Statement of Work
Setting up Kinly Cloud for Google Meet Interop

Kinly

Statement of Work
Setting up Kinly Cloud for Google Meet Interop

Table of Contents

1 Planning and design

1.1 Domains and certificates for Google Meet interop

1.2 DNS and SRV

2 Implementation

2.1.1 Customer G Suite configuration

2.1.2 Google Meet Interoperability settings

2.1.3 Controlling access to gateway interoperability

2.2 Firewall Openings

Statement of Work
Setting up Kinly Cloud for Google Meet Interop

1 Planning and design

NOTE: If you already have the Cloudroom service from Kinly Cloud, no additional certificates or DNS records are required to allow gateway services to Google Meet – please go to section 3.

1.1 Domains and certificates for Google Meet Interop

You first step is to decide which domain is to be used when dialing into the Kinly Cloud gateway.

This is the domain that will be used by Skype for Business clients and other video conferencing systems when dialing into a Google Meet conference.

Dialing into a Google Meet conference			
	Customer domain	**Example**	**Note**
Domain		@meet.example.com	

To set the domain, follow these steps:

(i) Generate a certificate signing request (CSR)

After a domain is chosen, Kinly will create the CSR, and hand this over to the you.

(ii) Certificate signing

If you are responsible for you own domains, you will need to get the CSR signed with a Certification Authority (CA). If your domains are managed by a third party, you will need to get the third party to get the CSR signed.

(iii) Send the certificates to Kinly

When the CSR has been signed, send the certificate details to your technical contact at Kinly. The certificate details should be sent via email and the ZIP password sent via SMS.

Once these are received Kinly will add the certificate to the service, and your technical contact will send you the required internal and external DNS configuration details.

You will need to configure your own internal and external DNS (see section 1.2) and verify that the service is reachable from both internal networks and external networks.

Statement of Work
Setting up Kinly Cloud for Google Meet Interop

1 Planning and design

1.2 DNS and SRV

This section sets out the DNS details required for directing traffic for the chosen domain to the cloud (see section 1.1 for details on selecting your domain name).

- Example DNS change: Kinly Cloud – Gateway services for Google Meet

  This section assumes that the gateway domain is**: meet.example.com**

A Records

Device	IP	Target
Kinly Gateway Server	(Provided by Kinly)	(Provided by Kinly)

SRV Records

Domain	Service	Protocol	Port	Target
meet.example.com	h323cs	tcp	1720	(Provided by Kinly)
meet.example.com	h323ls	udp	1719	(Provided by Kinly)
meet.example.com	sip	tcp	5060	(Provided by Kinly)
meet.example.com	sips	tcp	5061	(Provided by Kinly)
meet.example.com	sipfederationtls	tcp	5061	(Provided by Kinly)

