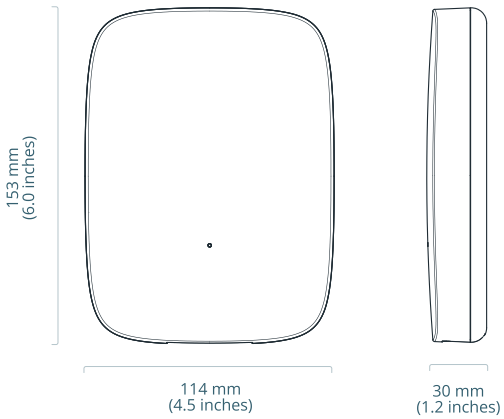
DISRUPTIVE
TECHNOLOGIES

Product Datasheet

Cloud Connector

Rev 1.3

Overview



Description

Cloud Connectors relay data from wireless sensors that communicate over the SecureDataShot™ wireless protocol to the cloud via cellular or ethernet connectivity. From the cloud, the data can be integrated into other services using REST APIs and webhooks or viewed directly in Studio (web application).

Features

- No setup or configuration
- Supports up to 10,000 sensors
- Automatic software updates
- Built-in SIM card with a cellular roaming agreement
- Automatically connects to cellular network

Specifications

Radio & Communication

Communication Protocol	SecureDataShot™
Radio Frequency	868 MHz / 915 MHz
Radio Range	See sensors for details

Cellular Connectivity (optional)

Technology	4G/LTE (CAT1 / CAT M1)
Roaming	Europe & North America
Sim Card	Internal eSIM

Power Supply

Plug Type	Barrel Jack
Voltage	5V DC
PoE Support	PoE Splitter

Mechanical Properties

Size	153x114x30 mm / 6x4.5x1.2 in
Weight	200 grams / 7 oz
IP Rating	IP20
Mounting Method	Screws

Product Name	Product Number	Region	Order Code
Cloud Connector EU - Cellular	102505	Europe	102572
Cloud Connector US - Cellular	102506	North America	102573
Cloud Connector EU - Ethernet Only	102673	Europe	102672
Cloud Connector US - Ethernet Only	102644	North America	102674

How it works

The Cloud Connector is a gateway that relays data from wireless sensors that communicate using the SecureDataShot™ protocol to a cloud service via cellular or ethernet connectivity. Simply plug in power and start collecting data from wireless sensors. The cellular version ships with an internal SIM card that allows it to automatically roam between cellular networks without any configuration required by the user.

Excellent wireless coverage

The Cloud Connector is designed to cover a large area within a building.

Sensor roaming

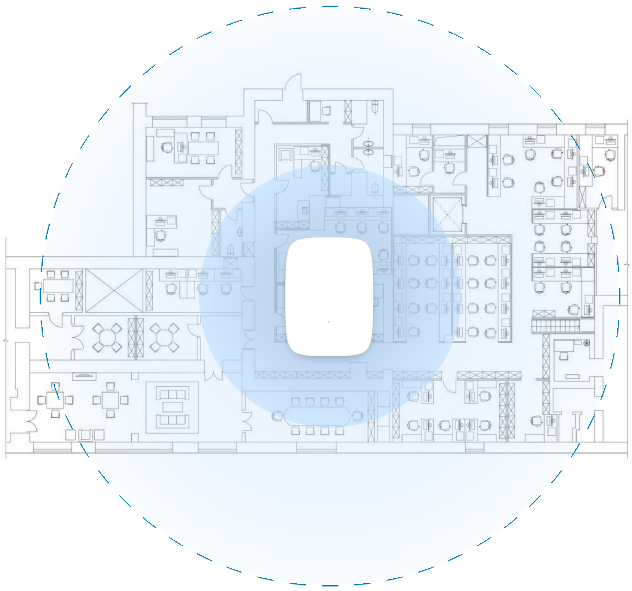
Wireless sensors can roam freely between Cloud Connectors.

