Security in the Kinly Cloud

Kinly

kinly.com

Security in the Kinly Cloud

Table of Contents

Security in the Kinly Cloud

This whitepaper will focus on the following security topics in relation to the Kinly Cloud service:

1 **Virtual Room (VMR) Security**

- Virtual Meeting Room Calls
- Encryption on Virtual Meeting Rooms based on participant types
- Kinly Cloud Portal control interface for Virtual Meeting Room Calls
- Access control to VMR

2 **Video Device Registration**

- Registering endpoints to the Kinly Cloud Service
- Information required from registered video devices

3 **Points of Presence, Data Types and Storage**

- Service Network: Points of Presence (PoPs) and Cloud Services
- Types of data used and stored by the Kinly Cloud Service
- Locations of data stored by the Kinly Cloud Service
- Access to data

4 **Service Network Monitoring and Maintenance**

- Network/Data center security
- Security Patches

Security in the Kinly Cloud

1 Virtual Meeting Room Calls

Kinly Cloud provides Cloud-based video bridges known as Virtual Meeting Rooms (VMRs). VMRs allow multiple participants to meet and collaborate. They also serve as the platform for interoperability between disparate video-enabled and audio-only communities, including participants using standards-based H.323/SIP, Skype-for-Business (S4B), Microsoft Teams participants, WebRTC and PSTN dial-in.

VMRs negotiate encryption with participants if the platform they are using supports this capability. Each party connected to a VMR port is handled as a PtP call between itself and the Multipoint Control Unit (MCU) resource controlling the call for the VMR. As such, if the party can support encryption the call-link between the participant and the VMR will be encrypted. If the party cannot support encryption, the call-link between the participant and the VMR will be allowed to connect but it will be unencrypted. PSTN dial-in participants, by virtue of the technology being used, will join VMR calls as an unencrypted audio-only participant.

1.1 Encryption methods used

- AES 128-bit encryption for media
- TLS for SIP call control
- SRTP for SIP media
- H.235 for H.323 media
- AS-SIP

AS-SIP is a superset of SIP signalling requirements deemed necessary by the United States Department of Defence (DoD). It is fully supported in the Kinly Cloud service, including DSCP tagging, secure TLS signalling and SRTP media security.

The following table provides guidance on encryption for the various participant categories:

Participant type, Encryption and Encryption Technology

Participant Type	Encryption Status	Encryption Technology
H.323/SIP Endpoints	Dependent on capabilities of external party	SIP TLS or H.323 H.235 signaling Secure RTP (AES-128)
Skype for Business (Lync)	Encrypted	SIP TLS signaling Secure RTP (AES-128)
Web Browser (WebRTC)	Encrypted	Secure HTTP signaling Secure RTP (AES-128)
PSTN Dial-In and External Audio	Unencrypted	N/A

1.2 Kinly Cloud Control Interface

Kinly Cloud delivers an intuitive interface, Kinly Cloud Portal, that allows users to control the CloudRoom from virtually anywhere and on any device.

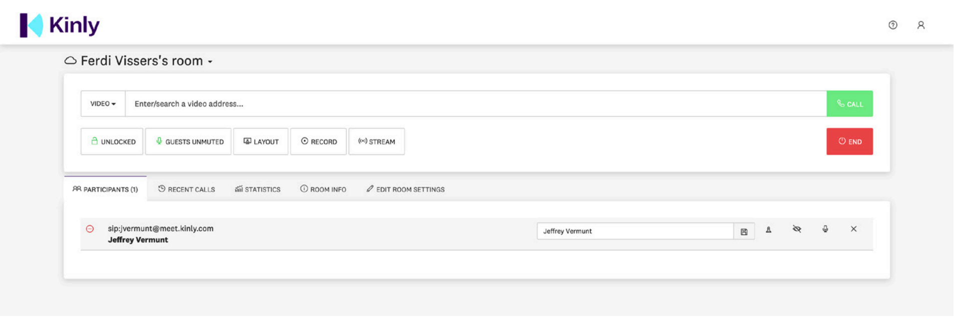
From a security perspective, the Control Interface gives users the ability to lock the room during a conference, to prevent any new users interrupting the call. It also provides a central point to manage the users' PIN codes and passwords.

Security in the Kinly Cloud

1 Virtual Meeting Room Calls

1.3 High-level feature description

The Kinly Cloud Portal can be tailored and branded to fit the needs of users and companies, and ensures a good user experience, high quality, flexibility and security.



