Engage. Explore. Empower.

Connecting Visionaries in Radiation Safety, Science and Industry

MIRION Connect 24

Annual Users' Conference

July 29 - August 2 | Omni Dallas Hotel, Dallas, TX

MIRION TECHNOLOGIES

AIM Advanced Troubleshooting Tips and Tricks

Daniel Allen

Manager, Software Integration Engineering

Mirion Connect | Annual Users' Conference 2024

Dallas, Texas

MIRION Connect 24
Annual Users' Conference

Engage. Explore. Empower.

Introductions

MIRION Connect 24
Annual Users' Conference

Your Trainer

Daniel Allen

Manager, Software Integration Engineering

- Dallas, TX [Carrollton]
- 12 years in Nuclear Security
- Masters Information Systems Management
- Served as SW Lead, Project Manager, Engineering Manager

Function Keys

Function Keys

Video Advance – allows an operator to cycle through the alarm queue manually

Function Keys:

- **CTRL + Home** – move to the top of the alarm queue
- **ALT + Up** or **ALT + Down** – cycle through the queued alarm videos.

Mouse Selection:

- From the **Alarm Summary**, click an alarm. In the **DETAILS** pane, click **Play** to view the associated video.

Function Keys

Function Key	Action	Description
F1	Online Help	Opens the Online Help
F2	Expand UI	Expands UI to DETAILS Pane
F4	Silence	Silences the audible alarm at the workstation
F5	Acknowledge	Acknowledges the selected alarm on the Alarm Summary
F6	Clear	Allows the selected alarm on the Alarm Summary to be cleared
F7	Device Settings	Opens Device Settings
F8	Badges	Opens the Badges screen

Function Keys

Function Key	Action	Description
ALT + A	UI Menu Bar	Opens the AUTHORIZATIONS window
ALT + B	UI Menu Bar	Opens the BADGES window
ALT + C	UI Menu Bar	Opens the CONTROLS window
ALT + R	UI Menu Bar	Opens the AIM REPORT MANAGER application
ALT + S	UI Menu Bar	Opens the SUMMARIES window
ALT + T	UI Menu Bar	Opens the System window
CRTL + Print Screen	Screen Capture	Copy the active window
SHIFT + Print Screen	Screen Capture Desktop	Copy the entire desktop

Network Failure Detection Logic

Network Failure Detection Logic

- Basic tools for analyzing network problems – LINADM and PING

- LINADM
  - The LINADM tool provides an overview of the LINSYS nodes and connections.
    - If the connection is "up", the LINSYS node is communicating to the other LINSYS node.
    - If the connection is "down", the LINSYS node is not able to communicate to the other LINSYS node.
    - If the connection is "progress", the LINSYS node in progress is failing to be established properly. "Progress" state may require a rebuild of the LINSYS cache.

Network Failure Detection Logic

- When the System detects a problem and two nodes appear not to communicate, basic tests can help assess the situation

- PING
  - The ping command tests the network link between two machines.
    - Open a Command Prompt and ping the network link between the computers.
    - Run the ping with the same names in the LINSYS configuration.
      - If ping reports errors on both sides, it is likely a hardware problem, a TCP/IP configuration issue, or a LINSYS configuration issue.
      - If ping reports errors on one side only, it can be a TCP/IP configuration issue.
    - Open Windows Task Manager on each computer.
    - Check that the LINSYS processes are running.

Understanding Failover

Understanding Failover

- A system failover occurs when the backup server takes over the functions of the primary server. Failover occurs automatically when a critical hardware or software error is detected.

- Critical Hardware Failure
  - When the backup system is unable to detect the primary server. The cause of the failover may be the failure of the primary server, the auxiliary memory, or the I/O subsystem.
  - When a critical process on the primary host processor fails and the system is unable to restart it. Failover also occurs if software fails while performing a critical task.

Understanding Failover

- The backup server starts as the primary server in a warm start. Software restarts as necessary and redirects all peripheral devices to the new primary.
  - When the system detects a failover, the backup server starts within 30 seconds as the new primary server.
  - Within 60 seconds, the backup server is operating as the primary server at the same operating level as before the failover and with no loss of data.

Understanding Failover

- The server that had been the primary before failover tries to restart as the backup server.
  - It tries to startup as the Backup server to a maximum number of times according to the MAX_STARTUP_ATTEMPTS configuration option found in integration_process.txt.
  - If it is unable to restart itself, check the server for error messages to identify and correct the problem
  - If it cannot correct the problem, it restarts the server as the backup.

- An administrator can initiate a manual failover from any server or workstation. A manual failover might be performed to investigate a system-wide problem or to perform preventive maintenance.