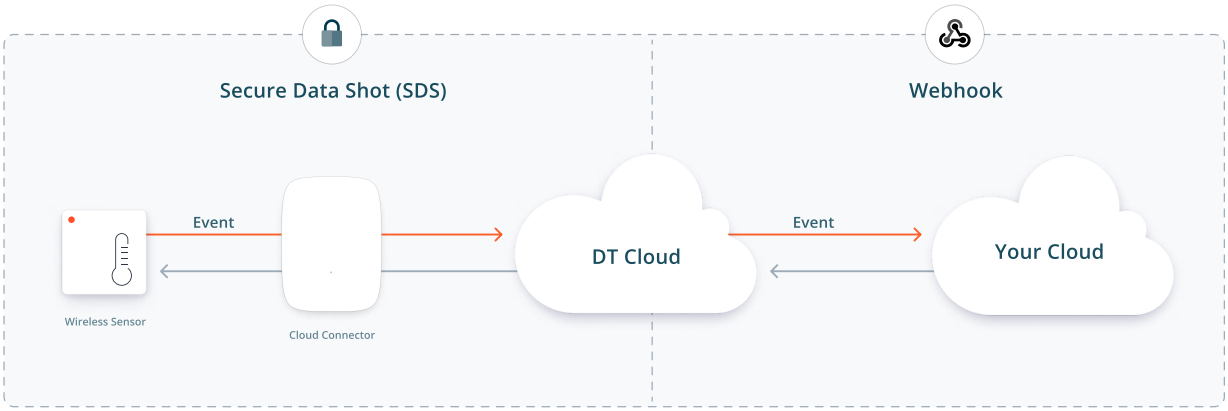
Supports up to 10,000 sensors

A single Cloud Connector can relay data from thousands of sensors at the same time.

4G/LTE Support

Cellular enabled Cloud Connectors automatically connect and roam between cellular networks.





Wireless Sensors

Wireless sensors instantly connect and send data to the cloud via SecureDataShot™

Cloud Connectors

Cloud Connectors automatically connect and relay data to the cloud service

Cloud Service

No servers, databases, or on-prem clients to manage - simply install sensors and integrate the data into your own service.

Wireless Sensor Communication

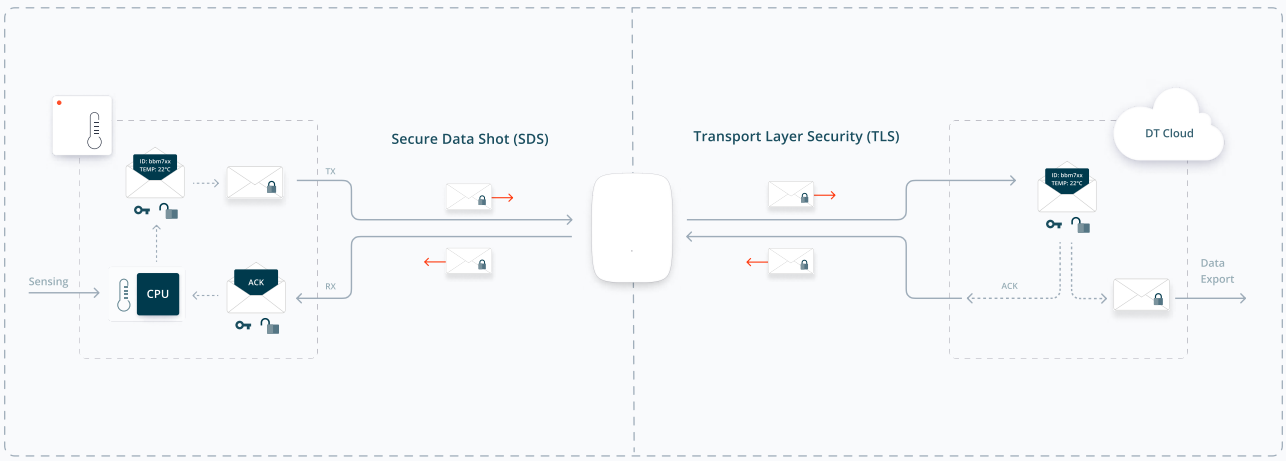
Sensors from Disruptive Technologies communicate using SecureDataShot™ on sub GHz ISM band, a wireless communication protocol specifically designed to make reliable wireless sensors that are easy to use while maintaining the highest security possible without compromising the user experience.

Unlike traditional wireless sensor systems, with SecureDataShot™, there is no concept of pairing or commissioning devices onto the network. The sensors automatically send data through any SecureDataShot™ enabled gateway and can securely roam between gateways. Secure roaming reduces installation time and increases reliability because there is no way for sensors to disconnect from a gateway or the network. In addition, it lets each gateway communicate with thousands of sensors simultaneously.

Secure by default with SecureDataShot™

SecureDataShot™ creates a secure communication channel between the sensor and the cloud instead of between the sensor and the gateway. This reduces the potential for a manipulator-in-the-middle attack by exploiting vulnerabilities in the security architecture of gateways. Cloud Connectors can forward data to and from sensors but cannot decrypt the sensor data.