Statement of Work
Setting up Kinly Cloud for Google Meet Interop

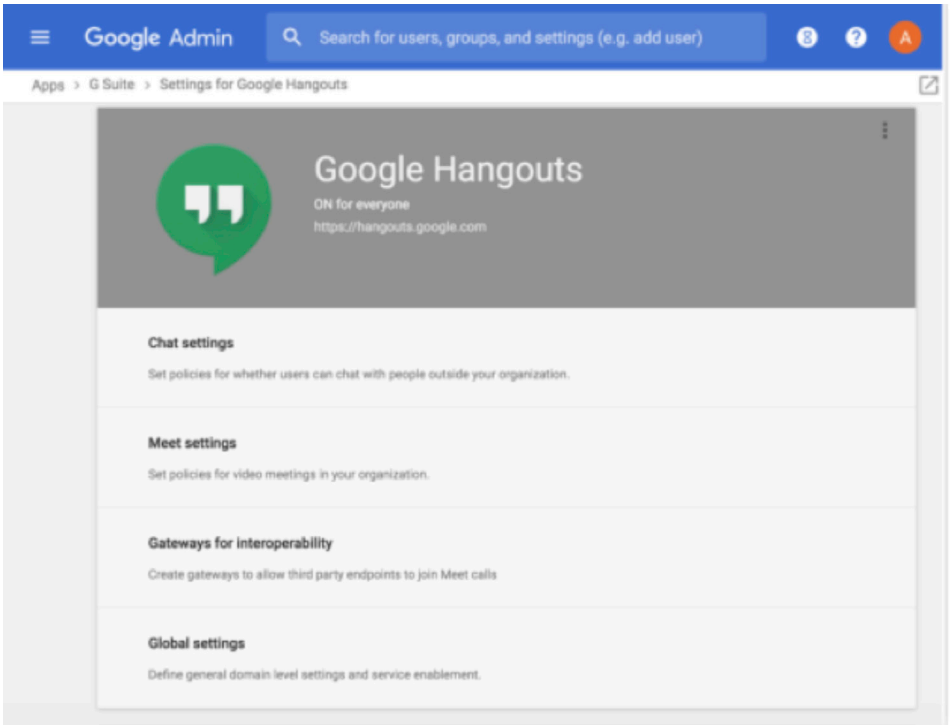
2 Implementation

2.1.1 Customer G Suite Configuration

To allow gateway services from Kinly Cloud to access your Google Meet environment, you need to configure your G Suite account as follows:

(i) Go to Google Hangouts Settings

You can configure your Google Hangouts Meet settings from the Google Admin console via **Apps > G Suite > Google Hangouts.**



(ii) Generate your gateway access tokens

To set up your trusted and untrusted gateway access tokens in the G Suite Admin Console:

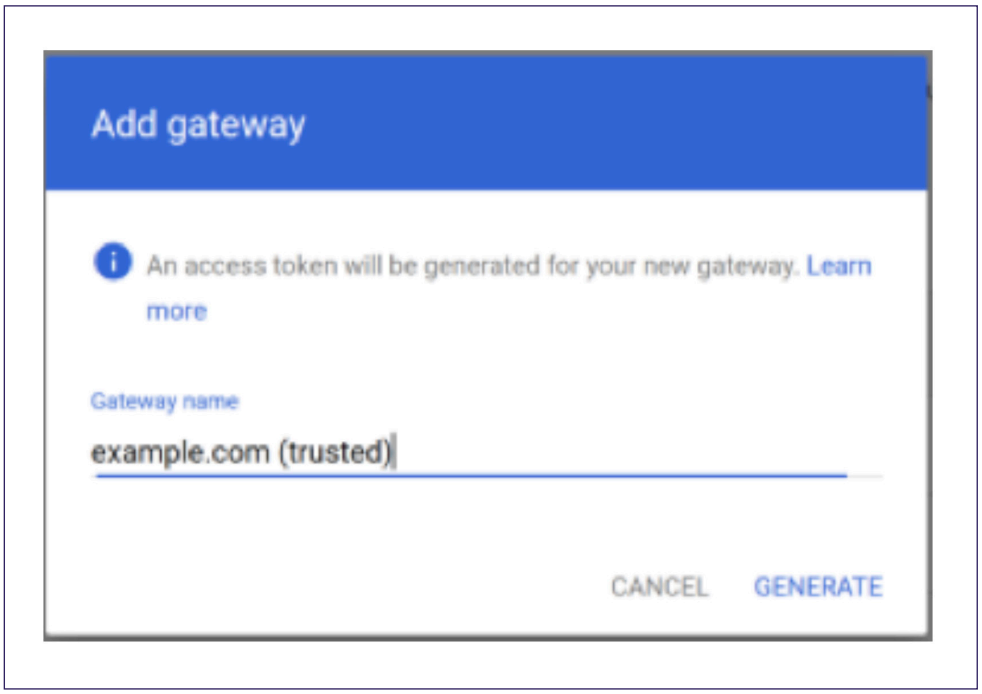
Go to **Apps > G Suite > Google Hangouts > Gateways for Interoperability.**

Select **Add Gateway.**

Enter a gateway name, for example the domain of the gateway domain plus a “trusted” or “untrusted” label, for example “meet.example.com (trusted)”.

