Q-SYS REFLECT SECURITY & PRIVACY

Version 3.0

Customer Guide for the Q-SYS Reflect Cloud Service

1. EXECUTIVE SUMMARY

Q-SYS Reflect is a cloud-hosted AV remote monitoring and management platform. It enables centralized monitoring, configuration, analytics, and remote support for Q-SYS Cores and peripherals deployed across global enterprise environments. As organizations increasingly rely on connected AV and collaboration infrastructure, security, privacy, and resilience become foundational expectations rather than optional features. This guide provides a transparent, high-level explanation of how Reflect is designed, operated, and protected, so that new and existing customers can confidently adopt the service.

Security at QSC™ is treated as a core engineering and operational discipline rather than a feature bolted on at the end. Reflect is built on a modern cloud-native architecture hosted on Microsoft Azure, leveraging established platform security capabilities while adding application-level controls specifically designed for the Reflect service. These controls span identity management, network connectivity, encryption, secure development, vulnerability management, monitoring, and operational response. Together, they form a defense-in-depth posture intended to protect customer data, device communications, and service availability.

This guide is intended for customers, prospective customers, AV integrators, IT and security teams, procurement reviewers, and partners who are evaluating or operating Reflect. It is written as a public reference and is linked from the Q-SYS website. While this guide provides substantial depth, it is not exhaustive. Where more detailed information is required—such as for formal vendor risk assessments, data processing agreements, or regulatory reviews—additional materials are made available through the QSC Trust Center and vendor-assessment channels under appropriate confidentiality terms.

2. ABOUT Q-SYS REFLECT

Q-SYS Reflect is a cloud-hosted Software-as-a-Service (SaaS) platform that enables organizations to centrally manage, monitor, and gain operational insight into their Q-SYS deployments. Reflect connects to on-premises Q-SYS Cores through a secure, outbound, certificate-authenticated channel, providing administrators with visibility into system health, device status, and operational events without requiring complex inbound network exposure on the customer side.

Reflect is used across a wide variety of environments, including corporate meeting spaces, education campuses, hospitality, performance venues, transportation, government, and large enterprise office deployments. Typical users include AV integrators who design and deploy Q-SYS systems, IT administrators who manage day-to-day operations, and customer end users who consume reporting and operational telemetry. Each role has different operational needs, and Reflect provides role-based access to align permissions to those needs.

Core capabilities of Reflect include centralized device registration and inventory, remote monitoring of system health, event and alert notifications, performance and usage analytics, firmware update orchestration where supported, and integrations with operational platforms such as IT service management systems. These capabilities are delivered through a secure web portal and supporting APIs, all hosted in the Reflect cloud.

3. SECURITY PRINCIPLES AND APPROACH

Reflect security is guided by a small number of consistent principles applied across architecture, engineering, and operations. These principles are not abstract; they translate into concrete design choices that customers can observe in connectivity behavior, identity flows, and data handling.

- Defense in depth: multiple, independent layers of control are applied so that the failure of any single control does not compromise the entire system.
- Least privilege: users, services, and personnel are granted only the access strictly required to perform their function, and elevated privileges are limited in scope and duration.
- Secure by design: security requirements are defined during architecture and design phases, not retrofitted after deployment.
- Zero trust mindset: trust is not assumed based on network location; identity, device posture, and authorization are validated at each interaction wherever feasible.
- Transparency and accountability: security activities are logged, auditable, and reviewed through internal governance and customer-facing assurance processes.

Reflect operates under a shared responsibility model that is typical of modern SaaS services. QSC is responsible for securing the platform, infrastructure, application, and operational processes. Customers are responsible for securing their on-premises networks and devices, properly managing identity and access for their users, and configuring Reflect according to documented best practices. The table below summarizes how responsibility is divided.

AREA	QSC RESPONSIBILITY	CUSTOMER RESPONSIBILITY
Cloud infrastructure	Secure configuration, patching, and monitoring of the Reflect cloud platform.	Not applicable.
Application security	Secure development, testing, and remediation of Reflect application code.	Not applicable.
Identity platform	Operation of centralized identity (QSC ID / CIAM) and federation endpoints.	Configuration of SSO, MFA, and role assignments within the customer environment.
User management	Documented role model and permission enforcement.	Provisioning and de-provisioning of users, periodic access reviews.
On-prem devices	Documentation of secure connectivity requirements.	Secure deployment, network controls, and timely updates for Q-SYS Cores and peripherals.
Data input	Encrypted handling of data once received by Reflect.	Appropriate use of the service and avoidance of submitting unautahorized sensitive data.
Incident response	a Detection, response, and notification for platform-level incidents.	Response to incidents in customer environments and timely communication with QSC.

