



Lick Automated Planet Finder Observatory



Operations Manual

CI No. EMB07782-01

EOS SPACE SYSTEMS PTY LIMITED
111 CANBERRA AVENUE GRIFFTH, ACT, 2603
A.B.N. 25 100 248 253
TELEPHONE 61 2 6222 7900
FACSIMILE 61 2 6299 7687

DOCUMENT CONTROL

Prepared	Signed <i>Jan Rathi</i>	Date <i>26/10/06</i>
Checked	Signed <i>[Signature]</i>	Date <i>26/10/2006</i>
Approved	Signed <i>Jan Rathi</i>	Date <i>26/10/06</i>

<i>1</i>	<i>26/10</i>	<i>Initial Release</i>	<i>r</i>	<i>[Signature]</i>
Issue	Date	Description	Checked	Approved

Index	
-------	--



Lick Automated Planet Finder Observatory



Operations Manual

CI No. HBO07782-01

EOS SPACE SYSTEMS PTY LIMITED
111 CANBERRA AVENUE GRIFFTH, ACT, 2603
A.B.N. 25 100 248 253
TELEPHONE 61 2 6222 7900
FACSIMILE 61 2 6299 7687

DOCUMENT CONTROL

Prepared	Signed	Date
Checked	Signed	Date
Approved	Signed	Date

Issue	Date	Description	Checked	Approved

Index	
-------	--

TABLE OF CONTENTS

1. INTRODUCTION	7
2. USER SAFETY	8
2.1 General Personnel Safety	8
2.2 Crush Points	8
2.3 Emergency Stop Facility	9
3. SYSTEM OPERATION WARNINGS	11
3.1 General Warnings	11
3.2 System Familiarization	11
3.3 Access to the Telescope Enclosure	12
3.4 System Logbook	13
3.5 System Configuration	14
3.6 Precautions Before Moving Telescope Axes	15
3.7 Sun Avoidance	15
4. ENCLOSURE SYSTEM OVERVIEW	17
4.1 Dome	17
4.1.1 Description	17
4.1.2 Safety Systems	18
4.2 Software	19
4.2.1 Description	19
4.2.1.1 Node States	20
4.2.1.2 Dome States	20
4.2.1.3 Life Lines	22
4.2.1.4 Personnel Safe	22
5. SYSTEM OPERATIONS	24
5.1 Enclosure Start	24
5.1.1 Normal Start	24
5.2 Enclosure Stop	29
5.3 Manual Controls	30

5.4	UPS	33
5.5	Software Controls	34
5.5.1	System Management Interface	34
5.5.1.1	Description	34
5.5.1.2	Logon	34
5.5.1.3	Starting the Observatory Control System	35
5.5.1.4	Stopping the Observatory Control System	36
5.5.1.5	Starting an Individual Server	36
5.5.1.6	Stopping an Individual Server	36
5.5.1.7	Forcibly Stopping an Individual Server	37
5.5.1.8	Terminating an Individual Server	37
5.5.1.9	De-registering an Individual Server	37
5.5.2	Dome User Interface	38
5.5.2.1	Description	38
5.5.2.2	Logon	40
5.5.2.3	General Features	40
5.5.2.4	Safety	47
5.5.2.5	Shutters	49
5.5.2.6	Front / Rear Shutter	52
5.5.2.7	Azimuth	56
5.5.2.8	Vent Doors	60
5.5.2.9	Vent Door 1 – 4	61
5.5.2.10	Cooling Systems	64
5.5.2.11	General Digital Outputs	66
6.	ENCLOSURE END OF TRAVEL RECOVERY	68
6.1	Overview	68
6.2	Normal Operation: Telescope Movement Limits	68
6.3	Enclosure Failsafe Operation	69
7.	COMMON ENGINEERING PROCEDURES	70
8.	SOFTWARE UTILITIES	71
8.1	Device Browser	71
8.1.1	Description	71
8.1.2	Logon	73
8.1.3	General Features	74
8.1.4	Menus	74

8.1.4.1	File	75
8.1.4.2	Mode	75
8.1.4.3	View	75
8.1.4.4	Subscribe	75
8.2	User and Permission Configuration	76
8.2.1	Authentication Interface	76
8.2.1.1	Description	76
8.2.1.2	Logging in	79
8.2.1.3	Adding a new user	79
8.2.1.4	Editing a user	81
8.2.1.5	Removing a user	82
8.2.1.6	Adding a new group	83
8.2.1.7	Editing a group	84
8.2.1.8	Removing a group	86
8.2.1.9	Adding an access control list	87
8.2.1.10	Editing an access control list	88
8.2.1.11	Removing an access control list	90
8.2.1.12	Assigning an access control list to a command	91
8.2.1.13	Removing an access control list from a command	92
8.2.1.14	Marking a command as configured	92
8.2.1.15	Clearing access control list configurations	93
8.2.1.16	Removing an unmatched command	93
8.2.1.17	Saving changes	93
8.2.2	Resource Management Interface	94
8.2.2.1	Description	94
8.2.2.2	Logging in	95
8.2.2.3	Creating resources	95
8.2.2.4	Editing resources	96
8.2.2.5	Deleting resources	97
8.2.2.6	Creating a proxy	97
8.2.2.7	Removing a proxy	98
8.2.2.8	Jumping to a proxy's resource	99
8.2.2.9	Adding resources to a command	101
8.2.2.10	Removing resources from a command	103
8.2.2.11	Clearing a command's resource configurations	104
8.2.2.12	Marking a command as configured	105
8.2.2.13	Removing an unmatched command	106
8.2.2.14	Changing command views	107
8.2.2.15	Viewing the initialization report	108

8.2.2.16	Saving changes	108
8.3	Log Viewer	109
9.	FAULTS AND MAINTENANCE	111
9.1	Software Maintenance	111
9.1.1	Backup of Configuration files	111
9.1.2	Archival of old log files	111
9.1.3	Reboot the machines	112
9.2	Troubleshooting	112
9.2.1	Common Problems	112
9.2.2	Using Log Viewer to Diagnose Problems	113
9.3	Known Issues	Error! Bookmark not defined.

1. INTRODUCTION

This document describes the correct use of the Lick APF co-rotating observatory for EOS telescopes over 1.5m in aperture. Recommended management techniques, safe operation and facilities for enhancing the observing quality of the telescope are included. EOS recommends that this guide be used as the basis of personnel training before certifying any person as a licensed operator of the observatory system.

User installed or designed equipment may be described in this document, but EOS does not warrant the safety of such third party equipment as used.

2. USER SAFETY

2.1 General Personnel Safety

The observatory systems using the IceStorm Series II enclosures are often highly automated, and as such the movement of servo controlled components may begin without prior warning. **DO NOT** place parts of the body in apertures which can close without first conducting a safety analysis of the operation with other users. The shutter especially is powerful enough to lift its parts while heavily laden with ice, and crush damage could be fatal or lead to amputation.

After entering the door, safety is every user's business. Children should not be allowed into the building while power is applied to systems without the most careful supervision and knowledge of safety features.

2.2 Crush Points

The following parts of the enclosure involve mechanical hazard unless electrically isolated:

Front door: this door is steel and strong winds create a potential hazard.

L1 floor gap: this gap separates a moving mass of over 20 tonnes from the static part of the dome. Do not reach into the gap.

L2 azimuth support bogeys: although hard to reach, the support wheels can be reached with fingers.

Lateral guide rollers: these too can be reached with fingers, despite being hidden.

Vent doors: the momentum of these doors when closing, and the nature of the seals, make this a potential hazard during maintenance operations.

Shutter: the aperture is accessible via the lower sill, and represents a crush hazard whenever the shutters are moving closed. Exposed gaps between moving and static parts may also be dangerous.

Night operations: stair wells and trip hazards from equipment on floors must be considered when performing night maintenance such as telescope collimations. The Telescope Optical Tube assembly can move without warning, although no azimuth hazard exists with a co-rotating enclosure. Hard hats are advisable.

Mains voltages: within cabinets, only qualified personnel should make adjustments or repairs.

2.3 Emergency Stop Facility

On each level are red illuminating Emergency STOP (ESTOP) buttons. Pushing a button activates the ESTOP low level controls and cuts power to all servo controlled systems immediately. The pressed button flashes, and all other ESTOP buttons illuminate to show the ESTOP status at all levels in the enclosure. Pulling on the flashing button releases the hold on the ESTOP condition, allowing software commands to re-establish power to the servo systems.



Active ESTOP switch: typical location

NOTE: releasing an ESTOP button does not remove the ESTOP condition: it allows the condition to be explicitly reset by either software commands or the manual reset button.



ESTOP and ERESET Buttons on Level 1: Lick Installation

Note the Az EOT Override button in the figure above: it is an override for the possible condition whereby the telescope exceeds all of its azimuth limit switches and the enclosure azimuth limits actuate on the cable wrap. See 6 Enclosure End Of Travel recovery for full details.

The Azimuth Enable Override on the right photo may sometimes be located between the azimuth drive systems, and is used during site engineering tests where full software control is undesirable. Be very careful using this system, as it bypasses several safety systems in software.

ESTOP of the enclosure sends a comparable signal to the telescope enclosure, causing a telescope ESTOP condition also. This condition is reset separately from the enclosure condition.

3. SYSTEM OPERATION WARNINGS

3.1 General Warnings

The observatory is a complex system in which any of a number of things can go wrong or behave unexpectedly. While all efforts have been made to ensure safe and correct operation of the system it is impossible to completely predict or prevent damage or injury resulting from accident or misuse. Therefore:

Be careful at all times when operating the system.

In particular you should follow the instructions in this document exactly as written. Some of the procedures described in this document involve complex steps. Making a mistake on any of these steps will usually cause the system to fail. Sometimes it fails in obvious ways, such as not moving when commanded, while at other times the failure can be very difficult to detect, such as a small error in the system clock. In a few cases not following the instructions carefully can damage the telescope.

If after several attempts things don't appear to be working as described, shut down the system and start from the beginning. If this still doesn't help, contact authorized engineering support personnel. It is impossible to predict what could go wrong and provide instructions for overcoming every problem. Similarly it is difficult, even for experts, to work out why the system is not behaving as it should.

3.2 System Familiarization

Become familiar with the system.

Learn how the system works by watching someone else operate it. Gain experience working under the guidance of others before attempting to operate the system without supervision. Know what to expect and why so that you can recognize when the system is not operating correctly.

Act quickly to avoid damage or injury.

The system can be very easily damaged by the wrong action or simply by not acting quickly enough when things go wrong. If you see the telescope or enclosure acting strangely be ready to stop it in

an instant. Particular things to watch for are oscillations, jerky motion, moving too fast or moving too close to an end limit.

The Emergency Stop buttons are the best way to stop the telescope from moving in an emergency. Know where they are and be ready to use them at all times. If this is impractical then plan ahead what you would do in an emergency.

Failure may also occur in the electronics or other parts of the system. If you think you see or smell smoke, or you hear unusual sounds from the telescope or cabinet, press the Emergency Stop button, turn off all the power, and then investigate. Do not restart the system until you are certain that nothing has been damaged.

Investigate problems before continuing.

If a problem occurs, such as the telescope stops tracking, try to determine the cause of the problem before attempting the operation again or rebooting the system. This is important because damage to the telescope may have occurred, or damage could be prevented by removing the cause of the problem so it doesn't happen again. See the following section on Troubleshooting for steps to take when trying to resolve a problem.

Report all accidents or incidents as soon as possible.

This may prevent further damage or injury from occurring and will also help to ensure it doesn't happen again. Advice can also be given on the possible consequences to system performance and suggested tests to conduct to determine if damage has occurred and whether the system is operational.

3.3 Access to the Telescope Enclosure

Do not approach the telescope while in use.

There are several dangers associated with being near the telescope while it is in use, even when it is idle.

The most obvious danger is being struck by or caught in the moving mechanisms. The motors which drive the system are powerful and can easily cause injury or damage. Even if the telescope appears stationary it is not safe to be under the Optical Tube Assembly. As a remotely operated system the elevation drive can move without warning.

There is also the risk of causing damage to the telescope by bumping or jarring it. The telescope is a precision optical instrument and the delicate optical and mechanical components can be easily broken or knocked out of alignment. Always take care when moving around near the telescope. Casual visitors should be escorted by expert users and provided with safety instructions. Children should not be allowed to enter the enclosure: it is a remotely operated machine moving over 20 tonnes of suspended mass without warning.

If you wish to work on or near the telescope press an Emergency Stop button. This will ensure that the telescope cannot move.

Always inform others if you intend working on the telescope. Because the telescope can be controlled remotely it is possible for someone to start up the system without realizing that you are nearby. Reset of ESTOP conditions should not be regarded casually. Be certain it is safe to do so.

In some cases it will be necessary to work on the telescope while it is operating, for example during maintenance or when measuring performance. In these situations always observe the Emergency Stop button nearest to you and be prepared to use it in an instant. If this is not possible then have someone else attend an Emergency Stop button and watch for danger.

3.4 System Logbook

When several people or groups are sharing the telescope it is important to communicate information about the status of the system.

Use a system logbook.

EOS recommends the establishment of a logbook which everyone working with the telescope will use to record the status of the system and any problems which have been encountered. Each time the telescope is used, create a new entry in the logbook recording your name, the date and time, and the work you will be doing. If problems occur make a note of them. If previous problems have been fixed note this down too. At the end of the session indicate whether the telescope is still operational or whether there are problems which should be addressed and prevent it from being used.

A notice board may also be useful for quickly indicating the current state of the system and its outstanding problems. However, the ultimate reference should be the system logbook.

Check the operational status of the system.

At the start of each session check the logbook (or notice board) to determine whether the telescope is operational, whether any new problems have surfaced or old ones have been solved, and to refresh your memory about the existing known problems.

Check before turning on the power.

If the power to the system has been turned off make sure you know why before attempting to start the system up. The system may have been turned off because a serious fault was observed, and turning it on again could damage system components.

3.5 System Configuration

Do not add, remove or modify any system components.

It is important to consider the operation of the entire system when making any changes to the configuration of any part of it. The servo systems have been carefully tuned and are very sensitive to changes. If the system becomes unstable it can oscillate, leading quickly to damage to the drive mechanisms. Changes in OTA balance can also adversely affect tracking performance in various ways which may not be immediately apparent.

Many of the components have been placed very precisely to provide optimum performance and not obstruct telescope motion. The positioning and alignment of the optical components are particularly important.

If you wish to add, remove or change any of the hardware contact authorized engineering support personnel to discuss the proposed change and any possible risks to the system.

3.6 Precautions Before Moving Telescope Axes

Some precautions should be taken before attempting to move the telescope.

Check for telescope obstructions.

Check that the telescope axes will move freely around in their travel and not catch on or scrape any equipment which may have been left lying around. This is a common problem during testing and maintenance when several people have been working on the telescope. In particular look for:

- items near the telescope
- equipment loosely or temporarily attached to the telescope — these may come free as the telescope moves around and fall onto the primary mirror
- any changes to the observatory: new devices, parts moved or removed, etc. — these can interfere with the normal operation of the telescope and enclosure, affecting performance or causing obstruction

When operating the system in the enclosure be ready to use the telescope's own Emergency Stop button and press it if the telescope begins to move out of control, enclosure starts slipping (i.e. motor moving but enclosure not moving), runs into an obstruction, or if something else goes wrong (e.g. smoke appears, loud scraping noises are heard, etc.). Similarly for the software ESTOP during remote operations.

Telescope: Note that if the telescope PLC control programs have been disabled with *PEWin* then the telescope ESTOP button should not be pulled out until the motors have been turned off through software.

3.7 Sun Avoidance

Avoid pointing the telescope at the Sun.

Excessive light and heat easily damage the delicate optical components, including any instruments mounted to the telescope. Even sunlight falling on the primary mirror at an angle can cause damage — the reflected rays may focus on the enclosure roof and start a fire. Even if the enclosure roof is closed, sunlight may get through small cracks.

The current system has no built-in Sun avoidance. The user must exercise appropriate caution when operating the telescope during the day to minimize the risk of exposure to direct sunlight:

- Keep the telescope pointed at least 25° away from the Sun at all times.
- Do not leave the telescope parked in a position where the Sun could move into its field of view within the next 24 hours. It is recommended that when not actively in use the telescope should be pointed to the North (0° azimuth).

4. ENCLOSURE SYSTEM OVERVIEW

4.1 Dome

4.1.1 Description

At its core the IceStorm Series II dome is controlled by multiple semi independent microcontroller based processing units (nodes). These nodes are interconnected via a CANopen¹ communications bus and under normal operating conditions, receive commands and transmit status data from/to the main control computer along this bus. This distributed processing architecture allows the main control computer to issue commands and monitor the results, but alleviates the need for its involvement in the actual low level control of the electro-mechanical systems.

There are two CAN buses in use in the dome; one for the main electro-mechanical components, the other for the air-conditioning system.

The electro-mechanical CAN bus has the following devices:

- Azimuth controller
- Front and Rear shutter controllers. Depending on the configuration the shutters Motor Drives may also appear on this bus
- 4* Vent Door controllers
- Safety node
- Digital I/O (connected to devices such as house lights, fans, snow melt)

Air-conditioning CAN bus:

- 3 * Fan Control Units (FCU), each consisting of
 - Coil temperature sensor
 - Cooling/heating output control

¹ CANopen is a development of the Bosch CAN bus system, and is highly regarded among field-bus systems in terms of reliability and flexibility. It has excellent bus arbitration and error detection facilities, behaves well in sub-optimal electrical environments, as well as the ability to operate reliably at higher levels of bus utilisation.

- Loop controller, controls cooling valve and fan
- Nominally 3* Temperature, Humidity and Dewpoint (THüD) sensors. Note that there may be any number of these THüDs installed in various locations as required.

4.1.2 Safety Systems

There are conflicting ‘safety’ requirements for the enclosure. On the one hand, under certain conditions (eg Mains power fail) the enclosure needs to be able to close down autonomously, while on the other any personnel working in the enclosure need to be confident that the systems will only move under their explicit command.

In order to try and ensure both types of safety the enclosure has its own safety system built into it. This included various software states and behaviours, along with various buttons throughout the enclosure. There are buttons to enter into, and recover from several Emergency conditions. The three Emergency conditions (in priority order) are:

- E-Stop – this will stop all motion as quickly as possible and ensure that no further movement occurs while this remains active. There are six (6) E-Stop buttons throughout the enclosure. There is a manual Emergency Reset button located on level one (1) that will reset the E-Stop state (assuming no inputs are active).
- E-Close – this will close the enclosure shutters and vent doors, and hold them closed while active. There is one E-Close button located just inside the front door of the enclosure.
- E-Secure – as per E-Close, only with a lower priority. See Personnel Safe section for more details. This is entered into either autonomously as a result of some input (eg UPS or rain sensor), or via software control.

Under ‘normal’ conditions the enclosure is in the mode to protect the equipment, so the devices (shutters and vent doors) may move at any time without warning. To enter into the mode where personnel safety is the priority use the Personnel Safe key switch located just inside the front door of the enclosure (near the E-Close button). Please note that this mode does **NOT** provide a guarantee that there will be no motion. If you are working on or near the various hardware systems and do not want them to move it is best to also remove power from the system drives. See Personnel Safe section for more details.

4.2 Software

4.2.1 Description

The software for the enclosure follows a common Client/Server architecture. The Servers are software components that are responsible for the control of various hardware components of the observatory (eg Telescope and Dome), or for offering some other service that is used by other servers or clients. The Clients in this system are generally Graphical User Interfaces (GUIs). The clients have a limited amount of intelligence and control the various components through the controlling servers. The servers can be (and are) arranged in a hierarchical manner allowing more appropriate interfaces and control over larger parts of the system at the higher levels. For example the server controlling the whole Dome is a parent of the various servers that talk with and provide basic control over the various CAN busses that communicate with the low level nodes. It is more appropriate to communicate with the Dome Server than it is to communicate with the CAN Server to control the Dome, however to perform low level engineering tasks it is sometime useful to be able to connect and control the lower levels.

The software can be divided into several categories or layers: Control System, Device Control, and Observatory Control. The Control System is responsible for low level services that all other layers rely on, like the provision of system configuration, the ability to locate other servers, user management etc. The Device Control layer is responsible for the control of the hardware in the system, for example the Telescope and Dome servers. The Observatory Control is generally responsible for the higher level co-ordination of the components to perform tasks, for example to Open the Dome, position the Telescope, and take an exposure with the Camera.

It is also possible (and likely) for each installation to have its own customer supplied components. Generally these will be at the Device Control and Observatory Control layers. Some installations also run a separate set of components of their own design and implementation and only use the EOS supplied components to control the EOS supplied hardware.

4.2.1.1 **Node States**

A consistent state model is used for several of the safety critical sub-systems. These are:

- Shutters
- Vent Doors
- Azimuth

4.2.1.2 **Dome States**

4.2.1.2.1 Fault

The device is not able to drive/control its hardware. All software commands that will cause motion are rejected when in this state. The ResolveFault can be used to attempt to recover from this state.

4.2.1.2.2 E-Stop

In this state all motion will stop as quickly as possible and will remain stopped. Any software or manual controller commands to move the system will be rejected. The Safety node has six E-Stop input buttons that are located throughout the enclosure. If ANY of these buttons is active, or if the Software E-Stop is active then the E-Stop output will become active. Once it has become active it will remain so until a command is issued to reset it; this command will be rejected if any of the inputs (physical or software) are still active.

4.2.1.2.3 Manual Hardware

Each of the devices has a manual override key switch. If this becomes active then the device will transition into this state. From this state all software commands will be rejected; the only way to control the device is via the manual inputs.

4.2.1.2.4 E-Close

When in this state the device will 'close' itself. All software commands will be rejected. This state/mode is latched, in that a reset command is required to clear this state even if the input condition is cleared.

4.2.1.2.5 Personnel Safe

This state is to offer a user who is physically inside the enclosure the confidence that the only movement that will occur will do so from an action from someone inside the enclosure. All autonomous behavior (close due to Mains power failure, for example) will be prevented in this mode.

In this mode all software commands will operate as per normal; however the higher level software (CAN, Telescope and Ice Storm II Servers) will use an IP address filter to only allow commands from pre-configured locations.

4.2.1.2.6 Manual Software

This is a state to allow ‘unsafe’ movement of the devices via the software interface; typically this will allow ‘jog’ type commands that will ignore limit switches etc. It is expected that they would only be used in emergencies and then only when the hardware is visible via a camera or by direct viewing.

4.2.1.2.7 E-Secure

This is similar to E-Close except with a lower priority. This state is also ‘latched’. The Safety node is responsible for propagation of this information. There are several inputs that can be configured to be E-Secure inputs. The current system is configured to have one input. This input has a timer associated with it that will start to decrement whenever the input becomes active. If the timer reaches 0 zero then the E-Secure ‘output’ becomes active. Each of the input timers has an associated ‘reset’ command. The IceStorm II Server is currently configured (hard-coded at present) to send a timer reset command only to the UPS E-Secure input when it receives the ESecureHoldOff command.

4.2.1.2.8 Autonomous

This is the ‘normal’ state, all software commands are allowed.

Node Inputs							
Fault	E-Stop	Manual Drive Key	E-Close	Personnel Safe Key	Software Manual	E-Secure	Mode
Active	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care	Fault
Inactive	Active	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care	E-Stop
Inactive	Inactive	Active	Don't Care	Don't Care	Don't Care	Don't Care	Manual H/W
Inactive	Inactive	Inactive	Active	Don't Care	Don't Care	Don't Care	E-Close
Inactive	Inactive	Inactive	Inactive	Active	Don't Care	Don't Care	Personnel Safe
Inactive	Inactive	Inactive	Inactive	Inactive	Active	Don't Care	Manual S/W
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Active	E-Secure
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Autonomous

Dome state priority table

4.2.1.3 *Life Lines*

A LifeLine message (aka watchdog, life guard, heartbeat etc.) is a message between two points that is used to inform one or both ends of the connection if there is a communication issue between the two points.

The various low-level controllers on the CAN bus (shutters, vents doors, azimuth etc.) have several levels of LifeLine messages. There is a LifeLine between the device and the CAN bus controlling PC that is used to ensure that the CAN bus correctly functioning. There is a LifeLine between the device and the Safety node that is used to ensure that the device knows the current safety relevant information of the system. There is a LifeLine between the devices and the high level software to ensure that something is controlling the enclosure. If any of these LifeLine messages fails to get to the devices they will take the appropriate safe action (depending on the Dome State above).

An example of a how this helps is: if the high-level software that is controlling the enclosure crashes while the enclosure is open the Application LifeLine will eventually timeout and the enclosure will close to protect itself.

4.2.1.4 *Personnel Safe*

The aim of Personnel Safe mode is to ensure that the only movement that will occur is as a result of some action that a person inside the dome has instigated. In practice this means turning off the autonomous (equipment protecting) movement, and limiting the number of places software commands can be issued. This limiting is implemented by restricting the IP addresses that various servers will accept commands from, ideally to only machines located physically inside the enclosure. As the dome is co-rotating it is best if Telescope motion is also limited, thus IP address filtering occurs on several servers, including: DomeServer; TelescopeServer; and the low level CANServers(s). As it is not up to the DomeServer to know about the Telescope Server the Personnel Safe functionality is implemented in a separate server that can act as a parent to all the above mentioned servers.

Personnel Safe mode is entered into when the server recognises that the Personnel Safe switch has been activated. The server will put the low level devices on the CAN bus into Personnel Safe mode by issuing a command to the Safety node, and it will inform the various servers to apply a set of IP addresses as a filter.

When the server recognizes that the key has become active it will start to flash the light inside the switch in order to indicate that it has seen the switch become active and is attempting to put the enclosure into Personnel Safe mode. It will issue the appropriate commands, and wait for all the relevant devices (shutters, azimuth and vent doors) to enter people safe mode. **Only when everything is in the correct mode will the server make the light stop flashing and stay on.**

The server will continuously monitor the state of the dome and will detect if any of the devices are no longer in Personnel Safe mode. At present the only action that will occur as a result of this is that the light will again flash. It is possible (and also safer) to make some sort of siren sound or light flash etc to notify any personnel that the dome is no longer in Personnel Safe mode.

The other issue with the current implementation is that modern networking bandwidth and tools like Remote Desktop and VNC allow a remote user to easily take control of machines that are inside the dome and issue commands as if they were standing in front of the local machine. There is currently nothing to prevent this. It is strongly recommended that the machines that will be used inside the dome are not accessed remotely for normal operations.

When DISENGAGING the People Safe mode, a thorough safety check of all moving interfaces is recommended:

- Shutters
- Vent Doors
- Drive Wheels
- Support Bogeys
- Seals (pier and ringwall)
- L1 Floor Edges (pier and outer edge)

Look for tools, debris, rags, displaced equipment, and fasteners.

