

Kollective PoC Guide - Kaltura Media Space

This document provides a simple guide to implement the Kollective ECDN in your environment and assumes a familiarity with the terms within and associated documents such as the ECDN Technical Brief. Trial activation through integration and network configuration is completed in 5 simple steps and typically takes just a few minutes.



Trial Setup

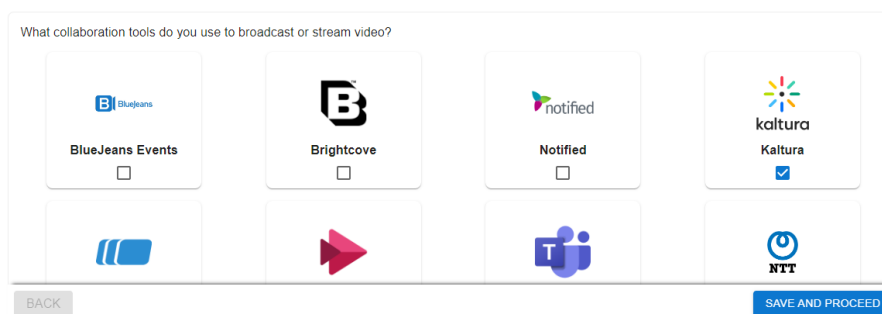
Step 1 - Create Account

To register for the trial navigate to <https://portal.kollective.app/free-trial>, click on "Start Today" and enter your details. During this process you will be prompted to logon using your AAD, SAML or Google Workspace account with your standard Single-Sign-On credentials. Depending on your local policy, an AAD administrator approval may be required to accept the permissions that enables your enterprise SSO.

A successful login will result in creation of a secure customer tenant within Kollective.


Step 2 - Configure Integrations

The Kollective portal provides a configuration wizard which prompts you with the partner platforms that are enabled for ECDN integration. Select the required integration and click "Save and Proceed":



The portal will provide the instructions and configurations specific to your Kollective tenant. It will be a requirement to forward the Tenant ID and Token to Kaltura for enablement of Kollective within your Kaltura tenant, (note there are also dependencies around cluster enablement, embedded content and player versions that the Kaltura team are aware of that must be configured also).

YOU'RE ALMOST THERE!



KALTURA CONFIGURATION

VIA KALTURA MEDIA SPACE (KMS) ADMIN UI

- Your MediaSpace will need to be enabled for Kaltura Webcast Events
- The Kollective streaming module will need to be installed
- Sign into the KMS Admin (its your usual KMS url with admin appended).
- Find and click on the Kollective streaming modules from the menu on the left of the page (you may wish to press Ctrl-F and search for Kollectivestreaming).
- Choose enabled: Yes
- Copy and paste the serviceToken and tenantId into the respective boxes provided
 - Tenant ID

tenantId
 - Service Token

appToken
- Click Save

BACK
SAVE AND PROCEED

Step3 - Define Network Configurations

There is a default configuration that enables peer-to-peer (P2P) content delivery within the same /24 IPv4 and /64 IPv6 subnets. Most customers will typically "Enable Network Customisation" and apply the following configurations:

- Global Policy
 - Used when there is no configured Location. The default policy that groups users by /24 IPv4 subnet will be acceptable for most trials but can be modified as required. If you wish to disable peering for unknown Locations this is applied at this level also as is a default bitrate configuration.
- Create Locations
 - Allows configuration of site boundaries based on public/private IP addressing or URL Probe. Locations are created manually or via a simple import process by using the available template.

NETWORK SETTINGS AND CONFIGURATION

Ensuring your network has the optimal set-up and configuration is key to successfully delivering video to your organization. Kollective has terrific "Out of the Box" settings that work well for most networks, a configuration wizard to make entering your VPNs, home users and network locations straightforward and easy, and an advanced option if your network has additional complexities and would benefit from Kollective Technical Support. Find the option that works best for you below! For more information on IP anonymization and mDNS, please see the [documentation space](#) of the Customer Portal.

Enable Network Customization

Create Global Policy
 Create Locations
 Create Policies
 Assign Policies to Locations

Configure your Network Locations

⚠ You must save network settings for location changes to take effect. Importing additional locations is not allowed while there are unsaved changes.