4. CLOUD INFRASTRUCTURE AND HOSTING SECURITY

4.1 Cloud Infrastructure and Hosting Security

Reflect is hosted on Microsoft Azure, a major global cloud platform with extensive independently audited compliance attestations, including but not limited to SOC 1, SOC 2, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and various regional certifications. By building Reflect on Azure, QSC inherits a strong baseline of physical, environmental, and infrastructure security controls maintained and audited at the cloud provider level. QSC then layers Reflect-specific application, identity, network, and operational controls on top of that foundation to deliver an end-to-end secure service. The certifications referenced above are held by Microsoft Azure and apply to the underlying cloud infrastructure and platform services provided by Microsoft; they do not, by themselves, constitute certification of the Reflect application. Independent assurance activities specific to the Reflect service are described in Section 19.

The use of a major cloud provider also enables Reflect to take advantage of mature platform services for identity, secrets management, monitoring, threat detection, and high availability. These platform services are continuously updated and improved by the cloud provider, which reduces the risk of using outdated or unmaintained components in critical security paths.

4.2 Network architecture

Reflect uses a layered cloud network architecture. Public-facing traffic is fronted by global edge services that provide TLS termination, distributed denial of service protection, and a Web Application Firewall (WAF) for filtering common web exploit patterns. Behind the edge, application workloads run in managed Kubernetes environments where workload identities, network segmentation, and access policies are enforced. Internal communication between services is restricted, and access to sensitive backing services such as databases, message queues, and key vaults is limited to authorized application identities and network paths.

Administrative and operational access to Reflect cloud resources is restricted, logged, and protected with strong authentication. Where applicable, just-in-time access and approval workflows are used to limit standing privileged access. Secrets, certificates, and signing keys are stored in managed key vault services and are not embedded in source code or container images.

4.3 Tenant isolation

Reflect uses logical tenant isolation to keep customer data separated. Each customer organization is associated with its own identifiers and access scopes, and the Reflect application enforces authorization checks so that users can only access data for organizations to which they have been granted permission. While multiple customers may share underlying compute and storage resources at the platform level, application-layer isolation prevents cross-tenant access through normal use of the service.

4.4 High availability and resilience

Reflect is designed for high availability using cloud-native architectural patterns. Workloads are deployed across multiple availability zones where supported, and the service uses load balancing, auto scaling, and managed databases with built-in redundancy to maintain availability during routine failures. Operational runbooks, automated deployment pipelines, and continuous monitoring help reduce time to detect and recover from incidents. Resilience is treated as an evolving discipline; the team regularly reviews architecture, performs targeted testing, and improves recovery procedures based on lessons learned.

5. NETWORK CONNECTIVITY AND BOUNDARY PROTECTION

A common concern when adopting a cloud-managed AV platform is whether the cloud service requires inbound access into the customer network. Reflect is deliberately designed to minimize that pattern. For standard device management, the Q-SYS Core initiates outbound HTTPS over TCP 443 to the Reflect cloud, and after registration persistent communication is maintained using Secure WebSocket (WSS) connections over the same outbound channel. As a result, the majority of Reflect monitoring, configuration, and analytics functions do not require customers to open inbound firewall ports. Certain capabilities—such as Reflect Relay, Core Manager access workflows, and future features—may rely on additional connectivity mechanisms. Customers should consult the product-specific connectivity documentation for these features to understand the associated network requirements.

Because standard cloud connectivity is outbound-initiated, customers typically do not need to open inbound firewall ports, expose internal devices to the internet, or operate dedicated VPN tunnels for routine use of Reflect. This significantly reduces the network attack surface compared to architectures that depend on inbound management access. Customers should still apply standard egress controls, allow-list documented service names, and monitor outbound traffic according to their security policies.

The table below summarizes the protocols and ports relevant to Reflect connectivity from a public-facing perspective.

