OvrC Security and Privacy Standards

ADI Global Distribution Inc. (referred to herein as “ADI”) are committed to the security, availability, and privacy of the OvrC software platform. This document provides information about the measures ADI employs with respect to OvrC’s security, availability, and privacy. It also provides information about the security features and functions available to integrators and end users.

White Paper | August 2026

Abstract

OvrC is ADI's remote monitoring and management (RMM) platform that enables integrators to configure, manage, and troubleshoot IP-enabled devices via a secure internet connection from any location. ADI also provides a consumer-facing application called OvrC Connect that allows integrators to give their customers self-help troubleshooting tools.

Using OvrC, integrators can manage the activities of an end user's network devices through a secure internet connection. This includes updating firmware, monitoring system health and performance, adjusting configurations, and configuring predefined self-healing behavior to address device malfunctions.

ADI prioritizes security and privacy because it recognizes the importance of secure access to end users' networks and devices. OvrC is designed and operated in accordance with industry standards such as NIST and other tech industry methodologies. ADI also routinely leverages third-party security assessors to validate OvrC's cybersecurity posture.

This document assumes that readers are familiar with cloud computing and secure network communications technologies.

How OvrC operates

OvrC is a Software as a Service (SaaS) platform that can be used on any device with an internet connection. OvrC uses two distinct methods to enable devices to communicate with the platform.

1) OvrC-enabled devices: These connect directly to OvrC by leveraging persistent WebSocket connections that allow bidirectional communication between the OvrC user and the device connected to the OvrC platform. This method only allows communication with the device. It does not perform network scans or speed tests, minimizing OvrC's impact on network traffic. Examples of OvrC-enabled devices include WattBox power conditioners, Araknis access points and switches, and Episode amplifiers.

2) OvrC Pro devices: In addition to performing the functions of an OvrC-enabled device, these devices scan for IP devices connected to the local network, perform periodic network health checks, execute port scans on the LAN, and run speed tests, all on schedules defined by the integrator. Finally, OvrC Pro devices can communicate with IP devices that are not OvrC enabled. Examples of OvrC Pro devices include Araknis routers, Control4 controllers, and OvrC Pro Hubs.

Device claiming

When an OvrC-enabled or OvrC Pro device connects to the internet, that device communicates securely to the OvrC servers. OvrC then creates a record for that device using its globally unique MAC address.

As part of securely mapping devices to a specific owner and location, an integrator creates a record for the end user in their OvrC account, adds a location for that end user, then claims the device at that location on behalf of that end user. Claiming the device requires the integrator to provide the device's MAC address and Service Tag number to validate that they have custody of the device. OvrC then appends the device record, attaching it to that integrator and end user.

Additionally, once installed, an OvrC Pro device scans the network periodically, claims devices discovered through the scan, and maps them to the location.

Application security

OvrC is a proprietary platform developed by ADI personnel. While ADI occasionally leverages third-party developers under strict contract protection, ADI retains full ownership of all the code.

As detailed below, ADI employs a defense-in-depth strategy to protect against various threats, meaning that ADI implements multiple layers of security to safeguard systems and data. This layered approach to security is applied to all levels within the organization. ADI's engineers and cybersecurity personnel take proactive measures to protect integrator and end-user data. These teams work collaboratively to prioritize the safety of ADI products, applications, websites, and services.

ADI regularly enhances OvrC's security and data integrity through updates, patches, and configuration changes, providing advisories to integrators as needed. ADI employs threat intelligence and industry security reports to monitor and address threats to automation and smart-living environments and allow for rapid detection and mitigation in the event of a cyber compromise.

Secure coding

OvrC software engineering updates are made through a code repository management system. Code updates are deployed to cloud instances using a configuration management tool with code rollback capability. Artifacts are built on an automated integration and delivery platform, stored in a cloud storage service, and retrieved by cloud instances via the configuration management tool. Industry-leading tools perform routine static and dynamic code analysis evaluating for OWASP Top 10 vulnerabilities. Static code analysis and container scanning tools scan all push requests before publishing an update. Once a build is published, the dynamic code analysis tool monitors its integrity.