Diagnosis and Recovery

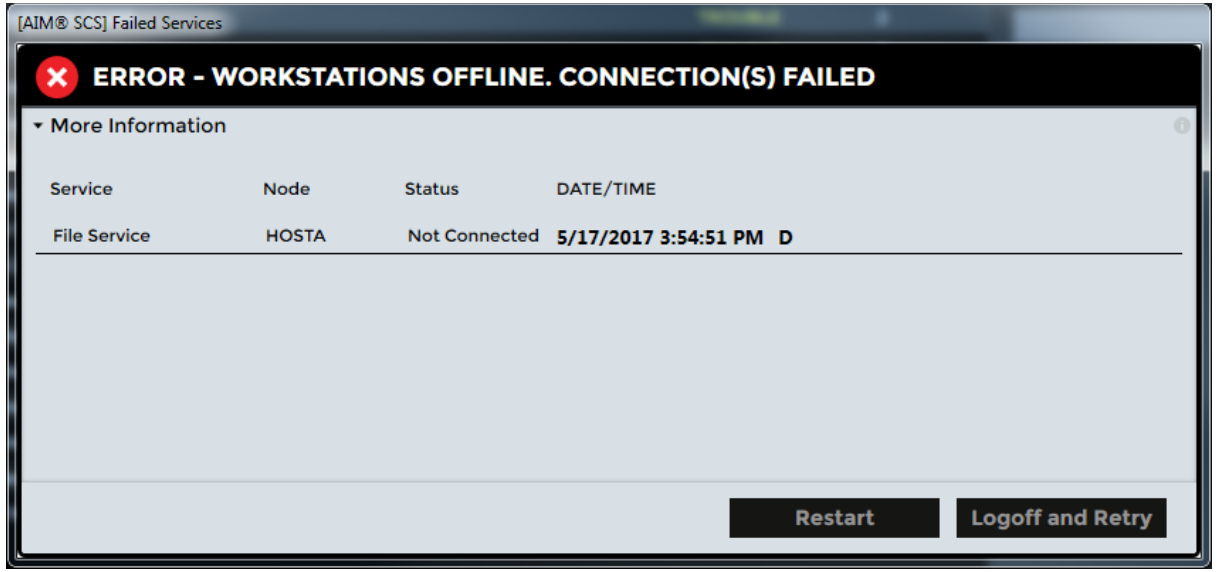
Diagnosis and Recovery

- AIM UI Startup Failure
  1. Verify the presence of the AIMSCS.exe executable in aimref/site/bin/AIMSCS folder
  2. Open the most recent log file (aimref/site/log/AimScs.log). Check for error messages.
  3. Open the Windows Event Viewer (Windows Logs | Application) to view application errors and warnings.
  4. Verify that all environment variables are set to the correct value.

Diagnosis and Recovery

Workstation AIM UI Connection Failure

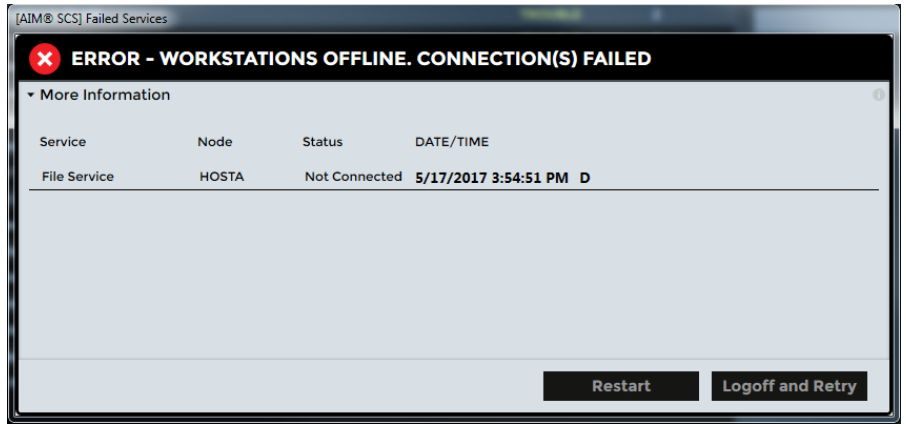
- If a connection failure occurs and the system exhausts all attempts to reconnect the services, one or more windows display **Error - Workstations offline. Connections Failed**



Diagnosis and Recovery

Workstation AIM UI Connection Failure – Con't.

- When this window displays:
  - Use the Task Manager to determine which services are running.
  - Verify that the primary server is ready.
  - Click **Restart** to let the workstation retest the connection. This closes and opens the UI.
  - If the problem persists, click **Logoff and Retry**. The system logs off and tries to connect to all of the required services. When logged out, the button is **Retry**.