PROTOCOL / SERVICE	PORT(S)	PURPOSE
HTTPS (TLS 1.2+)	443/TCP	Core-to-Reflect cloud connectivity, registration, web portal access, CIAM / SSO flows.
Secure WebSocket (WSS)	443/TCP	Persistent secure communication channel between Core and Reflect after registration.
DNS	53/UDP and TCP	Resolution of Reflect and identity service names. DNS-based discovery is required because endpoints sit behind load balancers and CDNs.
NTP	123/UDP	Accurate time synchronization to prevent TLS handshake and token validation errors.

Public service names referenced by Reflect connectivity include reflect.qsc.com for the Reflect platform and ciam.qsc.com for centralized identity and authentication flows. Customers are advised to allow-list DNS service names rather than IP addresses, because endpoints may move behind load balancers, content delivery networks, or regional deployments. Hardcoding IPs can lead to connectivity failures and is explicitly discouraged in Reflect connectivity documentation.

6. DEVICE IDENTITY AND REGISTRATION

Reflect uses certificate-based device identity to establish trust between the Q-SYS Core and the cloud service. Registration is initiated by an authorized user from the Core Manager interface. The Core then establishes an outbound HTTPS connection to Reflect and presents identifying information tied to its license. Reflect validates the identity, signs the Core certificate request, and returns a signed certificate. The Core uses that signed certificate to establish a secure, authenticated WebSocket channel for ongoing communication.

This model provides several benefits. It ties device identity to a verifiable cryptographic credential rather than relying solely on shared secrets, it leverages the existing license entitlement chain to validate device authenticity, and it ensures that ongoing communication is mutually authenticated. Because registration occurs over an outbound channel initiated by the customer, there is no need to expose inbound access to the device, and the customer retains operational control over when a device is registered or claimed into an organization.

7. IDENTITY AND ACCESS MANAGEMENT (IAM)

User identity for Reflect is centralized through QSC ID and the QSC Customer Identity and Access Management (CIAM) service. Centralizing identity allows QSC to apply consistent security controls across users, integrate with enterprise identity providers, and provide a single point of policy enforcement for authentication, authorization, and session management.

7.1 Single Sign-On and Federation

Reflect supports modern federation protocols. Documented federation methods include SAML 2.0 and OpenID Connect (OIDC), allowing enterprise customers to integrate Reflect authentication with their existing identity providers such as Microsoft Entra ID, Okta, Google Workspace, and others that support these standards. Federated authentication enables customers to apply their own enterprise policies—including conditional access, device compliance checks, password rotation, and risk-based authentication—to Reflect access.

7.2 Multi-Factor Authentication (MFA)

Reflect supports multi-factor authentication for user sign-in, either through the centralized identity service for direct logins or through the customer's identity provider when SSO is used. QSC strongly recommends that customers require MFA for all users with administrative or write privileges and consider requiring it for all users.

7.3 Credential and password handling

For users authenticating directly through QSC ID, password handling follows current industry-standard practices. Passwords are never stored in plaintext, are protected using salted cryptographic hashing, and are subject to minimum complexity, lockout after repeated failed attempts, and other controls maintained by the centralized identity service. Customers using SSO inherit their identity provider's password policy.

7.4 Sessions and tokens

User sessions and tokens have defined lifetimes. Tokens are exchanged through server-side flows where applicable and are not exposed in cleartext during normal use. Sessions can be terminated, and tokens can be invalidated through standard identity management workflows. Reflect's connectivity guidance recommends accurate device time (via NTP) to prevent token validation errors.

7.5 Role-Based Access Control (RBAC)

Reflect uses role-based access control to govern user actions within the service. Documented roles include Organization Owner, Site Manager, Administrator, Technician, Viewer / Read-only, and Custom roles. Permissions are scoped so that users can only act on the organizations, sites, and devices they are authorized to manage.

ROLE	TYPICAL PERMISSIONS
Organization Owner	Full administrative control of the organization, including user management and configuration.
Site Manager	Manages sites, devices, and operational settings within their assigned scope.
Administrator	Performs administrative tasks within the organization or assigned scope; typically broader than Technician.
Technician	Operational and troubleshooting tasks on assigned devices and sites; limited administrative actions.
Viewer / Read-only	Read-only access to monitoring information; cannot make changes.
Custom roles	Tailored permission sets to fit specific organizational needs while preserving least privilege.