5. SYSTEM OPERATIONS

5.1 Enclosure Start

Generally the system will be left in such a way that it will be possible to ‘start’ the system with a few simple software commands. If the system needs to have power switches toggled and buttons pushed in order to be ready for operations then it is not going to be particularly well suited to remote operations. As such, once the enclosure is fully commissioned and tested it will be normal to leave the system powered up and to use the software only to prepare and shutdown the enclosure.

5.1.1 Normal Start

Under these ‘normal’ conditions there is nothing to be done to prepare the dome for use. It should be possible to use the Dome GUI to enable and drive the various systems. Alternatively it should be possible for higher level software (either EOS or customer supplies) to start co-ordinating telescopes, shutters, vent doors etc.



Lick Power Distribution Switchboard



Azimuth Vector Drives at Lick



Lick Emergency Response Controls On Drive Cabinet



Lick Emergency Controls: ESTOP, E-RESET, Azimuth Override, End Of Travel Override

5.2 Enclosure Stop

The normal shut down procedure is to ensure that the shutters and vent doors are closed and all the drives are disabled. It is normal to leave the all software running and all the circuit breakers on; this is so that the system can be run remotely without the need for on-site personnel to be turning on/off circuit breakers.

5.3 Manual Controls

Each of the four vent doors and the combined shutters all have a manual control box so that the systems can be controlled manually by personnel on site and in the absence of any high level software. Each box consists of a backlit switch, which is used to select manual or software operations, and buttons used to control the direction of movement. When a device is in the Manual control state the control switch will have its LED illuminated and the buttons on the box will be the only way to control the device – the software will not be able to move the device, but will be able to monitor the status.

The boxes for the vent doors have Open and Close buttons which when depressed will move the vent doors in the respective directions. The shutter manual control box has forward (fwd) and reverse (rev) buttons for each of the front and rear shutters. The fwd button will drive the shutter towards the ‘front’ horizon (i.e it will drive the rear shutter towards the front shutter, or the front shutter away from the rear), and the rev button towards the rear (i.e. drive the rear shutter away from the front shutter, or the front shutter towards the rear).

The buttons that control the movement (Open, Close and fwd, rev) will only move the device while the button is depressed. In the case of the shutters the shutter will accelerate to a maximum speed (which is slower than the ‘normal’ software moves) and maintain this while the button is held. Releasing the button will cause an immediate stop; the shutter will apply the brakes and disable the motor. Care **must** be taken when using the shutter manual controls as the shutters will completely ignore all limits when being used in this way. It will be possible to drive the shutters into each other or into their end of travel limits. It is also a little tricky to correctly ‘close’ the shutters in this way and provide a correct weather seal.

The vent door manual control boxes are located near each vent door.



Manual Vent Door Controls

The manual control box for the shutters is located on the level 3 floor hanger beams.



Manual Shutter Controls

The azimuth may also have a manual override enable capability, this is a customer option. However as it is a co-rotating enclosure there are no Move buttons. The control consists of a single push button that will enable the azimuth drives, thus allowing the dome to follow, and align to, the telescope. It is used mainly during installation, when telescope input is unavailable.



Azimuth Enable Software Override: Lick

5.4 UPS

The enclosure contains an Un-interruptible Power Supply (UPS) on level 1. This will provide power to at least the shutters and vent doors along with their respective nodes, and the dome control PC. The UPS capacity is specified on a per site basis, but will generally be able to fully close the shutters and vent doors several times. If the system does not have UPS on the telescope and instrument(s) then any observations in progress when mains power fails will be spoiled as the telescope will no longer be able to track. The safety system has an input from the UPS to ensure that the dome closes a short time after the mains power fails. See the *E Secure Hold Off* section for more information. The dome will still be able to be controlled via software and manual commands while the mains power is down.



Lick UPS: Customer Supplied

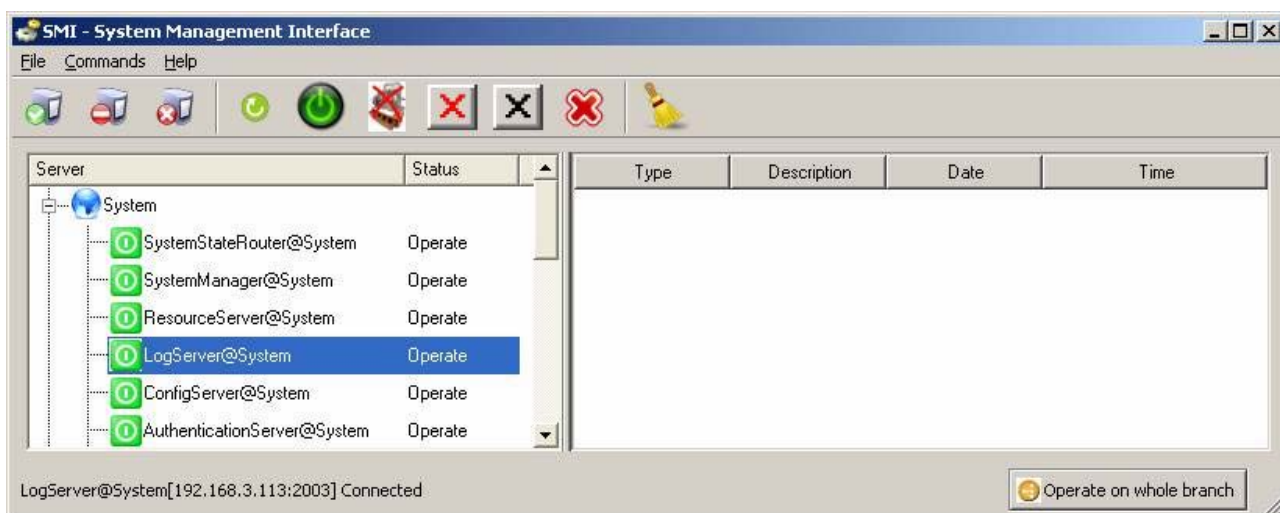
5.5 Software Controls

5.5.1 System Management Interface

5.5.1.1 Description

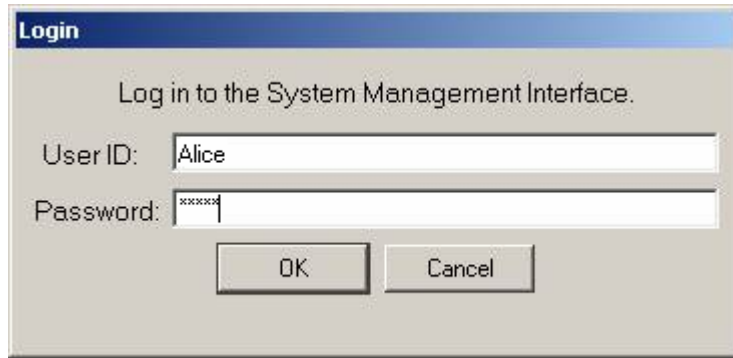
The System Management Interface (SMI) is an administrator-level tool for easily starting and stopping server applications on any machine on the network. It provides a status tree-view showing all servers and an events pane for feedback on commands the user issues.

As a general ‘user’ of the system it should not be normal to have to use this interface. If you find yourself starting and stopping the system (or parts of it) regularly please contact EOS for further advice.



5.5.1.2 Logon

When accessing the SMI you will first be asked to log on. However, this only happens if the core servers are running. Otherwise you will be prompted after the system is started. You will be presented with the following dialog box:




Enter a valid user name and password into their respective fields and click OK.

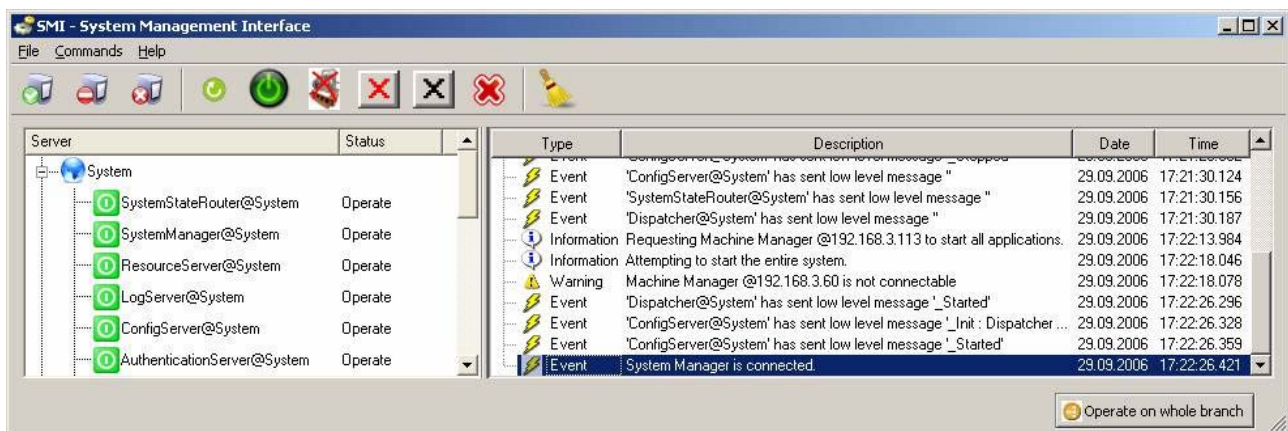
If you entered a valid user name and password then you will be presented with the System Management Interface.

If you entered an invalid user name and password pair then you will be informed, at which point you can try again:




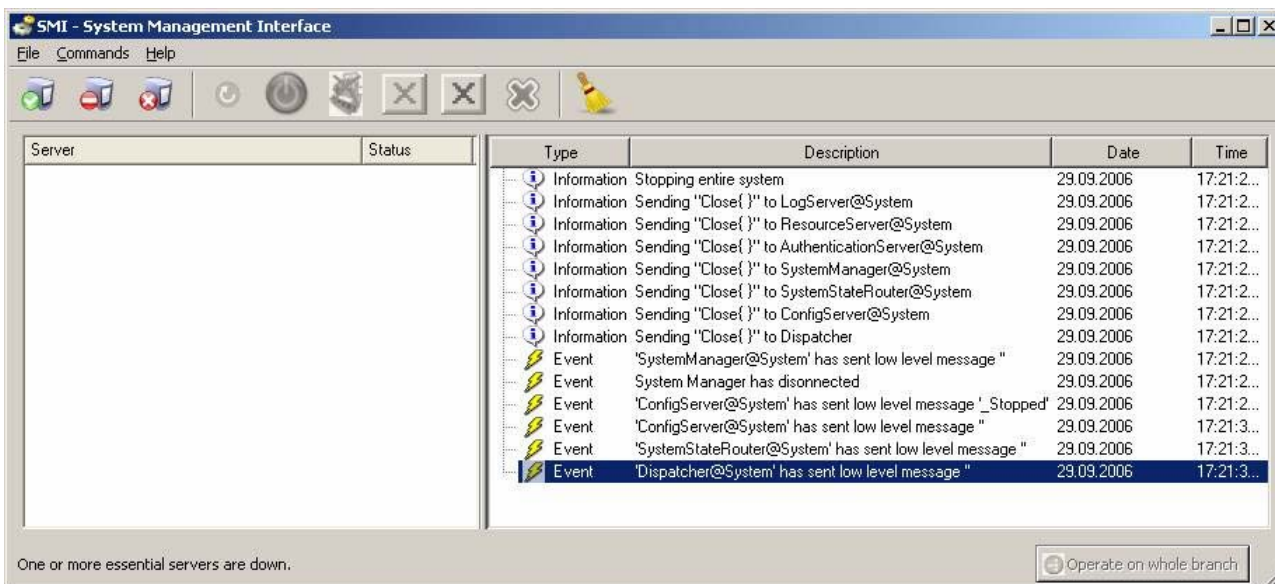
5.5.1.3 Starting the Observatory Control System

To start all if the server in the observatory click on the icon  “Start entire system”. The server tree view pane should be populated and the essential servers coloured green to indicate normal operation. Feedback will appear describing the startup. Then, if you have not already logged on, a logon dialog will be presented.




5.5.1.4 Stopping the Observatory Control System


To stop the observatory, click on the icon  “Stop entire system”. In the server tree view pane servers start changing to light grey, and then the tree view will disappear. Feedback will appear describing the shutdown.




5.5.1.5 Starting an Individual Server

Opening branches of the tree-view, the user can select individual servers. The user can then start that server by clicking the icon  “Start selected device server”. Feedback should appear in the events pane, and the server icon should become lit up.


5.5.1.6 Stopping an Individual Server

The user can close a server by selecting its icon, then clicking the icon  “Send non-forcible close command to selected device server”. This will only close the server if the server agrees to it. This is to allow servers running sensitive equipment to shutdown only under the correct circumstances. Feedback should appear in the events pane, and if the server closes the icon will change to light grey, otherwise it should be unchanged.


5.5.1.7 *Forcibly Stopping an Individual Server*

The user can close a server by selecting its icon, then clicking the icon  “Close selected device server forcibly”. This will close the server regardless of whether the server agrees to it. Feedback should appear in the events pane, and the server icon will change to light grey.

5.5.1.8 *Terminating an Individual Server*

The user can close a server by selecting its icon, then clicking the icon  “Forcibly terminate selected device server”. This will attempt a process-level terminate on the server regardless of whether the server agrees to it. Feedback should appear in the events pane, and the server icon will change to dark grey, indicating the server has not been correctly deregistered. To correctly deregister the server, the user should use the deregister command.

5.5.1.9 *De-registering an Individual Server*

If a server is dark grey in the tree-view (as will most likely occur if the Terminate is used), this means that the server is registered with the Dispatcher as currently operating, but the server is not contactable or has terminated. As long as a server is registered, other instances of the server will be prevented from starting. The user can deregister a server by selecting its icon, then clicking the icon  “Deregister selected device server from Dispatcher”. Feedback should appear in the events pane, and the server icon will change to light grey, indicating the server has been deregistered. However this command of itself does not guarantee the server process is actually terminated.

5.5.2 Dome User Interface

The Dome Client is a graphical user interface, provided to enable all common IceStorm Series II hardware functions to be accessed through software.

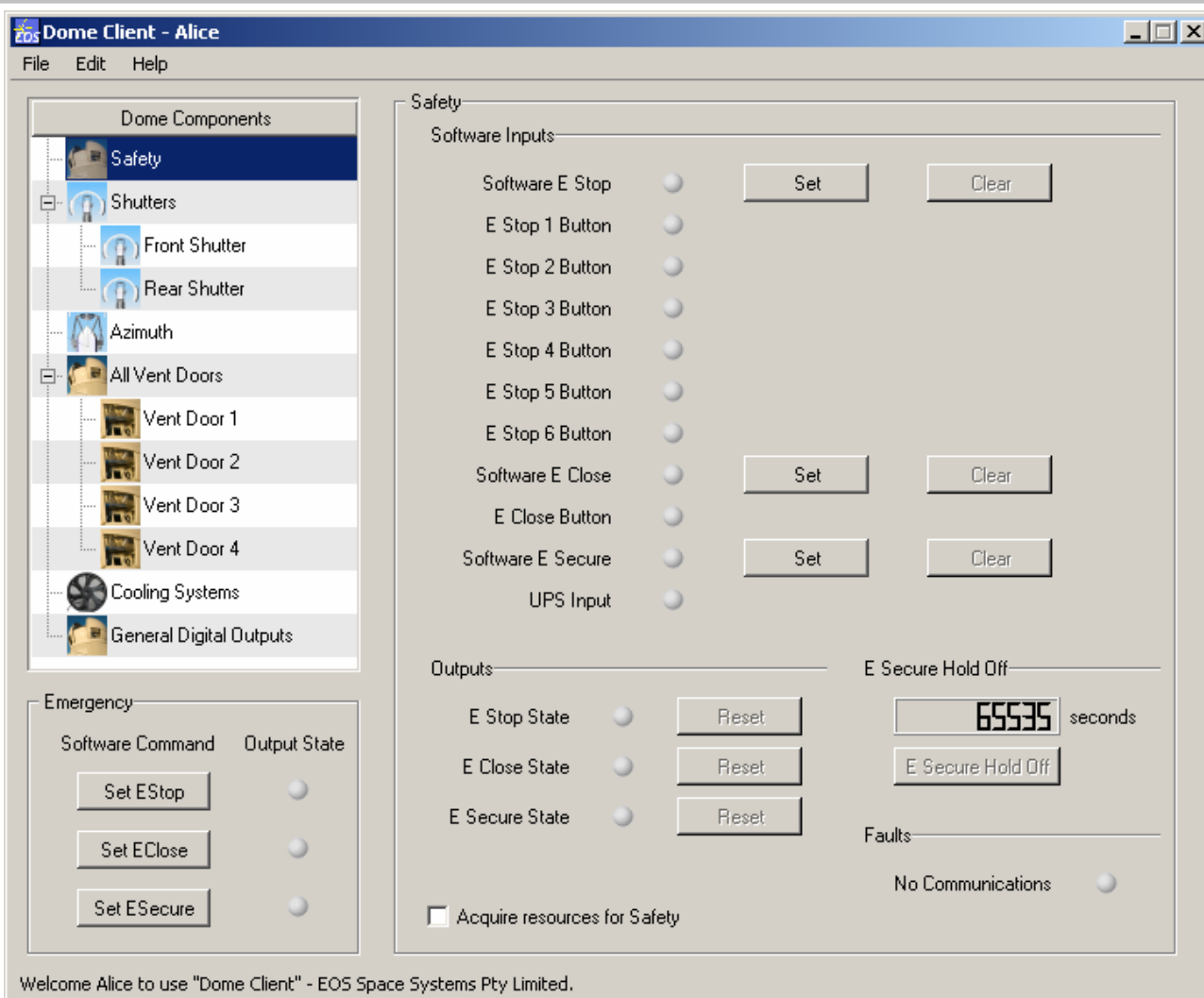
5.5.2.1 *Description*

The Dome Client presents the IceStorm II enclosure as a set of related sub-systems, including:

- Safety
- Shutters (Front and Rear)
- Azimuth
- Vent Doors (1 through 4)
- Cooling Systems
- General Digital Outputs

Each of these sub-systems is accessible through a dedicated control panel, accessed by clicking the required sub-system from the Dome Components list/tree.

The following figure shows the Safety control panel of the Dome Client:

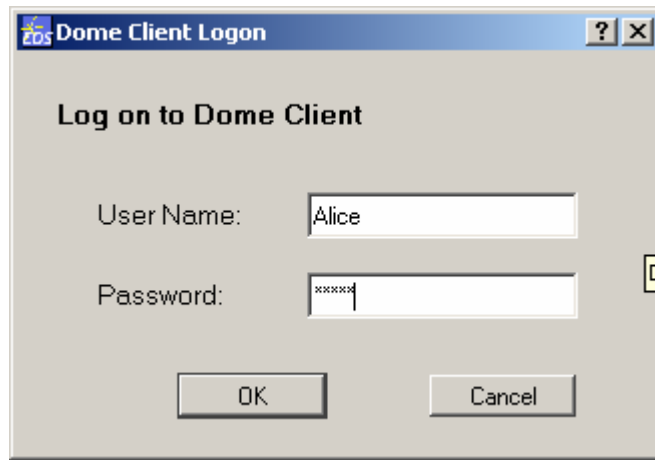


The major features of this interface include:

- buttons and checkboxes – submit commands to the Dome Server
- indicator lights – indicate status as reported by the Dome Server. These will illuminate as follows:
 - grey - connected, available, attribute not ‘active’
 - orange - not connected, no communication, attribute value not known
 - green - active state for this attribute (e.g. this vent door now open)
 - red – active, where this is generally a non-normal or error condition. For example an E-Stop button.
- text fields – show data reported by the Dome Server, and accept command parameters

5.5.2.2 Logon

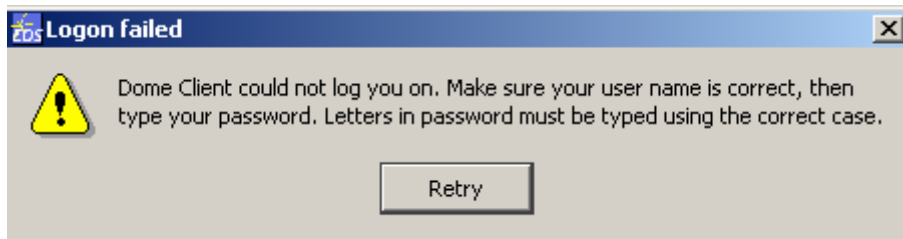
When accessing the Dome Client you will first be asked to log on. You will be presented with the following dialog box:



Enter a valid user name and password into their respective fields and click OK.

If you entered a valid user name and password then you will be presented with the Dome Client interface.

If you entered an invalid user name and password pair then you will be asked to try again:



5.5.2.3 General Features

5.5.2.3.1 Resource Acquisition

The software control system implements a facility called Resource Management. This facility makes it possible for a given user to take temporary ownership of various system resources, such as hardware devices. Once such a resource is owned by a user, certain aspects of its behaviour become unavailable to other users until the owner releases the resource. So Resource Management is relevant in the case of hardware or devices that may not be useable by two or more users at the same time.

The IceStorm Series II enclosure contains devices which cannot be safely or sensibly operated by more than one user at a time. In order to operate such devices you must acquire ownership of their resources.

The Dome Client makes this easy by presenting a checkbox on all control panels, labelled ‘Acquire resources for ...’. The exact label depends on the control panel being viewed. You will note that some of the buttons on the control panels are disabled until you have acquired the resources associated with that control panel.

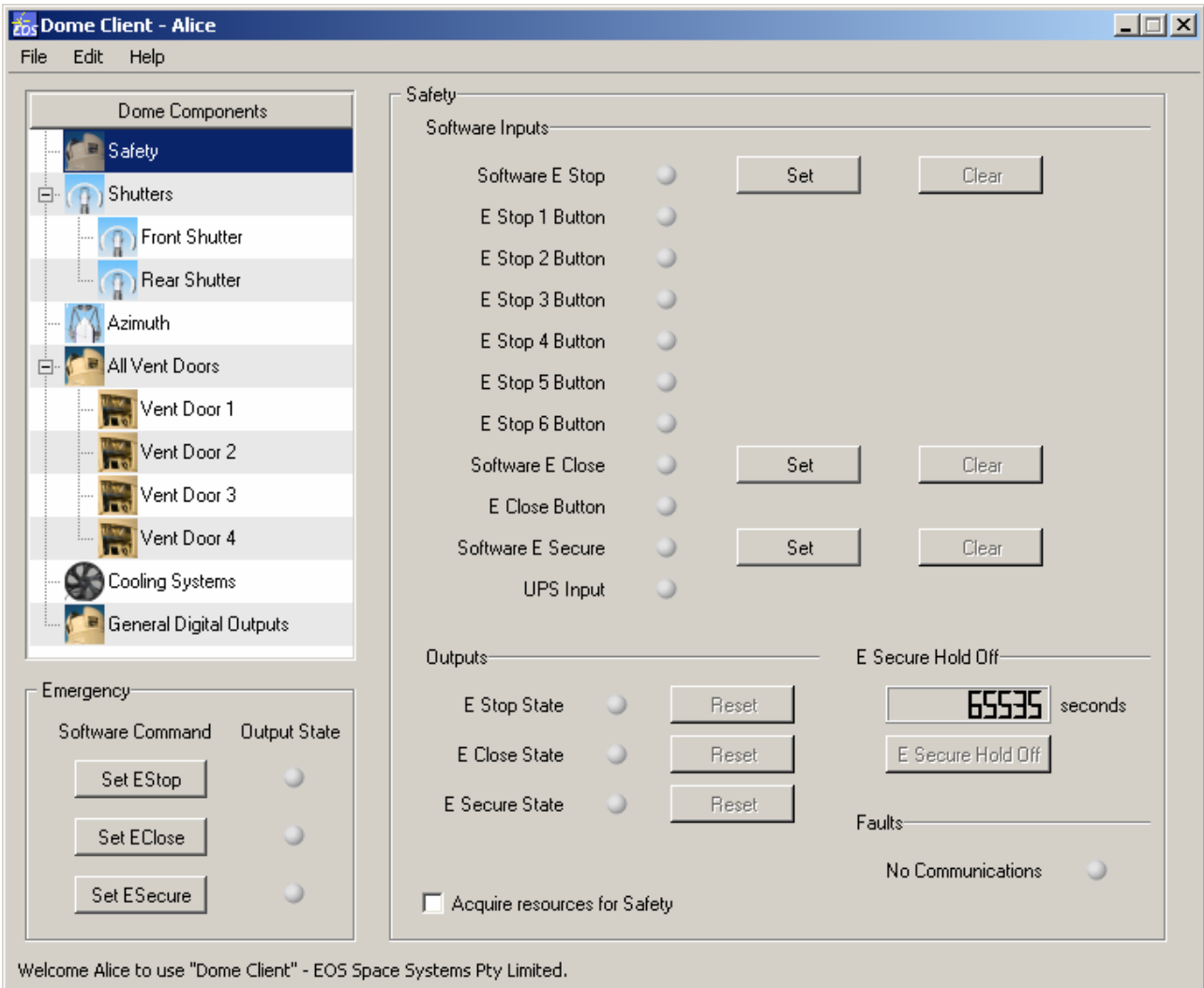
Other buttons are not disabled, even if no resources have been acquired. These buttons execute commands which do not require ownership of resources, and tend to include commands in the following categories:

- emergency stop
- get data

Emergency stop commands are typically not governed by Resource Management, as it would be unsafe to restrict these commands to only a single owning user (who may not be aware of the emergency, particularly if they are away from their screen or are using the system remotely). Note that while it is possible for any user to set an emergency stop, typically only the owner of the relevant resources can clear this condition.

