Kaltura Video Messaging architecture and setup guide for Microsoft Office 365

Last Modified on 04/22/2025 10:04 am IDT

This article is designated for administrators.

About

This guide describes how to configure Kaltura Video Messaging (aka 'Pitch') for use with your Office 365 Enterprise deployment. This guide is intended for Office 365/Azure administrators, and Kaltura admins in your organization that configure your instance of the Kaltura Platform.

Kaltura Video Messaging is a cloud-hosted web application built on top of the Kaltura Platform, which allows users to send personalized video-centric email messages that grab recipient's attention and result in up to 300% increase in open and click-through rates. Video Messaging allows your users to record a personalized video and send an HTML email with links to a personalized landing page with that video message embedded within the landing page.

Communications

Authentication and authorization

Application Authentication

Server-to-Server authentication and authorization between Video Messaging and Microsoft Office365 is handled via Oauth2. For more information, see the article on Microsoft Identity Platform and OAuth 2.0 Authorization Code Flow.

User Authentication

Video Messaging users from your organization are authenticated to the Video Messaging application via SAML 2.0 using the Identity Provider of your choice. User management, authentication, and authorization to use the application is handled by your organization's Identity Provider.

Video Messaging can integrate with any Identity Provider that supports SAML 2.0.

Hosts

All Video Messaging services are hosted in the kaltura-pitch.com domain on the Amazon Web Services infrastructure. You will need to allow users access (via network

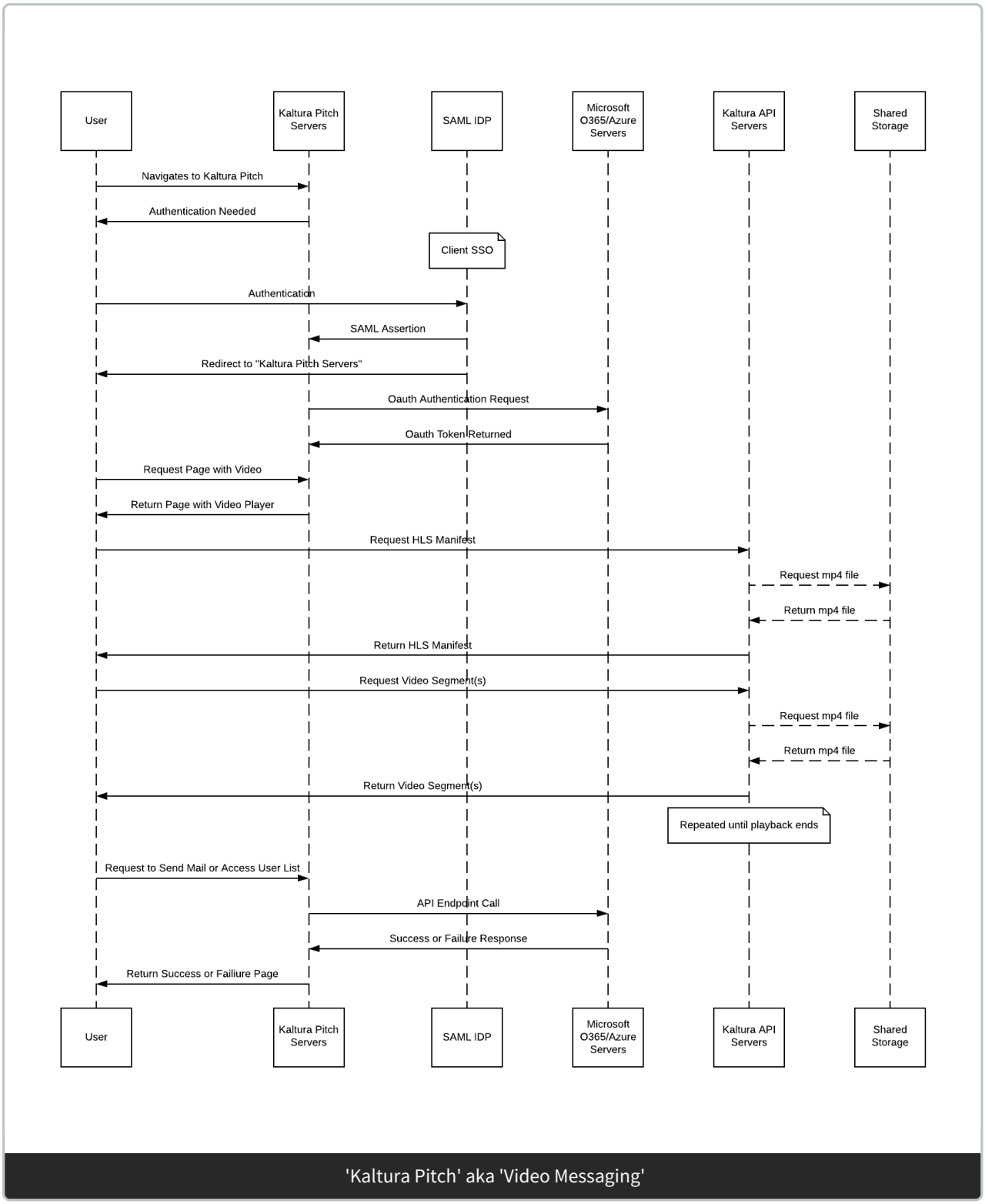
firewall, web application, firewalls, proxies, or VPN gateways) to *.kaltura-pitch.com or <your-organization>.kaltura-pitch.com.

