DRYAD

CONNECTING THE NATURAL WORLD

SILVANET DOCUMENTATION

JUNE 7, 2024

Document Number:	1.0-0100-3.4.1
Document Revision Number:	3.4.1
Document Status:	Released
Issue Date:	June 7, 2024

Getting Started with Silvanet

Learn how to setup and test a deployment of the **Dryad SilvanetÔ Wildfire Detection System** to provide ultra-early forest fire detection in public and private forests. Learn how the system sends Fire alerts to registered users if a smoldering fire is detected.

Wildfires cause up to 20% of global CO2 emissions, the same amount that traffic (all cars, aircraft and ships combined) put into the air. And human activity is responsible for about 80% of wildfires. Furthermore, wildfires have a devastating impact on biodiversity with more than 3 billion animals killed and they cause more than $140 billions of economic losses each year.

Dryad's Silvanet™ provides ultra-early detection of forest fires, with large-area monitoring, real-time warning and reliable prevention. Our solar-powered sensors, which are placed directly into the forest, use ultra-sensitive gas sensors to monitor the composition of the air and detect fires using embedded artificial intelligence. The sensors then send an alert signal over our large-scale IoT mesh network. Our cloud monitoring platform collects this data which sends out alerts in case of a detected fire. Because a forest environment may cause interference with mobile network operator coverage, the Silvanet™ System uses our key innovation - our own wireless network infrastructure which is a solar powered mesh network architecture that enables large-scale, off-grid deployments.

We recommend two deployment stages - a small Pilot stage and a large Live stage. The Pilot stage demonstrates Silvanet's™ core functionality and basic scalability of the system and has a duration of approximately 2-4 months. The Live stage is a large-scale deployment across the targeted forest and has a deployment duration of 10-15 years.

Silvanet™ System

The Silvanet™ System consists of a network of *Silvanet Sensors* connected to the *Silvanet Cloud* in a mesh network of *Mesh Gateways* and *Border Gateways*. The sensors are permanently attached to trees about 3 meters above the forest floor and send periodic messages about the environmental to the Silvanet Cloud.

Silvanet Suite network

Automatic notifications

If a Dryad Silvanet™ sensor detects a smoldering fire within range of the sensor, automated notifications are immediately sent to authorized users via the Silvanet™ Mesh network, Silvanet™ Cloud and Internet. Users immediately receive information about the exact location of the sensor(s) that detected the fire through an email and on the Dryad Site Management app.

Compliance

Antennas

	Brand	Model Name	Antenna Type	Gain (dBi)
GPS	Dryad	GPSANT- 0001	Trace Antenna	-
LoRa	ALFA	AOA-915-5ACM	Dipole	5
LoRa	ALFA	AOA-868-5ACM	Dipole	5
WWAN	Delock	Nr. 88980	Dipole	-
P-GSM900				-0.03
DCS 1800				2.45
LTE Band 1				1.38
LTE Band 3				2.45
LTE Band 8				-0.03
LTE Band 20				-0.4
LTE Band 28				-0.25

EU Compliance

CE Radiation Exposure Statement

This equipment should be installed and operated with a minimum distance of 24 cm between the radiator and your body.

CE Operating Bands and Maximum Output Power

Equipment	Model	PoE Layout	Cellular (WWAN)	Satellite
Silvanet Border Gateway	SBG-2	With	With	With
Silvanet Mesh Gateway	SMG-2	Without	Without	Without

Bands	Gain (dBi)	Power (dBm)	EIRP (dBm)
		LoRa	
M	5	11.02	16.02
N	5	10.65	15.65
P	5	19.30	24.30
		2G	
900	-0.03	35	34.97
1800	2.45	35	37.45
		LTE Cat-M1 (eMTC)	
B1	1.38	25.70	27.08
B3	2.45	25.70	28.15
B8	-0.03	25.70	25.67
B20	-0.4	25.70	25.30
B28	-0.25	25.70	25.45
		LTE Cat-NB1 (NB-IoT)	
B1	1.38	25.70	27.08
B3	2.45	25.70	28.15
B8	-0.03	25.70	25.67
B20	-0.4	25.70	25.30
B28	-0.25	25.70	25.45

Referred to Article 10(9), CE simplified EU declaration of conformity

Hereby, Dryad Netwoks GmbH declares that the radio equipment type 1. Silvanet Border Gateway, SBG-2; 2. Silvanet Mesh Gateway, SMG-2 are in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following address: https://docs.dryad.app/about/declarations.html

USA Compliance

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 23cm between the radiator and your body.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Company contact details

Name: Dryad Netwoks GmbH
Contact: https://www.dryad.net/support

Canada Compliance

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

ISED Statement

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L’émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d’Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L’exploitation est autorisée aux deux conditions suivantes :

1. L’appareil ne doit pas produire de brouillage;
2. L’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.

The transmitter module may not be co-located with any other transmitter or antenna.	Le module émetteur peut ne pas être coïmplanté avec un autre émetteur ou antenne.

ISED Radiation Exposure Statement

This equipment complies with ISED RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 34cm between the radiator and your body.	Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 34cm de distance entre la source de rayonnement et votre corps.

Quick start

This Quick start briefly explains how to build a deployment Packet assign it to a Silvanet user who deploys the Packet's Silvanet sensors and gateways in a defined area of a forest. After the devices are deployed, a deployment test can be run.

Requirements

To do the steps in this tutorial, ensure you have the following:

- Login credentials to the Silvanet Site Management app obtained from Dryad
- Installed the Silvanet Dryad Deployment app on your smartphone

Deployment steps summary

Build a deployment Packet using the Dryad Deployment app.

Assign the Packet to a user who will deploy the devices in the Packet.

Deploy the devices at the locations specified in the Packet.

Test the deployment.

Access Site Management app

The Site Management app is used to plan deployments and to monitor the devices in the site. It is connected to the Silvanet Cloud which receives data from the sensors via Mesh Gateways and Border Gateways. This data is then displayed in the Site Management app.

Go to dryad.app and sign in using your username and password provided to you from Dryad.

> **Note**: If this is the first-time logging in, you need to change your password. However, you cannot change your username.

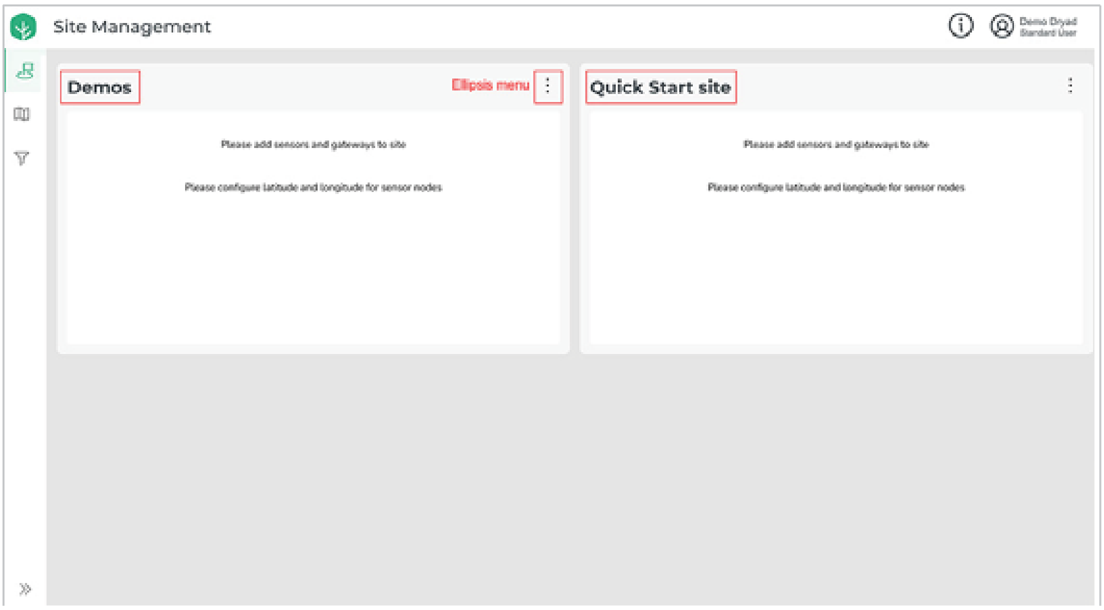
Open a Site

Sites are accessed on the Site Management dashboard. It displays all Sites to which you have been granted access. You may see one or more Sites on the dashboard, depending on your access level.

Info: A Site groups together sensor devices and gateways within a geographical area or with similar characteristics.

1. After logging in, the Site Management dashboard appears showing the sites assigned to you.

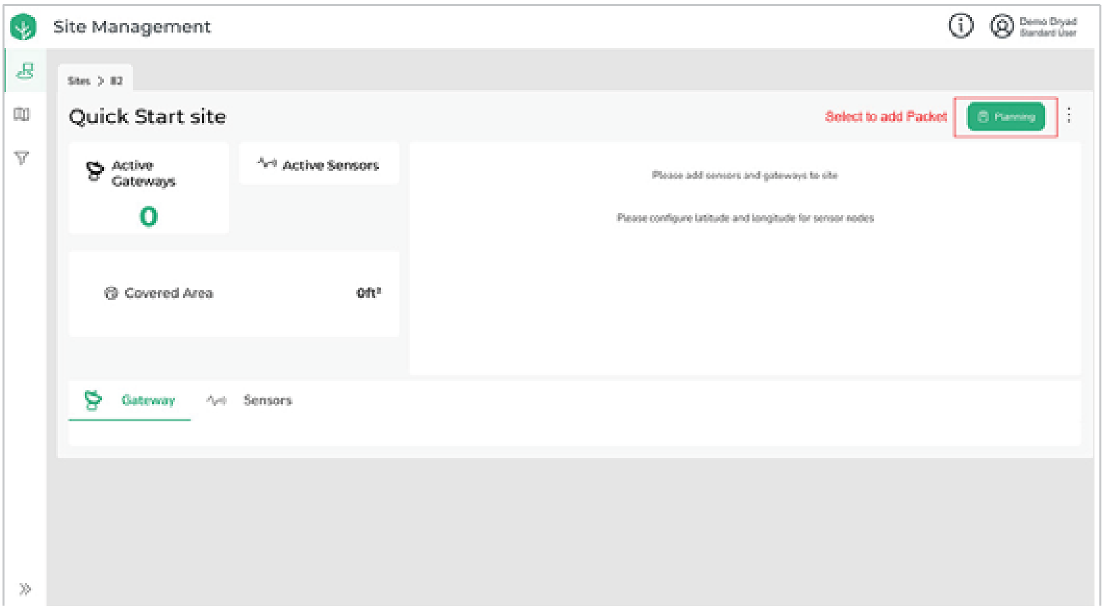
2. Select **Open** from the ellipsis menu in the header of a Site to open the Site dashboard. Alternatively, you can select a Site name link to open the Site.



Open a Site from the Site Management app

Build a Deployment Packet

Planning your deployment of Silvanet devices begins by building Deployment Packets. This is done using the Site Dashboard. The Site Dashboard shows any previously deployed gateways and sensors as well as the area covered by your Silvanet devices.



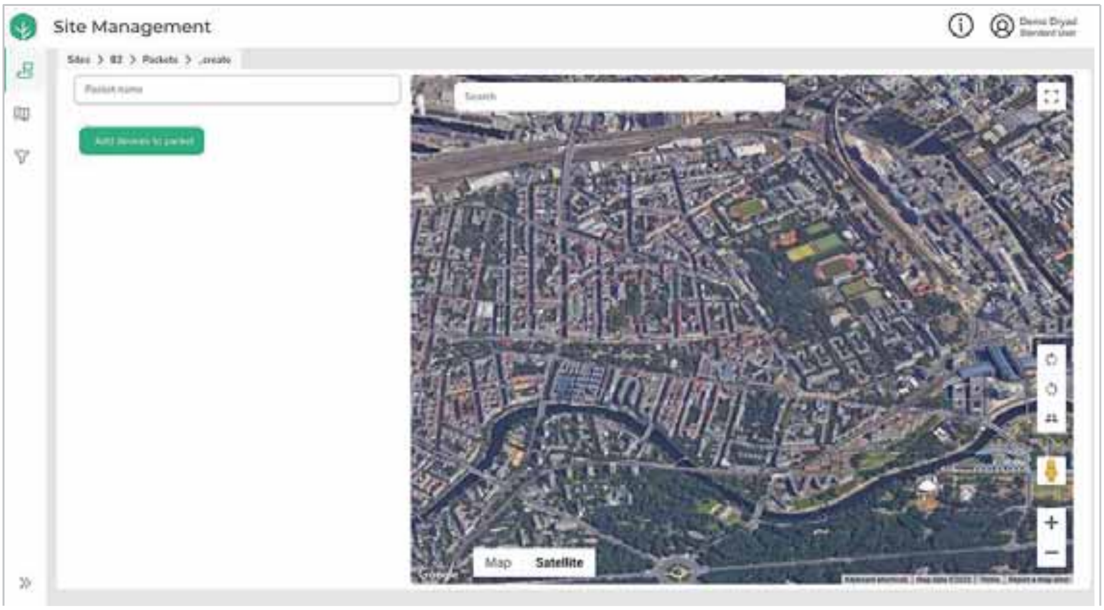
Site Dashboard

A *Deployment Packet* is a set of Silvanet devices (sensors and gateways) to be deployed in a Site. Each device in a Packet has its own GPS coordinates which are set during the building of the Packet. These GPS coordinates are used to find the location where the devices are to be deployed. Once deployed, the GPS coordinates are updated to the actual location of the device.

Info: Measurements in the Site Management app can be displayed in either square meters or square feet, depending on your account settings.

Add a new Packet

1. From the Site Dashboard, select **Planning**.
2. In the Packet dashboard, select **Add Packet**.
3. On the next page, give the packet a descriptive name.



Add a new Packet using the Packet Dashboard

4. Center the map on the location where you plan to deploy the Silvanet Suite devices.

> **Tip:** You can use the Search function to locate the area on the map.

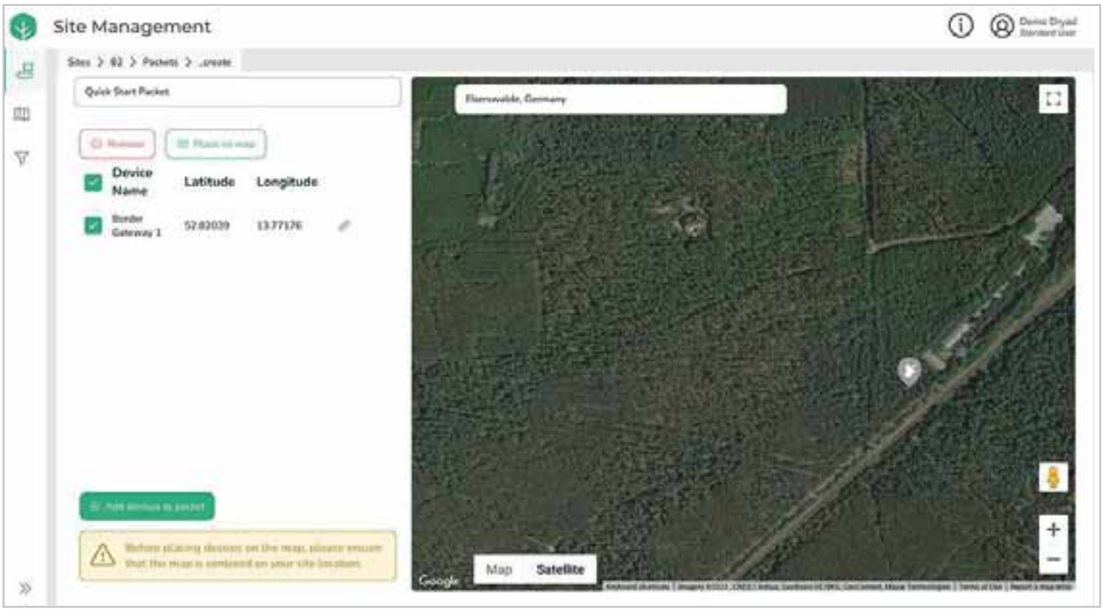
Add Border Gateway to a Packet

1. From the Packet dashboard, select **Add devices to packet** to display the device options.

2. Select **Border Gateway** from the **Choose device type** dropdown, enter the amount of Border Gateways to add, then select Add.

3. Place the new Border Gateway on the map by first selecting the Border Gateways, then select **Place on Map**. The Border Gateway icon appears as a gray (inactive) icon on the map.

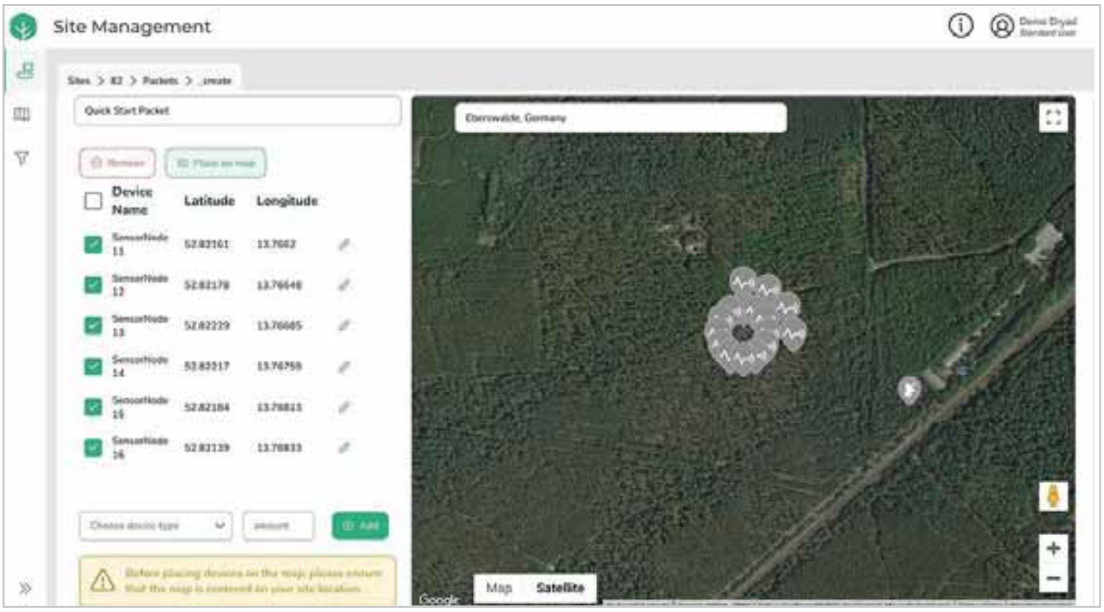
4. Select **Save** to save the Packet to the Silvanet Cloud.



Add Border Gateways to Packet and place on map

Add sensors to the Packet

1. From the Packet dashboard, select **Add devices to packet** to display the device options.
2. Select **Sensor** from the **Choose device type** dropdown, enter the number of sensors to add, then select **Add**.
3. Place the new sensors on the map by first selecting the sensors from the list of devices, then select **Place on Map**. The sensors appear as gray (inactive) icons on the map.
4. Select **Save** to save the Packet to the Silvanet Cloud.



Add sensors to Packet and place on map

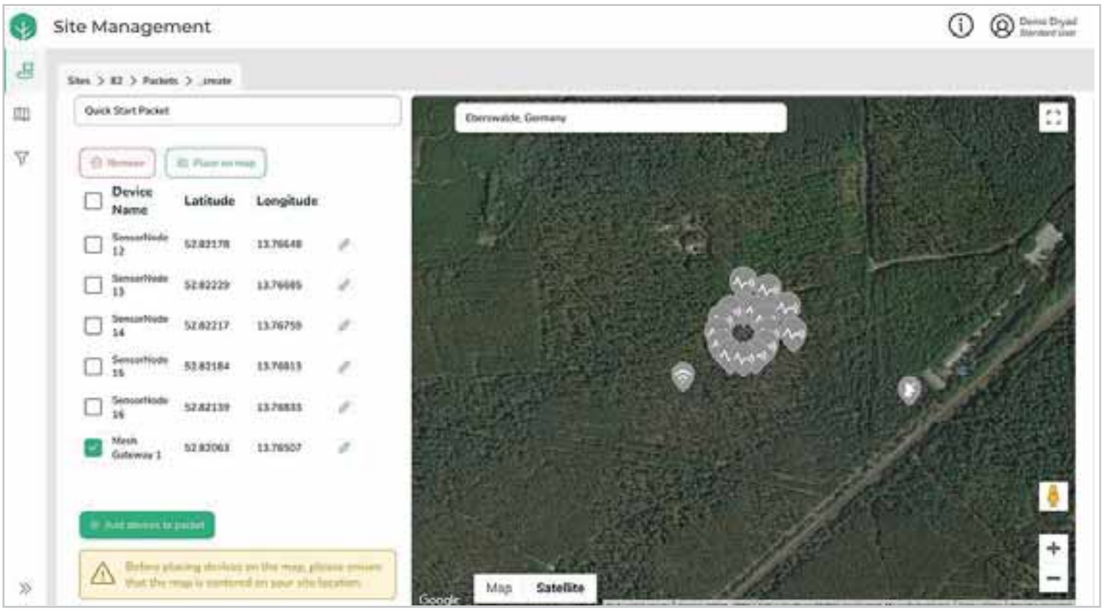
Add Mesh Gateways to a Packet

1. From the Packet dashboard, select **Add devices to packet** to display the device options.

2. From the **Choose device type** dropdown, select **Mesh Gateway**, enter the amount of Mesh Gateways., then select **Add**.

3. Place the new Mesh Gateways on the map by first selecting the Mesh Gateways from the list of devices, then select **Place on Map**. The Mesh Gateway icons appear as gray (inactive) icons on the map.

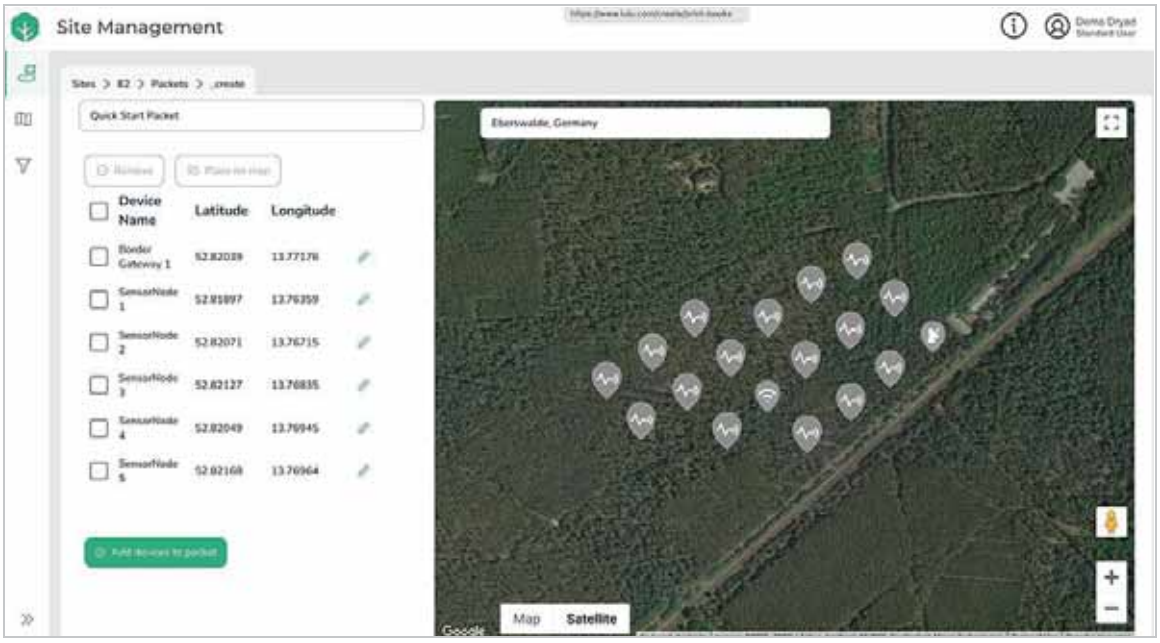
4. Select **Save** to save the Packet to the Silvanet Cloud.



Add Mesh Gateway to Packet and place on map

Place devices at planned locations

With the devices added to the map, you can now move the icons to their estimated final locations.



Moving devices to estimated final location

Tip: You can verify the distances between devices by enlarging to full screen mode and selecting a device icon. When selecting on a device icon on the map, the device's distances to the three nearest devices are shown on connecting lines. This helps you determine the device's distances to other devices.

Placing devices at planned locations

Place the Border Gateway(s)

- Select a location in the Site where the device has access to a power supply and has internet connectivity. See Border Gateway deployments for deployment options.
- The Site Management app updates the planned GPS coordinates of the Border Gateway.

Place the sensors

- Use a grid pattern with approximately 100 meters between sensors.
- Place the first sensor with line of sight to the Border Gateway.
- Continue placing the sensors in a grid consisting of rows of sensors, ensuring each device is approximately the same distance away from other sensors (for example, 100 m).
- The Site Management app updates the planned GPS coordinates of the sensors.

Place the Mesh Gateways

- Ensure the Mesh Gateway is no more than 2-3 km from either a Border Gateway or other Mesh Gateways.
- Locate a position on the map where the Mesh Gateway provides access to sensors within a radius of 1 km. Depending on the number of sensors, more than one Mesh Gateway may be required to provide adequate coverage.

- The Site Management app updates the planned GPS coordinates of the Mesh Gateways.

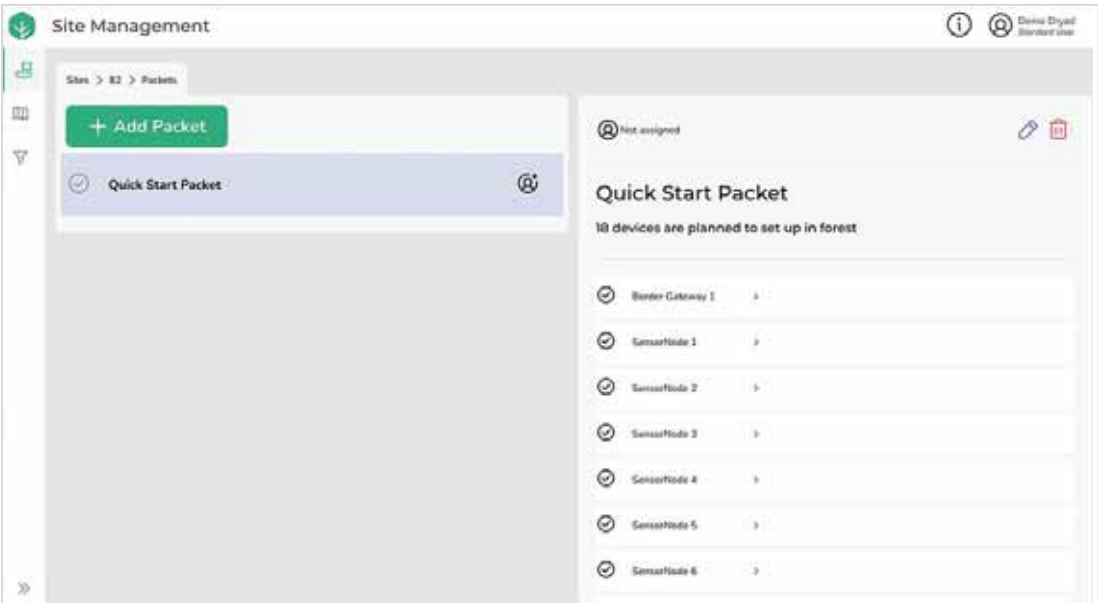
Save the Packet

1. Select **Save** to save the new Packet to the Silvanet Cloud.
2. Return to the Packet dashboard by selecting **Back**.

Assign Packet to a user

Assign the completed Packet to a registered user who deploys the devices.

1. From the Packet dashboard, select the **Assign** icon next to the new Packet.
2. From the list of available users, select a use, the select **Assign**.



Assign Packet

The Packet's devices are now ready to be deployed in the forest.

Deploy devices

When the forestry worker enters the forest to deploy the sensors and gateways for a Site, the deployment location for each device can be found using the Dryad Deployment app which runs on a Smartphone.

Warning: Always work in teams of two when entering a forest to deploy the devices.

Device IDs

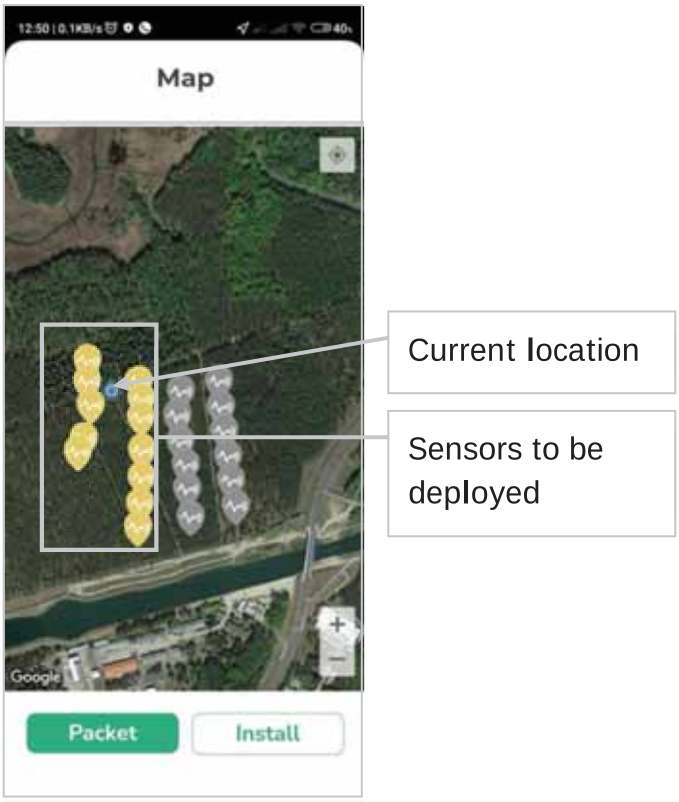
Each device has its own Device Id. This is provided as a text string and a QR Code on a label attached to the device. When the device ID is automatically entered using the QR Code (or manually entered using the text string) prior to attaching it to the tree, the app updates the planned location of the device to its actual location.

Deploy the sensors

1. Register the deployment location of the sensor.
2. Install the sensor on a tree.

Register the deployment location

1. Open the Dryad Deployment app on your smartphone. All Packets assigned to you are shown.
2. Open the assigned Packet for the devices you are about to deploy.
3. Using the Dryad Deployment app, move towards the first sensor deployment location. Your location appears as a blue dot.

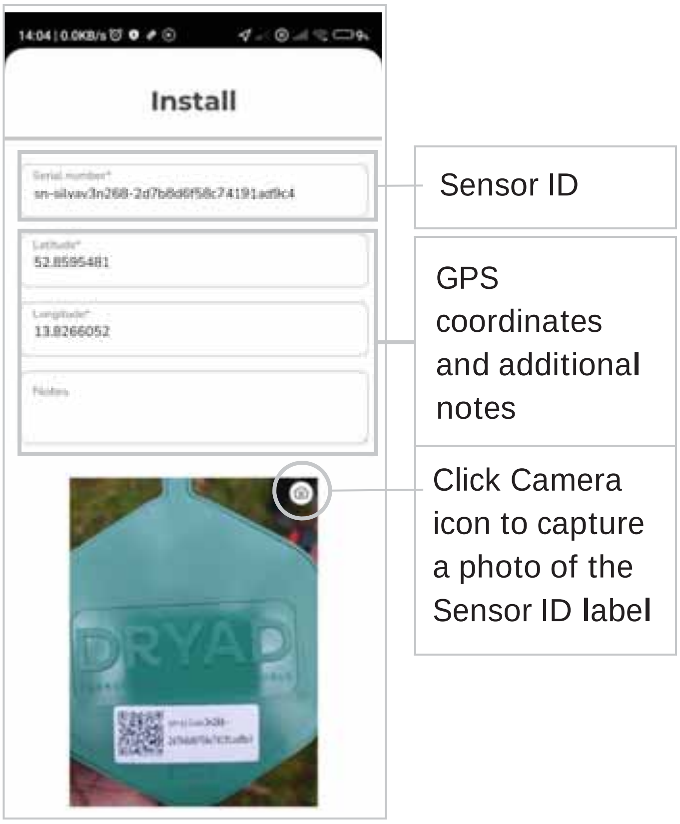


Deploy sensors

4. When a location is found for the sensor based on the deployment guidelines, scan the QR Code of the sensor by selecting Install.

5. You can add notes about the deployment location in the Notes field.

6. Select the Camera icon to use the camera on the Smartphone to take a picture of the Sensor ID label on the back of the device.



ID, GPS coordinates and photo of sensor

7. Save the changes by selecting **Save**. The sensor's ID and actual location are saved to the Silvanet Cloud.

Install the sensor on a tree

1. Find a location on the tree that is at least 3 meters above the forest floor and facing the sun at 12:00 noon.

2. If required, clear a small area of bark so the sensor sits flat and horizontal.

3. Attach the sensor to the tree using a tree nail (or crop wire) and spacer.

Sensor attached using tree nail and spacer

Attached sensor using tree nail

4. Repeat the same procedure until all sensors have been deployed.

Deploy the Border Gateway

1. Scan the QR Code of the Border Gateway using the same procedure described for sensors.

2. Attach the Border Gateway and its solar panel to a tree or pole. Use tree nails, U-clamps, or crop wire to attach the gateway and solar panel.

3. Attach the antennas to the Border Gateway where the LoRa antenna on top, LTE-M antenna on bottom and SWARM satellite antenna on side.

Deploy the Mesh Gateways

1. Scan the QR Code of the Mesh Gateway using the same procedure described for sensors.

2. Attach the Border Gateway to a tree or pole using tree nails or crop wire.

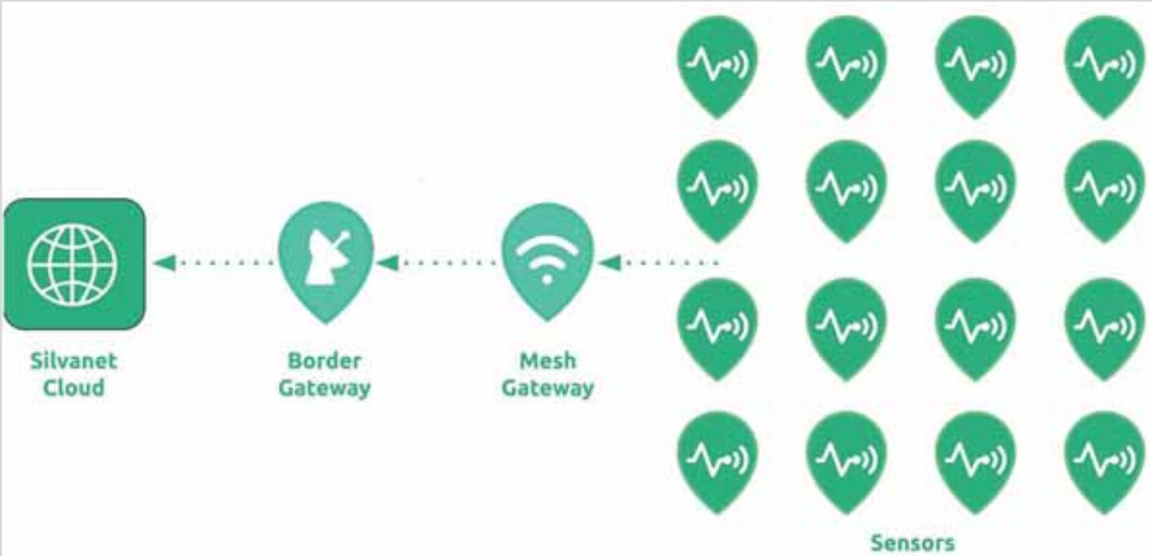
Test the deployment

Once the devices have been deployed, run a test to verify the deployment.