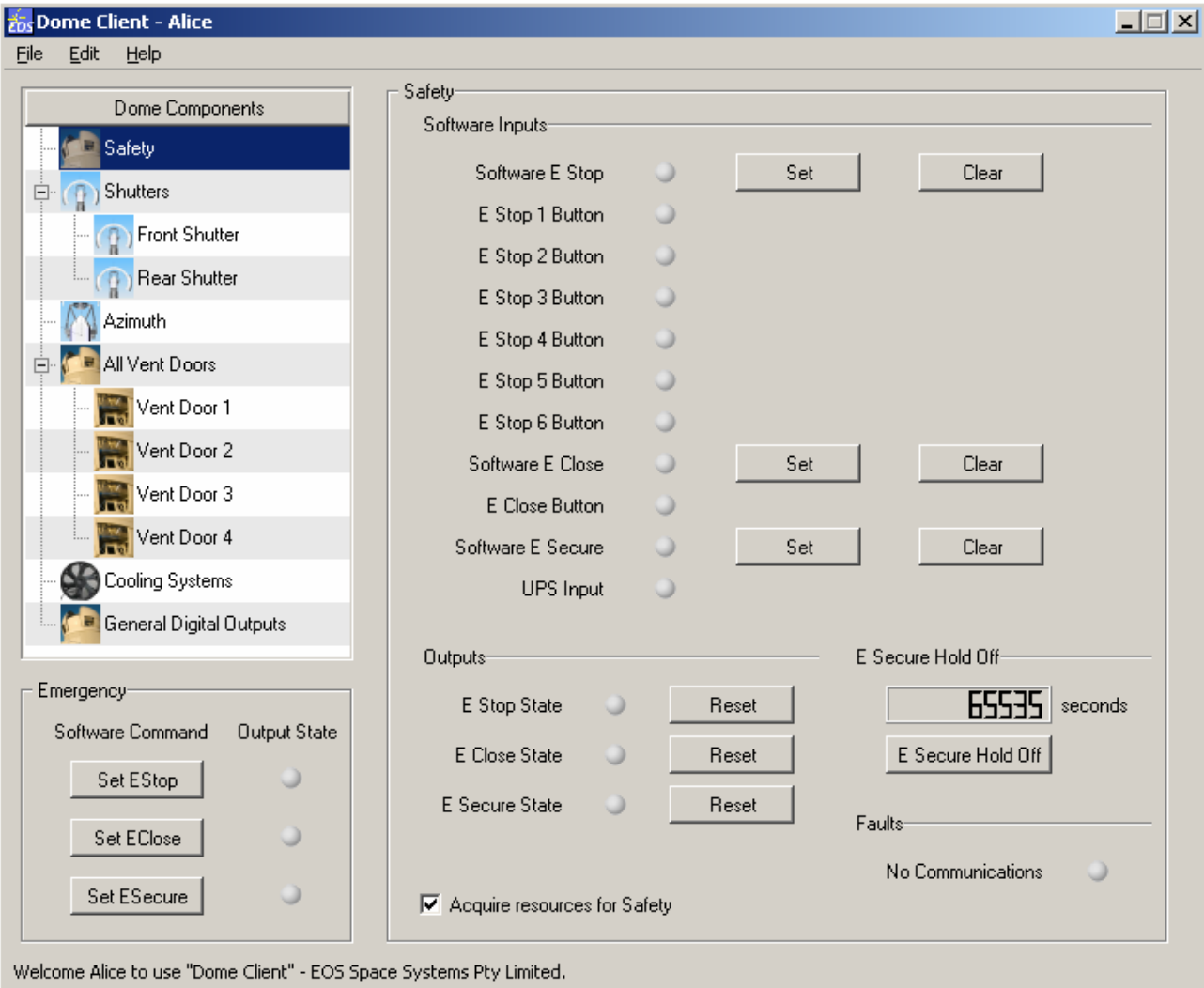
Get data commands typically do not alter the observable behaviour of devices and so are not usually subject to Resource Management.

As an example of acquiring resources, consider the basic Safety control panel:



Note that the buttons which Clear or Reset the various software emergency states are disabled. So is the button to set the E Secure Hold Off. These buttons require you to first acquire the control panel's resources.

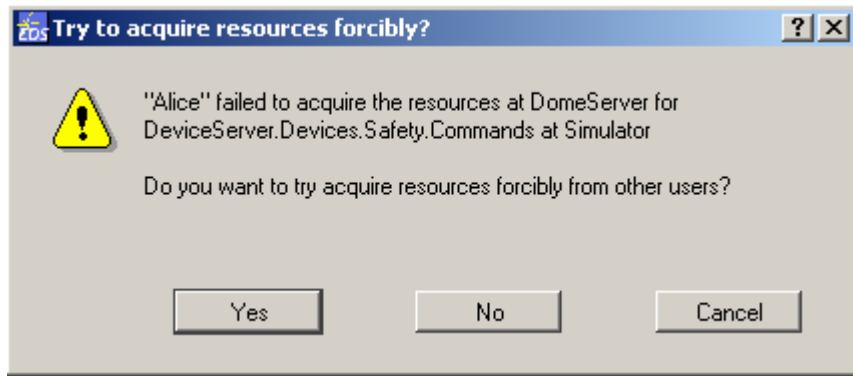
If you click the 'Acquire resources for Safety' checkbox, and if the resources are available, then you should see the following:



Note that the previously-disabled buttons are now enabled. As the owner of the resources you now have exclusive rights to execute these commands without interference from other users.

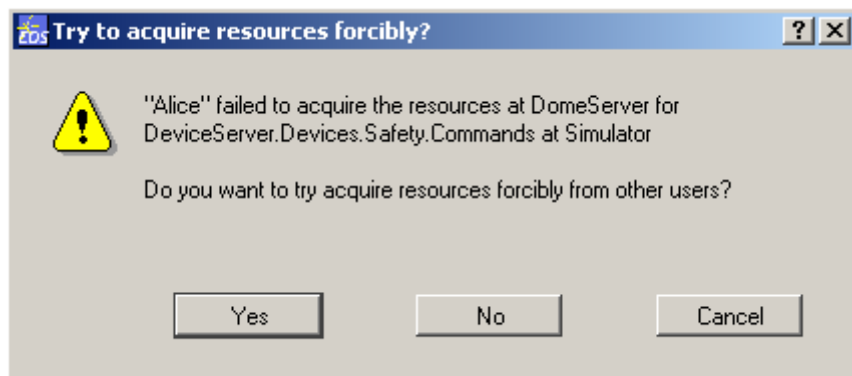
When you are finished with resources you should release them, by un-checking the relevant checkbox. If you close the Dome Client then all resources you held will be automatically released.

Should you try to acquire resources that are already owned, in general this will be denied and you will see the following dialog box:

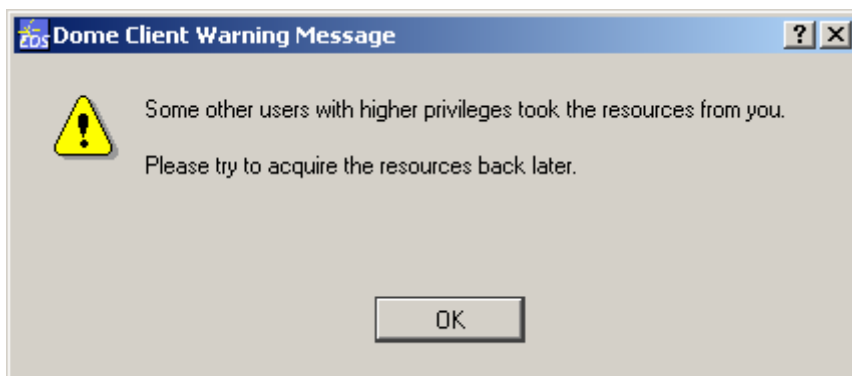


You can attempt to take the resources from their owner by clicking 'Yes'. Your attempt will only be successful if you have a higher *Rank* than the resource owner. If your attempt is successful then you will become the resource owner and the previous owner will lose their ability to execute the corresponding resource-managed commands.

If your attempt is not successful then you will be presented with the following dialog box:



As described above, it possible for a user of higher *Rank* to take resources from a user of lower Rank. Should a user of higher rank take a resource from you then you will be presented with the following dialog box:



5.5.2.3.2 Emergency Controls

All control panels within the Dome Client feature the following emergency command buttons (in the lower left hand corner of the window):

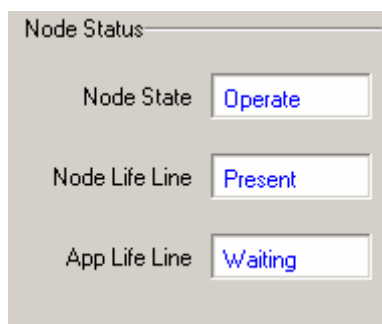
- Set E Stop
- Set E Close
- Set E Secure

When these commands are executed the corresponding Output State indicator will illuminate.

These controls are not resource-managed and so are available to all users at all times. These commands should only be used in an emergency situation and that you may interrupt the work of another user by executing them.

Note that these emergency conditions cannot be cleared except by the owner of the safety resources.

5.5.2.3.3 Node Status



The front and rear Shutters, the Azimuth and the Vent Door control panels all display some common status attributes. These are:

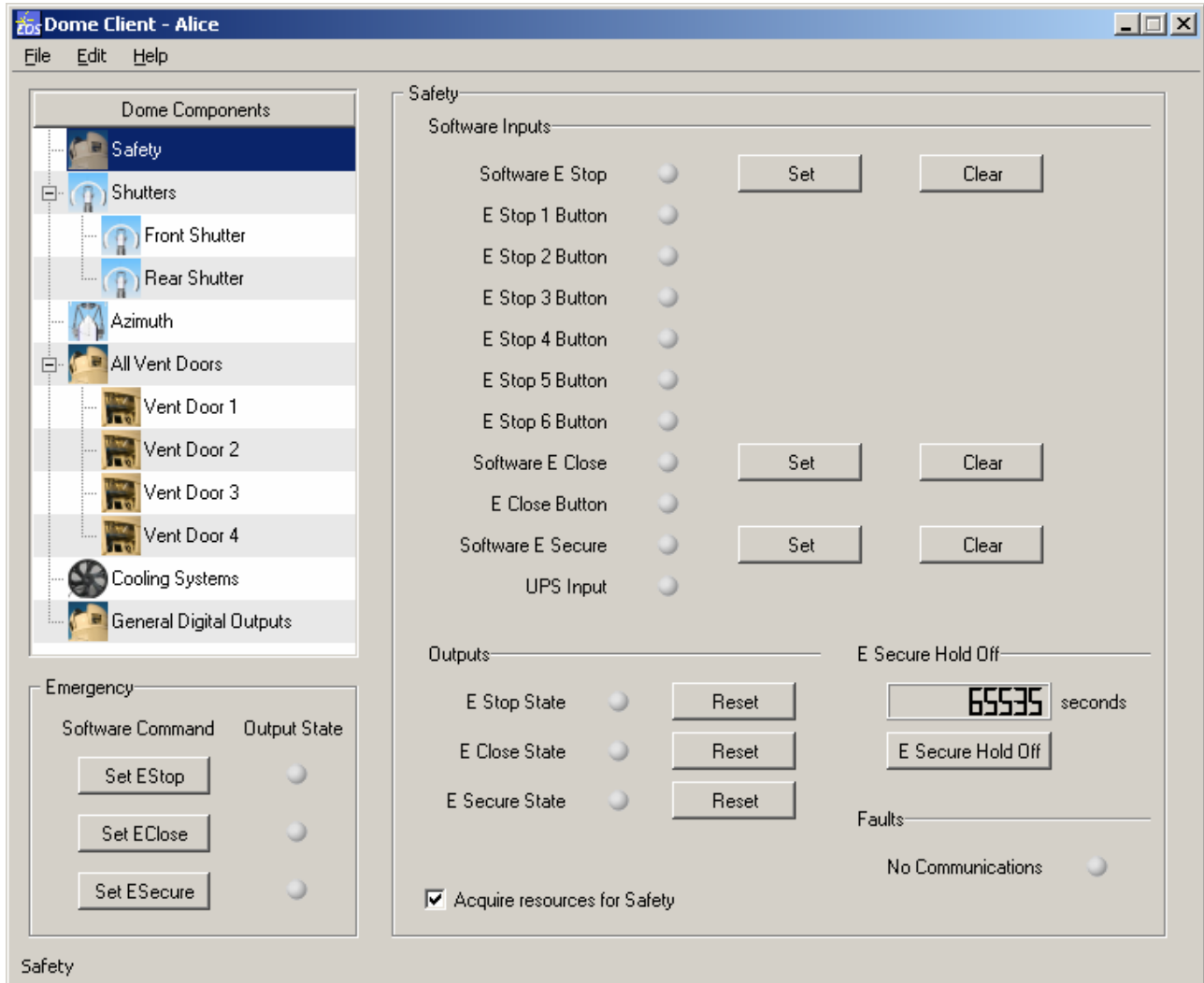
- Node Status – the basic node state. This will be one of:
 - Init – the node is initialising
 - Operate – the node is in some form of operating state. The Dome State will be one of: Manual Hardware; Manual Software Personnel Safe or Autonomous at this time.
 - Emergency – the node is in an emergency condition. The Dome State will be either E Close, E Stop or E Secure
 - Fault – the node is in some form of fault.

- Node Life Line – this displays the current status of the low-level node-to-CAN PC lifeline message. It will be one of:
 - Present – the lifeline message is being actively sent and received
 - Broken – the lifeline message has timeout out. The node will take some sort of safe action.
 - Waiting – the node is expecting to receive a lifeline message and is waiting for the first one. Until the first lifeline message is received the timeouts will not occur; this is to enable the system to start in a staged fashion without the lifeline breaking immediately.
 - Disabled – the lifeline is not being used as part of the safety system.
- App Life Line – this displays the current status of the application-level lifeline message between the node and the high level software controlling it. It can be the same set of values as the Node Life Line.

5.5.2.4 Safety

5.5.2.4.1 Description

The Safety control panel provides access to the safety functions and state of the IceStorm Series II enclosure.



This control panel includes the following controls and outputs:

5.5.2.4.2 Software Inputs

This tab has indicators and control for the various inputs to the safety system. The buttons, set and clear, are able to control the state of the respective software E condition input. The UPS Input is the only electrical input currently configured into the E Secure system. Each of the indicator lights

displays the status of the respective E input, from the various software inputs and buttons. A grey light means the condition is not active, red is active.

The UPS input may be red (Active) without the E Secure output being active. See E Secure Hold Off for details.

5.5.2.4.3 Outputs

Each of the E conditions (E-Stop, E-Close and E-Secure, see Safety Systems for details) is a latched state, in that once they become active they need for the input to become inactive **and** to be explicitly Reset before the output becomes inactive. This tab displays the status of the E condition outputs (which is mirrored in the Emergency tab to the left) and provides the Reset buttons to clear each of these outputs.

5.5.2.4.4 E Secure Hold Off

The E Secure system is implemented in such a way that each of the inputs (UPS only in this case) has a count down timer attached to it that must count down to zero before the output becomes active. This is to allow the user and any higher level software a chance to hold off on entering the E Secure state until they are ready. For example if the user is in the middle of taking a camera exposure and does not want to close due to mains fail until the exposure is complete. This feature should be used carefully as it is deliberately overriding an inbuilt safety system, and the user **must** be prepared to take full responsibility.

The display indicates the number of seconds until the E Secure output becomes active. If there are multiple active inputs then this will be the lowest of these. A value of 65535 indicates that no inputs are currently active.

The button will instruct the Safety node to restart all the active timers (in this case only UPS).

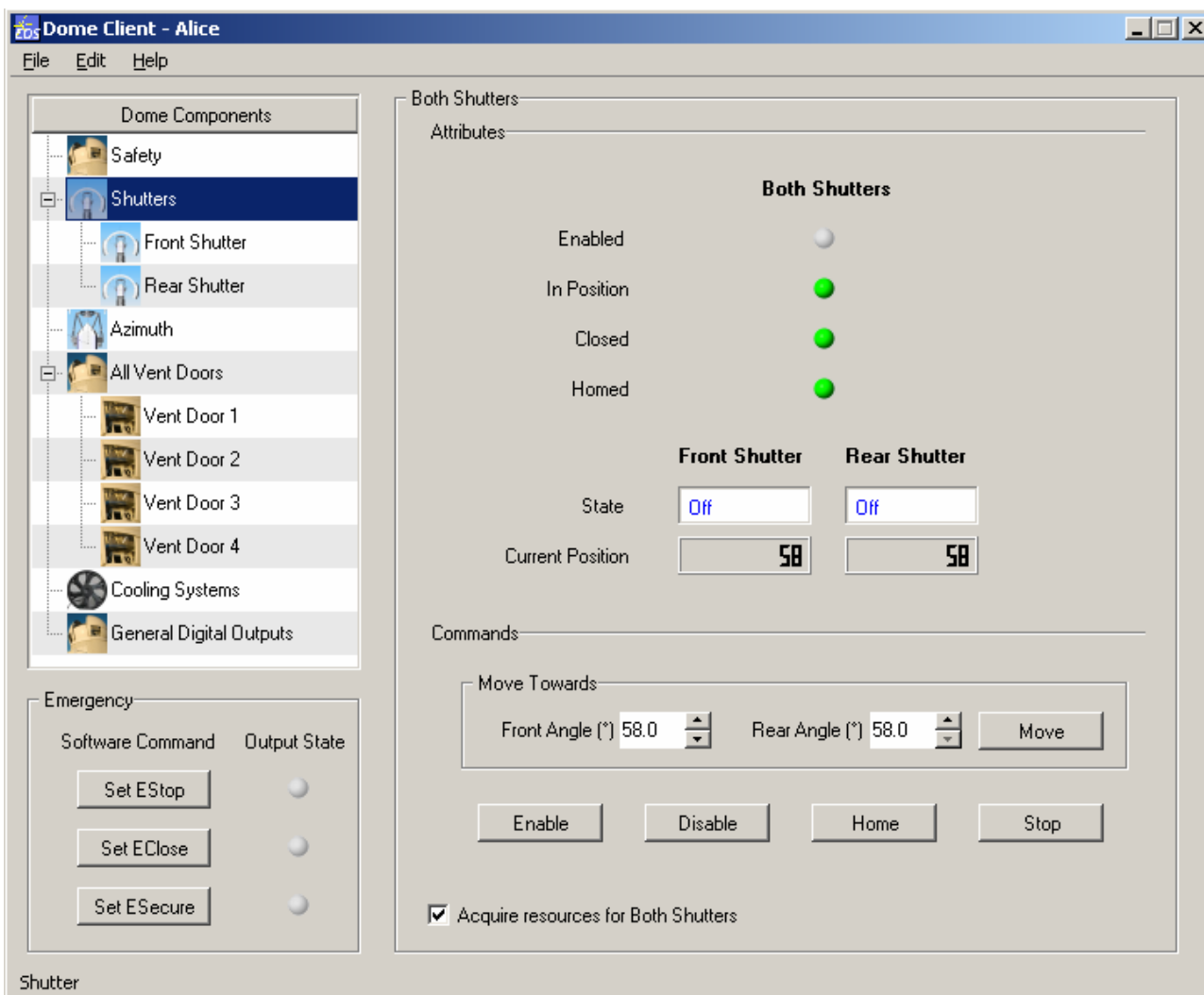
5.5.2.4.5 Faults

If the No Communications indicator is orange then Dome Client is not able to communicate with the server, if it is red then the server cannot communicate with the low level device. Operation of the enclosure via the Dome Client will not be possible until the communications issue is resolved.

5.5.2.5 Shutters

5.5.2.5.1 Description

The Shutters control panel provides access to the functions and state of both shutters of the enclosure.



This control panel includes the following controls and outputs:

5.5.2.5.2 Attributes

The indicators are as follows:

- Enabled – Will be active (green) if **both** front and rear shutters are enabled, grey otherwise.

- In Position - Will be active (green) if **both** front and rear shutters are in position, grey otherwise.
- Closed - Will be active (green) if shutters are 'closed'. The shutters are defined as closed when they are both at their home position and are touching. At this position they will be sealed.
- Homed – Will be active (green) if **both** front and rear shutters know their home position, grey otherwise. If the shutters do not know their home position they will **not** be able to be moved until a Home sequence has been successfully completed.

The State text boxes for each of the front and rear describe the state of the shutters internal state machine. Will be one of:

- Off – the drives are off and the brakes are applied.
- On – the drives are on, the brakes released, and the shutter is stationary
- Stopping – performing a controlled and profiled stop
- Homing – performing a home sequence
- Moving – performing a normal point to point move
- Stepping – not implemented
- Speeding – not implemented
- Fault – not implemented
- Invalid – the state can not be ascertained

The Current Position text boxes display the current position of each of the front and rear shutter. These will only be valid if the shutter has been homed.

5.5.2.5.3 Commands

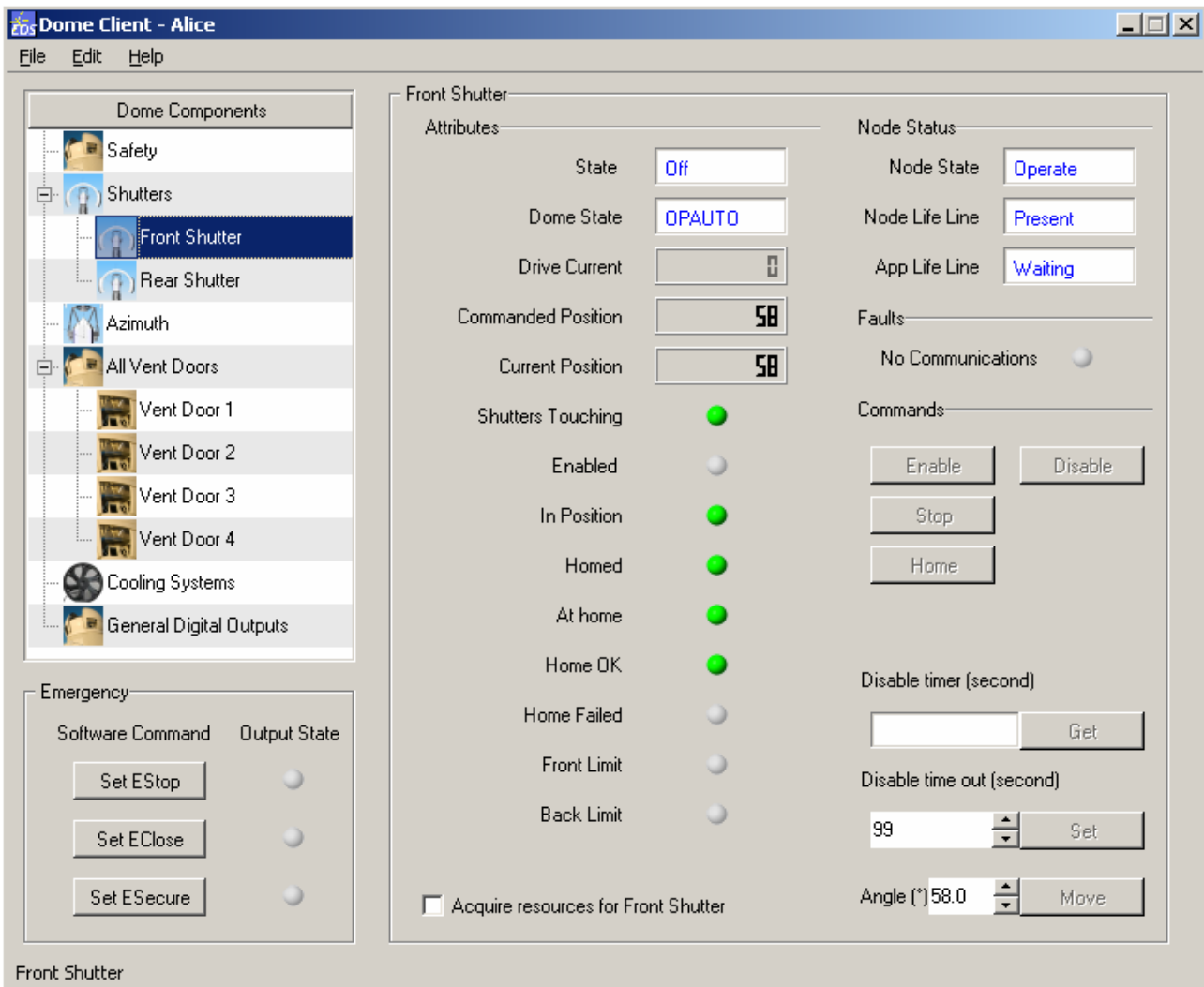
Each of these commands will act on **both** the front and rear shutters.

- Enable - will enable both shutters
- Disable - will disable both shutters. If they are currently moving this will produce a harsh stop with the brakes being immediately applied.
- Home - will perform a homing sequence on both shutters. It may be necessary to enable the shutters before this command will be accepted, see E Secure Hold Off for more details. If **both** the shutters are touching and they are both "At home" then the shutters will use their current position as the home position.
- Move - The positions for the move commands are measured in degrees from the 'front' horizon. The two input (spin) boxes contain the desired angles. It may be necessary to enable the shutters before this command will be accepted, see E Secure Hold Off for more details.
- Stop – stops the motion of both shutters. This will be a controlled/profiled stop.

5.5.2.6 Front / Rear Shutter

5.5.2.6.1 Description

These two control panels provide access to the individual shutters. The interfaces for the front and rear shutters are identical. These control panels provide a more detailed set of controls and feedback than the combined shutters panel.



5.5.2.6.2 Attributes

This tab displays textual feedback for the following:

- State – The current internal shutter state. See **###Error! Reference source not found.** for details
- Dome State - the current Dome State (see 4.2.1.2 for details) of the selected shutter.
- Drive Current – not implemented
- Commanded Position - the position (in degrees from the ‘front’ horizon) the shutter was last commanded to. If the shutter has not yet been commanded to a position (since it has been powered up), this value will be invalid.
- Current Position - the current position (in degrees from the ‘front’ horizon) of the shutter. If the shutter has not been successfully homed (ie the Homed indicator is not green) then this value will be invalid.

And the indicators for:

- Shutters Touching - indicates if the front and rear shutters are touching. This may occur at any position, and even if the shutters are moving.
- Enabled – The current enabled status of the shutter. If enabled then the drive is active (servo’ing) and the brakes are released.
- In Position – the shutter is at the position it is supposed to be.
- Homed – the shutter knows where the Home position is. This is important because the system uses a relative encoder system, thus needs an absolute reference point (home) to be able to achieve absolute positioning.
- At home – the shutter is currently at its home position. Note that this means that the home switch is being activated by the home dog, which is true for a relatively large movement (several centimetres).
- Home OK – the last Home command completed successfully
- Home Failed – the last home command failed.
- Front Limit – active if the shutter has reached its front end-of-travel limit. If this occurs while moving then the shutter will immediately transition to the Off state and will apply the brakes. Assuming the shutter has been homed it will be possible to re-enable the shutter and command it to a position that is moving out of the limit, i.e to a larger angle. Under normal

conditions the software should not allow a move that will reach this limit. If you are able to use this interface to drive the shutter into the limit please contact EOS for further advice.

- Back Limit – same as the Front Limit except to recover you will need to move to a smaller angle (i.e towards the front).