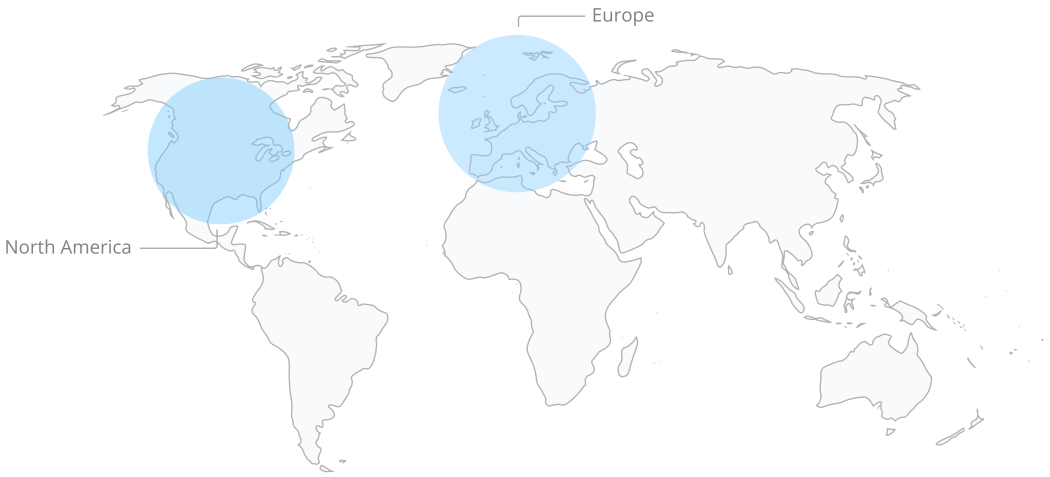
- During manufacturing, each sensor is assigned a unique 256 bit assymmetric encryption key, generated by a tamper-proof 140-2 Level 3 certified hardware security module.
- Cloud Connector includes a Secure Element (SE) for hardware Root of Trust.
- The public part of the asymmetric key is exchanged with Disruptive Technologies cloud via encrypted channels.
- In addition to the keys assigned during manufacturing, the sensor and cloud also hold a unique SecureDataShot™ session key.
- Sensor data is encrypted using symmetric AES-128 encryption/decryption in CCM-mode.
- Cloud Connectors are provisioned with Transport Layer Security (TLS) certificates to establish a secure connection between the Cloud Connector and the cloud.



Cellular Communication (optional)

Cellular-enabled Cloud Connectors ship with a pre-configured internal SIM card that enables them to relay data from sensors to the cloud using 4G/LTE cellular network technology. As soon as it is powered on, the Cloud Connector will automatically connect to a cellular network in the area. The connection status, signal strength and other relevant parameters can be viewed in DT Studio or through the APIs.

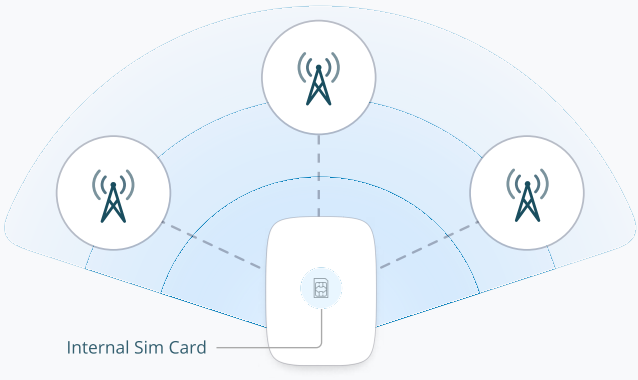
Currently, mobile networks in North America and Europe are supported.



Connect anywhere with eSIM and seamless roaming

Disruptive Technologies partners with the best Mobile Virtual Network Operators (MVNO) in the world to deliver seamless connectivity. Through MVNOs, the Cloud Connector has access to multiple mobile network operators and their wireless network infrastructure.

Once powered, it will search for and establish a connection with a cellular network in the area. This process typically takes a couple of minutes. After that, data will stream seamlessly to the Cloud without any setup or configuration.



Cloud Connector

Seamless roaming between mobile network operators

Technical Specification

Sensor Wireless Communication

Radio Protocol	SecureDataShot™	
Radio Frequency	**EU**: 868 MHz SRD band	**US**: 915 MHz ISM band
Transmit Power	< 100 mW	
Wireless Range	See sensor specifications for more detail.	

Cellular Communication

Communication Standard	**EU**: Cat 1 LTE FDD B1/3/7/8/20/28	**US**: Cat M1 LTE FDD B2/B4/B5/B12/B13/B25/B26/B66/B85
Transmit Power	**EU**: Power Class 3 (23dBm±2dB) for LTE FDD bands	**US**: Power Class 5 (21dBm±1.5dB) for LTE FDD bands

Operating & Storage Conditions

Operating Conditions	**Temperature**: 0 to 50°C (32 - 120°F) **Humidity**: 10 to 90% relative humidity (non condensing)
Storage Conditions	**Temperature**: 0 to 70°C (32 - 158°F) **Humidity**: 10 to 90% relative humidity (non condensing)

Power Supply & Consumption

Power Supply	5V DC @ 2A	
Plug Type	**Type**: Barrel - OD: 5.5mm ID: 2.1mm	**Polarity**: Positive polarity
Power Consumption	Average < 3W[1]	