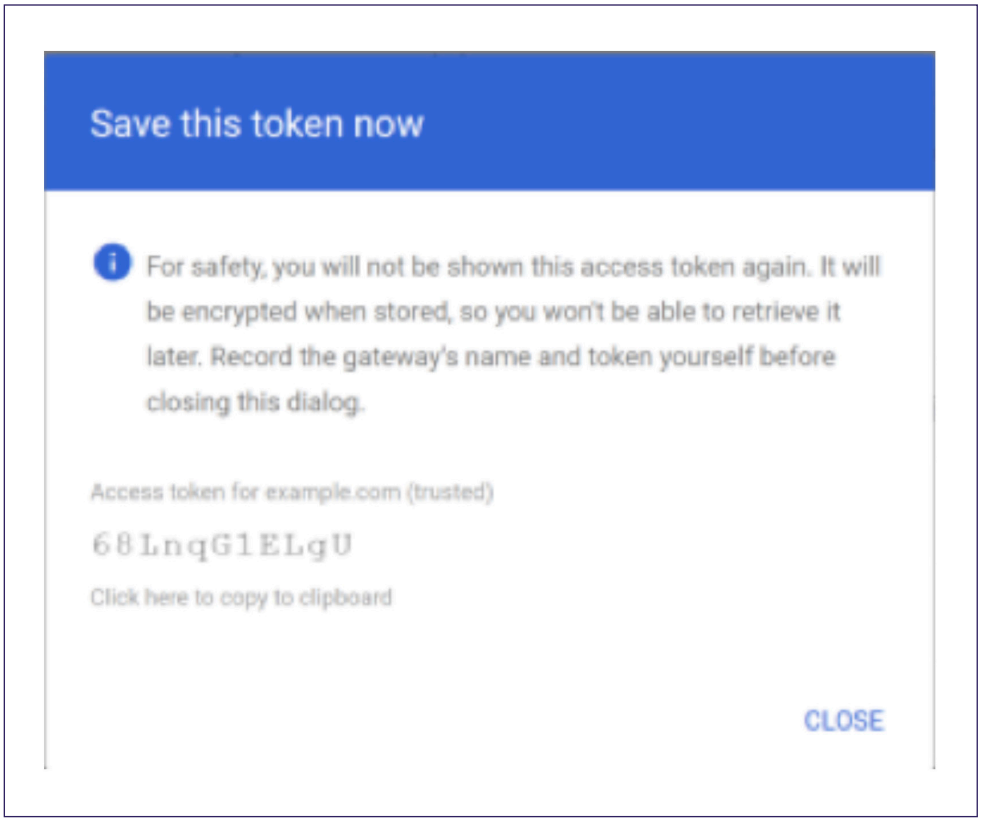
Statement of Work
Setting up Kinly Cloud for Google Meet Interop

2 Implementation



Select **Generate.**

You will now be shown the generated access token.



This token must be saved and passed to kinly

To do this, use the option to copy the token to your clipboard.

NOTE: This is the only time you will be able to see the token before it is stored and encrypted in G Suite, so it is crucial you do not skip this part.

Repeat Step 2 to create the untrusted token as well. In total two (2) tokens must be passed to Kinly.

Statement of Work
Setting up Kinly Cloud for Google Meet Interop

2 Implementation

2.1.2 Google Meet Interoperability settings

You also need to enable Hangouts Meet interoperability to allow other systems to dial into your Hangouts Meet calls. You do this via **Apps > G Suite > Google Hangouts** and then configure the **Meet settings.**

Make sure all boxes are ticked. Then go down to the “Interoperability” at the bottom of the menu on the left hand side of the screen.

This section needs to be filled out with the details you received from Kinly during the design phase.

