Intuiface's Cloud-based Infrastructure

Table of Contents

Document scope and content

This document describes:
- four Intuiface usage models, from the most open model (where all Intuiface cloud-based services are used) through the most closed model (where none are used).
- global architecture for the Intuiface Cloud Infrastructure
- links and dataflow between Intuiface Player, Composer, and various servers
- how and where Intuiface data are stored
- all endpoints reachable by Intuiface Player and Composer.

To understand this document:
The Intuiface platform has three licensable products: Intuiface Composer, Intuiface Player and Intuiface Analytics. Composer is the editor and it is used to create experiences. (Experiences contain all content, primarily media, code and metadata files). Player is the runtime and it is used to run experiences. Composer runs on Windows PCs while Player runs on multiple operating systems. Analytics runs in the cloud (For more about Composer, Player, and Analytics, see our Overview page.) Composer and Player can be used without Internet access. However, several features – like Analytics - are only available if access to various Intuiface servers is granted. These servers are collectively referred to as the **Intuiface Cloud Infrastructure** within this document.

Summary of Intuiface Usage Models

Intuiface's infrastructure requirements are quite flexible. As a result, multiple options are available, enabling selection of the one most appropriate for a given set of IT restrictions and preferences. The following four scenarios are examples of possible Intuiface usage models, from the most open model (where all Intuiface cloud-based services are used) through the most closed model (where none are used).

Full Cloud

Use Intuiface Cloud Storage or a private Amazon S3 bucket to store published Intuiface experiences. (Intuiface projects are referred to as "experiences".) All Intuiface cloud services such as remote experience deployment onto Player as well as Analytics are available.

Hybrid

Use an in-house FTP/FTPS server behind a firewall to store published Intuiface experiences, while still taking advantage of all Intuiface cloud services such as remote experience deployment onto Player as well as Analytics. Both Composer and Player must have access to the FTP/FTPS server.

No Experience Publishing

Experiences are not published to the Intuiface Cloud, an Amazon S3 bucket, or an FTP/FTPS server. Intuiface experiences are deployed either manually or via in-house automated means. All devices running Composer and Player have at least occasional access to the Internet, so their licenses can be

checked and renewed when required. Players can use Analytics; locally stored data points are sent to the Analytics server when Player has access to the Internet.

Offline

Intuiface experiences are managed using a LAN file system and deployment onto Player is an in-house responsibility. (With Players offline, it is not possible to remotely deploy to them or manage them). Also unusable is Analytics and any of the cloud-hosted social media platforms supported by Intuiface. Intuiface's offline licensing option is also required, involving manual license requests submitted to Intuiface Technical Support. All in all, about 80% of Intuiface capabilities will be accessible. (Still impressive by any measure!)

Introduction and Global Architecture

The Intuiface Cloud Infrastructure can be broken down into three distinct cloud-based components:

1. Intuiface Cloud Storage: Stores and manages experiences published to cloud storage provided by Intuiface. (Alternatively, experiences can be stored on a private Amazon S3 bucket or on a in-house FTP/FTPS server).
2. Intuiface Business Management Infrastructure (IBMI): Manages Intuiface user information, metadata for published experiences, and all business-related processes.
3. Intuiface Analytics Management Infrastructure (IAMI): Manages and stores data points collected by Analytics feature.

