SYNERGY SKY
Making video meetings easy

Dronning Eufemias gate 16, 0191 Oslo, Norway

SYNERGY CONNECT GO WHITEPAPER

Building Digital Trust and Security in Modern Video Collaboration
April 2025

THIS WHITEPAPER provides an overview of the security architecture, governance framework, and operational safeguards for the Synergy SKY CONNECT GO service. Building on Synergy SKY's commitment to digital trust, the following sections outline how CONNECT GO handles data, manages access, and enforces compliance measures while maintaining confidentiality, integrity, and availability of its services.

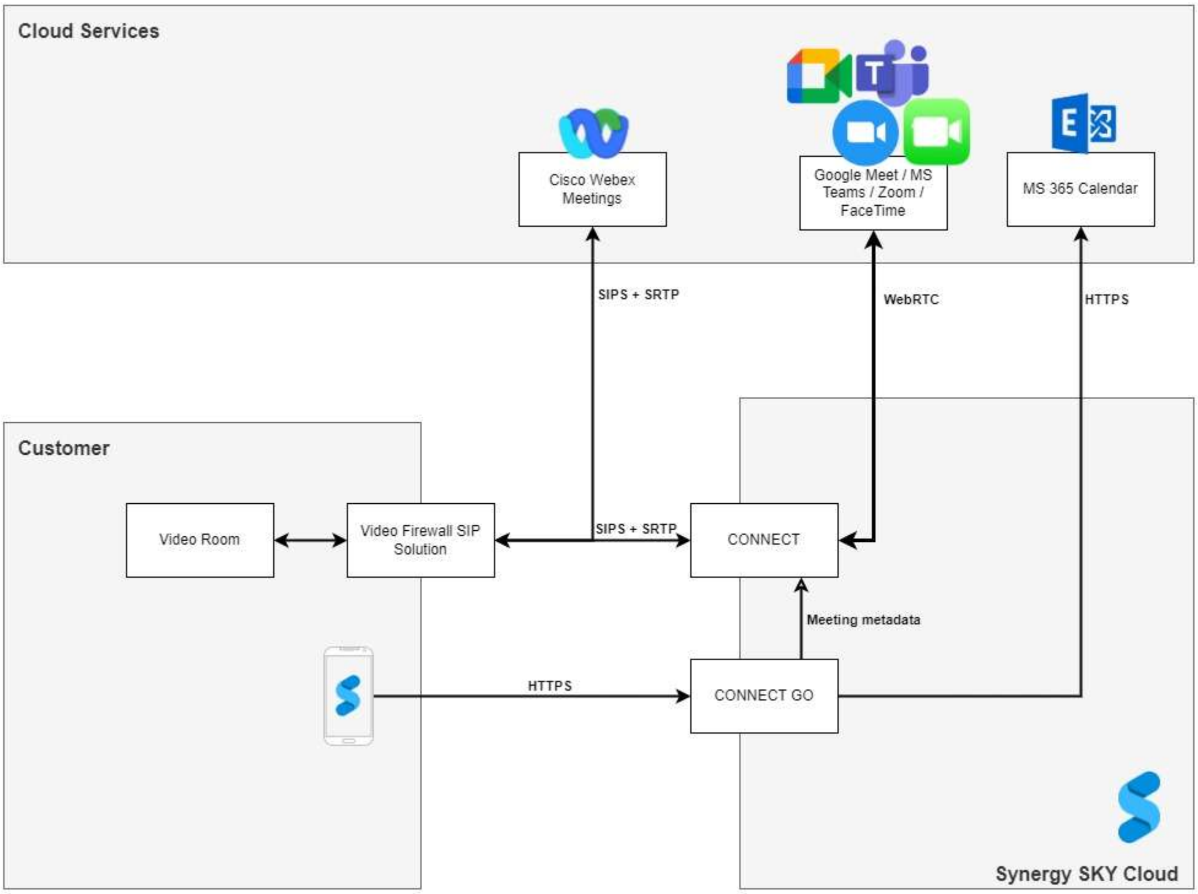
SCOPE

The scope of this document is the CONNECT GO web-based solution and its associated components, including the user-facing webpage, calendar integration (via Microsoft Graph API and Azure Application), and the CONNECT backend to which room systems connect. Where relevant, the document references Synergy SKY's Information Security Management System (ISMS) which is certified to ISO/IEC 27001. This whitepaper does not address other Synergy SKY features or third-party services outside of the direct operational requirements for CONNECT GO.