If you need to allow access via IP address, please contact your Customer Success Manager, or open a ticket with Kaltura Customer Care to obtain the most recent list of Kaltura IP addresses.

Ports and Protocols

All communications between the Kaltura Platform and Office 365 use SSL on TCP port 443 encrypted with TLS 1.2 or better.

Data flow diagram



'Kaltura Pitch' aka 'Video Messaging'

Administrative Setup for Office 365/Azure

Video Messaging is an Oauth2 application that interfaces with Microsoft Azure AD on Office365 to deliver email on behalf of your users. This section describes the administrative configuration required for Video Messaging.

Required privileges

The following table describes permissions required by the Video Messaging application from Office365 to send emails on behalf of your users.

Azure permission	Functionality
Maintain access to data you have given it access to.	Maintain access to data for the authenticated user.
Send mail as you	Allows the app to send mail as the authenticated user.
Read your relevant people list.	Allows the app to read a list of people in the order that's most relevant to the authenticated user. This includes the user’s local contacts, contacts from social networking, people listed in your organization's directory, and people from recent communications.
Read all users' basic profiles	Allows the app to read a basic set of profile properties of other users in your organization on behalf of the authenticated user. Includes display name, first and last name, email address and photo.
View your email address	Allows the app to read the authenticated user’s primary email address.
Sign in as you.	Allows the user to sign in to the app with your work or school account and allows the app to read the user’s basic profile information.

Microsoft API Endpoints

With the permissions described in 3.1, Video Messaging makes the following MS Graph API calls:

- /v1.0/me/sendmail

- /v1.0/me/people - List People
- /v1.0/users - using a filter of startswith on displayName, surname, mail, userPrincipalName - to provide an auto-complete experience when the user fills out recipients of video message.

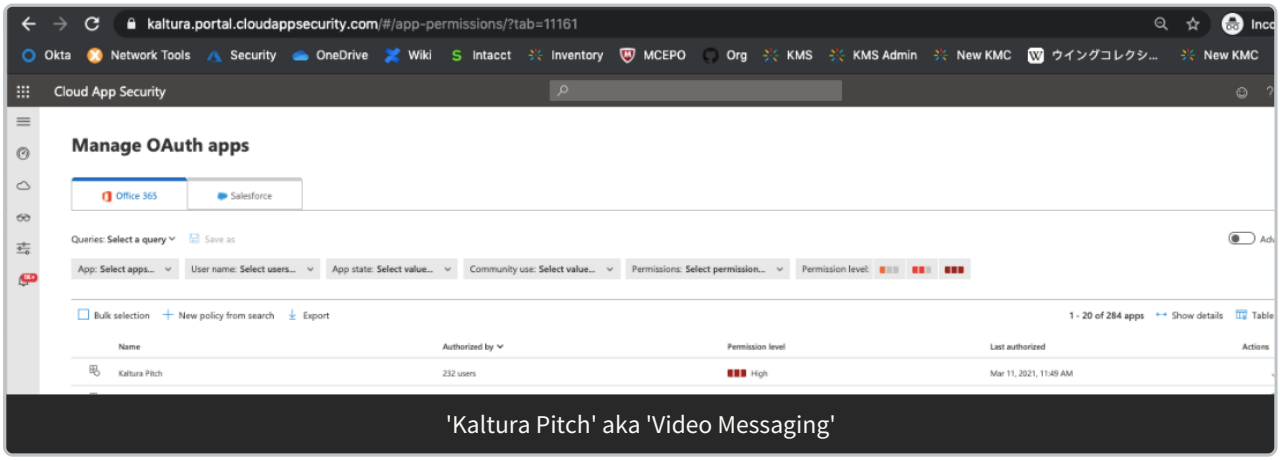
Office 365/Azure Administrative Configuration

Allow OAuth Applications

To allow Video Messaging users to send email via your Office 365 system, administrators must create an OAuth application policy for the Video Messaging application with the API scopes defined here using the Microsoft Cloud App Security Administrator. Your administrator will need to create or approve the Video Messaging app under their OAuth policies, as shown in the following screenshot.

