TECHNICAL DATA SHEET

Controls-Cloud by Cochrane Supply

TABLE OF CONTENTS

PRODUCT DEFINITION

Controls-Cloud by Cochrane Supply is a managed virtual machine hosting service that is purpose-built for the building controls industry. It provides contractors and system integrators with a simple, secure way to deploy Windows or Linux servers for hosting building automation supervisory software in the cloud. Designed for reliability and cybersecurity, Controls-Cloud integrates multifactor authentication and encrypted remote access to safeguard both technician and end-user connections. The service leverages trusted global cloud providers and includes scheduled data backups to ensure operational continuity. Delivered as a subscription, Controls-Cloud enables contractors to deliver scalable, professional, and secure hosting for their customers' building automation systems without the complexity of managing infrastructure.

Standard Server Configurations

Controls-Cloud offers several standard server configurations to meet a range of performance and project requirements. Each option is available with either the latest **Windows Server** or **Ubuntu LTS** operating systems.

Server Tier	vCPU	Memory (RAM)	Storage
Standard	4	8 GB	128 GB SSD
Moderate	8	16 GB	240 GB SSD
Large	12	32 GB	512 GB SSD
Enterprise / Custom	Custom	Custom	Custom

TECHNICAL OVERVIEW

Controls-Cloud provides a **fully managed** hosting environment that simplifies deploying and maintaining building automation servers in the cloud. Cochrane Supply handles all configuration, security, and connectivity of the underlying technologies. The result is a secure, reliable, and professionally supported platform for hosting and accessing building automation systems in the cloud.

Host Platforms

Controls-Cloud operates on trusted global cloud providers including **Hetzner**, **OVHcloud**, **DigitalOcean**, **Microsoft Azure**, and **Amazon Web Services**. These platforms offer high availability, strong physical and network security, geographic redundancy, and scalable performance to meet the demands of modern building automation systems. Cochrane Supply manages all provisioning, maintenance, and monitoring, so customers never need to create or maintain their own cloud accounts. Host platforms for standard server options are selected based on reliability and cost-effectiveness, but deployments can be arranged on a specific provider when project requirements call for it.

Secure Building Network Connectivity

Securely connecting remote building networks and OT / BAS devices to your cloud server is critical. Our recommended connectivity approaches are designed to preserve isolation, encryption, and ease of deployment while allowing remote sites to seamlessly integrate with your BAS supervisor software. We have two recommended connectivity methods: dedicated edge routers from **Teltonika** + virtual private overlay networking with **ZeroTier**, and the open standard **BACnet Secure Connect** (BACnet/SC).

Teltonika Routers

We recommend using industrial-grade routers from Teltonika Networks. These routers are designed for professional / industrial deployment with robust hardware and hardened firmware (RutOS, based on OpenWRT). For example, the **RUTX10** router offers gigabit Ethernet ports, VLAN support, and integrated VPN options, Wi-Fi, Bluetooth, and remote management capability. When cellular connectivity is required (e.g. remote sites without wired WAN links), the **RUTX11** (or similar cellular model) provides LTE / cellular fallback or connection, giving flexibility for remote or mobile sites. These routers are cost-effective compared to custom hardware or expensive edge appliances, and are easy to manage remotely via Teltonika's management system.

ZeroTier

ZeroTier is a software-defined network overlay that acts like a distributed network hypervisor: it creates a virtual private network (VPN + SD-WAN + overlay) that connects devices, VMs, containers, and edge routers across wide area networks **as though they were on the same local network**, all without the need to punch holes in firewalls or involve end user IT departments.

All traffic is end-to-end encrypted using strong cryptography. ZeroTier networks enforce private virtual LAN boundaries, use cryptographic identities for devices, and preserve privacy by minimizing metadata.

Teltonika routers support a built-in ZeroTier agent, making it easy to set up. Our recommended configuration joins the Teltonika router's local LAN to the ZeroTier virtual network.

Cochrane Supply handles the setup and configuration of the ZeroTier virtual network. Controls-Cloud customers only need to set up their routers to join the virtual private network. This simple process consists of entering a provided ZeroTier Network ID, and sending in your corresponding ZeroTier Node ID and LAN information.

BACnet Secure Connect

BACnet Secure Connect (BACnet/SC) is a modern secure transport layer for the BAS / BACnet world. It replaces or augments traditional BACnet/IP or MSTP, but adds encryption, certificate-based authentication, and reliable TLS + WebSocket channels. In this architecture, supported remote building devices (BACnet/SC nodes) maintain **outbound** TLS (HTTPS / WebSocket over TLS v1.3) connections to a hub in the cloud or central location, so there is no need to open inbound firewall ports or rely on UDP broadcast or BACnet BBMD tunneling. The remote nodes only need outbound internet connectivity to reach the hub; they do not require poking firewall holes or static IPs. The cloud-hosted supervisor (e.g. running the Niagara Framework in the Controls-Cloud VM) is capable of hosting the BACnet/SC hub endpoint, making integration seamless for remote building connectivity.

Secure Technician Access

Protecting privileged access to your cloud server is essential. Controls-Cloud enforces multi-factor authentication for every technician session, ensuring that only authorized personnel can access the infrastructure.