Ferdi Vissers's room

sip:jvermunt@meet.kinly.com
Jeffrey Vermunt

Jeffrey Vermunt

Key meeting controls tokens

- Ability to lock meeting so that no one can interfere
- Add / remove participants
- Visibility on who is in the meeting
- Audible and visible notifications of when people leave and join
- If meeting is locked, guests are left in the waiting area until host lets them in
- Ability to move guests in and out of Lobby
- Possibility to select and add Host and guest PIN code
- Guests are in held in Lobby area until Host has arrived
- Ability to promote a guest to meeting host
- Ensure secure delegation of rights to control the meeting
- Mute guests to avoid disturbance in the meeting

1.4 Access control

There are two ways to restrict access to the CloudRoom; PIN code and locking the conference.

Locking the conference

If you want to prevent any further participants from joining a conference after it has started, you can lock it from the Kinly Cloud user interface. After a conference has been locked, participants who are attempting to join the conference will be kept in the Lobby until they are allowed access by the Host.

In addition, if the conference is locked the Host can remove participants from the conference and place them in the Lobby.

This would be valuable in a board meeting where you have invited a participant to present a short topic. You would not want them to join the meeting until you are ready for them and would also not want them to be present for the rest of the meeting after they have finished their presentation. The Host would be able to see when they are in the Lobby ready to present, and let them in when appropriate, and also lock them out again afterwards.

Pin Codes

For added security, you can set up your CloudRoom with PIN numbers. You can use the same PIN for all participants, or use separate PINs to differentiate between Hosts and Guests. When a participant connects to a Cloud Room that has a PIN, they are greeted with an Interactive Voice Response (IVR) screen where they are asked to enter the PIN number. They must enter the correct PIN before they can join the conference.

1 Virtual Meeting Room Calls

1.5 Certificates

Kinly Cloud utilises security certificates for cloud-based applications to ensure the integrity and secure client access. The certificate requirements are dependent on the chosen deployment model, and the applications to be hosted in the Kinly Cloud.

2 Video Device Registration

2.1 Privacy of communications using SIP TLS and SRTP

The Kinly Cloud supports direct registrations of hardware-based (endpoints) video devices from several vendors, providing cloud-based call control, processing, and interworking for signaling and media. The native signaling protocol used by the service is SIP, and security is enforced by requiring encrypted signaling via SIP TLS. For video and audio media, the data is encrypted to AES-128 standard, resulting in Secure Real Time Transport (SRTP) media streams.

The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. Kinly Cloud ensures privacy of all audio and video calls by enabling (by default) encrypted signaling using SIP TLS and encrypted media using Secure Real-time Transport Protocol (SRTP) for all communications on audio and video.

SIP TLS works in the same way as HTTPS, which we use daily on a secure webmail access or online banking access. This means that the overall security model of SIP TLS is based on the digital certificate verification process.

SIP signaling communication over TLS provides great value as it hides access to sensitive information from any unauthorized third party and provides a secure method of exchanging keys for SRTP media encryption, which ensures privacy of all data (audio, video and presentations) sent using the Kinly Cloud service

For encryption and decryption of data (and hence providing confidentiality), SRTP (together with SRTCP) utilizes AES as the default cipher.

NOTE: Kinly Cloud also supports H323 registrations and both signaling and media is encrypted with H.235 and AES-128.

2.2 Video Device Parameters and Firmware

The Kinly Cloud Service Network will only configure sufficient settings on a registered video device to allow it to operate on the Cloud Video Service. These settings include parameters to uniquely identify it on the Service Network, and to set its calling profile.

The parameters which are set include:

- Display Name
- SIP URI video address
- Company Phone book address
- SIP Proxy / H323 Gatekeeper
- Keep alive timer

The Kinly Cloud Service Network leaves the management of video device firmware levels to the end-user, so that the end-user can maintain the User Interface they prefer. The Kinly Cloud Service Network does require that the device firmware levels are above the minimum version level required for direct registration support to the Cloud Video Service, and we do recommend that firmware levels used should include fixes for known security vulnerabilities.

3 Points of presence, Data Types and Storage

3.1 Points of Presence (PoPs)

Customers can select their Points of Presence based on their specific requirements. This can be customized per their individual provisioning and can be limited to specific countries or regions. This is to help customers comply with any potential regulatory or policy requirements.

Kinly Cloud currently maintains Points of Presence in multiple global locations, including:

- Oslo, NO
- London, UK
- Frankfurt, DE
- Singapore, MY
- Ashburn, US
- Finland, FI
- Sao Paolo, BR

Kinly Cloud PoPs are hosted at Data Centers managed by service providers such Google Cloud Platform, IBM Cloud and Basefarm. Each of the facilities has multi-factor security for access, including but not limited to human security, security cameras, photo identity card access and key access to the equipment rack. Each facility is compliant with the main security compliance standards, such as SOC2, SSAE16 and ISO 27001.