Detailed documentation about how to create Oauth polices and assigned permissions can be found in the following articles:

- OAuth App Policies
- Manage OAuth Apps



'Kaltura Pitch' aka 'Video Messaging'

Configure Video Messaging Single Sign On (SSO) for User Access

Video Messaging authenticates users to the Video Messaging application via SAML 2.0. Please contact your Kaltura Customer Success Manager to configure SSO.

If your organization uses Kaltura Video Portal already, and you want the same users to have access to Video Messaging, then it is usually simply a matter of replicating the SAML configuration from Kaltura's Video Portal to Video Messaging.

If you do not use Kaltura's Video Portal, or you want to further restrict access to Video Messaging, you will need to create and configure a new application/service within your Identity Provider, and then work with a Kaltura Integration Engineer to configure this

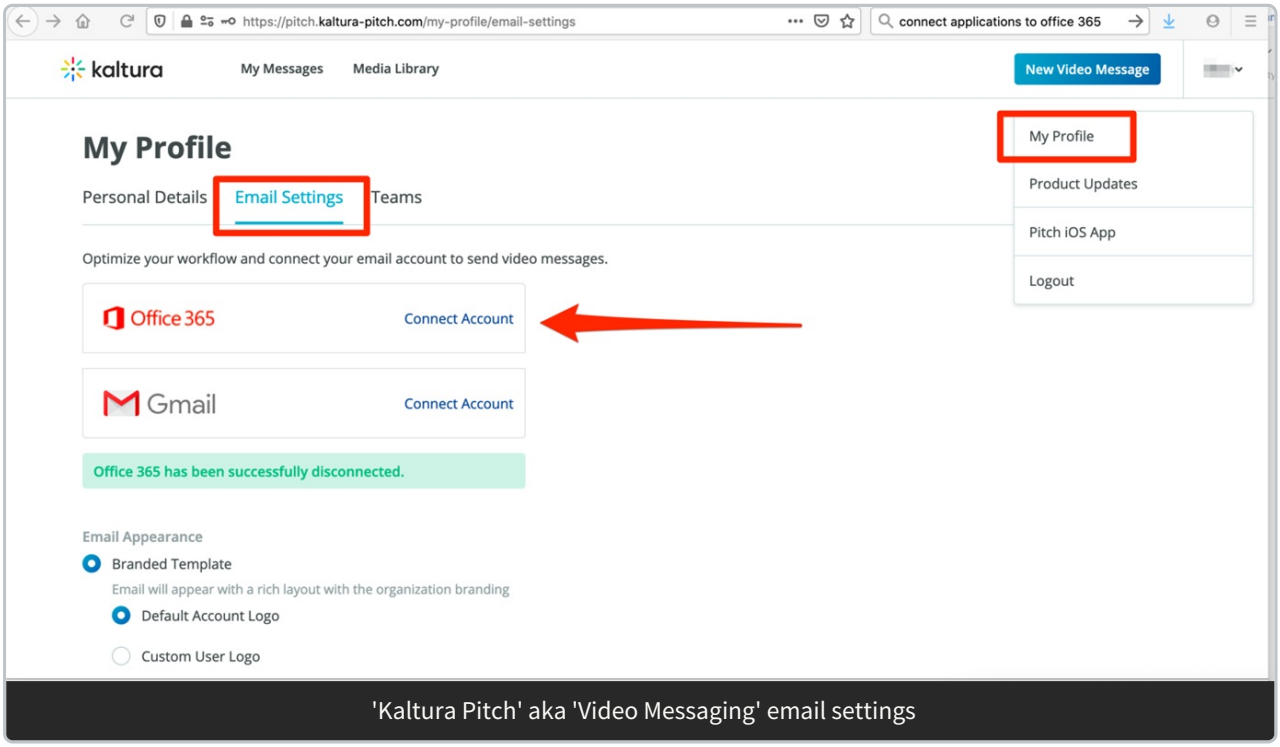
with the Video Messaging Administrator. Your Kaltura Customer Success Manager or Account Executive can assist in scheduling an Integration Engineer.