Keeper Connection Manager

We use Keeper Connection Manager, a web-based remote access gateway developed by Keeper Security. It provides agentless, **web browser-based remote access** to your server's operating system. Users authenticate with a username/password plus a time-based one-time passcode (TOTP) provided by their registered authenticator (e.g. Duo, Microsoft Authenticator, Google Authenticator). Cochrane Supply handles the deployment and configuration, so customers simply log in via web browser and select their server.

Twingate

We also support Twingate, a zero-trust network access solution. Twingate requires a client application to be installed on Windows or mobile devices, and authentication requires a username/password and a time-based one-time passcode (TOTP) provided by a registered authenticator (e.g. Duo, Microsoft Authenticator, Google Authenticator).

The client establishes an encrypted TLS tunnel to your Controls-Cloud virtual private network, and because of its peer-to-peer / NAT traversal design, there is no need to open inbound firewall ports. Your device will appear to be on the same private network as your cloud server, enabling you to use **locally installed tools** to directly connect to your cloud server or virtual private network devices.

Secure End User Access

Exposing the web dashboards or user interfaces of your building automation system (BAS) to the public internet introduces significant risks: credential theft, replay attacks, phishing, brute-force attacks, unauthorized access, or exposed sensitive building or occupant data. A compromised dashboard can allow attackers to interfere with HVAC,

access occupancy data, or disrupt operations. To protect end user exposure, we enforce access controls and multi-factor protections.

Pangolin

Controls-Cloud uses Pangolin by Fossorial, a tunneled reverse-proxy and identity-aware access control platform. It acts as a secure reverse proxy and access gateway for web applications, enabling you to expose private dashboards without opening firewall ports or directly exposing servers. It supports email whitelisting and one-time passcodes (OTP) sent via email as a second factor.

When configured, only users from your authorized email domains or individual email addresses can request access; they receive a one-time passcode which must be entered to reach the BAS supervisor's web interface. Because access is tied to valid email accounts, once a former employee loses access to their corporate email, they no longer receive passcodes — effectively revoking their dashboard access automatically.

Data Backup and Retention

Reliable data protection is a fundamental requirement for maintaining operational integrity and recoverability. Controls-Cloud implements a managed backup strategy to ensure that critical files and configuration data can be restored in the event of data loss, corruption, or system failure.

Synology Active Backup for Business

Backups are performed using Synology Active Backup for Business, a secure and widely adopted enterprise backup solution. This platform supports encrypted data transfer, integrity verification, and granular recovery options. Cochrane Supply manages the entire backup process, including scheduling, monitoring, and restoration. Customer file data is backed up to an off-site Synology storage system twice weekly. Both full and individual file restores are supported, allowing recovery to any previous version retained by the system. All backup data is preserved for a minimum of 30 days following the end of a Controls-Cloud subscription, with assistance available for data export upon request. Backup data may also be destroyed at an earlier date upon request.

CYBERSECURITY FAQS

Is Controls-Cloud SOC 2 Type II certified?

Controls-Cloud and Cochrane Supply are not SOC 2 Type II certified, however the Controls-Cloud product is designed and provisioned in compliance with SOC 2 Type II, and all Controls-Cloud host platforms are SOC 2 Type II certified. This answer also applies to FedRAMP, StateRAMP, and ISO 27001 certification. While Cochrane Supply does not hold those certifications, our host platforms do.

If this is a concern, all potential access to your server from Cochrane Supply (such as access to assist with setup or troubleshooting) can be revoked.

Is server data encrypted in transit and at rest?

Controls-Cloud's recommended access and connectivity strategies utilize secure, encrypted protocols for data in transit (ZeroTier, Keeper Connection Manager, Twingate, Pangolin, BACnet/SC, Synology Active Backup for Business, etc.). Data is not encrypted automatically at rest. Customers are free to install additional software on their servers to provide this functionality.

Is vulnerability scanning and penetration testing provided?

Any kind of vulnerability scanning or penetration testing must be provided and performed by the customer if required. Controls-Cloud servers are provided for the customer's exclusive use. Customers are free to install additional security software and perform penetration testing against any access points to the system. Do note that server tier recommendations do not include considerations for additional software, and higher tiers may be necessary for this kind of software.

Does Controls-Cloud provide a documented Disaster Recovery Plan? Or physical security details?

Controls-Cloud itself does not have a documented Disaster Recovery Plan, but one can be obtained from our host platforms, as well as details about their physical security. It is up to our customers to incorporate their Controls-Cloud servers into any of their own Disaster Recovery Plans that they may provide to end users. Any additional software required can be installed by our customers onto their server.

Are Windows/Linux updates automatically installed?

Operating system updates are not set up for automatic installation when you receive access to your Controls-Cloud server. All automatic updates must be set up and configured at the customer's discretion.

Can technicians share privileged access to a Controls-Cloud server?

Technicians cannot share their privileged access to their Controls-Cloud server with other identities. Keeper Connection Manager and Twingate require each technician to register their login with an authenticator that they must have access to at all times (such as on a mobile phone).

How is Cochrane Supply able to access my Controls-Cloud server? How is this access secured?

Cochrane Supply can log in to your server using Keeper Connection Manager for setup and troubleshooting assistance. This can be revoked at any time by changing your Windows or Linux admin password (but please notify us in advance so you do not negatively impact your own access).

Cochrane Supply technicians do not share access of any kind, and have individual accounts secured with the same level of multi-factor authentication as customers. Accounts are created for specific, privileged employees who provide direct assistance to customers. These employees receive annual information security training. If an employee is terminated or departs from the company, their access is automatically revoked.