OVERVIEW OF CONNECT GO ARCHITECTURE

CONNECT GO enables seamless meeting connections between a user's video room system and popular meeting platforms (e.g., Microsoft Teams, Zoom, Google Meet, Apple FaceTime, Cisco Webex, Cisco Meeting Server). The architecture follows these primary steps:

- first, a video system dials into CONNECT, triggering the generation of a unique QR code for that session;
- second, the user scans the QR code with a mobile device, launching the CONNECT GO webpage and authentication through Microsoft Entra;
- third, upon successful authentication, the webpage retrieves the user's calendar entries and allows the user to select a desired meeting; and
- finally, meeting details are securely transmitted to CONNECT, which establishes the connection in the room while the webpage functions as a remote control for meeting management.



DATA RETENTION AND PROTECTION

Data retention and protection measures within CONNECT GO ensure that user information is managed responsibly and securely at every stage of its lifecycle. By employing stringent cryptographic methods, enforcing defined retention periods, and adhering to ISO 27001 requirements, the service protects sensitive data from unauthorized access and fosters confidence in its security posture. The following paragraphs detail the specific practices that govern how CONNECT GO handles user metadata, meeting data, and related information.

User metadata consists primarily of a hashed version of the user’s email address and a stored profile photo, both of which are retained for a maximum of 30 days. This window balances personalization and support needs with the principle of minimal retention, reducing the risk of unnecessary data exposure. Similarly, meeting credentials and other connection details—such as meeting passwords and IDs—are maintained by CONNECT for 30 days to accommodate customer support and ensure a robust audit trail in the event of service inquiries or incident analysis.

Encryption is employed both in transit and at rest, allowing data transmissions (e.g., QR link, OAuth tokens, meeting hyperlink) to remain secure throughout the user’s interaction with the CONNECT GO platform. By leveraging TLS protocols and industry-standard cryptographic algorithms, Synergy SKY maintains confidentiality and integrity of information as it moves between devices and services. Data at rest, including any stored logs or retained meeting details, is likewise protected using encryption mechanisms that align with recognized international standards.

Finally, Synergy SKY maintains a practice of anonymizing and hashing user identifiers when processing or logging system events. This method reduces the risk of directly exposing personal data while preserving the ability for authorized personnel to correlate and troubleshoot issues. The combined effect of these measures demonstrates Synergy SKY’s dedication to safeguarding user privacy and meeting the rigorous demands of ISO 27001.

IDENTITY AND ACCESS MANAGEMENT (IAM)

CONNECT GO employs a robust identity and access management model by leveraging Microsoft Entra as its authentication backbone and by enforcing best practices for token handling. The service requires user consent to delegated permissions, ensuring that individuals specifically agree to share their calendar data. If enterprise policies demand additional restrictions, administrators can set consent requirements that align with organizational risk thresholds and governance standards. Within the CONNECT GO environment, OAuth tokens, refresh tokens, and related credentials are managed under strict lifecycle rules. These tokens expire at intervals defined by Microsoft Entra configurations, forcing re-authentication and thus reducing the risk of perpetually valid sessions.

GOVERNANCE, RISK MANAGEMENT, COMPLIANCE

Synergy SKY's governance, risk management, and compliance activities are anchored by a formal Information Security Management System (ISMS) that underpins CONNECT GO. These activities encompass a range of policies, frameworks, and processes designed to safeguard data confidentiality, integrity, and availability at every stage of its use.

