SENDES DAU

User manual

SN



english

Contents

0. Technical specifications 4

1. Product introduction 5

1.1 Device layout 5

1.2 Device design — version without mast 6

2. Start -up 6

2.1 Connected to operation mode 6

2.2 Device power supply 7

2.3 Considerations 7

3. Important notes 7

3.1 Safety information 7

4. Network requirements for connectivity with the sendes systems 9

5. Warranty 14

6. Statement on the Use of SENDES DAU Technology 15

Package content

Content	Units
1. SENDES DAU	1
2. Omnidirectional antennas	4
3. ADSB antenna	1
4. Mast (optional)	1
5. Antenna container	1
6. LMR400 cables	4
7. AC power cable	1
8. Keys	2
9. Rapid-deployment tripod (optional)	1
10. Mounting brackets (optional)	1

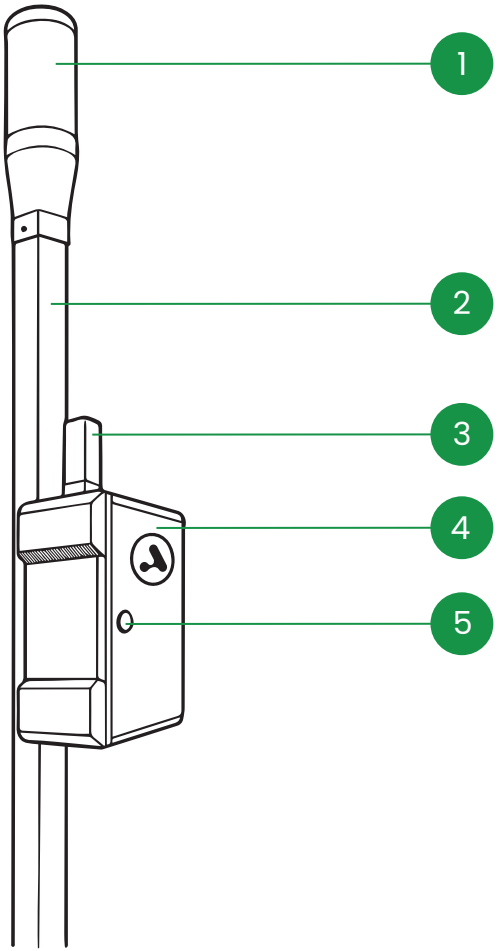
***NOTE**: If any of the above items is damaged or missing, please contact your retailer.*

Technical specifications

Product	Stationary system for drone detection, identification, and tracking
Technology	Real-time radio-frequency decoding and communication decryption
Dimensions	Cabinet: 400 × 208 × 600 mm (L × W × H) Antenna: 200 × 400 mm (D × H) LMR400 cables: Up to 4 m in length
Weight	Cabinet: 18 kg Antenna: 4 kg Cabling: 100 g/m
Installation	Stationary on mast, rooftop, tower, or rapid-deployment tripod
Detection modules	**Standard version:** DJI at 2.4 and 5.8 GHz (Lightbridge and OcuSync protocols) and Remote ID at 2.4 GHz. **Full version:** DJI at 2.4 and 5.8 GHz (Lightbridge and OcuSync protocols), Remote ID at 2.4 GHz, WiFi at 2.4 GHz, ADS-B at 1,090 MHz, and RF at 900, 1,400, 2,400, and 5,800 MHz **Operating range** **DJI:** Up to 10 km / **Remote ID:** Up to 4 km / **WiFi:** Up to 800 m / **ADS-B:** Up to several tens of km / **RF:** Up to 1,000 m *(under optimal conditions)*
Operating range	DJI: Up to 10 km / Remote ID: Up to 4 km WiFi: Up to 800 m / ADS-B: Up to several tens of km RF: Up to 1,000 m *(under optimal conditions)*
Antenna	Omnidirectional
Power supply	220-240 VAC o 12 VDC (requires inverter)
Power consumption	70 W (max.)
Connectivity	RJ45 Ethernet (fixed IP) and/or 3G / 4G LTE
Protection	IP55
Operating temperature	-20°C to +55°C
Operation	SENDES Ecosystem

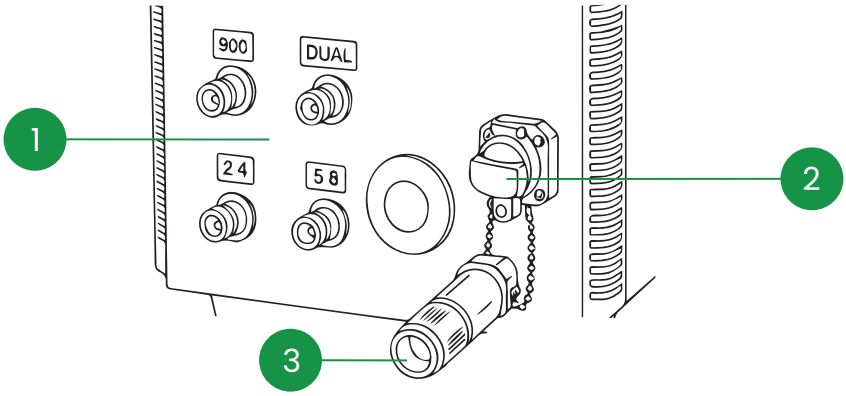
1. Product introduction

1.1 Device layout



1. Omnidirectional antenna container 2. Mast
3. ADS-B antenna 4. SENDES DAU 5. Lock

1.2 Device design — version without mast



1. Omnidirectional antenna container 2. Power connector
3. RJ45 Ethernet port for WAN/Internet

2. Start -up

2.1 Connected to operation mode

SENDES-DAU will only operate with active Internet connection. This can be done via 4G connectivity in the rapid-deployment versions or through a wired Ethernet connection.