Name ↑	Internal Subnets	Public Ips	Policy	Tags	Actions
<input type="checkbox"/> EU HQ	10.0.0.0/16, 10.1.0.0/16, 10.255.0.0/16				<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> Remote Users	192.168.0.0/16		Peering Disabled		<input type="checkbox"/> <input type="checkbox"/>

- Create Policies:
 - Policies create specific controls for content including Peering enablement, Bitrate controls, EdgeCache selection, Cluster size and per location Privacy controls.
- Assign Policies to Locations:
 - Policies are created on a 1-to-many basis. On creation of Policies these should be applied to relevant Locations, either manually or via the import. The available filtering options can be used to select multiple Locations for assignment.

On completion of Network Configurations click "Save and Proceed."

Step 4 - Manage Privacy Settings

Privacy Settings are available to control the data that Kollective captures and stores for analytics purposes. Within this Step there are 3 configuration options:

- Enable Custom Privacy Settings
 - Toggles used to enable storage at a global level of specific event and user criteria. Note that some fields are only relevant with a Kollective agent installed.

PRIVACY SETTINGS

Enable Custom Privacy Settings
Enables the ability to set additional constraints on the data that is collected and stored in Kollective's analytics.

DATA COLLECTED

Event Title
This comes from the event name entered into the video app that was used to deliver your event.

Internal IP
Commonly referred to as a private IP, this is the IP address of the computer that your videos or content were delivered to.

External IP (Coming Soon)
Commonly referred to as a public IP, this is the IP address for large portions of your network such as a router or a switch.

Machine Name
In order to take advantage of this reporting feature, you must have a Kollective Agent installed on the end-user's computer to receive it. The machine name refers to the name used to label the end user's computer.

Machine User
If you are using Kollective Agents for peering and/or software delivery, you can take advantage of our ability to collect and store the machine name of the device that Kollective delivered to. This eases your ability to know exactly which machines in your network participated in peering or consumed content in your network.

User Email
Please be advised, in some countries in the EU, corporate email addresses have been determined to be Personally Identifiable Information and should be treated with great care. In order to enable this feature, please reach out to your account team as we require a data processing agreement (DPA) to meet GDPR requirements.

O365 ID
This is the anonymized ID that users in the Office 365 video applications are given. This data can only be collected for video delivered through either Microsoft Teams or Stream.

- PII Access
 - Toggle to globally enable or disable access to fields such as IP and email address for visibility within analytics. If disabled individual users can be enabled to access on a per-user basis.
- Microsoft Analytics Link Settings
 - Toggle to enable a link to Kollective Portal in Microsoft Teams Live Events.

Step 5 - Invite Users

This step of the wizard is used to enable "Automatic User Approval" or invite individual users to the portal. On logon to the portal users can be assigned privileges using Role Based Access Control.

Customer Pre-requisites

Network Pre-requisites

With the assumption that Browser Based Peering will be used for a trial, there are very few pre-requisites and ECDN functionality will typically work out of the box in most environments. The requirements document at <https://portal.kollective.app/docs> provides an overview of network requirements and associated hosts. Partner front-end integration connectivity will also be required.

IP Address Anonymisation Whitelisting

IP Address Anonymization is a feature of modern browsers that support WebRtc to conceal the internal IP address of the desktop from any site on the web that may be deliberately invoking WebRtc to obtain IP address and compromise the privacy of the user. We **strongly** recommend that IP Address anonymisation is disabled for relevant integration URLs via a simple GPO. An overview and instructions are provided at <https://portal.kollective.app/docs/ip-address-anonymization-and-mdns>.

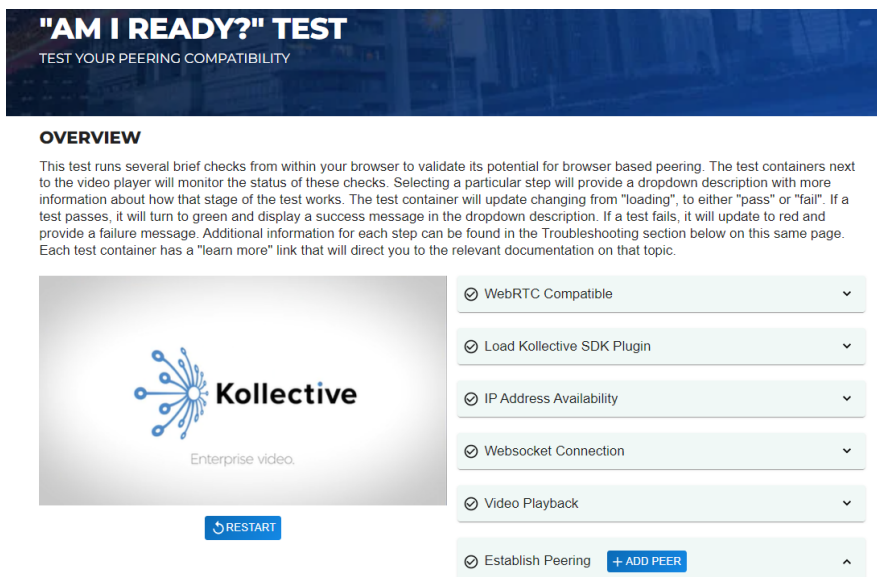
https://*.kollective.app and https://*.mediaspace.kaltura.com should be enabled for anonymisation in the relevant policy.