7.6 QSC operational access

Access by QSC personnel to production systems and customer data is restricted to authorized roles, granted on a need-to-know basis, protected by strong authentication including MFA, and logged for review. Where feasible, just-in-time or approval-based elevation is used so that standing privileged access is minimized. Internal access activity is subject to monitoring and periodic review.

8. DATA PROTECTION

8.1 Encryption in transit

Reflect protects data in transit using HTTPS/TLS across all cloud-facing communication paths. The minimum supported version is TLS 1.2, and TLS 1.3 is used where supported by both endpoints. TLS is enforced across the Reflect web portal, backend APIs, device-to-cloud connectivity (established using mutual TLS with certificate-based authentication), CIAM authentication flows, and Secure WebSocket (WSS) sessions established after device registration. Legacy insecure protocols (HTTP or TLS below 1.2) are not supported.

Customers are advised not to perform TLS interception on traffic destined for Reflect and identity endpoints, because the registration and ongoing communication flows rely on certificate-based trust. TLS interception can break these flows and create connectivity issues. Where a proxy is required, customers should configure it to tunnel HTTPS and to permit Secure WebSockets without inspecting the encrypted payload.

8.2 Encryption at rest

Reflect protects customer data at rest using industry-standard AES-256 encryption. Cryptographic keys are managed through centralized key management services such as Azure Key Vault, with documented practices for key rotation and access control. Keys used to protect customer data are not accessible to end users directly and are subject to the same least-privilege and logging requirements as other sensitive components of the platform.

8.3 Data classification and handling

Reflect handles several broad categories of data: configuration data describing how systems and devices are set up, telemetry and operational data describing system health and behavior, log and event data used for monitoring and troubleshooting, and limited user identity data such as names and email addresses used to authenticate and authorize access. These categories are subject to appropriate handling, retention, and access controls.

8.4 Data minimization

Reflect is designed to collect only the data needed to operate the service effectively. The platform does not capture audio or video content from Q-SYS systems as part of its standard operation. Telemetry and operational data are scoped to what is required for monitoring, support, and analytics.

8.5 Retention and deletion

Customer data is retained for as long as needed to provide the Reflect service. Customers can request deletion of their data through standard support and account management processes, and QSC will follow defined internal procedures to remove customer data while preserving any logs required for legal, regulatory, or security purposes. Backups are retained for defined periods to support disaster recovery and are also subject to controlled deletion as backup cycles complete.

9. APPLICATION SECURITY AND SECURE SOFTWARE DEVELOPMENT LIFECYCLE

Reflect follows a documented secure software development lifecycle (SSDLC) that integrates security throughout design, development, build, test, deployment, and operations. The goal is to identify and address security issues as early as possible, when remediation is least disruptive, and to provide continuous assurance that the product meets defined security expectations as it evolves.

9.1 Secure design and threat modeling

New features and architectural changes are subject to secure design review and, where appropriate, threat modeling. These activities help identify trust boundaries, authentication and authorization needs, data sensitivity, and likely attack paths before code is written.

9.2 Secure coding and developer enablement

Developers follow secure coding standards and receive periodic security training relevant to their roles. Security guidance is integrated into engineering documentation, code review practices, and team rituals to ensure security considerations are addressed alongside functional ones.

9.3 CI/CD pipelines and build-time security

Reflect is delivered through automated continuous integration and continuous delivery (CI/CD) pipelines. These pipelines run unit and integration tests, dependency scans, static analysis, and container image scans as part of every build. Builds that fail critical security checks are blocked from progressing, and detected issues are routed to engineering teams through tracked workflows.

9.4 Application security testing

Static Application Security Testing (SAST) and Software Composition Analysis (SCA) are used to identify vulnerabilities in first-party code and third-party dependencies. QSC uses tools such as Black Duck to support SAST and SCA workflows. Dynamic Application Security Testing (DAST) is performed against running environments using tools such as OWASP ZAP and Burp Suite, focusing on common web vulnerabilities including those listed in the OWASP Top 10.

9.5 Container and infrastructure-as-code security

Container images used by Reflect are scanned for known vulnerabilities, and base images are kept current to limit exposure from outdated components. Infrastructure-as-code is reviewed for misconfigurations, secret leakage, and policy violations before being applied to environments.