Security and penetration testing

ADI adopts many techniques through the product development lifecycle to test system security. The ADI team examines applications from the inside out as part of the CI/CD pipeline, searching for conditions that may indicate a weakness or vulnerability. The team also performs regular web application penetration testing on the platform to imitate the behaviors that an attacker may use to circumvent security controls. The following resources safeguard OvrC's code:

- **Dedicated security team:** ADI engineering and security teams are on call 24/7 to respond to security alerts and events.
- **Training and awareness:** ADI employees are periodically trained in security best practices, emerging threats, and data privacy.
- **Network vulnerability scanning:** OvrC's cloud platform undergoes regular internal and external vulnerability scanning to identify vulnerable systems.
- **Threat intelligence & vulnerability feeds:** ADI regularly reviews various threat intelligence feeds. This proactive monitoring raises visibility to risks and promotes overall security posture.
- **Cybersecurity incident response:** In the case of potential incidents, an investigation is escalated to the ADI cybersecurity team and pertinent product and legal teams. Each team is regularly trained in cybersecurity incident response processes, comprising preparation, identification, containment, eradication, recovery, and lessons learned phases. These processes are designed to assess and resolve the situation quickly, regardless of timing.
- **Software scanning / external reviews:** OvrC cloud software undergoes ongoing cybersecurity code scanning and reviews as part of the product software development lifecycle. This approach proactively identifies vulnerabilities, insecure coding, and adherence to security standards. Identified issues are assessed and addressed in accordance with risk.
- **IP-based products:** ADI employs an independent cybersecurity company to conduct vulnerability tests on a subset of the company's IP-based products and platform.

Perimeter security

ADI's perimeter security includes several key practices:

- **Security defenses:** OvrC resides behind Cloudflare, which provides firewalls, bot deterrence, DDoS protection, and custom rules to protect against vulnerabilities specific to OvrC.
- **Patch and security update management:** OvrC keeps hosts up to date with security patches to address known vulnerabilities.
- **Continuous vulnerability management:** ADI regularly scans servers to detect and address system-level vulnerabilities.
- **Logging and auditing:** ADI logs critical system activities, and audits the logs for unusual activity.

Network security

OvrC has adopted the NIST 800-171 guidelines for security standards.

ADI network security architecture consists of multiple security zones. More sensitive systems, like database servers, are protected in the most trusted zones. Other systems are housed in zones commensurate with their sensitivity, depending on function, information classification, and risk. Depending on the zone, additional security monitoring and access controls apply. DMZs operate between the corporate network and the internet, and internally between different zones of trust.

System alerts are handled by on-call cybersecurity and cloud incident response teams, which provide operations, network engineering, and security coverage.

Data transmission and storage

ADI has adopted industry standards (including encryption, web application firewalls, and SSL) to safeguard the platform's security and protect the confidentiality of personally identifiable information. OvrC requires that data be accessible wherever the integrator may be. OvrC saves data securely in the cloud using leading cloud providers. All data is encrypted at rest and in transit, and access to data is minimized per the principle of least privilege. While at rest, data in the OvrC databases is encrypted using AES-256. When data needs to be processed, it is decrypted, used, and then discarded or encrypted before storage. OvrC also supports TLS encryption of email.

Communication between the device and OvrC

All external OvrC communication is initiated by the device. Most devices use the HTTPS protocol, which encrypts communication to the OvrC servers with SSL/TLS. Many third-party devices, as well as ADI's OvrC-enabled devices, have a local user interface used for configuration. If supported by a third party device's technology, an OvrC Pro device can establish a secure communication tunnel to the device's local user interface. When a tunnel is established, it stays open for a limited time. For continued communication after this period, the device must initiate a new tunnel.

Identity and access management

Integrator access and end-user authentication are handled using a leading identity platform. OvrC can be configured to use a designated single sign-on (SSO) platform and offers multifactor authentication capabilities.

User management

Each custom-integration business is assigned a unique OvrC account, with the capability of creating individual user accounts for each integrator employee. The business is responsible for adding, removing, and managing access through OvrC's Groups and Permissions feature. The group(s) to which integrator employees are assigned determines their access to end users and devices. Businesss create groups to fit their needs and customize permissions for each group as their business requires. Each integrator employee or shared user can belong to multiple groups. Changes made to a user's permissions are instantaneous, and when a user is removed, all active web sessions for that user are immediately terminated. The business is responsible for managing access rights to its OvrC account.

Permissions fall into the following categories:

- **Owner:** Registered account owner and has all administrative permissions. Each account has only one owner.
- **Administrative:** Controls corporate account settings, users, groups, and permissions.
- **Delete:** Can remove customer devices, locations, and accounts.
- **Snapshots:** Able to view still images from surveillance and media over IP.
- **Access:** Adjust which customers' systems a group can monitor.