Testing & Validation

As mentioned above Kollective provides various mechanisms to validate connectivity, prior to integration, using sandboxed video testing with in-built validation. The 3 tests that are available are:

Am I Ready?

A simple first test that proves connectivity across individual or a range of hosts is available at <https://portal.kollective.app/peering-compatibility> via portal logon. To run the test simply follow the link and a unique URL will be generated, after performing connectivity checks, the player will load and playback begins. To add browser sessions click on the “Add Peer” button to open another tab with the session, and then wait for the metrics to update to show that peering is taking place between the two sessions.



"AM I READY?" TEST
TEST YOUR PEERING COMPATIBILITY

OVERVIEW

This test runs several brief checks from within your browser to validate its potential for browser based peering. The test containers next to the video player will monitor the status of these checks. Selecting a particular step will provide a dropdown description with more information about how that stage of the test works. The test container will update changing from "loading", to either "pass" or "fail". If a test passes, it will turn to green and display a success message in the dropdown description. If a test fails, it will update to red and provide a failure message. Additional information for each step can be found in the Troubleshooting section below on this same page. Each test container has a "learn more" link that will direct you to the relevant documentation on that topic.

WebRTC Compatible

Load Kollective SDK Plugin

IP Address Availability

Websocket Connection

Video Playback

Establish Peering **+ ADD PEER**

Kollective
Enterprise video
RESTART

Note that IP Anonymisation (see above) affects this test (and the Rapid Network Test below). In addition be aware that analytics are not stored for the “Am I Ready” test.

Rapid Network Test

A more enhanced test to prove the ECDN in your environment and allow multiple configurations during testing. On enablement of the Rapid Network Test at <https://portal.kollective.app/rapid-test> a test event is created within the Portal that can be distributed to users, with the benefit that results are stored in Analytics. In addition there is no portal login requirement when using the RNT.

Network Readiness Test

The NRT enables the ability to test at scale using 1000s of end-user devices running a silent (user unaware) network readiness test and analyse results from across your enterprise. Additional detail is available within the Kollective ECDN Technical Brief and at <https://portal.kollective.app/network>

Integration Validation

To validate that integration configurations have been synchronised, simply, create and start a new live event in Teams. After the event has started and users have joined you can use the Kollective dashboard at <https://portal.kollective.app/dashboards> to view and validate events in progress.

Live events, both test and real, are used to evaluate and review the performance of the Kollective ECDN. The two major metrics are Quality of Experience (is the user experience sufficiently acceptable for the user to clearly receive the message) and Bandwidth Savings at a per Location or Cluster basis (is it reducing the traffic sufficiently to avoid congesting the network).



The following table represents sample test criteria:

Sample Test	Method	Relevant Metrics	Criteria
Small test event	Run a live event. Have at least 5 users on same network location access the event ensuring that users join at the same time and are connected for at least 10 minutes.	Bandwidth Saving (Is there peering between nodes?) QoE (Does the video load and playback smoothly?)	Users receiving the same stream at same time initiate peering amongst each other. Changes in user behaviour does not affect other users. Each user receives content at an acceptable quality/bitrate and without buffering.
Large event	Repeat to a larger audience across multiple locations.	BW Savings Globally and per Location QoE Globally and per Location Audience reach	

What Next

The PoC does not have usage limitations, so can be used for optimising real events at unlimited scale. After the trial is complete (30 days), the configuration will expire, but the setup and data will not be removed unless specifically requested. This means that there is no further configurations or activations required once you choose to become a Kollective customer. Kollective can assist you with interpreting the data from the trial to understand how further improvements can be made address other requirements.

Associated Resources

- Kollective Customer Portal - <https://portal.kollective.app>
- Documentation - <https://portal.kollective.app/docs>
- Analytics - <https://portal.kollective.app/dashboards>

Kollective PoC Guide - Kaltura Media Space

Document Created: 28 March, 2023

Last Modified: 29 March, 2023