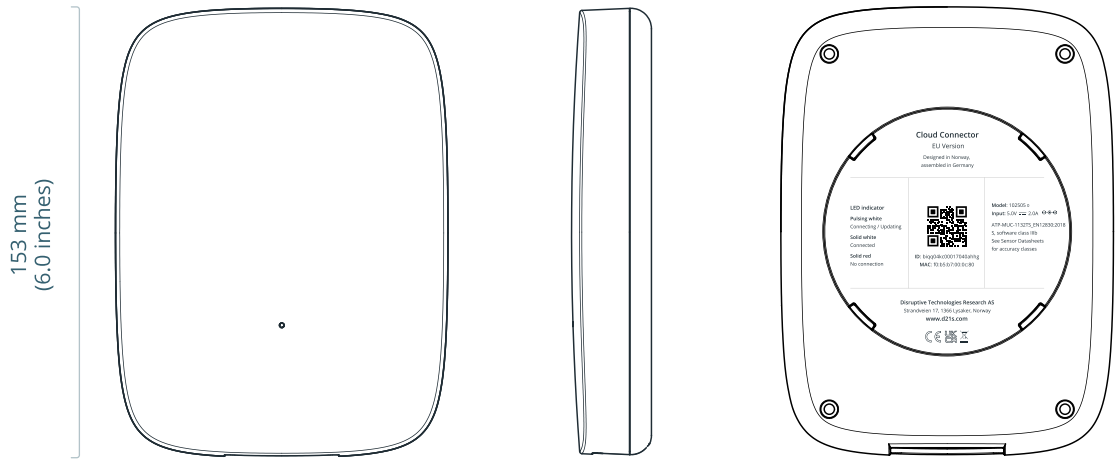
(1):The average power consumption of the Cloud Connector will vary depending on whether Ethernet or Cellular mode is used.

Certification & Compliance

	EU: CE, UKCA	**US/Canada**: FCC, ISED, UL Contains FCC ID: 2ATFX-102545 Contains FCC ID: ZMOMA510GL Contains IC: 25087-102545 Contains IC: 21374-MA510GL UL Certified, File No: E489020

Mechanical Properties

Size	153 x 114 x 30 mm | 6 x 4.5 x 1.2 inches
Weight	200 grams | 7 oz
Material	Polycarbonate (PC)
Ingress protection	IP20
Mounting method	Screws or adhesive (wall mount)



Regulatory Marking
(EU version)

Product Variants

EU Version	**Product number**: 102505	**Region**: Europe
EU Version (Ethernet only)	**Product number**: 102673	**Region**: Europe
US Version	**Product number**: 102506	**Region**: North America
US Version (Ethernet only)	**Product number**: 102644	**Region**: North America

Installation Guidelines

1 Connecting to power

Use the provided power supply to power the Cloud Connector.

2 Connecting to the Cloud

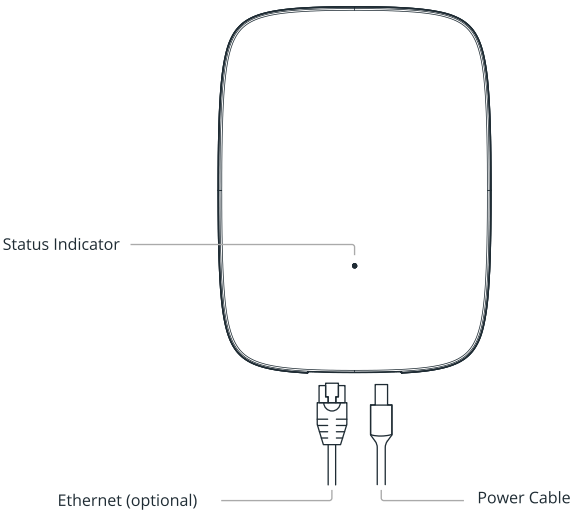
If the device has a cellular modem, it will automatically start connecting to the cloud service. If not, plug in an ethernet cable to establish a connection.

3 Observe the Status Indicator

Pulsing White
Connecting / updating, this can take up to a few minutes.

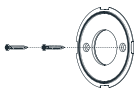
Solid White
Connected to the internet and fully operational.

Solid Red
Not connected, visit d21s.com/help for troubleshooting.



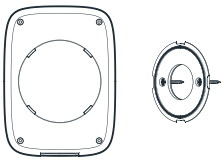
Installation Guidelines

Wall or Ceiling Installation

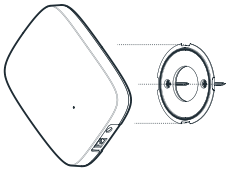


Secure the mounting bracket to the wall with screws.

If mounted below 2 meters (6.5 feet), the adhesive can be used alone.



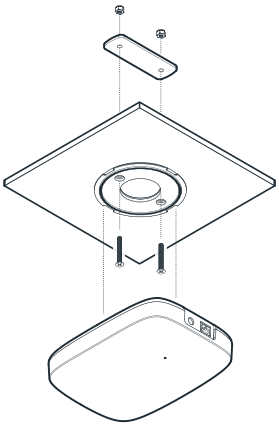
The Cloud Connector attaches to the bracket with a friction bayonet mount.