9.6 Vulnerability remediation SLAs

Vulnerabilities are triaged based on severity and exploitability. Critical and high-severity issues are subject to defined internal service level objectives for remediation, and remediation status is tracked through internal issue tracking systems.

9.7 Penetration testing and responsible disclosure

Reflect is subject to regular third-party penetration testing performed by external security firms. Penetration testing is conducted against appropriately scoped environments designed to evaluate the security of the Reflect service while minimizing operational impact. Findings are tracked, prioritized, and remediated through internal workflows. QSC welcomes responsible disclosure of suspected security issues from researchers, customers, and partners through documented contact channels.

10. VULNERABILITY AND PATCH MANAGEMENT

Beyond application-level testing, Reflect operates a continuous vulnerability management program covering the cloud infrastructure, container workloads, and supporting components. Cloud security posture management is supported using tools such as Wiz, alongside native cloud capabilities such as Microsoft Defender for Cloud. These tools provide continuous visibility into misconfigurations, exposed services, vulnerable workloads, and policy drift.

Findings are reviewed and prioritized based on severity, exploitability, and customer impact. Patching of underlying platform components is handled through a combination of cloud-provider-managed services and QSC-managed deployment pipelines. The internal vulnerability lifecycle—identification, validation, prioritization, remediation, and verification—is tracked through engineering systems for accountability and reporting.

11. LOGGING, MONITORING, AND DETECTION

Reflect generates platform and application logs that support both operational monitoring and security detection. These include authentication events, administrative actions, service-level events, system health events, and integration events. Logs are centralized to support correlation, investigation, and retention.

Cloud-native detection capabilities, including Microsoft Defender for Cloud and complementary tooling, are used to surface security-relevant signals. Alerts are routed to operational and security teams for triage. Time synchronization across components is maintained through NTP so that events can be correlated reliably across systems.

For customer-facing visibility, Reflect provides APIs for exporting system and device events such as registration, health, and network activity. This allows customers to integrate Reflect operational data with their own monitoring, SIEM, or analytics platforms. Where SOC 2 or other compliance regimes apply, audit logs supporting required control evidence are maintained for review.

12. BACKUP, DISASTER RECOVERY, AND BUSINESS CONTINUITY

Reflect operates with a documented approach to backups, disaster recovery, and business continuity. Customer data and supporting metadata are backed up using cloud-native services with retention periods designed to support both routine recovery and longer-term resilience scenarios. Backups are encrypted using the same standards as production data at rest.

Recovery objectives, including Recovery Time Objective (RTO) and Recovery Point Objective (RPO), are defined and periodically reviewed. Restore procedures are tested to validate that backups are usable and that recovery steps can be executed effectively. The architecture leverages cloud-native availability patterns such as multi-zone deployment and managed redundancy to minimize the likelihood and impact of regional service disruptions.

13. INTEGRATIONS AND API SECURITY

Reflect exposes APIs to support integrations with operational, monitoring, and IT service management platforms. API access is authenticated and authorized; calls cannot be made anonymously, and authorization checks ensure that callers can only access data they are entitled to see. API rate limits and abuse-protection mechanisms help defend the service against denial of service patterns and credential abuse.

A representative integration is the Reflect application for ServiceNow. In that integration, the customer generates an API token within their Reflect instance and configures the ServiceNow application to use that token. The token grants only the level of access defined within Reflect for that token, and can be revoked and regenerated by the customer at any time; depending on configuration, it may also have an expiration period after which it must be renewed.

The integration is read-only with respect to Reflect data, except for a troubleshooting identifier that is shared transparently and governed by the Reflect privacy policy.

Customers building their own integrations are encouraged to follow least-privilege principles, treat API tokens as sensitive credentials, store them securely, rotate them periodically, and revoke them when no longer needed. QSC continues to evolve the Reflect API security model toward more granular scopes, shorter-lived credentials, and additional authentication options as the platform develops.

14. PRIVACY AND DATA COLLECTION

Reflect collects only the data needed to operate and improve the service. Typical categories of data collected include device metadata (such as device identifiers and configuration attributes), operational telemetry and event data, log data for support and troubleshooting, and user identity information such as name and email used for authentication and authorization

Reflect does not capture audio or video content from Q-SYS systems as part of its standard operation. QSC does not sell customer personal data. Data processing activities are governed by the QSC Privacy Policy and applicable terms of service, and customers may request additional information about subprocessors and data flows through standard channels.