To install a SIM card in the SENDES-DAU (only in rapid-deployment versions):

- Before inserting the SIM card into the slot, make sure the SENDES-DAU is powered off.
- Make sure the SIM card has the PIN code disabled.
- Remove the ruggedized slot cover and insert the SIM card in the correct orientation.
- Replace the ruggedized cover.
- Power on the SENDES DAU

To provide Internet via Ethernet cable:

- Connect the Ethernet cable to the WAN/Internet Ethernet port of the SENDES-DAU and provide Internet access through an external router.
- The SENDES-DAU will obtain an IP address using the router's DHCP.

Check the network requirements for more details about the connectivity options and configurations.

2.2 Device power supply

You should only use the supplied power cables to power the SENDES-DAU. Using third-party cables or power sources will void the warranty.

2.3 Considerations
(Rapid-Deployment Version)

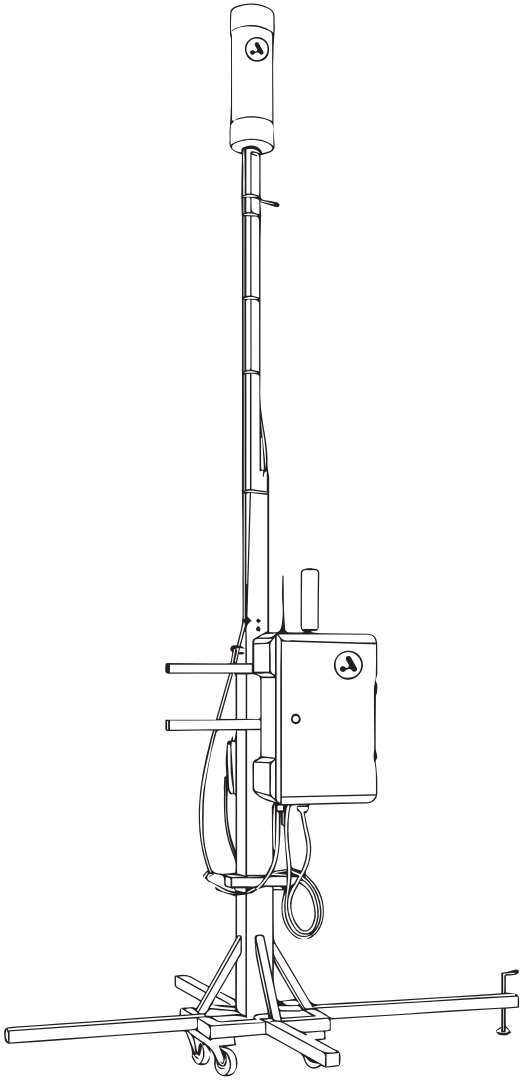
1. For the GNSS positioning system to take effect, you should wait 2 to 3 minutes after turning on the device and ensure you are in an environment with GNSS signal, such as outdoors.
2. Keep in mind that using the SENDES-DAU indoors may interfere with GNSS positioning and the device's 4G connection.

3. Important notes

3.1 Safety information

- To avoid the risk of electric shock, disconnect the power cable from outlets and sockets before relocating the system.
- If the power supply is damaged, do not attempt to repair it yourself. Contact a qualified service technician or your distributor.
- Before turning on and connecting the SENDES-DAU to the power source, carefully read all manuals included in the package.
- Before using the product, ensure that all cables are correctly connected and that the power cables are not damaged. If any damage is detected, contact your distributor immediately.
- Place the product on a stable surface.
- Avoid dust, moisture, extreme temperatures, and prolonged exposure to sunlight.
- Only use the supplied power cables to power the SENDES-DAU. Using third-party cables or power sources will void the warranty.
- Do not attempt to disassemble the equipment; this could cause damage or electric shock and will void the warranty.
- Avoid placing the equipment near heat sources, radiators, or devices that generate strong magnetic fields.

- Ensure that the power outlet and electrical installation meet the voltage and current requirements of the equipment.
- Keep ventilation grilles free of dust and objects that could block airflow.
- Do not pull on the power cable to disconnect the equipment; always hold the plug.
- In case of smoke, unusual odors, or strange noises, immediately disconnect the equipment and contact technical support.



Need help?
sos@asdt.eu
support.asdt.eu

4. Network requirements for connectivity with the sendes systems *(Update: 25/11/2025)*

Introduction

ASDT equipment, both detection and neutralization, can operate through a wired network connection or using 4G LTE technology.

From the ASDT development department, it is recommended to connect the SENDES systems through a wired network, preferably a dedicated fiber exclusive to the equipment or installation. This configuration minimizes connectivity fluctuations and ensures that the equipment has an independent network, separate from the client's network, to which it connects using a static IP or via DHCP, avoiding complex configurations.

In stationary equipment, both connection methods can be combined to ensure uninterrupted intercommunication. In this case, the 4G LTE network acts as a backup in the event of failures in the main wired network.

In the case of wired connections, SENDES equipment can be configured to operate behind the client's firewall or proxy, ensuring compliance with local network security policies. To achieve this, the devices' network parameters, such as IP addresses, ports, and required authentication, can be adjusted, allowing secure and customized integration within the client's infrastructure.

Firewall Configuration

When it is not possible to have a dedicated fiber for the installation equipment and the existing client network must be used, it is recommended that this network have a **firewall** to ensure infrastructure security.

A firewall is a security system designed to act as a barrier between an internal network and external networks, such as the Internet. Its main function is to control and filter incoming and outgoing data traffic according to predefined rules, protecting systems against unauthorized access, cyberattacks, and other threats.

By allowing only the necessary and secure connections, the firewall helps maintain the integrity of the network.
In the case of SENDES systems, the client's firewall is essential to ensure secure communication between the equipment and ASDT servers, complying with the specific configurations required for proper operation.
To achieve this, it is essential to configure a set of specific parameters in the client network's firewall or in any other device acting as an intermediary between the SENDES systems and the ASDT servers. These configurations apply to both detection systems (SENDES DAU and SENDESCOPE) and neutralization systems (SENDES SJ and SENDES SJ-BOX).