Align the slots and move the Cloud Connector onto the bracket.

Turn the Cloud Connector 45° degrees to secure it in place and connect the power cable.

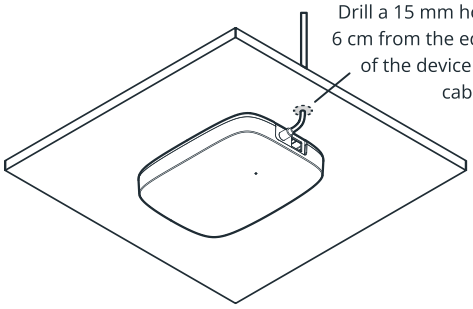
Drop Ceiling Installation



Remove the tile from the ceiling to perform the installation.

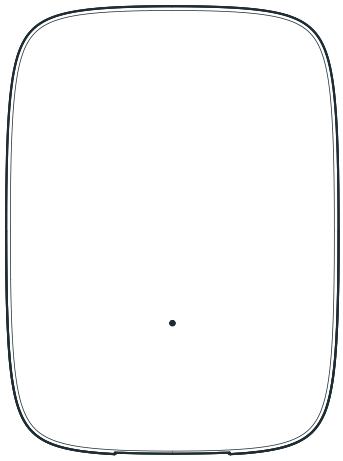
The mounting bracket is attached to the tile using the provided backing plate with two screws and nuts.

The Cloud Connector attaches to the bracket with a friction bayonet mount.

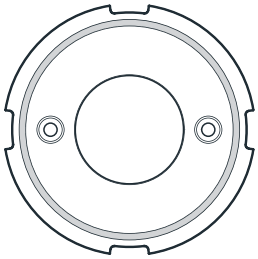


Drill a 15 mm hole, 6 cm from the edge of the device for cables.

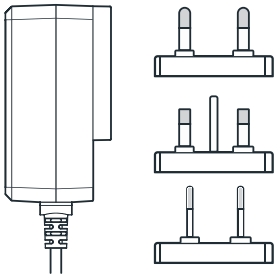
In the box



Cloud Connector



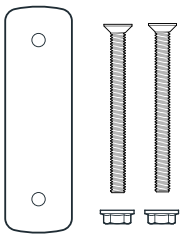
Mounting bracket with
adhesive backing



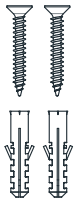
Power supply
+ regional plugs

Cabel length: 2.5 m / 8.2 feet

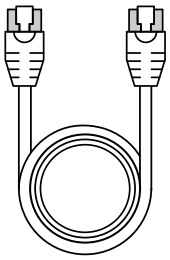
Safety & Use leaflet with
installation instructions



Drop ceiling bracket
+ screws and nuts



Wall screws
+ wall plugs



Ethernet cable

(Included with the Ethernet Only
version of the Cloud Connector)

Ordering Information

Europe

Product Name	Order Code	Region	Quantity
Cloud Connector EU (2nd Gen) - Cellular	102572	Europe	1
Cloud Connector EU (2nd Gen) - Ethernet Only	102672	Europe	1

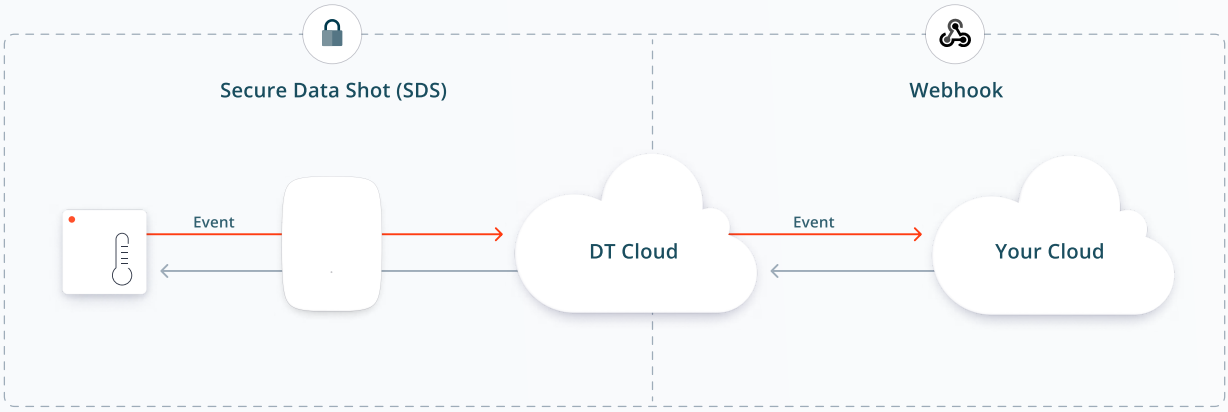
North America

Product Name	Order Code	Region	Quantity
Cloud Connector US (2nd Gen) - Cellular	102573	North America	1
Cloud Connector US (2nd Gen) - Ethernet Only	102674	North America	1

Subscriptions

Product Name	Order Code	Region	Quantity
Cloud Connector - 1 Year Cellular Service	800025	Global	1
Cloud Connector - 3 Year Cellular Service	800026	Global	1
Cloud Connector - 5 Year Cellular Service	800027	Global	1

Solution Overview



Wireless Sensors

Wireless sensors instantly connect and send data to the cloud via SecureDataShot™

Cloud Connectors

Cloud Connectors automatically connect and relay data to the cloud service

Cloud Service

No servers, databases, or on-prem clients to manage - simply just install sensors and integrate the data into your own service.