These three components are outlined in red in the global architecture diagram below:
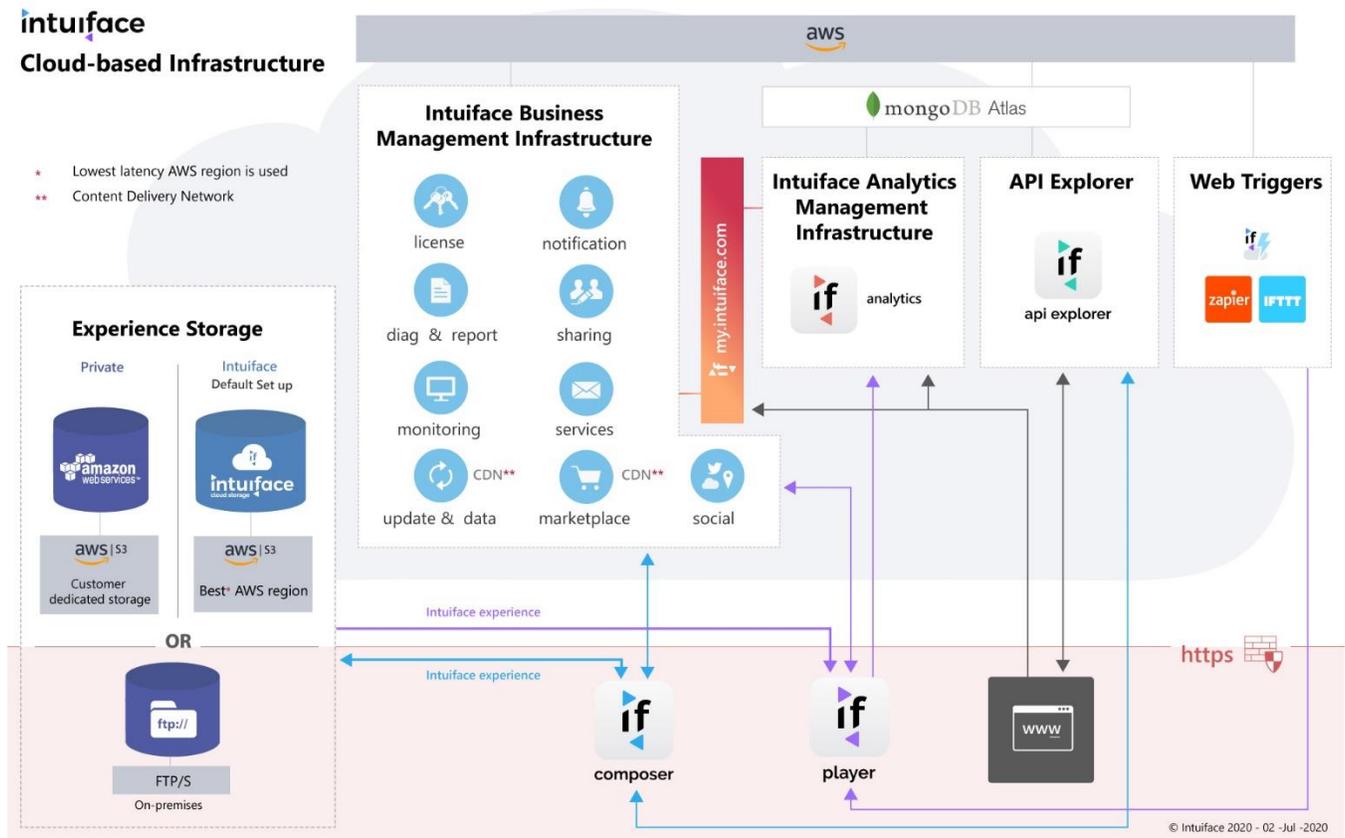
For an overview of how Intuiface works, visit our online Overview page

Global security considerations

Intuiface Cloud Infrastructure is entirely based on Amazon Web Services (AWS), which offers a high level of information security (confidentiality, integrity and availability) as demonstrated by several security-related certifications (including ISO27001, SOC 1, SOC 2, SOC 3).

All Intuiface Cloud Instructure traffic uses https TLS/SSL v1.2. Player and Composer only need outbound connections so only outbound port 443 must be opened for Intuiface Composer and Player to access Intuiface servers. No inbound connection is used by Player and Composer.

Intuiface's entire AWS infrastructure is protected by the AWS Firewall, and all data are encrypted at rest.

Server status can be monitored at status.intuiface.com. On that site one can register for notification about server issues – via text message or email – in real-time. See Track Status of Intuiface Cloud Services for more information.

NOTE: Intuiface received its ISO/IEC 27001:2013 certification in April 2020. Both Intuiface Player and Composer, Intuiface Cloud Storage, Intuiface Business Management Infrastructure (IBMI), and Intuiface Analytics Management Infrastructure (IAMI) are within the scope of this certification.

Intuiface Experience Storage

If a user wishes to publish an Intuiface experience – a prerequisite for sharing and remotely deploying that experience - three storage options are available: Intuiface Cloud Storage, a user-configured Amazon S3 bucket, or a user-configured FTP/FTPS server.

Documentation for how to select and configure the preferred Intuiface experience storage option can be found online.

Intuiface experiences do not have to be published to be deployed to other devices. See our article about how to deploy unpublished experiences for details.

Intuiface Experience Storage does not retain a history of experience versions. Only the most recently published instance of an experience is saved. As a result, experience versions should be backed-up from the Windows PC on which they have been edited in Composer using an independent, user-driven process.