Required Configuration

1. Network settings:

- Assign a **static IP** for each system, including the subnet mask, gateway, and the DNS servers required for domain resolution.

2. Outgoing connections:

- Allow outgoing connections to the subdomains of *.**asdt.eu** and to other IPs on the following ports, which are detailed at the end of the document:
  - **80 (HTTP), 443 (HTTPS), 4000 y 5883**

3. Remote access:

- Enable port **22 (SSH)** and **21 (FTP)** for outgoing connections.

4. Time synchronization:

- Configure an **NTP** server for precise synchronization of the device's clock.

5. Connectivity tests:

- Allow the use of the **PING** command to the gateway, the DNS servers provided by the client, and the subdomains of .asdt.eu, as well as to the various anti-drone systems in the installation.

6. Visualization systems:

- Additionally, for the Command and Control (C2) equipment, access must be allowed to the domains .**openstreetmap.org, mapbox.com,** and **unpkg.com**, specifically for the visualization systems.

Proxy Configuration

A specific case of security systems in the client's network, similar to a firewall, is the use of a proxy. A **proxy** is an intermediary server that acts as a bridge between network devices and external services, managing and filtering connection requests, which allows controlling access and improving network security and performance.
Although ASDT considers that a firewall in the network is sufficient to ensure the security and proper operation of the SENDES systems, there are client infrastructures that require the use of a proxy. In these cases, it is possible to configure the proxy on the SENDES devices, although with some limitations.
The implementation of a proxy may be necessary to comply with the client's network policies, but it is important to note that this connection method is not preferred due to the restrictions it may entail.

Required Configuration

1. Network settings:

- Assign a **static IP** for each system, including the subnet mask, gateway, and the DNS servers required for domain resolution.

2. Outgoing connections:

- Allow outgoing connections to the subdomains of **.asdt.eu** and to other IPs on the following ports, which are detailed at the end of the document:
  - **80 (HTTP), 443 (HTTPS), 4000 and 5883**

3. Time synchronization:

- Configure an **NTP** server for precise synchronization of the device's clock.

4. Connectivity tests:

- Allow the use of the **PING** command to the gateway, the DNS servers provided by the client, and the subdomains of .asdt.eu, as well as to the various anti-drone systems in the installation.

5. Remote access:

- Enable port **22 (SSH)** and **21 (FTP)** for outgoing connections.
- If it is not possible to enable remote connection via SSH, remote access for ASDT technical support must be ensured through a tool provided by the client's infrastructure, such as a VPN.

6. Visualization systems:

- Additionally, for the Command and Control (C2) equipment, access must be allowed to the domains **.openstreetmap.org, mapbox.com,** and **unpkg.com**, specifically for the visualization systems.

7. Proxy settings:

- Provide the **proxy IP and port** to manage HTTP and HTTPS connections.
- Provide **authentication credentials** if the proxy requires them.

Connectivity via 4G LTE

SENDES detection and neutralization equipment can operate via 4G LTE connection, providing a flexible and reliable connectivity option. For operation over 4G LTE, it is necessary to use a SIM card without a PIN, allowing automatic and continuous connection without manual intervention.
The 4G LTE option can be used in two ways:

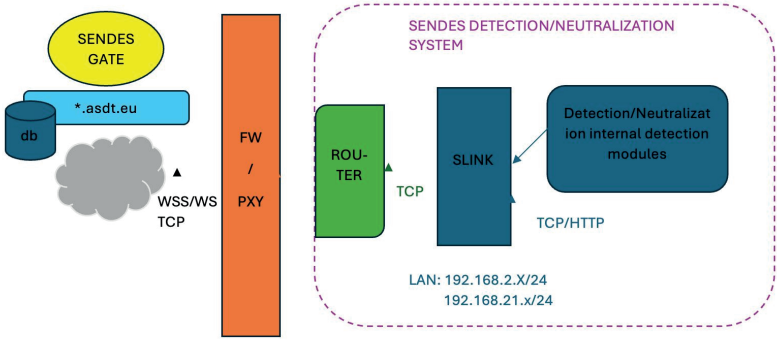
1. **Primary connection:** This option is ideal for portable equipment or systems whose connectivity depends on 4G, as it allows operation in locations where a wired network is not available.
2. **Wired network backup:** If a wired network is used as the primary connection, 4G can be configured as a backup option, ensuring service continuity in the event of a wired network failure or interruption.

In this way, 4G LTE provides flexibility and reliability, adapting to different connectivity needs depending on the environment and installation requirements.

Important consideration: When neutralization is activated, the connectivity of detection or neutralization equipment in the area operating on 4G LTE may be temporarily lost, depending on the frequency that has been activated. For more information, please contact the ASDT technical department.

Architecture diagram

The solution architecture is represented in the following diagram, which details the connections between the different modules that make up the detection system, as well as the interactions between the system and the external environment.



Subdomain Details

The following table details the different ASDT subdomains. It is preferable to accept the general subdomains of *.asdt.eu, *asdt.io in the firewall.

NAME	DNS	ASSOCIATED IP	PORTS	OUTGOING SSH ports 22 y 21
SENDES Gate	sendesgate.asdt.eu	185.196.43.15	443, 80	NO
	sendesgate.asdt.io	*	443, 80	NO
Security	security.asdt.eu	185.196.43.11	443, 80	NO
Manager	manager.asdt.eu	38.252.226.201	443, 80, 4000	YES
	manager.asdt.io	*	443, 80, 4000	YES
Backup	xmanager.asdt.eu	51.83.205.137	443, 80, 4000	YES
	devserver.asdt.eu	51.83.198.230	80	NO
		13.37.222.104, 8.211.58.246	443, 80, 5883	NO
	gitlab.asdt.eu	51.83.158.204	443, 80	NO
		185.196.43.16	443, 80	NO

It is preferable to allow the subdomains specified above in firewall, proxy, etc., rules using the DNS domain name rather than the associated IP, if available, since the latter may change on ASDT's side. If allowing by domain is not possible, it must be explicitly indicated to the technical department.