Why use a cloud based sensor solution?

Zero-touch Connectivity

No pairing needed. Sensors automatically communicate through all Cloud Connectors which results in a quick and easy installation process.

24/7 Monitoring

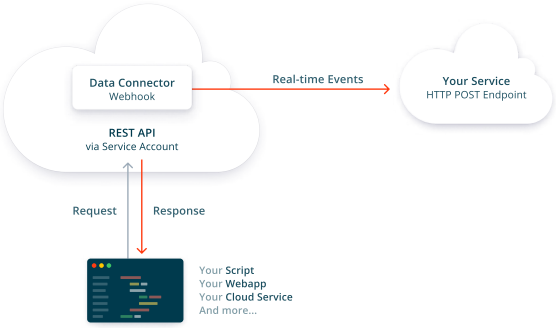
All Disruptive system components are instrumented and monitored 24 hours per day, 7 days per week. Anomalies trigger alarms and notifies our response team.

Easy to Scale

Cloud Connectors support thousands of sensors and the cloud service automatically scales for users with increasing number of sensors.

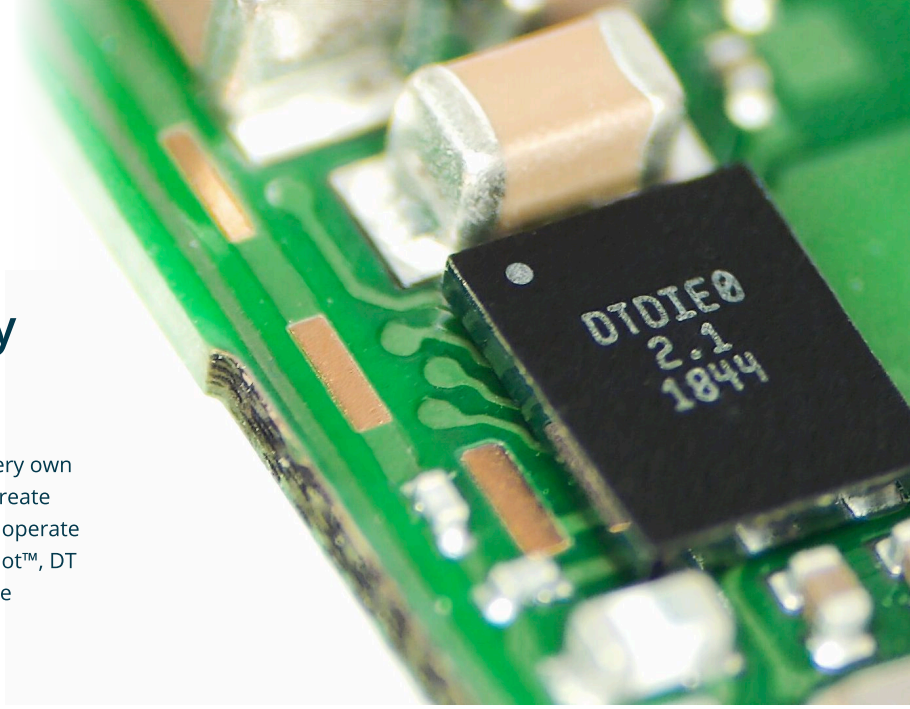
Centralized Management

No servers, databases, or on-prem clients to manage. A modern cloud platform enables secure access on any device from anywhere in the world.



REST API & Webhooks

Easily integrate the sensor data into your own, or a third-party service, using our REST API or webhooks.



Take advantage of industry leading battery life with DT Silicon

DT Wireless Sensors are powered by DT Silicon - our very own proprietary chip technology that makes it possible to create sensors that use an order of magnitude less energy to operate than other wireless sensors. Paired with SecureDataShot™, DT sensors have superior battery life while maintaining the highest level of security and ease-of-use.