Intuiface Cloud Storage (default option)

Intuiface Cloud Storage is built on top of Amazon S3 (Simple Storage Service) and uses Amazon IAM services. The Amazon S3 region closest to the country of a given Intuiface account (determined via GeoIP) is selected as the content storage location for experiences published by that account. The closest Amazon S3 region is determined during the first experience publish for the account.

Amazon S3 storage is designed for high integrity and availability. According to Amazon, the durability of each file is 99.999999999%[1] and availability is 99.99%.

---

[1] This means that if your 1000 experiences each 1000 different files, you will – on average - only lose a file every 100 000 years.

In order to retrieve or update an experience, the user must use Composer or Player; there are no external links to the experience or its content.

For the United States, regardless of an account's location, us-east-1 is used for the AWS region.

Upon request sent to support.intuiface.com, the default cloud storage location of an Intuiface account can be changed to some other location.

To use Intuiface Cloud Storage, Player and Composer must be permitted to access the domain **amazonaws.com.** Alternatively, you may restrict access to the URLs listed in the table below.

The following table lists the default locations of Intuiface storage per country or world region as well as their domains.

Region in the world	Default Location of Intuiface Storage	Domain used by Intuiface
US + Central-America	US (North Virginia)	s3.us-east-1.amazonaws.com
Canada	Canada (Montreal)	s3.ca-central-1.amazonaws.com
South-America	Brazil (Sao Paulo)	s3.sa-east-1.amazonaws.com
Europe	Germany (Frankfurt)	s3.eu-central-1.amazonaws.com
	Ireland	s3-eu-west-1.amazonaws.com
	Great-Brittan (London)	s3.eu-west-2.amazonaws.com
	France (Paris)	s3.eu-west-3.amazonaws.com
Japan area	Japan (Tokyo)	s3-ap-northeast-1.amazonaws.com
Korea area	Korea (Seoul)	s3.ap-northeast-2.amazonaws.com
India area	India (Mumbai)	s3.ap-south-1.amazonaws.com
Singapore area including China	Singapore	s3-ap-southeast-1.amazonaws.com
ANZ area	Australia (Sydney)	s3-ap-southeast-2.amazonaws.com

All Intuiface experiences stored in Intuiface Cloud Storage are storage-level encrypted (at-rest encrypted) using Amazon S3-Managed Keys (SSE-S3), based on AES 256-bit cypher.

We provide temporary token-based content segmentation to ensure separation between Intuiface Accounts.

User-configured Amazon S3 bucket

This is similar to Intuiface Cloud Storage but the bucket is created, managed and paid for by the user's organization. Refer to creating an AWS S3 bucket to store your experiences to understand how to create such Amazon S3 bucket as well as to enhance security by restricting IP access to the Amazon S3 bucket. When using a private Amazon S3 bucket, you may use one of five additional regions:

- South-Africa,

- Bahrain,
- USA: Oregon,
- USA: Ohio,
- USA: North California

Amazon S3 storage was designed for high durability and availability. According to Amazon, the durability of each file is 99.999999999%[2]. Availability is 99.99%.

User-configured FTP/FTPS server

A user-configured FTP/FTPS server can be located behind a firewall, in the LAN, or on the Internet. Due to the various implementation options available for FTP/FTPS servers, IT skills are required for successful configuration. FTP/FTPS server must also be appropriately sized – with particular focus on bandwidth – to accommodate large deployments with multiple Players making simultaneous requests.

Intuiface Business Management Infrastructure (IBMI)

All user and Intuiface experience metadata are stored in an AWS RDS (Relational Database Service) database, an AWS managed database, located in the eu-west-1 region of Europe. These metadata include:

- Intuiface account email & password (salted-hashed sha256)
  - Includes company name, user first and last name, alternate contact email address
- User ID for the Intuiface account,
- Billing information if the user has purchased the product online using a credit card (only the last four last digits and expiration date of a credit card are stored)
  - Includes list of invoices
- License information
  - Includes License ID, Device ID, Intuiface application name, and Intuiface application version
    Collectively named the **Intuiface ID (IF-ID)**
  - Also includes name of the device on which the license is in use
- List of cloud storage connectors (**Storage-ID**):
  - If Intuiface Cloud Storage: its location
  - If FTP/FTPS or Amazon S3: encrypted credentials and its location
- List of cloud-stored experiences. For each experience:
  - Includes Intuiface Experience ID, Intuiface Experience name, Intuiface Experience size, Intuiface Experience initial scene snapshot image, collectively named the **Intuiface Experience Metadata (IF-XP)**
  - Also includes the Storage ID of the storage option associated with the experience

---

[2] This means that if your 1000 experiences contain each 1000 different files, you will – on average - only lose a file every 100 000 years.