5. Warranty

The warranty for the systems supplied by ASDT Corporation S.L.U. shall be valid for a period of twelve (12) months from the date of delivery of the system, regardless of the actual installation date. In the case of portable or handheld systems, the batteries, being considered consumable items, are covered by a specific warranty period of six (6) months.

The warranty covers the main components of the system, including electronic cabinets, processing systems such as computers and control boards, communication systems including routers and switches, frequency amplifiers, decoding and decryption modules, power supplies, chargers, connectors and cabling, signal amplification and filtering systems, as well as the omnidirectional and/or directional antennas supplied by ASDT.

During the warranty period, ASDT guarantees the availability of the necessary parts required for the repair of the affected equipment. Once this period has expired, the availability of spare parts identical to the original ones cannot be guaranteed; however, where necessary, components of equal or superior quality will be used, ensuring at all times the preservation of the system's functionality.

The warranty shall be automatically void in the event of improper use of the system or use other than that specified by ASDT, as well as in cases of modifications, opening, or repairs carried out by unauthorized personnel. The warranty does not cover external damage resulting from accidents, negligence, extreme weather conditions, or acts of vandalism; damage occurring during transport not managed by ASDT that has not been duly reported; installations not carried out by authorized technicians; or the use of components or cabling not supplied or expressly authorized by ASDT.

The warranty claim process shall be initiated by reporting the incident via email to support@asdt.eu, and it is recommended to simultaneously inform the ASDT-designated contact person. Upon receipt of the notification, an initial remote diagnosis will be carried out and, where applicable, the equipment may be requested to be sent to the factory for evaluation. ASDT will perform a technical assessment of the defect to determine whether it is covered under warranty. If the defect is covered, the equipment will be repaired or replaced in accordance with the terms of this warranty. If the incident is not covered, a corresponding technical report will be issued, together with a detailed quotation and an estimated timeframe for the intervention.

6. Statement on the Use of SENDES DAU Technology

Dear Customer,

We hereby state that SENDES DAU, a technology developed by ASDT Corporation SLU, is designed and intended primarily for civil applications. This technology aims to address and mitigate potential threats related to the detection, analysis, and management of drone activities, contributing to the protection of critical facilities and ensuring the security of civil assets and infrastructures.

ASDT systems have been specifically designed and manufactured to identify and neutralize threats posed by civil and commercial drones, in order to minimize the risk of potential incidents caused by negligence or hostile acts. ASDT shall not be held liable for failure to detect or neutralize devices operating in airspaces affected by non-commercial, military, launched, catapulted, or falling devices.

At ASDT, our commitment to the ethical and responsible use of technology is paramount. We strive to develop and promote solutions that enhance social well-being and strengthen the protection of critical infrastructure. SENDES DAU is specifically tailored to meet the requirements of civil applications, including airspace monitoring, detection of unauthorized drone incursions, support for surveillance operations, law enforcement activities, and emergency response scenarios.

Although SENDES DAU is not explicitly designed for military use, we acknowledge that certain customers may consider its application within advanced security contexts. In such cases, it is essential to emphasize that any such use must strictly comply with international laws, applicable regulations, and ethical guidelines governing the deployment of this type of technology.

ASDT maintains a strong commitment to transparency and full compliance with all applicable legal frameworks. Furthermore, ASDT collaborates exclusively with responsible partners and clients to ensure that the deployment of SENDES DAU technology adheres to ethical standards and international requirements.

Should you have any questions or require further information, please do not hesitate to contact us.



español

Contenido

0. Especificaciones técnicas 16
1. Introducción al producto 17
1.1 Diseño del dispositivo 17
1.2 Diseño dispositivo versión sin mástil 18
2. Inicio del dispositivo 18
2.1 Conectado a modo operaciones 18
2.2 Alimentación dispositivo 19
2.3 Consideraciones 19
3. Notas importantes 19
3.1 Información de seguridad 19
4. Requisitos de red para la conectividad con los sistemas sendes 21
5. Garantía 26
6. Declaración sobre el uso de la tecnología SENDES DAU 27

Contenido del paquete

Contenido	Unidades
1. SENDES DAU	1
2. Antenas omnidireccionales	4
3. Antena ADSB	1
4. Mástil (opcional)	1
5. Contenedor Antenas	1
6. Cables LMR400	4
7. Cable de alimentación AC	1
8. Llaves	2
9. Trípode de rápido despliegue (opcional)	1
10. Soportes de montaje (opcionales)	1

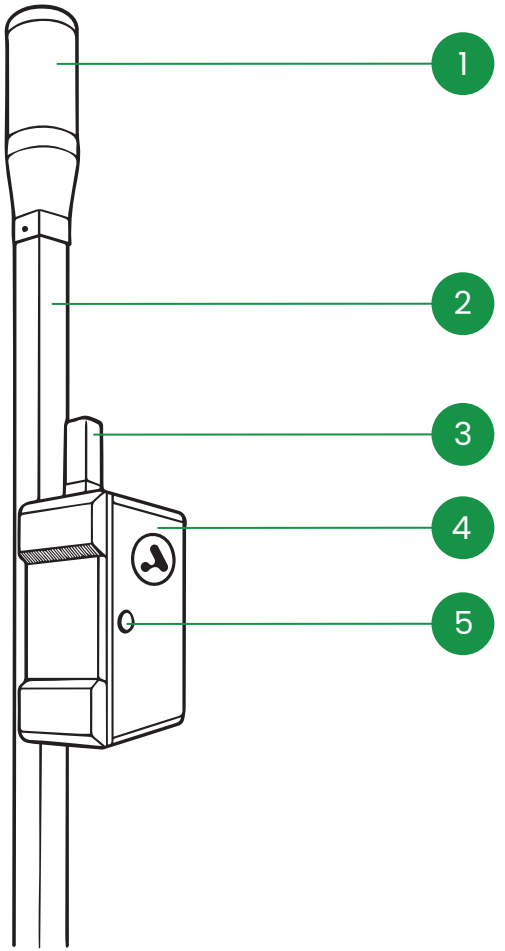
NOTA: Si alguno de los elementos está dañado o falta, comuníquese con su distribuidor.