This test uses a controlled fire set in the middle of the sensors. The Silvanet System should respond to the smoke from the fire by sending **Fire alerts** to registered users via email and displayed in the Site Management app.

Silvanet Suite

Dryad's wildfire detection system, the *Silvanet Suite*, is a network of devices installed in a forest and a set of browser and smartphone apps connected to the Silvanet network through the Silvanet Cloud.



Silvanet Suite network

Silvanet Suite devices:

- **Silvanet sensors** detect forest fires during the early stages (even during the smoldering phase.
- **Silvanet Mesh Gateways** extends the Silvanet Network to allow for large-scale deployments of Silvanet sensors.
- **Silvanet Border Gateways** provides connectivity between the Silvanet Mesh Network and the Silvanet Cloud.
- **Silvanet Cloud platform** which receives messages via the Internet from the Silvanet devices deployed in the forest and provides the connection to the Silvanet Suite apps.

Silvanet Wildfire Sensor

The *Silvanet Wildfire Sensor* is designed to detect forest fires during the early stages (even during the smoldering phase, within the first 60 minutes) and to monitor the microclimate by measuring temperature, humidity and air pressure.

Silvanet sensor

Key features

- Gas sensor

  The sensor includes a gas sensor that combines ultra-low-power Air Quality sensing with a precise gas sensing mode. Hydrogen, carbon monoxide, carbon dioxide and other gasses are detected at the ppm level with built-in artificial intelligence to reliably detect a fire and avoid false positives.

- LoRa/LoRaWAN connectivity

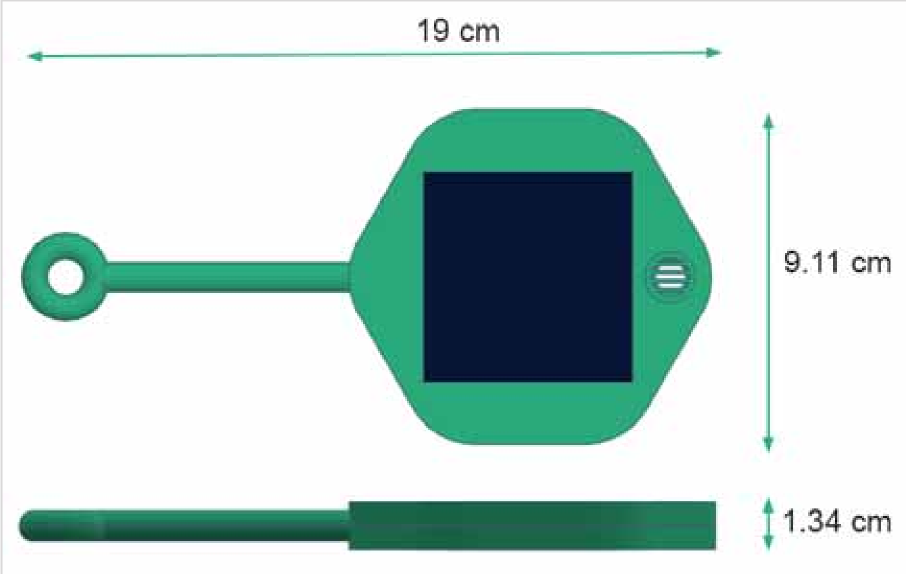
  To connect with the Silvanet Network, the sensor uses a LoRA-integrated radio to connect to a robust LoRaWAN mesh network within a large forest environment. This allows the sensors to connect to distributed LoRaWAN-enabled Silvanet Mesh Gateways and Border Gateways.

- Solar powered

  It can run maintenance-free for 10 to 15 years without the need of batteries, avoiding the use of lithium and other toxic materials. It obtains its energy source from a built-in solar panel. As a precaution against the device itself starting a fire, it stores its energy in supercapacitors rather than batteries. A loop allows it to be attached directly to trees using tree nails or crop wire (temporary use only).

Dimensions and weight

The dimensions of the Silvanet sensor are (L x W x H) 19 cm x 9.11 cm x 1.34 cm. The sensor weighs 136g.

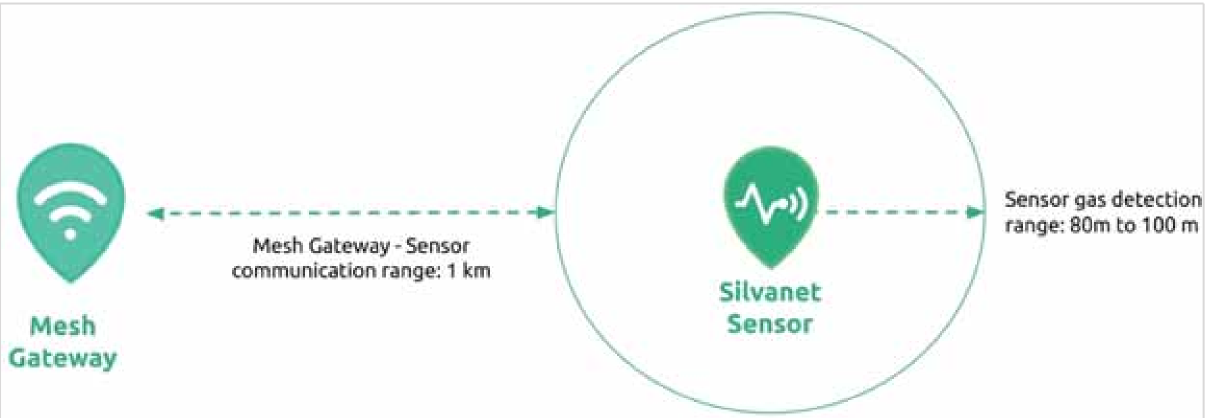


Silvanet sensor dimensions

Info
Ingress protection of the housing is IP65. This means the housing is completely protected against dust and water resistance.

Sensor range

Silvanet sensors detect environmental air quality within a radius of 80 m to 100 m (260 ft to 320 ft) for 60 min detection of 2m x 2m fire. It can communicate with Mesh and Border Gateways that are 1 km away from the sensor, depending on topology.



Sensor ranges

BME688 gas sensor

The Silvanet Wildfire sensor uses the Bosch BME688 Gas Sensor to monitor the microclimate of the forest. It is a low-energy hydrogen sensor that detects the presence of a smoldering fire over distances of up to 115m. The gas sensor detects the presence of *Volatile Organic Compounds* (VoCs) and *Volatile Sulfur Compounds* (VSC) and detects these compounds at <20 ppm.

Environmental detection

The BME688 sensor can detect CO (Carbon Monoxide), CO_2 (Carbon Dioxide), H_2, (Hydrogen), VOC (Volatile Organic Compounds), Temperature, Humidity and Air pressure.

The BME688 sensor monitors the microclimate of the forest by reading the following environmental values:

- Gas resistance: Outputs the IAQ (Index for Air Quality), VOC and CO2 equivalents (ppm). The gas scan result is a % value.
- Humidity: Outputs relative humidity
- Air pressure: Outputs pressure in Pa
- Temperature: Outputs temperature in Celsius

This gas sensor has built-in environmental sensing using Artificial Intelligence (AI) to generate a normalized value for the environment in which it has been placed.

Measurement conditions

In the Silvanet sensor, the BME688 sensor provides measurements under the following conditions:

- Pressure: 300 to 11000 hPa
- Humidity: 0 to 100%
- Temperature: -40 to 85°C

Power consumption

The Silvanet sensor has very low energy consumption which is provided by its built-in solar panel. As a precaution against the device itself starting a fire, the sensor stores its energy in supercapacitors rather than batteries.

The two key components of the sensor that consume energy are the BME688 gas sensor and the LoRa radio. The gas sensor consumes ~3.9 mA in standard gas scan mode. The radio consumes 7W of energy to operate so it can continue to operate in a shaded location for ~6 hrs.

Power supply

The sensor requires sufficient energy to support continuous operation over a 24 hr. period while still having enough reserve power to support the heating and powering of the BME688 sensor and to send a burst of messages when a fire is detected.

Idle/active modes

Normally, the Silvanet Sensor Node is in idle mode. It activates every 60 seconds to read the air quality / gas sensor and every 2 hours to read the environment. It then sends a single packet to the Silvanet Server via the Mesh Gateway and Border Gateway. These data packets contain normal (non-fire detection) environmental data - temperature, pressure and humidity internal values. These values can be viewed in the Site Management app.

Built-in solar panel

The sensor includes on its front housing a 60mm x 60mm solar cell. It continuously generates energy during the daytime and recharges the device with sufficient power for the next 24 hours. After sunset, it begins to discharge until sunrise. After sunrise, it begins to recharge to 100% within about an hour.

Each day the solar panel harvests 7Ws in the constrained conditions of a forest. The required energy can be generated using a 60mm x 60mm solar panel.

Info
Sufficient ambient light is available in forests to provide sufficient light for the solar panel. Forests are never entirely dark during the day, even with a thick forest canopy.

Supercapacitor Energy Storage

The Silvanet sensor uses a set of supercapacitors to store energy for use by the radio and BME688 sensor and other components. It stores the energy for day-to-day tasks and has a reasonable amount of reserve power to operate the gas sensor and radio module in case a potential fire is detected. As supercapacitors have an expected lifespan of 10 years or more, the sensors are essentially maintenance free. This allows for an expected lifespan of the sensor between 10 and 15 years.

Supercapacitors have a high capacity but a small maximum voltage of 2.7V so a series of capacitors are loaded to 4V. Capacitors are fully charged to 5.2V.

Info

Power supply is stored in supercapacitors rather than rechargeable batteries as rechargeable batteries can ignite. Using batteries would defeat the purpose of a wildfire detection system.

Silvanet Mesh Gateway

The Dryad *Silvanet Mesh Gateway* extends the Silvanet Network to allow for large-scale deployments of Silvanet Sensors throughout large forested areas.

Silvanet Mesh Gateway

Large deployments of standard LoRaWAN networks are typically beyond the reach of the standard single-hop direct connection between sensors and gateways. Messages from Silvanet sensors hop from Mesh Gateways to Mesh Gateways until messages reach the Silvanet Border Gateway(s). Consequently, Silvanet Networks can be extended to large deployments beyond the reach of the sensors.

The patent-pending architecture uses a multi-hop mesh network of Gateways interconnected with LoRa and each serving as a standard LoRaWAN gateway to Silvanet Wildfire Sensors and 3rd party sensors.

Key features

- Provides range extending capabilities by using the same LoRaWAN network as the sensors to receive and forward messages.
- Placed in the forest itself, forming a mesh network with a typical distance of 2-6 km depending on topology and physical placement of the Mesh Gateways.

- Does not require direct 4G/LTE-M radio or Ethernet connectivity which ensures low power consumption supported by the built-in solar panel.
- Supports FUOTA (Firmware Update Over-the-Air) to allow its firmware to be updated remotely as required.
- The typical coverage area of a single Mesh Gateway is between 2 to 6 km, depending on the physical terrain, the density and type of forest.
- Each Mesh Gateway supports up to 100 sensors.

Info
As the Silvanet Mesh Gateway is proprietary to Dryad, the device is not open to 3rd party applications.

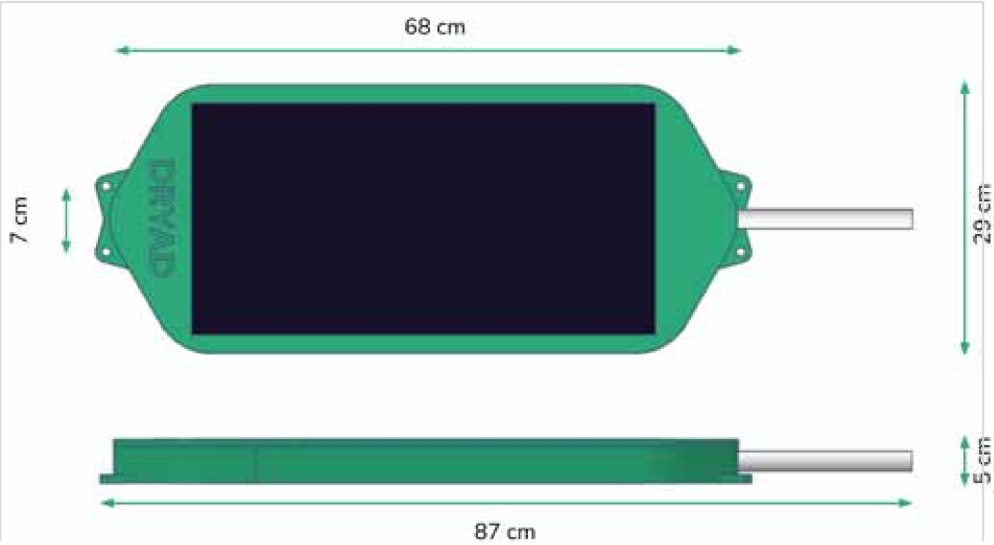
Connectivity

Each forest is unique. Different topology, difficult terrain, mountains, valleys, any feature that blocks transmissions are some of the many challenges facing quality connectivity.

However, the Mesh Network uses LoRaWAN (Long Range Wide Area Network) to overcome transmission obstacles within a forest. LoRaWAN is a technology built on top of LoRa, a patented frequency modulation ideal for low-power, wide area networks such as required by Dryad Silvanet.

Dimensions

The dimensions of the Silvanet Mesh Gateway are (LxWxH) 68 cm (87 cm with antenna) x 29 cm x 5 cm and weighs 2.8 kg.



Mesh Gateway dimensions

Range

The Silvanet Mesh Gateway can communicate with other Gateways (Mesh / Border Gateways) in a range of several kilometers. The actual range may vary depending on environmental conditions.

Mesh Gateway range

Power consumption

The Mesh Gateway has low power consumption which is supplied by its built-in solar panel to provide its daily energy needs. The power consumption is calculated to be 3997Ws.

Power supply

Due to the reduced power consumption compared to a Border Gateway, it requires a smaller solar cell size of 50 X 25 compared to the Border Gateway.

Connecting to Border Gateways

Mesh Gateways automatically register with the Silvanet Cloud during the deployment process.

Silvanet Border Gateway

The Silvanet Border Gateway provides connectivity between the Silvanet Mesh Network and the Silvanet Cloud. The Border Gateway communicates with the Silvanet Cloud through the Internet to relay messages from sensors via the Mesh Network.

It is typically placed at the edge of a forest and, ideally, near a power supply. However, these gateways are LoRaWAN compliant which means they can communicate directly with Silvanet sensors, if within range.

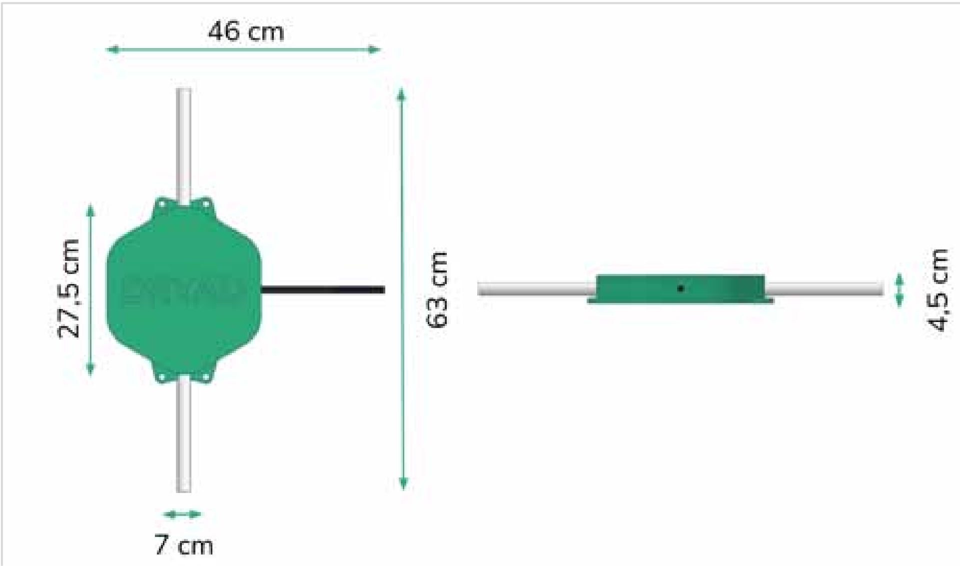
Silvanet Border Gateway

Key features

- Connects to Mesh Gateways and sensors via a LoRaWAN mesh network.
- Connects to the Internet using Mobile networks, Ethernet or SWARM satellite.
- Wireless connectivity is provided by its built-in LTE-M radio (using 4G/LTE-M with 2G/GPRS fallback).
- Wired connectivity is provided by its built-in Ethernet adapter.
- For remote deployments without mobile network coverage and no access to mains power, it has built-in support for connecting to the SWARM satellite network. Furthermore, it can operate on mains power or powered by a solar cell.
- Supports FUOTA (Firmware Update Over-the-Air) to allow its firmware to be updated remotely as required.
- The typical coverage area of a single Mesh Gateway is between 2 to 6 km, depending on the physical terrain, the density and type of forest.
- Each Border Gateway can support the deployment of up to 20 Mesh Gateways.
- Uses mains power supply through PoE (Power over Ethernet). If PoE is unavailable, the solar panel included with the device can also provide for its daily energy requirements.

Dimensions

The dimensions of the Silvanet Border Gateway are (LxWxH) 27.5 cm (63 cm with antennas) x 46 cm (with SWARM antenna) x 4.5 cm and weighs 1.3 kg.



Border Gateway dimensions

Range

The Silvanet Border Gateway can communicate with other Mesh Gateways and Border Gateways in a range of several kilometers. The actual range may vary depending on environmental conditions.

Border Gateway ranges

Communication

Mesh Network connectivity

Using LoRaWAN, the Border Gateway communicates with Mesh Gateways and directly with sensors, if they are within range. The Border Gateway receives messages from sensors via one or more Mesh Gateways and forwards them to the Silvanet Cloud via the Internet.

Internet Connectivity

The Border Gateway provides Internet connectivity to the Silvanet Cloud through either LTE-M, Ethernet and Satellite.

- Ethernet (wired - recommended)

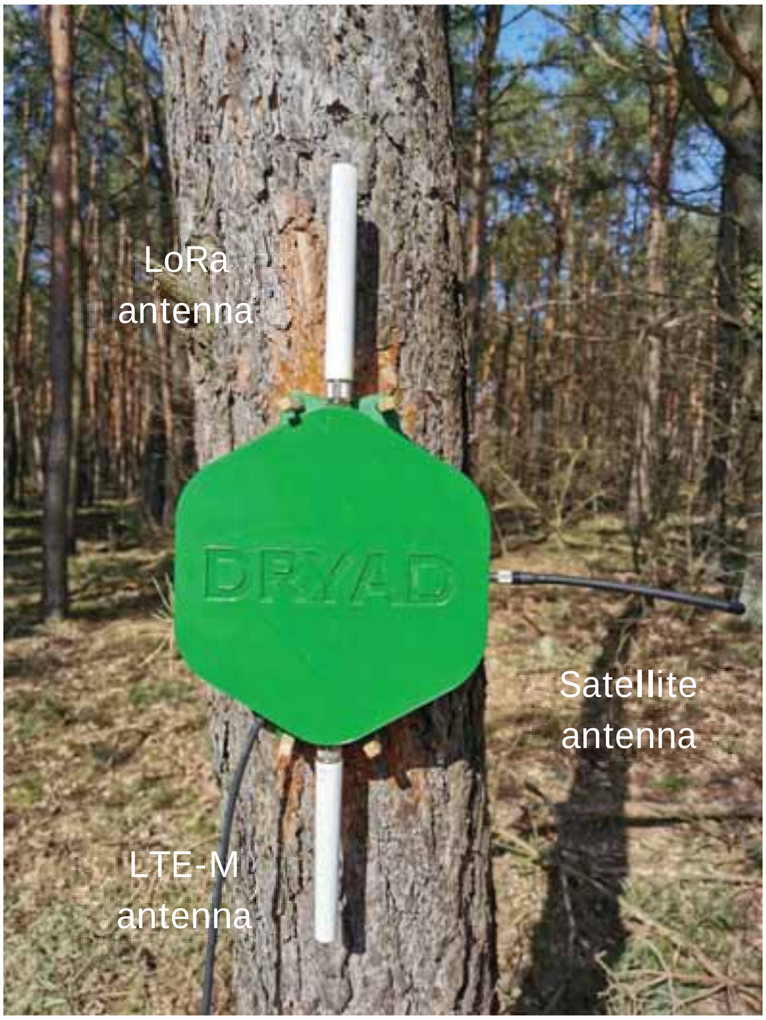
  We recommend using the Border Gateway's built in Ethernet connectivity which requires access to a router. The Gateway supports Power over Ethernet (PoE).

- LTE-M/2G (mobile)

  The Border Gateway provides built-in support for LTE-M, which requires access to a 4G network with 2G fallback (GPRS). LTE-M (Cat-M1) is suitable for IoT. An LTE-M antenna is provided to connect to a 4G network.

- SWARM Satellite (backup)

  Should Ethernet and LTE become unavailable or if the Border Gateway is deployed in a remote location, a SWARM antenna is provided for Satellite uplink using the SWARM satellite network. Messages sent by SWARM are only Alerts. Dependence on a Satellite uplink should only be used for remote deployments where there is no mobile network coverage AND no access to mains power.



Silvanet Border Gateway antennas

Firmware updates (FUOTA)

The Border Gateway supports FUOTA (Firmware Update Over the Air) with high flexibility. Large file transfers are successfully made securely and reliably even with eventual interruptions of the power supply and, consequently, sensor operation.

Firmware is updated using a chunked image transfer (no compression). All Silvanet sensors in a Site are updated at the same time using Multicast. To do this the LoRaWAN Network Protocol is temporarily switched to Class B which allows two-way communication.

To cope with low power and the various regional regulatory requirements, both the downlink fragment size as well as the periodicity are highly configurable allowing for stretching a FUOTA process even to a week.

Power Consumption

The Silvanet Border Gateway requires an *increased* power supply compared to the Silvanet Mesh Gateway. All components of the Border Gateway are assumed to be always on as it needs to listen to any messages sent by Mesh Gateways and/or sensors. To be always on it needs a constant power supply, either through a mains power supply or using its external solar panel.

Power supply

Continuous (24 hour) operation of the Border Gateway requires a power supply of 5415Ws. We recommend providing a power supply using PoE (Power over Ethernet) connected to a mains power supply. If PoE is unavailable, the solar panel included with the device can also provide for its daily energy requirements.

Solar Panels

The Border Gateway includes an external solar panel that is 45cm by 45cm and is permanently connected to the Border Gateway. This provides a continuous power supply to charge the supercapacitors.

The solar panel ensures charging capabilities. This guarantees a power supply to the Border Gateway should a power outage occur for an extended period, such as ten hours or even two days.

Supercapacitors

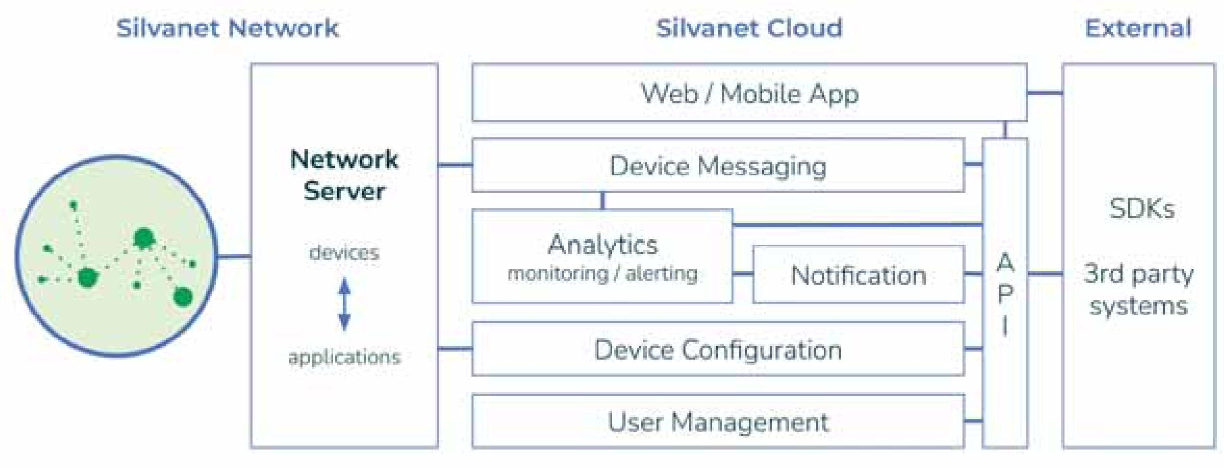
The Silvanet Border Gateway uses supercapacitors to provide the 5415Ws power supply (5415Ws). This type of capacitor provides a large amount of power for a short duration and is continuously recharged using an external power supply, either Mains (directly or via a PoE) or solar panel.

If the solar panel is the main source of power, the supercapacitors allow the device to continue receiving power for several hours if the solar panel loses generating capacity (no sunlight) or if a power outage occurs in the case of mains power supply.

Info
Power supply is stored in supercapacitors rather than rechargeable batteries as rechargeable batteries can ignite. This would defeat the purpose of a wildfire detection system.

Silvanet Cloud Platform

The *Silvanet Cloud platform* captures data served by the Silvanet Mesh Network and received from the Silvanet sensors. It connects with the Site Management app, which is a web application, as well as the Deployment app which is run on a Smartphone. Data that is captured and served by the Silvanet Cloud is accessible wherever a user has Internet access.



Silvanet Cloud Platform

Each Dryad customer is provided with their own username and password to access the Silvanet Cloud. Dryad currently manages access to the Silvanet Cloud. Each new user must be added by request to Dryad only.

From the user's perspective, this gives registered users access to a client which is a collection of Sites, where each Site is scalable to allow for adding more Silvanet devices as well as additional users. Typically, a customer has only one Site, but customers can request multiple sites that are geographically dispersed.

Info
Sites are currently added by Dryad internal Admins. In the future, a Site Admin will be allocated to specific users who will be able to create sites for clients and to create users.

Silvanet Suite Apps

A user interacts with the Silvanet Cloud Platform and by extension their deployed sensors and gateways using two Silvanet Suite apps, one web-based and the other an app running on the user's Smartphone:

- The *Site Management app* (dryad.app) is accessed through a browser and is used to plan deployments and view environmental data from all sensors in a Site. It also shows if any device is active, inactive or has detected a fire.

  The name of a Site can be changed as required. Also, settings can be changed, such as Metric/Imperial unit systems, date format and time format.

- The *Dryad Deployment app* is used to deploy Silvanet sensors and gateways in the planned location of these devices.

Site Management app

The Site Management app is used to plan deployments and to monitor the devices in the site. It is connected to the Silvanet Cloud which receives data from the sensors via Mesh Gateways and Border Gateways. This data is then displayed in the Site Management app.

Site Management app

A Site is the geographical area where a network of Silvanet sensors and gateways are deployed to monitor the forest. The Site Management app (dryad.app) displays all Sites that Dryad has created and administered for you. Using your username and password, you are granted access to all Sites to which you are registered.

Accessing Site Management

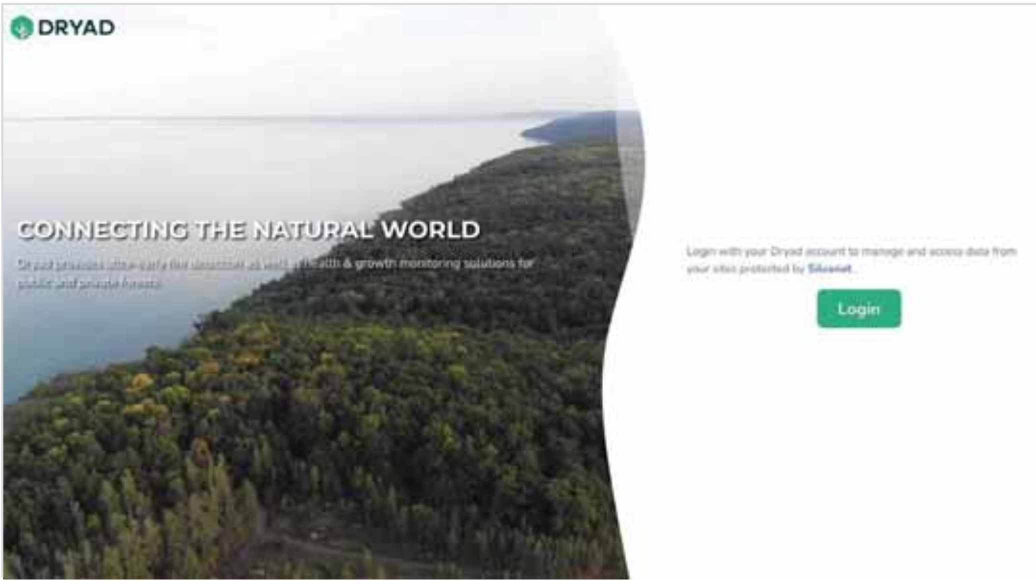
Accessing the Site Management app requires a user to be registered with Dryad. After registration, a registered user is provided with login credentials. The user enters their credentials in the log in page, then is required to change their password.

Info
This section assumes you have been registered with Dryad and have access rights to the Site Management app. Contact Dryad if you have not received your access credentials.

To access the Site Management app:

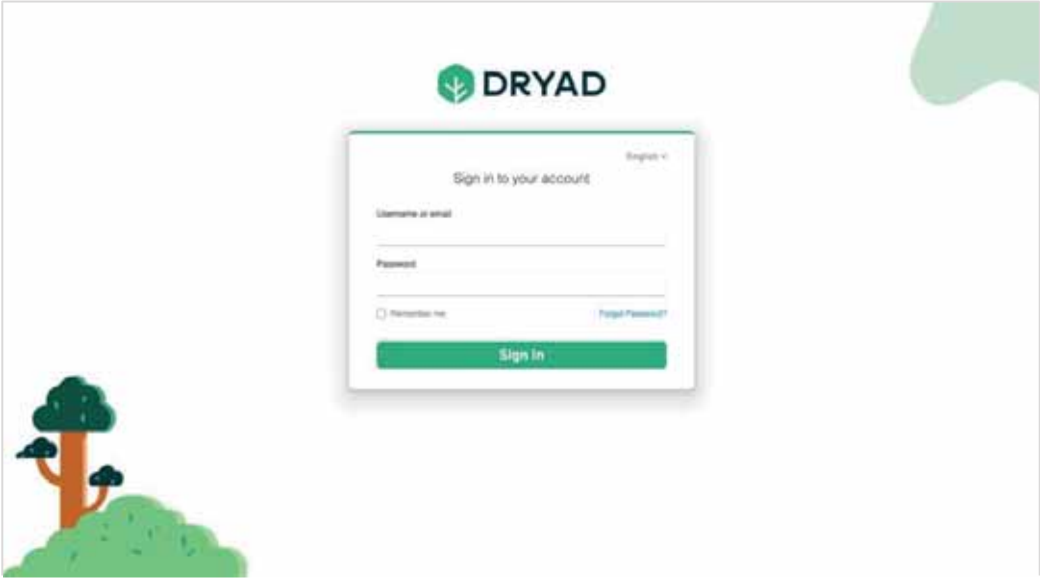
1. Ensure you are a registered user with Dryad and have the required user credentials.

2. Go to dryad.app, then select **Login**.



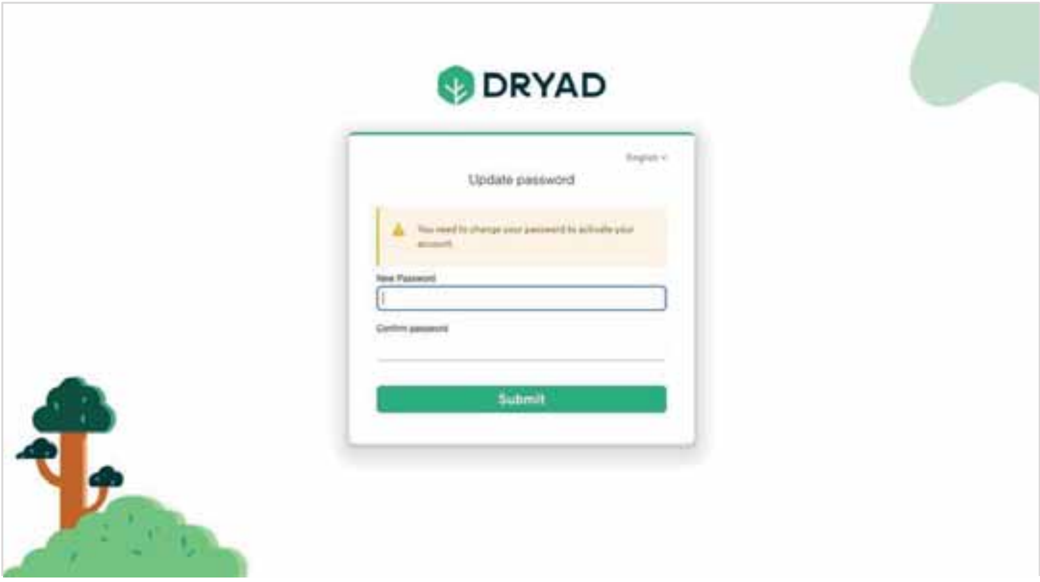
Site Management login

3. In the Sign in form, enter your username and password provided to you by Dryad, then select **Sign In**.



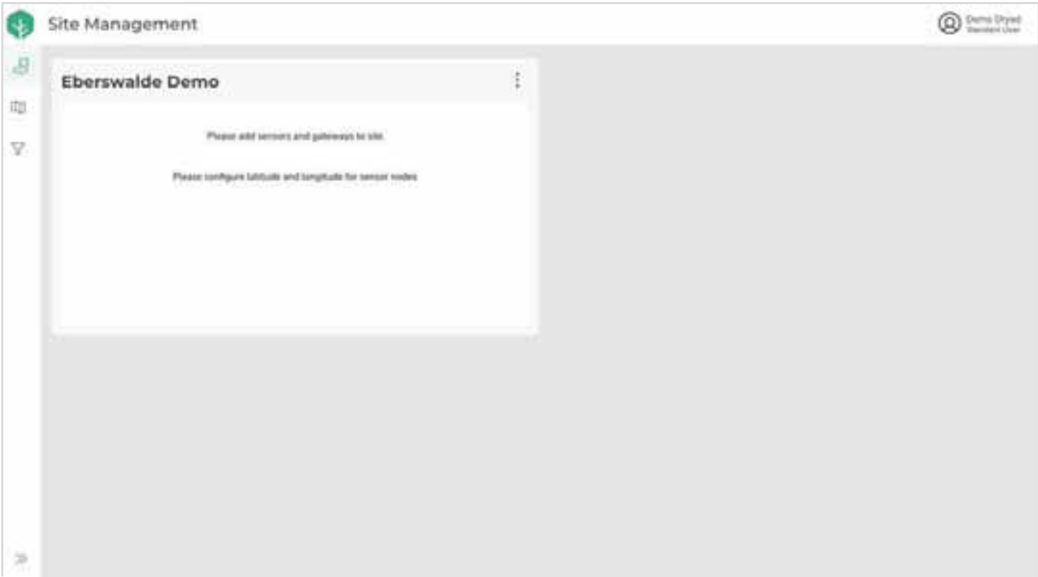
Enter your username and password to sign in

4. If this is your first log in, you are required to change your password. You cannot change your username.



Update password

5. After logging in, the Site Management Dashboard appears showing the *Sites* view.



Site Management dashboard

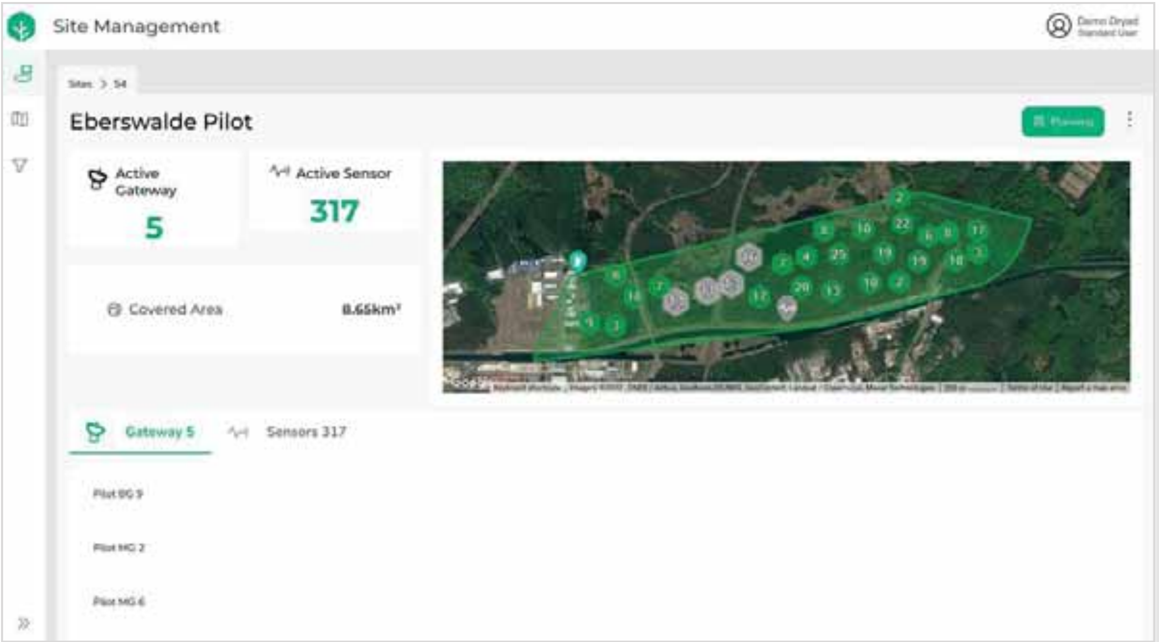
6. All sites that you have access to are displayed on this page.

