoff as the controller of the instrument.

#### Note

E-mail notification will remain enabled after control is released.

---

### E-Mail Notices

This function allows configuration of the e-mail notification feature. In order to use e-mail, you must have entered a valid gateway address in the IGC100. A valid Simple Mail Transfer Protocol server (SMTP) address is also required. The gateway address is required so the EWS can access the SMTP server. The SMTP server is the machine (typically outside your network) that accepts e-mail and routes it to the appropriate address. These addresses should be obtained from your local network administrator.

Remember, e-mail is inherently unreliable - SMTP servers fail, delivery time is inconsistent, you don't read your mail regularly, etc. *Use e-mail notification as a backup*



to an interlock system, not in replacement of one. Since the only purpose of e-mail is to alert users to process control changes, this button will be functional only if the IGC100 has the Process Control option.

E-Mail Configuration		
SMTP Server: (IP or mnemonic)	<input type="text" value="129.156.023.040"/>	
From: (Set if needed)	<input type="text" value="igc100@fablab.net"/>	
Send Email To: (Primary addr.)	<input type="text" value="et1@fablab.net"/>	
Cc Email To: (Secondary addr.)	<input type="text" value="let@fablab.net"/>	
Send at most :	<input type="text" value="16"/> E-mail notices	
E-mail is :	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled
<input type="button" value="Send A Test Message"/>		<input type="text" value="Type a test message here."/>
CH#/Desc.	Event:	Message Text (up to 50 chars):
<input checked="" type="checkbox"/> CH1 GATE VALVE	Activation:	<input type="text" value="Gate valve closed! Call x2441"/>
	Deactivation:	<input type="text" value="Gate valve open"/>
<input checked="" type="checkbox"/> CH2 HEATING JACKET	Activation:	<input type="text" value="Heating Jacket back on"/>
	Deactivation:	<input type="text" value="Heat Jacket is off; check wires"/>
<input checked="" type="checkbox"/> CH3 TURBO PWR	Activation:	<input type="text" value="Turbo pump running."/>
	Deactivation:	<input type="text" value="Turbo pump is off! Call x2441"/>
<input type="checkbox"/> CH4 WATER LINE	Activation:	<input type="text"/>
	Deactivation:	<input type="text"/>

Figure 8-16. E-Mail configuration web page.

### Testing the E-Mail Function

It is very important to test the e-mail function before using it routinely. If any address is incorrect, you will never get an e-mail notice.

1. Set the SMTP address. Make sure you type it correctly. If you are using a verbose address (relay.mailhandling.com), make sure the DNS address was entered correctly on the IGC100.
2. Set the "from" address. The SMTP may require a "from" address that has a certain domain name. The domain name is typically the string after the '@' sign in an e-mail

address. For example, if your e-mail address is me@mycompany.com, you may wish to use igc100@mycompany.com as the "from" address. Ask your network administrator if a particular domain name is required to use your SMTP server.

3. Set the "to" address; this is the e-mail address where you want notifications to be sent.
4. Click the 'Send A Test Message' button.

To learn the fate of your e-mail message, click 'E-Mail Status'. Your sent e-mail and the reply from the SMTP server will be listed there. Any reply other than "250 - OK" is an error. Click 'E-Mail Status' again to refresh the status if it was listed as "-2 -Awaiting reply". If the SMTP reply is "-1 : No Reply", a connection to the SMTP server was never made. Re-check your physical network connection as well as the gateway and SMTP addresses. If no error occurs, but you still do not receive the email, check the "from" and "to" addresses used.

### **Using the E-Mail Function**

Once you have successfully tested the e-mail function, you can set a carbon copy (CC) address to send a copy of the notice to another user. Use only one e-mail address in the CC field.

1. Set the e-mail notices to "Enabled". A test message can always be sent by clicking the "Send A Test Message" button, even if e-mail notification is disabled. If you will be unable to receive e-mail for an extended period, it is a good idea to disable relay-linked e-mail notification.
2. Set the maximum number of relay-linked e-mail notices the EWS is allowed to send. This feature prevents accidental flooding of your mailbox. The default is 16. You probably wish to limit this number even further. The maximum cannot be set higher than 32.
3. Link process relays to e-mail notices by clicking their checkboxes. The subject line of each e-mail will be the channel number of the relay that changed and its new state, e.g. "Channel 1 : Inactive".
4. Enter a message you wish to send in the notification for both the activation and deactivation of the relay. Note the message cannot be more than 50 characters long.
5. Click "Use This E-Mail Configuration" to store your e-mail setup in the EWS. Verify the configuration is correct by clicking "E-Mail Status".
6. Test that your configuration by manually changing the state of a linked relay from the front panel.

If you wish to clear the configuration when you begin a new process, click "Erase This E-Mail Configuration".

To reset the e-mail count after a number of e-mails have been sent, disable then re-enable e-mail.

### **Note**

E-mail notification remains enabled after control is released.