Especificaciones técnicas

Producto	Sistema estacionario de detección, identificación y seguimiento de drones
Tecnología	Decodificación descifrado en tiempo real de radiofrecuencias
Dimensiones	Armario: 400 x 208 x 600 mm (L x W x H) Antena: 200 x 400 mm (D x H) Cables LMR400: Hasta 4 m de longitud
Peso (aprox.)	Armario: 18 kg Antena: 4 kg Cableado: 100 g/m
Instalación	Estacionaria en mástil, azotea, torre o en trípode de rápido despliegue
Módulos de detección	**Versión estándar :** - DJI en 2.4 y 5.8 GHz (protocolos Lightbridge y OcuSync), y Remote ID en 2.4 GHz **Versión full:** - DJI en 2.4 y 5.8 GHz (protocolos Lightbridge y OcuSync), Remote ID en 2.4 GHz, WiFi en 2.4 GHz, ADS-B en 1.090 MHz y RF en 900, 1.400, 2.400 y 5.800 MHz
Distancia operativa	**DJI:** Hasta 10 km **Remote ID:** Hasta 4 km **WiFi:** Hasta 800 m **ADS-B:** Hasta varias decenas de km **RF:** Hasta 1.000 m *(en condiciones óptimas)*
Antena	Omnidirectional
Alimentación	220-240 VAC o 12 VDC (requiere inversor)
Potencia de consumo	70 W (máx.)
Conectividad	Ethernet RJ45 (IP fija) y/o 3G / 4G LTE
Protección	IP55
Temperatura operativa	-20ºC to +55ºC
Operación	SENDES Ecosystem

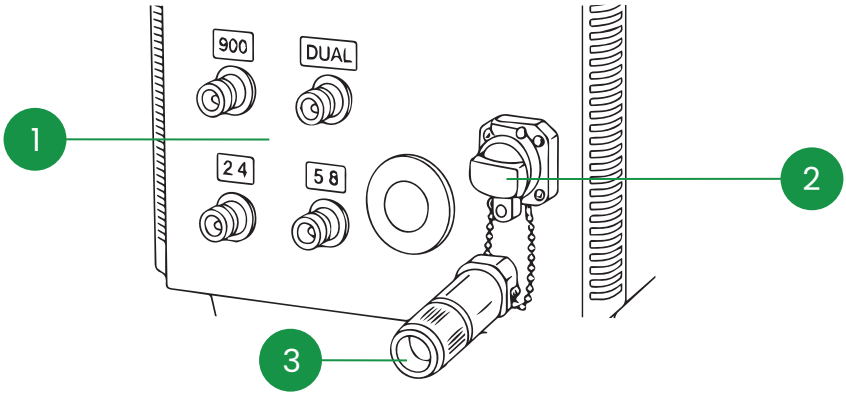
1. Introducción al producto

1.1 Diseño del dispositivo



1. Contenedor de antenas omnidireccionales 2. Mástil
3. Antena ADSB 4. SENDES DAU 5. Cerradura

1.2 Diseño dispositivo versión sin mástil



1. Contenedor de antenas omnidireccionales
2. Puerto Ethernet RJ45 para WAN/Internet 3. Conector Alimentación

2. Inicio del dispositivo

2.1 Conectado a modo operaciones

Dependiendo de sus necesidades, el SENDES-DAU puede operar con o sin una conexión a Internet activa. Si desea utilizarlo con acceso a la red, puede hacerlo mediante conectividad 4G en las versiones de rápido despliegue o a través de una conexión por cable Ethernet.

Para instalar una tarjeta SIM al SENDES-DAU(Solo en versiones de rápido despliegue) :

- Antes de instalar la tarjeta SIM en la ranura, asegúrese de que el SENDES-DAU está apagado.
- Asegúrese de que la tarjeta SIM tiene el código PIN deshabilitado.
- Retire la cubierta rugerizada de la ranura y coloque la tarjeta SIM en la orientación correcta.
- Coloque otra vez la cubierta rugerizada.

Para dar internet via cable ethernet:

- Conecte el cable ethernet al puerto ethernet WAN/internet del SENDES-DAU; y proporcione acceso a internet con un router externo.
- El SENDES-DAU obtendrá la dirección IP utilizando el DHCP del router.

2.2 Alimentación dispositivo

Usted debería usar únicamente los cables de alimentación suministrados para alimentar el SENDES-DAU. El uso de cables o fuentes de alimentación de terceros anulará la garantía.