User setup

Initial user login and configuration

Once your Office 365 instance is configured to allow Video Messaging as an OAuth application, and SAML authentication is configured, allowed users will be able to configure their Video Messaging application to send mail via O365.

After a users log into their Video Messaging instance at https://<your-organization>.kaltura-pitch.com, they will be able to configure the connection to O365 by navigating to “My Profile,” > Email Settings as illustrated in the following screenshot:



'Kaltura Pitch' aka 'Video Messaging' email settings

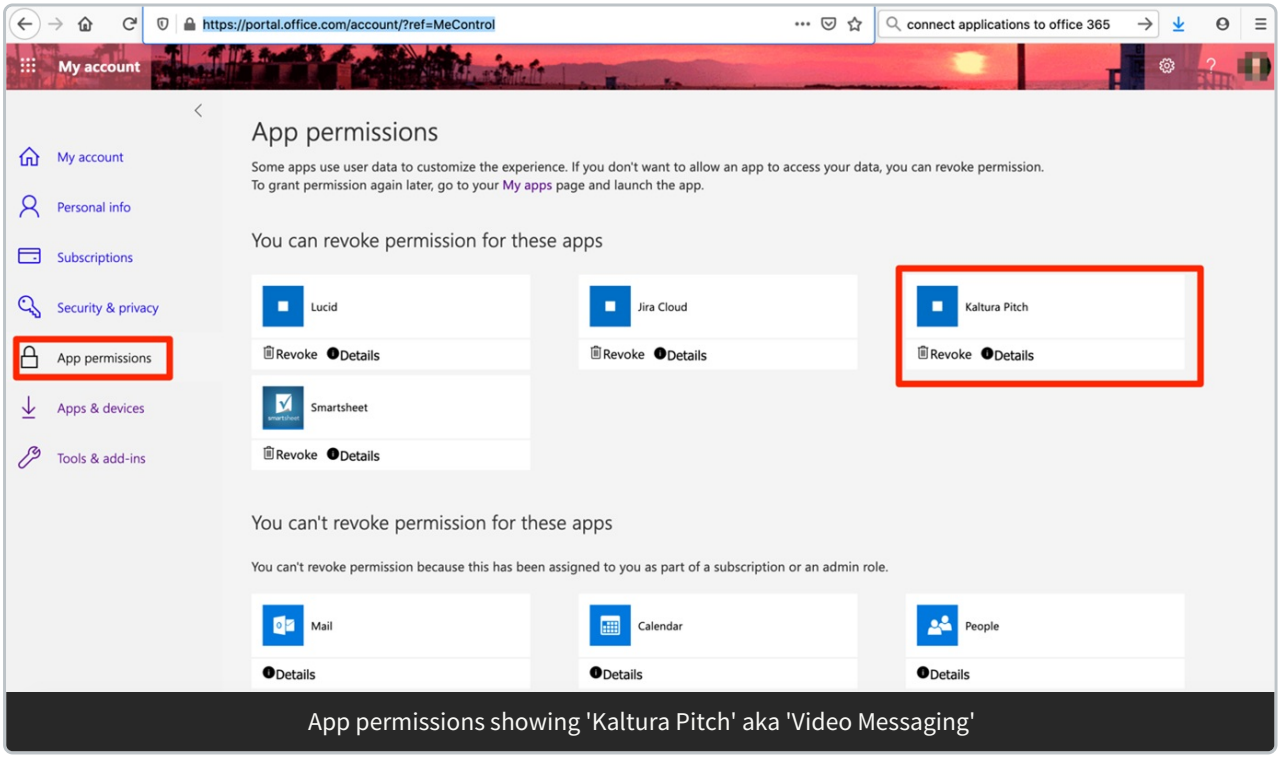
Setting up a Custom Signature Feature

Users may want to set up a customized signature to appended to their Video Messaging messages. For more information see the article about the Video Messaging custom message signature feature.

Revoking Video Messaging application permissions

Video Messaging users can disconnect Video Messaging from Office 365 through the “My Profile” screen within the Video Messaging application.

Application permissions can further be explicitly revoked in the “My Account” section of their Office 365 Portal at: https://portal.office.com/account/?ref=MeControl. The Video Messaging application permissions are revoked under the “App Permissions” setting, as shown in the following screenshot. If the user is a member of multiple Video Messaging organizations, there may be more than one entry for Video Messaging under App Permissions.



App permissions showing 'Kaltura Pitch' aka 'Video Messaging'