

# IBM Watson IoT Platform Lite

Last Updated: 2021-12-10

IBM Watson IoT Platform Lite is a cloud-hosted service on IBM Cloud that makes it simple to derive value from Internet of Things (IoT) devices.

The product documentation Watson IoT Platform Lite is available from [IBM Cloud Docs](#). Additional information about the services of the Platform Service component can be found in this topic and in the [Maximo Asset Monitor](#) product documentation.

- [Quotas](#)
- [Basic concepts](#)
- [Service status](#)
- [Contacting support](#)

## Organizations

When you register with the Platform Service, you are provided with an organization ID, a unique six character identifier for your account. Organizations ensure that your data is only accessible by your devices and applications.

After registration, [devices](#) and API keys are bound to a single organization. When an [application](#) connects to the service by using an API key, it registers to the organization that is associated with that API key.

**Important:** For security reasons, direct communication between different organizations is not possible. To transmit data between two organizations, you must register one application with each organization and have the two applications communicate with each other to transfer data.

**Note:** Your organization ID is different from your [IBM Cloud organization](#).

## Devices

A device can be anything that has a connection to the internet and that can push data into the cloud. However, devices cannot communicate directly with other devices, instead devices accept commands from applications, and send events to applications.

Devices in Platform Service are identified by a unique authentication token. Devices must be registered before they can connect to Platform Service.



## Devices

A device can be anything that has a connection to the internet and that can push data into the cloud. However, devices cannot communicate directly with other devices, instead devices accept commands from applications, and send events to applications.

Devices in Platform Service are identified by a unique authentication token. Devices must be registered before they can connect to Platform Service.

Platform Service recognizes two classes of device:

Device type	Description
Managed devices	Devices that contain a device management agent. A device management agent is a set of logic that allows the device to interact with the Platform Service Device Management service by using the Device Management Protocol. Managed devices can perform device management operations, including location updates, firmware downloads and updates, restarts, and factory resets.
Unmanaged devices	Devices without a device management agent. Unmanaged devices can connect to the Platform Service and send and receive events and commands, but they cannot send device management requests or perform device management operations.

## Platform Service security

Last Updated: 2021-05-07

As a cloud-hosted service the IBM Watson™ IoT Platform service embeds security as an important aspect of its architecture.

The following document answers some common questions about how your organization's data is protected, focusing on specific areas:

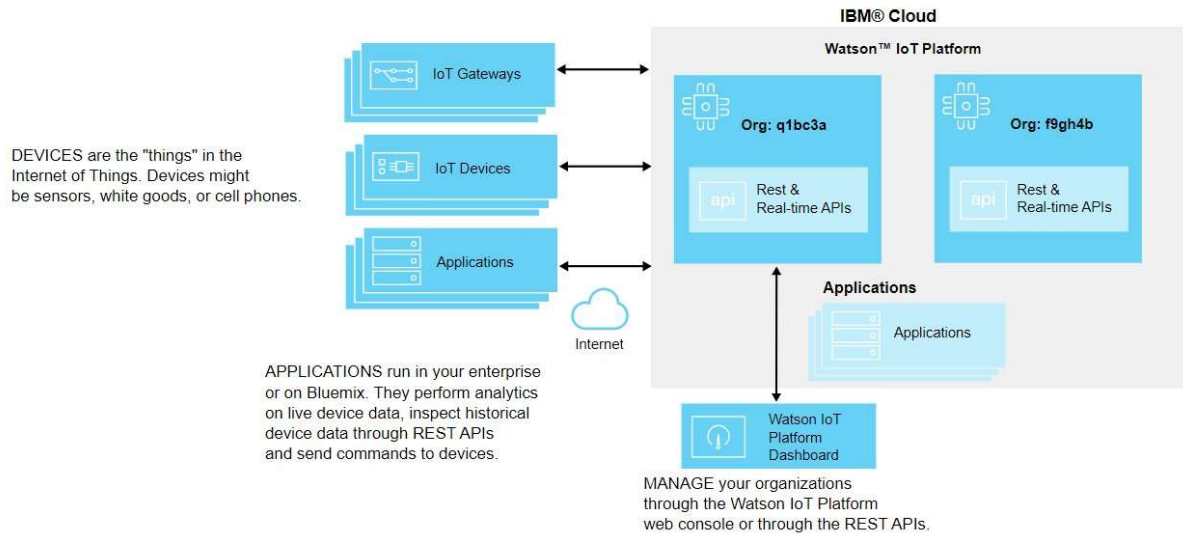
- Compliance: external standards, which set benchmarks for security.
- Authentication: assuring the identity of users, devices or applications that are attempting to access your organization's information.
- Authorization: assuring that users, devices, and applications have permission to access your organization's information.
- Encryption: assuring that data is only readable by authorized parties only and cannot be intercepted.

## Platform Service and IBM Cloud

Platform Service runs within IBM Cloud platform and so relies upon both IBM Cloud and IBM Cloud Infrastructure for access and connectivity. The reliance upon IBM Cloud and IBM Cloud Infrastructure makes IBM Cloud and IBM Cloud Infrastructure security and reliability important to users of Platform Service

# Platform Service Terminology

Watson IoT Platform ORGANIZATIONS are how you can group common devices and applications. Devices and applications in the same organization work easily together.



## How do we prevent IoT data leaking between organizations?

The topic space in which devices and applications operate is scoped within a single organization. When authenticated, the Platform Service transforms the topic structure by using an organization ID based on the client authentication, making it impossible for data from one organization to be accessed from another.