## Ion Gauge Power

**Warning!**  
Turning an ion gauge on or off from a remote interface can be dangerous. Make sure you understand your vacuum system and any process controls that depend upon ion gauge data before using this feature.

This function allows you to turn an ion gauge on or off, as well as choose the filament usage mode.

Ionization Gauge Parameters		
Gauge Parameters	IG1	IG2
Location	MAIN CHAMBER	IG2
Status	0 - Gauge OK	13 - Emission off
Emission	EMISSION ON	EMISSION OFF
Filament	Filament 1	Filament 1

Ionization Gauge Controls		
Emission	ON <input checked="" type="radio"/>	ON <input type="radio"/>
	OFF <input type="radio"/>	OFF <input checked="" type="radio"/>
Filament	Filament 1 <input checked="" type="radio"/>	Filament 1 <input checked="" type="radio"/>
	Filament 2 <input type="radio"/>	Filament 2 <input type="radio"/>
	Both <input type="radio"/>	Both <input type="radio"/>

Figure 8-17. Controlling the Ion Gauge.

## Change Relays

### Warning!

Changing relay states from a remote interface can be dangerous. Make sure you understand your vacuum system and all process controls you have in place before using this feature. This feature will not be functional if the IGC100 does not have the process control option.

By clicking this button, you receive a web page showing the current state of all eight relays of process control. You can set a relay to be active, inactive, or under automatic control. To send your desired relay states to the IGC100, click the button labeled "Click Here To Set All 8 Relays".

Function : CONTROL

Process Control Status at 11sep01 at 11:00 AM

Channel	1	2	3	4
Description	GATE VALVE	HEATING JACKET	TURBO PWR	WATER LINE
Current State	ACTIVE	ACTIVE	ACTIVE	ACTIVE
	MANUAL	MANUAL	MANUAL	MANUAL
Desired State	<input type="radio"/> Inactive	<input type="radio"/> Inactive	<input type="radio"/> Inactive	<input type="radio"/> Inactive
	<input checked="" type="radio"/> Active	<input checked="" type="radio"/> Active	<input checked="" type="radio"/> Active	<input checked="" type="radio"/> Active
	<input type="radio"/> Auto	<input type="radio"/> Auto	<input type="radio"/> Auto	<input type="radio"/> Auto

Click Here To Set All 8 Relays

Channel	5	6	7	8
Description	DETECTOR	DIFF PUMP	PULSED VALVE	MECH PUMPS
Current State	INACTIVE	ACTIVE	INACTIVE	ACTIVE
	AUTO	MANUAL	MANUAL	MANUAL
Desired State	<input type="radio"/> Inactive	<input type="radio"/> Inactive	<input checked="" type="radio"/> Inactive	<input type="radio"/> Inactive
	<input type="radio"/> Active	<input checked="" type="radio"/> Active	<input type="radio"/> Active	<input checked="" type="radio"/> Active
	<input checked="" type="radio"/> Auto	<input type="radio"/> Auto	<input type="radio"/> Auto	<input type="radio"/> Auto

Figure 8-18. Relay control web page.

# Networking Terms

Some terms that are used throughout this application note are defined here.

## Server

A server is simply a computer capable of delivering data to another computer. Typically, the server is *only* used to deliver data and all its resources are allocated to that task.

## IP Address

Each computer that is connected to the world wide web needs to have a unique address in order for other machines to access that computer. An IP address is made up of four bytes. It is often expressed as a set of three digit numbers separated by a '.', e.g. 209.239.160.084.

## Static IP Address

A static IP address never changes. Static IP addresses are often used for servers, so that computers on the web can find them.

## Dynamic IP Address

A dynamic IP address changes frequently. Often, clients have dynamic IP addresses that are assigned to them when they boot up. When you use a dial-up connection, an IP address is assigned to you each time. This means you get a different IP address every time you logon from a dial-up connection.

## Fictitious IP Address

Networks that are not directly connected to the world wide web sometimes use fictitious IP addresses valid only for local communication. Machines connected to this type of network are not directly accessible from outside that network. This improves security of the network and conserves the number of real IP addresses required for a facility. A network of fictitious addresses can be connected to the web using a router.

## MAC Address

The media access control (MAC) address is another unique address that belongs to the physical network interface card. It is sometimes called an 'ethernet address'. It is often expressed as a series of hexadecimal codes separated by a dash (for example, 00-00-1A-18-FF-00). The Internet Protocol (IP) maps each machine's individual MAC address to an IP address.

## DNS Address

People have a difficult time remembering and using long strings of numbers, so domain name servers are in use. You can think of these machines as a kind of telephone book - they associate a particular IP address (209.239.160.084) with a string of characters (www.thinksrs.com). A DNS is not required to use the EWS, but it can make your life a little easier.

## SMTP Address

In order to send e-mail, a special machine called a Simple Mail Transfer Protocol server is often used. These servers respond to commands for sending e-mail and will forward your messages to the recipient's local mail handling machine.