5.5.2.6.3 Commands

This tab provides the ability to control the shutter, specifically to:

- Enable - will enable the shutter. If the shutter was Off this will transition it into On, activating the motor drive and releasing the brake.
- Disable - will disable the shutter. If it is currently moving this will produce a harsh stop, with the brakes being immediately applied. The shutter state will transition to Off.
- Stop - will stop the shutter. If is moving the state will transition to Stopping, then On once the move is complete.
- Home - will perform a homing sequence on the shutter. This involves moving the shutter to find the edge of the homing dog. If **both** the shutters are touching and they are both “At home” then the shutters will use their current position as the home position. . It may be necessary to enable the shutters before this command will be accepted, see Disable Timeout below for more details.
- Get Disable Timer - not implemented
- Set Disable Time Out - the low level shutter node will not accept a move command if the shutter is in the Off state. The DisableTimeout allows the server to automatically enable the shutter before issuing a Move (or Home) command, and it will disable the shutter “seconds” seconds after the move has completed (it will actually disable it once the shutter has been in the On state for “seconds” seconds, so if you send an enable and no move it will still be disabled automatically). A value of zero (0) will disable this feature.
- Move - sends the shutter to the desired angle. Depending on the Disable Timeout (see above) the shutter may need to be enabled before this command will be accepted.

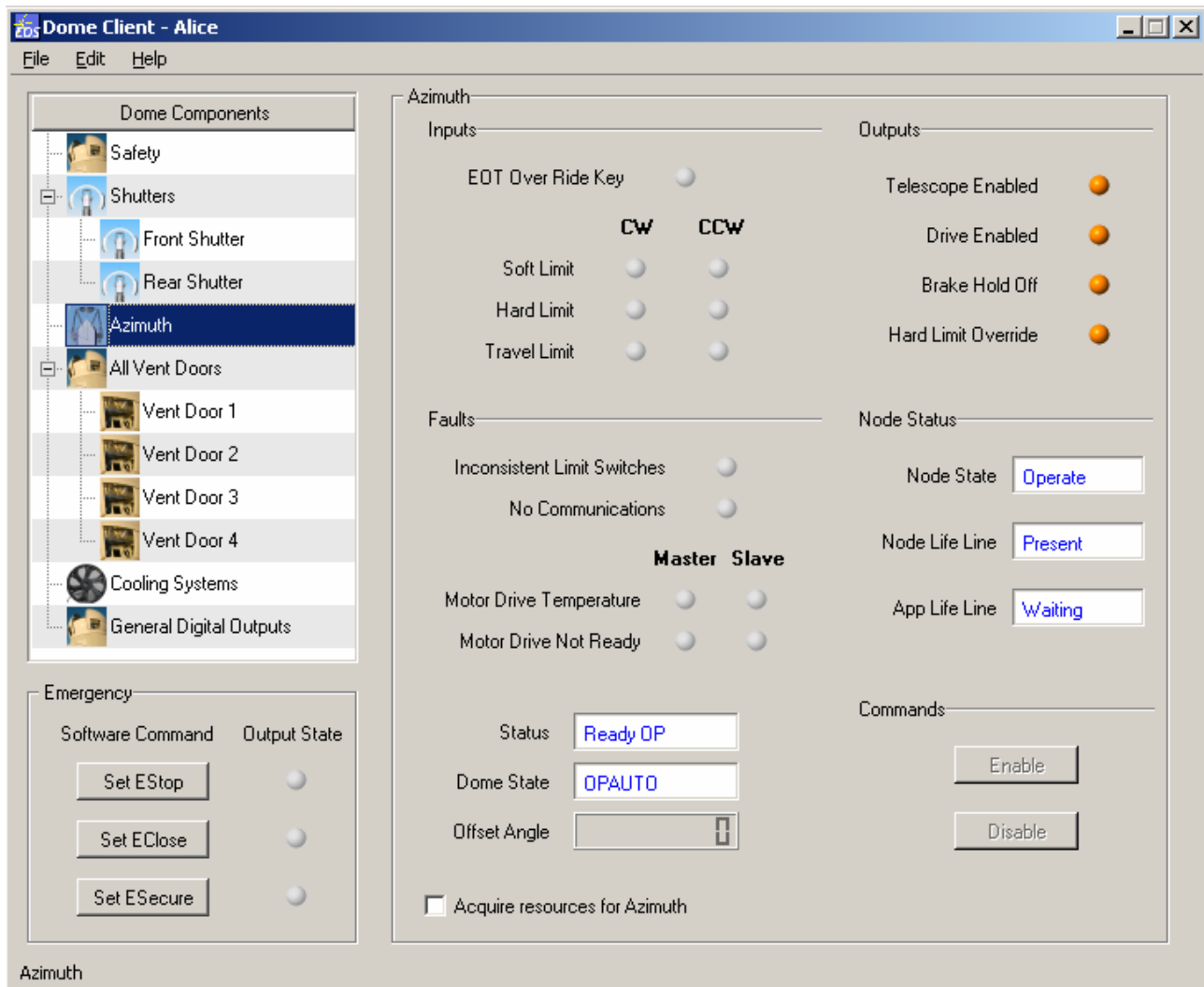
5.5.2.6.4 Faults

If the No Communications indicator is orange then Dome Client is not able to communicate with the server, if it is red then the server cannot communicate with the low level device. Operation of the enclosure via the Dome Client will not be possible until the communications issue is resolved.

5.5.2.7 Azimuth

5.5.2.7.1 Description

This control panel provides controls and feedback for the Azimuth sub-system of the IceStorm Series II enclosure. This enclosure is co-rotating, so will follow the azimuth rotation of the telescope if it is enabled. As such the interface is fairly simple, with the ability to enable and disable it and nothing else.



5.5.2.7.2 Inputs

- EOT Over Ride Key - the status of the End-Of-Travel override key switch. This key switch is used as part of the end of travel recovery procedure, see the Enclosure End Of Travel recovery section for more details.
- Soft Limit (Clock-Wise and Counter-Clock-Wise) - the status of the relative 'soft' limits between the telescope and dome. Under normal circumstances the dome should be able to maintain alignment, however various conditions may cause this limit to become active. The dome should attempt to prevent further movement into this limit by either slowing itself down (assuming it is overtaking the telescope) or by disabling further movement of the telescope in the direction of travel (assuming the telescope is going faster than the dome).
- Hard Limit (CW and CCW) - the status of the relative 'hard' limit between the telescope and dome. This is serious enough that the dome will disable power to the drives when this input becomes active, and will require a new Enable command to be issued (and thus a new alignment phase where the dome will align to the telescope).
- Travel Limit (CW and CCW) - the status of the absolute travel limits of the dome. These are **very** serious limits to be active. If the dome can get into either of these limits then there has been several safety mechanism failures including telescope software limits, and telescope end of travel limits. If either of these limits becomes active the dome will immediately remove power from its drives and signal the telescope to stop. There is a specific recovery procedure to follow if these limits become active, as at this point in the travel it is close to causing mechanical damage to the cable chain. See the Enclosure End Of Travel recovery section for details. If this limit becomes active please inform EOS.

5.5.2.7.3 Faults

- Inconsistent Limit Switches - this indicates if the various input switches are in an inconsistent state. For example if both the CW and CCW EOT switches are active.
- No communications - If the No Communications indicator is orange then Dome Client is not able to communicate with the server, if it is red then the server cannot communicate with the low level device. Operation of the enclosure via the Dome Client will not be possible until the communications issue is resolved.
- Motor Drive Temperature (Master and Slave drives) - indicates the status of the temperature of the motors, will be red if in error, grey otherwise. The azimuth system uses two drives, Master and Slave, to provide adequate power to move the dome.

- Motor Drive Not Ready - indicates the readiness of the drives. The drives in this system provide the majority of the functionality and intelligence. If either of them are not ready then the azimuth will be in either Disable or Fault state.

5.5.2.7.4 Outputs

This tab is not implemented and the indicators will always be orange.

5.5.2.7.5 Status feedback

- Status - the current internal state of the azimuth node. This will be one of:
 - Disabled – this is the startup and recovery state. In this state the drives are off and dome will not follow the telescope.
 - EStop – the azimuth is in an EStop condition (as should the rest of the dome be).
 - Ready OP – The azimuth is ready to operate. In this state the azimuth is able to communicate with its drive motors, and is ready to be enabled.
 - Align – the azimuth has been enabled and is establishing the initial alignment between the telescope and dome. As soon as it has done this (the relative limits are no longer active) it will transition to Run
 - Run – the azimuth is active and will follow the telescope.
 - EOT Recovery – the device is in the End-Of-Travel recovery state. This means that the azimuth was at one end of travel and the EOT key switch was active when the Enable command was issued. This state will remain active until the EOT Key switch is de-activated.
 - Fault – this state is entered into whenever a fault condition is detected in any other state. A fault may be a problem with the drives or an invalid combination of input switches
 - Drive Recovery – entered into whenever a ResolveFault or Reset command is received while in the Fault state.
- Dome State - the current Dome State (see 4.2.1.2 for details) of the azimuth.
- Offset Angle - not implemented.

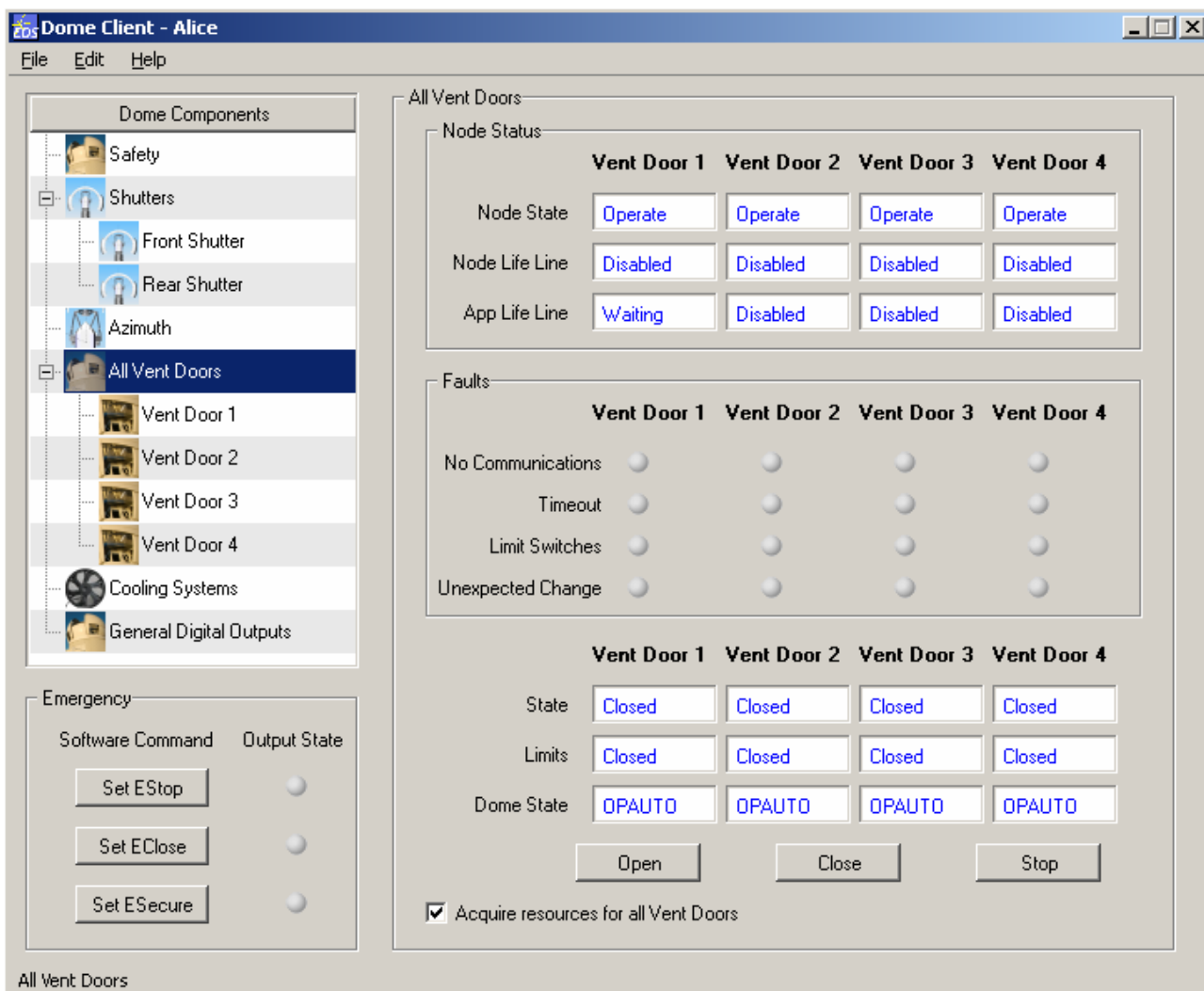
5.5.2.7.6 Commands

- Enable - this will enable the domes azimuth drive, thus allowing the dome to centre itself on the telescope. If there is any offset between the dome and telescope when this command is issued the dome will 'jump' to correct it. Once enabled the dome will follow the telescope.
- Disable - will disable the domes azimuth drive. The drive will be disabled, and the signal between the dome and the telescope enabling movement in the telescope azimuth will be de-activated, thus effectively stopping the telescope in azimuth. If the dome is moving when this command is issued then the dome will coast to a halt (though it will do this fairly quickly), and it may be possible for the dome and telescopes relative alignment to be lost.

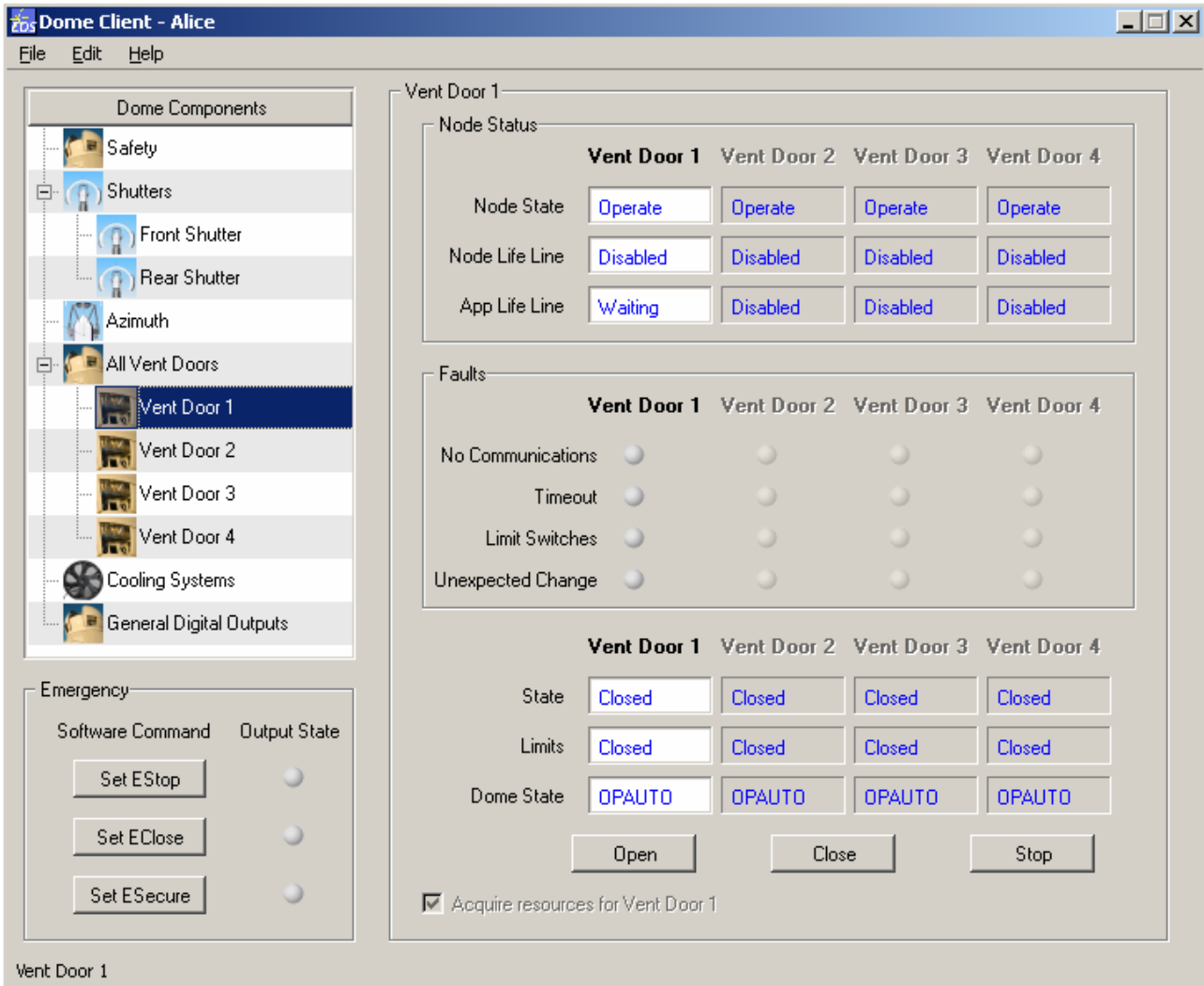
5.5.2.8 Vent Doors

5.5.2.8.1 Description

This control panel provides access to control and monitor all the vent doors simultaneously. The functionality of the buttons is the same as for each individual vent door.



5.5.2.9 Vent Door 1 – 4



5.5.2.9.1 Description

These control panels allow control and monitoring of the vent doors. All of the panels will display the status of all of the vent doors, however depending on the selected panel you will be able to control either all door simultaneously, or only the selected door.

5.5.2.9.2 Faults

- No Communications - If this indicator is orange then Dome Client is not able to communicate with the enclosure, if it is red then the server cannot communicate with the low level device.
- Timeout – the request move took longer than the required time.
- Limit Switches – the input switches are in an invalid state (eg both Opened and Closed)
- Unexpected Change – the limit switches changes state when not expected to do so.

5.5.2.9.3 State feedback

- State - the current state of the vent's internal state machine. Will be one of:
 - Stopped – the vent door is not moving and is not either Opened or Closed.
 - Opened – the door is stopped at the Opened switch
 - Closed – the door is stopped at the Closed switch
 - Moving Open – the door is moving towards the Opened position
 - Moving Closed – the door is moving towards the Closed position
 - Fault – the door is in a fault state, see fault Indicators above.
- Limits - the current status of the vent doors limit switches. Will be one of:
 - Stopped – no switches active
 - Opened – the opened position switch active
 - Closed – the closed position switch active
 - Fault – in a state the is not logical/possible
- Dome State – the current Dome State (see 4.2.1.2 for details) of the vent door(s)

5.5.2.9.4 Commands

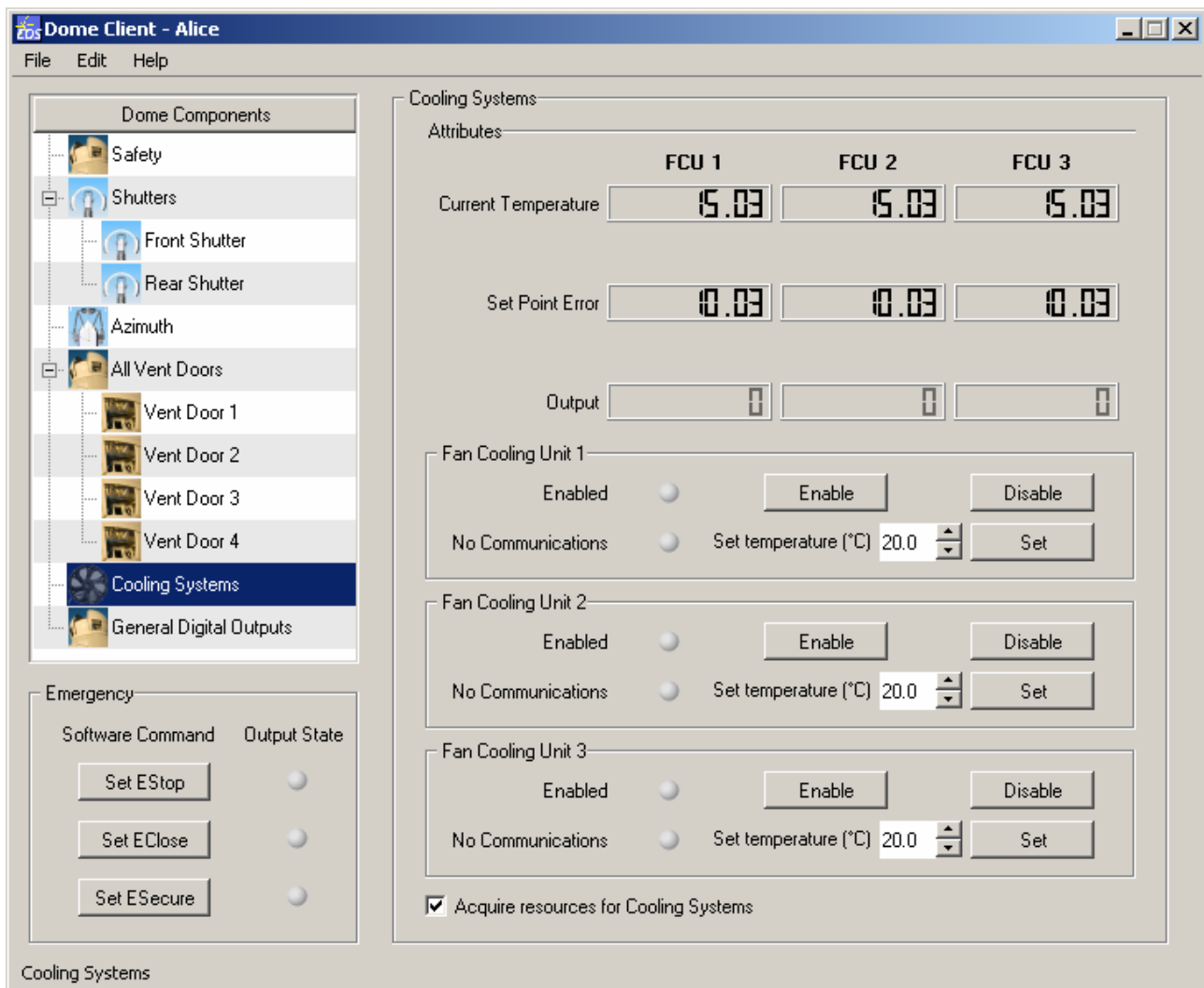
- Open - will cause the selected vent door(s) to open. If already open the command will be ignored.
- Close - will cause the selected vent door(s) to open. If already open the command will be ignored.
- Stop - will cause the selected vent door(s) to open. If already open the command will be ignored.

5.5.2.10 Cooling Systems

5.5.2.10.1 Description

The cooling system is made up of three (semi) independent Fan Control Units (FCU). FCU 1 is located in the equipment space and as such is not directly related to optical seeing. FCUs two and three are both in the observing space, so should be set to similar (if not the same) values to avoid them fighting each other.

The controls for all three FCUs behave identically.



The aim of the cooling system is to precondition the inside of the dome, particularly the sensitive optics, to the expected temperature at the time the enclosure is opened (or when observations will be started).

5.5.2.10.2 Attributes

- Current Temperature - indicates the current input temperature of the FCU. This input temperature will generally be averaged over sensors throughout the space, and will be averaged over several readings.
- Set Point Error - the difference between the set point and the current temperature. Ideally in a system that is Enabled and well tuned this will be zero, or very small.
- Output - the percentage output the system. This is the opening of valve that is regulating coolant through the cooling coil.

5.5.2.10.3 Indicators

- Enabled - the status of the system. If enabled then the system will turn on the fan to move air through the coil, and will regulate the coil temperature in order to ensure that the current temperature is equal to the set point temperature.
- No communications – If this indicator is orange then Dome Client is not able to communicate with the enclosure, if it is red then the server cannot communicate with the low level device.

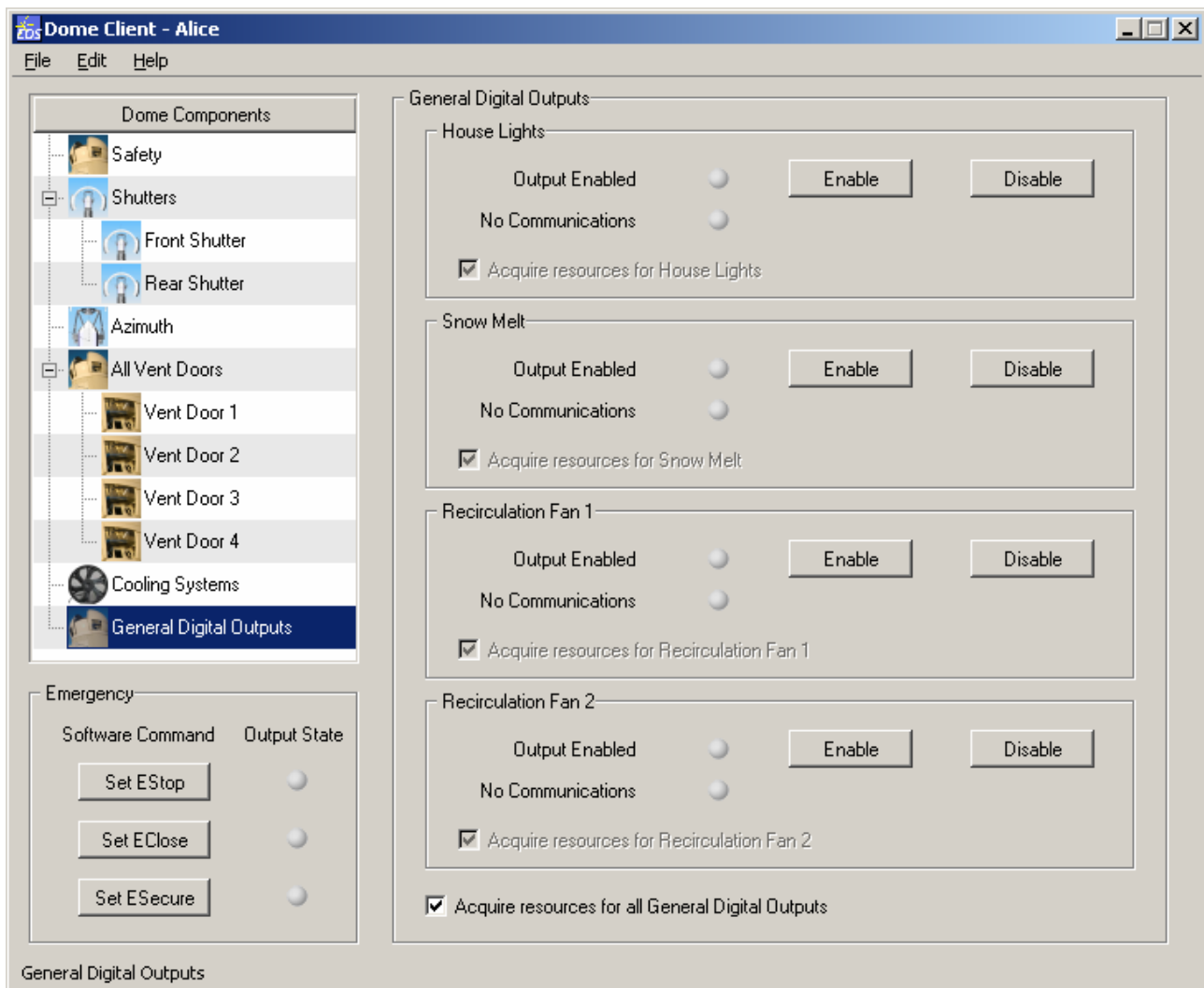
5.5.2.10.4 Commands

- Enable - enable the cooling system. Will turn on the fan and regulate the coil temperature.
- Disable - disable the cooling system. Will turn off the fan and stop coolant flowing through the coil.
- Set - set the desired set point. This is the temperature the system will attempt to maintain. As this is a cooling only system a set point that is above the current temperature will not be achievable.