- Enables tiny sensors with long battery life
- Tailor made for the SecureDataShot™ protocol

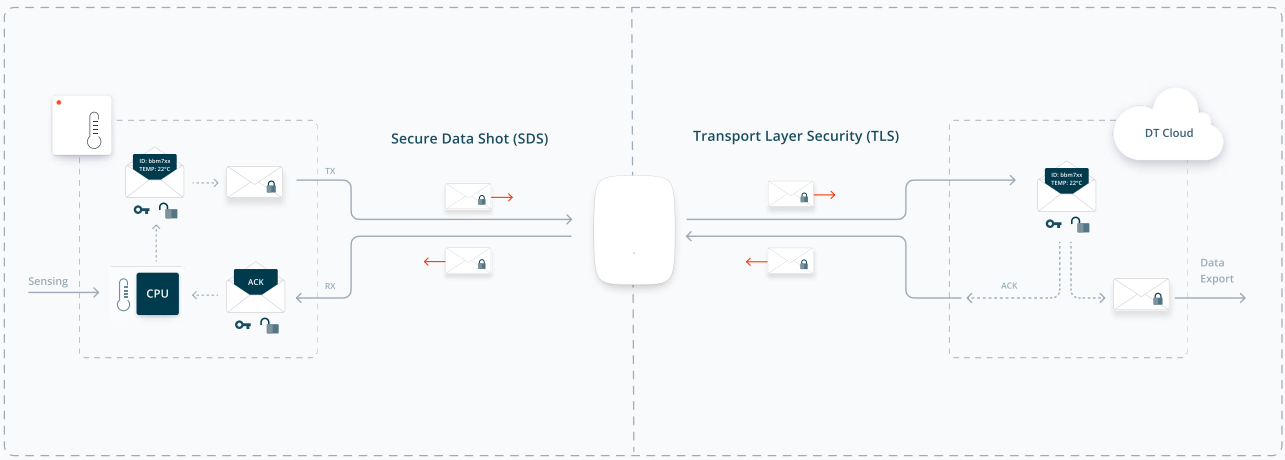
Secure by default with SecureDataShot™

SecureDataShot™ creates a secure communication channel between the sensor and the cloud instead of between the sensor and the gateway. This reduces the potential for a manipulator-in-the-middle attack by exploiting vulnerabilities in the security architecture of gateways.

- Cloud Connectors can forward data to and from sensors but cannot decrypt the sensor data.
- During manufacturing, each sensor is assigned a unique **256 bit assymmetric encryption key**, generated by a tamper-proof 140-2 Level 3 certified hardware security module.
- The public part of the asymmetric key is exchanged with Disruptive Technologies cloud via encrypted channels.

The purpose of the keys is to allow sensors to communicate securely with the cloud. In addition to the keys assigned during manufacturing, the sensor and cloud also hold a unique SecureDataShot™ session key.

- Sensor data is encrypted using symmetric AES-128 encryption/decryption in CCM-mode.
- Disruptive Cloud Connectors are provisioned with Transport Layer Security (TLS) certificates to establish a secure connection between the Cloud Connector and the cloud.



Fleetmanagement & Data Insights with Studio

Device Overview

Sort devices into projects for easy access and get an overview over data, health status and radio coverage

Flexible Dashboards

Get a quick overview of sensors and compare data with easy-to-use drag-and-drop dashboard cards

Access Control

Create role-based user accounts for people and services that need access to sensor data

Notifications

Set up simple rules for sensors and receive automatic sensor triggered notifications

Data Forwarding & API Integrations made simple

Data Connectors / Webhooks

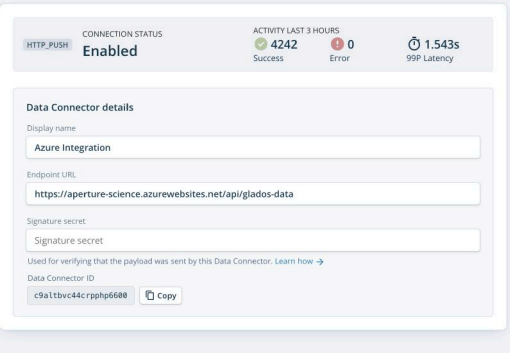
Easily configure secure webhooks to forward the data to your own service.