All user and Intuiface experience metadata are storage-level encrypted (at-rest encrypted) using AWS RDS default encryption key of Intuiface.

Experience publishing and downloading flows

- In response to a Publish request, Composer retrieves experience storage temporary credentials from sharing.intuilab.com then directly accesses the user's storage environment and publishes all of the required[3] files that are part of an Intuiface experience (.ifx, .ifx.json and all media).
- In response to a Download request, Composer or Player retrieves experience storage temporary credentials from sharing.intuilab.com then directly accesses the user's storage environment and downloads all of the required[3] files that are part of an Intuiface experience (.ifx, .ifx.json and all media).
- In response to the Deployment (or Push) of an experience to a Player, initiated via the Intuiface Share and Deploy console (https://my.intuiface.com/shareanddeploy/#/devices), a command is prepared to be read by the Player. Player (or the Player Agent on Windows devices) regularly polls commands at monitoring.intuilab.com. When an Experience Deployment (or Push) command is waiting, Player interprets the command and retrieves experience storage temporary credentials from sharing.intuilab.com then directly accesses the user's storage environment and downloads all of the required files that are part of an Intuiface experience (.ifx, .ifx.json and all media).
- Temporary credentials delivered to Composer or Player remain available for a limited amount of time for security reasons.

An experience is never stored nor ever transits through IBMI. IBMI's main responsibility is to establish a proper connection between the Intuiface Experience Storage where a particular experience is stored and a Composer or Player instance where this experience is authored or played.

Intuiface Analytics Management Infrastructure (IAMI)

The Intuiface Analytics Management Infrastructure exists to support the Analytics feature. It gathers and collates user-specified data collected by Intuiface Player, as well as facilitates data-based chart and dashboard creation for measuring and monitoring user-defined KPIs (key performance indicators).

IAMI servers are located on AWS in the us-east-1 region of the United States.

Information collected by an Intuiface experience when using the Intuiface Analytics feature - i.e. the Intuiface ID and all data point content - are stored in a MongoDB databased hosted on www.mongodb.com/cloud/atlas which, in turn, is running on AWS in the us-east-1 region of the United States.

---

[3] Intuiface optimizes the publish/download process by only uploading/downloading files that have been modified, added, or deleted from an experience.

List of all services used by Intuiface

Web sites used for Intuiface

Web site	Intuiface Subdomain	Service Description	Cloud Infrastructure	Also Requires Access To
Public website	https://www.intuiface.com		Webflow (webflow.com)	
Management Console	https://my.intuiface.com	User account and license management, license purchase, experience deployment, experience sharing, access to collected data points	IBMI	www.intuiface.com (for pricing & purchase)
Support site	https://support.intuiface.com	Intuiface Support site and Help Center (documentation)	Zendesk	https://my.intuiface.com (for single sign-on)
User Community	https://community.intuiface.com	Open discussions within and among the Intuiface user community	Discourse (discourse.org)	https://my.intuiface.com (for single sign-on)

Services used by Composer and Player

This set of subdomains has been designed so the Intuiface user's Enterprise IT authority may decide which, if any, subdomain to block using their organization's firewall. Of course, preventing access to a subdomain will prevent usage of the features it enables.

NB: All services listed below require the URL https://license.intuilab.com to be accessible. If not accessible, no other service will be available.

Intuiface Service	Intuiface Subdomain	Service Description	Data Exchanged Across Firewall	Used by	Cloud Infrastructure	Also Requires Access To
Windows installers	https://data.intuilab.com	Download of installers for Composer and Player on Windows	Installers	Any web browser. Composer & Player can also download and run their latest installer if manually instructed to do so.	IBMI	
Android Player installers	android.intuiface.com	Download of installers for Android Player	Installers	Any Web browser.	IBMI	
Other Player installers	sssp.intuiface.com webos.intuiface.com brightsign.intuiface.com	Download of installers for Player on Non-Windows/Android devices	Installers	SSSP / LG webOS / BrightSign devices	IBMI	
Licensing	https://license.intuilab.com	License activation, license check and login	• IF-ID • Computer Name • Email/password if login	Player & Composer	IBMI	
Composer & Player on Windows update	https://update.intuilab.com	Information about update availability. There is no auto-update feature. This service is limited to update availability notification.	IF-ID	Player & Composer	IBMI	
Experience publish & download	https://sharing.intuilab.com		• IF-ID • IF-XP	Player & Composer	IBMI	Domains used for the storage NOTE: For Intuiface storage see above for the list of used domains.
Remote Player management	https://monitoring.intuilab.com	Remote Player software upgrade	• IF-ID			https://data.intuilab.com