3.2 Types of Data Stored

Kinly Cloud provides a cloud-based video service that enables subscribers to register video endpoints to the cloud for call-control and routing, as well as access to video bridges to facilitate multi-participant collaboration. The video service should be considered solely as a secure conduit for real-time video and audio communications between participants. It does not store participants' data beyond that which is necessary to uniquely identify them on the service for the purpose of call processing to initiate, route, maintain and terminate calls. Call Detail Records (CDRs) are generated by the video services to allow subscribers and their organizations to track call activity, such as confirming appropriate reporting on call frequency and duration. Kinly Cloud will use aggregated CDRs to help understand macro call trends and evolve the service to best serve the needs of our customers, as well as providing technical support for specific calls when necessary.

To be able to access the video service, users will be asked to provide a minimum of information so that they can establish unique identities on the service for call processing and personal account maintenance. At the individual level, this will user data includes a name and an e-mail address.

The following is a summary of the data requested by Kinly Cloud. Any additional data accessible by an end-user of the Cloud Video Service is in the form of Call Detail Records.

Types of data required to identify a specific user include:

- First Name, Last Name
- Email address
- Contact Phone (optional)
- Video address

Types of data generated and stored during use of the video service may include:

- Type of video device and software level
- Internal and external IP address assigned to the video device
- Start and stop time for video calls
- Parties the video device initiated calls to, and received calls from
- Media statistics for the video calls (bandwidth use, packet loss, jitter)
- Signaling and media paths used in call establishment and tear-down

3 Points of presence, Data Types and Storage

3.3 Data Encryption, Storage and Access

Web portal access

All data and communications in the Kinly Cloud are stored securely and encrypted by default. All web-based communications use HTTPS, which is a widely used secure communications protocol. HTTPS also utilizes the SSL/TLS protocol, which adds an additional later of security when communicating with and managing devices, users and additional services on the Kinly Cloud platform.

User provisioning

User provisioning can be done either by manually creating a user, CSV import or via customer integrated SAML 2.0 driven Single Sign On (SSO).

If provisioning is done without SSO, Kinly Cloud will need to store the user password for the service.

If SSO is used, the username will be stored, but since the authentication will take place on the customer's own systems, no password will be stored by Kinly Cloud. The SAML integration means the password is not read by Kinly at any stage.

Storage

All data stored for the service is handled by Kinly Cloud-managed ISO27001-certified data center located in Oslo Norway, or in Google Cloud data centers with encryption at rest for all data. Kinly has full control over which country data is stored in. Only Kinly authorized personnel can access data. Authorization is only given on a need-to-know basis or for operational purposes. Data center service providers do not maintain or access data. Depending on the customer requirement, data can be limited to a specific country or region.

Access

Access to the infrastructure and data in the Kinly Cloud is limited to Kinly operations and technical support staff. These staff members may access elements of the Kinly Cloud Service via VPN and subsequent to that, secure terminal sessions via SSH, and Web-based UI sessions via HTTPS.

The remote access to the core components is secured by named accounts, with two-factor authentication. The accounts are controlled in an IAM (identity access management) system where delegation of rights is controlled. Access is logged for traceability and attempts to access accounts are monitored continuously.

4 Network and Data Center Security and Maintenance

4.1 Network and Data Center security

Kinly Cloud physical and virtual servers, which comprise the infrastructure behind the Kinly Cloud Service, are installed at reputable and highly secure third-party data centers. The use of carrier-independent service providers, carrier-neutral data centers, and Internet exchanges ensures the best possible "last mile" connectivity from the customer locations to our services. These data center vendors also ensure the highest-grade secure facilities, restricting physical access as well as maintaining the highest security certifications such as SOC2, SSAE16 and ISO 27001, while offering operational reliability with an average uptime of more than 99.99%.

Within each data center, Kinly Cloud maintains virtual servers hosting various services, along with other devices to manage and secure the PoP (points of presence). The services and devices within each PoP are monitored by Kinly Operations. Operation monitoring and logging also includes maintains a close watch on activity like access to tools, the creation/modification/termination of subscriptions, traffic loads on PoP devices, system CPU loads and disk I/O rates. Notification alarms are sent to Kinly Cloud technical staff
when events occur which fall outside configured thresholds.