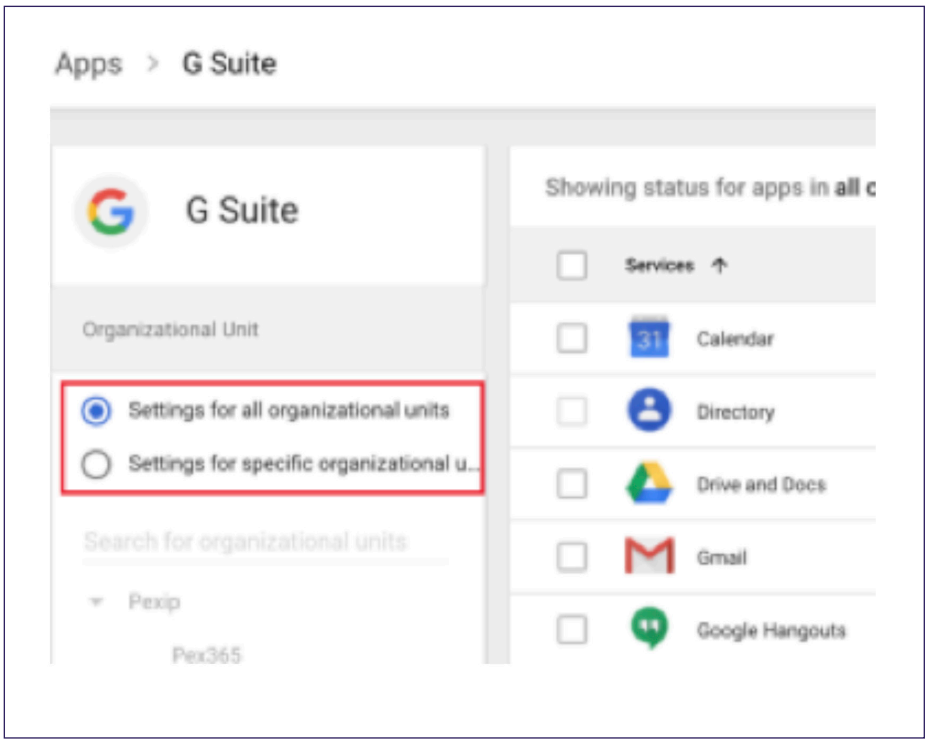
- **PIN prefix**
  This is optional, but Kinly may instruct you to add one
- **Gateway IP address used for external guest joining instructions**
  This IP will be provided by Kinly
- **Gateway DNS address used for external guest joining instructions**
  This is the gateway domain for example meet.example.com.

Statement of Work
Setting up Kinly Cloud for Google Meet Interop

2 Implementation

2.1.3 Controlling access to gateway interoperability

Once you have completed you interoperability settings, you can enable everybody in the organization to offer gateway interoperability to their Google Meet conferences, or limit this to specific organizational units. See the screen shot below for details.



Statement of Work
Setting up Kinly Cloud for Google Meet Interop

2.2 Firewall openings

NOTE: If you already have the Cloudroom service from Kinly Cloud, no additional firewall rules are needed to allow gateway services.

The following firewall rules must be in place at to reach KinlyCloud gateway services to Google Meet.

Endpoints deployed behind NAT From Trust to Untrust (outbound)

Protocol	Ports	Comment
TCP	443 / 1720 / 2776 / 5060 / 5061	Provisioning/signaling
TCP	443 / 389 / 636	Phonebook
UDP	123	NTP
UDP	1719 / 2776 / 2777 / 3478	Signalling and media
UDP	20000 – 65535	RTP/RTCP (media)

Endpoints deployed without NAT From Trust to Untrust (outbound)

Protocol	Ports	Comment
TCP	443 / 389 / 636 / 1720 / 5060 / 5061	Phonebook/signaling
UDP	123 / 1719 / 3478	NTP / signaling
UDP	1024 – 65535	Media

Protocol	Ports	Source	Comment
TCP	1720 / 5060 / 5061	Any	Signaling
UDP	1024 – 65535	Any	Media/signaling

From Untrust to Trust (inbound)

Skype for Business From client / SfB Edge to Kinly Cloud

Please note that you must also redirect Skype for Business to the Google Meet gateway domain.

Protocol	SRC Ports	Desk Ports	Comment
TCP / UDP	Any	40000 – 49999	RTP/RTCP/RDP/DTLS/RTMP/STUN/TURN
TCP	Any	5061	SIP / TLS
TCP	Any	80	HTTP

Skype for Business From Kinly Cloud to client / SfB Edge

Protocol	SRC Ports	Desk Ports	Comment
TCP / UDP	40000 – 49999	Any	RTP/RTCP/RDP/DTLS/RTMP/STUN/TURN
TCP	33000 – 39999	5061	SIP / TLS

Statement of Work
Setting up Kinly Cloud for Google Meet Interop

2.2 Firewall openings

WebRTC From client to Kinly Cloud

Protocol	SRC Ports	Desk Ports	Comment
TCP / UDP	Any	40000 – 49999	RTP/RTCP/RDP/DTLS/RTMP/STUN/TURN
TCP	Any	80	HTTP
TCP	Any	443	HTTPS

WebRTC From Kinly Cloud to client

Protocol	SRC Ports	Desk Ports	Comment
TCP / UDP	40000 – 49999	Any	RTP/RTCP/RDP/DTLS/RTMP/STUN/TURN