Views

The Site Management dashboard provides access to three view options: a *Sites* view, a *Maps* view and a *Devices* view.

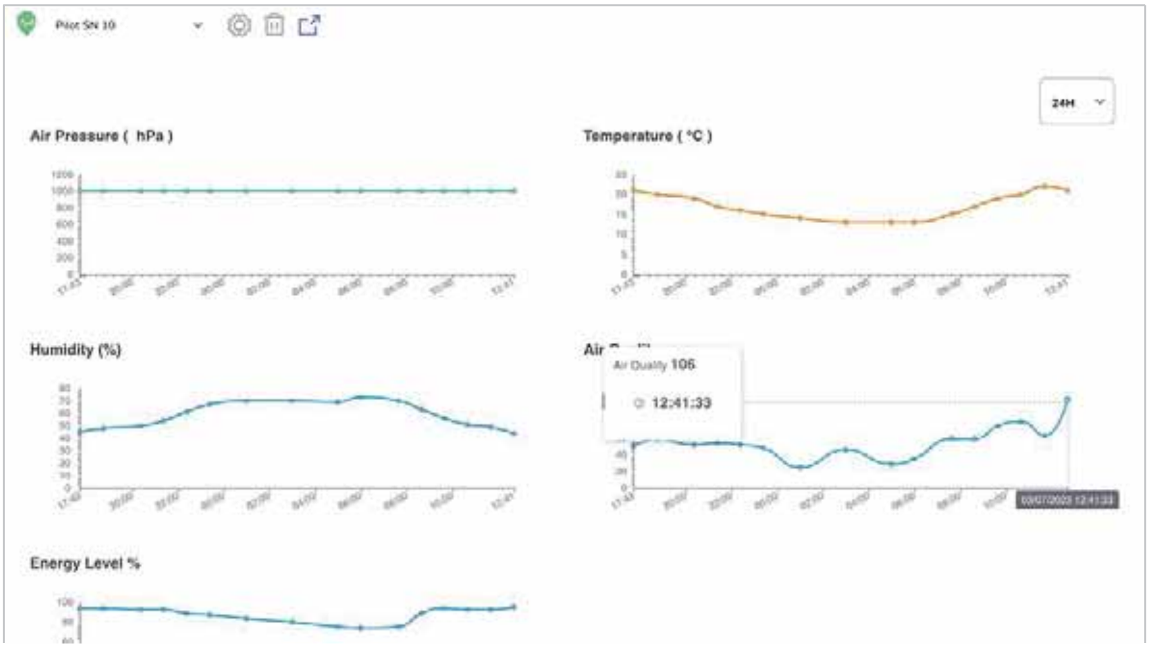
Sites view

The *Sites* view displays all Sites that a user has rights to administer and manage. Selecting the name of a Site opens the Site Dashboard.



Sites dashboard

The Site dashboard allows a user to drill down and view the current readings from a sensor, including Air Pressure (hPa), Temperature (°C), Humidity (%) and Air Quality. It also shows the current Energy Level of the sensor superconductors (%).



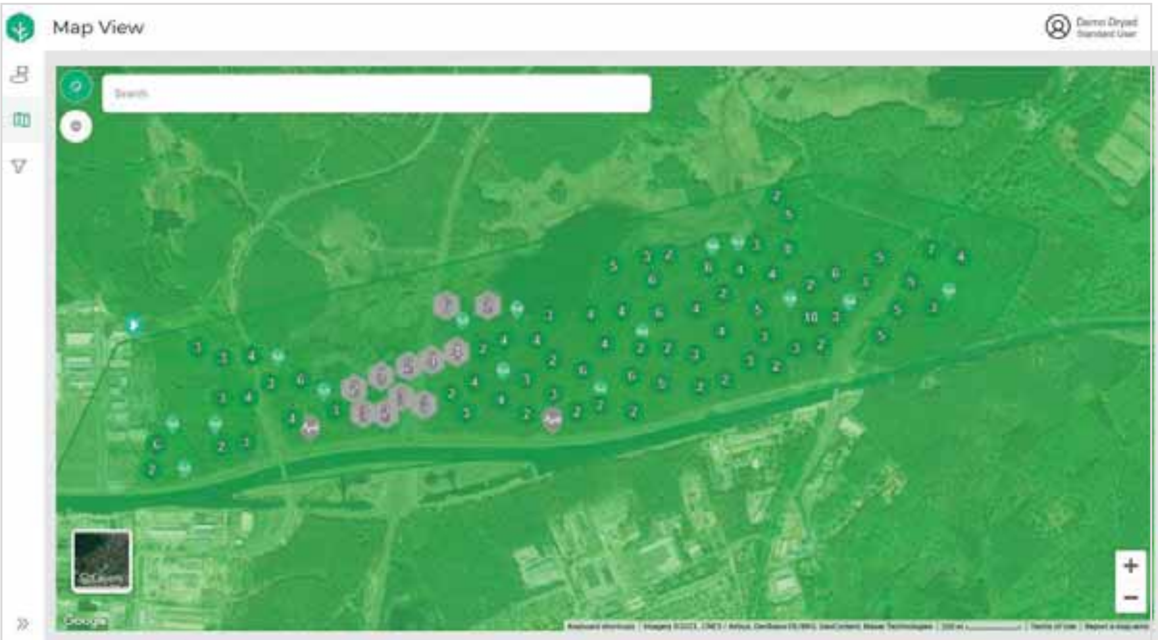
Sensor readings

Map view

The *Map* view provides a convenient view for selecting sites. If many sites are managed, this allows for a quick selection of the site based on a map location. Displaying a site shows the status of each deployed device.

Map view

The *Map* view also provides an overlay of temperatures sourced from Google Maps which shows areas of higher levels of fire risk.

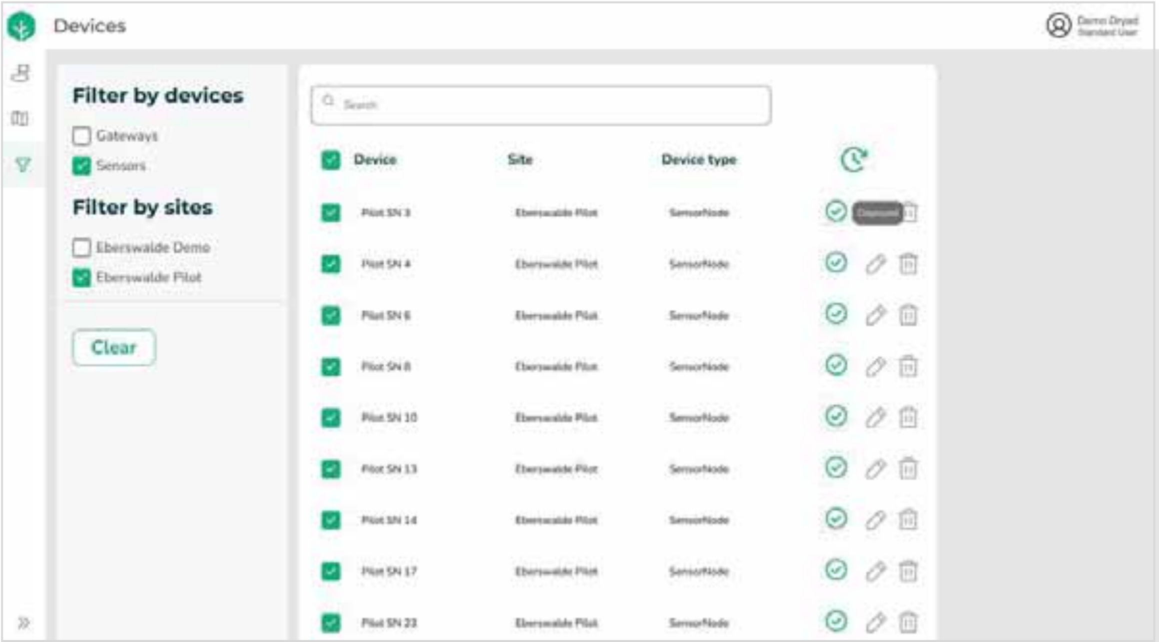


Map View with fire risk overlay

Device view

The *Device* view provides a quick search function to find specific sensors or gateways using the device ID. Searches can be filtered by device or by site.

Selecting a sensor displays in a sidebar the current data from the sensor. You can select a data time range showing values over 5, 7, 12 or a 24-hour timescale.



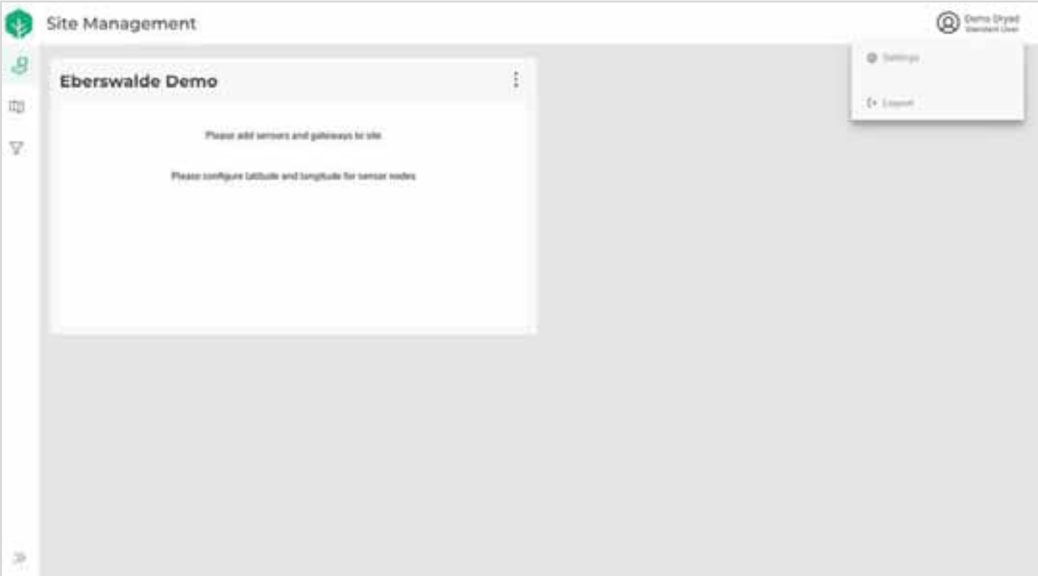
Device View

Change user settings

You can change the units displayed in the Site Management app, as well as the Date and Time formats.

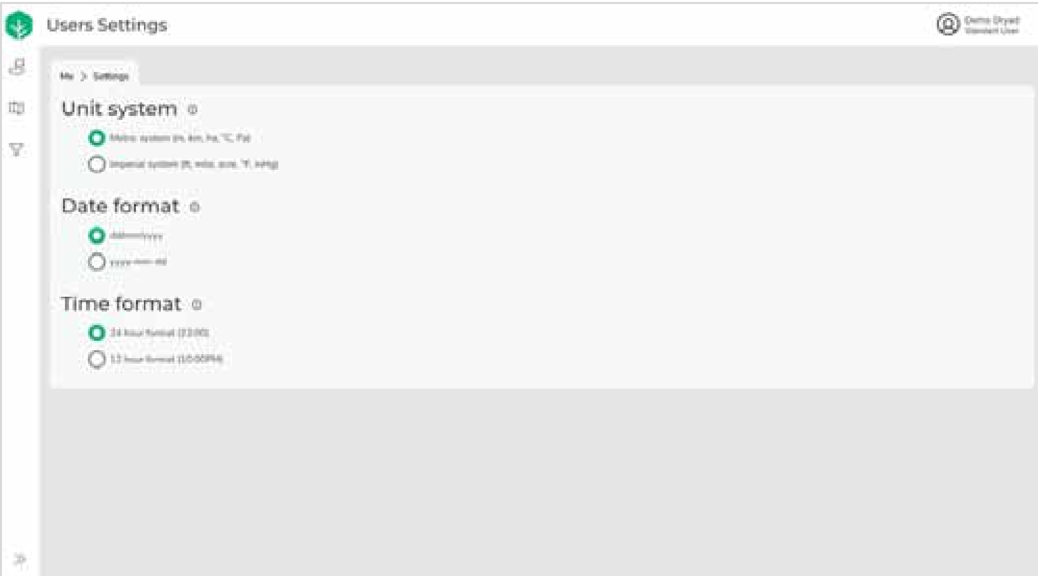
To change user settings:

1. Hover over the login name on the upper right corner of the app to reveal a menu, then select **Settings**.



User settings menu

2. Change settings as required.



User settings

3. Select the Dryad logo to return to the main dashboard.

Edit a Site name

If required, you can change the name of a Site.

To edit a Site's name:

1. From the Site Management homepage, select the Site ellipsis menu, then select **Edit**.

2. In the **Edit Name** field, rename the Site.

3. Select **Submit**.

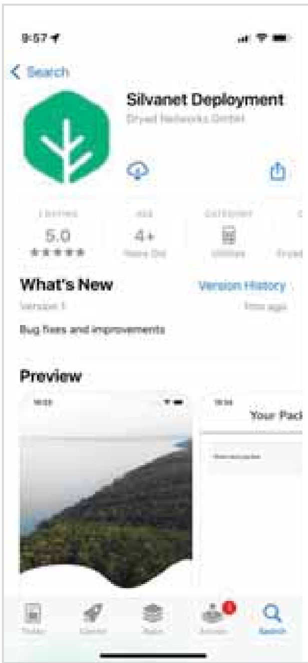
Silvanet Deployment App

The *Silvanet Deployment app* displays Packets assigned to users who use this app to locate the planned deployment location (GPS coordinates) of the sensors and gateways. Once located, the user scans the QR Code of the device into the app to provide the exact GPS coordinates (longitude and latitude) of the sensor or gateway in the app.

Info
The Silvanet Deployment app is available on both Apple App Store and on Google Play.

To install the Deployment app:

1. Search for Dryad on your Smartphone's App Store or Google Play.



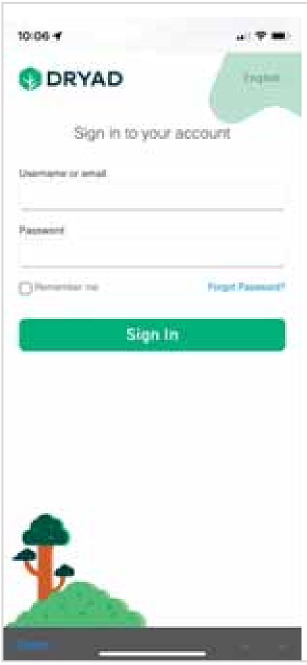
Silvanet Deployment app

2. Install the app on your Smartphone.

3. Select **Login** to continue.

Click Login

4. Enter your registered email address and password.



Enter login credentials

5. The Packets page appears listing Packets that have been assigned to you.

Packets page

6. After opening a Packet and locating the deployment location, the forest worker adds the Device ID, GPS coordinates, notes and a picture of the device's label in the app. These details are then saved to the Silvanet Cloud.

Installation completed

Deployment planning

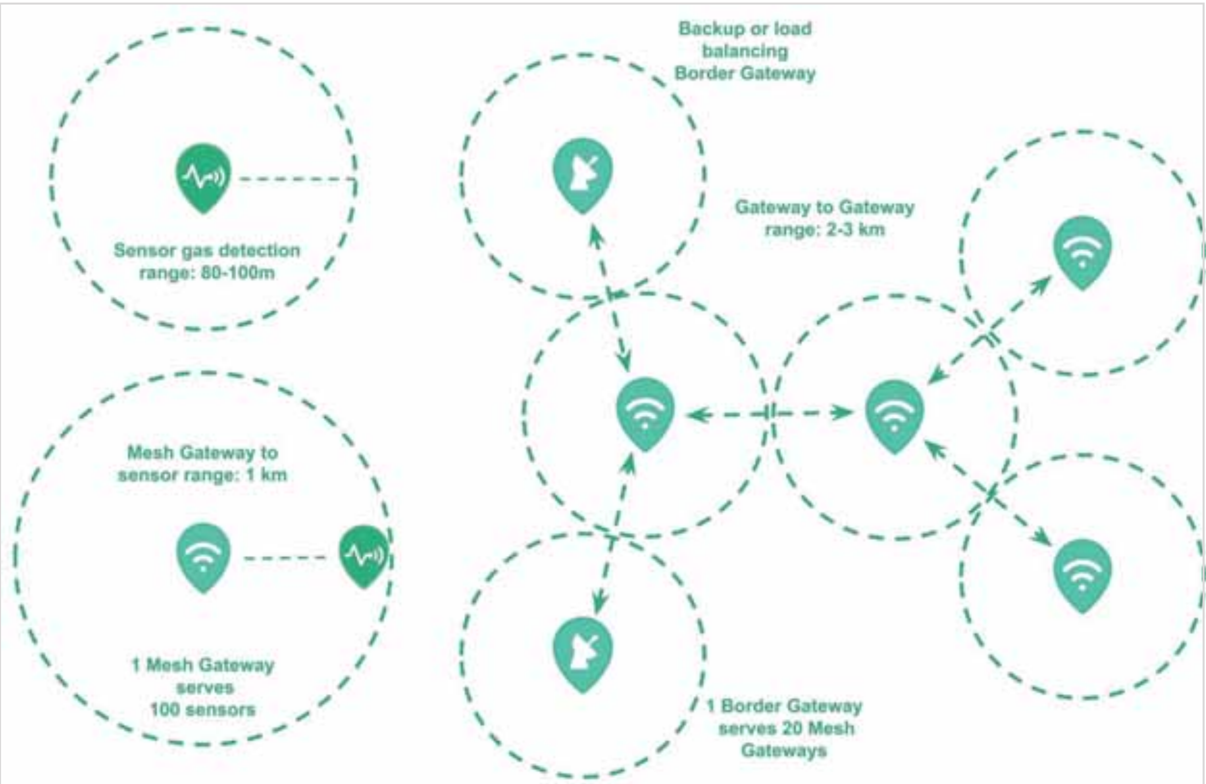
Deploying the Silvanet devices in a forest location require significant planning to achieve effective fire detection. Take time to read the topics in this section to learn how to plan your deployments of the Dryad Silvanet Suite.

Deployment guidelines

To plan for a successful deployment of the Dryad Wildfire Detection System, ensure the correct ratio of devices, determine sensor deployment density and carefully follow the Mesh Gateway and Border Gateway guidelines.

Device ratios / ranges

This section describes the ratios and ranges of Silvanet sensors, Mesh Gateways and Border Gateways in a typical Silvanet System deployment. Device ratios and ranges can be illustrated as follows:



Device ratios and ranges

Device Ratios

A single Mesh Gateway can support up to 100 Sensors while a single Border Gateway can support up to 20 Mesh Gateways.

When planning Pilot or Live installations, we recommend the following ratios:

Devices	Ratio	Description
# of sensors to Mesh Gateways	100:1	Sensors: Mesh Gateway
# of Mesh Gateways to Border Gateways	20:1	Mesh Gateways: Border Gateways

Device ranges

When determining the location of devices in a site, ensure sensors and gateways are well within range for sending and receiving messages.

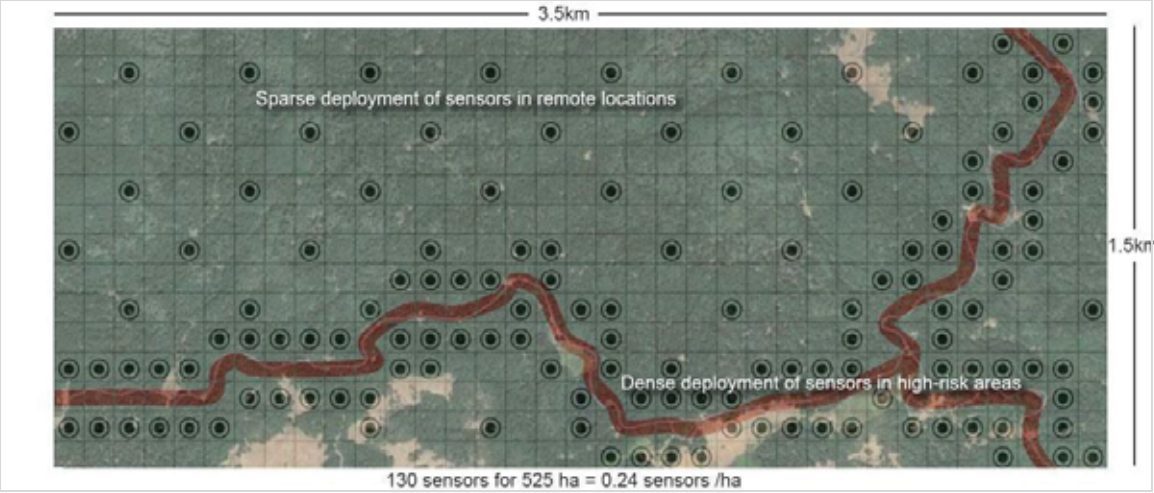
Info
Range values are dependent on the Site topology such as hills, valleys, density of trees and structures in the forest deployment locations.

Device ranges are listed in the following table.

Devices	**Range**
Border Gateway to Mesh Gateways	2 km to 3 km
Mesh Gateway to Mesh Gateway	2 km to 3 km
Sensor to Mesh Gateway	1 km
Sensor gas detection	80 m to 100 m

Sensor density

Sensor density is based on the **level of human activity** near a forest. This can include hiking paths, rail lines, roads, bridges, homes, or other locations where it is expected humans have interactions (or not) with a forested area. Density can be determined by **Density values per hectare**.



Deployment density example

Human activity level

When planning sensor deployments, the amount of human activity in an area determines the distances between sensors for that area:

- High human activity: 80-100m

  Dense deployment of sensors in high-risk areas. In areas with increased human interaction, plan for a dense deployment of sensors. We recommend a short distance between sensors - approximately 80 to 100m between sensors.

- Low human activity: 400 to 500m

  Sparse deployment of sensors in remote locations. In areas with little to no human activity, the distance between sensors can be increased to approximately 400 to 500m between sensors.

With this approach of variable density, the overall system cost can be reduced while maintaining an overall good wildfire detection time and rate.

Additionally, sensor deployment density determines location guidelines for Mesh Gateways and Border Gateways.

Density values per hectare

More than 80% of wildfires can be attributed to human activity, depending on the region. In remote areas, natural events such as lightning strikes usually cause wildfires.

Wildland Urban Interface (WUI) is a location where "*burnable structures are interspersed within wildland fuels*". A broader term is "*Wildland Industrial Interface*" where industrial infrastructure (such as roads, powerlines and railways) intermingles with wildland fuels (source: Canada Wildfire). WUI as defined by the United States Fire Administration:

The WUI is the zone of transition between unoccupied land and human development. It is the line, area or zone where structures and other human development meet or intermingle with undeveloped wildland or vegetative fuels.

Based on WUI, we recommend the following density values:

- **Dense**: 0.7 devices per hectare (0.7/ha).

  Dense deployment of sensors next to roads, campsites or parking lots.

- **Sparse**: 0.1 devices per hectare (0.1/ha).

  Sparse deployment of sensors in remote locations such as deep within forests.

Mesh Gateway guidelines

Use the following guidelines when planning the deployment of Mesh Gateways in your Site.

Item	Guideline	Description
Device ratio	1 Mesh Gateway to 100 sensors	See Device ratios/ranges.
Location	Maximum 1 km radius from sensors	Place Mesh Gateways in locations that enable them to cover nearby sensors in a radius of approximately 1 km.
Range	Several kms distance from other Mesh Gateways/Border Gateways, depending on topology.	Mesh Gateways can communicate over longer ranges than sensors. Depending on the topology and type of forest, Mesh Gateways can communicate from 2 km to 3 km from other Mesh Gateways/Border Gateways
Sunlight	Install on a hillside or sunny location	Install Mesh Gateways on a hillside or sunny location. It needs to be installed facing the sun at 12:00 noon (northern or southern hemisphere). If installed ong a tree, it should not be covered by branches. To receive maximum sunlight, it is best installed on a pole, if possible.
Height on trees	3 m from forest floor	To protect the Mesh Gateway from human or animal interference and to give a better line of sight to other Getaways within range, install the device 3m above the forest floor.

Border Gateway guidelines

When planning Border Gateway deployments, consider how you plan to provide the device with a reliable power supply and continuous access to the Internet. This section provides recommendations and types of deployment scenarios to assist you.

Planning guidelines

The LTE-M radio in the Border Gateway uses a reasonable amount of power so the power supply needs to be addressed when locating a site to mount the device. Ideally, it should be installed in a location with mains power.

Use the following guidelines when planning the deployment of Border Gateways in your Site.

Item	Guidelines	Description
Location	Several kms distance from Mesh Gateways, depending on topology	Place the Border Gateway in a location no more than 2-3 km from Mesh Gateways. Also, due to its connectivity to the internet, it requires more energy and the location should be chosen carefully. Ideally, it should be placed in a location with access to a reliable power supply (mains power) but it can also be powered by its pre-connected solar panel in off-grid locations.
Power supply	Reliable access to a power supply	Due to Internet connectivity and always-on requirements, the Border Gateway needs a reliable power supply. It can also be powered by its pre-connected solar panel in off-grid locations.
POE Requirements	Voltage range: 36V-57V	The Border Gateway requires a PoE Injector (Adapter) that provides a voltage range of between 36V and 57V. The PoE must be IEEE 802.3af compliant. |
Solar panel deployment	Towards sun at 12:00 (northern or	The pre-connected solar panel acts as a backup to charge the device's internal energy storage

Item	Guidelines	Description
	southern hemisphere)	(supercapacitors). If a loss of power occurs, the solar cell will keep the system running, thus keeping the Silvanet Network functioning. Select a location with direct sunlight (such as a hillside) and keep it free from branches that obscure direct sunlight. Ideally, it should be placed on a tree or pole away from other trees in the forest.
Internet connectivity	Use Ethernet for Internet connectivity (recommended)	The Border Gateway should be connected to the Internet using a fixed-Internet connection (Ethernet) but it can also be connected to the Internet using its built-in wireless connectivity (4G/LTE-M with 2G/GPRS fallback).
Maximize range	Place on a hillside to maximize range and sunlight (recommended)	The Border Gateway should be installed on a hill to maximize the range. If the Border Gateway is to be powered by solar, select a sunny location with direct sunlight. If it is installed on a tree, the solar panel should not be covered by branches.
Satellite connectivity	Provide a clear line of site for SWARM Satellite backup	For satellite connectivity, the Border Gateway provides a SWARM antenna to connect the Silvanet Network to the Internet. It therefore needs a clear line of sight to connect to a satellite.
Backup	Provide a backup Border Gateway (recommended)	For larger deployments (greater than 1000 sensors) provide a backup Border Gateway.

Deployment scenarios

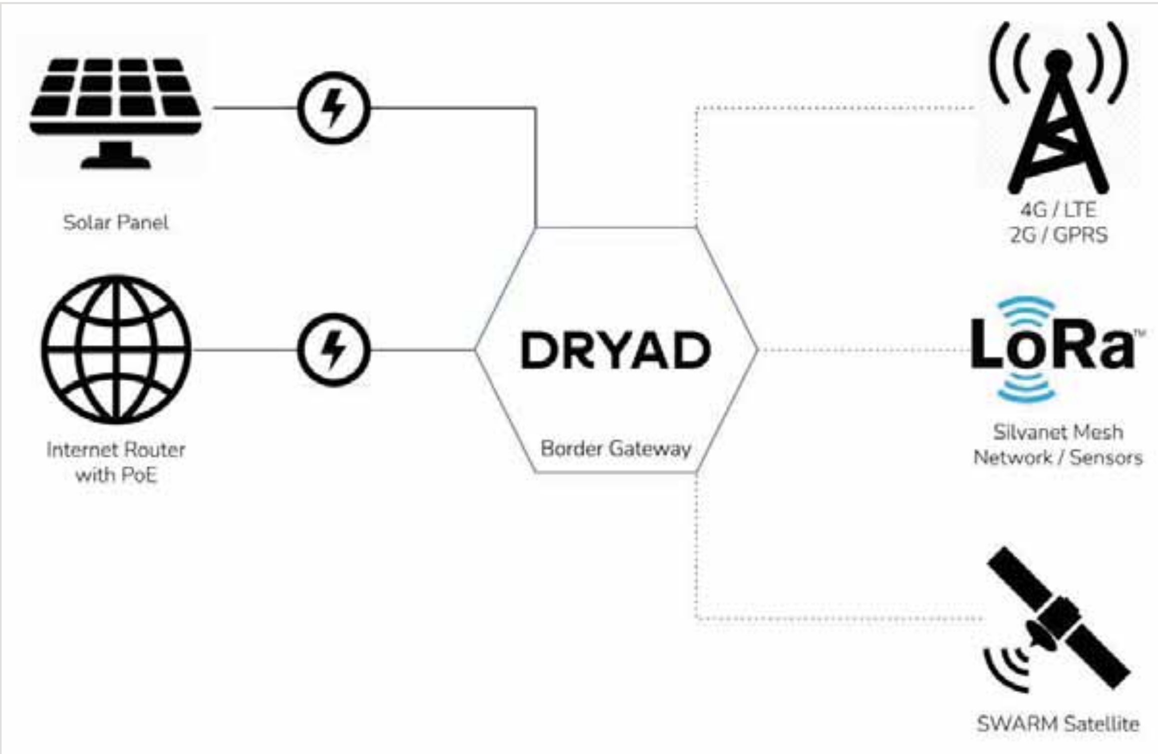
Depending on the availability of electricity and Internet, the following sections describe the possible scenarios for Border Gateway deployments.

Setup with a PoE-ready router

In a setup with a Power over Ethernet (PoE)-ready router, the Border Gateway obtains a power source from an Internet router that includes PoE. A separate PoE Injector is not needed.

This setup includes the following:

- Border Gateway connection: Connected to the router with a single Ethernet cable.
- Router type: Cable or ADSL router that includes support for PoE



Setup with a PoE-Ready Router

Feature	Description
Internet connectivity	The Border Gateway is connected to the Internet router using an Ethernet cable.
Power supply	The Border Gateway uses the PoE and an Internet connection provided by the router. In this setup, a separate PoE Injector is not needed.

Feature	Description
Backup	In case of power failure or loss of Internet connectivity through Ethernet, the Border Gateway can use its built-in 4G/LTE-M (or 2G/GPRS) mobile radio or its SWARM Satellite connectivity. In case of a power failure, backup power is provided by the solar panel.

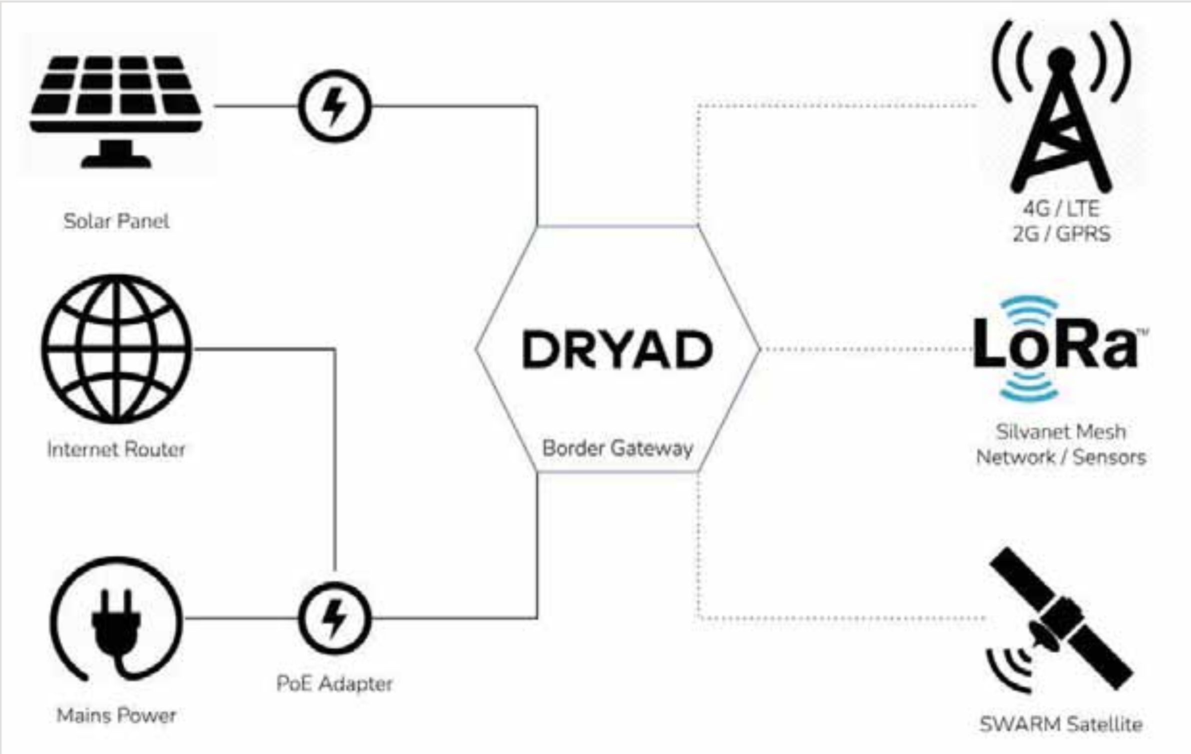
Setup with a router but does not support PoE

In a setup with a router that does not support PoE, the Border Gateway is connected to an Internet router such as a cable or ADSL router.