5.5.2.11 General Digital Outputs

5.5.2.11.1 Description

This control panel provides controls and feedback for the systems connected to the low level Digital Input/Output node. These all have a very simple control interface, in that they can be Enabled and Disabled, and they only have a single status indicator which shows the loop-back status of the output.



5.5.2.11.2 House Lights

The ability to control the house lights will vary from enclosure to enclosure as per site specific requirements.

- Output Enabled – this indicates the current status of the feedback of the house lights system. The indicator will be active (green) if any of the lights are on. This may vary on a per site basis.
- Enable – this will turn on all the lights connected to the system. It will not hold them on, so a user inside the enclosure may manually turn a specific light off using manual controls. This may vary on a per site basis.
- Disable – this will turn off all the lights connected to the system. It will not hold them off, so a user inside the enclosure may manually turn a specific light on using manual controls. This may vary on a per site basis.

5.5.2.11.3 Snow Melt

The “Snow Melt” is a cable running through both cable troughs of the shutters. The aim is to be able to melt any snow and/or ice that forms in this trough and prevent damage to electrical cables and the main shutter chains. It is up to the user or higher level software to control this system.

- Output Enabled – this will be true if both of the cables are active and heating
- Enable – turn on both cables
- Disable – turn off both cables

5.5.2.11.4 Recirculation Fan 1 and 2

- Output Enabled – will be true if the fan is powered
- Enable – turn on the fan
- Disable – turn off the fan

6. ENCLOSURE END OF TRAVEL RECOVERY

6.1 Overview

This section discusses the various azimuth movement limits, and how they are guarded by software based on digital inputs from limit switches. If several safety systems fail or are bypassed, a final hardware safety system comes into play, and recovery requires a higher level of care, as described below



Lick Emergency Controls: ESTOP, E-RESET, Azimuth Override, End Of Travel Override

6.2 Normal Operation: Telescope Movement Limits

Typically the higher level commands to the enclosure come from two sources:

- The enclosure interface allows the manual control of all telescope independent parts, such as shutters and vent doors.
- The telescope control computer may move the telescope, and the enclosure will follow the azimuth movement, using trimming feedback from the interface beam potentiometer. Shutters may also be controlled in a tracking mode if not opened fully.

The co-rotating enclosure will monitor its relative azimuth position to the telescope. If the proximity switches on the interface beam are tripped by a failure to follow the telescope correctly, the following actions will occur in the low level enclosure firmware:

Activation of the inner proximity switches will disengage telescope power in the direction causing the violation.

Activation of the outer proximity switches will have the same effect, with telescope servo power being removed by a latched switch. Pushing the telescope back into its limits by hand will remove the fault condition.

If the telescope rotates too far (as compared to enclosure following errors described above), then it will trip its own inner limit switches, called End Of Travel (EOT) limit switches. In this zone the software will stop movement and allow commands only in the recovery direction. A set of outer limit switches exist beyond the End Of Travel switches: these are known as Failsafe Limits. Once these are tripped, all telescope power is removed from servo systems, and the telescope must be repositioned by hand in its operating range.

6.3 Enclosure Failsafe Operation

However, the telescope can still be pushed by hand through both EOT and FS limits, and the enclosure will follow faithfully, until the cable chain end of travel is reached and the cables are destroyed. To prevent this, the cable chain itself has End of Travel limit switches: if these are tripped, enclosure drive power is cut off by a shunt trip circuit breaker in the main power distribution box. To recover, users must hold the Azimuth EOT Override key outside the enclosure drive cabinet, then reset the breaker and push the telescope back into its operating range. The Azimuth EOT Override key switch may then be released.

7. COMMON ENGINEERING PROCEDURES

Most common engineering procedures relate to periodic maintenance, and enclosure activities are covered in the Icestorm II Maintenance Manual HBO-7753. However, some observatory level engineering procedures are related to telescope calibrations. These will be described in future releases of this document, and will describe current operational techniques for such operations as:

- Star Calibration of the telescope
- Nasmyth or Cassegrain derotator calibration for optical axis location
- Collimation checking
- Active compensation calibration, as applicable, for:
 - Focus vs temperature
 - M2 tilt vs elevation/ ZA
 - M2 decentre vs elevation/ ZA

Note that these procedures are low level engineering processes requiring detailed knowledge of the servo systems and their software control systems. Many are only applicable to ultra wide field systems.

For more information, contact EOS Technologies in Tucson, Arizona.

8. SOFTWARE UTILITIES

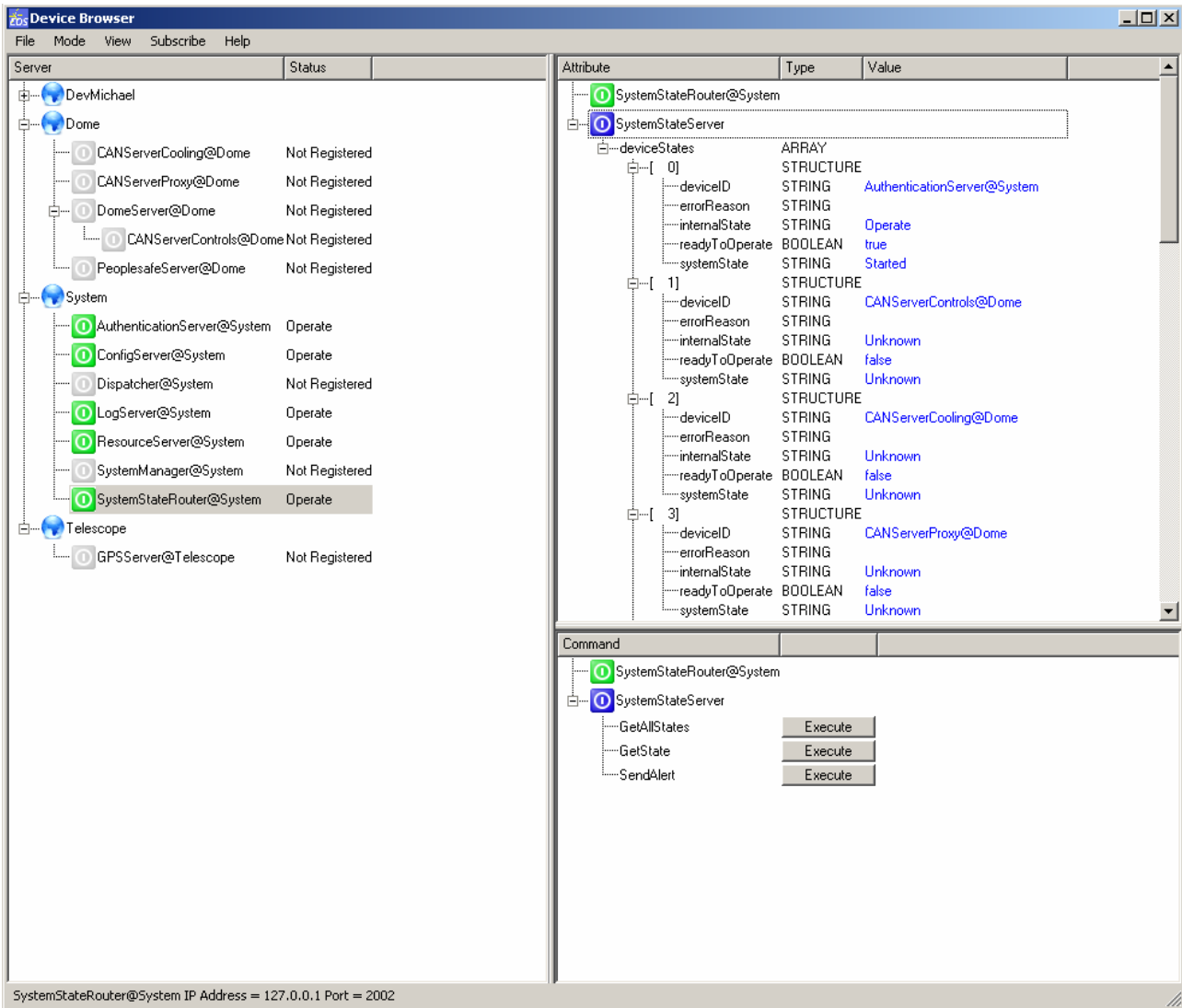
8.1 Device Browser

8.1.1 Description

The Device Browser is a low-level engineering tool which provides access to all state and all commands for all server applications in the Observatory Control System.

The Device Browser is a very powerful tool but it is not intended for casual use or general observatory operations. The Device Browser is intended to support trouble-shooting and engineering tasks.

The Device Browser enables the user to execute any and all commands on any server application. Note however that the Device Browser is a generic tool with no specific knowledge of any server application; it does not enforce any policy on what server commands may be executed or when they may be executed. This presents a potential safety hazard in the hands of users who are not qualified to use the Observatory Control System at such a low level. Therefore, observatory operators **MUST NOT** issue commands to any server application using the Device Browser, except under direct supervision or instruction from EOS.



The Device Browser displays the general state of all servers in the left-hand tree view. Servers are grouped by a logical 'Location', and within each Location each server has a unique 'Name'. The name and location of a server form its Identity (eg. TelescopeServer@Telescope).

Each server is shown using a coloured icon; the colour of the icon changes to reflect the server's state, as follows:

- Light grey - the server application is not registered with the *Dispatcher*. As far as the system is aware the server application is not running.
- Orange - the server application is in its **init** state. If the server application controls hardware devices then these may home or undertake some other startup procedure.
- Yellow - the server application is in its **ready** state. If the server application controls hardware devices then these should remain idle until the server enters the **operate** state.
- Green - the server application is in its **operate** state. If the server application controls hardware devices then these can be expected to be active or to move at any time.
- Red - the server application is in an **error** state. If the server application controls hardware devices then these can be expected to become disabled. Any problems must then be investigated before proceeding. The server application may then be able to be reset, at which point it may enter the **init** state.
- Dark grey - the server application is registered with the *Dispatcher* but cannot be contacted. This can occur if a server application crashes or a network connection is lost.

It will be noted that the servers are shown in a hierarchy, where any given server may have a parent server or children servers. This arrangement reflects the functional dependencies between servers, ie. a server may depend on child servers in order to perform its function, and a server may provide services to its parent server.

The Device Browser displays the internal state of one server application at a time, along with the commands made available by that server application. The displayed state is read-only and is useful for diagnostic purposes. The internal state of the server application is structured according to the server's *Schema*. The server's schema defines the structure of its internal state variables and also defines what commands can be executed by the server application.

The server application commands are accessed by clicking the corresponding 'Execute' button in the commands pane.

WARNING: Server application commands must not be issued except under direct supervision or instruction from EOS.

8.1.2 Logon

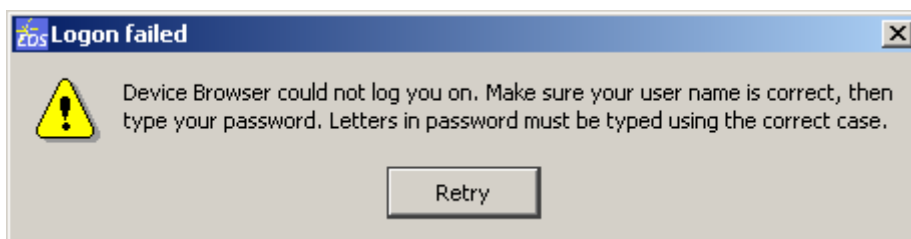
When accessing the Device Browser you will first be asked to log on. You will be presented with the following dialog box:



Enter a valid user name and password into their respective fields and click OK.

If you entered a valid user name and password then you will be presented with the Device Browser interface.

If you entered an invalid user name and password pair then you will be asked to try again:



8.1.3 General Features

The Device Browser can safely be used to explore the state of the Observatory Control System. The external state of all servers can be viewed in the tree view. The internal state of any server can be viewed by selecting that server in the tree view, upon which its state will be displayed in the Attributes pane (assuming the server can be contacted). It is always safe to use the Device Browser in this manner, ie. to browse the Observatory Control System's state.

When a server is selected in the tree view its commands will be made available in the Commands pane, below the Attributes pane.

WARNING: Server application commands must not be issued except under direct supervision or instruction from EOS.

8.1.4 Menus

The Device Browser provides a number of menus which control various functions, including the manner in which it presents data to the user.

8.1.4.1 File

- Exit – close the Device Browser.

8.1.4.2 Mode

- Device Locations
- Device Servers
- Show Devices

8.1.4.3 View

- Flat
- Hierarchical
- Numerics
 - Decimal
 - Octal
 - Hex
- Array Resizing

8.1.4.4 Subscribe

- Dirty Only – when a server application publishes its state data it does so in its entirety, unless the user has requested that only the data that has changed be published.
- On Change Only - server applications may publish their state data periodically regardless of change, however the Device Browser will only be sent data that has changed.
- Data Rate
 - Per 0.1 Second – displayed state data will be updated no faster than 10 times per second.
 - Per 0.5 Second – displayed state data will be updated no faster than 2 times per second.
 - Per 1.0 Second – displayed state data will be updated no faster than once per second.
 - Per 2.0 Second – displayed state data will be updated no faster then once very two seconds.

- Per 3.0 Second – displayed state data will be updated no faster than once every three seconds.
- At Server Rate – displayed data will be updated at whatever rate it is sent by the server application. Note that this may be problematic for servers that send their state data at high rates; the data may not be readable due to rapid display updates and the Device Browser may place heavy loads on the CPU trying to support the high display rate.

8.2 User and Permission Configuration

8.2.1 Authentication Interface

The Authentication Interface is a graphical user interface that provides an environment for managing user/group accounts and access control lists for the observatory system.

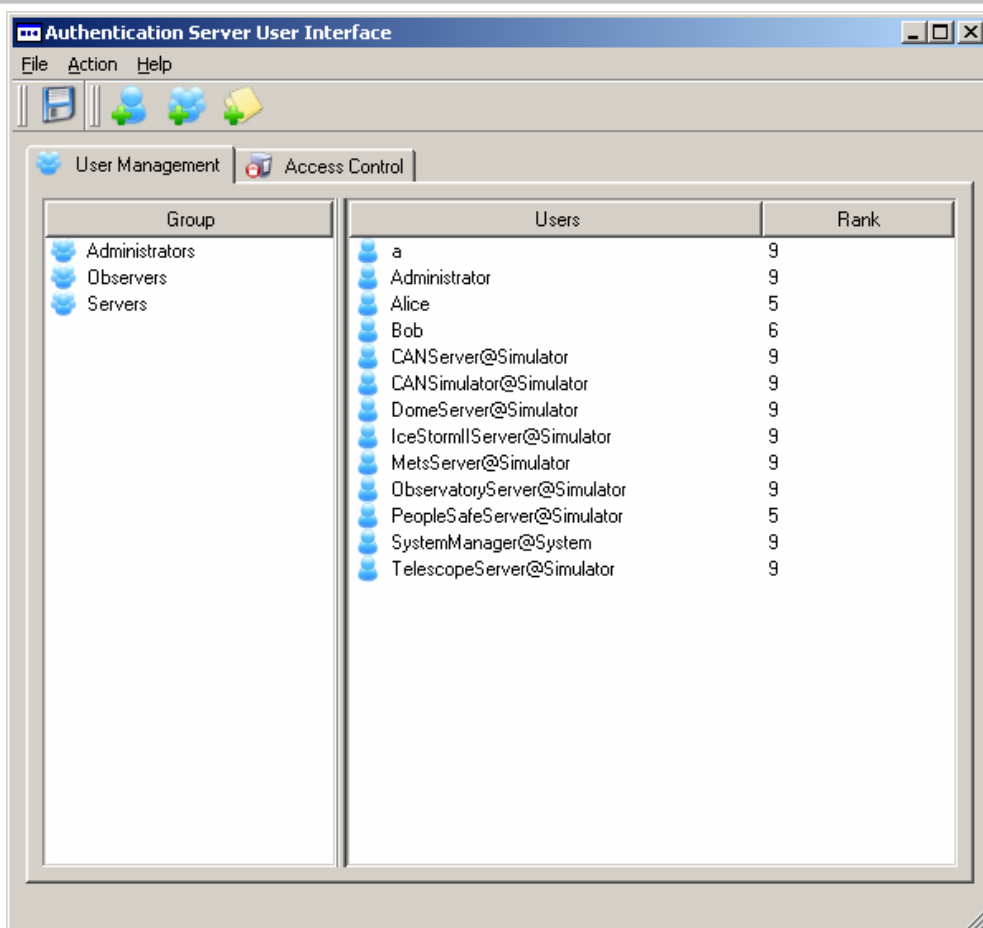
8.2.1.1 *Description*

The Authentication Interface consists of the following:

- A User Management tab
- An Access Control tab
- Several other menus, toolbars, and context menus

8.2.1.1.1 *User Management*

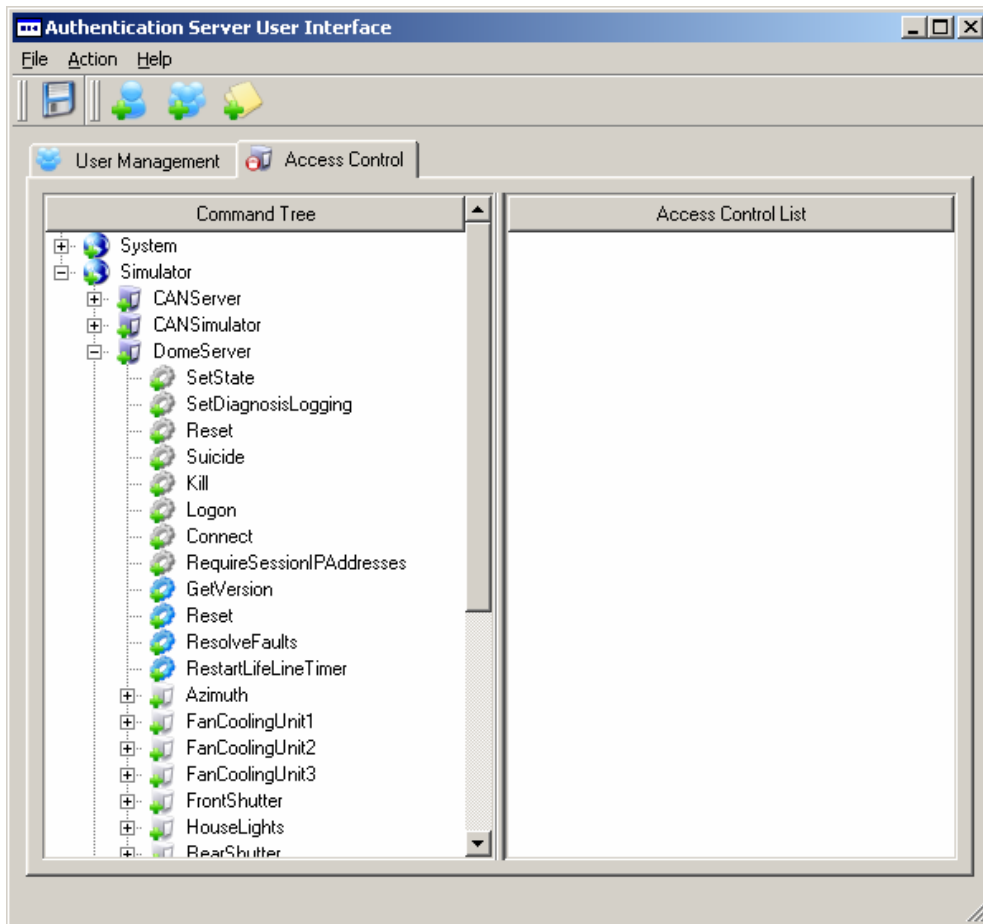
The user management tab of the Authentication Interface contains two main sections as can be seen in the following figure.



All group accounts are listed in the Group section and all user accounts are listed in the Users section. When you move the mouse over an account item, brief details about the account will be displayed as a tool tip.

8.2.1.1.2 Access Control

The following figure shows the access control tab:



The access control tab contains two sections; a command tree and an access control list section.

The command tree lists all the commands for the servers/devices that are within the observatory control system. The icon for an item (location, server, device, or command) in the command tree reflects an item's status. An icon with a green plus sign at its left bottom corner indicates that the item has not been configured with any access control list (i.e., allow all). An icon with a red cross-sign at its left bottom corner indicates that the item has been configured with access control lists, however a matching item cannot be found within the server schemas. An icon with an extra sign on it indicates the item is configured and has a matching item within the server schemas. Moving the mouse over an item will display brief details about the command as a tool tip.

The Access Control List (ACL) section contains all of the access control lists that exist. An ACL is composed of a set of ordered access control entries. Moving the mouse over an access control list item will display brief details about the access control list as a tool tip.

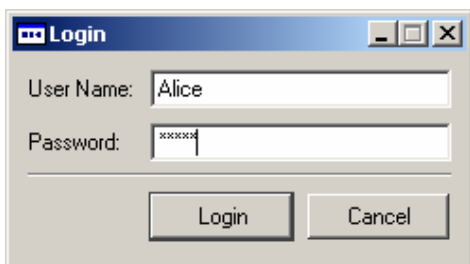
8.2.1.1.3 Menus, Toolbars, and Context Menus

Menus, Toolbars, and Context Menus are provided for modifying the configurations and may be accessed by right-clicking the mouse. Note that the menus, toolbars, and context menus may be disabled depending on the current selected/focused items in the different windows.

8.2.1.2 Logging in

To log in to the Authentication Interface:

1. Launch the application. A login dialog will be displayed as follows:

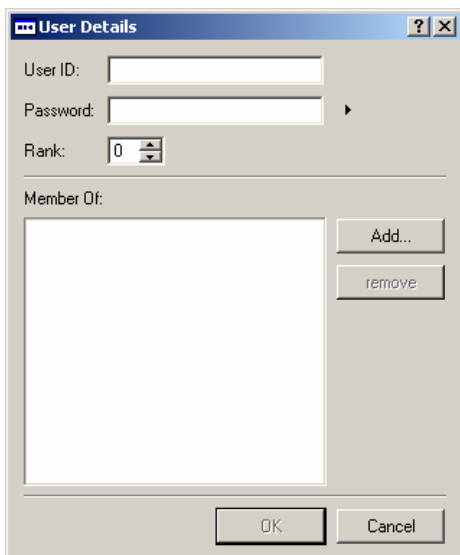


2. Enter a valid username and password and then click on the Login button. If you entered a valid username and password combination the application will successfully launch and you will be taken to the main screen. However, if you entered an invalid username and password combination a warning message will be displayed. Clicking the OK button on the warning will return you to the login dialog where you can attempt to log in again.

8.2.1.3 Adding a new user

To create a new user account:

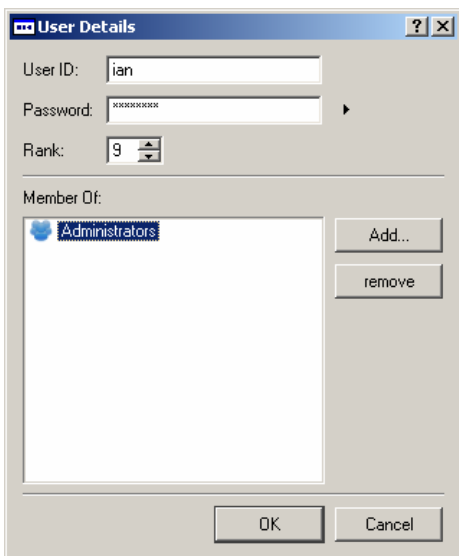
1. Click Action | Add New User from the main menu. A User Details dialog will be displayed.



2. Enter the new user’s details into each of the fields. Note that to enter a password you first must click the “right arrow” button that is located to the right of the Password field.
3. Assign a priority for the new user by entering a number in the Rank field.
4. To assign the new user to a group, click on the Add button. A Group Choices dialog will be displayed.



5. Select the group(s) you wish to add this user to and click OK. You will be returned to the User Details screen and the selected group(s) will be displayed in the “Member Of” section. An example of a completed User Details screen is as follows:



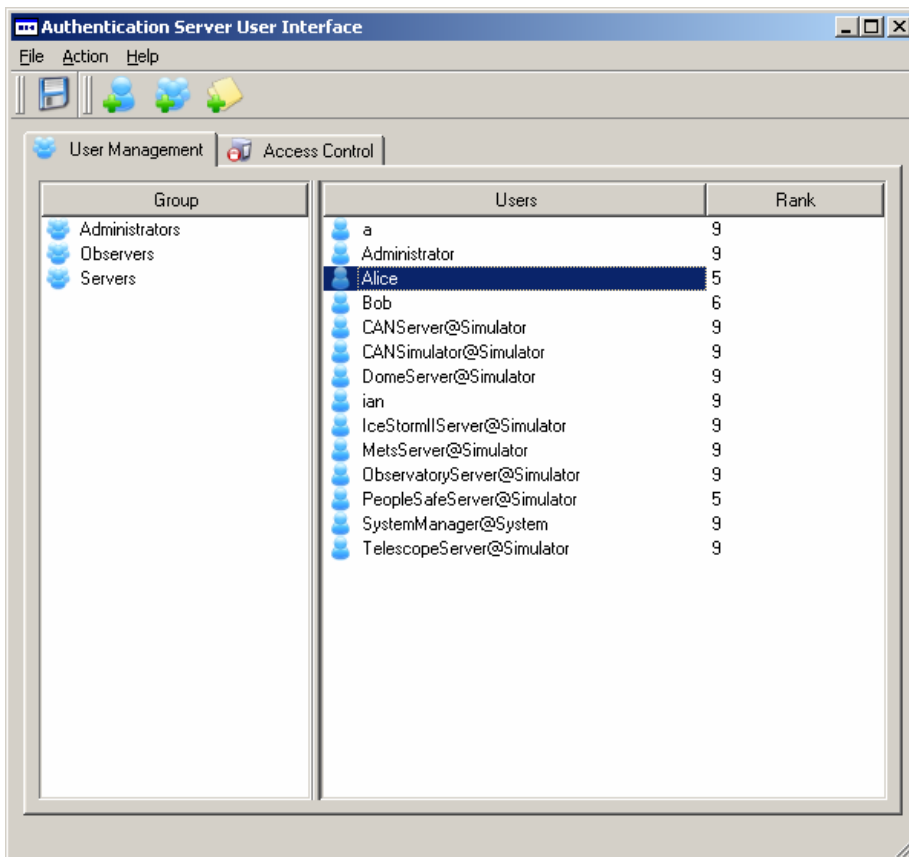
6. When you are satisfied with the new user’s details, click the OK button. You will be returned to the main screen and the new user will now appear in the Users section of the User Management tab.