Where applicable laws such as the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) apply, QSC provides mechanisms for customers and data subjects to exercise rights such as access, deletion, and correction subject to applicable law and contractual obligations. Specific procedures may vary based on contractual arrangements and jurisdictional requirements. Phase 1 regionalization (described in the next section) further strengthens the privacy posture for European and Asia-Pacific customers by enabling regional data hosting for new organizations.

15. REGIONAL HOSTING AND DATA RESIDENCY (PHASE 1)

Reflect regionalization is being delivered in phases. Phase 1 introduces regional data hosting for new customer organizations in Europe (hosted in Germany) and Asia-Pacific (hosted in Singapore). The intent is to allow customers with regional data residency requirements to use Reflect while keeping their application-specific data at rest in the assigned region. In Phase 1, the Q-SYS RoomSuite Collaboration Bar is the only supported device class for regional hosting. Support for additional Q-SYS devices and services will be evaluated and introduced in future phases.

For additional details on supported features, limitations, and deployment considerations, refer to the Reflect Regional Hosting and Data Residency FAQ available through the QSC Trust Center and your Q-SYS account team.

In Phase 1, the organization is the unit of regionalization. When a new organization is created, it is assigned to a region, and the Reflect application enforces that the organization's data is stored in cloud infrastructure within that region. Cross-region data migration is not available in Phase 1, and devices claimed into a regional organization communicate only with the cloud endpoints in that organization's assigned region. Users who manage organizations in multiple regions switch region context rather than viewing aggregated data across regions.

Phase 1 has an important limitation that is disclosed transparently. Global identity and authentication services remain centralized during Phase 1 and may process limited user identity metadata outside the customer's assigned region under existing contractual and legal safeguards. QSC will maintain logging and documentation sufficient to demonstrate an organization's assigned region, the location of its data at rest, and access to that data for audit or compliance inquiries.

Phase 1 data-hosting summary

CATEGORY	EXAMPLES	PHASE 1 HOSTING EXPECTATION
Customer content data	Configuration, telemetry, logs, user-generated content	In region for the assigned customer organization.
Identity and authentication data	User credentials and account metadata	Centralized during Phase 1; regionalization evaluated in future phases.
Operational evidence	Assigned region, data-at-rest location, access records	Supported through logging and documentation for audit and compliance.

16. SECURITY OPERATIONS AND INCIDENT RESPONSE

Reflect cloud operations are monitored continuously by QSC engineering and operations teams. Security events are surfaced through cloud-native detection capabilities and internal monitoring tooling, and are triaged through documented incident response processes. Incident response follows a standard lifecycle: detection, triage and classification, containment, eradication, recovery, and post-incident review.

Customer notification commitments for confirmed security incidents are aligned with contractual obligations and applicable regulatory requirements such as GDPR breach notification timelines where relevant. QSC also coordinates with customers, partners, and external researchers on responsible disclosure of suspected security issues, providing a defined channel for reporting and structured handling of incoming reports.

Post-incident reviews are used to identify root causes, contributing factors, and improvement opportunities. Resulting actions—such as architectural changes, control improvements, or process updates—are tracked to completion through internal engineering systems.

17. PERSONNEL SECURITY AND OPERATIONAL CONTROLS

QSC applies personnel security controls to staff with access to production systems and customer data. These include background screening where permitted by local law, mandatory acceptance of acceptable use and confidentiality policies, and periodic security awareness training tailored to roles.

Internal access to production environments follows least-privilege principles. Privileged access is granted only as required, protected with strong authentication including MFA, and logged for review. Separation of duties is enforced where appropriate so that no single individual can both develop and unilaterally deploy or modify production systems without controls.

Administrative access events are monitored, reviewed, and retained for compliance and forensic purposes. When personnel change roles or leave the company, access is revoked through documented offboarding workflows.

18. THIRD-PARTY AND SUPPLY CHAIN SECURITY

Reflect depends on a curated set of third-party services and software components. Vendor risk is managed through a vendor assessment process that evaluates security posture, compliance, and data handling for critical subprocessors. Significant changes to subprocessor usage that affect customer data handling are managed through internal review processes.