Note
The Border Gateway requires a PoE Injector (Adapter) that provides a voltage range of between 36V and 57V. The PoE must be IEEE 802.3af compliant.

This setup uses the following:

- Border Gateway connection: Connected to the LAN-port of the POE injector with an Ethernet cable
- PoE Injector: (*PoE Adapter*) plugged into a mains power supply.
- Router: Connected to the LAN-port of the PoE Injector with an Ethernet cable.



Setup with a Router (No PoE)

Feature	Description
Internet connectivity	The Internet router connected to the PoE Injector to provide Internet connectivity.
Power supply	The PoE Injector plugged in to the mains provides the power supply for the Border Gateway.
Backup	In case of power failure or loss of Internet connectivity through Ethernet, the Border Gateway can use its built-in 4G/LTE-M (or 2G/GPRS) mobile radio or its SWARM Satellite connectivity. In case of a power failure, backup power is provided by the solar panel.

Info

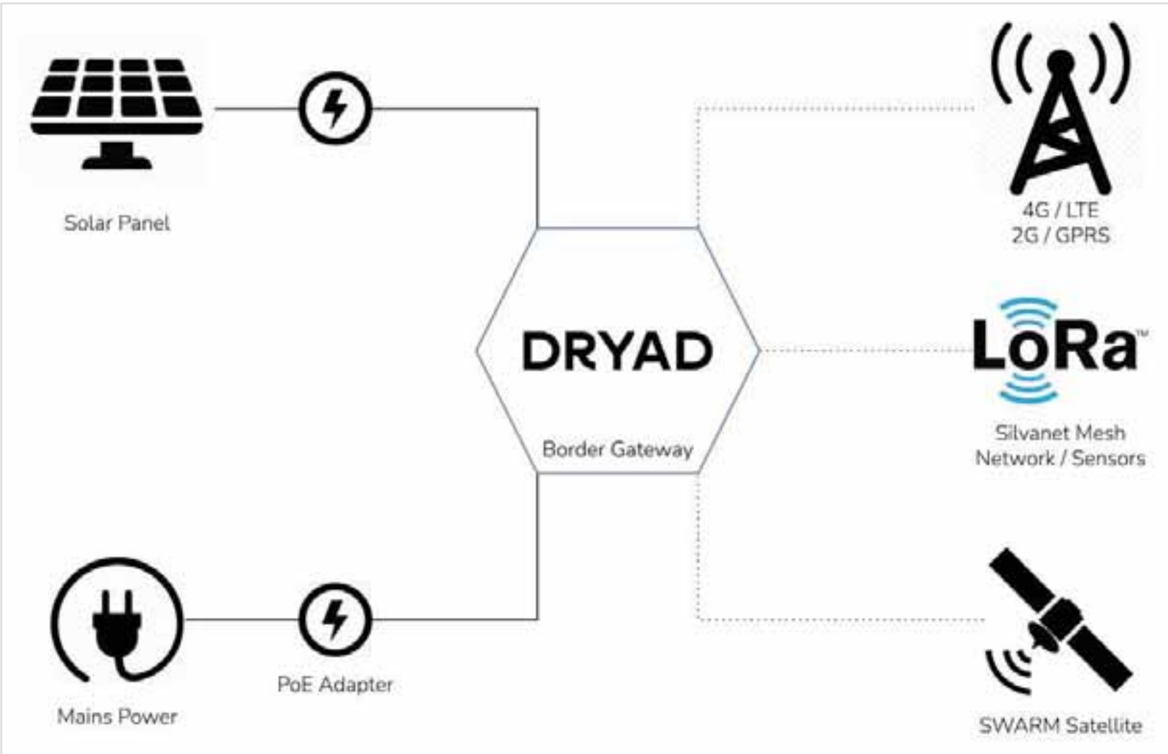
When using the built-in Ethernet connection, this setup is supported only in combination with a PoE Injector. The solar panel does not provide enough energy to support Ethernet connectivity of the border gateway.

Setup without router but with mains power

In this setup, the Border Gateway is deployed in a location without a fixed-line Internet connection (without a router) but does have mains power.

This setup uses the following devices:

- Border Gateway connection: Connected to the LAN port of the PoE Injector with an Ethernet cable.
- PoE Injector: Plugged into the mains power supply.



Setup without router but with mains power

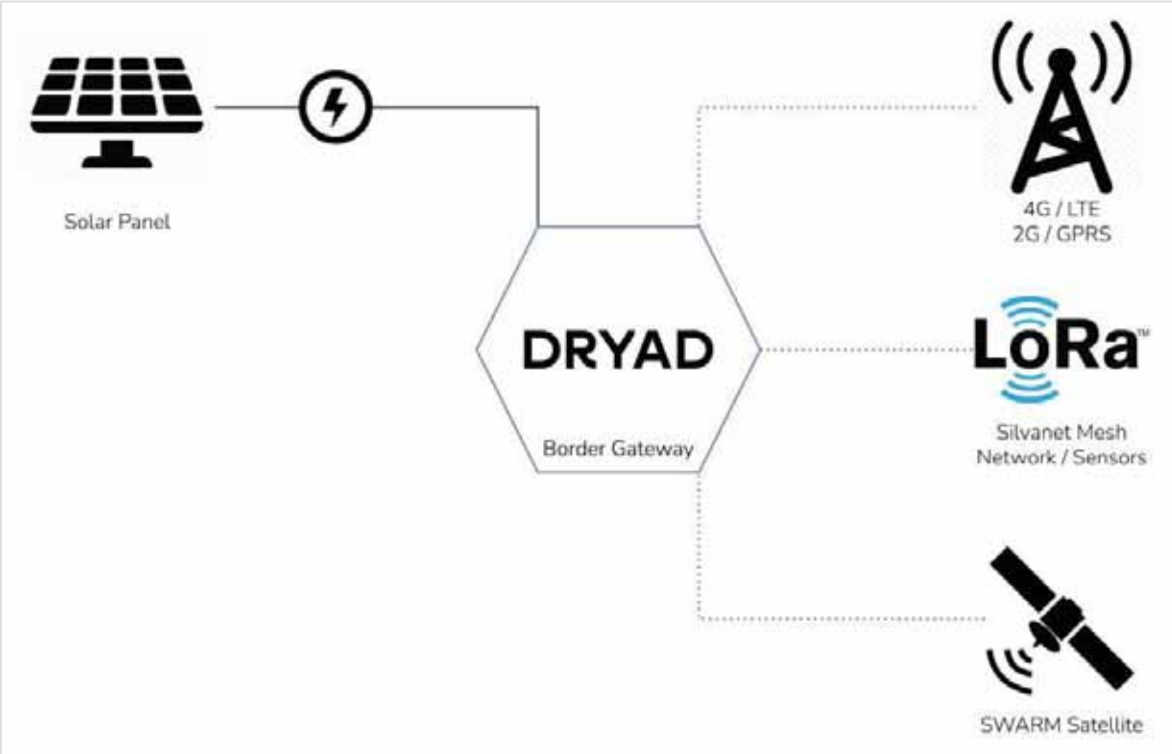
Feature	Description
Internet connectivity	Provided by the Border Gateway's built-in 4G/LTE 2G/GPRS radio.
Power supply	Powered by the PoE Injector plugged into a mains power supply.
Backup	In case of power failure or loss of Internet connectivity through Ethernet, the Border Gateway can use its built-in 4G/LTE-M (or 2G/GPRS) mobile radio or its SWARM Satellite connectivity. In case of a power failure, backup power is provided by the solar panel.

Setup without router and without mains power

Often Internet connectivity and a mains power source is unreliable in remote locations. Border Gateways deployed in these types of locations have neither fixed-line Internet connectivity or a reliable power supply. However, the Border Gateway can use its solar panel and a SWARM Satellite uplink to send Fire alert signals to the Silvanet Cloud.

This setup uses the following devices:

- Border Gateway: No connection to any router or mains power supply.



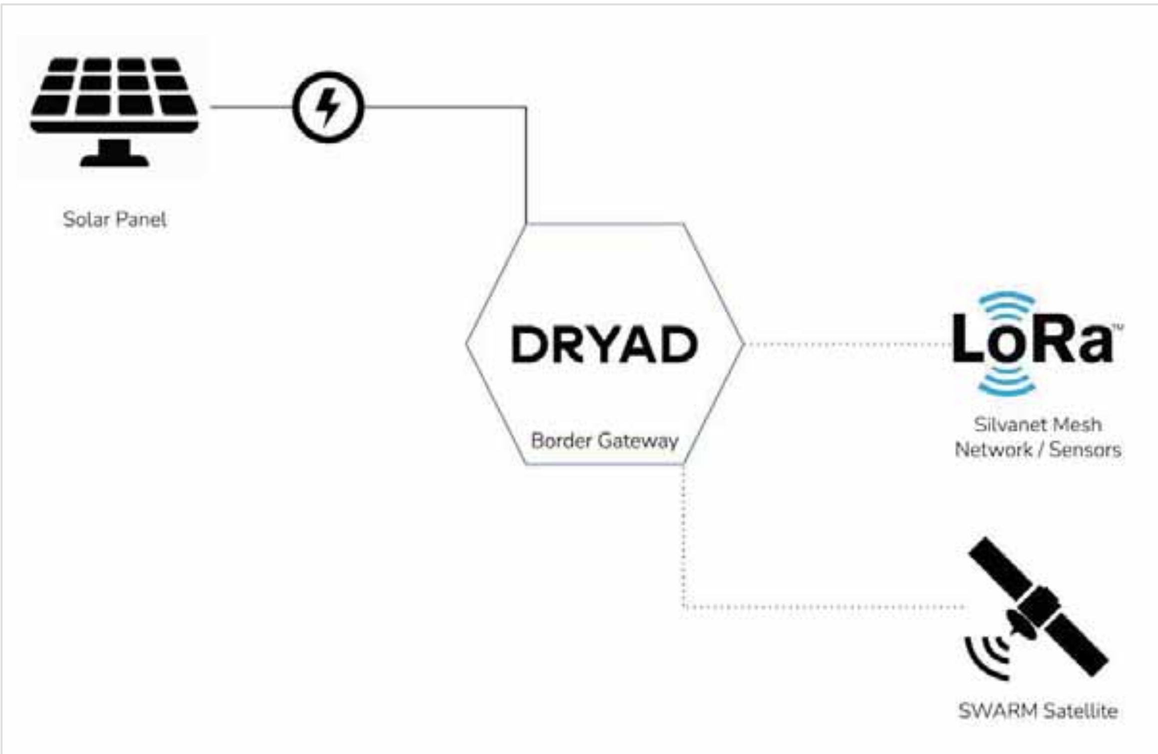
Setup without router and without mains power

Feature	Description
Internet connectivity	Provided by the Border Gateway's built-in LTE-M 2G/GPRS mobile radio if a mobile tower is accessible. Otherwise, it uses a SWARM Satellite uplink.
Power supply	Powered by the solar panel which charges the Border Gateway's internal energy storage. However, depending on the amount of sunlight, data transfer might be limited.
Backup	In case of power failure or loss of Internet connectivity through Ethernet, the Border Gateway can use its built-in 4G/LTE-M (or 2G/GPRS) mobile radio or its SWARM Satellite connectivity. In case of a power failure, backup power is provided by the solar panel.

Backup setup

Normally, as a fallback, the Border Gateway supports several methods to ensure uninterrupted Internet connectivity:

Loss	Backup
Loss of mains power supply	The Border Gateway is connected to the Internet router using an Ethernet cable.
Loss of Internet connectivity (Ethernet)	Due to loss of power or network failure, the mobile data connection (4G/2G) is used.
Loss of Internet connectivity (Ethernet and Mobile)	SWARM satellite uplink functions as an emergency backup. In this situation, only Fire alarms are sent. As the system runs in power saving mode, no other sensor data can be transmitted.



Warning

Should the installation location of the Border Gateway have neither a mains power supply nor access to a mobile network (LTE-M 2G/GPRS), the Border Gateway can still transmit minimal messages to the Swarm Satellite. However, messages are restricted to Fire Alerts only. This scenario is applicable, for example, where natural disasters like thunderstorms or earthquakes bring down Internet connectivity.

Deployment types

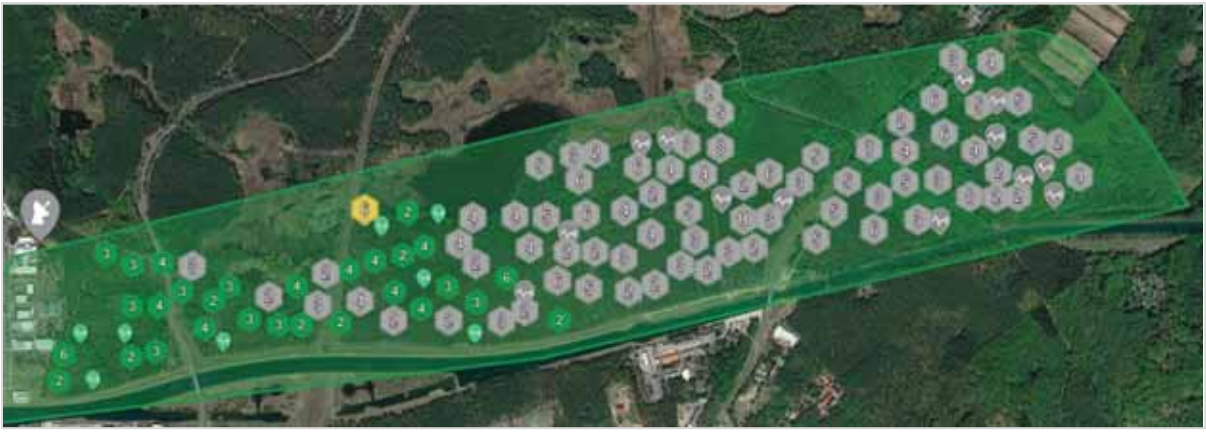
Dryad recommends using two types of deployments to help you plan for and implement the Dryad Wildfire Detection System:

- **Pilot Deployment**: Consists of 400 sensors and a minimum of 6 Mesh Gateways and 1 Border Gateway. This type of deployment is used to validates the scalability of the Silvanet System in a realistic environment.
- **Live Deployment**: Result of a Pilot deployment is used to determine the required number of sensors and gateways to effectively cover the entire forest location of the Site.

Pilot deployments

A Pilot deployment validates the scalability of the Silvanet System in a realistic environment. 400 sensors and at least 6 Mesh and Border Gateways are used to monitor an area of about 400 to 500 hectares.

The following shows an example Pilot deployment with the Border Gateway on the edge of the forest and sensors connected via Mesh Gateways to the Border Gateway.



Example Pilot deployment

The Pilot Deployment typically includes the following devices with the required treenails and other accessories:

- 400 Silvanet sensors (installed using treenails or crop wire)
- 5 Silvanet Mesh Gateways (additional Mesh Gateways can be added depending on topology)

- 1 Silvanet Border Gateway (an additional Border Gateway is recommended for redundancy)

Guidelines

Use the following guidelines when planning Pilot deployments.

Guidelines	Description
Understand the terrain of the Site area	As the Pilot uses Mesh Gateways, the deployment area can be hilly, rocky and beside roadways. However, we recommend line of sight between Mesh Gateways and Border Gateways.
Sensor spacing	Sensor spacing can be 80 to 100 m between the sensors. Additionally, the sensors can be temporarily attached to trees using crop wire rather than permanently using tree nails.
Number of Mesh Gateways	A Pilot deployment uses from 4 to 8 Mesh Gateways for an area of 400 to 500 hectares, depending on the terrain and RF signal propagation conditions. Hilly areas need more Mesh Gateways. Less dense and relatively level forest floors need less Mesh Gateways where 4 should be sufficient.
Border Gateways requirements	We recommend powering the Border Gateway using a reliable power supply and where it can have Ethernet Internet connectivity. It is also possible, but not recommended, to power the Border Gateway using only its solar panel.
Preparing a deployment plan	Consider how the deployment teams must traverse the forest so they can efficiently use the time. With such a large deployment area, several teams of two workers may be required to deploy all the sensors. Ensure you prepare one site Packet per team, considering how the team must navigate through the forest. Ideally, create one Packet for one day's worth of work for a single team.

Important

To deploy 400 sensors and Gateways, a team of 2 people can deploy 20 to 50 devices a day. However, this depends entirely on the difficulty of the terrain and state of the forest floor. In general, deployment is achieved quicker when more teams are available to deploy the devices.

Live deployments

Large-scale *Live* deployment takes into consideration the results of a Pilot deployment which is used to determine the required number of sensors and gateways to effectively cover the entire deployment location.

Treenails are used to permanently attach the sensors to trees rather than crop wire.

Guidelines

The scale and scope of the deployment determine the planning parameters such as device location and targeted detection time:

The scale and scope of the deployment determine the planning parameters such as device location and targeted detection time.

Parameter	Description
Site dimensions	How many hectares will be protected with the Silvanet System? This determines the number of devices to be deployed.
Human activity	Does the area have a high density of human activity or is it a mixture of high- and low-density human activity? This determines the density of sensor deployments per area
Number of devices	How many sensors are required to cover the Site area and how many Mesh Gateways and Border Gateways would be needed? This is determined by the Site dimensions and human activity.
Internet connectivity	Does the Border Gateway have Ethernet connectivity or only LTE-M mobile connectivity? This determines the location of the Border Gateway in the Site.
Build and assign Packets	Once these parameters have been determined, the Site Management app is used to plan the deployment and assign Packets for users to deploy the devices in the target area of a forest.

Number of devices

When planning Live deployments, follow the guidelines for device ratios / ranges:

- Number of Sensors to number of Mesh Gateways: 100 to 1
- Number of Mesh Gateways to number of Border Gateways: 20 to 1

Density guidelines

Following the guidelines for sensor deployment density:

- Areas of high human activity, distance between sensors should be no further than 100 m between devices.
- Areas of low human activity, distance between sensors can be from 400 m to 500 m between devices.

Additionally, planning for large-scale deployments requires following the location guidelines for Mesh Gateways and the deployment setup of Border Gateways.

Packet preparation

The Site Management app (dryad.app) provides a convenient way to plan the deployment locations of sensors and gateways. The result of this planning is a *Site Packet*.

Site Packets are prepared in the Silvanet Site Management app based on the Planning deployment guidelines and deployment types.

Once built, the new packet is assigned to a registered user who accesses this Packet in the Silvanet Deployment app installed on a Smartphone. The devices indicated in the Packet are then ready to be deployed in the locations set in the Packet.

Note
Several Packets can be created within each Site. Each Packet can consist of the devices expected to be deployed per day / per forest worker.

Preparing Site Packets involves the following steps:

1. Opening a Site in the Site Management app
2. Building a Packet of sensors and gateways and mapping the location of each device
3. Assigning Packets to registered users for deploying devices in the forest location

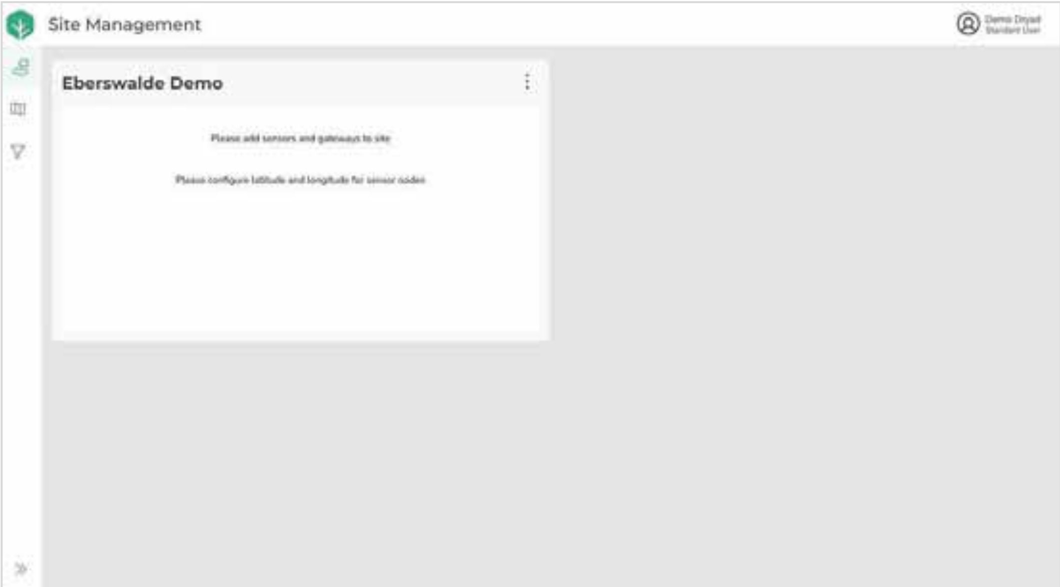
Info
A Packet defines the Silvanet sensors and gateways that are to be deployed in a Site. The Site Management app is used to build and assign Packets to registered users. It is also used to monitor the deployed sensors and gateways of the Site.

Open a Site

The first step in preparing Site Packets is to select a Site from the Site Management app.

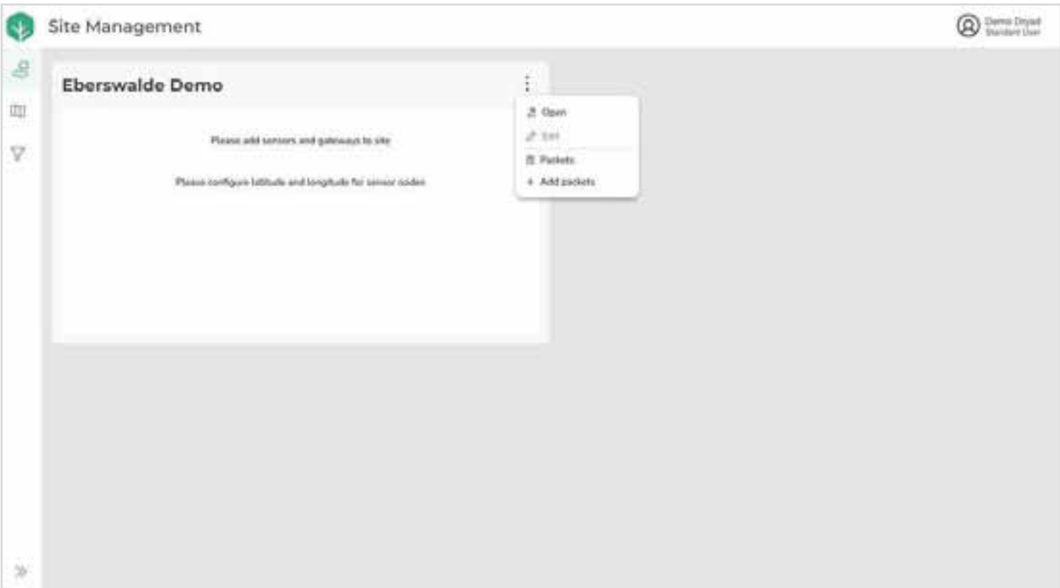
To open a Site:

1. Log in to dryad.app. The Site Management app appears.



Site Management dashboard

2. From a Site, select the ellipsis menu on a Site, then select **Open.**

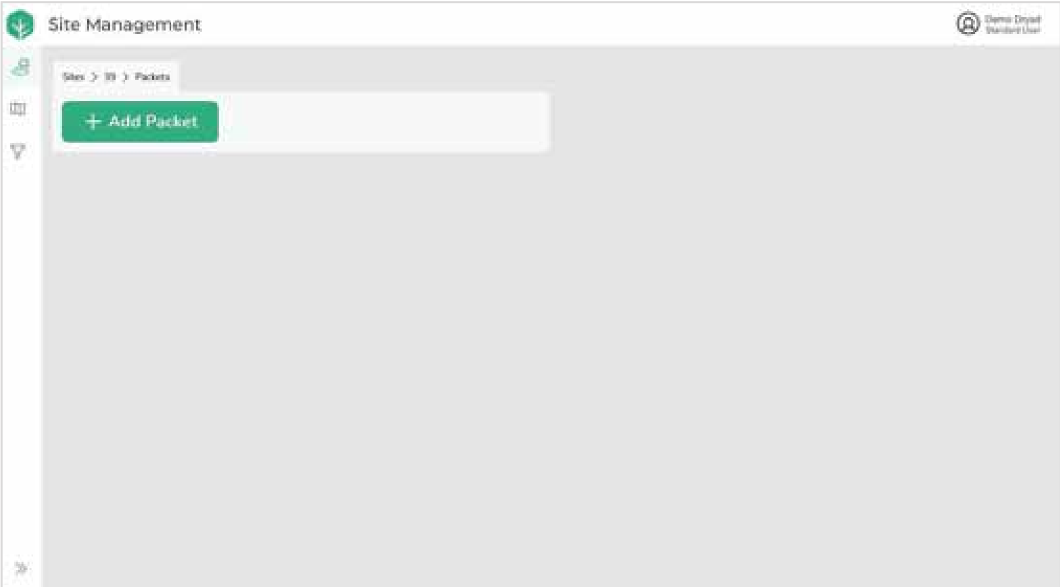


Open a Site

3. The Site's dashboard appears. If devices have already been deployed to this Site, a map of the Site and the number of currently active gateways and sensors appears.

Site dashboard

4. Select **Planning** to open the Packet planning page. Any existing Packets appear here.



Packet planning page

5. Begin building a Packet for the Site.

Info

Sites are currently added by Dryad internal Admins. In the future, a Site Admin will be allocated to specific users who will be able to create sites for clients and to create users.

Build a Packet

After opening a Site in the Site Management app, begin planning the deployment of Silvanet devices. This is done by building one or more *Packets* that define the number and planned GPS coordinates (latitude and longitude) of Silvanet Sensors and Gateways to be deployed in a Site.

Tip
You can create as many Packets as are required for the Site. For example, you can create several Packets for one day's deployment for multiple teams.

Building a Packet involves the following steps:

1. Create a new Packet.
2. Use the Map tools to search for the Site location.
3. Add the required number of devices.
4. Place the device icons on the map to determine planned GPS coordinates.
5. Save the Packet.

Info
This section assumes you have selected a Site from the Site Management homepage. For more information, see Opening Sites.

Guidelines

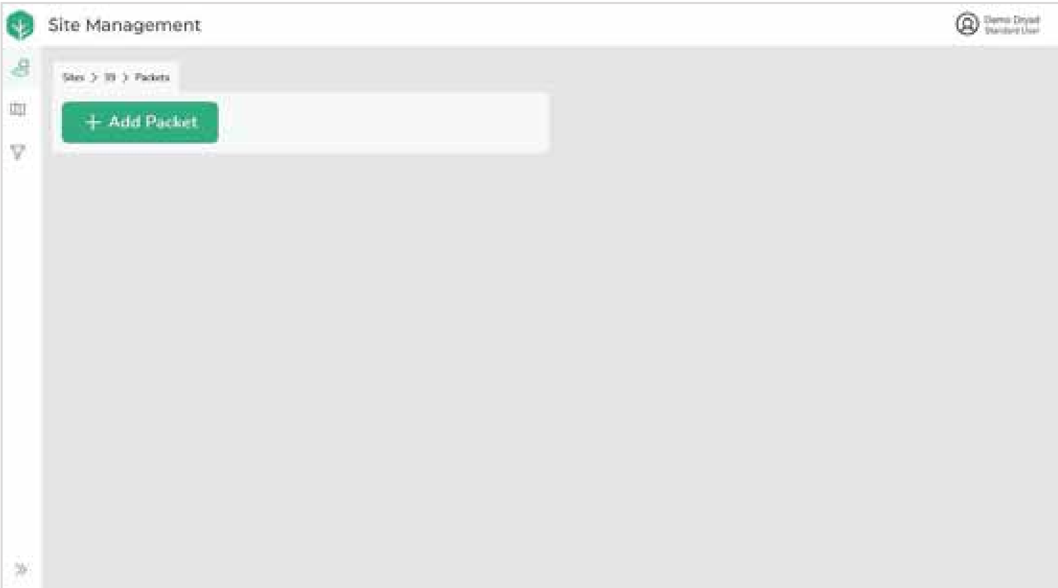
When building Packets, consider the following guidelines:

- Human activity and Site topology to determine density of sensors in various parts of the Site, as described in *Sensor density*.
- Location of sensors in the WUI and in deep forests to determine the density value per hectare, as described in *Density value per hectare*.
- Ratio of sensors to Mesh Gateways / Border Gateways, as described in Ratios.
- Distance between sensors and range between sensors and Gateways, as described in Device ranges.

Create a new Packet

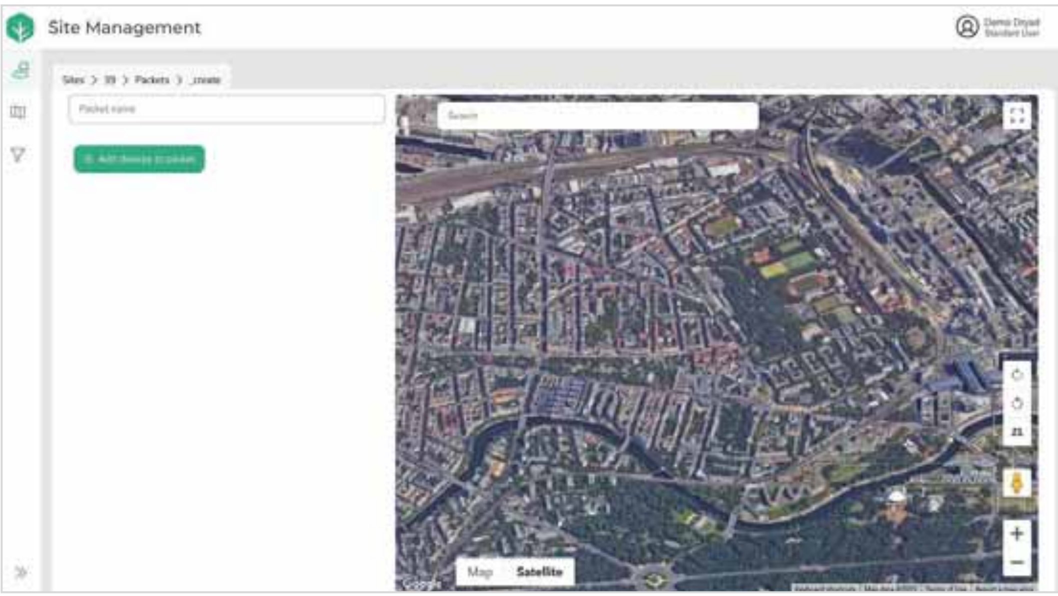
To create a new Packet:

1. From the Site dashboard select **Planning**. The Packet planning page appears. Other Packets may appear on this page.



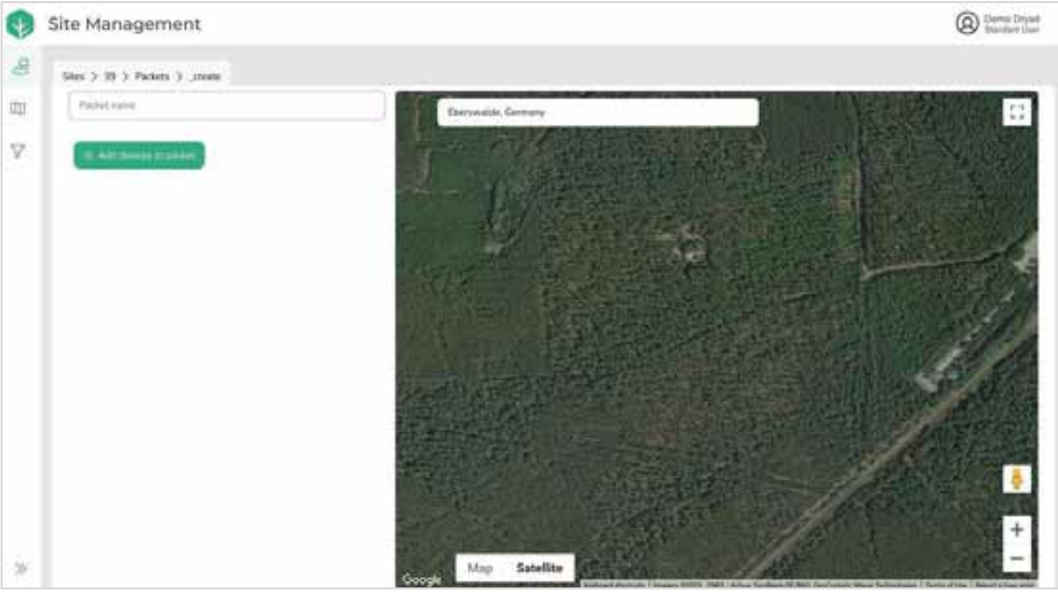
Packet planning page

2. Select **Add Packet** to begin building the Packet. The Packet building page appears with a default location shown in the map (if you allow the application to determine your location, otherwise no map appears).



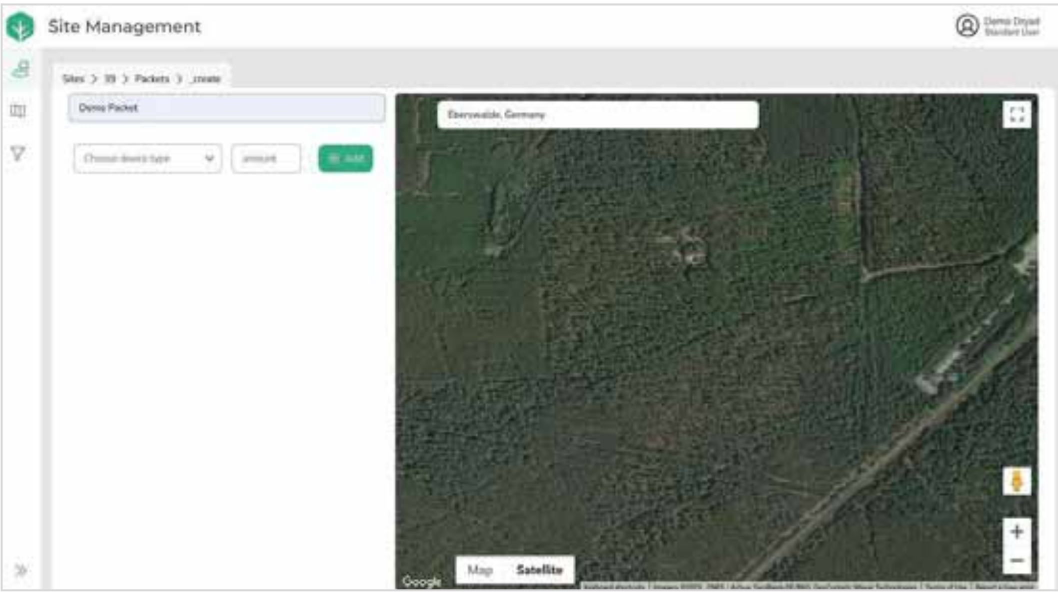
Build Packet page

3. In the **Search** field enter a location to center the Map on the planned location for the deployments. Use the Map tools to zoom in or out on the location.