2.3 Consideraciones
(Versión de despliegue rápido)

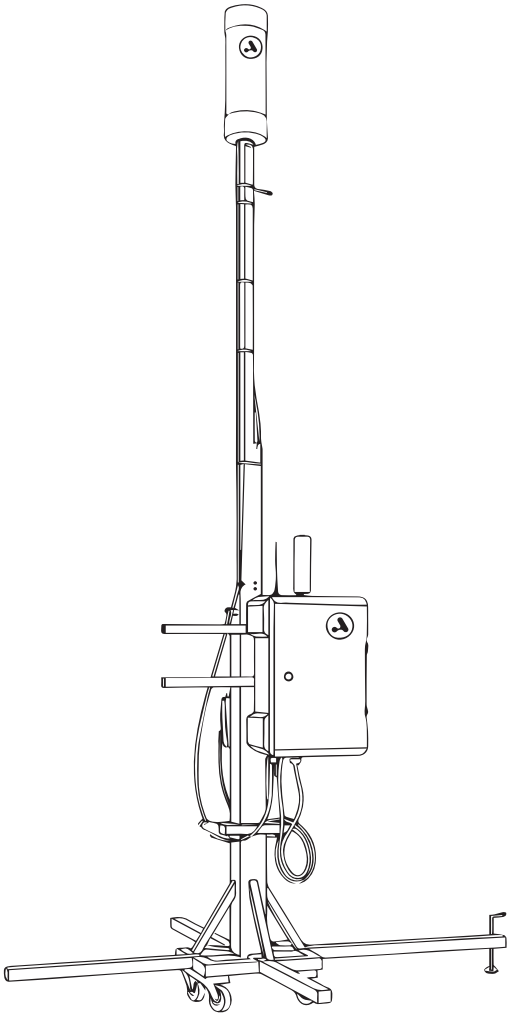
1. Para que el sistema de posicionamiento GNSS haga efecto, debe esperar entre 2 o 3 minutos después de encender el dispositivo y asegurarse de estar en un entorno con señal GNSS, como el exterior.
2. Tenga en mente que el uso del SENDES-DAU en interiores puede interferir con el posicionamiento GNSS y la conexión 4G del dispositivo.

3. Notas importantes

3.1 Información de seguridad

- Para evitar el riesgo de descarga eléctrica, desconecte el cable de alimentación de los puertos y tomas de corriente antes de reubicar el sistema.
- Si la fuente de alimentación está dañada, no trate de arreglarlo usted mismo.
- Contacte con un técnico de servicio cualificado o con su distribuidor.
- Antes de encender y conectar el SENDES-DAU a la fuente de energía, lea atentamente todos los manuales incluidos en el paquete.
- Antes de utilizar el producto, asegúrese de que todos los cables estén conectados correctamente y que los cables de alimentación no estén dañados. Si detecta cualquier daño, contacte con su distribuidor inmediatamente.
- Coloque el producto en una superficie estable.
- Evite polvo, humedad, temperaturas extremas y una exposición al sol prolongada.
- Solo puede utilizar los cables de alimentación alimentar el SENDES-DAU. El uso de cables y fuentes de alimentación de terceros hará que pierda la garantía.
- No intente desmontar el equipo; esto podría causar daños o riesgo eléctrico y anular la garantía.
- Evite colocar el equipo cerca de fuentes de calor, radiadores o equipos que generen campos magnéticos fuertes.

- Asegúrese de que la toma de corriente y la instalación eléctrica cumplan con los requisitos de voltaje y corriente del equipo.
- Mantenga las rejillas de ventilación libres de polvo y objetos que puedan bloquear el flujo de aire.
- No tire del cable de alimentación para desconectar el equipo; siempre sujete el enchufe.
- En caso de humo, olor extraño o ruidos inusuales, desconecte inmediatamente el equipo y contacte con el servicio técnico.



Need help?
sos@asdt.eu
support.asdt.eu

4. Requisitos de red para la conectividad con los sistemas sendes *(Actualización: 25/11/2025)*

Introducción

Los equipos de ASDT, tanto de detección como de neutralización, pueden operar mediante conexión a una red cableada o utilizando tecnología 4G LTE.

Desde el departamento de desarrollo de ASDT, se recomienda conectar los sistemas SENDES a través de una red cableada, preferiblemente una fibra dedicada exclusiva para dicho equipo o instalación. Esta configuración minimiza las fluctuaciones de conectividad y asegura que los equipos dispongan de una red independiente, separada de la red del cliente, a la que se conectan mediante una IP estática o a través de DHCP, evitando configuraciones complejas.
En los equipos estacionarios, ambas formas de conexión pueden combinarse para garantizar una intercomunicación ininterrumpida. En este caso, la red 4G LTE actúa como respaldo en caso de fallos en la red principal cableada.

En el caso de conexiones cableadas, los equipos SENDES pueden configurarse para operar detrás de un firewall o proxy del cliente, garantizando el cumplimiento de las políticas de seguridad de la red local. Para ello, es posible ajustar los parámetros de red de los dispositivos, como las direcciones IP, puertos y autentificación necesaria, permitiendo una integración segura y personalizada dentro de la infraestructura del cliente.

Configuración de Firewall

Cuando no sea posible disponer de una fibra dedicada para los equipos de la instalación y se debe utilizar la red existente del cliente, es recomendable que esta red cuente con un **firewall** para garantizar la seguridad de la infraestructura.

Un firewall es un sistema de seguridad diseñado para actuar como una barrera entre una red interna y redes externas, como Internet. Su principal función es controlar y filtrar el tráfico de datos entrante y saliente según reglas predefinidas, protegiendo los sistemas frente a accesos no autorizados, ataques cibernéticos y otras amenazas.

Al permitir únicamente las conexiones necesarias y seguras, el firewall contribuye a mantener la integridad de la red.

En el caso de los sistemas SENDES, el firewall del cliente es fundamental para garantizar una comunicación protegida entre los equipos y los servidores de ASDT, cumpliendo con las configuraciones específicas requeridas para su correcto funcionamiento.
Para ello, es imprescindible configurar una serie de parámetros específicos en el firewall de la red del cliente o en cualquier otro dispositivo que actúe como intermediario entre los sistemas SENDES y los servidores de ASDT. Estas configuraciones aplican tanto a los sistemas de detección (SENDES DAU y SENDESCOPE) como a los sistemas de neutralización (SENDES SJ y SENDES SJ-BOX).

Configuración requerida

1. Configuración de red:

- Asignar una **IP estática** para cada sistema, incluyendo la máscara de red, la puerta de enlace (Gateway) y los servidores DNS necesarios para la resolución de dominios.