Service Accounts

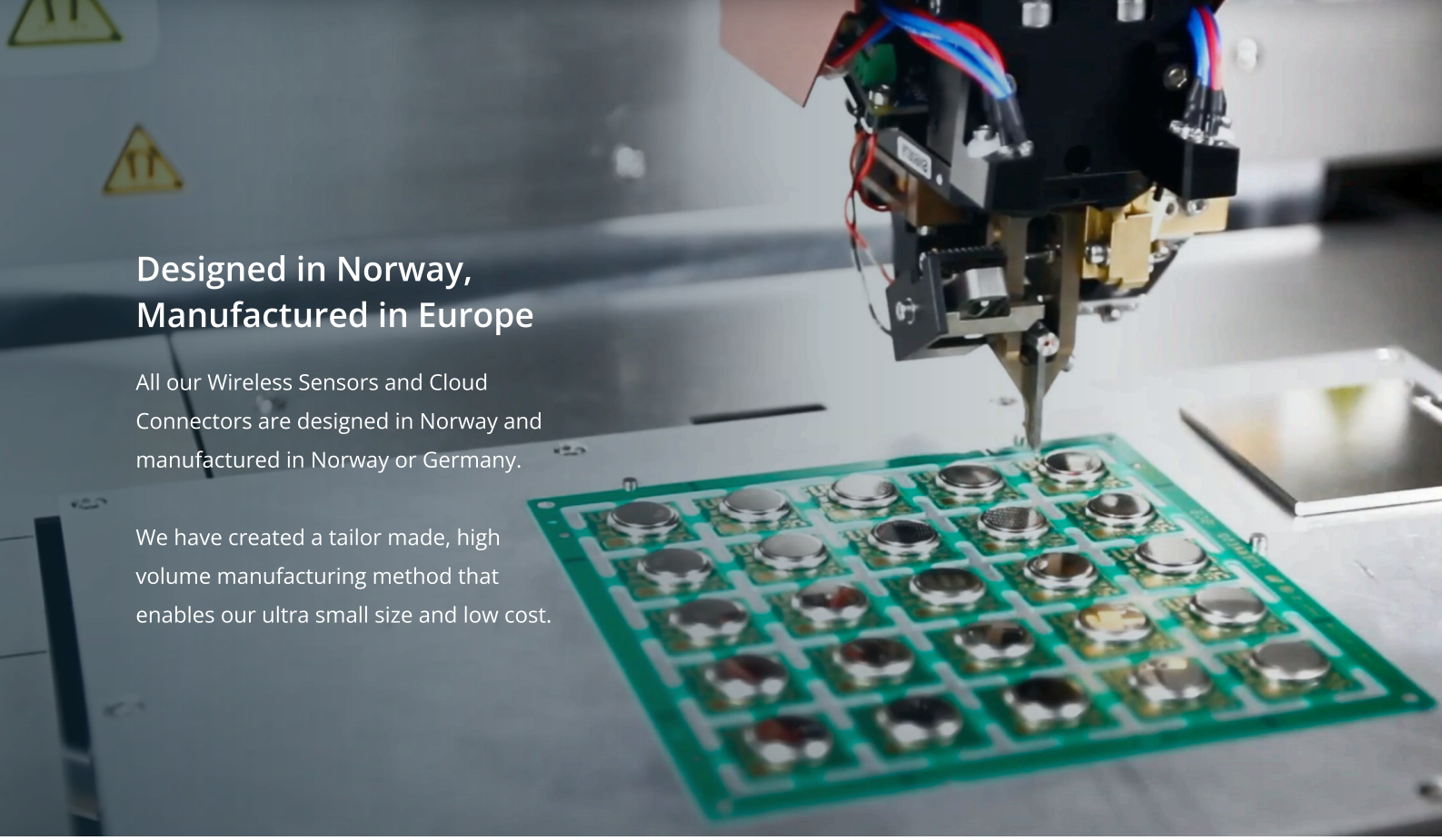
Create and manage role-based service accounts to let your own cloud service authenticate with the REST API.

Sensor Emulators

Create emulated sensors to test your API integrations without access to physical hardware.



Azure aws Google Cloud IBM Cloud



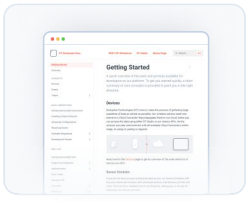
Designed in Norway, Manufactured in Europe

All our Wireless Sensors and Cloud Connectors are designed in Norway and manufactured in Norway or Germany.

We have created a tailor made, high volume manufacturing method that enables our ultra small size and low cost.

Ready to learn more?

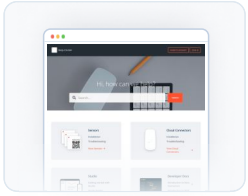
To learn more about DT's wireless sensor solution and how you can benefit from it, visit our website or schedule a demo with a member of our sales team at **https://www.disruptive-technologies.com/contact-us** or contact us directly via email at **sales@disruptive-technologies.com**



Developer Docs

Browse our developer documentation to find everything you need to know about the system, tutorials, integration guides, and API references.

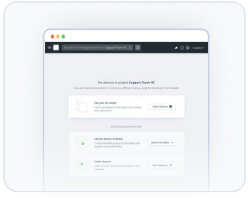
Learn more



Support Center

Browse our support center to find details about our products, technology, installation guidelines, and answers to frequently asked questions.

Learn more



Sign Up for Studio

Create a Studio account and test our software and API integrations using emulated sensor events.

Learn more

Revision History

Revision 1.0	**Change**: Initial release **Date**: November 1st, 2022
Revision 1.1	**Change**: Added UL Certification **Date**: January 19th, 2023
Revision 1.2	**Change**: Added ingress protection **Date**: May 10th, 2023
Revision 1.3	**Change**: Added overview and updated document design **Date**: February 9th, 2024