Search Site location

4. Enter a name for the Packet, then select **Add devices to packet**.



Enter Packet name

5. Select **Save** to save your changes to the Packet (you may need to scroll down to see the Save button).

6. Begin adding devices to the Packet. See the following sections for details.

Note

The order of adding devices to Packets is entirely arbitrary. The following example show Border Gateways added first but sensors could equally be added first.

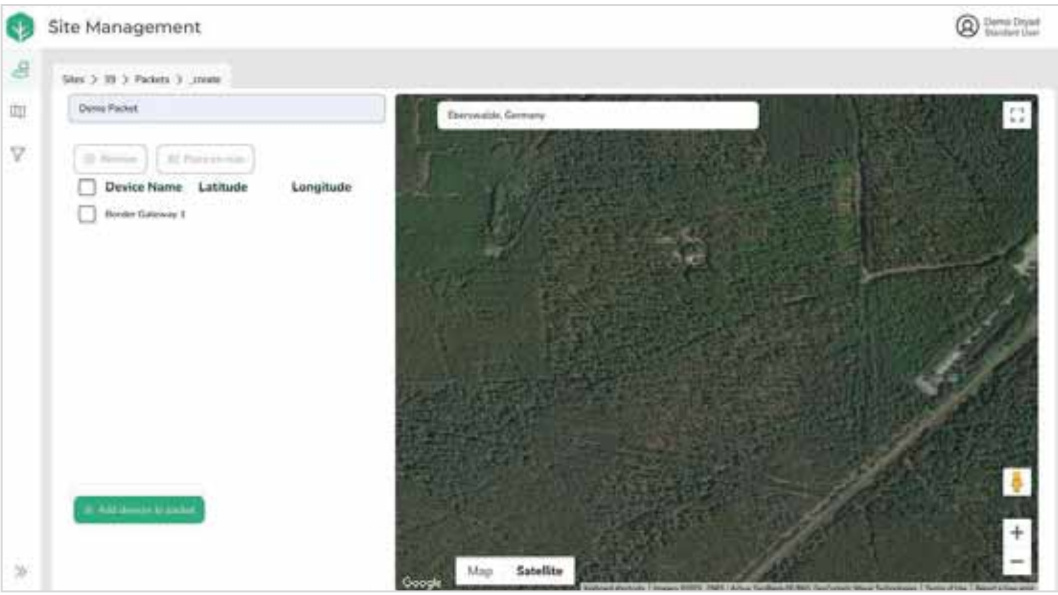
Add Border Gateways

A deployment needs 1 Border Gateway for every 20 Mesh Gateways. We recommend a backup Border Gateway for larger deployments.

Choose amount of Border Gateways

To add one or more Border Gateway(s) to the Packet:

1. Ensure the map is centered on the deployment location.
2. Select **Add devices to packet**.
3. From the **Device Type** dropdown menu, Select **Border Gateway**.
4. Enter the amount of Border Gateways to add to the Packet, then select **Add**.



Add a Border Gateway to Packet

5. Select **Save** to save your changes to the Packet (you may need to scroll down to see the Save button).

Note
If the approximate location of the Border Gateway(s) is not known beforehand, you can save the Packet by selecting Save.

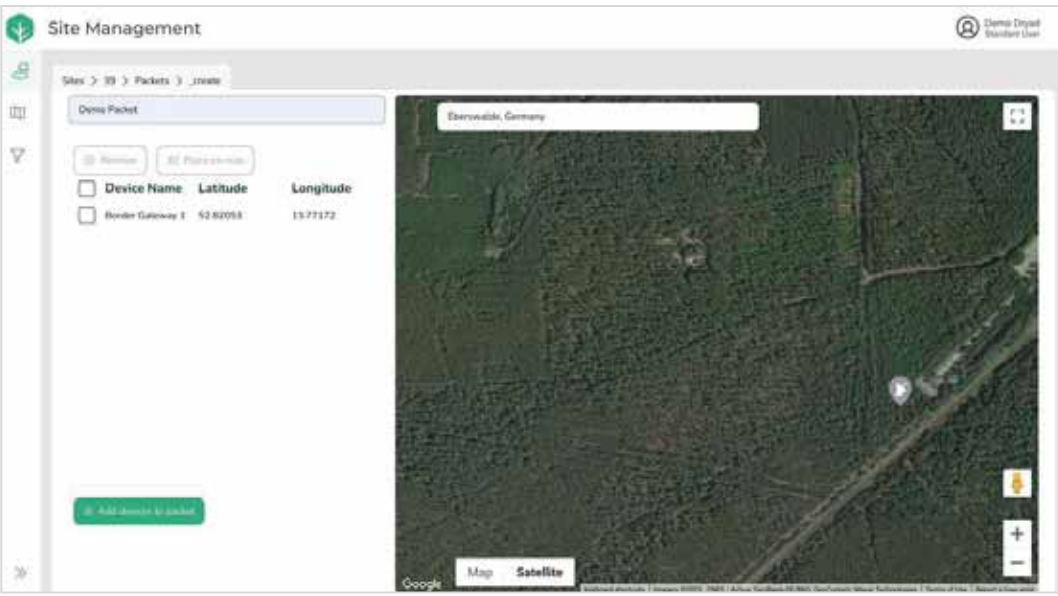
Determine Border Gateway GPS coordinates

Placing the Border Gateway on the map generates the GPS location for the device.

To place a Border Gateway on the map:

1. Select the Border Gateway(s), then select **Place on Map**.
2. The Border Gateway appears on the map as an icon centered in the view.
3. Using drag and drop, move the Border Gateway icon to the approximate location of the planned deployment. The GPS coordinates of the planned location appear next to the device in the list.

Tip
You can switch to full screen mode to view a larger map when placing the Border Gateway.



Placing Border Gateway on the map

4. Select **Save** to save your changes to the Packet (you may need to scroll down to see the **Save** button.

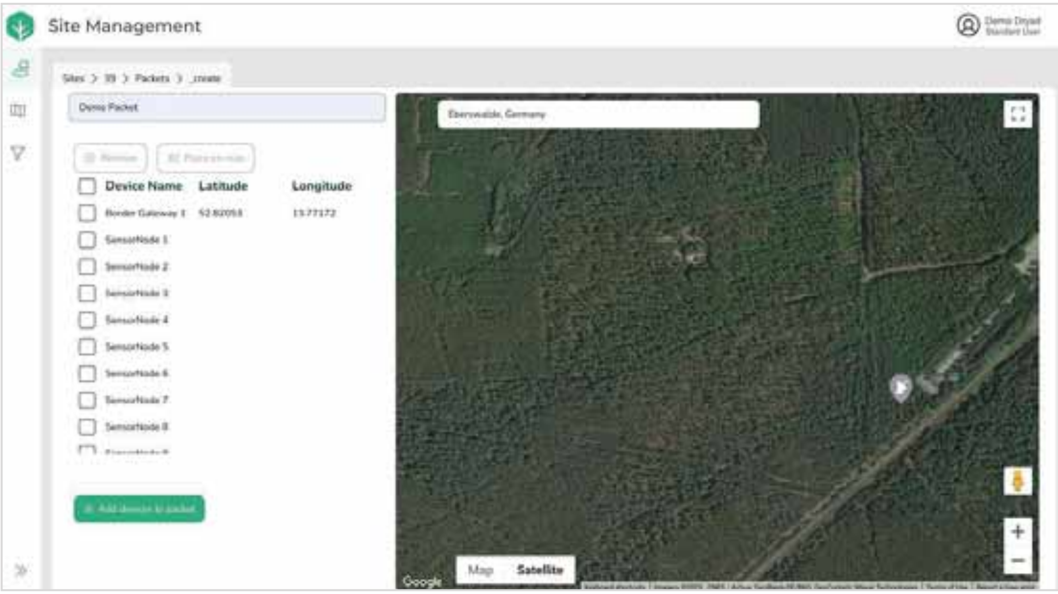
Add sensors

Before adding sensors, you need to know the number of sensors you plan to deploy. Consider deployment density when placing sensors on the map.

Choose amount of sensors

To add sensors to the Packet:

1. Ensure the map is centered on the deployment location.
2. Select **Add devices to packet**.
3. From the **Device Type** dropdown, select **Sensor**.
4. Enter the number of sensors to add to the Packet.



Adding sensors to Packet

Note
If the approximate location of the sensors is not known beforehand, you can save the Packet by selecting **Save**.

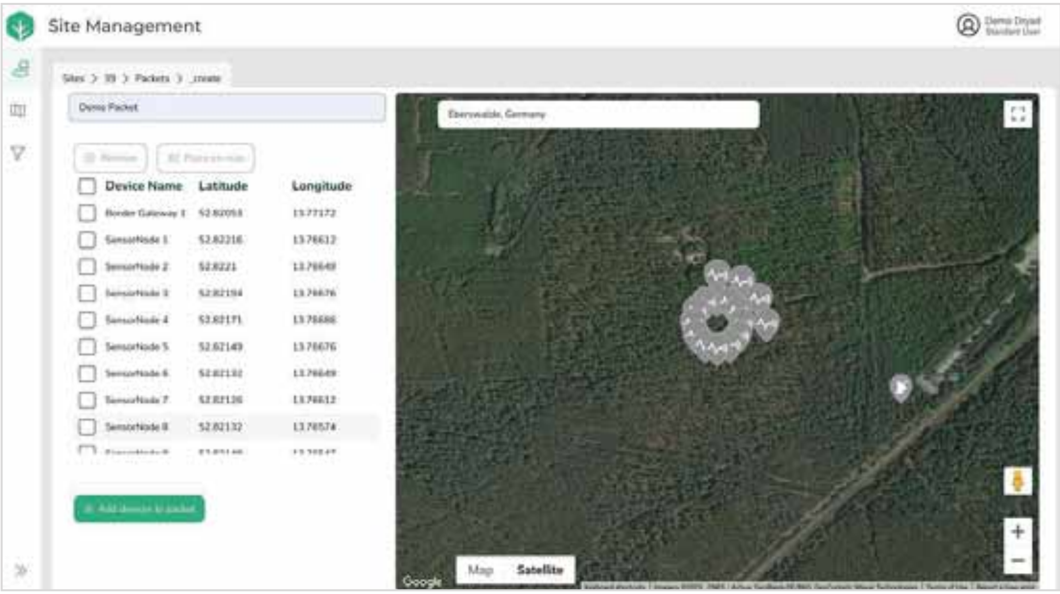
Determine sensor GPS coordinates

Placing sensors on the map generates the GPS location for each sensor. Ensure the map is centered on your Site location before continuing.

Note
Plan for sensors to be deployed away from paths and streets. Place the sensors a meter or so away from a path or street to prevent the device from damage due to vandalism.

To place the sensors on the map:

1. Select the sensors, then select **Place on map**. The sensors appear on the map centered in a default location. The current GPS coordinates of the sensors appear next to the devices.



Placing sensors on the map

2. Using drag and drop, arrange the sensors on the map according to sensor deployment guidelines.

Note
You can view the map in full screen mode for easier placement. Use the standard map tools to move around the map. Distances between devices appear when moving icons.

Arranging sensors on the map

3. Select **Save** to save your changes to the Packet (you may need to scroll down to see the **Save** button.

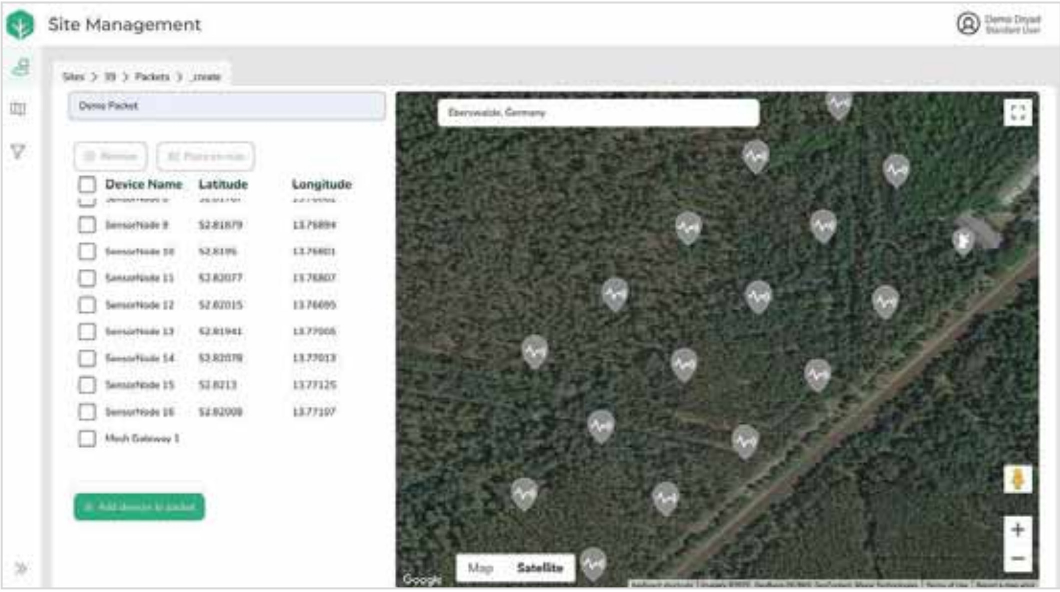
Add Mesh Gateways

A deployment needs 1 Mesh Gateway for every 100 sensors. More Mesh Gateways may be required depending on the topology of the forest.

Choose amount of Mesh Gateways

To add Mesh Gateway(s) to the Packet:

1. Ensure the map is centered on the deployment location.
2. Select **Add devices to packet**,
3. From the **Device Type** dropdown menu, select **Mesh Gateway**.
4. Enter the number of Mesh Gateways to add to the Packet.



Add Mesh Gateways

Note
If the approximate location of the Mesh Gateway(s) is not known beforehand, you can save the Packet by selecting **Save**.

Determine Mesh Gateway GPS coordinates

To place Mesh Gateways on the map:

1. Select the Mesh Gateways, then select **Place on Map**.
2. The Mesh Gateways appear on the map as icons.
3. Using drag and drop, arrange the Mesh Gateway icon(s) on the map according to deployment guidelines.

Placing Mesh Gateways

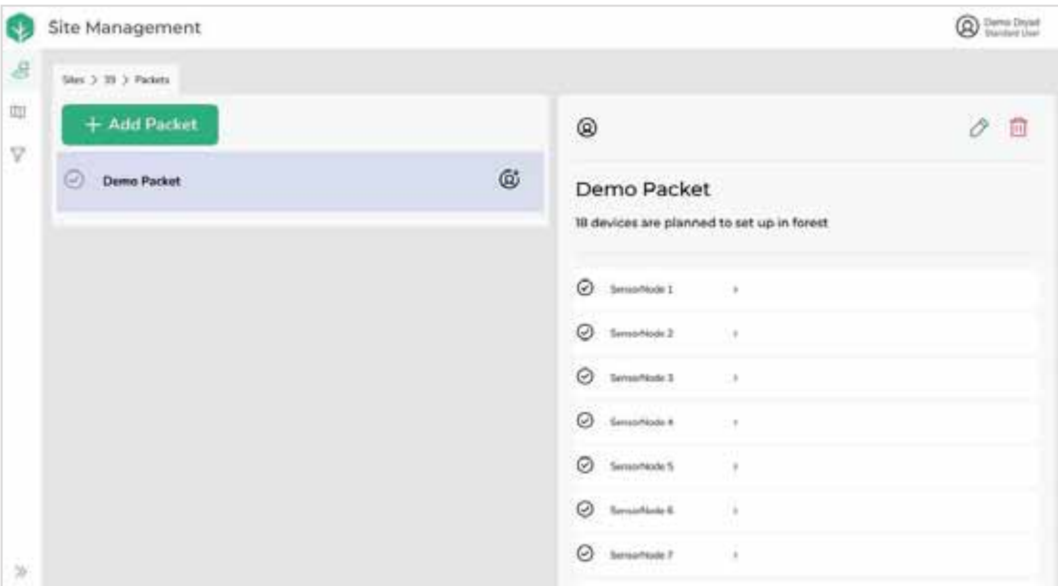
4. Select **Save** to save your changes to the Packet (you may need to scroll down to see the **Save** button.

Finish up

With the devices added to the Packet and placed on the map, the packet needs to be assigned to a user.

To finish up:

1. Once the Packet has been saved, select **Back** to return to the Packet Overview page.



Completed Packet

2. The Packet now needs to be assigned to a registered user of the Silvanet System.

Assign Packets

Once a Packet has been built, the deployment of the devices in the forest is assigned to a registered user of the Deployment app. The assignment process delegates the deployment work to a specific person, such as a forest worker who will install the devices.

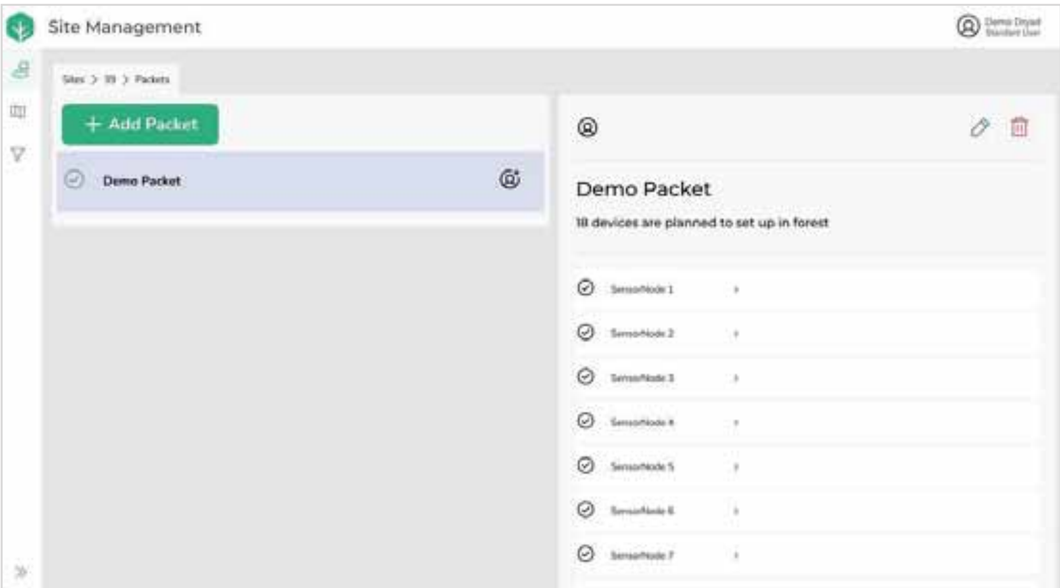
Important
Before a Packet is assigned, the person who will deploy the devices needs to be registered with the Site Management app, preferably using their names. Contact Dryad for details.

To assign a Packet to a registered user:

1. In the Build Packet page, ensure the new Packet has been saved.

2. Select the **Back** button to return to the **Packet Overview** page.

3. Your new Packet appears in the list of Packets but is unassigned.



Packet finished

4. Select the **Assign** icon.

Assign button

5. The **Assign** dialog appears showing a list of registered users.

6. Choose a user, then select **Assign**.

7. Packet information is now assigned to the user.

8. The new Packet now appears in the Silvanet Deployment app on the Smartphone of the assigned user.

9. The Packet can now be used to deploy the devices in the Site's forest locations.

Sensor GPS coordinate updates

If a sensor has been relocated (for example, moved to another tree), the new GPS coordinates (latitude and longitude) of the sensor need to be updated in the Site Management app.

To update a sensor's longitude and latitude values:

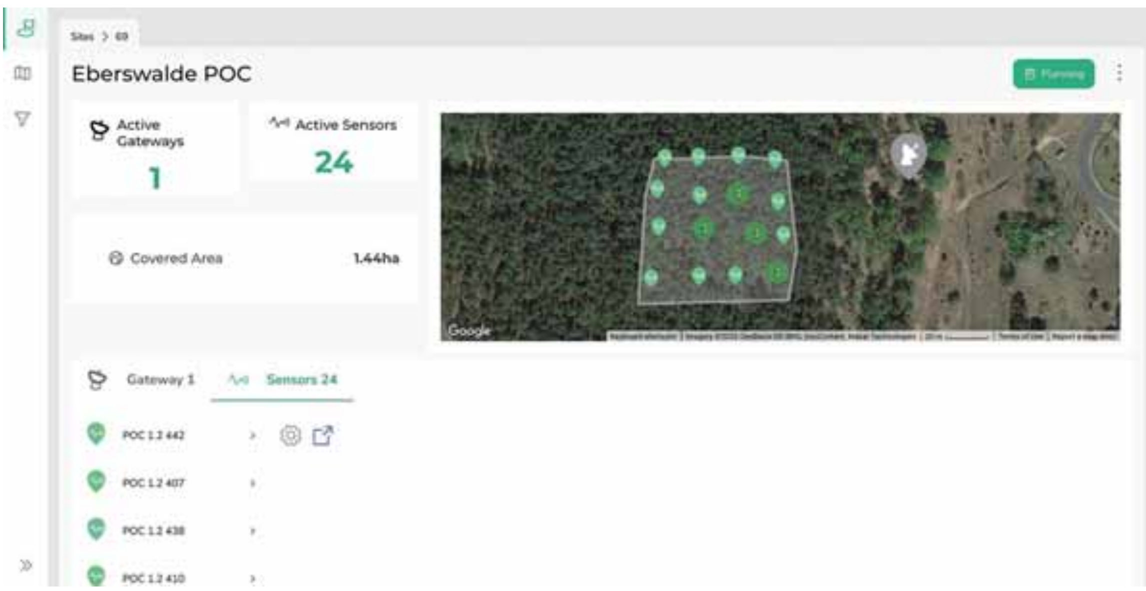
1. Using a Smartphone's map app, find your current location.

2. Make a copy of your current latitude and longitude.

3. Open the Site in the Site Management app and click the **Sensors** tab in the Site Management dashboard.

4. Find the sensor that needs its coordinates updated.

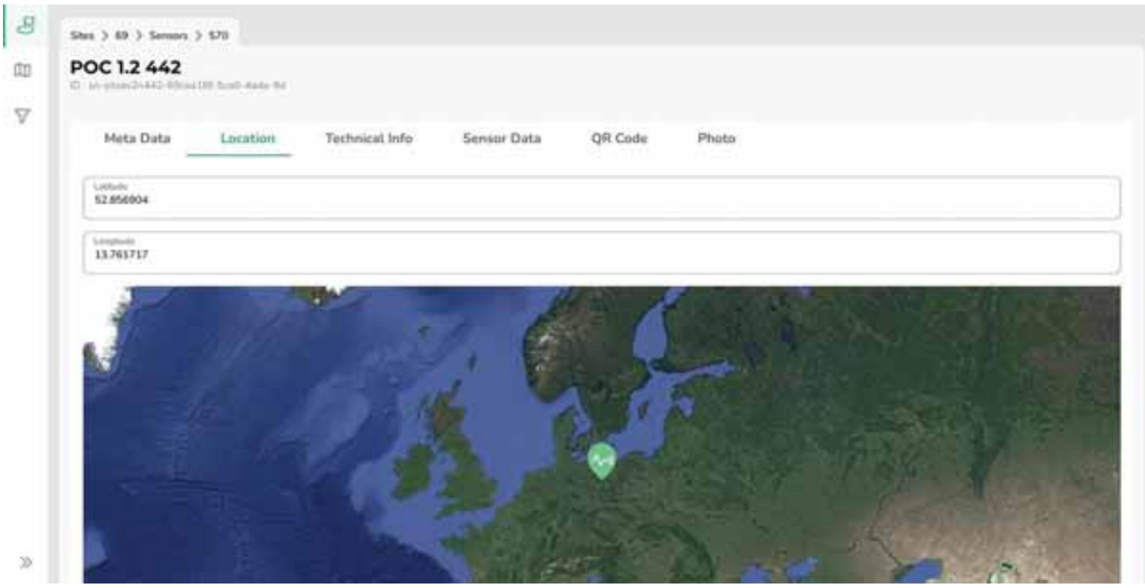
5. Hover over the sensor name to display the options, then select **Edit**.



Select sensor

6. In the **Edit** view, select the **Location** tab.

7. Enter the new latitude and longitude coordinates, then select **Submit**.



Update the latitude and longitude values for the device

8. The changes will be reflected in the Site dashboard.

Device deployment

After building one or more Packets for a Site, the users assigned to the Packets can begin deploying the devices in the forest. The Silvanet Deployment app installed on a Smartphone is used to deploy the Silvanet devices.

We recommend creating a deployment plan before entering the forest based on the Packets that have been built. This means knowing where you plan on deploying the Border Gateway, the Mesh Gateways and the sensors.

Preparation guidelines

Before entering the forest to begin the deployment, prepare a plan to deploy the sensors in the forest. Prepare your walk through the forest beforehand to install the sensors in the most efficient manner.

Warning
When installing the devices, always work in teams of at least two people when walking through the forest to locate the planned GPS coordinates of the devices and while using ladders to install devices on trees. Ensure the ladder is safely leaned against the tree and is stable. Have a helper securely hold the ladder.

Note
Besides routine precautions when entering a forest, make sure that the battery of the used smartphone is fully charged (we recommend bringing a power bank).

Prepare a plan to deploy the sensors in the forest. Prepare your walk through the forest beforehand to install the sensors in the most efficient manner.

Guideline	Description
Smartphone	Ensure you have a Smartphone fully charged with working GPS and a backup charger like a power bank.
Install the Silvanet Deployment app.	Ensure you have installed on the Smartphone the Silvanet Deployment app and have one or more Packets assigned to you.
Start the Dryad Deployment app while you have a good wireless connection.	Before you enter the forest, ensure you have downloaded your assigned Packets to the Deployment App while you have good mobile connection. This allows the app's local database to be updated with the device information such as GPS coordinates in your assigned Packets.
Cache the Map page to the Deployment app	While connected to the mobile network, load the Map page to cache the map to ensure you have access to the Map view should a mobile connection become unavailable (offline usage).
Ensure you have the correct number of devices.	Before going to the forest, ensure you have the correct number of devices, spacers, treenails and crop wire (if required) for deploying your Packet. Use a waterproof box with a handle to keep the devices safe and dry while in the forest.
Be prepared to install devices at the correct height and direction.	All devices (sensors and gateways) must be installed at a correct height, which is at least 3 meters above the forest floor. They also need to face in a southerly direction for maximum irradiation on the solar panels. This means bringing a ladder high enough for this purpose.

Required deployment tools

You may need one or more workboxes, depending on how many devices are planned for a day's deployment.

You need a 16-foot (5 meter) ladder. A folding ladder makes carrying it through the forest easier.

16ft (5m) ladder

Use waterproof boxes for devices and tools. The following is an example good quality toolbox.

Example waterproof toolbox

Use a waterproof toolbox for carrying sensors and the following for the sensors:

- Knife and shears (or snips) for cutting branches and crop wire (if required)
- (optional) Crop wire for temporarily deploying devices
- Bring several rolls of reflective bands, tape or some other method for identifying trees with installed sensors.

Toolbox ready with (select) tools for deploying sensors

Use a second waterproof toolbox containing the following tools:

- Compass (analogue or digital)
- Cordless drilling machine
- 10 mm wood drill bit (an optional 6mm drill bit to begin drilling into hardwood trees)
- Hammer
- Pencil

- 17mm wrench (for U-clamps)
- Small Phillips screwdriver
- Small axe

Tip
When drilling into a hardwood tree, start with a smaller drill bit then drill the final hole with the 10mm drill bit. Also, ensure you are using a drill bit for wood.

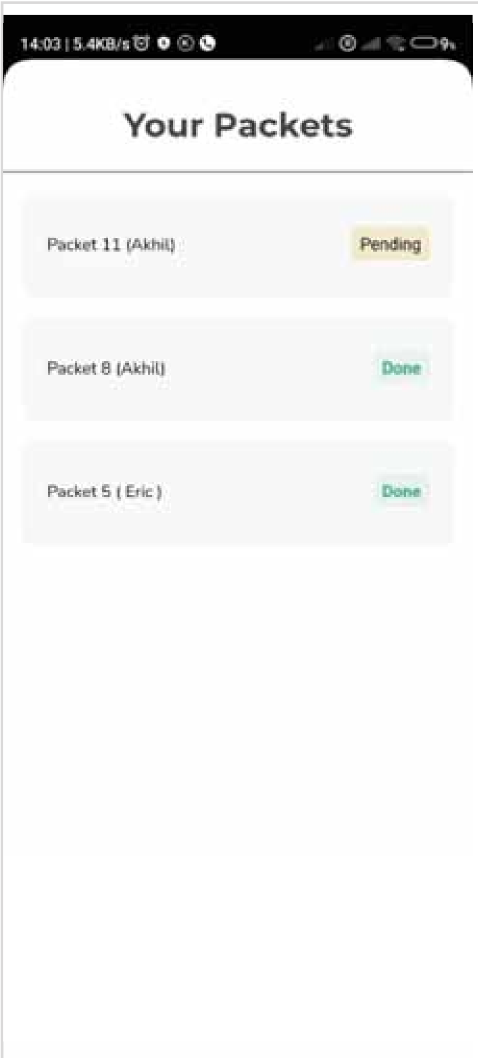
Navigating to Site location

After your preparations are ready to deploy a Packet's devices, use the Silvanet Deployment app to navigate your way to the deployment area.

To locate the deployment area of the forest:

1. Open the Silvanet Deployment app on your Smartphone.

2. In **Your Packets**, select the Packet that has been assigned to you.



Assigned Packets

3. The Packet shows the current task and list of devices. Expanding a device item shows the planned geographical coordinates for that device.

List of sensors to be deployed

4. Scroll to the bottom of the list of devices and select **Map** to open the Map view. The Map view contains the planned position of every device in the map. Your current location appears on the map as a blue icon.

Map view of planned deployment location

5. Find the planned GPS location (a tree) using the Map view. A 20m overlay appears around the planned location. You can locate an appropriate tree within this radius.

Deployment location

6. Once you have found the location of the Site, you can now begin installing a sensor or gateway.

Deployment guidelines

This section provides guidelines which you should follow when deploying sensors in a Site location.

Important
Read this section carefully to ensure you are deploying devices, including sensors, to achieve effective fire detection. Failure to follow these guidelines will result in the system not working as designed.

Warning
AFTER SENSORS HAVE BEEN DEPLOYED, CALIBRATED AND SETTLED, DO NOT INTERACT WITH THE SENSORS AS THIS WILL CAUSE ERRORS WITH SENSOR VALUES AND COULD ALSO RESET THE SENSOR CALIBRATION. .

General guidelines

When planning sensor deployments, we recommend the following:

Item	Guideline	Description
Location	80 m to 100 m apart from other sensors	Install sensors to detect environmental air quality in a radius of 80 m to 100 m.
Range	1 km from Mesh or Border Gateways	Install sensors no further than 1 km from either a Border Gateway or Mesh Gateway.
Sunlight	Install in the direction where the sun would be at 12:00 noon	Sensors need to be installed facing the sun at 12:00 noon (northern or southern hemisphere) to provide maximum exposure to sunlight (even in cloudy conditions).
Height on trees	3 m from forest floor	To protect the sensor from human or animal interference, install the device 3m above the forest floor.

Item	Guideline	Description
Device ratio	100 sensors to 1 Mesh Gateway.	See Device ratios/ranges.
Sensor deployment density	80m to 100m / 400m to 500m	Spacing between sensors should be 80 m to 100 m for areas of high human activity, 400 m to 500 m for areas of low human activity. See below for details.
Density values per hectare	0.7/ha to 0.1/ha	Based on WUI (Wildland Urban Interface) we recommend 0.7/ha sensors for a dense WUI and 0.1/ha sensors for a sparse WUI. See below for details.

Sensor deployment guidelines

Guideline	Description
Bring sufficient sensors for a day's work	Ensure you have brought sufficient sensors, treenails, spacers (and crop wire, if required) for the day's installation plans.
Select a healthy tree on which to deploy the sensor	The assigned user locates a tree closest to the GPS coordinates set for a sensor using the Silvanet Deployment app. Also, ensure the tree is healthy and not likely to fall over or be harvested.
Sensor needs to be 3 m above the forest floor on the tree.	Dryad recommends installing the sensor on the tree approximately 3 meters above the level of the forest floor. At this height, the device is most sensitive to fire detection and it obtains an increased amount of light on its solar cell. Furthermore, at this height it avoids disturbances from most human and animal interactions.
Sensor should face towards the	The sensor needs to be oriented towards the direction of the sun (where it would be at 12:00 noon). Use a compass to

Guideline	Description
sun (at 12:00 noon).	identify true South (in the northern hemisphere) or true North (in the southern hemisphere). This maximizes the amount of light that hits the solar panel.
Use the spacer to keep the sensor away from the tree bark.	A 2cm spacer is provided to deploy the sensor slightly away from the trunk of the tree. This avoids direct contact with the tree and allows tree sap to flow down the tree behind the sensor. The spacer also helps keep the sensor away from the moisture in the tree. Furthermore, the spacer allows the sensor to hang vertically rather than laying directly against the bark of the tree which could cause it to tilt at an angle. Also, hanging the sensor vertically improves the radio range of the device.

Mesh Gateway deployment guidelines

Guideline	Description
Unobstructed solar panel	The device has a large built-in solar panel to provide for the Mesh Gateway's increase power requirements. However, the solar panel needs an unobstructed area to obtain sufficient sunlight to charge the device.
Direction towards sun at 12:00 noon	The Mesh Gateway needs to be oriented towards the direction of the sun (where it would be at 12:00 noon). Use a compass to identify true South (in the northern hemisphere) or true North (in the southern hemisphere). This maximizes the amount of light that hits the solar panel.
Install 3m above forest floor	If installed on a tree, install the Mesh Gateway at least 3 meters above the forest floor, depending on available sunlight in the location. At this height, the device has less interference from human or animal interactions.

Border Gateway deployment guidelines

Guideline	Description
Ensure a reliable power source	The Border Gateway can obtain power from a mains power source, from PoE (Power over Ethernet) or from its solar panel.
Ethernet connectivity recommended	We recommend providing the device with access to Ethernet connectivity.
Deploy at edge of forest	Deploy the Border Gateway at the edge of a forest and, ideally, near a reliable power supply.
Install 3m above forest floor	Install the Border Gateway at least 3 meters above the forest floor, depending on available sunlight in the location. At this height, the device has less interference from human or animal interactions.
Needs clear line of site	Whether the Border Gateway is installed on a tree or a pole, it needs a clear line of sight to communicate via wireless mobile networks or satellite communication.
Solar panel provides backup power supply	To provide for a fallback power supply if a loss of power occurs, it uses the solar panel but it needs direct sunlight to maximize sunlight irradiation.
Clear access to sun for solar panel	The solar panel needs an unobstructed area to obtain sufficient sunlight to charge the device in case of mains power failure.
Solar panel directed towards the sun as 12:00 noon	Use a compass to identify true South (in the northern hemisphere) or true North (in the southern hemisphere). This maximizes the amount of light that hits the solar panel.