2. Conexiones salientes:

- Permitir las conexiones salientes hacia los subdominios de *.asdt.eu y en otras IPs, en los siguientes puertos, que se detallan al final del documento:
  - **80 (HTTP), 443 (HTTPS), 4000 y 5883**

3. Acceso remoto:

- Habilitar el puerto **22 (SSH)** y **21 (FTP)** para conexiones salientes.

4. Sincronización de hora:

- Configurar un servidor **NTP** para la sincronización precisa del reloj del equipo.

5. Pruebas de conectividad:

- Permitir el uso del comando PING hacia la puerta de enlace (Gateway), los servidores DNS proporcionados por el cliente y los subdominios de ***.asdt.eu**; así como hacia los distintos equipos anti-drones de la instalación.

6. Sistemas de visualización:

- Además, para los equipos de Puesto de Mando y Control (PMYC), se debe permitir el acceso a los dominios ***.openstreetmap.org, mapbox.com** y **unpkg.com**, específicamente para los sistemas de visualización.

Configuración de Proxy

Un caso específico de sistemas de seguridad en la red del cliente, similar al firewall, es el uso de un proxy. Un **proxy** es un servidor intermedio que actúa como puente entre los dispositivos de una red y los servicios externos, gestionando y filtrando las solicitudes de conexión, lo que permite controlar el acceso y mejorar la seguridad y el rendimiento de la red.

Aunque ASDT considera que un firewall en la red es suficiente para garantizar la seguridad y el funcionamiento adecuado de los sistemas SENDES, existen infraestructuras por parte del cliente que requieren el uso de un proxy. En estos casos, es posible configurar el proxy en los dispositivos SENDES, aunque con algunas limitaciones.
La implementación de un proxy puede ser necesaria para cumplir con las políticas de red del cliente, pero es importante tener en cuenta que este método de conexión no es el preferido debido a las restricciones que puede implicar.

Configuración requerida

1. Configuración de red:

- Asignar una **IP estática** a cada sistema, junto con su máscara de red y los servidores DNS necesarios para la resolución de dominios.

2. Conexiones salientes:

- Permitir conexiones a los subdominios de ***.asdt.eu** y otras IPs, a través de los siguientes puertos, que se detallan al final del documento:
  - **80 (HTTP), 443 (HTTPS), 4000 and 5883**

3. Sincronización de hora:

- Configurar un servidor **NTP** para la sincronización precisa del reloj del sistema.

4. Pruebas de conectividad:

- Permitir el uso del comando **PING** hacia la puerta de enlace (Gateway), los servidores DNS proporcionados por el cliente y los subdominios de *.asdt.eu; así como hacia los distintos equipos anti-drones de la instalación.

5. Acceso remoto:

- Habilitar el puerto **22 (SSH) y 21 (FTP)** para conexiones salientes.

- En caso de no ser posible habilitar la conexión remota mediante SSH, se debe garantizar el acceso remoto del servicio técnico de ASDT mediante una herramienta de trabajo propia de la infraestructura del cliente, como por ejemplo una VPN.

6. Sistemas de visualización:

- Además, para los equipos de Puesto de Mando y Control (PMYC), se debe permitir el acceso a los dominios ***.openstreetmap.org, mapbox.com y unpkg.com,** específicamente para los sistemas de visualización.

7. Configuración del proxy:

- Proporcionar la **IP y el puerto del proxy** para gestionar las conexiones HTTP y HTTPS.
- Facilitar las **credenciales de autenticación** si el proxy lo requiere.

Conectividad mediante 4G LTE

Los equipos de detección y neutralización SENDES pueden operar mediante conexión 4G LTE, proporcionando una opción de conectividad flexible y confiable. Para su funcionamiento a través de 4G LTE, es necesario utilizar una **tarjeta SIM** sin PIN, lo que permite una conexión automática y continua sin requerir intervención manual.

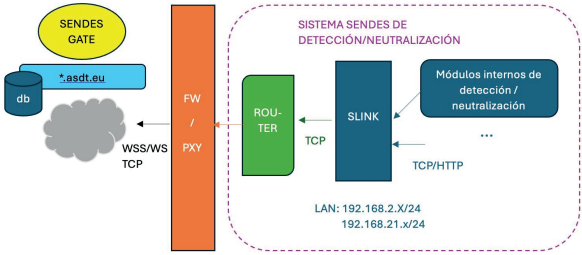
La opción de 4G LTE puede utilizarse de dos formas:

1. **Conexión primaria:** Esta opción es ideal para equipos portátiles o sistemas cuya conectividad depende del 4G, ya que permite su funcionamiento en ubicaciones donde no esté disponible una red cableada.
2. **Respaldo de la red cableada:** En caso de que se utilice una red cableada como conexión principal, el 4G puede configurarse como una opción de respaldo, asegurando la continuidad del servicio en caso de fallo o interrupción de la red cableada. De esta forma, el 4G LTE ofrece flexibilidad y fiabilidad, adaptándose a diferentes necesidades de conectividad según el entorno y los requisitos de la instalación.

Consideración importante: Es posible que, al activar la neutralización, se pierda temporalmente la conectividad de los equipos de detección o neutralización de la zona que operen en 4G LTE, dependiendo de la frecuencia que se haya activado. Para más información, por favor, contactar con el departamento técnico de ASDT.

Diagrama de arquitectura

La arquitectura de la solución está representada en el siguiente diagrama, donde se detallan las conexiones entre los diferentes módulos que componen el sistema de detección, así como las interacciones entre el sistema y el entorno exterior.



Detalle de los Subdominios

En la siguiente tabla se detallan los diferentes subdominios de ASDT. Es preferible aceptar en el firewall los subdominios generales de *.asdt.eu, *asdt.io.