- ISO 27001 Alignment. Synergy SKY operates an ISMS conforming to ISO 27001, mapping internal controls to each operational component of CONNECT GO in order to ensure systematic management of information security risks.
- Risk Assessments. Periodic risk assessments identify and evaluate threats to the confidentiality, integrity, and availability of data processed by CONNECT GO. Each identified risk is documented and addressed with clear mitigation strategies that are tracked over time.
- Policies and Procedures. Formal policies govern data retention, incident response, user access management, and other critical operational areas. These guidelines also detail the handling of encryption keys, token storage, and the secure termination of sessions.
- Incident Response. Synergy SKY maintains a documented incident response plan that outlines responsibilities, escalation channels, and communication protocols. This plan facilitates rapid detection, containment, and resolution of security incidents, preserving overall service integrity.

MONITORING AND CONTINUOUS IMPROVEMENT

Monitoring of CONNECT GO involves comprehensive logging, penetration testing, and vulnerability scans conducted on a regular basis to validate ongoing security measures. System logs capture vital events, including user authentication sessions, calendar queries, and administrative updates, providing the foundation for both real-time alerts and post-event forensic analysis. Where potential weaknesses emerge, Synergy SKY's internal processes ensure rapid remediation by tracking vulnerabilities through documented workflows that allocate clear responsibilities. In keeping with ISO 27001 principles, the organization also conducts scheduled internal audits and management reviews, which inform a cycle of continuous improvement. These audits validate that security controls remain effective over time and that newly discovered best practices are systematically integrated, thereby preserving a robust and resilient security posture.

DATA FLOW AND LIFECYCLE

This section describes the journey of data within CONNECT GO, beginning with QR code creation and ending with the conclusion of a video meeting. By examining each stage of this flow, we highlight how data is generated, transmitted, stored, and ultimately retired in accordance with security best practices and Synergy SKY's ISO 27001-aligned policies. These are described in the following sections:

- QR Code Generation and Display
- User Authentication and Calendar Integration
- Meeting Selection
- Meeting Connection and Interaction
- Session Termination - Meeting End

QR Code Generation and Display.

At the initiation of a call, CONNECT creates a unique QR code that it displays on the video system's screen. This code is valid only for the current session and is designed to become invalid once scanned, thereby eliminating opportunities for malicious reuse. Because it appears on a physically restricted screen, the QR code remains visible only to authorized individuals within the meeting room, and only until scanned. In addition, the QR code is delivered via an encrypted video stream, preventing external interception. This transmission method enhances security by ensuring that no static QR codes are exposed, reducing the risk of social engineering attacks.

User Authentication and Calendar Integration.

After scanning the QR code, the user is directed to the CONNECT GO webpage, which integrates with Microsoft Entra for identity verification. Single Sign-On and Multi-Factor-Authentication is handled as per the company's Microsoft Entra configuration. When authentication is successful, the various access and refresh tokens are issued by Microsoft Entra and cached within the CONNECT GO environment. These tokens adhere to the configured token lifetimes as set by the Microsoft Entra policies within the organization, promoting secure session management and minimizing the possibility of unauthorized reuse.

https://learn.microsoft.com/en-us/entra/identity-platform/refresh-tokens

CONNECT GO uses an Azure Application, which requires user consent, to access calendar data securely via Microsoft Graph API. The Azure Application consent process is governed by enterprise settings in Microsoft Azure, which an Azure administrator can configure in three different ways:

1. Do not allow user consent
2. Allow user consent for apps from verified publishers, for selected permissions
3. Allow user consent for apps

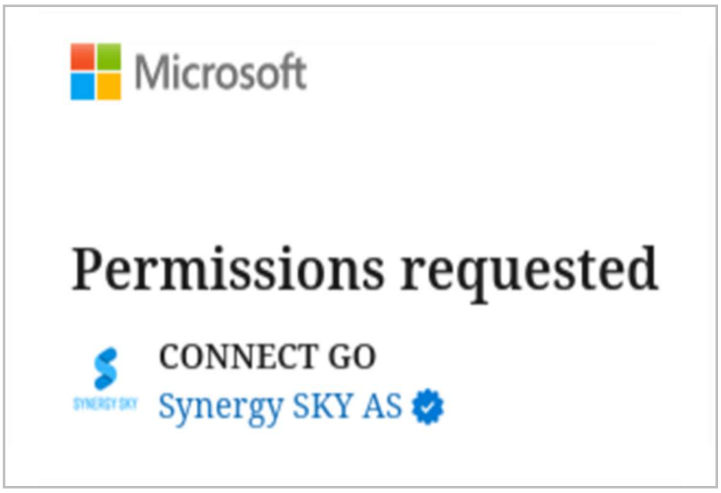
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent?pivots=portal