Device ID registration

Before deploying a device such as a sensor or gateway on a tree or pole, you first need to register the device ID with the Silvanet Cloud. This is done in the Silvanet Deployment app.

Once the device ID is registered with the Silvanet Cloud, the device associated with the device ID is linked to the GPS location set during registration. Data from the sensor can then be sent via the Silvanet mesh network to the Border Gateways and forwarded on through an Internet connection to the Silvanet Cloud.

The device ID is provided on the back of every device as a QR code and as a text string.

Example sensor device ID

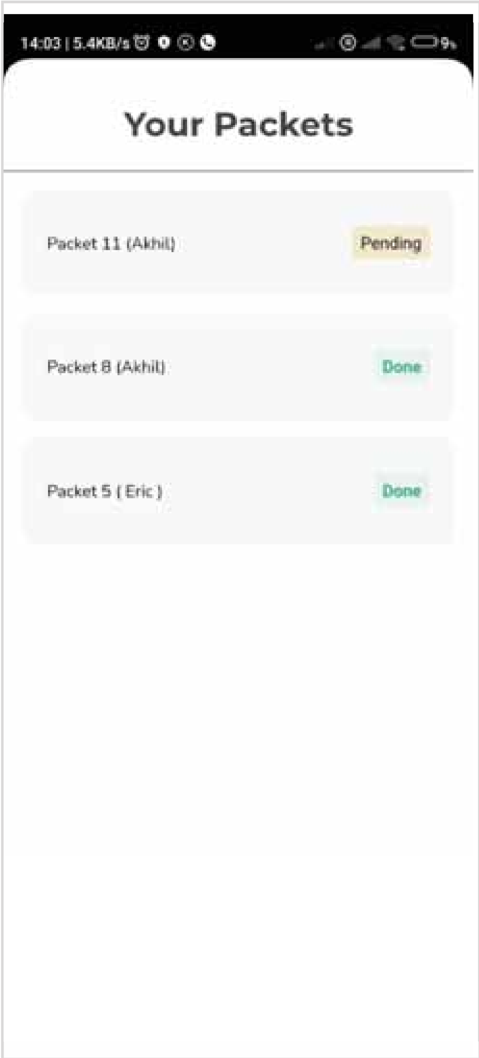
Note
The example in this section uses sensors, but the same procedure is used to register device IDs for both Mesh Gateways and Border Gateways.

Register device ID using QR Code

To register a Silvanet device using the QR Code:

1. Login to the Dryad Deployment app using your account credentials.

2. Select the Packet assigned to you. A Packet showing **Pending** indicates the Packet has not yet been deployed.



Packets assigned to you

3. Open the Packet. The Packet overview page appears showing a list of sensors to be deployed.

List of sensors to be deployed

4. Select the **Map** button to view the deployment plan.

5. Zoom into one of the sensor icons to find the planned location of a sensor. Your current location appears on the map as a blue icon. The following shows two rows of successfully installed sensors (on the left) and two rows of sensors to be installed (on the right).

Map view of planned deployment location

Note
Grey icons in the Map view indicate a sensor inactive. In this case, it has not been installed and is not yet synced with the Silvanet Cloud.

6. Move through the forest to the planned GPS location in the map view. A 20m overlay appears around the deployment location. Select an appropriate tree within this circle on which to install the sensor.

Deployment location

7. Select **Install** to open the QR Code scanner. On the reverse side of the device is the device Id which is provided as a QR Code and in text form.

8. Focus the app on the QR Code on the device to automatically scan the Device ID. The Deployment app automatically fills in the sensor's Latitude and Longitude using the Smartphone's GPS location.

QR code automatically scanned

Note
If you do not know what a QR Code looks like, click **Show me QR code**.

9. After scanning in the QR code, add important information such as observations about the location of the sensor (located on a hillside, within shadow of a cliff, and so on) in the **Notes** field. Select the **Camera** icon to take a photo of the sensor ID.

Installation complete

10. Select **Save** to complete the installation. The sensor icon on the **Map** view changes to yellow which indicates the sensor was successfully synced to the Silvanet Cloud.

Successfully installed

The Deployment app redirects to the Packet overview. The sensor can now be attached to the tree.

Register device ID manually

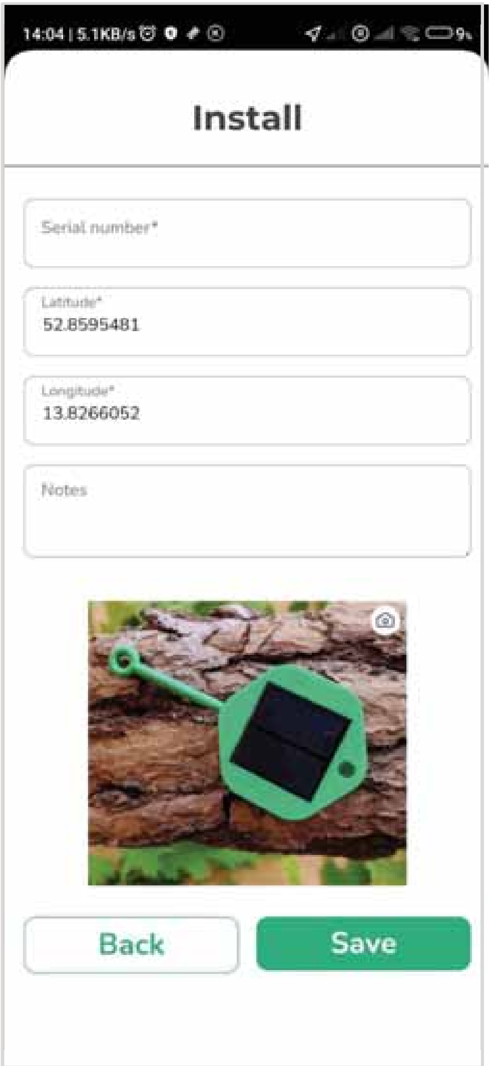
If scanning the QR Code cannot be done for any reason, you can manually add the Sensor ID to the **Serial Number** field.

To manually enter the sensor ID:

1. On the Scan QR Code page, select **Enter manually**.

Enter manually Sensor ID

2. Read the sensor ID on the back of the sensor and enter in the **Serial Number** field in the **Install** page that appears.



Install page

Tip

To easily copy the sensor ID, you can use a scan text app such as Google Lens. Copy the sensor ID, then paste the ID in the **Serial Number** field.

Scan sensor ID

3. After scanning in the QR code, add important information such as observations about the location of the sensor (located on a hillside, within shadow of a cliff, and so on) in the **Notes** field. Select the **Camera** icon to take a photo of the sensor ID.

Installation completed

4. Select **Save** to complete the installation. The sensor icon on the **Map** view changes to yellow which indicates the sensor was successfully synced to the Silvanet Cloud.

Successfully installed

The Deployment app redirects to the Packet overview. The sensor can now be attached to the tree.

Sensor deployment

Sensors are deployed based on GPS coordinates set in the Packet to determine their location in the Site. Afterwards, they can be "forgotten". They do not need any further maintenance. Any software updates to the sensors are then done remotely.

Warning
AFTER SENSORS HAVE BEEN DEPLOYED, CALIBRATED AND SETTLED, DO NOT INTERACT WITH THE SENSORS AS THIS WILL CAUSE ERRORS WITH SENSOR VALUES AND COULD ALSO RESET THE SENSOR CALIBRATION. DRYAD STRONGLY ADVISES LEAVING THE SENSORS ALONE ONE THEY ARE DEPLOYED.

Guidelines

Guideline	Description
Bring sufficient sensors for a day's work	Ensure you have brought sufficient sensors, treenails, spacers (and crop wire, if required) for the day's installation plans.
Select a healthy tree on which to deploy the sensor	The assigned user locates a tree closest to the GPS coordinates set for a sensor using the Silvanet Deployment app. Also, ensure the tree is healthy and not likely to fall over or be harvested.
Sensor needs to be 3 m above the forest floor on the tree.	Dryad recommends installing the sensor on the tree approximately 3 meters above the level of the forest floor. At this height, the device is most sensitive to fire detection and it obtains an increased amount of light on its solar cell. Furthermore, at this height it avoids disturbances from most human and animal interactions.
Sensor should face towards the sun (at 12:00 noon).	The sensor needs to be oriented towards the direction of the sun (where it would be at 12:00 noon). Use a compass to identify true South (in the northern hemisphere) or true North (in the southern hemisphere). This maximizes the amount of light that hits the solar panel.

Guideline	Description
Use the spacer to keep the sensor away from the tree bark.	A 2cm spacer is provided to deploy the sensor slightly away from the trunk of the tree. This avoids direct contact with the tree and allows tree sap to flow down the tree behind the sensor. The spacer also helps keep the sensor away from the moisture in the tree. Furthermore, the spacer allows the sensor to hang vertically rather than laying directly against the bark of the tree which could cause it to tilt at an angle. Also, hanging the sensor vertically improves the radio range of the device.

Deployment overview

1. The assigned user locates a tree closest to the GPS coordinates set for a sensor using the Deployment app.

2. After scanning in the sensor's QR Code, the actual position of the sensor is saved to the Silvanet Cloud. See Device ID Registration.

3. Once a sensor is successfully linked to its actual position in the Silvanet Cloud, it can then be installed on a tree.

4. The sensors are designed with a loop which is used to attach the device to a tree with a treenail (or crop wire if attached temporarily).

See also
To learn how to register the sensor ID in the Deployment app, see *Install device IDs*.

Sensors can be attached to trees using treenails for permanent attachment or using crop wire for temporary attachment.

Important
When locating a tree on which to install a sensor, look for indications that the chosen tree may be in poor health, is planned for cutting or is in any way unlikely to survive for the duration of the lifetime of a sensor. Find another tree within the designated radius (20m) of the planned location.

Warning

Keep safety foremost when attaching sensors to trees. Make sure the ladder is stable when leaned against the tree, especially when leaned against thinner trees. Have the second person hold it to stabilize it while climbing the ladder.

Using treenails

Treenails are wooden pegs to securely attach sensors to the tree. They are fed through a loop in the sensor and spacer then hammered into the tree.

Holes are pre-drilled into the tree to receive the treenail. As treenails are made of wood rather than metal, they are harmless to the tree. And as they expand due to the tree's moisture, they end up securely attaching the sensor to the tree for a very long time. This is the recommended method as each sensor requires only a single treenail to securely deploy it to a tree.

To deploy a sensor to a tree using treenails:

1. With the help of an assistant, stabilize the ladder against the tree.
2. Locate the correct height (3 m) and direction (facing sun at 12:00 noon).
3. Carefully remove a small portion of the bark with an axe at that location. Try not to excessively damage the tree.

Remove small area of bark at the install location

4. Carefully drill a hole approximately 6-7 cm into the tree using a 10 mm drill bit. Do not drill deeper than this recommended depth to prevent unnecessary damage to the tree.

Tip
When drilling into a hardwood tree, start with a smaller drill bit to drill a pilot hole then drill the final hole with the 10mm drill bit. Also, ensure you are using a drill bit for wood. This prevents the wood from splitting.

Carefully drill 10mm hole

5. Insert a treenail through the sensor's loop, slip a spacer onto the treenail, then carefully hammer the treenail into the hole drilled into the tree, ensuring the treenail is not damaged.

Hammer in treenail through sensor and spacer

6. Ensure the sensor is securely deployed to the tree and hanging loosely and vertically.

Sensor attached with treenail and spacer

7. (Optional) Mark the tree with the sensor using a reflective band or some other identifying marker to easily locate the tree later.

Tree with attached sensor indicated by a marker

Using crop wire (temporary only)

Sensors can be attached using crop wire for short term installations. Crop wire is typically used in agricultural settings such as greenhouses. This solution should only be used for a limited time as the wire will eventually interfere with growth in the tree's girth.

To deploy a sensor using crop wire:

1. With the help of an assistant, stabilize the ladder against the tree.
2. Locate the correct height (3 m) and direction (facing sun at 12:00 noon).
3. Cut a length of crop wire at least 50% longer than the circumference of the tree.
4. Insert crop wire through the spacer and sensor as shown below.

Insert crop wire through sensor and spacer

5. Tighten the crop wire around the tree. Ensure it is securely attached and that the sensor cannot slip or move.

Sensor attached with crop wire

14-day calibration period

Once deployed, the Silvanet sensor needs to perform a calibration to determine a value for normal air in the environment around the sensor. This is critical for allowing the sensor to detect a smoldering fire.

The calibration period is approximately 14 days after deployment and during this period the sensor does not detect smoldering fires. It may also send false Fire Alerts during this period, up to possibly even a month after deployment.

Warnings

Sensors are very sensitive to any changes in the environment including something as simple as touching them or moving them. Any interaction with a sensor triggers a Phase 1 alert, which in turn may trigger a Phase 2 process which causes the sensor to perform a set of gas scans to determine if it has detected a fire.

Warning
AFTER SENSORS HAVE BEEN DEPLOYED, CALIBRATED AND SETTLED, DO NOT INTERACT WITH THE SENSORS IN ANY WAY.

Examples of sensor interactions

Interacting with sensors includes:

- Touching the sensors in any way
- Moving the sensors in any way
- Being in proximity to the sensors
- Having vehicles nearby the test setup
- Bringing any source that could trigger the Phase 1 alert nearby the sensors, including cigarettes, machinery, breathing on the sensor and so on

Allow sensor to return to normal values

If interactions with a sensor have triggered a Phase 1, the sensor needs at least 2 to 4 hours to return to normal values. During this period, the sensor does not measure any changes in the environment. After this period, the sensor is ready again to begin fire detection procedures.

Firmware updates

Firmware updating is done using FUOTA (Firmware Update Over The Air) to transmit updates to all devices simultaneously.

Dryad engineering checks firmware versions of the sensors and if updates are needed then three days are usually required send updates to the sensors. This is because updates are sent in reasonably sized data sections rather than one large update. Generally, Dryad engineering notifies the customer before performing any firmware updates to a Silvanet deployment.

Factors affecting the length of time for FUOTA:

- Strength of device communication (good vs poor communication)
- Supercapacitor energy storage levels (high vs low energy storage).

Mesh Gateway deployment

The Silvanet Mesh Gateway acts as a range extender to allow widespread deployments of Silvanet Sensors using a mesh network. It can be attached to a healthy tree or it can be attached to a self-standing, stable post, pole or pillar that is unlikely to be moved or tampered with.

The Mesh Gateway is equipped with an LoRaWAN antenna to communicate with the Silvanet sensors and gateways using Dryad's network of Mesh Gateways and Border Gateways.

Guidelines

Guideline	Description
Unobstructed solar panel	The device has a large built-in solar panel to provide for the Mesh Gateway's increase power requirements. However, the solar panel needs an unobstructed area to obtain sufficient sunlight to charge the device.
Direction towards sun at 12:00 noon	The Mesh Gateway needs to be oriented towards the direction of the sun (where it would be at 12:00 noon). Use a compass to identify true South (in the northern hemisphere) or true North (in the southern hemisphere). This maximizes the amount of light that hits the solar panel.
Install 3m above forest floor	If installed on a tree, install the Mesh Gateway at least 3 meters above the forest floor, depending on available sunlight in the location. At this height, the device has less interference from human or animal interactions.

Deployment overview

1. The assigned user locates a tree or pole closest to the GPS coordinates set for a Mesh Gateway using the Deployment app.

2. After scanning in the Mesh Gateway's QR Code, the actual position of the device is saved to the Silvanet Cloud. See Device ID Registration.

3. Once a Mesh Gateway is successfully linked to its actual position in the Silvanet Cloud, it can then be deployed.

4. Attach the antenna to the device.

See also

To learn how to register the Mesh Gateway ID in the Deployment app, see Device ID Registration..

Attach to a tree

Use the treenails to attach the Mesh Gateway to a tree. The Silvanet Mesh Gateway has two loops at the top and two at the bottom for the treenails.

To attach the Mesh Gateway to a tree:

1. Lean the ladder safely against the tree, making sure it is stable. Have an assistant hold the ladder, if possible.

2. Locate the correct height (about 3m above forest floor level) on the tree and a southerly direction (where the sun would be at 12:00 noon) where to install the Mesh Gateway. Remove any branches that might interfere with maximum sunlight irradiation.

3. If required, carefully remove a small portion of the bark with an axe where the two holes for the treenails will be drilled. This allows the gateway to hang vertically on the tree.

Remove small area of bark at the install location

4. Drill the top holes using the 10mm drill bit approximately 6–7 cm into the tree. The distance between the holes must be 70 mm.

Tip

When drilling into a hardwood tree, start with a smaller drill bit then drill the final hole with the 10mm drill bit. Also, ensure you are using a drill bit for wood.

Drill two holes space 7 cm apart

Note

If you plan on drilling the bottom holes before attaching the Mesh Gateway to the tree, you can use the Mesh Gateway as a template to locate the positions to drill the bottom holes.

5. Hammer the treenails through the top loops of the Mesh Gateway into the drilled holes. Be careful not to damage the device while doing so. You may need a second worker to support the Mesh Gateway.

Mesh Gateway attached at the top

6. With the Mesh Gateway attached to the tree at the top, drill through the bottom loops of the device approximately 6-7 cm into the tree. Do not damage the Mesh Gateway while drilling through the loops.

Drill the bottom two holes

7. Carefully hammer the treenails through the bottom loops into the holes so as not to damage the device.

8. Attach the LoRaWAN antenna to the Mesh Gateway.

Note
To maximize the radio connection of the Mesh Gateway, the antenna should have at least a finger-width distance from the trunk. Pull the Gateway as far as possible away from the trunk until the loops contact the square ends of the tree nails.

Distance away from tree

9. Check to ensure the Mesh Gateway is securely connected to the tree and does not move.

Mesh Gateway deployed and 2 cm away from the tree

10. The Mesh Gateway is now deployed.

Completed deployment

Attach to a pole (recommended)

We recommend attaching the Mesh Gateway to a pole using the provided U-clamps to attach the device. This securely holds the device and can be tightened accordingly without damaging the device. Also, the device does not interfere with a living tree over the lifetime of the Mesh Gateway.

Info
The maximum diameter of a pole is 60.3 mm. A 17 mm wrench is used to attach the M10-nuts to the U-clamps.

To deploy the Mesh Gateway on a pole:

1. Arrange the U-clamp around the pole and through the predrilled holes of the Mesh Gateway.

Arrange clamps around pole

2. Ensure the Gateway is oriented properly (facing the sun at 12:00 noon) with the antenna connector facing upwards. You may need assistance holding the Mesh Gateway while doing this.

Note
To maximize the radio contact when deploying the Mesh Gateway onto a pole, ensure the top of the device is at the top of the pole (as shown below) so the antenna reaches above the Pole.

Mesh Gateway antenna is above top of pole

3. Hand-tighten the nuts on the U-clamp, then use the 17 mm wrench to tighten the nuts without excessive force to prevent damage to the Border Gateway.

4. Continue with the bottom of the Mesh Gateway as done with the top loops.

5. Attach the LoRaWAN antenna to the Mesh Gateway.

Mesh Gateway deployed on pole

6. Check to make sure the Mesh Gateway is securely connected to the pole and cannot move.

Border Gateway deployment

We recommend attaching the Silvanet Border Gateway (and its solar panel) to a tree or permanent structure located at the edge of the forest border. It can be attached to a fence, a cabin roof or any other type of building. When attached to a tree, use either treenails or crop wire (for temporary deployment). When attached to a pole, use the provided U-clamps.

Ensure the Border Gateway is deployed within range of one or more Mesh Gateways.

When planning deployments of Border Gateways, read Deployment scenarios in *Deployment planning* for more information.

Note
The cable between the solar panel and the Border Gateway is pre-connected. However, the Ethernet cable needs to be connected to the device.

Guidelines

Guideline	Description
Ensure a reliable power source	The Border Gateway can obtain power from a mains power source, from PoE (Power over Ethernet) or from its solar panel.
Ethernet connectivity recommended	We recommend providing the device with access to Ethernet connectivity.
Deploy at edge of forest	Deploy the Border Gateway at the edge of a forest and, ideally, near a reliable power supply.
Install 3m above forest floor	Install the Border Gateway at least 3 meters above the forest floor, depending on available sunlight in the location. At this height, the device has less interference from human or animal interactions.
Needs clear line of site	Whether the Border Gateway is installed on a tree or a pole, it needs a clear line of sight to communicate via wireless mobile networks or satellite communication.

Guideline	Description
Solar panel provides backup power supply	To provide for a fallback power supply if a loss of power occurs, it uses the solar panel but it needs direct sunlight to maximize sunlight irradiation.
Clear access to sun for solar panel	The solar panel needs an unobstructed area to obtain sufficient sunlight to charge the device in case of mains power failure.
Solar panel directed towards the sun as 12:00 noon	Use a compass to identify true South (in the northern hemisphere) or true North (in the southern hemisphere). This maximizes the amount of light that hits the solar panel.

Deployment overview

1. Using the Deployment app, locate a tree or pole closest to the GPS coordinates set for a Border Gateway using the Deployment app.

2. After scanning in the Border Gateway QR Code, the actual position of the Border Gateway is saved to the Silvanet Cloud. See *Device ID Registration*.

3. Once the Border Gateway is successfully linked to its actual position, the device can be deployed to a pole or tree.

4. The Border Gateway can be attached to a tree using treenails or attached to a pole using the supplied clamp.

5. Attach the solar panel to the same tree or pole but above the Border Gateway.

Attach to a tree

The Border Gateway has loops at the top and bottom of the device for deploying on trees using treenails. Any branches on the tree need to be removed so the solar panel has good irradiation from the sun to charge the device.

To attach the Border Gateway to a tree:

1. Lean the ladder safely against the tree, making sure it is stable and cannot fall while climbing the ladder. Have an assistant hold the ladder.

2. Locate the correct height where you will install the Border Gateway (approximately 3m above forest floor).

3. The solar panel needs to be attached in a direction where the sun would be at 12:00 noon.

4. If required, carefully remove a small portion of the bark with an axe where the two holes in the tree will be drilled. This allows the gateway to hang vertically on the tree.

Clear a small area of bark

5. Drill the top holes using the 10mm drill bit approximately 6–7 cm into the tree. The distance between the holes must be 70 mm.

Tip
When drilling into a hardwood tree, start with a smaller drill bit then drill the final hole with the 10mm drill bit. Also, ensure you are using a drill bit for wood. This ensures the wood in the tree does not split.

Drill two holes space 70 mm apart

6. Carefully hammer the treenails through the top loops of the Border Gateway into the holes. You may need a second worker to support the Border Gateway while hammering the treenails into the tree.

Border Gateway attached at the top

7. Continue with the bottom loops. Carefully hammer the treenails through the bottom loops into the tree.

Note
The Border Gateway loops can be used as a template to drill the lower holes. Be careful not to damage the Gateway case and use a drill with a sufficient length.

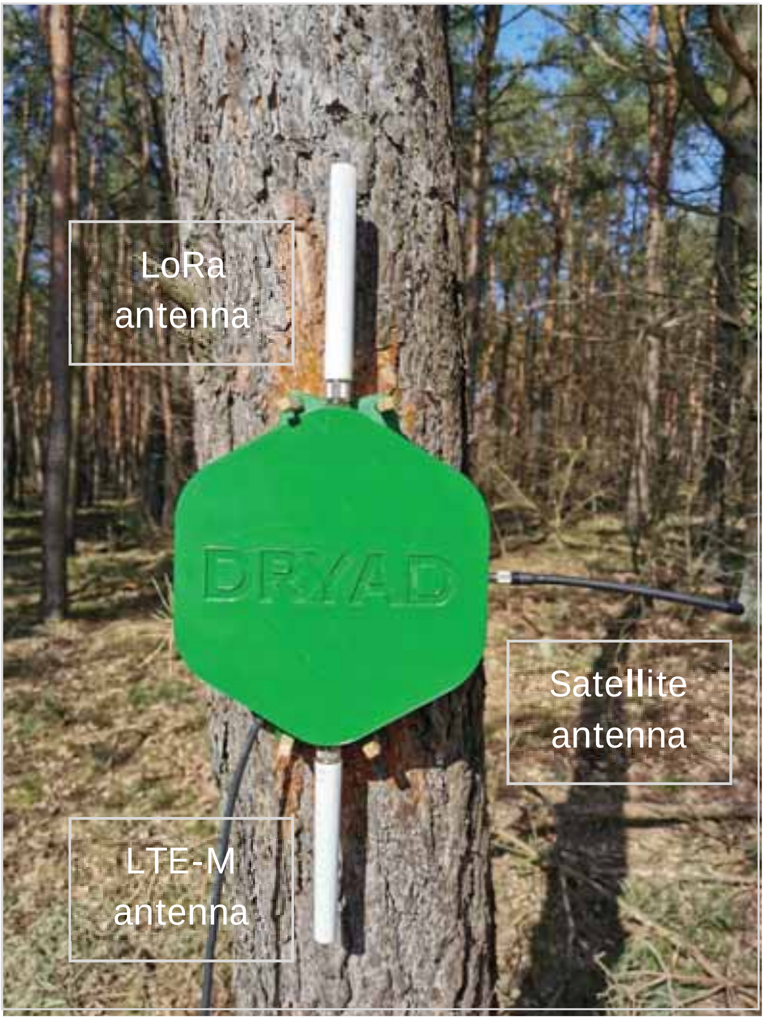
Important

To maximize the radio connection of the Border Gateway, the antenna should have at least a finger-width distance from the trunk. Pull the Border Gateway as far as possible away from the trunk until the loops contact the square ends of the tree nails.

Finger width distance from tree

8. Check to ensure the Border Gateway is securely deployed to the tree and does not move.

9. Attach the SWARM antenna, the LoRaWAN antenna and the LTE/4G antenna to the Border Gateway. If required, connect the Ethernet cable.. See Connecting the Ethernet (PoE) Cable below.



Silvanet Border Gateway with LoRa, LTE and SWARM antennas

10. Deploy the solar panel. See below.

Attach to a pole (recommended)

We recommend attaching the Border Gateway to a pole using the provided U-clamps to attach the device. This securely holds the device and can be tightened accordingly without damaging the device. Also, the device does not interfere with a living tree over the lifetime of the Border Gateway.

Note
The maximum diameter of a pole is 60.3 mm. A 17 mm wrench is used to attach the M10-nuts to the U-clamps.

To attach the Border Gateway to a pole:

1. Insert the U-clamp through the top holes of the Border Gateway and around the pole. You may need assistance holding the Border Gateway while doing this.

Border Gateway to a pole using a clamp

2. Ensure the Gateway is oriented properly with the antenna connector facing upwards, which ensure the Ethernet cable connector faces downwards.

Note
To maximize the radio contact when deploying the Mesh Gateway onto a pole, ensure the top of the device is at the top of the pole (as shown below) so the antenna reaches above the Pole.

3. Hand-tighten the nuts on the U-clamp, then use the 17mm wrench to tighten the nuts without excessive force to prevent damage to the Border Gateway.

Attaching a Border Gateway to a pole using a clamp

4. Attach the U-clamp on the bottom of the Border Gateway.

5. Ensure the Border Gateway is securely connected to the pole and cannot move.

6. Attach the antennas to the Border Gateway. If Ethernet is available, connect the Ethernet cable to the connector.

Border Gateway deployed on a pole

7. Attach the solar panel to the pole. See below.

Attach the solar panel

Once the Border Gateway has been attached to a pole or tree, attach the solar panel to the same tree or pole, if possible. The cable from the Border Gateway to the solar panel is pre-connected and is 2 m long. Crop wire is used to attach the solar panel to a tree or pole.

Note
We recommend attaching the Border Gateway and the solar panel to the same tree or pole. If the solar panel is attached to a different tree or pole, take care that the cable cannot become damaged by others using the forest or paths.

Follow these guidelines for deploying the solar panel:

- If the solar panel is attached independent of the Border Gateway, it cannot be more than 2 m away, ideally closer.
- Position the solar panel so that it is facing towards the sun (at 12:00 noon) to maximize sunlight irradiation.
- Ensure the solar panel cable is placed in such a way that it cannot be damaged by human or animal incidents.
- If the deployment location is a public area, we recommend the minimum height for both the Border Gateway and the solar panel to be 3m above the forest floor.

- Check also to make sure the solar panel is tightly connected to the tree or pole so that it cannot slip or turn during strong winds or other environmental actions.

The following shows the solar panel attached to a tree using crop wire:

Solar panel attached using crop wire

The following shows a completed Border Gateway and solar panel deployment:

Solar panel attachment completed

Connect the Ethernet (PoE) Cable

The Border Gateway provides a sealed RJ45 connector to attach an Ethernet cable to the device. The Ethernet connection can provide a continuous power supply to the Border Gateway through the PoE Adapter which uses a mains power supply.

For more information about Border Gateway deployment scenarios using a PoE Adapter, see Setup with a PoE-ready router in Deployment planning.

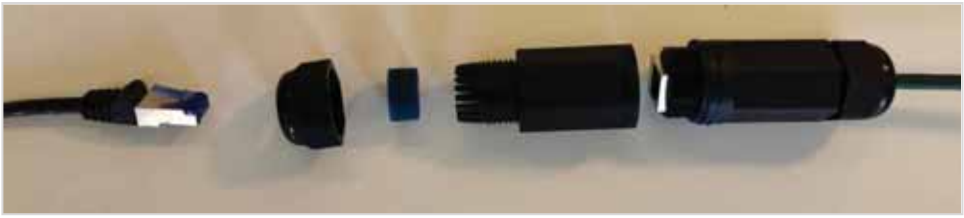
Note
When using Ethernet, the Border Gateway should be deployed as close as possible to the router and, ideally, on top of the building that houses the router.

To connect the Ethernet cable to the Border Gateway:

1. Open the Ethernet connector on the left side by unscrewing the cap (as shown below).

Border Gateway open Ethernet connector

2. Disassemble the Ethernet connector, including the end cap, sealing ring and housing.



Border Gateway disassemble Ethernet connector

3. Lead the Ethernet cable through the end cap, sealing ring and housing.

4. Connect the Ethernet cable with the Ethernet socket in the connector.

Border Gateway Ethernet connected

5. Reassemble the connector. Carefully seat the sealing rings in the housing without damaging the barbs, then screw the end cap on the housing and screw the housing to the connector.

Border Gateway reassembled

Deployment verification

After sensors and gateways have been deployed, use the Site Management app to verify the status of the devices.

To verify the deployment:

1. Login to the Site Management app.

2. Select the Site name from the available Sites.

3. In the Site's dashboard, select the Sensors tab. This tab is located below the Overview section of the Site dashboard.

4. The **Sensor** icon next to a sensor ID indicates whether the sensor has been deployed properly and is sending and receiving data. Refer to the document **Status Icon** for details.

The following shows an example sensor status showing gray, yellow and dark green status icons.

Sensor deployment status

Fire notifications

After the deployment of Silvanet sensors, 14 days are required for the sensors to calibrate or adapt to the environment in which they have been deployed. Before this calibration period ends, the sensors do not provide accurate readings which means they are not ready to detect fires. They may also generate false Fire Alerts during this period.

Phase 1 – test for air quality deterioration

After the sensors have been calibrated and ready to detect fires, the gas sensor embedded in the Silvanet sensor "smells" the air and generates Air Quality values. If the gas sensor detects a significant variation (deterioration) in air quality within a short period of time, it triggers a Phase 1 alert (yellow), which is not seen by end users.

Phase 2 – test for fire

The Phase 1 alert causes the gas sensor to perform a series of gas scans to measure the air. The scan results are compared to a Machine Learning (ML) model embedded in the sensor memory to determine the probability that the "smell" comes from a smoldering fire.

If the probability exceeds a defined threshold, then the sensor has predicted that a fire has occurred within the range of the sensor. This triggers a Phase 2 alert (red), which appears as Fire alerts in the user's Site Management app and as an email sent immediately to a user's email account.

User response to fire

When a registered user receives a Fire Alert, immediate action can be taken to extinguish the fire. The Fire alert also includes location of the detected fire.

Sensor calibration

After a Silvanet sensor has been deployed, the device's low-power BME866 gas sensor requires **14 days** to calibrate, that is, to "settle in". This ensures the gas sensor adapts to the environment in which the sensor has been deployed. After 14 days, the gas sensor environmental readings eventually stabilize to an optimal level of sensitivity. If any **gas scans** are performed after the sensors are ready, the sensor needs at least 1-2 hours to be ready again. Any **interactions** with the sensor cause a recalibration which takes at least 5 days.

Calibration process

WARNING: INTERACTING WITH DEPLOYED SENSORS AFTER THEY HAVE BEEN CALIBRATED AND "SETTLED IN" CAUSES ERRORS WITH SENSOR VALUES AND COULD ALSO RESET THE SENSOR CALIBRATION. FURTHERMORE, IF A SENSOR IS MOVED TO A NEW LOCATION, IT AUTOMATICALLY RUNS THE CALIBRATION PROCESS AGAIN.

Calibration process

When a sensor is delivered to the user, it is ready to be deployed, charged up and then calibrated. No additional settings need to be made to the device.

One day to charge the sensor after deployment

After the sensor is installed on a tree and synced to the Silvanet Cloud using the Dryad Deployment app, **1 day** is required to fully charge the supercapacitors. Once charged, the sensor's solar panel continuously charges the supercapacitors, except of course during the night.

14 days to calibrate the sensor

After the sensor has been fully charged, the sensor begins a calibration process which typically takes **14 days**. An algorithm running in the sensor automatically performs this calibration to adapt itself to the typical environment where the sensor has been deployed. The gas sensor does this by running gas scans for several days and uses the results to build an initial model (an air quality value) of the environment within range of the sensor. It then deploys this model and sets an auto-trigger configuration. This optimizes the sensor for fire detection and ensures any false positives are eliminated (sending fire alerts when there is no fire).

Sensor ready after 14 days

After the 14-day calibration period, the sensor is **ready** to detect fires.

After gas scans requires 1-2 hours to return to normal values

The sensor returns to normal values **1 to 2 hours** after the sensor performs gas scans as part of a Phase 2 fire detection process. This allows the sensor to stabilize and return to its base readings. The sensor does not measure any changes in the environment during the gas scans. See Allow sensor to return to normal values below.

Any interactions with the sensor causes the sensors to recalibrate for 5 days

If any **interactions** occurred with the sensor after deployment, **5 days** are required to recalibrate the sensor. Interactions include being moved by an animal or human or even being touched or breathed upon. This interaction causes a repeat of the calibration process, but not a full 14-day recalibration. This is why attaching the sensor at least 3 meters above the forest floor is important. Furthermore, if the sensor is moved to a new location, it automatically runs the calibration process again.

Continuous microclimate monitoring

After calibration, the gas sensor continuously monitors the microclimate of the forest air to measure *air pressure*, *temperature*, and *humidity*.