Note that adding a new user can also be initiated via a toolbar button or from within the context menu.

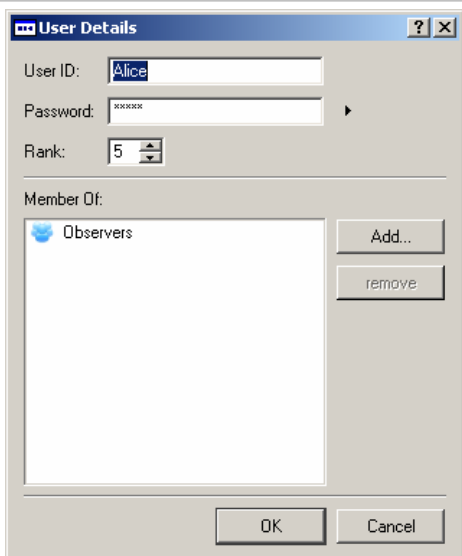
8.2.1.4 Editing a user

To edit a user account:

1. Open the User Management tab and click on the user to be edited.



2. Click Action | Edit Current User from the main menu. The User Details screen will be displayed.



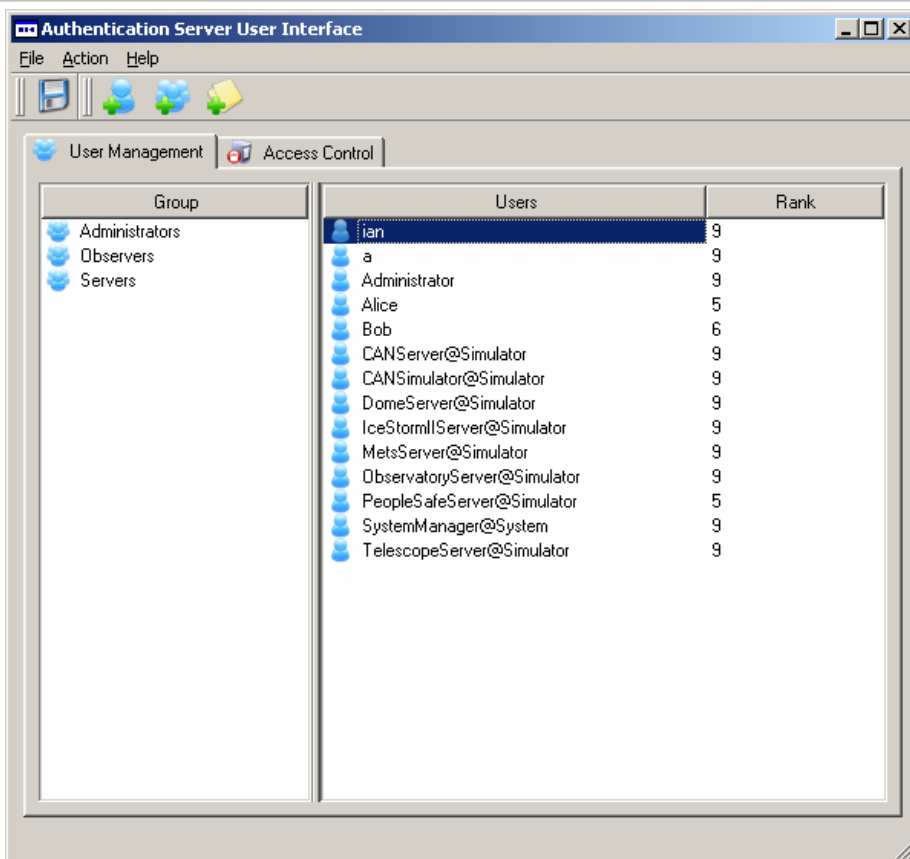
3. Edit the fields as necessary. Note that a user can have their password, rank, or group memberships changed.
4. Once you are satisfied with the changes, click the OK button to save. The user's details will be updated and you will be returned to the main screen.

Note that editing a user's details can also be initiated from the User Management tab by right clicking on the user's name.

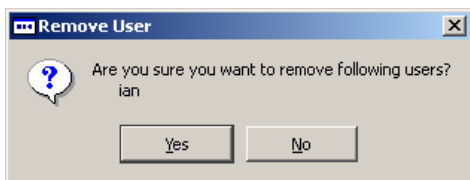
8.2.1.5 Removing a user

To delete a user account:

1. Open the User Management tab and click on the user to be deleted.



2. Click Action | Remove Selected User from the main menu. The following confirmation message will be displayed:



3. Click the Yes button to confirm the deletion. You will be returned to the main screen and the deleted user will no longer appear in the Users section of the User Management tab.

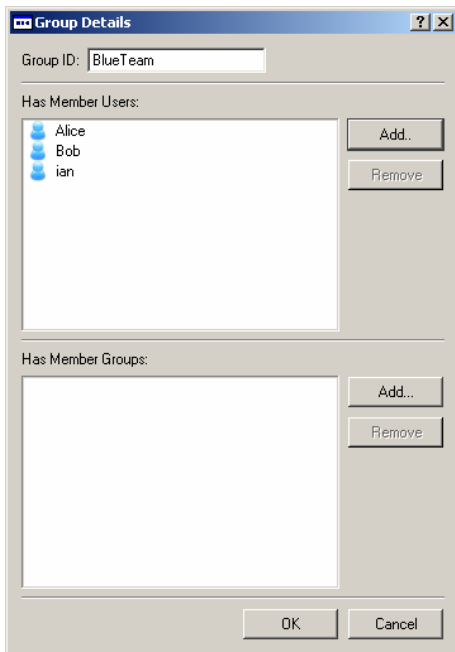
Note that deleting a user can also be initiated from within the context menu.

8.2.1.6 Adding a new group

To create a new user group:

1. Click Action | Add New User Group from the main menu. A Group Details dialog will be displayed.
2. Enter an identifier in the Group ID field.
3. To assign users to the group, click the Add button to the right of the Has Member Users list window. A Choices dialog will be displayed.

4. Select the user(s) that you wish to add to the group and click OK. After adding the users to the new group, the Group Details form will look as follows:



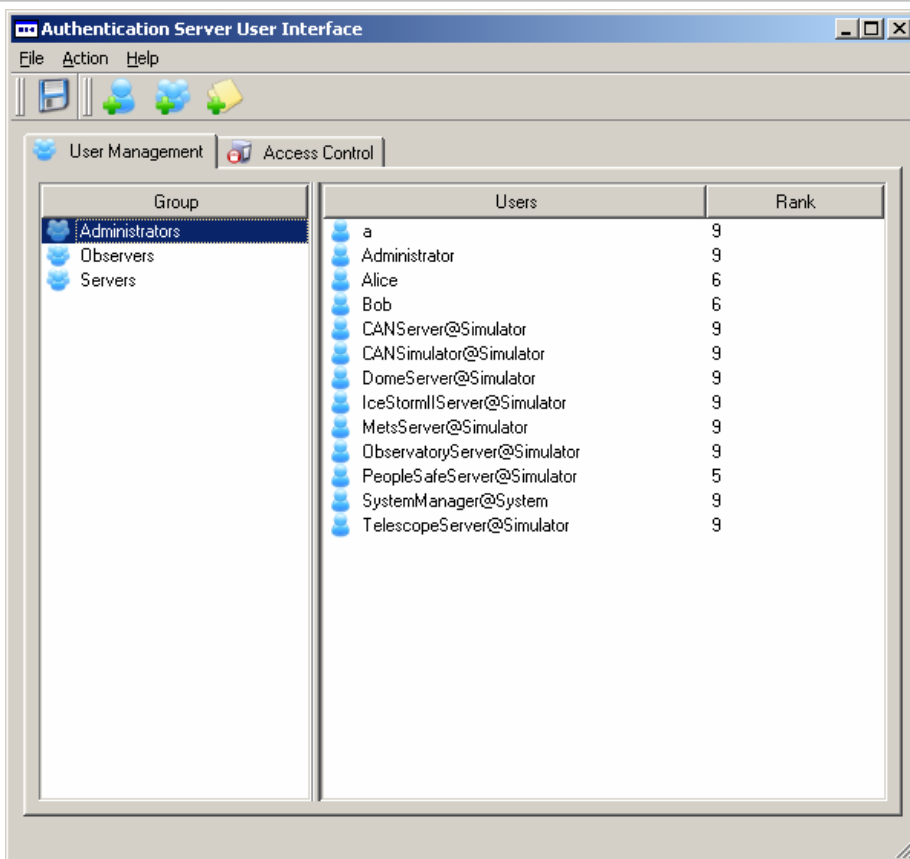
5. Click OK to confirm. You will be returned to the main screen and the new group will now be visible in the Group section of the User Management tab.

Note that adding a new user group can also be initiated via a toolbar button or from within the context menu.

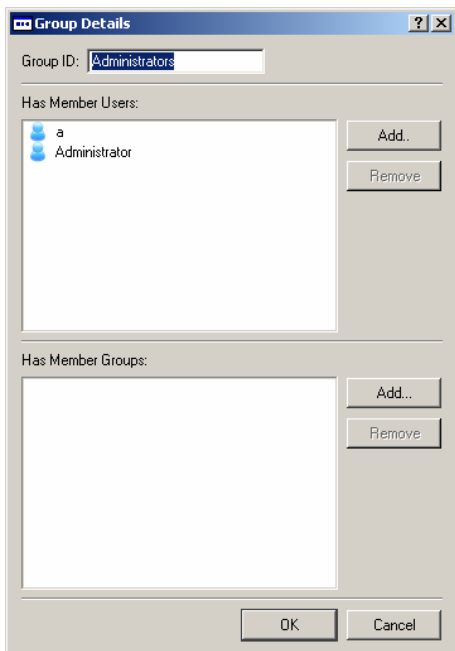
8.2.1.7 Editing a group

To edit a group:

1. Open the User Management tab and click on the group to be edited.



2. Select Action | Edit Selected User Group from the main menu. The Group Details form will be displayed.



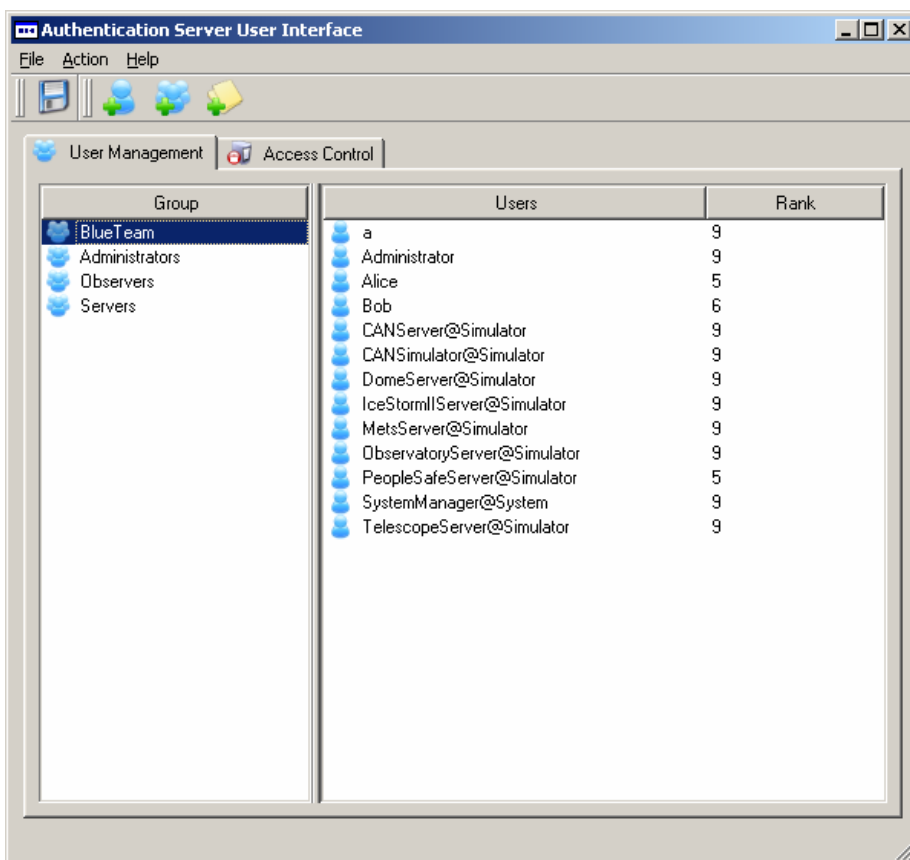
3. Make the necessary modifications to the group. Note that users can be added to the group by clicking the Add button and selecting the new user from the list. A user can be removed by selecting a user in the “Has Member Users” section and clicking on the Remove button.
4. Once you are satisfied with the modifications to the group, click the OK button to confirm. The modifications will be saved and you will be returned to the main screen.

Note that modifying a group can also be initiated from within the context menu.

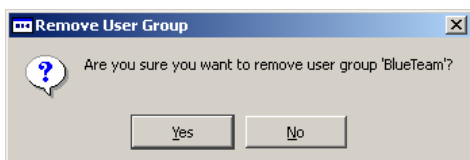
8.2.1.8 Removing a group

To delete a group account:

1. Open the User Management tab and click on the group to be deleted.



2. Click Action | Remove Selected User Group from the main menu. The following confirmation message will be displayed.



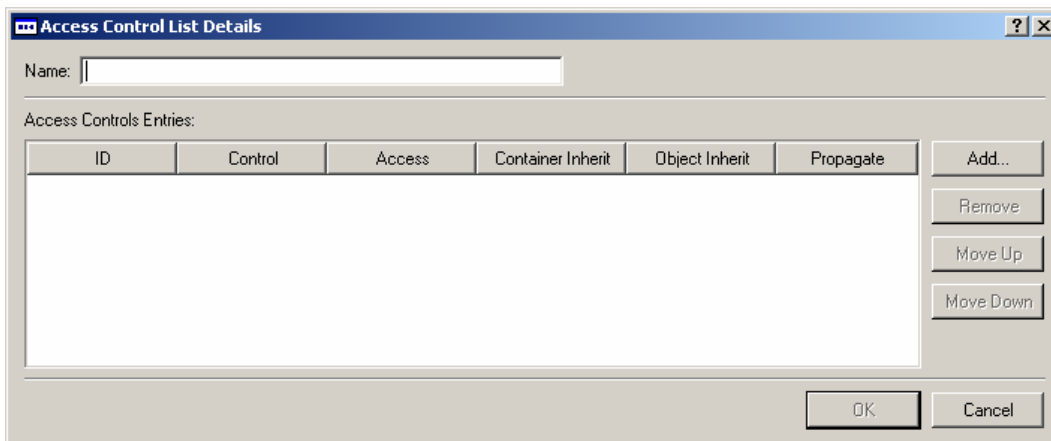
3. Click the Yes button to confirm the deletion. You will be returned to the main screen and the user group will no longer appear in the Group section of the User Management tab.

Note that deleting a group can also be initiated from within the context menu.

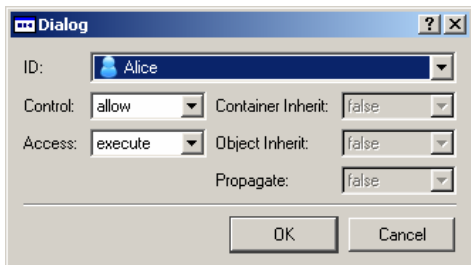
8.2.1.9 Adding an access control list

To create a new access control list:

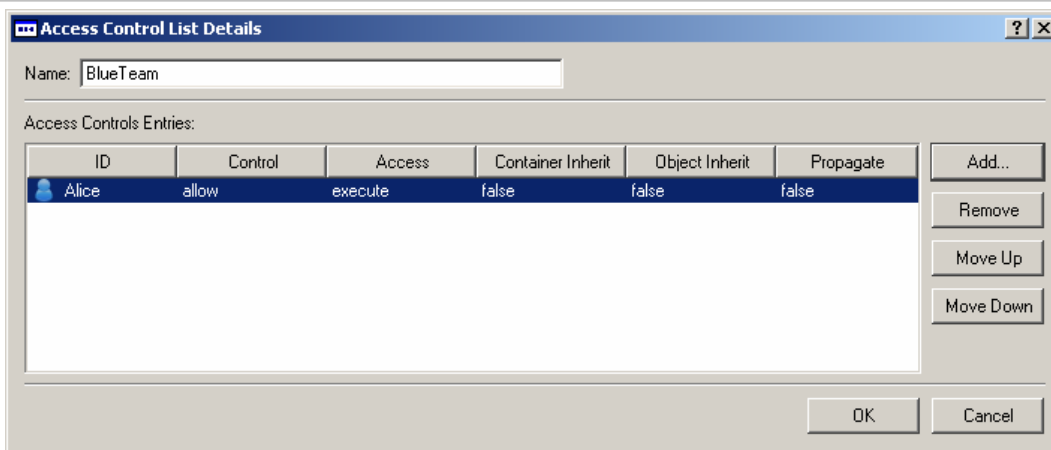
1. Click Action | Add New Access Control List from the main menu. An Access Control List Details dialog will be displayed.



2. Enter a name for the new Access Control List.
3. Click the Add button. A dialog to add access control entries will be displayed:



4. Select a User ID, a Control setting and an Access setting from the available drop-down lists.
5. Once you have made your selection, click OK to confirm. You will be returned to the Access Control List Details screen where the new entry will now be visible.



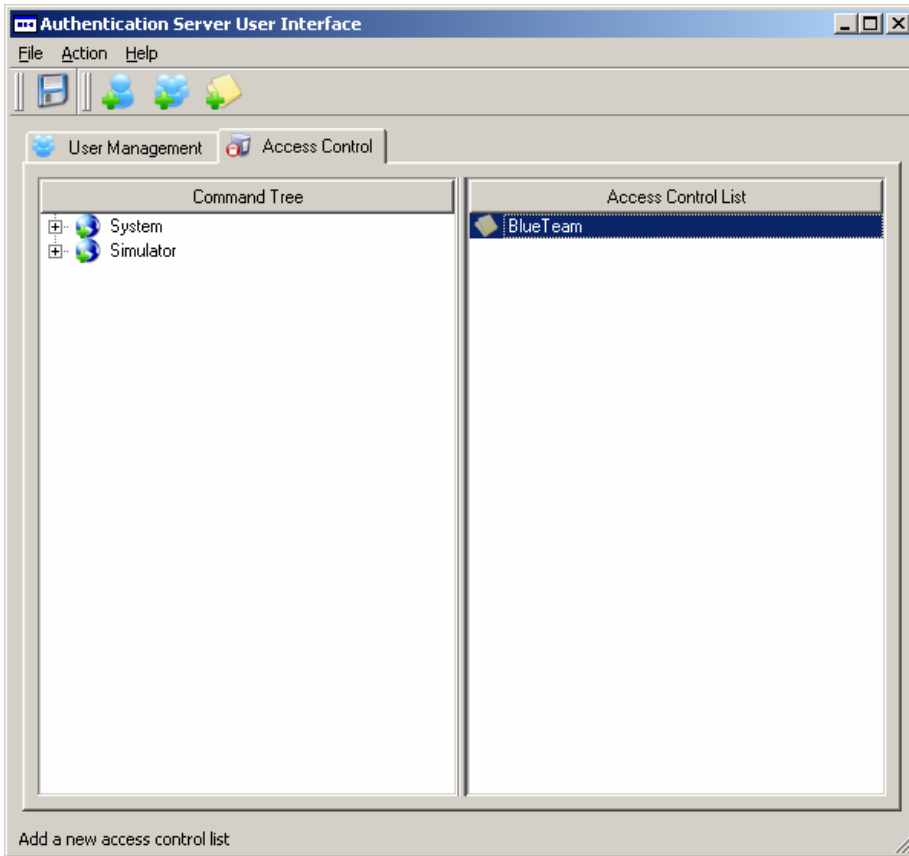
6. Add any additional entries to the access control list by repeating steps 3 – 5. The list can be re-ordered by selecting a row and clicking either the Move Up or Move Down buttons. A row can be removed from the list by selecting it and clicking on the Remove button.
7. Once you are satisfied with the new access control list, click the OK button to confirm the creation. You will be returned to the main screen and the new list will now appear in the Access Control List section of the Access Control tab.

Note that creating a new access control list can also be initiated from a toolbar button or from within the context menu.

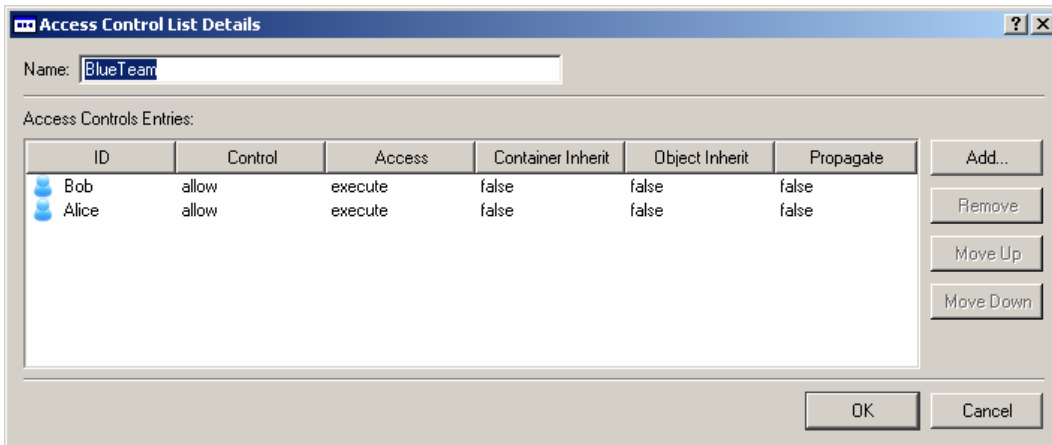
8.2.1.10 Editing an access control list

To edit an Access Control List:

1. Open the Access Control tab and click on the Access Control List to be edited.



2. Select Action | Edit Current Access Control List from the main menu. The access control list details will be displayed.



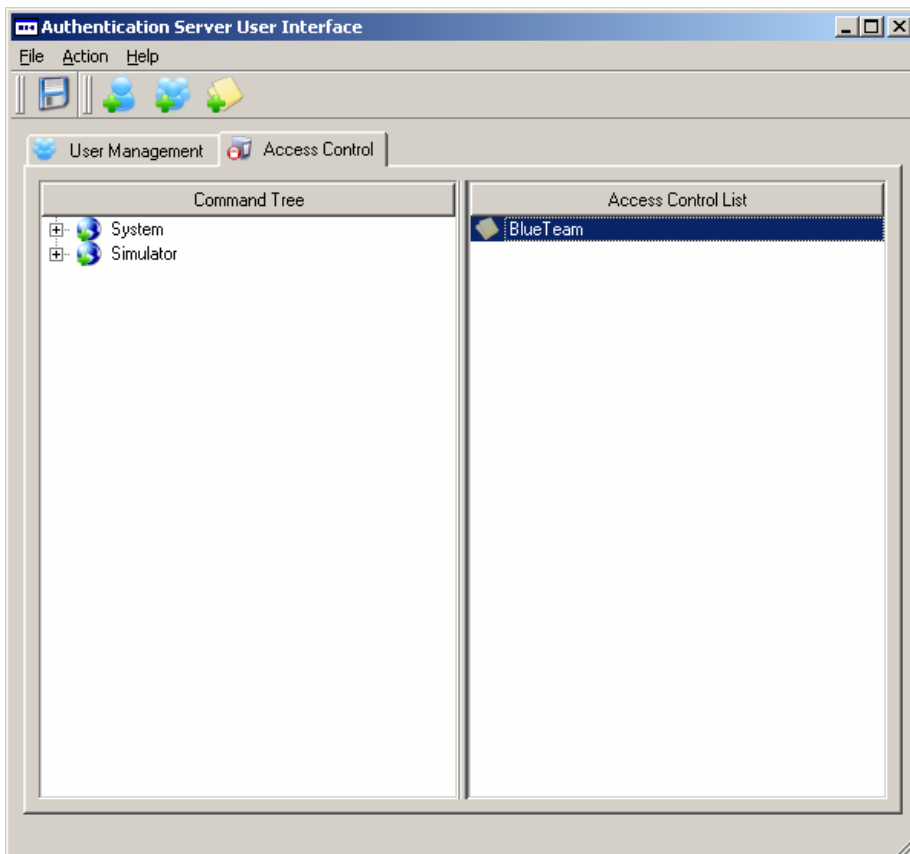
3. Edit the details as required. New rows can be added by clicking the Add button and specifying a user ID, a control setting, and an access setting. Users can be removed by selecting a row and clicking the Remove button. The rows can be re-ordered by clicking the Move Up or Move Down buttons.
4. Once you are satisfied with your modifications, click the OK button. The details will be updated and you will be returned to the main screen.

Note that editing an access control list can also be initiated from within a context menu.

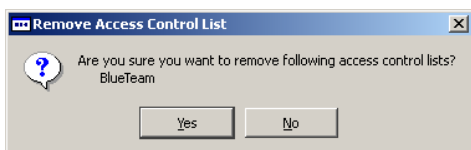
8.2.1.11 Removing an access control list

To delete an Access Control List:

1. Open the Access Control tab and click on the Access Control List to be deleted.



2. Click Action | Remove Selected Access Control List from the main menu. The following confirmation message will be displayed:



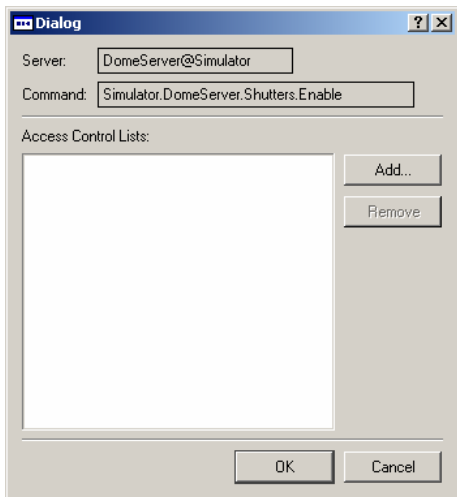
3. Click the Yes button to confirm the deletion. You will be returned to the main screen and the access control list will no longer be visible in the Access Control tab.