Kinly's global media Network enforces encryption in transit. Kinly's global data center Internet links perform full encryption on top to most customers' network service providers. Kinly only uses recognized service providers to ensure a high level of customer confidence. Private networking can also be provided with QoS (Quality of Service) tagging to further enhance customers security and eliminate potential third-party packet capture.

Security in the Kinly Cloud

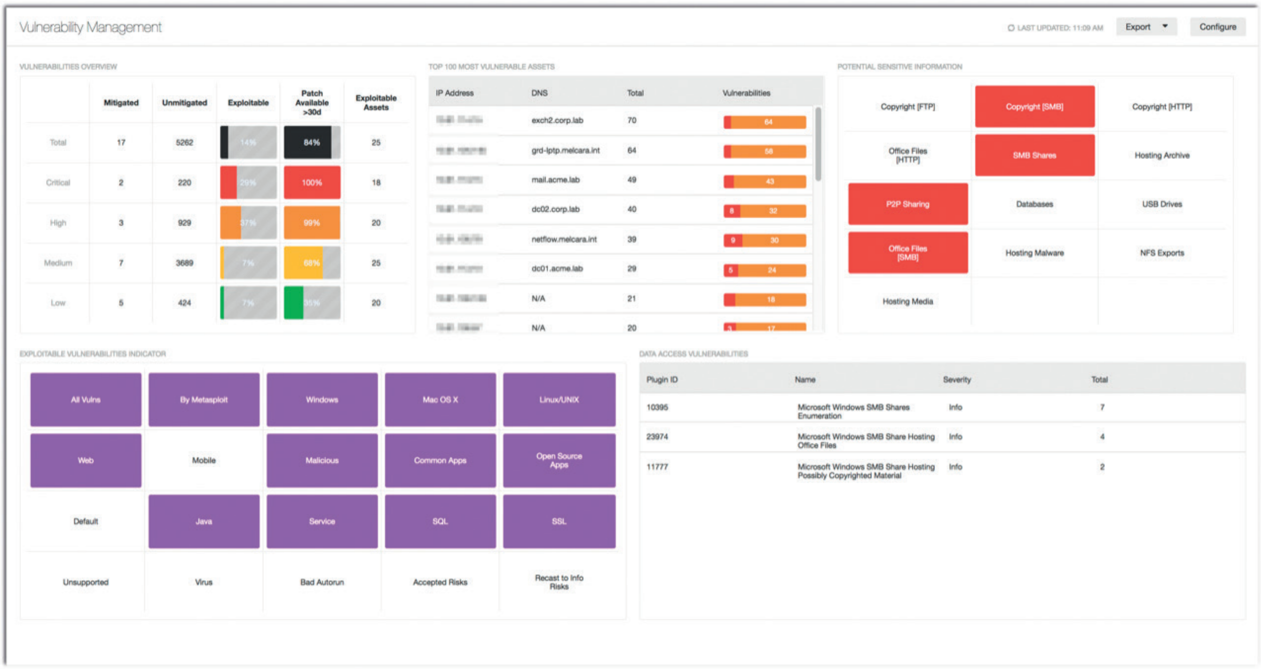
4 Network and Data Center Security and Maintenance

Monitoring

Kinly Cloud systems are continuously monitored on both an application and infrastructure level. Any anomalies in behaviour or possible security issues are escalated in accordance with our incident handling process.

Security scanning

Kinly performs weekly security and vulnerability scans on all systems using state-of-the-art vulnerability scanners, alongside regular third-party penetration test. Reports are provided on request.



VULNERABILITIES OVERVIEW

	Mitigated	Unmitigated	Exploitable	Patch Available >30d	Exploitable Assets
Total	17	5262	14%	84%	25
Critical	2	220	29%	100%	18
High	3	929	37%	99%	20
Medium	7	3689	7%	68%	25
Low	5	424	7%	35%	20

TOP 100 MOST VULNERABLE ASSETS

IP Address	DNS	Total	Vulnerabilities
[redacted]	exch2.corp.lab	70	64
[redacted]	grd-lptp.melcara.int	64	58
[redacted]	mail.acme.lab	49	43
[redacted]	dc02.corp.lab	40	8 32
[redacted]	netflow.melcara.int	39	9 30
[redacted]	dc01.acme.lab	29	5 24
[redacted]	N/A	21	18
[redacted]	N/A	20	3 17

POTENTIAL SENSITIVE INFORMATION

Copyright [FTP]	Copyright [SMB]	Copyright [HTTP]
Office Files [HTTP]	SMB Shares	Hosting Archive
P2P Sharing	Databases	USB Drives
Office Files [SMB]	Hosting Malware	NFS Exports
Hosting Media		