It also "smells" the air around the sensor for the presence of Volatile Organic Compounds (VOCs) and carbon monoxide. By continuously monitoring the microclimate, the gas sensor tracks historic readings of VOCs to produce a stable baseline called Normal Air which is unrelated to the presence of VOCs associated with a smoldering fire. This produces an Index of Air Quality (IAQ) value.

> **Note**: VOCs are compounds that have a high vapor pressure and low water solubility.
>
> The change in Air Quality (increase in IAQ) can be triggered by several events. Other environmental factors other than fires can cause a deterioration in air quality such as diesel engine fumes in the vicinity of the sensor, moving the sensor or even the breath of someone coming close to the sensor.

Normal and declining air quality

Continuous monitoring results in the sensor *learning* to distinguish between *Normal Air Quality* and *Declining Air Quality*. A decline in air quality is reflected as an increase in the IAQ value.

Note: *Normal Air Quality* is the result of the 14-day calibration period of the sensor. It is the baseline reading of the air quality. *Declining Air Quality* could be the result of fumes from a smoldering fire but it could also be the result of detecting gases such as diesel fumes from a passing truck or other factors other than a fire that caused a negative change in air quality.

This increase in the IAQ value, which is a deviation from normal air quality, triggers a process to determine if the deviation is the result of gasses produced by the smoldering phase of a fire in a forest. This begins with a Phase 1 detection process.

Sensor interactions

WARNING: AFTER SENSORS HAVE BEEN DEPLOYED, CALIBRATED AND SETTLED, DO NOT INTERACT WITH THE SENSORS AS THIS WILL CAUSE ERRORS WITH SENSOR VALUES AND COULD ALSO RESET THE SENSOR CALIBRATION. DRYAD STRONGLY ADVISES LEAVING THE SENSORS ALONE ONE THEY ARE DEPLOYED.

Sensor interactions trigger recalibration

Sensors are very sensitive to any changes in the environment, including something as simple as touching them or moving them. Any interaction with a sensor triggers a Phase 1 alert, which in turn triggers a Phase 2 process causing the sensor to perform a set of gas scans to determine if it has detected a fire.

Interacting with sensors includes:

- Touching the sensors (banging on it, hitting it)
- Moving the sensors (swinging it around the treenail)
- Being in proximity to the sensors (breathing on the sensor)
- Having vehicles, especially diesel trucks, nearby the sensors (driving by the sensor)
- Bringing nearby the sensor any environmental source that could trigger a Phase 1 alert such as cigarettes, machinery, and so on

Returning to normal values after gas scans

If a Phase 1 alert was triggered, the sensor needs at least 2 to 4 hours to return to normal values. During this period, the sensor does not measure any changes in the environment. After this period, the sensor is ready again to begin fire detection procedures.

Phase 1 alerts (yellow)

Each sensor in a deployment checks the air quality every minute. If within a short period of time (using a default sliding time window of 5 minutes) the air quality within the range of a sensor has significantly deteriorated, a Phase 1 alert is triggered. However, it is triggered only if the IAQ (Index of Air Quality) value has significantly increased by a value of 50 during this time.

WARNING: The sensor may not have detected a fire even though a Phase 1 alert was triggered. The change in Air Quality (increase in IAQ) can be triggered by several events. Other environmental factors can cause a deterioration in air quality such as diesel engine fumes in the vicinity of the sensor, moving the sensor, or even the breath of someone coming close to the sensor.

Phase 1 fire detection process

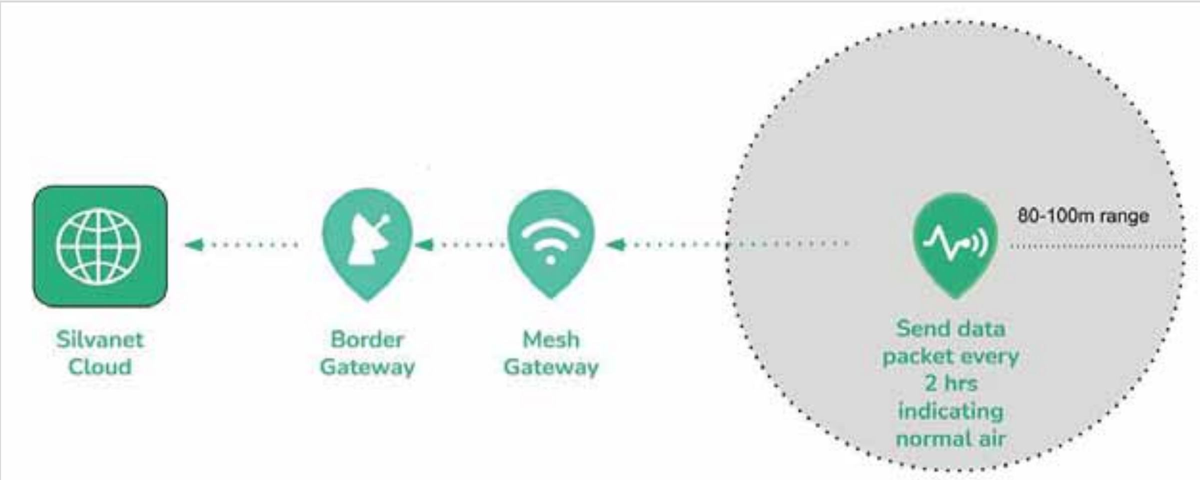
Step 1 - check air quality

Once every 60 seconds, the sensor checks Air Quality using an algorithm.

Step 1: Check air quality every 60 seconds

Step 2 - send data packets every 2 hours

Send data packets to Silvanet Cloud every 2 hours. As long as the sensor detects "**Normal Air**", that is, the baseline IAQ determined during calibration remains stable, it sends data packets to the Silvanet Cloud every two hours. These data packets contain *air pressure*, *temperature* and *humidity* readings.



Step 2: Send data packets every 2 hours

Step 3 - Deterioration of air quality triggers Phase 1 alert

If the **Air Quality has significantly deteriorated** (IAQ change > 50) within a short period of time (using a sliding window of 5 minutes), then the gas sensor issues a Phase 1 alert. This alert is sent to the Silvanet Cloud. Clients do not receive this alert but is used internally to determine why the sensor reacted.

Step 3: Deterioration of air quality triggers Phase 1 alert

Step 4 - Phase 2 fire detection process initiated

Phase 2 detection process is triggered to determine if the sensor has detected a fire. See [Phase 2 fire detection process](#).

Note: The sensitivity of the Phase 1 algorithm (threshold and sliding time window) can be configured remotely by Dryad's support team. In the future, Dryad is planning to enable self-configuration by customers using the Site Management app as well as an adaptive algorithm aimed at reducing the number of Yellow Warnings over time.

Phase 2 alerts (red)

After the sensor triggers a [Phase 1 alert](./fire-detection-phase1.md), the BME688 gas sensor triggers a Phase 2 fire detection process to determine if the observed deterioration in Air Quality is from a smoldering fire or from some other source. If this process determines a high probability that the sensor has detected a smoldering fire, then the sensor sends a Phase 2 alert to the Silvanet Cloud. Otherwise, the sensor needs to reset, which takes from 2-4 hours to complete.

Note: A smoldering fire is defined to be a slow, flameless combustion of a biomass material such as forest floor material, branches, leaves, and so on.

Gas scans and Fire Models

A Phase 1 alert is not necessarily an indicator of a fire (under normal conditions). It only indicates a change in IAQ value, where IAQ > 50. This alert triggers a process in the BME688 sensor which is a prescribed set of gas scans. Since gas scans consume a lot of energy, they are reduced to the required minimum and only start after a Phase 1 alert has been triggered.

Each scan consists of individual measurements of the raw resistance values taken at different temperatures. The ML model deployed on the sensor takes these measurements as input to determine if the observed change can be classified as wildfire smoke.

The results of the gas scans is the real test for a fire. Up to 60 gas scans are run but if the sensor determines a fire is the most likely cause for the deterioration of air quality before the gas scans have completed, the BME688 sensor stops running the gas scans and the sensor immediately issues a Phase 2 alert.

The sensor uses the built-in BME688 gas scan procedure along with a ML (Machine Learning) Model to determine if the change in air quality is from a fire or from some other source. ML (Machine Learning) Models are pre-trained in the Dryad laboratory and can be fine-tuned / programmed specifically for the species of trees present in a particular deployment. Updated models can be remotely installed in the sensors by Dryad's support team using FUOTA.

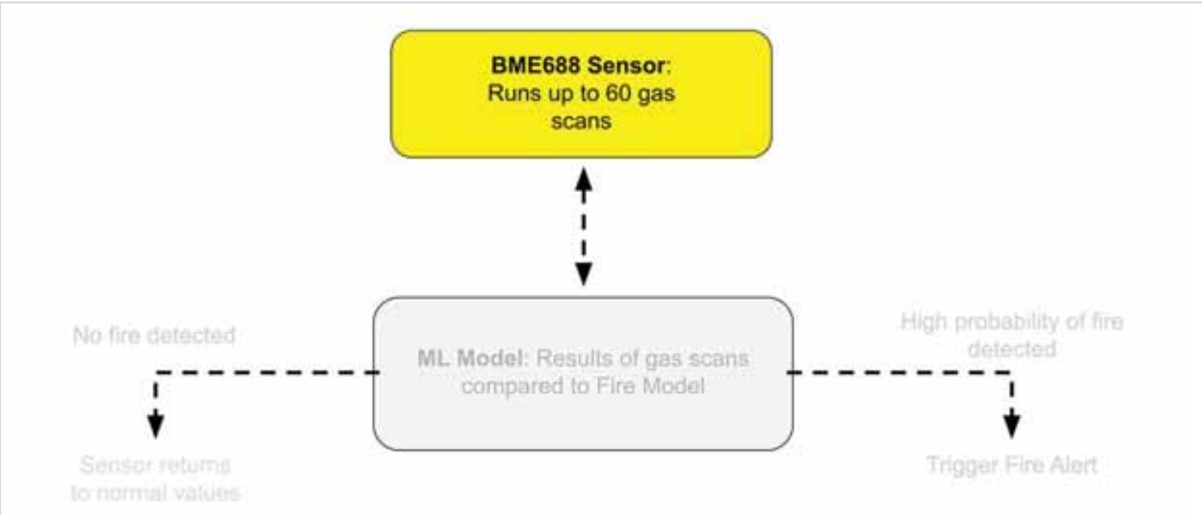
> **Warning:** After the sensor performs gas scans, it needs 1 to 2 hours for the sensor to return to baseline. While it is returning to baseline, it cannot take in any additional data to detect fires.**

Phase 2 fire detection process

A Phase 2 fire detection process happens within a very short period of time. From receiving the Phase 1 alert to determining if a fire is present, the sensor takes no more than 1-2 minutes.

Step 1 - BME688 sensor runs gas scans

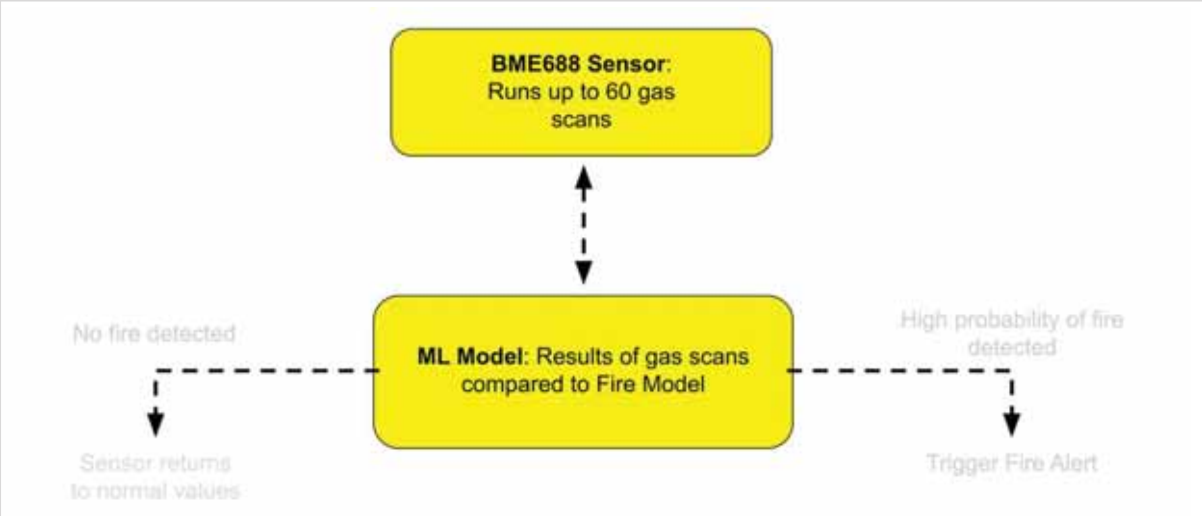
After a Phase 1 alert is triggered, the BME688 gas sensor automatically performs up to 60 consecutive gas scans (if necessary) which takes 1-3 minutes to complete. During the gas scan, the sensor measures hydrogen, carbon monoxide and other Volatile Organic Compounds (VOCs).



Gas sensor runs up to 60 gas scans

Step 2: Scan results compared to a ML Model

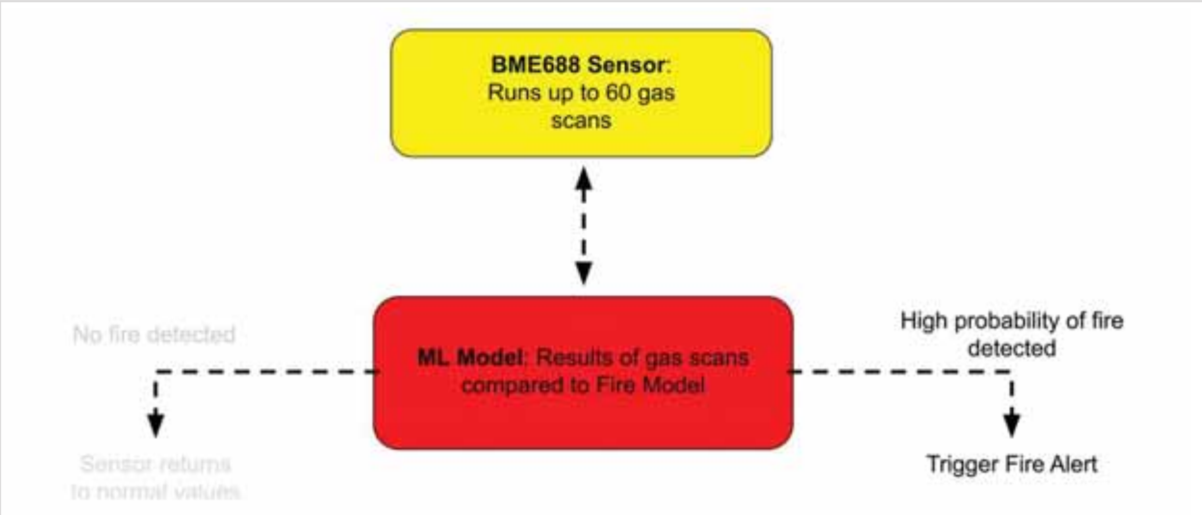
The Silvanet sensor uses a Machine Learning (ML) model to compare the gas scan measurements with pre-trained ML Models to reliably detect the gas composition typical for a wildfire. The ML process begins by taking readings from the BME688 gas sensor (gas scans) to determine if the observed disturbances can be classified as wildfire smoke.



Gas scan measurements compared to ML Model

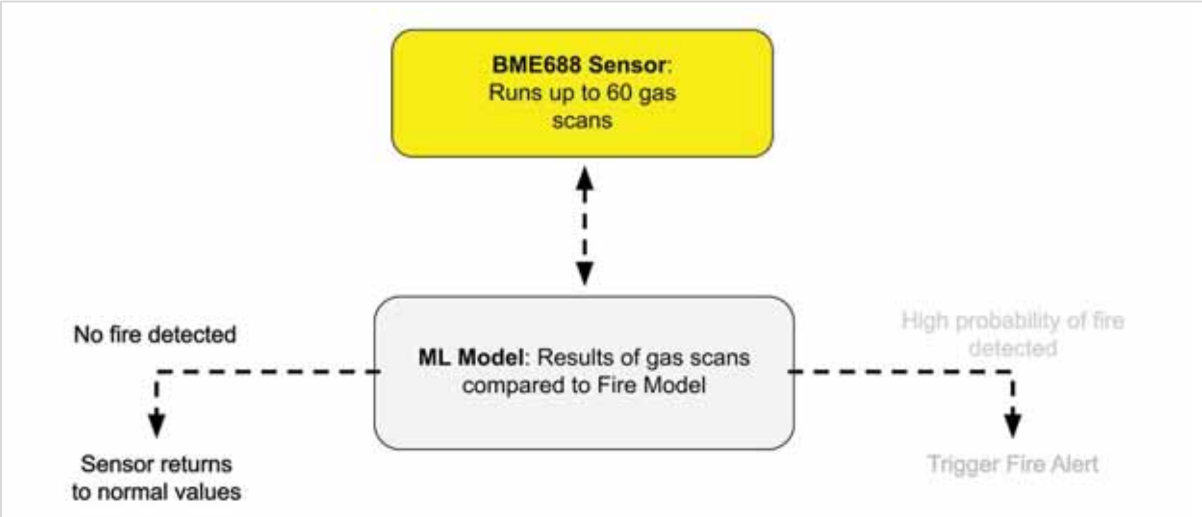
Step 3: Positive results triggers a Phase 2 Alert

If the ML model determines that the decline in air quality has a very high probability of being the result of a smoldering fire, the Silvanet sensor immediately sends a Phase 2 (Red) Alert to the Silvanet Cloud.



Fire detected

If the gas scans and ML Model determined some other source has caused the decline in air quality (diesel fumes or some other similar gases), then the sensor does not trigger a Phase 2 alert and must reset the sensor. This can take up to 2 to 4 hours.



No fire detected

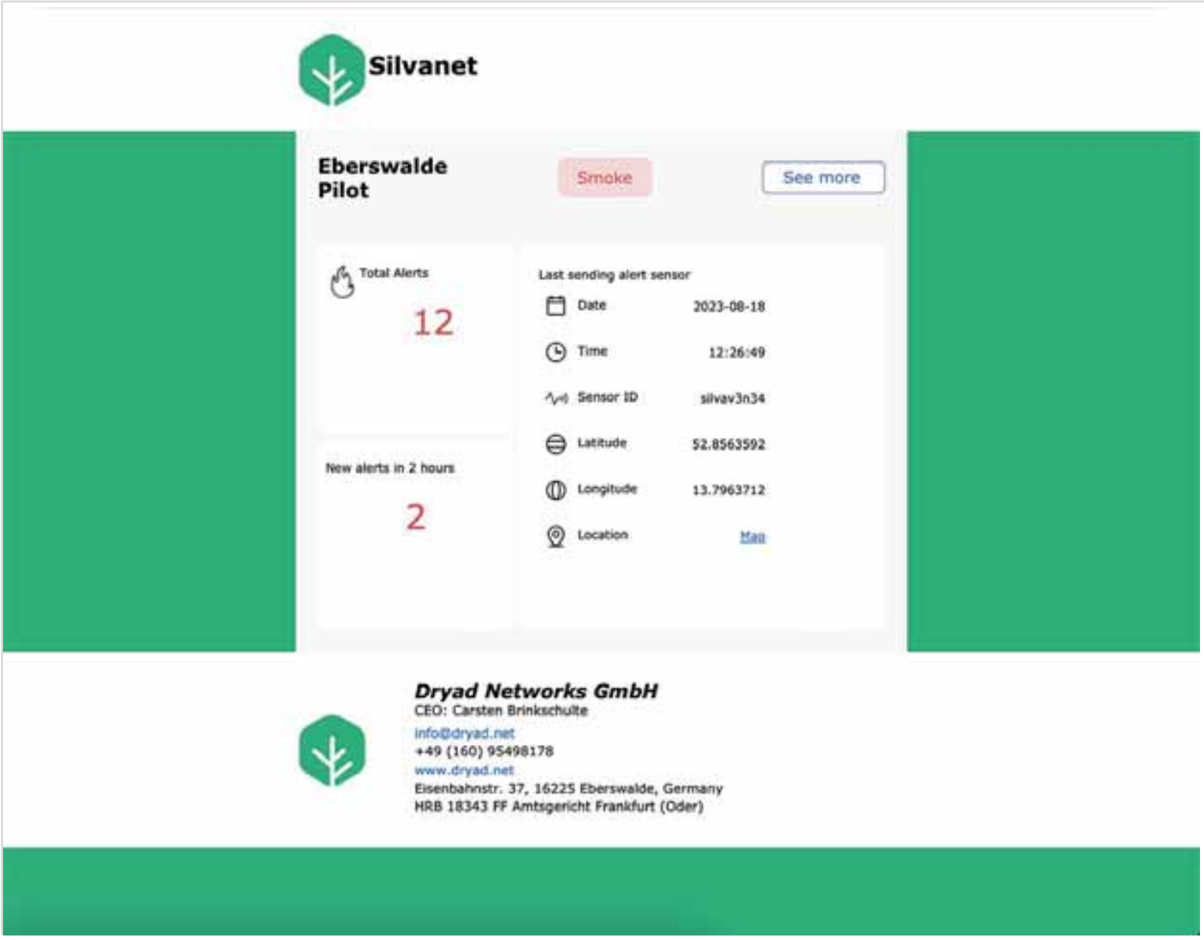
Step 4: Fire Alerts are sent immediately to the Silvanet Cloud

Phase 2 fire alerts initiate a packet stream where Fire alert data packets are sent via the Mesh Network to the Silvanet Cloud.

Phase 2 alert sent to Silvanet Cloud

Step 5: Fire notifications sent to users

The Silvanet Cloud then initiates an [**email alert notification**](./fire-alert-email.md) to the user's email account. A [**Fire alert icon**](./fire-alert-web.md) appears in the Site Management app belonging to the user's Dryad account.



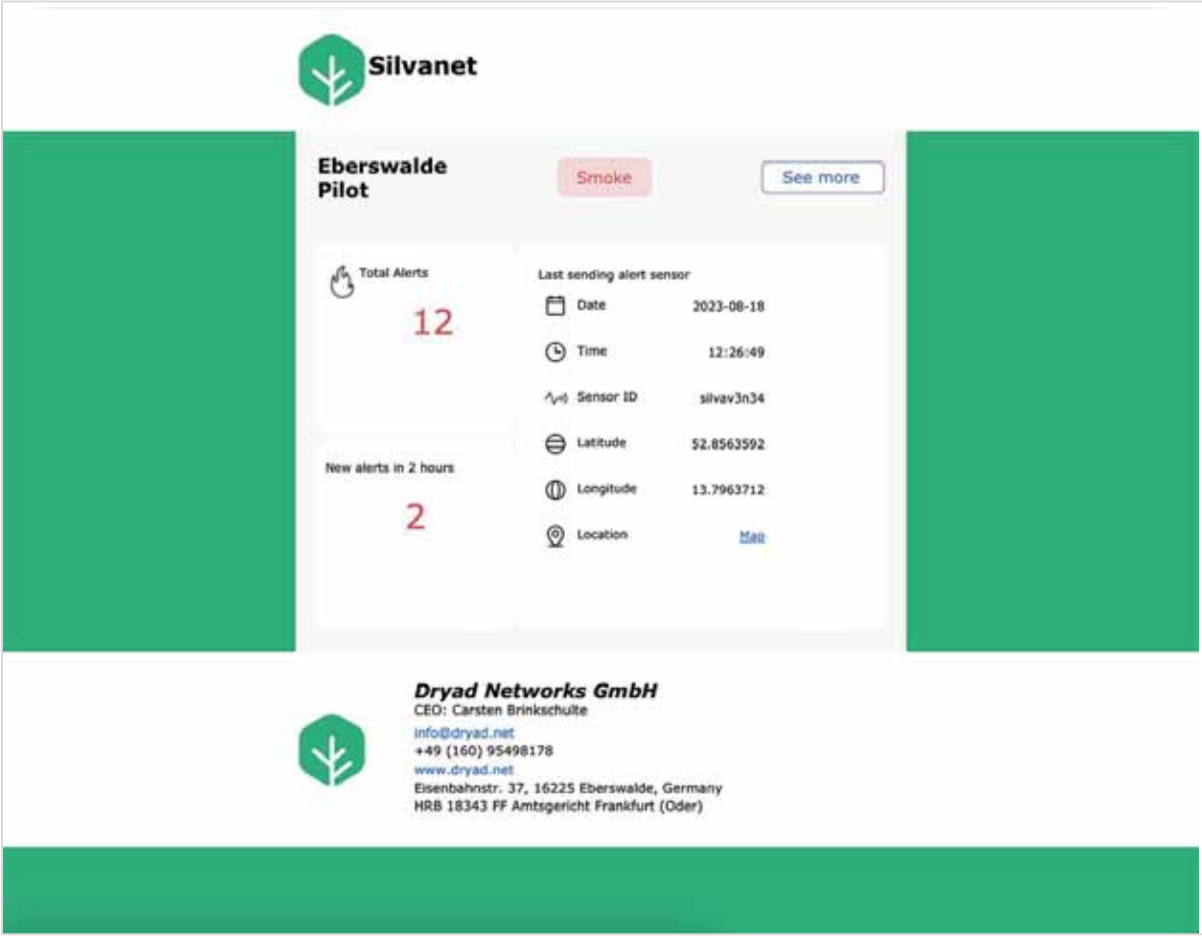
Email fire alert

Fire Alerts (Email)

If a sensor detected a fire which triggered a Phase 2 alert, a Fire alert is immediately sent to registered users who can then act to extinguish the fire. The Fire alert also appears in the user's account of Site Management app.

The Fire Alert email indicates which sensor sent the Phase 2 alert (providing its sensor ID). The email shows the date and time when the sensor sent the alert and includes the GPS coordinates of the sensor.

Selecting the **Map** link opens Google Maps showing the location of the sensor. If Google Maps is not installed, it launches a browser on the smartphone and opens Google Maps in the browser.

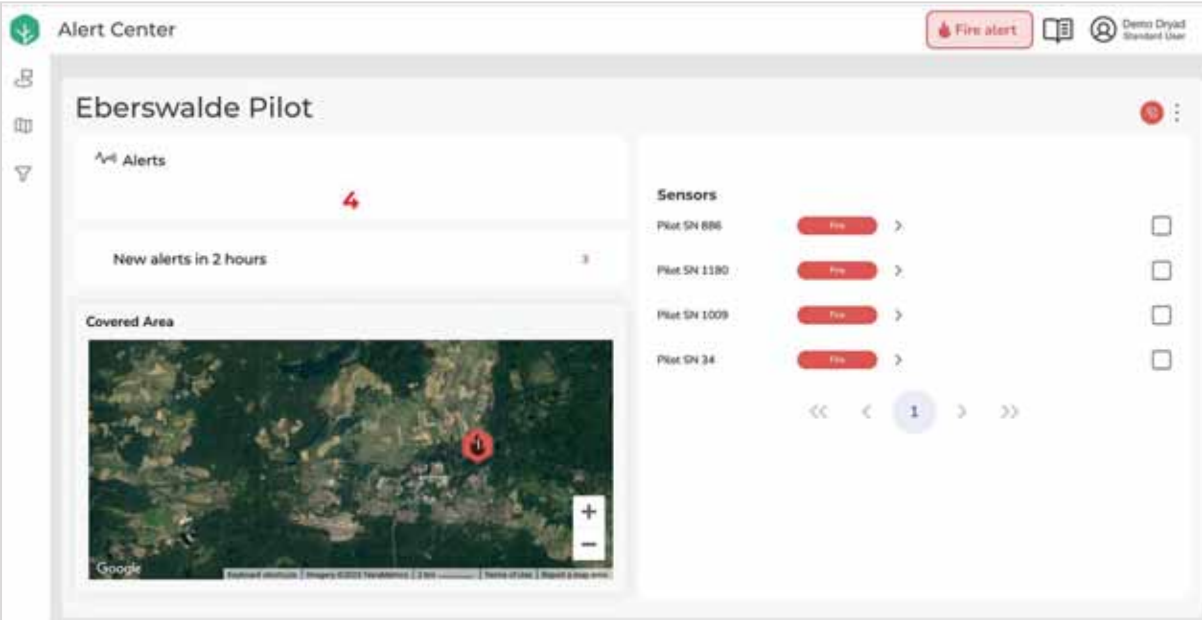


Example email fire alert

Fire Alerts (Dryad Web app)

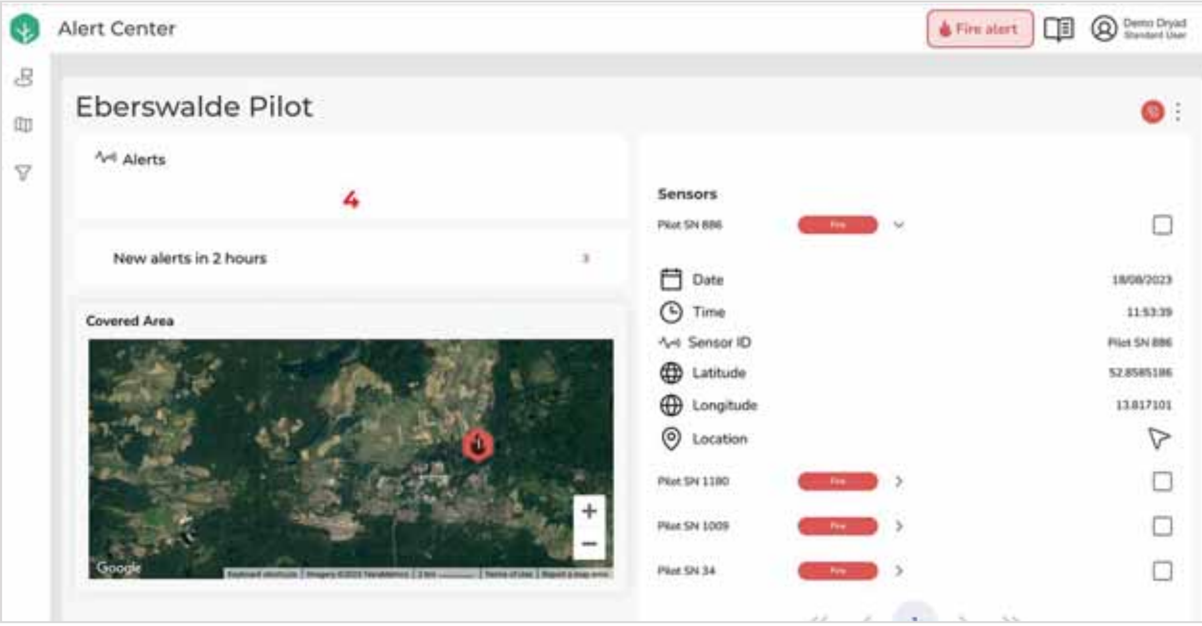
If a sensor detected a fire which triggered a Phase 2 alert, the Site Management app displays a Fire alert icon appears to warn a registered user of the fire. Selecting the alert icon displays in a Site map its location in the forest.

The following shows a fire alert in the top right corner of the Site Management app. Selecting the Fire alert icon provides detailed information about the location of the fire.



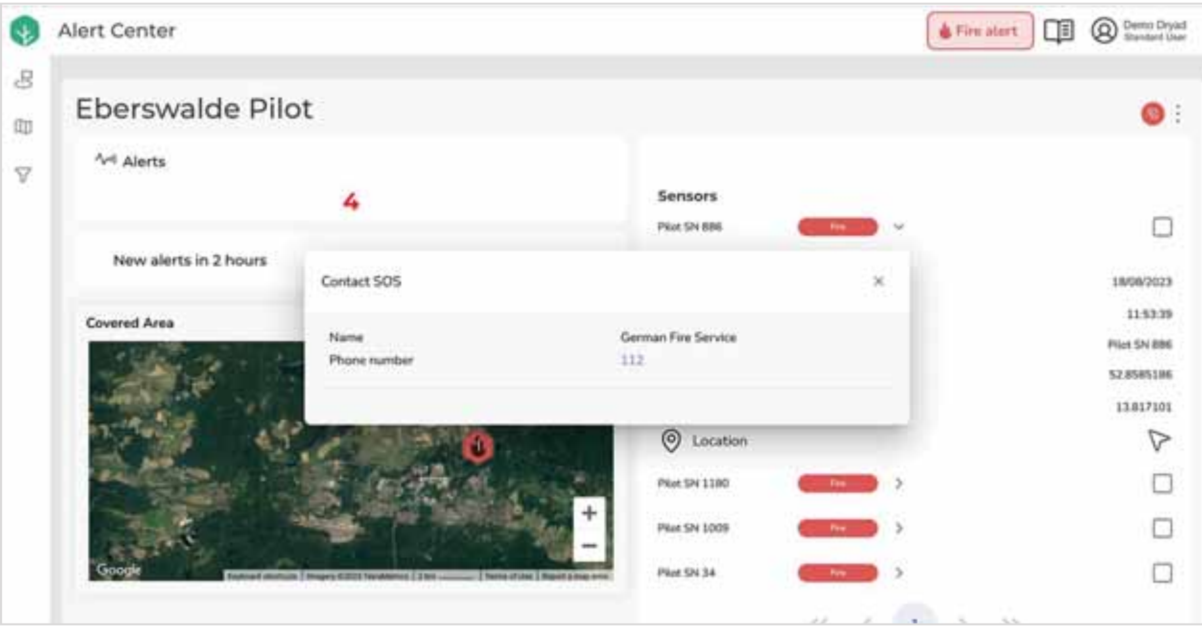
Fire alert icon

Selecting a Fire icon next to a sensor provides detailed information about the location of the sensor sending the Phase 2 alert.



Fire alert details

Selecting the **Phone** icon provides the phone number of the local emergency service contact information (fire department).



Emergency service contact information

Note
An MQTT interface is available for 3rd party alarm interfaces / apps. For more information, contact Dryad Support.

Deployment testing

When testing a deployment of the Silvanet System, ensure you have prepared the test according to the pre-test checklist and testing guidelines described in this section. Preparing for the test requires considerable preparations before safely burning a controlled test fire and reading the results in the Dryad Web app. Additionally, carefully follow the instructions for making modifications to the test setup.