The CONNECT GO Azure Application can also be deployed by utilizing Admin consent. This will let users log in without individually consenting on their first time.

https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent?pivots=portal

The Azure Application 'CONNECT GO' is published and verified by 'Synergy SKY AS'.

The CONNECT GO application utilizes "Calendars.Read" and "User.Read" delegated permissions to populate the user's calendar on their device. This calendar data is held in memory only during the user's session. It is only the user's profile photo, and a hash of their email address that is stored subject CONNECT's retention policy of 30 days.


Microsoft

Permissions requested

CONNECT GO

Synergy SKY AS

The profile photo, and a hash of their email address is stored in an encrypted database, using AES-256. And all data in transit between CONNECT GO, Microsoft 365 and our encrypted database is encrypted using TLS 1.2/1.3 to ensure confidentiality and integrity of the information.

Access requests, usage and statistics are available through native Microsoft Entra logging, providing an audit trail for compliance and security monitoring purposes. These audit materials help detect potential data exfiltration attempts and unauthorized access.

https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-audit-logs

Meeting Selection.

Once a user chooses a specific meeting, CONNECT GO transmits the necessary information—such as the meeting ID and password—to CONNECT over an encrypted channel. The following metadata is stored in CONNECT when joining a meeting:

- Meeting Type (E.g. Microsoft Teams, Google Meet, Zoom, Apple FaceTime, SIP-to-SIP)
- Joining hyperlink for the meeting
- Meeting ID & Password
- SIP URI & ID (e.g. Webex dialing information)
- Video Conference Password (e.g. when different from the native meeting password)

This metadata is stored in an encrypted database, using AES-256. And all data in transit to and from the database is encrypted using TLS 1.2/1.3

Meeting Connection and Interaction.

Upon receiving the details of the selected meeting, CONNECT redirects the existing video call to the selected meeting. At this point, the webpage on the user's device transitions into a remote control, enabling features such as layout adjustments and participant engagement (e.g., raising hands or sending emojis). These commands traverse secure channels and remain associated with the user's session until meeting completion. Connection information is retained for up to 30 days, aligning with operational requirements for auditing, incident troubleshooting, and customer support.

Session Termination - Meeting End.

At the end of a meeting, the session is closed, purging all unused calendar information from the service. The selected meeting metadata is retained for 30 days before automatic deletion. Logs are retained for 14 days before automatic deletion. Any unselected meeting information is ephemeral.

CONCLUSION

The security of CONNECT GO is underpinned by a well-defined architecture, thorough data lifecycle management, and robust governance processes. By integrating Microsoft Entra for identity and access control, encrypting data at rest and in transit, and maintaining strict retention policies, Synergy SKY fulfills stringent security and compliance standards. Ongoing risk assessments, vulnerability management, and adherence to ISO 27001 principles reinforce this posture, providing both users and administrators with confidence in the platform's integrity and resilience.

CONNECT GO - Security Overview

Security Feature	Implementation
Authentication	Microsoft Entra
Encryption (In Transit)	TLS 1.2/1.3
Encryption (At Rest)	AES-256
Session Security	Unique, expiring QR codes and OAuth token expiration
Meeting Metadata Retention	30 days, then auto-deleted (for selected meeting)
ISO 27001 Compliance	Identity Access Management, Encryption, Secure API Calls, and Data Retention Policies

CONNECT GO ensures end-to-end protection of user authentication, session management, data transmission and storage. By enforcing strong encryption standards and ISO 27001-aligned policies, Synergy SKY delivers a secure and compliant collaboration experience for enterprise customers.