Note that removing an access control list can also be initiated from within the context menu.

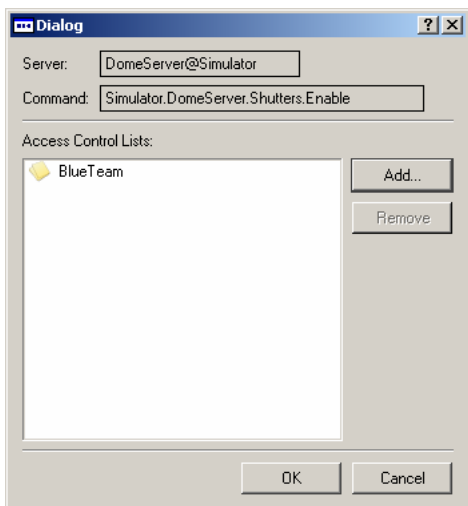
8.2.1.12 Assigning an access control list to a command

To assign an access control list to a command:

1. Open the Access Control tab, expand the Command Tree and double-click on the command. A Command Details dialog will be displayed for the command.



2. Click on the Add button. A Choices dialog will be displayed that lists the access control lists.
3. Select the access control list that you wish to add to the command and click the OK button. You will be returned to the Command Details screen and the access control list will now be visible.



4. Repeat steps 2 -3 to add any additional lists to the command. A row can be removed by selecting it and clicking on the Remove button.
5. Once you are satisfied with the access control lists to apply to the command, click the OK button to confirm. You will be taken back to the main screen. The tool tip details for the command will now also include the access control list just added.

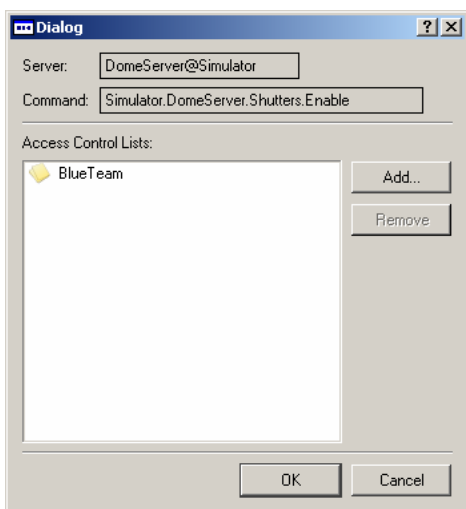
Note that assigning an access control list to a command can also be initiated via the Action | Edit Selected Command menu or by right clicking on the command.

Administrators can also drag an access control list (ACL) item and drop it onto the desired command item. If an ACL is dropped onto a leaf command item, the ACL is applied to the leaf command only. If an ACL is dropped onto a device item, the ACL is applied to all leaf commands under the device. The same logic applies to dropping an ACL onto a server item or a location item.

8.2.1.13 Removing an access control list from a command

To remove an ACL from a command

1. Open the Access Control tab, expand the Command Tree and double-click on the command. A Command Details dialog will be displayed.



2. Select the access control list to be removed and click the Remove button. The list will be removed from the command.
3. Click the OK button to confirm. You will be taken back to the main screen. The tool tip details for the command will no longer include the access control list.

Note that the remove access control list from command operation can also be initiated via the Actions menu or from the context menu.

Administrators can clear the access control list configuration of a command by right clicking on the command and selecting “Clear ACL Configurations”. The clear operation will clear all the ACL configurations that have been assigned to the command and set the status of the command to be “Un-configured” (i.e., allow all). If the clear operation is applied to a node command item, it is applied to all leaf command items under it.

8.2.1.14 Marking a command as configured

To mark a command as configured:

1. Open the Access Control tab, expand the Command Tree and click on the command to select it.
2. Click Action | Mark As Configured on the main menu. The icon for the command will change to indicate that the command has been configured. The tool tip status entry will display as “Configured”.

Note that the Mark As Configured operation can also be initiated from a context menu by right clicking on the command.

8.2.1.15 Clearing access control list configurations

To clear an access control list configuration:

1. Open the Access Control tab, expand the Command Tree and click on the command to select it.
2. Click Action | Clear ACL Configurations on the main menu. The icon for the command will change to indicate the access control lists have been cleared. The tool tip status entry will display as “Not Configured”.

Note that the Clear ACL Configurations operation can also be initiated from a context menu by right clicking on the command.

8.2.1.16 Removing an unmatched command

The application allows administrators to remove an unmatched command. The operation doesn't remove a command from the server schema but instead removes the command entry from the authentication configuration.

To remove an unmatched command:

1. Open the Access Control tab, and expand the Command Tree.
2. Right click on the unmatched command.
3. Select “Delete Selected Command” from the context menu. A confirmation message will be displayed.
4. Click on the Yes button to delete the command.

Note that the remove unmatched command operation can also be initiated from the Actions menu.

8.2.1.17 Saving changes

To save changes back to the configuration server simply click on the Commit button on the toolbar.

Note that if a loop(s) exists in the super/sub group relationship, the application will not allow the save operation to proceed.

8.2.2 Resource Management Interface

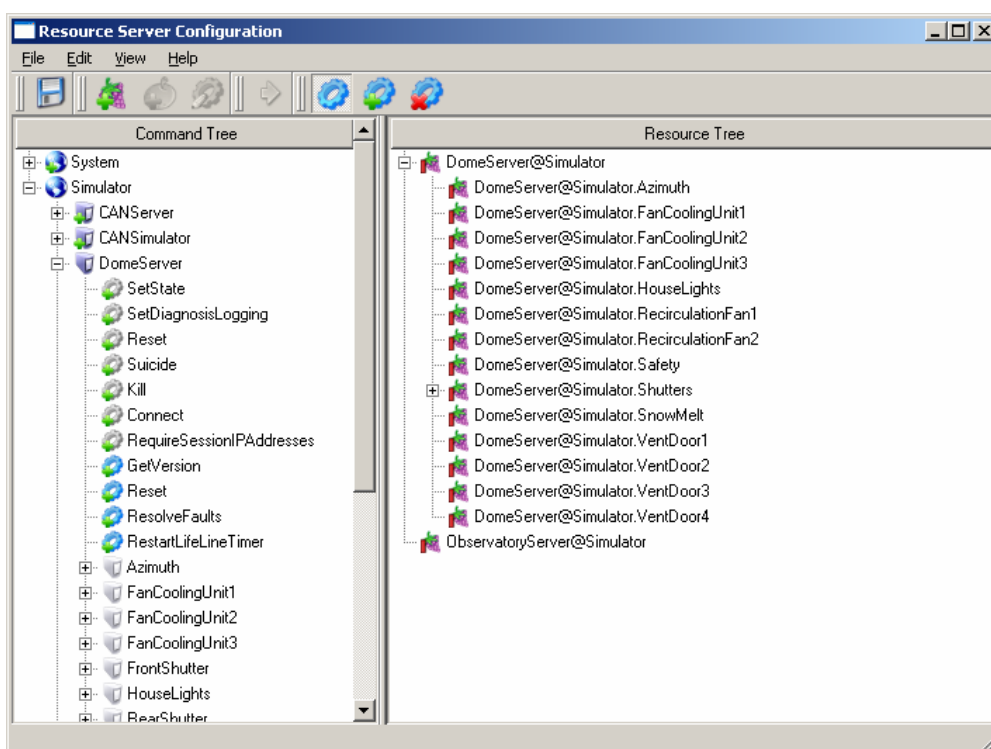
The Resource Management Interface is a graphical user interface that provides an environment for administrators to configure the resources that are required by a command before it can be executed within the observatory control system.

8.2.2.1 Description

The Resource Management Interface consists of the following:

- A Command Tree section.
- A Resource Tree section.
- Several other menus, toolbars, and context menus.

The main screen of the interface is displayed below.



8.2.2.1.1 Command tree

The command tree lists the commands for all servers/devices that are within the observatory control system. The icon of an item (location, server, device, or command) in the command tree tells the status of the item. An icon with a green plus sign at its left bottom corner indicates the item is not configured with any resource. An icon with a red cross-sign at its left bottom corner indicates the item is configured with resources, however a match item cannot be found within the server

schemas. An icon with an extra sign on it indicates the item is configured and has a matching item within the server schemas. When you move the mouse over an item, brief details about the item will be displayed as a tool tip.

8.2.2.1.2 *Resource tree*

The resource tree lists all resources that exist within the system. These resources are organized in a tree structure to reflect their relationships. When you move the mouse over a resource item, brief details about the resource will be displayed as a tool tip.

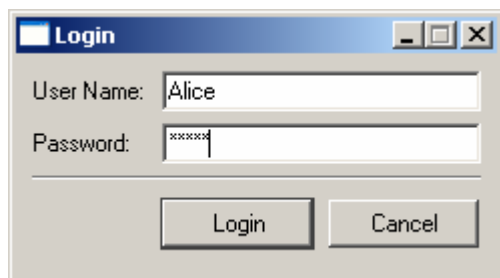
8.2.2.1.3 *Menus, toolbars and context menus*

Menus, toolbars, and context menus are provided for performing various actions within the application. The context menus can be accessed by right-clicking the mouse. Menu items may be enabled or disabled depending on the context in which they were invoked.

8.2.2.2 **Logging in**

To log in to the Resource Management Interface:

1. Launch the application. A login dialog will be displayed as follows:

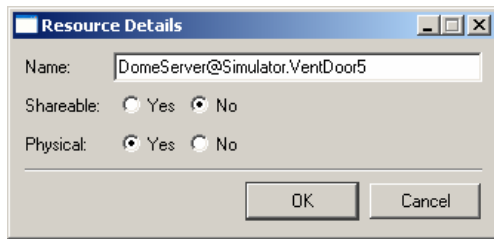


2. Enter a valid username and password and then click on the Login button. If you entered a valid username and password combination the application will successfully launch and you will be taken to the main screen. However, if you entered an invalid username and password combination a warning message will be displayed. Clicking the OK button on the warning will return you to the login dialog where you can attempt to log in again.

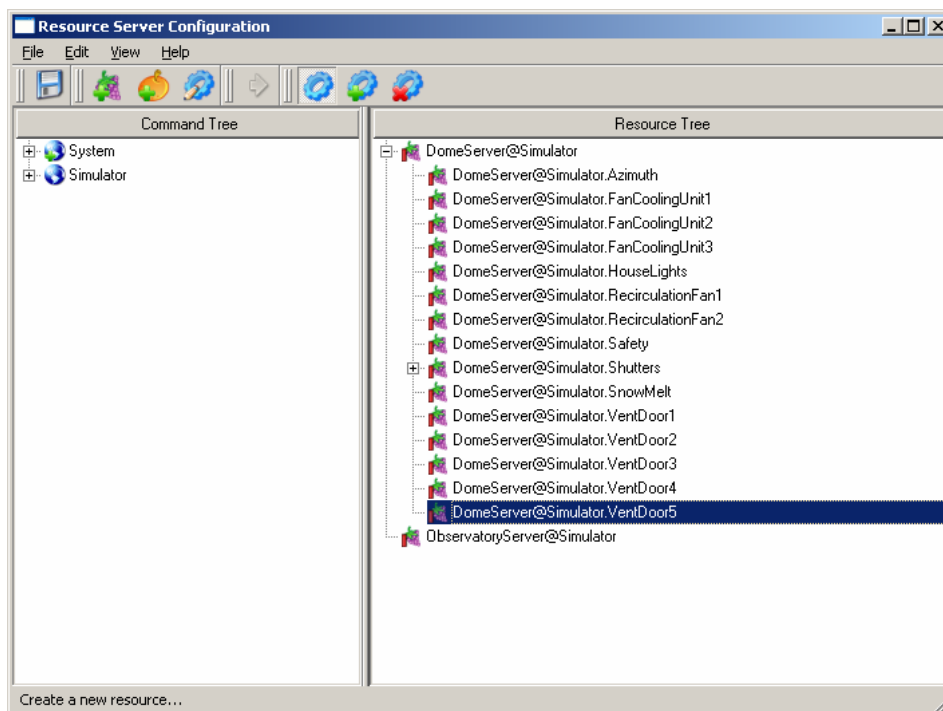
8.2.2.3 **Creating resources**

To create a new resource:

1. Click Edit | Create New Resource from the main menu. A Resource Details screen will be displayed.
2. Enter the name of the new resource and indicate whether it is sharable and physical status by clicking the appropriate radio buttons.



- Once you are satisfied with the new resource's details, click the OK button to confirm. You will be returned to the main screen and the new resource will now appear in the Resource Tree section.

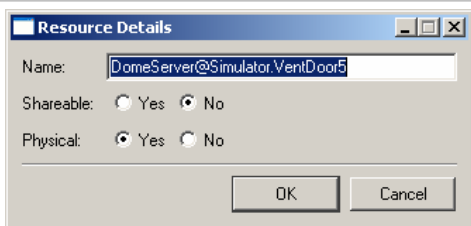


The create resource operation can also be initiated via a toolbar button or from within the context menu.

8.2.2.4 Editing resources

To edit a resource:

- Select the resource in the Resource Tree and click Edit | Edit Selected Resource from the main menu. A Resource Details screen will be displayed.



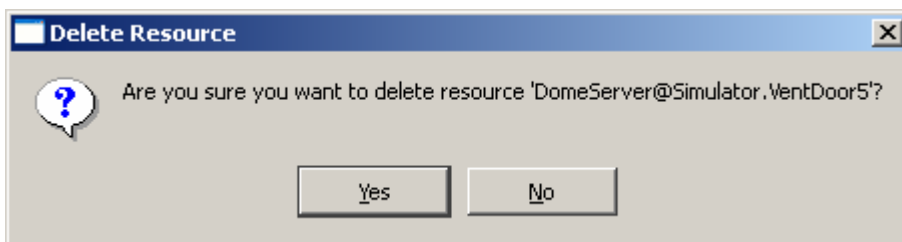
2. Edit the resource by entering new details into the appropriate fields.
3. Once you are satisfied with your modifications, click the OK button to confirm. You will be returned to the main screen and your modifications will now be visible in the Resource Tree section.

The edit resource operation can also be initiated by double-clicking a resource in the Resource Tree or by right clicking a resource and selecting “Edit Selected Resource” from the context menu.

8.2.2.5 Deleting resources

To delete a resource:

1. Select the resource to be deleted in the Resource Tree and click Edit | Delete Selected Resource from the main menu. A confirmation message will be displayed.



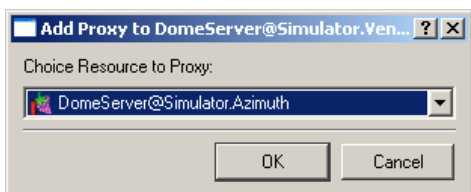
2. Click the Yes button to confirm. You will be returned to the main screen and the resource just deleted will no longer appear in the Resource Tree section.

The delete resource operation may also be initiated via the context menu.

8.2.2.6 Creating a proxy

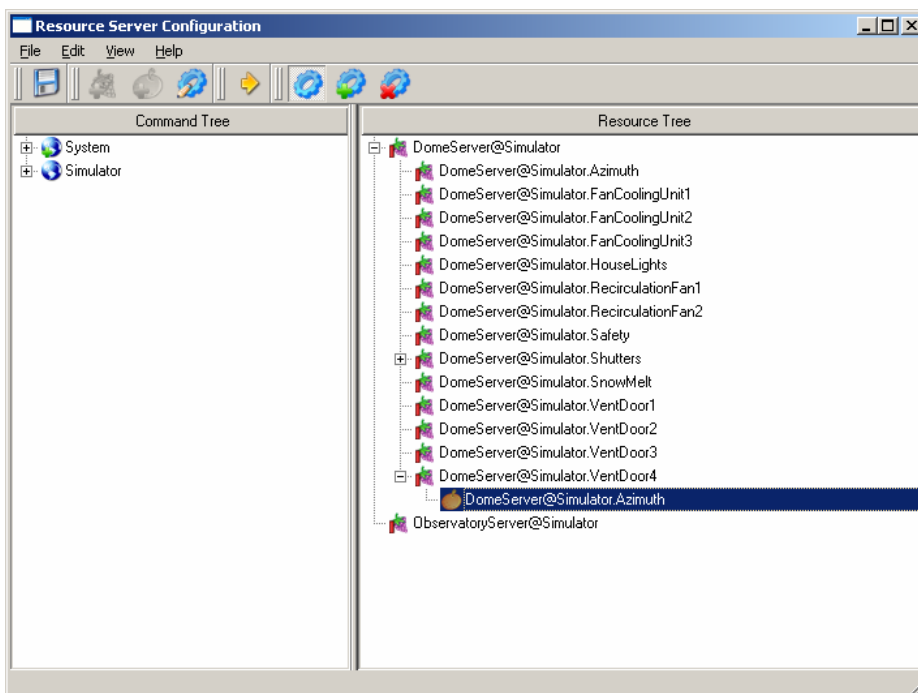
To configure a resource to proxy another resource:

1. Select the source resource in the Resource Tree and click Edit | Add New Proxy from the main menu. A Proxy Choice screen will be displayed.



2. Select the resource to proxy from the drop-down list.

3. Click the OK button to confirm. You will be returned to the main screen where the new proxy will now be visible.

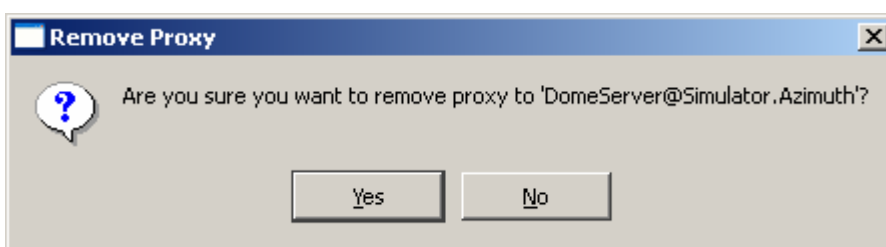


The Add New Proxy operation can also be initiated via a toolbar button or from within the context menu.

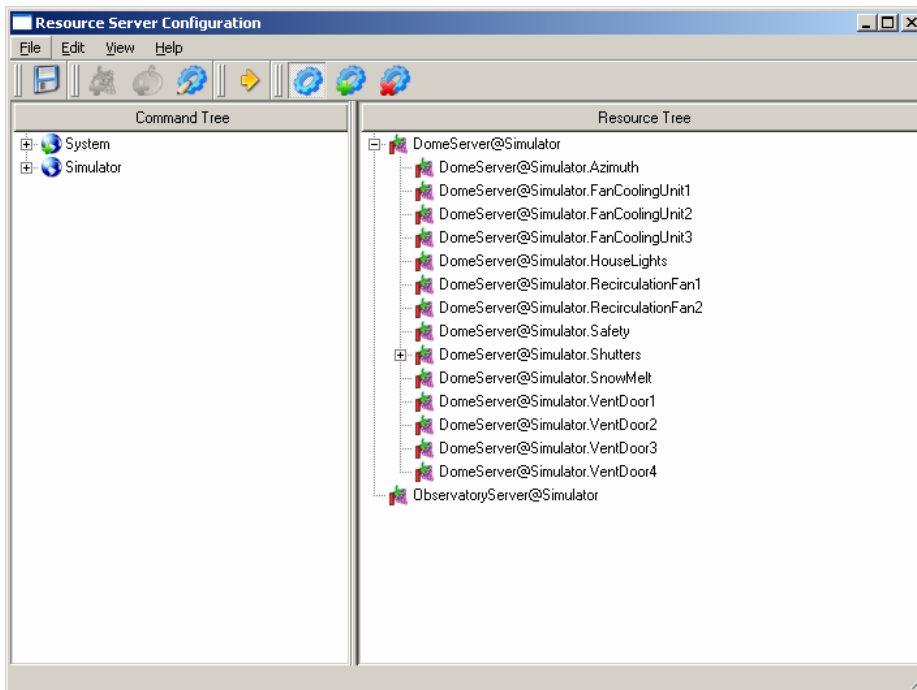
8.2.2.7 Removing a proxy

To delete a proxy:

1. Select the proxy to be deleted in the resource tree window and click Edit | Remove Selected Proxy from the main menu. A confirmation message will be displayed.



2. Click the Yes button to confirm. You will be returned to the main screen and the proxy just deleted will no longer be visible.

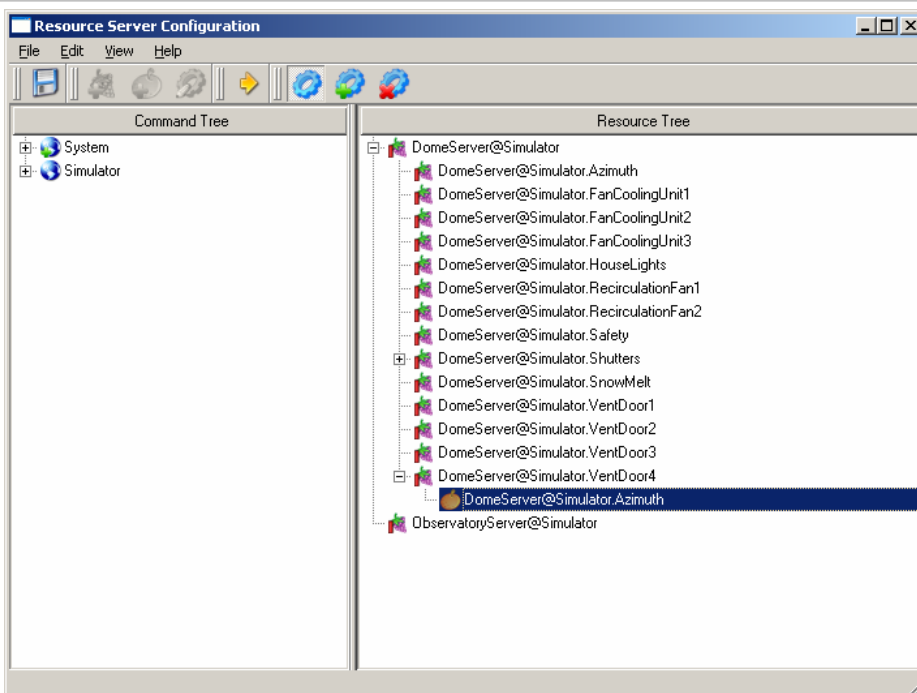


The Remove Proxy operation can also be initiated via the context menu.

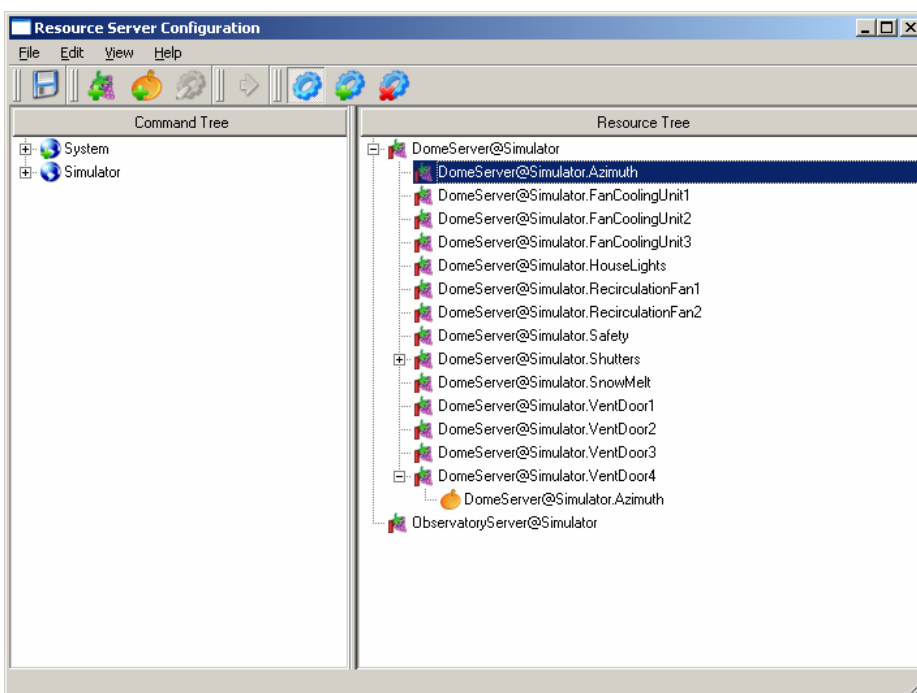
8.2.2.8 Jumping to a proxy's resource

To jump to a proxy's resource:

1. Select the proxy in the Resource Tree section by clicking on it. The proxy will be highlighted to indicate that it has been selected.



2. Click Edit | Jump to Resource on the main menu. The selected item in the resource Tree will jump to the actual resource that has been proxied.

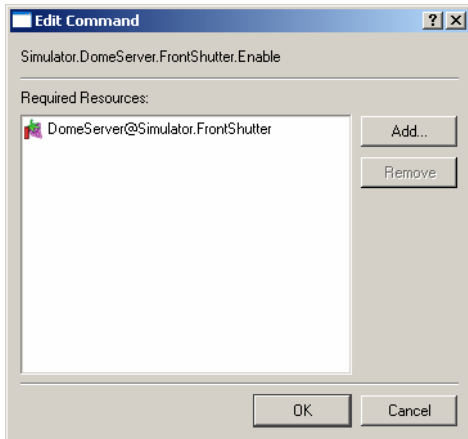


The Jump to Resource operation can also be initiated via the tool bar and from within the context menu.

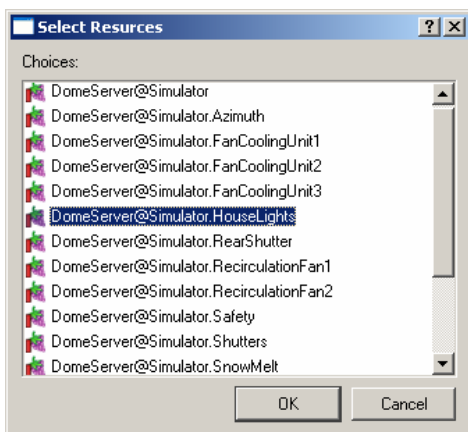
8.2.2.9 Adding resources to a command

To assign a resource to a command:

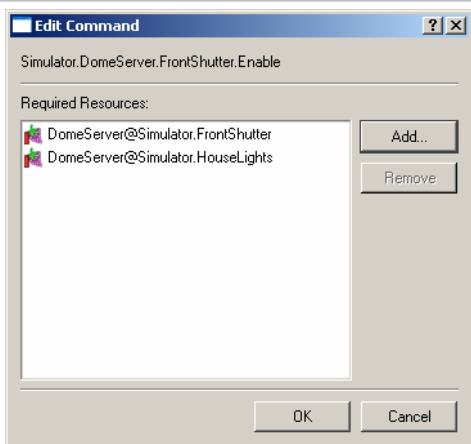
1. Select the command in the Command Tree and click Edit | Edit Selected Command from the main menu. The Edit Command screen will be displayed.