Shared access

In cases where users require access to a customer/location that is associated to a different business account, existing users can be granted shared access to specific customers and locations. As with employees, access and permissions are managed through the Groups and Permissions feature.

Physical security

ADI leverages Amazon Web Services (AWS) for OvrC cloud services. All physical and operational security processes are detailed in AWS's comprehensive security overview documentation, which outlines their data center controls, including:

- Physical and environmental security
- Fire detection and suppression
- Power management
- Climate and temperature regulation
- Storage device decommissioning
- Fault-tolerant infrastructure design
- Certifications

Availability, redundancy, and backup

OvrC's cloud service team targets 99.5% annual availability. ADI has historically beaten this target. OvrC status and availability are publicly available at status.SnapOne.com. ADI uses service clustering and network redundancies to eliminate single points of failure. A rigorous backup regimen provides for service data that is continuously replicated across primary and secondary disaster recovery systems and facilities.

Privacy

This section gives a brief outline of the ADI privacy policy and protections related to OvrC. For full details, see the links below:

- OvrC license agreement and terms of use details what ADI expects from integrators who use OvrC.
- Privacy policy related to OvrC details how the company treats all personal data used with OvrC.

In addition to the terms of use above, integrators that use OvrC to service, monitor, and troubleshoot their customers' devices should have their own privacy policies.

Data handling

If an end user would like to view, modify, or delete information held by OvrC, that person can make such request to ADI in accordance with the Privacy Policy linked above. The OvrC team asks the end user to verify their identity prior to processing such requests.

What information does OvrC collect?

The nature of OvrC's value to the integrator as a device configuration and management tool requires OvrC to store information about devices relevant to remotely monitoring and troubleshooting end users' devices. The end user owns the data, and the integrator can only process such data with the end user's consent.

OvrC stores information about devices that have been connected to the platform. Device data commonly collected through OvrC may include:

- Device brands, models, serial numbers, and Media Access Control (MAC) addresses
- The version of firmware on those products
- Names given to devices connected to the network
- The state of the device and whether it is online or offline
- The activities and configuration of a device

OvrC does not provide integrators with any access to substantive information on connected devices. For example, through OvrC, an integrator can see if a router is on and functioning but not the content the router sends or receives.

OvrC stores basic end-user data as added by the integrator. This information can include:

- Location or address where devices are installed
- End user contact information like name, address, email, and phone number
- The location's internet service provider

Compliance

OvrC stores and processes device data to provide value to the integrator as a remote management and configuration platform; ADI does not use this data for any purpose other than those outlined in the ADI Privacy Policy.

Who can access OvrC information

ADI may give information to:

- Any member of the company's user group, which means subsidiaries, affiliates, or a holding company and its subsidiaries, that supports the processing of personal data under this policy.
- Organizations that process data on ADI's behalf and in accordance with corporate instructions and the law (including any applicable privacy laws), including supporting the services offered through company sites. **Click here for a list of third-party service providers**.
- An independent integrator of the consumer's choice that is authorized to sell, install, or service ADI products.

ADI may disclose personal data to third parties in limited circumstances, as outlined in the **ADI Privacy Policy**.

ADI only shares personal data to the extent necessary to meet a legitimate purpose. The company does not sell data, including personal data, for monetary value. ADI does not use data obtained by OvrC for any advertising.

Where OvrC stores information collected in the EEA

With respect to information collected inside the UK or European Economic Area ("EEA/UK"), such data may be stored at a destination outside the EEA/UK that may not be subject to equivalent European data law.

When transferring information from within to outside the EEA/UK, ADI takes all steps reasonably necessary to protect personal data with appropriate safeguards, and treat it securely and in accordance with the **ADI Privacy Policy**.

For additional information on data privacy frameworks and their use for EEA/UK data, see the **ADI Privacy Policy**.

Certifications

OvrC is included under ADI's EU-US DPF registration. For more info see: **https://www.adiglobal.com/privacy/privacy-policy**

ADI does not currently possess a SOC 2 Type 2 certification. However, the OvrC platform is hosted on AWS. Many technical controls have been verified through AWS's security report. AWS holds numerous security certifications, which are available for review.

About ADI Global Distribution

ADI is a global specialty distributor of professionally installed low-voltage products serving commercial and residential markets through an omnichannel go-to-market platform. We offer over 500,000 products from more than 1,000 suppliers across key specialty low-voltage categories, complemented by a portfolio of exclusive brands including Control4, WattBox, OvrC and Triad.

To learn more, visit adiglobal.com.

White Paper rev 3 | August 2026