Diagnosis and Recovery

Workstation AIM UI Connection Failure – Con't.

- If the problem persists:
  - Determine if a loose connector, a bad cable, or other hardware fault related to the network connection is at fault.
  - Look under the Node heading to find the machine where the problem is occurring. This machine may be a workstation or a Host.
    - On the problem machine, open Task Manager.
    - Determine if the required AIM SCS services are running.
    - Restart those services as needed.
- When the AIM UI re-establishes a connection to a service, the Connection Failed screen closes. Once connections to all services are established, the system opens and a user can log on.

Control Panel Debugging

Control Panel Debugging

Debug a Control Panel when:

- Bringing up a Control Panel for the first time.
- Troubleshooting Control Panel connection issues.
- Troubleshooting alarm point issues (alarms not coming in when expected, wrong alarm coming in, etc).
- Troubleshooting door access issues.

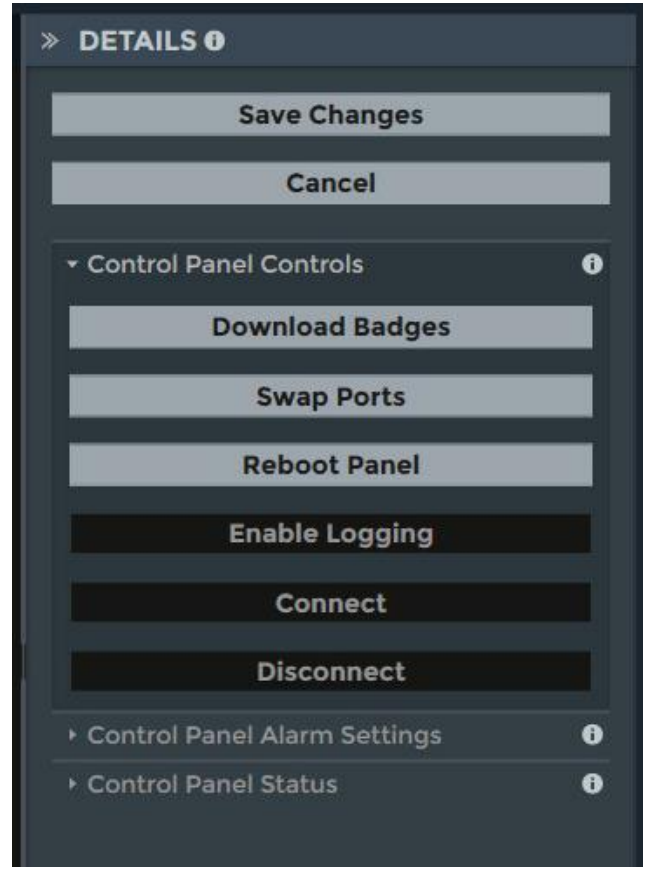
Things to remember:

- Control panel “debug” files have no size limit. Avoid leaving this turned on for large periods of time (2 weeks or more).
- The data is appended to an existing file, so delete any old files if a clean download is needed.

Control Panel Debugging

Set Up to Debug a Control Panel

1. Open Control Panel Controls in the DETAILS pane.
2. Select **Enable Logging** to start the action to create the debug file.
3. Select **Disable Logging** to stop the action of creating the debug file.



Output filename is xxx.txt where xxx is the Control Panel ID (CPID)

Control Panel Debugging

To capture a complete download

1. From the Control Panel Controls select the **Disconnect** option. This reboots the panel and keeps it unconnected.
2. Select **Enable Logging** to activate debugging.
3. Select **Connect** to reconnect with host with a complete download.
4. Once the panel is NORMAL, select the **Disable Logging** option to deactivate the debugging session.
5. Send Mirion Technologies the debug file.

Periodic Maintenance

Periodic Maintenance

Weekly Maintenance

- Check AIM Host total CPU utilization
- Check AIM Logs
- Check Windows Logs
- Check Server Status
- Check Host drives
- Check all server drives
- Check LINSYS health
- Check Oracle Exports

Periodic Maintenance

Monthly Maintenance

- Perform Backups

Semi-Annual Maintenance

- Review the User Rights on the Domain
- Review the *PSCS_User* and the *PSCS_Video* rights on the Hosts
- Review the Oracle SQLNet parameters
- Test AIM Failover – when complete the system is on the original host and both servers have been cold booted
- Remove Dust from all Servers
- Examine Network Switch Logs

Periodic Maintenance

Annual Maintenance

- Disk De-Fragmentation
  - Oracle backup
  - De-Fragment
- Remove Dust From All Servers and Workstations

Thank you – Questions?