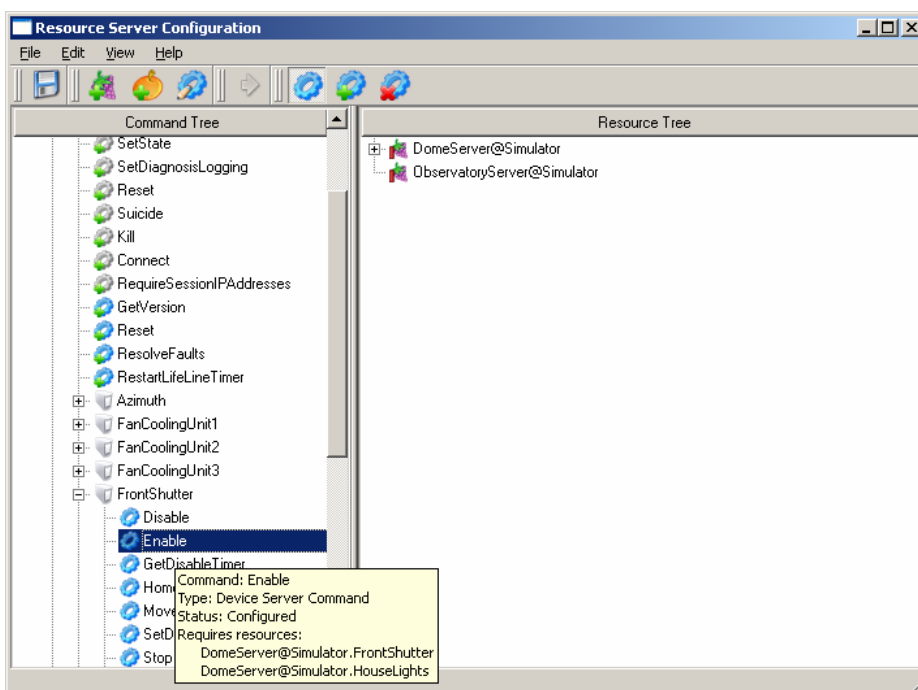
2. Click the Add button. A Choices screen will be displayed.



3. Select the resource to add to the command from the drop-down list and click the OK button to confirm your selection. You will return to the Edit Command screen and the new resource just added will now be visible.



4. Repeat steps 2 and 3 to add any additional resources that are required by the command in question. Note that you can remove a resource from the command by clicking the Remove button.
5. Once you are satisfied with the resources that have been assigned to the command, click the OK button. You will be returned to the main screen and the changes will now be visible in the Command Tree. Moving the mouse over the command just edited will display the tool tip that will now include the resources that were just added.



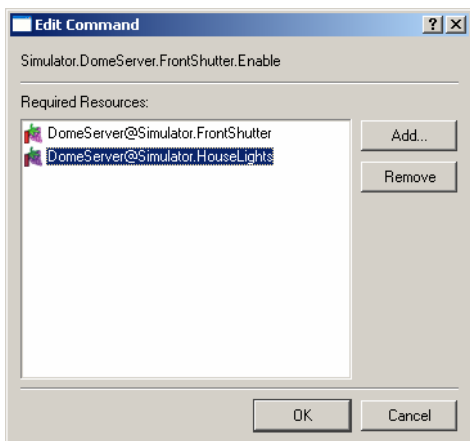
The Add Resource to a Command operation can also be initiated by double-clicking on a command or from within the context menu.

Administrators can also drag a resource item and drop it onto the desired command item. If a resource is dropped onto a leaf command item, the resource is applied to the leaf command only. If a resource is dropped onto a device item, the resource is applied to all leaf commands under the device. The same logic applies to dropping a resource onto a server item or a location item.

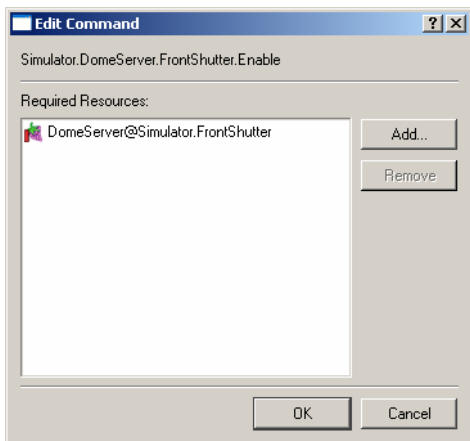
8.2.2.10 Removing resources from a command

To remove a resource from a command:

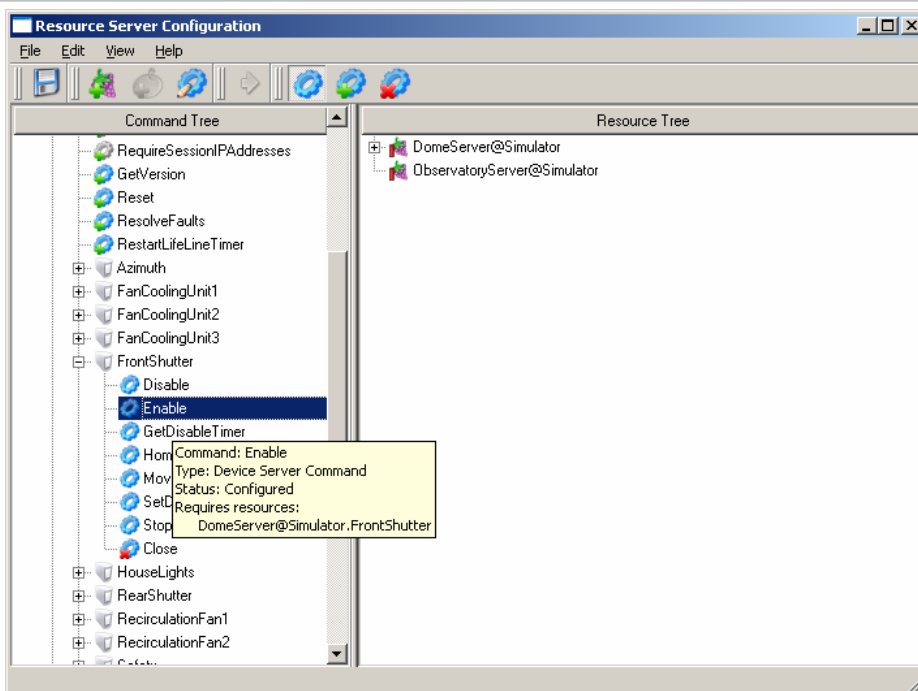
1. Select the command in the Command Tree and click Edit | Edit Selected Command from the main menu. The Edit Command screen will be displayed.



2. Select the resource to remove and click the Remove button. The resource will no longer be listed in the Required Resources section of the screen.



3. Click the OK button to confirm the removal. You will be returned to the main screen and the changes will now be visible in the Command Tree.



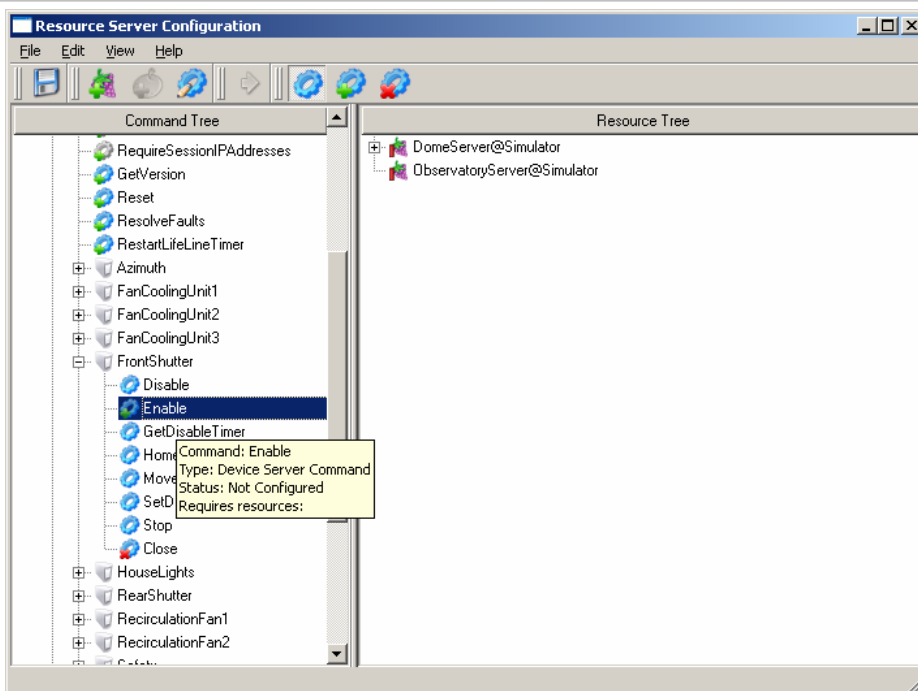
The Remove Resources from a Command operation can also be initiated by double-clicking on a command or via the context menu.

Note that administrators can also clear a command’s resources by right-clicking the command and selecting “Clear Resource Configurations” from the context menu. Refer to the Clear a Command’s Resource Configuration section for further details.

8.2.2.11 Clearing a command’s resource configurations

To clear all resources assigned to a command:

1. Select the command in the Command Tree and click Edit | Clear Resource Configurations from the main menu. You will be returned to the main screen where the icon of the command will have changed to “Not Configured” and all previously assigned resources will no longer be visible.

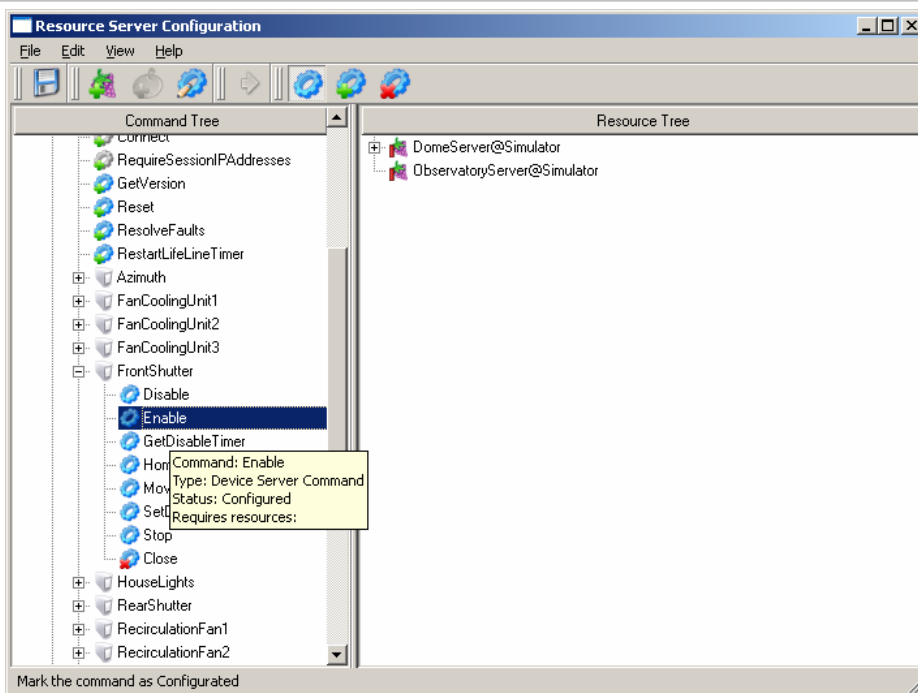


Clearing a command’s resource configurations can also be initiated by right-clicking on the command and selecting “Clear Resource Configuration’s” from the context menu.

8.2.2.12 Marking a command as configured

To mark a command as configured:

1. Select the command in the Command Tree and click Edit | Mark as Configured from the main menu. You will return to the main screen and the command will now be marked as configured. The icon will change to the configured icon and the status tip will now indicate that the command is configured.



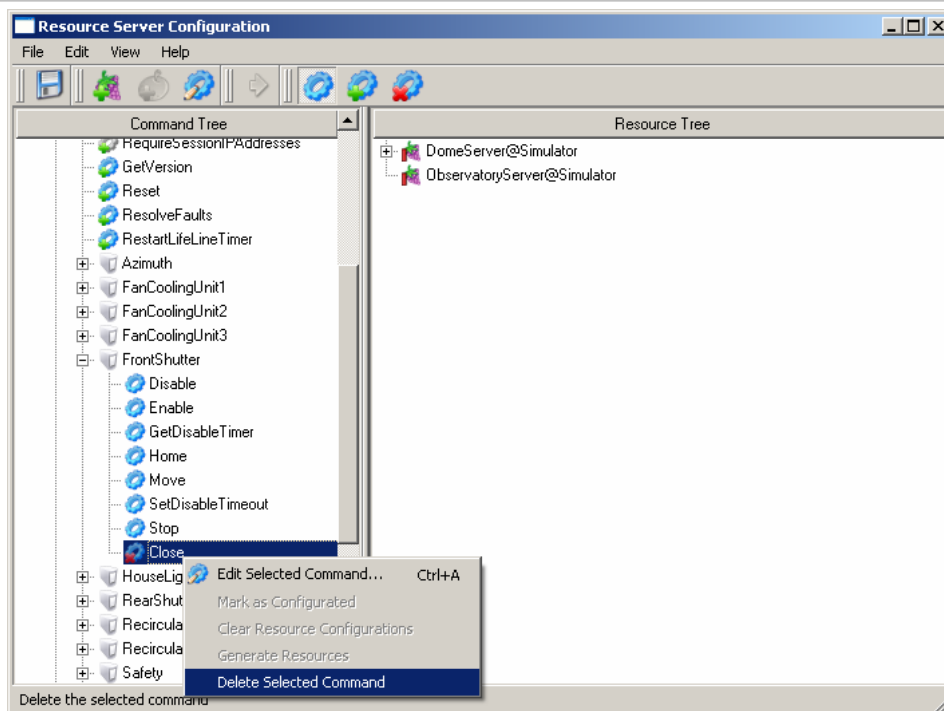
Marking a command as configured can also be initiated by right-clicking on the command and selecting “Mark as Configured” from the context menu.

8.2.2.13 Removing an unmatched command

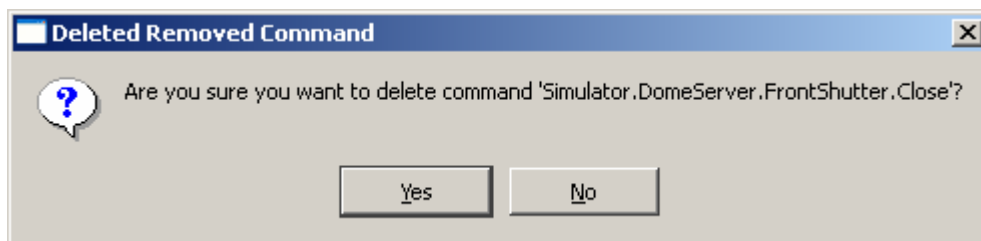
The application allows administrators to remove any unmatched commands. Unmatched commands are displayed with a red cross on the bottom left corner of their icon. Removing an unmatched command does not remove the command from the server schema. Rather, it removes the command entry from the resource configuration.

To remove an unmatched command:

1. Right click on the unmatched command. A context menu will be displayed.



2. Select “Delete Selected Command” from the context menu. A confirm message will be displayed.



3. Click the Yes button to confirm. You will be returned to the main screen and the command will no longer be visible in the Command Tree.

A command can also be deleted by selecting it and clicking Edit | Delete Selected Command from the main menu.

8.2.2.14 Changing command views

There are several different ways to view the commands in the Command Tree.

To view all commands:

1. Click on the View All Commands tool button or click View | View All Commands on the main menu. The command tree will display all available commands.

To view unconfigured commands only:

1. Click on the View Unconfigured Commands tool button or click View | View Unconfigured Commands on the main menu. The command tree will display only the commands that have a status of “Not Configured”.

To view unmatched commands only:

1. Click on the View Unmatched Commands tool button or click View | View Unmatched Commands on the main menu. The command tree will display only the commands that have a status of “Unmatched”.

8.2.2.15 Viewing the initialization report

To view the initialization report for the application:

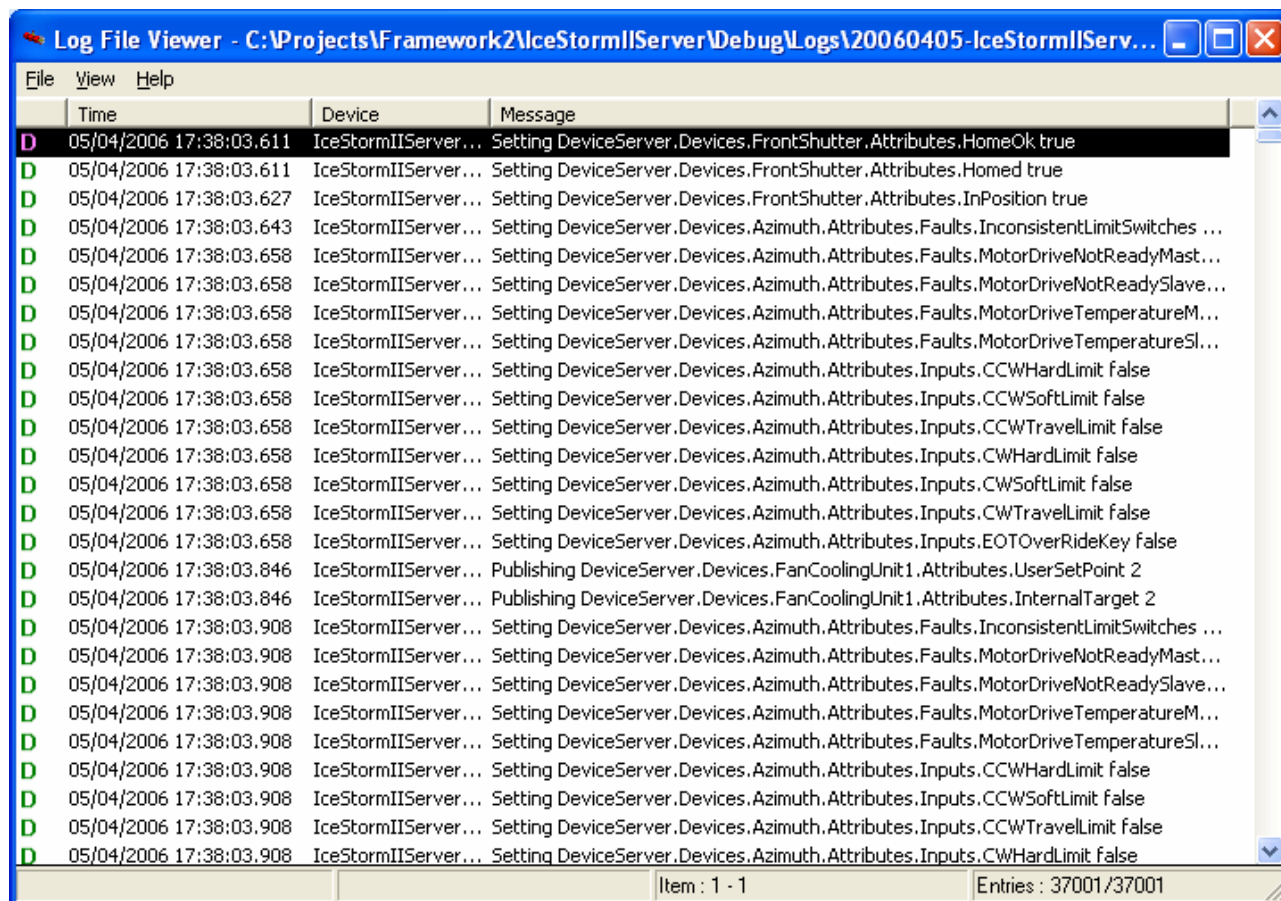
1. Click File | Report from the main menu. An initialization report containing the log that was generated when the application started will be displayed.

8.2.2.16 Saving changes

To save configurations back to the Configuration Server simply click on the Commit tool button. Note that if there is a loop(s) in a parent/child resource relationship or proxy relationship, the application will not allow the invalid configuration to be saved.

Changes can also be saved to the configuration server by clicking File | Commit on the main menu.

8.3 Log Viewer



Each EOS application writes diagnostic information to a log file (*.elf).

Log files are named in the format

YYYYMMDD-Application@Location-NN.elf

Log files contain a series of sequentially reported events. A new file is started each time a first log entry is recorded each day, or whenever the current file exceeds 5 Mb (in which case the number NN is advanced by 1). They are placed in a folder called Logs in the same folder as the application executable.

For each event, the date and time is recorded, accurate to within about 15 ms using the application's PC clock. Each log entry can be recorded as an exception, a state change, a diagnostic or a normal event. The server which made the entry is recorded, along with the text of the entry itself.

Log files can be viewed with the **Log Viewer**. The **Log Viewer** can also be used to search the list of log entries, display or hide all log entries sharing specified characteristics or export the log file as an ASCII file. To view a log file, open **Log Viewer** and drag the log file onto the **Log Viewer** window.

There is also a **LogServer** which collects log events from all servers and writes these to a log file in a similar manner to each EOS application. These system-wide logs are located of the DCC in `c:\eost\framework\servers\LogServer\Logs\`

Due to the complexity of the EOS applications, it is difficult to briefly describe the meaning of the log entries. EOS may request log files from time to time in order to assist in the diagnosis of technical and software problems.

9. FAULTS AND MAINTENANCE

This section describes regular maintenance of the software and how to diagnose and fix some problems in the system. It lists several known faults.

9.1 Software Maintenance

This section describes the software maintenance tasks which must be carried out to maintain trouble-free operation.

The software is relatively maintenance free and requires little additional maintenance effort beyond that given to normal computers, check disk space, the occasional disk defragmentation etc.

It is also suggested to carry out the following maintenance tasks as required.

9.1.1 Backup of Configuration files

The configuration files contain all sort of information to the various software components. This information includes data like range of travel, timeouts, last known positions, limits for currents etc. Some of the data is considered static in that it is set once when the enclosure is being commissioned, while other data is dynamic in that the applications update it as required.

The configuration for the enclosure can be found on the Dome Control Computer (DCC). It will be found on the c:\eost\framework\servers\configserver directory and sub-directories thereof.

9.1.2 Archival of old log files

Each server, and indeed some clients, in the system log various data into log files. This data can include general status information through to critical errors. Each component that uses the inbuilt logging service of the control system will generally create a log file at the location of the running executable file, and also send this information to the Log Server where all logging information is collated in a central location. There will be a new log file for each day (where a log entry was made – no log if no logging was required on that day), and a new file created once a size limit has been reached (currently five mega-bytes). There is currently nothing in the system to remove old log files, meaning that over time the hard drives will eventually fill up.

The Log Server can be found on the DCC machine. The log files are *.elf files and the centralized files can be found in the c:\eost\framework\servers\logserver\logfiles directory. There will also be log files in a Logs directory for each server, for example the Dome Server will be at c:\eost\framework\servers\domeserver with the log files in a Logs sub-directory under this.

9.1.3 Reboot the machines

The computers in the enclosure all run on Windows XP operating system. This is a big step forward in reliability terms compared to previous versions however it still benefits from the occasional reboot. If you find the system behaving in strange and unexplainable ways this should be one of the early troubleshooting trails.

9.2 Troubleshooting

Troubleshooting problems with the system involves first determining the cause of the problem and then finding a solution. Some problems and their solutions will be familiar to the long-time operator, while others may never have occurred before. Typical causes include operator errors, software bugs, and mechanical faults. Solving a problem usually involves simply removing the cause of the error. In extreme cases it may require redesign of a component. Occasionally the problem goes away when the operation is attempted a second time. This last type of problem, where the symptoms are intermittent, is the most difficult to diagnose and correct.

Whenever a problem occurs it is always a good idea to check the event log on the affected machine using *Log Viewer*. In the case of some problems the errors will be logged to the log file on the DCC. Most errors that occur are logged but not all are displayed to the user. Many of the errors are cryptic and can only be deciphered by suitably trained engineering support personnel.

If the problem is unusual, cannot be solved simply by repeating the offending command, or occurs frequently report it as soon as possible to authorized engineering support personnel describing the symptoms and what operation was being performed at the time and identifying the cause if you can.

If you can't see the reason for the problem try the operation again (or if necessary restart the system) but watch carefully for any signs of further problems. If problems persist contact authorized engineering support personnel.

Some common problems and their resolutions are described below. This list is by no means complete. Refer also to the section "Known Issues" which describes some known problems with the system. If after consulting these lists and checking the event log you cannot overcome a problem, seek technical assistance.

9.2.1 Common Problems

This section lists some of the more common problems and their possible resolution.

Applications fail to start

If an application shut down in an unusual way it may not have de-registered with the system. In this case a new instance of the application will not be able to start

because the system believes that there is already an instance of the server running. By using the System Management Interface (SMI) it will be possible to see the current status (according to the system) of the server. If its icon is grey and the Status is Not Contactable then use the de-register button to inform the system that the server is not running. Be sure that the server is not actually running before doing this, and it is often a good idea to check the processes tab on the Windows Task Manger to ensure that the process is not still running.

The Dome GUI displays orange indicator lights

If the GUI does not know the current state of some attribute it will colour the indicator light orange. The first step is to re-start the GUI and see if this resolves the problem. If not then the server (DomeServer@Dome) may need to be re-started. Use the SMI to do this.

what else?

Should it be necessary to re-start the system (or parts thereof) regularly please contact EOS for technical support and further advice.

9.2.2 Using Log Viewer to Diagnose Problems

Log Viewer is a tool for scanning the event log to look for clues to the cause of a particular problem.

There are two important characteristics of any error: text and context. The text comes from the *Message* part displayed by *LogView* and often contains enough information to diagnose the problem directly.

If this doesn't help you will have to consider the context of the error. Look for the first error message or event which occurred to see where the problem started. Use the timestamp on each event to determine which events occurred relatively close to the problem. If this doesn't help, look for the last related event to see the ultimate effect (e.g. the application terminated). Then check the errors and events in between to get progressively more contextual information.

9.3 Known Issues

There are several known issues with this version of the software.

Device Browser

If the *Device Browser* is running and is displaying the state of a server that is publishing a lot of information quickly this may heavily load the CPU to the point where the computer will become unresponsive. This is mostly only a problem if the Device Browser is subscribed at the server rate, see 8.1.4.4 for details.

Dome GUI

The Azimuth control panel of the Dome GUI has an Outputs tab that are always orange. The DomeServer is not publishing these attributes so the GUI cannot display any status. This will be fixed in a future version.

Shutter Firmware

The shutter firmware does not indicate if it is moving when in a manual mode (either software or hardware manual). The shutter states Stepping and Speeding are designed for these modes. This does not affect the functionality of the shutter, but is not desired.