SyncPro CloudOS Service

Security Reference Guide

Ver 1 (May 10th, 2020)

Contents

Revision History

Version	Date	Notes	Author
1	10-May-2020	Initial Release	OB

Introduction

SyncPro's CloudOS is a multi-tenant SaaS (Software as a Service) platform that allows customers and Managed Service Providers (MSP) to easily deploy, manage and monitor modern workplace IoT devices such as control systems, Unified Communications (UC) room kits, displays and more from one, centralized and secured platform.

The SyncPro CloudOS service may be used to view the status of a device, to configure various devices and network settings, to manage licenses, and to update devices firmware, software, and configurations.

CloudOS is hosted on Amazon Web Services (AWS) and seamlessly integrate with 3rd party services such as ticketing systems, messaging platforms, and other cloud services for a complete offering.

User Access

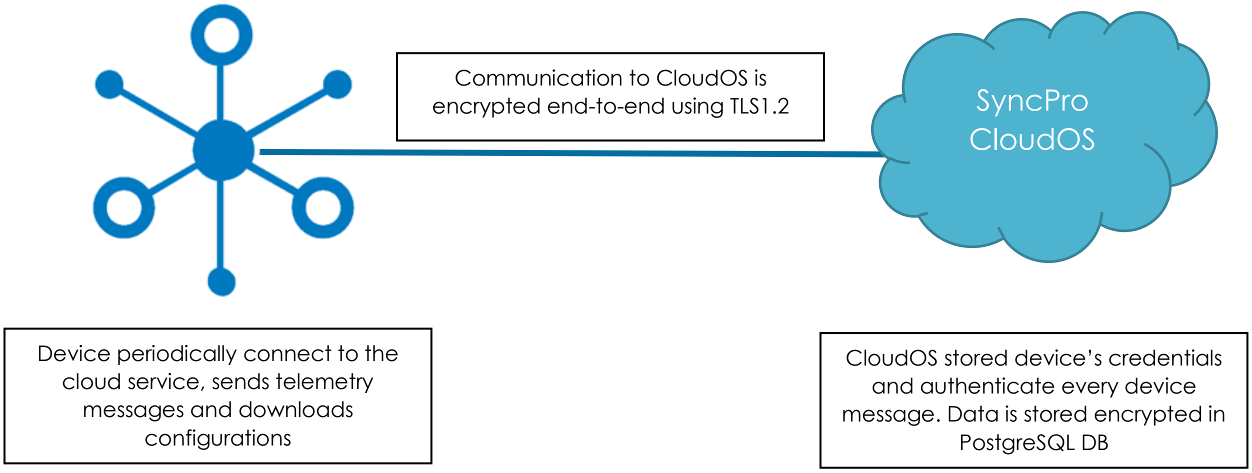
Each organization uses a unique tenant ensuring full data protection and preventing any possibility of cross-organizational data leaks.

If a customer chooses to, they may allow access to MSP to remotely configure, manage, and monitor their devices too by granting them access to their tenant.

IoT Devices Communication to the Cloud

All network communications are done from the organization's network to the cloud. No network connections are ever initiated from the cloud into the client's network and SyncPro devices open no listening ports.

Network communication is handled over HTTPS (port:433), ensuring a fully encrypted data channel between devices and the cloud. Every device can be configured to disable cloud communication. The devices connect to the cloud on TCP port 443 (HTTPS).



Communication to CloudOS is encrypted end-to-end using TLS1.2

Device periodically connect to the cloud service, sends telemetry messages and downloads configurations

CloudOS stored device's credentials and authenticate every device message. Data is stored encrypted in PostgreSQL DB

Data Storage

All data is stored securely in the cloud. Every API access is monitored and logged to identify intrusions or unauthorized access.

CloudOS stores the following information –

- Users information
- Devices' configurations and messages
- Organizational tree and devices hierarchy
- 3rd party integrations information (see below)
- Audit log and actions that were taken in the portal
- Configuration dumps from devices can be sent to the cloud following a request from the admin or by the device itself

Device Management

Devices can be claimed by the customer's tenant in one of few ways

3rd Party Cloud Integration

These devices are managed through a 3rd party cloud service such as Crestron XiO Cloud, Zoom, or others. CloudOS uses different authentication methods, based on the 3rd party solution provider (see below) to query the devices.

SyncPro Connected Devices

SyncPro Connected Devices are devices by different manufacturers that were designed to work natively with CloudOS. These devices are usually claimed by a customer using the device's MAC address and another unique identifier such as a serial number.

Custom Devices

Custom devices are created in the portal. When created, each custom device gets a unique ID (UUID) and access key that can be used by the system integrators to authenticate devices with the cloud

Policy and Process

SyncPro has a full Software Development Lifecycle to propose and approve changes at the product management level. The implementation of these changes is specified, and all source code is reviewed. Source code is kept in a Version Control System (VCS). Both the completion of the code review and the code reviewer is recorded in the VCS.

SyncPro has both incident response policies with dedicated support and DevOps teams monitoring our cloud services. CloudOS is hosted in Amazon Web Services (AWS). External penetration tests are also performed at regular intervals. Product security risks are cataloged in a secure area of SyncPro's task/defect management system. SyncPro's CloudOS service has a number of alerts and other monitoring agents in place for issue notification. These services also log all activity, and an audit log is available for end-users to monitor their account and device activity.

Integrations

CloudOS seamlessly integrates with several services to extend and enhance the functionality of the platform. Each integration is configured by the system admin and can be disabled at any time. CloudOS uses different authentication methods, based on the 3rd party solution provider, as detailed below –

1. **Ticketing Systems** –
   a. **ServiceNow** – Integration is done using user name and password to the ServiceNow instance. The password is saved encrypted
   b.
2. **Messaging Platforms** –
   a. **Microsoft Teams** – Currently, only webhook integration is supported using a unique user-defined webhook url.
   b. **Slack** - Currently, only webhook integration is supported using a unique user-defined webhook url.

3. **UC Platforms** –
   a. **Zoom** – SyncPro developed a Zoom application for the Zoom market place. Authentication is handled with OAuth 2.0.

4. **Other Cloud Platforms** –
   a. **XiO Cloud** – Integration is done using an account id and subscription key generated in XiO Cloud. XiO Cloud is read-only API, and CloudOS periodically query the customer's XiO instance to get devices' status, and trigger alerts.