NOMBRE	DNS	IP ASOCIADA	PUERTOS	OUTGOING SSH puertos 22 y 21
SENDES Gate	sendesgate.asdt.eu	185.196.43.15	443, 80	NO
	sendesgate.asdt.io	*	443, 80	NO
Security	security.asdt.eu	185.196.43.11	443, 80	NO
Manager	manager.asdt.eu	38.252.226.201	443, 80, 4000	YES
	manager.asdt.io	*	443, 80, 4000	YES
Backup	xmanager.asdt.eu	51.83.205.137	443, 80, 4000	YES
	devserver.asdt.eu	51.83.198.230	80	NO
		13.37.222.104, 8.211.58.246	443, 80, 5883	NO
	gitlab.asdt.eu	51.83.158.204	443, 80	NO
		185.196.43.16	443, 80	NO

Es preferible autorizar los subdominios en el firewall o proxy usando el nombre de dominio DNS, ya que las IP pueden cambiar por parte de ASDT. Si no es posible hacerlo por dominio, debe comunicarse expresamente al departamento técnico.

5. Garantía

La garantía de los sistemas suministrados por ASDT Corporation S.L.U. tiene un plazo de vigencia de doce meses a contar desde la fecha de entrega del sistema, con independencia de la fecha efectiva de instalación. En el caso de los sistemas portátiles o de mano, las baterías, al considerarse elementos consumibles, disponen de un plazo de garantía específico de seis meses.

La garantía cubre los principales componentes del sistema, incluyendo los armarios de electrónica, los sistemas de procesamiento tales como ordenadores y placas de control, los sistemas de comunicación como routers y switches, los amplificadores de frecuencia, los módulos de decodificación y descifrado, las fuentes de alimentación, cargadores, conectores y cableado, los sistemas de amplificación y filtrado de señal, así como las antenas omnidireccionales y/o direccionales suministradas por ASDT.

Durante el período de vigencia de la garantía, ASDT garantiza la disponibilidad de las piezas necesarias para la reparación de los equipos afectados. Una vez finalizado dicho período, no se garantiza la disponibilidad de repuestos idénticos a los originales; no obstante, en caso necesario, se emplearán componentes de calidad igual o superior, asegurando en todo momento el mantenimiento de las funcionalidades del sistema.
La garantía quedará automáticamente anulada en aquellos supuestos en los que se detecte un uso inadecuado del sistema o distinto al indicado por ASDT, así como en caso de modificaciones, aperturas o reparaciones realizadas por personal no autorizado. Asimismo, se excluyen de la cobertura los daños externos derivados de accidentes, negligencia, condiciones climáticas extremas o actos vandálicos, los daños producidos durante transportes no gestionados por ASDT que no hayan sido comunicados de forma oportuna, las instalaciones no realizadas por técnicos autorizados y el uso de componentes o cableado no suministrados ni expresamente autorizados por ASDT.

El proceso de reclamación de garantía se iniciará mediante la comunicación de la incidencia a la dirección de correo electrónico support@asdt.eu, recomendándose informar simultáneamente a la persona de contacto designada por ASDT. Tras la recepción de la notificación, se llevará a cabo un diagnóstico remoto inicial y, si procede, se solicitará el envío del equipo a fábrica para su evaluación. ASDT realizará una evaluación técnica del defecto con el fin de determinar si éste se encuentra cubierto por la garantía. En caso afirmativo, se procederá a la reparación o sustitución del equipo conforme a los términos de la garantía. En caso de no estar cubierta la incidencia, se emitirá el correspondiente informe técnico, junto con un presupuesto detallado y un plazo estimado de actuación.

6. Declaración sobre el uso de la tecnología SENDES DAU

Estimado cliente,

Por la presente, afirmamos que SENDES DAU, una tecnología desarrollada por ASDT Corporation SLU, está diseñada y destinada principalmente para aplicaciones civiles. Esta tecnología tiene como objetivo abordar y mitigar posibles amenazas relacionadas con la detección, análisis y gestión de actividades de drones, contribuyendo a la protección de instalaciones críticas y garantizando la seguridad de activos e infraestructuras civiles.

Los sistemas de ASDT han sido especialmente diseñados y fabricados para identificar y neutralizar la amenaza de drones civiles y comerciales, con el fin de minimizar el riesgo de posibles incidentes ocasionados por negligencias o actos hostiles. ASDT no se responsabiliza de la no detección o no neutralización en espacios aéreos afectados por dispositivos no comerciales, militares, proyectados, catapultados o desplomados.

En ASDT, nuestro compromiso con el uso ético y responsable de la tecnología es primordial. Nos esforzamos por desarrollar y promover soluciones que mejoren el bienestar social y refuercen la protección de infraestructuras críticas. SENDES DAU está específicamente adaptado para satisfacer las necesidades de aplicaciones civiles, incluyendo la monitorización del espacio aéreo, la detección de incursiones no autorizadas de drones, el apoyo a labores de vigilancia, el cumplimiento de la ley y los escenarios de respuesta ante emergencias.

Aunque SENDES DAU no está diseñado explícitamente para uso militar, reconocemos que determinados clientes podrían considerar su aplicación en contextos de seguridad avanzada. En dichos casos, es fundamental enfatizar que cualquier uso debe cumplir estrictamente con las leyes internacionales, las regulaciones vigentes y las directrices éticas que rigen el despliegue de tecnologías de este tipo.

ASDT mantiene un firme compromiso con la transparencia y el cumplimiento íntegro de todos los marcos legales aplicables. Asimismo, colabora exclusivamente con socios y clientes responsables para garantizar que el despliegue de la tecnología SENDES DAU se realice conforme a los estándares éticos y a los requisitos internacionales.

Si tiene alguna pregunta o requiere información adicional, no dude en ponerse en contacto con nosotros.

QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:

QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:

QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:

QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:

QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:

QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:
QUALITY CHECK:
FIELD TEST:
PACKAGING:
DATE:
NOTES:

