

What Does "Active System Console" Mean, and How Can I Access It?

TechRounder Help Center PDF

Live article: <https://www.techrounder.com/help/what-does-active-system-console-mean-and-how-can-i-access-it/>

By Vipin PG | Published May 15, 2026 | Updated May 15, 2026 | Topic: Solution | 4 min read

An Active System Console (ASC) is a web-based server management interface that gives IT administrators a real-time dashboard view of a server's hardware health, event logs, and system configuration - all without requiring physical access to the machine. The most widely known implementation is the Intelfi Active System Console (IASC), designed for Intel server boards and systems.

Think of it as the control panel for your server hardware. Instead of opening a chassis or rebooting into a BIOS menu, you log in through a browser and get a complete picture of what's happening at the hardware level.

What the Active System Console Shows You

- System Summary: Server name, BIOS version, GUID, IPMI version, firmware details
- Hardware Health: Chassis status, processor, memory, storage, cooling fans, voltage, and power sensors
- System Event Log (SEL): A full log of hardware-level events and alerts
- Configuration Options: Network settings, BMC (Baseboard Management Controller) configuration, serial-over-LAN, BIOS settings
- Asset Tracking: View installed components without opening the server
- Alerts: Email and SNMP notifications for hardware failures or threshold breaches
- Software Updates: Check for available firmware, BIOS, or driver updates

How to Access the Active System Console

Method 1: Web Browser (Remote or Local Access)

This is the primary and most common method. IASC runs a lightweight local web server on the host machine, accessible from any browser on your network.

1. Open a web browser (Firefox or Chrome recommended).
2. Navigate to the following URL, replacing 'SERVER_IP' with your server's IP address:
'https://SERVER_IP:9393/asc/'
3. You will likely see a browser certificate warning - IASC uses a self-signed SSL certificate. In Firefox, click Advanced > Accept the Risk and Continue . In Chrome, click Advanced > Proceed to [IP] (unsafe) . This is expected behavior on a trusted internal network.
4. Log in with your credentials. The factory default is: 'Username: admin Password: admin' Important: Change the default password immediately after first login. Leaving it as 'admin' is a serious security risk.
5. On first login, the console may be unresponsive for a few minutes while it collects initial hardware data. This is normal.

Method 2: Windows Start Menu (Local Access on the Server)

If you are physically at the server (or logged in via RDP) and IASC is installed on a Windows system:

1. Click Start > All Programs > Intel Server Management Software .

2. Select Intelfi Active System Console .
3. This opens the IASC login page in your default browser automatically.

Method 3: Skyhigh / McAfee Web Gateway Appliances

If you are working with a Skyhigh Security (formerly McAfee Web Gateway) hardware appliance, ASC access works slightly differently:

1. Connect to the appliance's management network.
2. Access via browser using: 'https://<appliance_IP>:9393'
3. Set an administrator password when prompted on first run. ASC starts automatically with the appliance on subsequent boots.
4. To disable ASC on this platform, run the following command via SSH: 'asc-disable'

Installing the Intel Active System Console (If Not Already Installed)

1. Download the IASC package from Intel's Download Center . Search for your specific server board model to find the compatible version.
2. On Windows: Run the installer executable with administrator privileges and follow the setup wizard. You will be prompted to reboot after installation.
3. On Linux: Run the installer package with root privileges: 'sudo ./install.sh'
4. After installation and reboot, access IASC via browser at 'https://localhost:9393/asc/' locally, or via the server's IP remotely.

Firewall Configuration for Remote Access

If you can access the console locally but not from a remote machine, the server firewall is almost certainly blocking the required ports. Open the following TCP ports on the server's firewall:

- 9393 - IASC web interface (required for remote access)
- 9191 - lighttpd web service
- 7777 - backend IPC socket

On Windows Server, add these as inbound rules in Windows Firewall. On Linux, using 'firewalld':

```
sudo firewall-cmd --permanent --add-port=9393/tcp
sudo firewall-cmd --permanent --add-port=9191/tcp
sudo firewall-cmd --permanent --add-port=7777/tcp
sudo firewall-cmd --reload
```

Common Errors and Fixes

- "Data is being retrieved, please retry" - Check that ports 9393, 9191, and 7777 are open on the firewall. Wait a few minutes for IASC to collect initial hardware data.
- "You are offline" - Verify the network connection between your browser and the server's BMC (Baseboard Management Controller). Ensure the BMC network interface is configured and reachable.
- Browser shows "Untrusted Connection" or "Invalid Certificate" - IASC uses a self-signed certificate. Override the browser warning to proceed (on a trusted internal network), or install your own certificate as described in the IASC User Guide.
- Buttons unresponsive in Internet Explorer - Go to Tools > Options > Security > Internet Zone > Custom Level > Scripting and enable all Active Scripting options. Use a modern browser like Firefox or Chrome instead.

Official sources and references

1. intel.com - content / www - <https://www.intel.com/content/www/us/en/download-center/home.html>