Intuiface Service	Intuiface Subdomain	Service Description	Data Exchanged Across Firewall	Used by	Cloud Infrastructure	Also Requires Access To
	https://monitoring.intuilab.com	Remote deployment of Intuiface experiences	• IF-ID	Player	IBMI	https://sharing.intuilab.com Domains used for the storage NOTE: For Intuiface storage see above for the list of used domains.
	https://monitoring.intuilab.com	1. Player restart 2. PC reboot 3. Player monitoring 4. Player event reporting	• IF-ID • Computer Name • Player Events (i.e. start, reboot)			
Marketplace	https://s3-eu-west-1.amazonaws.com	Access to free and for-sale experiences published by Intuiface and other sellers	• IF-ID	Player & Composer	IBMI	https://sharing.intuilab.com
Analytics	https://analytics.intuilab.com	Storage of data points	• IF-ID • Data point content	Player & Composer	IAMI	
Information notification	https://services.intuilab.com	Information displayed in the Composer's Messaging Window	• IF-ID	Composer	IBMI	https://notifications.intuilab.com
Usage reports	https://report.intuilab.com	Used by Intuiface Customer Support and for usage analysis	• IF-ID • Experience-independent Composer/Player events	Composer & Player	IBMI	
Crash reports	https://diag.intuilab.com	Used by Intuiface Customer Support	• IF-ID • Crash Stack • .ifx • OS information	Composer & Player (before v6.3)	IBMI	
	https://sentry.intuilab.com			Composer & Player (starting with v6.3)		

Intuiface Service	Intuiface Subdomain	Service Description	Data Exchanged Across Firewall	Used by	Cloud Infrastructure	Also Requires Access To
Third party services proxy	https://social.intuilab.com	Used as proxy server for Twitter, Weather, GeoIP	• Search string for Twitter feeds • City/zip code for weather • IP address for geolocation	Composer & Player	AWS us-east-1	
API Explorer	https://api-explorer.intuilab.com		• IF-ID • API Request URL • .ifd descriptor	Composer	AWS us-east-1	
Email as a service	https://services.intuilab.com		• IF-ID • Email fields: from/to/subject/body/attachment(s)	Composer & Player	IBMI	
Template & Design Accelerator Download	https://data.intuilab.com	Download templates and design accelerators into Composer		Composer	IBMI	
Am I online?	https://license.intuilab.com/isonline.html	Internet connectivity check		Player & Composer	IBMI	
Web Triggers	https://webtriggers.intuilab.com	Enables Player to receive a message from any device on the Internet (v6.2 and later)	• IF-ID • associated tags using Web Sockets on https port (443)	Player & Composer	AWS us-east-1	

Services associated with Third Party URLs

Intuiface Service	Third Party URL	Service Description	Used by	Cloud Infrastructure
Map Collection	Mapbox: https://api.mapbox.com Bing Maps: http://ecn.t[1-4].tiles.virtualearth.net/	Get map content when using the Map Collection for either of Intuiface's two map providers, Mapbox and Bing Maps	Composer & Player	Mapbox (mapbox.com) Bing Maps (bing.com/maps)
YouTube Asset	Any YouTube URL	Display a video in the YouTube Asset	Composer & Player	YouTube

Document updates

- 30_June-2020:
  - Document reorganization to better describe the Intuiface Platform
  - Additional details were added
- 12-June-2020:
  - Updating Intuiface Cloud Storage section, with a new storage located in France
- 18-May-2020:
  - Adding how to enhance security by restricting IP access to a user-configured Amazon S3 bucket
- 12-May-2020:
  - Document reorganization to better describe the various Intuiface Cloud-based Infrastructures
- 06-Jan-20:
  - Added this Document Updates section
  - Added a fourth scenario in Usage Models
  - Minor wording fixes
- 19ˉNov-19:
  - Added Intuiface Cloud Storage domain names for the default storage locations associated with each country or world region
  - Updated some hyperlinks
- 01-Jul-19:
  - Added a chapter describing 3 usage models