EXPLOITABLE VULNERABILITIES INDICATOR

All Vulns	By Metasploit	Windows	Mac OS X	Linux/UNIX
Web	Mobile	Malicious	Common Apps	Open Source Apps
Default	Java	Service	SQL	SSL
Unsupported	Virus	Bad Autorun	Accepted Risks	Recast to Info Risks

DATA ACCESS VULNERABILITIES

Plugin ID	Name	Severity	Total
10395	Microsoft Windows SMB Shares Enumeration	Info	7
23974	Microsoft Windows SMB Share Hosting Office Files	Info	4
11777	Microsoft Windows SMB Share Hosting Possibly Copyrighted Material	Info	2

Security incident management

All incidents, including security incidents, are logged in Kinly's ITSM system for processing at the relevant level by our operations team.

4.2 Security Patching

Kinly Cloud services run on Linux or Windows operating systems. The application portfolio consists of in-house developed applications as well as third-party vendor applications.

To mitigate any potential threats at operating system level or in the software components, Kinly Cloud follows the Common Vulnerabilities and Exposures (CVE) system [1]. This provides a reference-method for publicly known information-security vulnerabilities and exposures, and makes it easier to collect data on potential vulnerabilities across all Kinly systems and enhance security.

In addition to checking CVE notifications, Kinly Cloud also monitors security announcements from any vendors whose software and equipment is deployed in the Kinly Cloud Service Network. As security notifications from the various vendors are disclosed, Kinly assesses the threat and exposure level, and takes appropriate action to remediate any issues.

Servers are patched with security updates when vulnerabilities are reported. For urgent patches, a maintenance window will be scheduled so corrective action can be taken as quickly as possible but with least disruption to Kinly Cloud's global subscriber network – typically this is outside normal business hours in as many regions as possible. For non-urgent patches, the corrective action is rolled into the next regularly scheduled maintenance window.

5 Kinly Meeting Assistant

5.1 Data and Privacy

The Kinly Meeting Assistant smart phone app complies with all applicable privacy and data regulations, including GDPR. No user-owned data, including all information in the calendar, leaves the device and remains in the control and ownership of the end-user. The app has been subject to third-party security code review and pen-testing to ensure high quality security on both app and related service**s.**

For more information regarding Kinly's privacy policy, please refer to https://**www.kinly.com/privacy**

6 Google Cloud Platform appendix

6.1 Introduction

This appendix contains specific information regarding the Kinly applications delivered on Google Cloud Platform. Customer specific requirements regarding hosting region and data storage are addressed, as well as security features on the Google Cloud Platform [2] utilized by Kinly will be address during the on-boarding process. This appendix will highlight the security measures utilized by Kinly. For a complete reference refer to Google's documentation as listed in sources 3 & 4 at the end of this document.

6.2 Operations and Identity Management

Operations on customer-related infrastructure are only performed by authorized Kinly support and operations staff. Access is controlled by operations management via an Identity and Access Management (IAM) system. The IAM grants access using two-factor authentication. Attempts to access the system are monitored by Google 24/7 and suspicious activity is mitigated accordingly.

6.3 Internet Communication

Internet communication out to service providers peering points with Google is encrypted on top of standard TLS/SSL encryption. Google continuously monitors for attempted Denial of Service attacks, and takes effective measures to block suspicious. Access to customer platform is controlled by firewalls, which are setup and controlled by Kinly. Google operates sophisticated Intrusion Detection across the entire platform.

6.4 Secure Storage

All data is stored in selected Google Cloud Platform regions. All data at rest is encrypted. Specific regions can be requested by the customer.

6.5 Secure Deployment

Deployments in Google Cloud Platform are logically isolated. Access to data and infrastructure is controlled by Kinly's IAM. Internal traffic is encrypted between services. Sole tenant servers to provide further customer isolation are available on request

6.6 Physical Security

Access to data centers is limited to authorized Google personnel. Google uses multiple physical security layers to protect its data centers, including biometric identification, metal detection, cameras, vehicle barriers and laser-based intrusion detection systems.

6.7 Operations and Identity Management

Delivery platform is compliant with GDPR, ISO 27001 and most acknowledged industry standards [4].
Kinly Cloud is also compliant with ISO 27001 security standards.

7 References

[1] CVE - cve.mitre.org

[2] Google Infrastructure Security Design Overview
cloud.google.com/security/infrastructure/design/resources/google_infrastructure_whitepaper_fa.pdf

[3] Google Cloud Platform: Security
https://cloud.google.com/security/

[4] Google Cloud Platform: Standards, regulations and certifications
cloud.google.com/security/compliance/

Kinly

kinly.com