Software supply chain security is supported through Software Composition Analysis, dependency review, and—where feasible—use of signed artifacts and verified builds. Open-source components are monitored for known vulnerabilities and license risks, and dependencies are kept current through routine maintenance cycles. These practices help reduce the risk of compromise through the software supply chain.

19. COMPLIANCE AND ASSURANCE

Reflect is hosted on Microsoft Azure, which holds independently audited certifications including SOC 1, SOC 2, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and other regional and industry-specific certifications. These certifications are held by Microsoft and apply to the cloud infrastructure on which Reflect is built and provide a strong baseline of assurance at the platform layer. They should not be interpreted as certification of the Reflect application itself. Reflect-specific assurance is addressed separately through QSC's own program described below.

At the application and service layer, QSC is investing in independent assurance for Reflect itself. A SOC 2 readiness program is in progress for Reflect, focused on the Security and supporting trust services criteria. Reflect engineering and operational practices are aligned with widely recognized control frameworks such as the NIST Cybersecurity Framework principles and CIS Controls.

Customers with specific regulatory or contractual obligations—such as those operating in financial services, healthcare, government, education, or critical infrastructure environments—are encouraged to engage with QSC through standard vendor assessment and procurement workflows. Through those channels, QSC can share additional details under appropriate confidentiality terms, including responses to security questionnaires such as SIG, CAIQ, and HECVAT. Statements about future certifications in this document are forward-looking and are not a substitute for completed, formally audited reports.

20. CUSTOMER RESPONSIBILITIES AND RECOMMENDATIONS

While Q-SYS operates the Reflect platform, customers play a critical role in protecting their own environments and data. The following practices help customers maximize the value of Reflect security capabilities and align with the shared responsibility model described earlier in this document.

- Use strong identity practices: integrate Reflect with your enterprise identity provider via SSO, and require MFA for users with administrative privileges at a minimum.
- Apply least-privilege role assignments and review user access periodically. Assign Viewer / Read-only roles when full administrative access is not needed.
- Allow-list Reflect service names (such as reflect.qsc.com and ciam.qsc.com) in firewall and proxy policies, and avoid hardcoding IP addresses.
- Avoid TLS interception of traffic to Reflect and identity endpoints, as it can disrupt certificate-based trust flows used for device registration and ongoing communication.
- Keep Q-SYS Core firmware and Q-SYS Designer software up to date so that documented secure connectivity and control paths are available.
- Maintain accurate time on Q-SYS Cores using NTP to prevent TLS and token validation issues.
- Treat Reflect API tokens as sensitive credentials: store them securely, rotate them periodically, and revoke them when no longer needed.
- Monitor relevant Reflect events through the available export APIs and integrate them with your operational and security monitoring tools where appropriate.
- Report any suspected security issues affecting Reflect or your usage of it through official QSC channels promptly.

21. GETTING HELP AND REPORTING SECURITY ISSUES

Customers can engage QSC through standard support and account management channels for routine questions and issues. For routine product support, customers can contact Q-SYS Support at https://support.qsys.com/contact-us. For security-specific concerns, QSC provides defined channels for vulnerability reporting and responsible disclosure. Researchers, customers, and partners are encouraged to report suspected vulnerabilities affecting Reflect through these channels rather than through public disclosure, so that QSC can validate, prioritize, and remediate issues before they may be exploited.

Additional security documentation, vendor assessment artifacts, and certifications—as they become available—will be published through the QSC Trust Center and shared under appropriate terms during vendor assessment workflows. Customers requiring confidential security materials should engage their QSC account team to initiate the appropriate process.

22. DOCUMENT SCOPE AND DISCLAIMER

This guide provides a public, high-level overview of how Reflect is designed, operated, and protected. It is intended to be useful for customer evaluation, internal alignment, and routine security and privacy questions. It is not an exhaustive technical specification, and it does not replace contractual terms, privacy notices, data processing agreements, or formally audited compliance reports.

Service architecture, endpoints, regional capabilities, integrations, and implementation details may evolve over time as the Reflect platform develops. QSC may update this document periodically to reflect significant changes. Forward-looking statements about features, certifications, or capabilities are provided for context only and are not commitments.

Where customer-specific requirements apply, including legal, contractual, regulatory, or industry-specific concerns, customers should engage QSC through standard support, vendor-assessment, or account-management workflows to obtain tailored information under appropriate confidentiality terms.