Connecting to ISAAC

Using the ISAAC Workspace

ISAAC® Workspace is the operational portal and main management interface for your ISAAC® system. In the Workspace users can access defined Control Panels, view and update the Schedule, use ISAAC®'s advanced monitoring features, and manage the system.

As a standards-compliant web application access to the Workspace only requires a network connection and a modern browser. ISAAC® also supports limited access from tablets and mobile devices.

Integrating Systems

Using the built-in ISAAC® Connect™ features you can centralize network access to other system components in the ISAAC® Workspace. ISAAC® Connect™ allows you to open VNC, Remote Desktop, SSH, or Telnet connections directly in the browser. End users no longer need to download clients and have spreadsheets of addresses and credentials; the ISAAC® Workspace securely stores details for each connection allowing administrators fine-grained control of access to all connected systems.

Users can customize and organize their Workspace to suit their needs. Every user can choose what items are visible and how those Control Panels are sorted and displayed, empowering them to take charge of their environment and best use the tools they need.

As a browser-based system this configuration is automatically applied no matter where or how that user is connecting, all without complicated management or overhead.

Working Remotely

The only requirement for use of the ISAAC® Workspace is network access to the system.

For systems that desire remote access all that is needed is extension of the network from ISAAC® to the user through a VPN or similar technology. All ISAAC® features and hardware fully support routed IP traffic, so existing IT teams and infrastructure can be leveraged natively. The ISAAC® Workspace uses standard HTTP and requires no special firewall rules to be made.

ISAAC® does not proxy connections between end users and devices that may be serving Control Panels. This means that for a user to have access to a Module's panel(s) they will need network access to those devices. When implementing routing, firewalling, or VPNs the client <-> device path must be considered for users to have access to those items.

There are no limitations to where ISAAC® Workspace native Control Panels (management/scheduling features, CMS features, and ISAAC® Connect™ panels) may be accessed from as they are internal to the ISAAC® system.

Remote Management

All ISAAC® hardware is designed from the beginning for remote access and network management. ISAAC® servers have dedicated management connections on all configurations. There are no operational requirements for KVM connections to ISAAC® hardware, ISAAC® servers can be fully managed over the network (including a built-in Browser-based KVM for advanced troubleshooting when needed).

By leveraging the Monitoring and Logging features of the ISAAC® Workspace users can oversee and maintain their systems from anywhere with network access from the devices of their choosing.

Technical Specifications

Supported Browsers

- Preferred: Google Chrome (version 70 or greater)
- New Microsoft Edge
- Firefox (version 65 or greater)
- Safari (version 13 or greater)

ISAAC® Connect™ supported protocols

- SSH
- Telnet
- VNC
- Microsoft Remote Desktop

Required incoming protocols/ports

- HTTP(S) – TCP: 80, 443, 8099

Optional incoming protocols/ports

- HTTP(S) – TCP: 8000, 8080
- HTTP(S) – TCP 9000
- SSH – TCP:22 (for Debug)
- RESP - TCP: 6379
- PostgreSQL - TCP: 5432
- Node-Red - UDP: 5000-32000 (Blocks of 20 ports)

Optional outgoing protocols/ports

- SSH – TCP: 22 (Default)
- Telnet – TCP: 23 (Default)
- VNC – TCP: 5900 (Default)
- RDP – TCP&UDP: 3389 (Default)
- Updates – TCP: 80/443 (Default)
- SMTP – TCP 465/587 (Default)
- SNMP – UDP 161 (Default)