Deployment testing with a controlled test fire

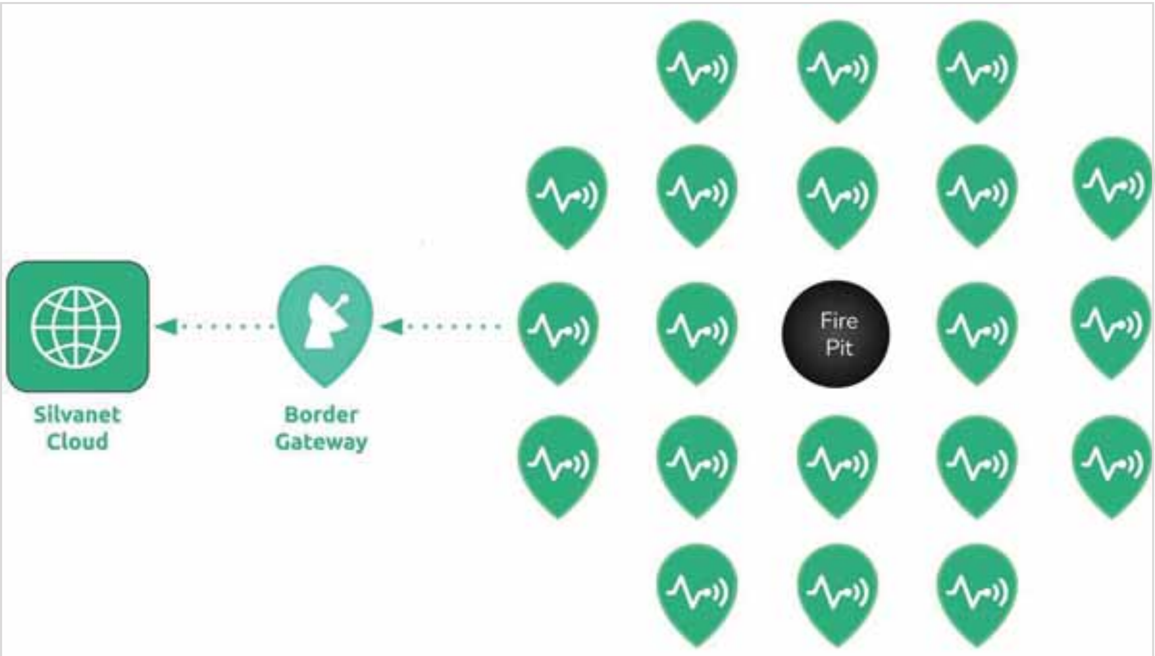
Warning
AFTER SENSORS HAVE BEEN DEPLOYED, CALIBRATED AND SETTLED, DO NOT INTERACT WITH THE SENSORS AS THIS WILL CAUSE ERRORS WITH SENSOR VALUES AND COULD ALSO RESET THE SENSOR CALIBRATION.

Test deployment

A test deployment allows you to burn a small test fire (about the size of a BBQ fire) and get a Fire Alert message from the sensors.

Without having built up a complete system, this example test deployment demonstrates the basic steps to deploy and test the core functionality of Silvanet System.

Device	Description
Sensors	Use two boxes of Silvanet Sensors (10 in each box) and deploy the sensors in a tight grid of approximately 15m distance from each other. By reducing the distance between the sensors, the detection time and amount of burning material needed for testing and validation is significantly reduced.
Gateways	Uses one Border Gateway to receive data from the sensors and to connect to the Internet.



Example test deployment

Deploy the sensors using a grid pattern and place the Border Gateway at the edge of the forest near a path or roadway. If possible, place it where it can obtain a power supply and/or Ethernet connectivity.

As the sensors are deployed in a dense grid, the test deployment does not need a Mesh Gateway. It does, however, require line of sight from all sensors to the Border Gateway. It should not be set up in hilly terrain where hills or large rocks could interfere with the wireless signals.

Pre-test checklist

Warning
DO NOT PROCEED WITH A TEST IF YOU HAVE NOT READ THESE STEPS.

Ensure you have read the following checklist before beginning the deployment test.

Step	Item	Description
Step 1	Prepare deployment Packet	Site Packet is prepared for the deployment of Border Gateway and sensors.
Step 2	Deployed Border Gateway	Border Gateway is deployed with a reliable power supply. Border Gateway has Internet connectivity via Ethernet or LTE-M mobile.
Step 3	Deployed sensors	Sensors are deployed at the locations set in the Packet and the Device IDs (QR Codes) are scanned into the Packet in the Deployment app.
Step 4	Verify deployment	Using the Site Management app or the Deployment app, ensure the sensors are sending data to the Silvanet Network.
Step 5	Do not interact with deployed sensors	Once deployed, **DO NOT INTERACT** with sensors before or during a test.
Step 6	Allow 14 days for sensors to calibrate	Sensors **MUST be allowed to calibrate** in the planned location for 14 days.

Step	Item	Description
Step 7	Prepare test fire material	Dry test fire material and store it indoors for at least 14 days. This can be done concurrently to the calibration period. Fire department has been informed of the test fire.
Step 8	Notify Fire Department	Ensure the local Fire department has been informed of the test fire.
Step 9	After test, safely discard fire ashes	Remove burnt material before putting in new material. Ensure burnt material from any previous test fire has been thoroughly put out and no embers are hidden in the ashes as they can ignite other material.
Step 10	If required, modify the test setup	When modifying the test, change only one element per test. For example, change the type of burning material but do not move the sensors.
Step 11	4-5 hr. sensor settle-in period. required	After modification, let the sensors settle for 4-5 hours after any changes to the test, such as new burning material or sensor spacing.

See also

For more information about planning and deploying the hardware of the Silvanet System, refer to the **Planning Deployments** and **Deploying Silvanet Devices** documents.

Testing guidelines

Read the following guidelines carefully to get the most out of running controlled fire tests using the hardware of the Silvanet solution.

Ensure Internet connectivity

Ensure the deployed Border Gateway is connected to Internet.

The deployed Border Gateway MUST has a reliable power source and is fully charged before testing.

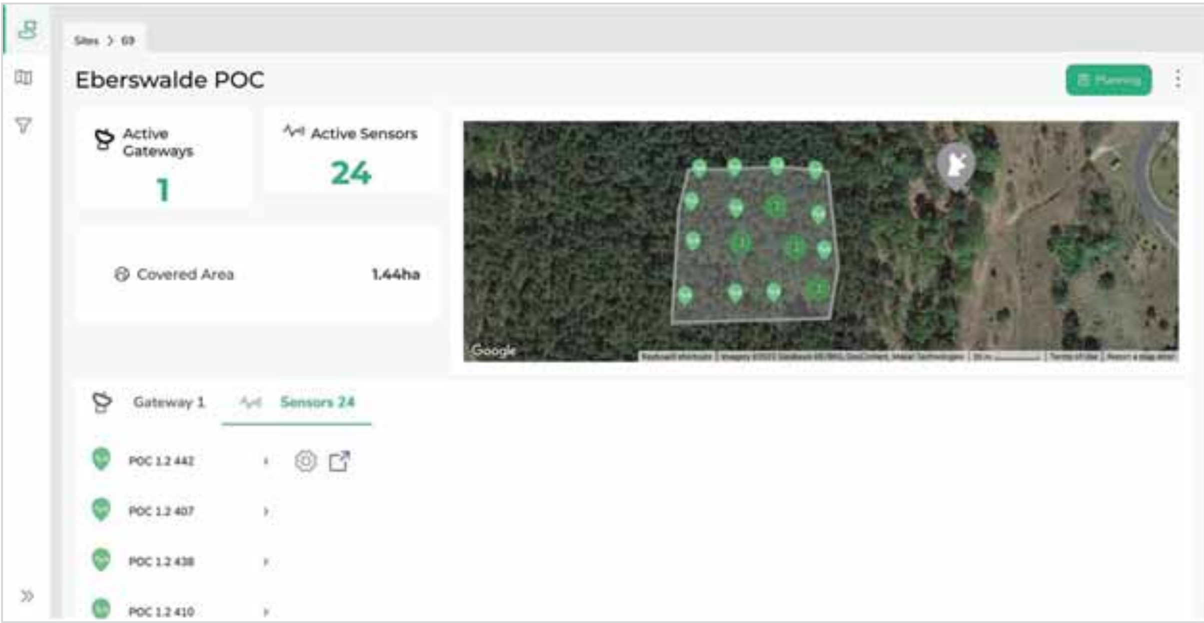
- If the border gateway is powered only by the solar panels, then it most likely enters power saving mode during the night. Allow the Border Gateway to fully charge in the morning before testing.

Note
Fire alerts will be handled with priority and will wake up the modem from power save mode.

The Border Gateway MUST be online with a stable connection either through cellular modem or POE (Power Over Ethernet).

- After the sensors and Border Gateway have been deployed and charged, ensure they are communicating with the Silvanet Network.

- You can verify this using the Site Management app. From the Site Management app, select the test site. In the Site dashboard, active sensors appear as green icons while inactive sensors appear as gray icons.



Connected sensor

DO NOT INTERACT WITH SENSORS AFTER DEPLOYMENT

The gas sensor in the Silvanet sensor is very sensitive to outdoor changes. Consequently, moving, touching or interacting with the sensors influences the sensor readings and the sensor calibration settings.

For the sensor to return to normal values so that a valid test can be performed, the sensor needs at least 1 hour to return to its base readings. Consequently, the sensor is less sensitive to changes in the environment if a test is run during this stabilization period and consequently, fire detection may be affected.

The stabilization period (4-5 hours) required after touching or moving sensors can cause an interference with the test, which results in faulty test results. So, we strongly advise leaving the sensors alone once they are deployed.

Warning

AFTER SENSORS HAVE BEEN DEPLOYED, CALIBRATED AND SETTLED, DO NOT INTERACT WITH THE SENSORS AS THIS WILL CAUSE ERRORS WITH SENSOR VALUES AND COULD ALSO RESET THE SENSOR CALIBRATION.

Use homogeneous material for test fire

Use a collection of homogeneous material (uniform in size and composition) for the test fire that creates smoke and is freshly cut.

Guideline	Description
Similar plant material to final deployment location	Collect between 5 and 10 kg of typical plant material similar to the final deployment location, including smaller and bigger twigs, leaves as well as freshly cut and previously dried branches with needles.
Ensure material is dried and stored	Dry out in advance the collected material and store them in a cool, dry location. Use the duration of the calibration period to allow the material to dry out and to be ready for burning.
Weigh material for one test fire	Weigh the branches with a scale before placing them on the fire pit. This allows for using the same material with the same amount for each test.
Enough material required for 30-minute burn	Collect sufficient material to keep the fire burning for up to 30 minutes.

Ensure Calibration period is complete

Confirm that the deployment is complete and the deployed sensors have completed their **14 days initial calibration period**.

No testing should be conducted prior to the completion of the initial calibration period since the sensors will not provide accurate readings.

Burn a realistic test fire

Ensure you have sufficient homogeneous material to burn and maintain a test fire. To reflect conditions of real wildfires, the **test fire should not diminish as the test runs**. The fire should not resemble a BBQ fire.

As the wind direction cannot be controlled, provide sufficient time for smoke from the test fire to hit the sensors.

Ensure test fire burns for at least 30 minutes

Ensure you continually feed the fire with material to keep the fire burning for at least 20-30 minutes to allow smoke from the test fire to reach the sensors. The sensors are built to detect fire at the smoldering phase - before there is an open fire.

Normally, time to detection is within minutes (less than 1 hour from ignition). This is dependent on fuel volume, wind speed and wind direction. A denser deployment will decrease the time to detection and detection rate.

Use an initial and a modified test setup

Before beginning the test fire, ensure you allow the sensors to perform the 14-day initial calibration period. **Sensors will not provide accurate readings when tested before or during the calibration period**. Afterwards, start the test fire and begin testing Silvanet.

After obtaining results from the initial round, perform additional tests by modifying only one aspect of the test. Possible modifications include:

- Distance from fire to the sensors. The further away the sensors are from the fire, detection time becomes longer.
- The location of the fire within deployment. Take into consideration the 2-to-4-hour cool-down period of the sensors between tests.
- Burning different materials in the test fire.

Important
For repeated tests. the same type and weight of material for burning MUST be identical to that used in the initial test.

Allow sensors to settle (4-5 hrs) between tests

When performing fire tests, it is common practice to repeatedly light a fire and check the response. However, repeatedly exposing the sensors to smoke in short time intervals results in poor sensor performance. After being exposed to smoke, the sensors need time to settle and restore their original fire detection sensitivity.

Consequently, after completing a test, give the sensors time to return to normal values. Any smoke retained inside the sensor mesh and housing needs to dissipate to allow the sensors to return to normal values. Ideally, the longer the wait, the more smoke can dissipate from the sensor.

The minimum necessary time gap between tests **MUST be 4-5 hours**. Original sensitivity will be restored only after approximately **5 hours**. Any modification of the test setup requires that the environmental sensor in the device needs time to settle back to normal values (its baseline).

Note
Weather conditions may influence the time required for the sensor to return to baseline settings.

Test preparations

When preparing tests, ensure you use a realistic test location and be aware of the natural behavior of wildfire smoke. Also, use several setups of the sensors based on your specific purpose for the tests.

Use realistic test locations

Use a forest location like the final deployment location.

We strongly recommend running the test in a location that is like its intended destination. Do not run the test in a location that is vastly different from their intended destination. Running a test in an urban parking lot, for example, will cause discrepancies. The sensors are primarily forest sensors and urban areas will affect the functionality.

Tip
Use the **Map** view of the Silvanet Deployment app to find the ideal location for the test fire.

Be aware of smoke behavior and test locations

Because wildfire smoke behaves differently in different locations, select a location that is realistic and reflects the final deployment environment.

A parking lot, work yard or an urban area may not be the best location for a setup although it may be convenient. The results of a test in those types of locations would not be very useful. For example, under a forest canopy, wind behavior is different from wind behavior in an open area such as a work yard.

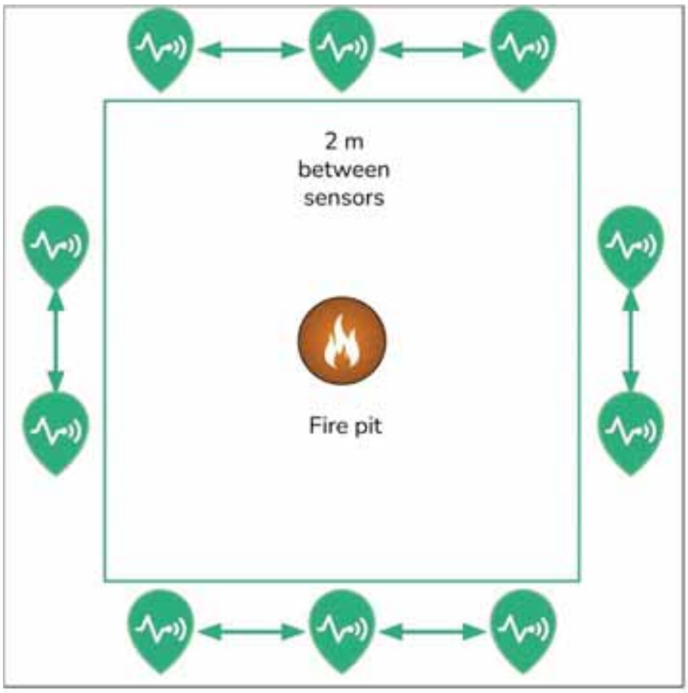
Consider sensor deployment arrangements

A shorter distance between deployed sensors results in quick detection times while increasing the distance between sensors leads to longer detection times. Therefore, use different sensor spacings depending on the objective of the fire tests (quick detection vs. longer distance between test fire and sensors).

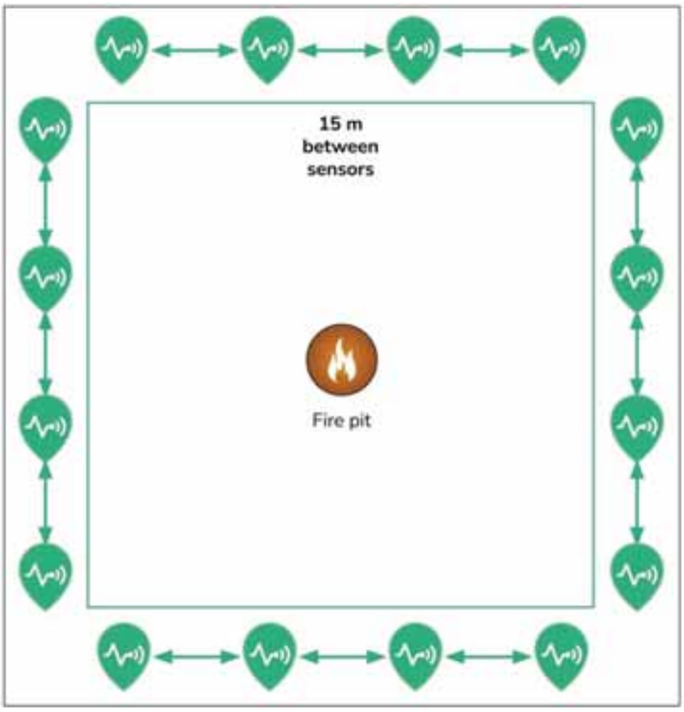
Note

Ensure the sensors are at least 3 meters above ground level.

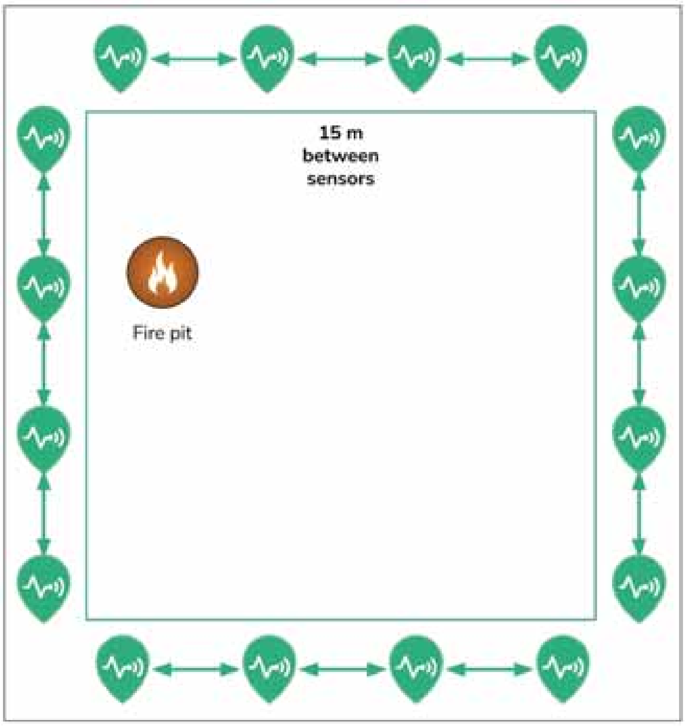
The following shows several deployment arrangements:



10 sensors with 2 m distance between each sensor with fire in the center



16 sensors with 15 m distance between sensors and fire in center



16 sensors with 15 m distance between sensors and fire located near or beside a sensor

See also
For more information about planning and deploying the hardware of the Silvanet System, refer to the **Planning Deployments** and **Deploying Silvanet Devices** documents.

Controlled test fire

Carefully follow these steps to burn a controlled test fire:

1. Note test fire material weight
2. Burn test fire continuously for 30 minutes
3. Ensure continuous exposure to smoke
4. Expect fire alerts
5. Record the results
6. Ensure fire is completely extinguished

Warning
Contact the local fire department / authorities and clarify whether you are allowed to make a fire. Take precautions and make sure you can extinguish the fire. Do not leave hot ash in the forest. Ensure the Fire department has been informed of the test fire. Also, as a precaution, have sufficient water available to be able to extinguish the fire after the test.

Step 1: Note test fire material weight

Record the weight and type of material you plan on burning. You need this information for any follow up tests so you consistently use the same weight and type of material for each test fire.

- Record the weight of the material you plan on burning for the duration of this test fire, including the material you plan on adding to keep the fire burning.
- Record the type of material you plan on burning.

Step 2: Burn test fire continuously for 30 minutes

After the sensors and Border Gateway have been deployed and the sensors have connectivity to the Silvanet network, you are ready to burn a test fire to generate smoke.

1. Use a metal fire pit with a diameter of approximately 1 m and place it in the middle of the deployed sensors.

Controlled fire setup

Note
A BBQ-type fire may not provide the appropriate level of smoke, nor duration.

2. Start the test fire by igniting small, dry branches and slowly grow the fire. See [Homogeneous material for test fire](#).

Warning
Do not use any artificial fire lighters as these have a different chemical composition and set free other burning gasses that can create false measurements from the sensors. Ensure the fire does not send out sparks and that it consists mostly of smoke due to the burning needles.

Burning test fire

3. Burn the fire for approximately 30 minutes by using small branches to keep the fire going. Add smaller branches with needles on top of the fire. Constantly feed the fire with fresh material to ensure the fire continuously burns for 30 minutes.

Note
Ensure the fire is generating smoke rather than having a burning camp-fire style fire.

Step 3: Ensure continuous exposure to smoke

Sensors need an exposure of 1-5 min of smoke exposure to trigger a Phase 1 process. Visually confirm smoke from the fire reaches the sensors.

Ensure sensors have at least 1 minute of continuous exposure to smoke to trigger the ML model in the sensor. This model investigates the smoke to determine if it is fire smoke or from some other source.

Step 4: Expect fire alerts

The expected time between the ignition of the fire and receiving a fire alert should be within minutes. You should expect a Fire alert in the Site Management app and receive a Fire alert email.

A **Fire alert** icon in the map for the Site displays the fire's location. View the details of a fire by selecting a Fire alert Icon.

Fire alert icons in a Site map

Step 5: Record the results

During and after the test, document the results of the test. The record of the test results should include the following information:

- Distance of sensors from the fire pit
- Measurement of the amount of burning material used (weigh the material added to the fire during the burn)
- Duration of the burn
- Visual confirmation of smoke hitting the sensors (**IDEALLY, AS A VIDEO**)

The test conditions must be documented exactly. For example, document the wind direction, wind speed, changing winds and other environmental conditions which allows for an accurate evaluation of the reaction of the sensors.

Note
Take videos and/or pictures of the fire during the test. They are useful during troubleshooting. The results are useful for creating and updating the ML model with data from real-world tests.

Step 6: Ensure fire is completely extinguished

Take the time required to **completely extinguish** the fire. Look for any embers under the burnt material. Do not let any embers escape the fire pit/bowl and ignite the surrounding ground material.

Warning
Ensure that the burnt material has been put out thoroughly and there are no hidden ambers. This is to avoid a fire unintentionally starting.

Test modifications

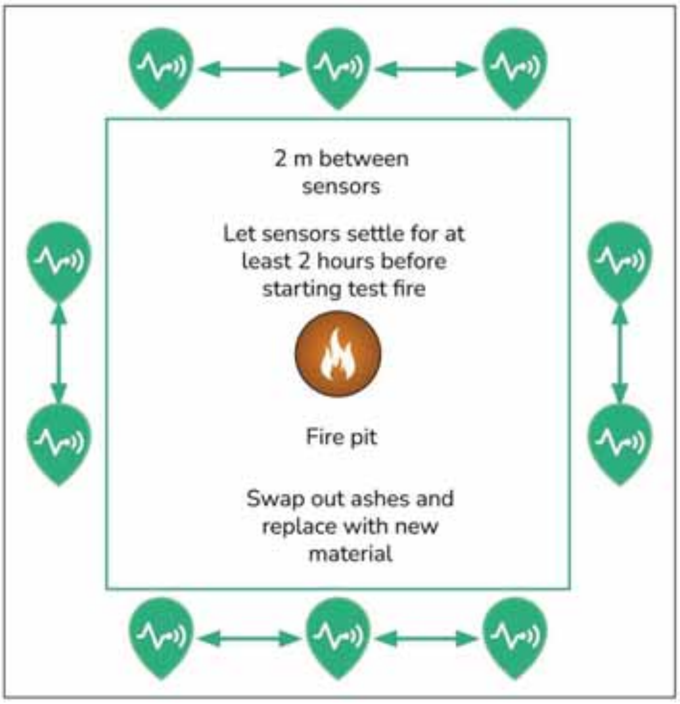
When you modify the testing environment, it is best practice to only change **one element** at a time while keeping the other elements the same.

Important
Any time sensors are moved, they need at least **5 days to stabilize (recalibrate)** in their new locations. So, it is not advised to move sensors prior to testing. However, if the sensor location remains the same but another aspect of the test is modified, 4 **to 5 hours** are needed for the sensors to settle (return to ready state).

Change burning material

If you burn forest material but need to test the Silvanet System with other materials such as creosote-soaked wood (railroad ties), then change **ONLY** the burning material without making any other modifications to the test. This way you only modify one element.

Important
Any changes you make require time to let the sensors settle, at least 4 to 5 hours.



Modified test setup with new burning material (2m spacing)

To change the burning material:

1. Clear out the ashes from the previous test and replace with new material.
2. Let the sensors settle for at least **4-5 hours**. This allows any smoke within the sensor chamber to clear and allow the gas sensor to reset. See Let sensors settle.
3. Burn a test fire as described in Burn test fire continuously for 30 minutes.
4. Record the results of the test, including wind conditions and other parameters. For details, see Record the results.

Change test location

If you change the test location within the 1 km range of the Border Gateway, you may not need to change the location of the Border Gateway. However, if the sensors are further away to make the Border Gateway out of range, you need to move the Border Gateway and update the GPS coordinates of the Border Gateway in the Site Management app.

Prepare the sensors and Border Gateway for the test as was done for the initial PoC setup, with some exceptions.

(1) The sensors need **5 days** to stabilize (recalibrate) after setup so the fire detection capabilities of the Silvanet System should not be tested during this period.

(2) The longitude and latitude of the new location needs to be changed for each sensor in the Silvanet solution.

When changing test location:

1. Redeploy the Border Gateway (if required).
2. Use the existing Deployment Packet. Another Deployment Packet does not need to be built. (Optionally, another Packet can be made with the new location coordinates, if required.)
3. Arrange the sensors as suggested in Ideal deployment arrangements.
4. Update the sensor location, as described in Updating sensor location coordinates.

5. Let the sensor stabilize (calibrate) to the new location for **10 days**.

6. Burn a test fire, as described in Burning test fire continuously for 30 minutes.

7. Record the results of the test, including wind conditions.

8. Modify the test by changing burning material.

Example test plan

The following shows an example test plan for a four-week duration.

Week	Test type	Day	Settling in period	Material (examples only)	Sensor spacing
1-2	None	1 - 14	14 days	n.a.	n.a.
3	Initial	1	2 hr.	Douglas Fir	5 m
3	Material	2	2 hr.	Creosote Railroad Tie	5 m
3	Material	3	2 hr.	Pressure-treated poles	5 m
3	Distance	4	2 hr.	Douglas Fir	10 m
3	Distance	4	2 hr.	Douglas Fir	15 m
3	Distance	5	2 hr.	Douglas Fir	80 m
3	Distance	5	2 hr.	Douglas Fir	100 m
4	Location	6 - 10	4 days	n.a	n.a
5	Initial	11	2 hr.	Douglas Fir	5 m
5	Material	12	2 hr.	Larch	5 m
5	Material	13	2 hr.	Maple	5 m
5	Distance	14	2 hr.	Douglas Fir	10 m
5	Distance	14	2hr.	Douglas Fir	15 m
5	Distance	15	2 hr.	Douglas Fir	80 m
5	Distance	15	2 hr.	Douglas Fir	100 m

Status icons

Status icons allow for easy identification of the status of Silvanet sensors, Mesh Gateways and Border Gateways. They are displayed in the Map view of a Site in the Site Management app.

Sensor status icons

Icon	Status
	Dark green (Active) Sensor is active and has sent data within the past 6 hours. Sensors send messages every two hours (default setting for transmissions) so an active sensor should have sent data within this timeframe.
	Yellow (Monitor) Sensor has not sent data to the Silvanet Cloud within the last 6 to 12 hours and should be monitored for activity.
	Gray (Inactive) Sensor is inactive and has not sent data for more than 12 hrs. Reasons could be sensor not connected to Border Gateway, battery drained, as well as other issues.
	Yellow Warning (Phase 1) Silvanet sensor gas sensor in progress determining if it has detected a fire.
	Fire Warning (Phase 2) Silvanet sensor’s gas sensor determined it has detected a fire and has sent an alarm.

Mesh Gateway status icons

Icon	Status
	Dark green (Active) Mesh Gateway is active and has sent data within the past 6 hours.
	Yellow (Monitor) Mesh Gateway has not sent data to the Silvanet Cloud within the last 6 to 12 hours and should be monitored.
	Gray (Inactive) Mesh Gateway inactive and has not sent data to the Silvanet Cloud for 12 hours. Take immediate action to resolve the issues preventing transmissions.

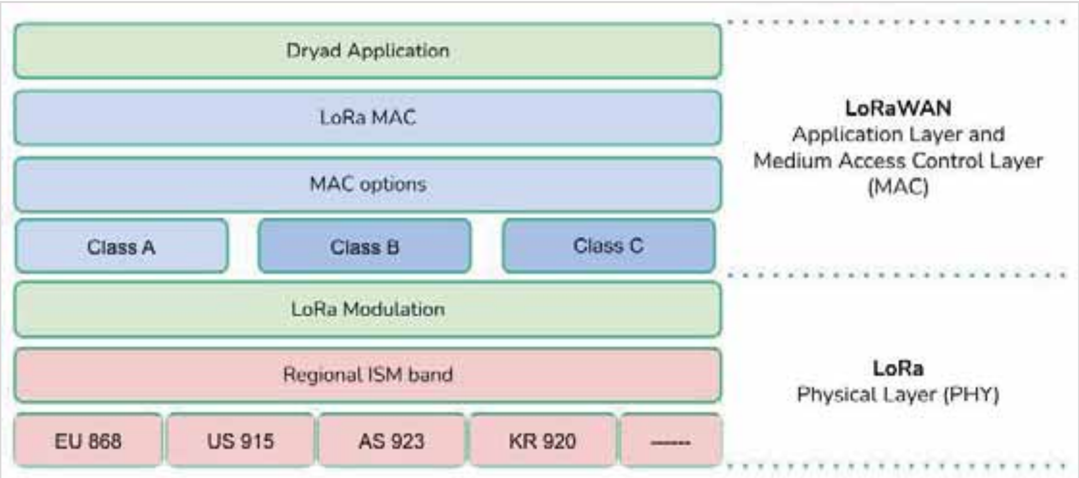
Border Gateway status icons

Icon	Status
	Dark Green (Active) Border Gateway is active and sending data.
	Yellow (Monitor) Border Gateway has not sent data to the Silvanet Cloud within the last 6 to 12 hours and should be monitored.
	Gray (Inactive) Border Gateway inactive and has not sent data to the Silvanet Cloud for 12 hours. Take Immediate action to resolve the issue preventing data transmissions.

LoRa and LoRaWAN in Silvanet

ISO Model

Dryad Silvanet devices use LoRa in the Physical layer while LoRaWAN provides Mesh Networking between Silvanet devices. LoRaWAN uses frequencies based on country-specific regulations.



LoRa radio stack

LoRa

LoRa is implemented in the Physical (PHY) Layer to provide a long-range communication link between LoRa-enabled devices (Silvanet sensors and Gateways). The key advantages of using LoRA in Silvanet are its low power usage and its long range. It is ideal for Dryad Silvanet devices as they send small amounts of data over long distances every two hours under normal conditions. This allows for the use of solar panels to power the devices.

LoRa translates data from the MAC layer into radio frequency (RF) signals transmitted using the Chirp Spread Spectrum (CSS) modulation method. LoRa networks can achieve a maximum throughput of 50 Kbps (100 bytes/min in normal conditions).

Additionally, it is approved as a standard for Low Power Wide Area Networking (LPWAN) by the ITU (International Telecommunication Union). As it operates in the license-free sub-gigahertz bands (such as 915 MHz, 868 MHz and 433 MHz), it is subject to interference and retransmissions.

LoRaWAN

LoRaWAN is a Medium Access Control (MAC) Layer protocol that manages communication between sensors and gateways in the Silvanet Network. It is a software built on top of LoRa hardware and defines, amongst other things, when data packets are transmitted and the format of those messages. Each node in a LoRaWAN network contains its own unique Device ID.

Silvanet sensors and LoRaWAN

Silvanet Sensors (the end-devices) use LoRaWAN to transmit messages to any Mesh Gateway or Border Gateway within range, which is typically 1 km, depending on topology. The LoRaWAN mesh network is transparent (invisible) to the sensors and the Silvanet Cloud. A group of Mesh Gateways and Border Gateways appear as a single LoRaWAN gateway to sensors.

Silvanet Mesh Gateways and LoRaWAN

The proprietary Silvanet Mesh Gateway uses LoRaWAN to enable large-scale deployment of Silvanet devices. It enables deployments in the challenging environment of forests where leaves, trees, hills and topology often inhibit radio waves. In these types of environments, the range of traditional LoRaWAN gateways is very limited which prevents them from sending and receiving messages deep into forests.

Silvanet Border Gateways and LoRaWAN

Silvanet Border Gateways use LoRaWAN to communicate with Mesh Gateways (or directly to sensors if they are within range). The Border Gateway forwards messages from sensors and Mesh Gateways to the Silvanet Cloud over the Internet using LTE-M mobile radio, fixed line (Ethernet) connectivity or SWARM satellite connectivity.

FUOTA

Firmware Update Over the Air (FUOTA) is a standard for distributing firmware updates using unicast or multicast. Its greatest benefit is delivering updates over the air to many devices at the same time in an efficient and secure manner.

LoRaWAN supports FUOTA and End-to-End 128 bit AES encryption.

The Silvanet Cloud sends ML Model and firmware updates to all sensors in a Site using FUOTA. Update times are dependent on strength of device communication as well as supercapacitor energy storage levels.

Border Gateways are responsible for transmitting messages to all devices in the Silvanet Mesh Network for firmware updates using FUOTA.

LoRaWAN frequencies

The following is a select list of countries.

Region	Country	Frequency band 1 (MHz)	Frequency band 2 (MHz)	Frequency band 3 (MHz)	Frequency band (4 MHz)	Frequency/ Antenna (MHz)
Europe	Germany	433.05 - 434.79	863 - 870			868
	Greece	433.05 - 434.79	863 - 870			868
	Spain	433.05 - 434.79	863 - 870			868
	Portugal	433.05 - 434.79	863 - 870			868
	Romania	433.05 - 434.79	863 - 870			868
	Italy	433.05 - 434.79	863 - 870			868
America	USA			902 - 928		915
	Canada			902 - 928		915
	Brazil			902 - 907.5	915 - 928	915
	Argentina			902 - 928	915 - 928	915
Australia	Australia	433 - 435			915 - 928	915
Asia	Indonesia				923 - 925	915
	Thailand	433.05 - 434.79			920 - 925	915

Region	Country	Frequency band 1 (MHz)	Frequency band 2 (MHz)	Frequency band 3 (MHz)	Frequency band (4 MHz)	Frequency/ Antenna (MHz)
	India		865 - 867			868
	Turkey	433.05 - 434.79	863 - 870			868
	Jordan	433.05 - 434.79	865 - 868			868
	South Korea				917 - 923.5	915
Africa	Sierra Leone					
	Egypt	433.05 - 434.79	863 - 870 /865 - 868			868
Middle East	UAE	433.05 - 434.79	863 - 870 /870 - 875.8		915 - 921	868
	Saudi Arabia	433.05 - 434.79	863 - 870			868
	Lebanon	433.05 - 434.79	863 - 870			868

Silvanet Glossary of Terms

A

Term	Description
ALOHA	Random access protocol. LoRaWAN networks use an ALOHA based protocol so end devices do not need to peer with specific gateways.

B

Term	Description
Border Gateway	Receives message from Mesh Gateways and Silvanet Wildfire sensors using LoRaWAN and forwards them using one of three services - 4G, Ethernet or SWARM satellite.

C

Term	Description
Chirp	LoRA is based on Chirp Spread Spectrum (CSS) where a CHIRP (Compressed High Intensity Radar Pulse) is a type of signal that is the carrier of data. Chirps have two types of signals: upchirp and downchirp. An upchirp increases in frequency while a downchirp decreases in frequency.

D

Term	Description
Datagram	A connectionless protocol that doesn't guarantee delivery. It is a "self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network."

Term	Description
DevAddr	Device Address.
DevEUI	Device Extended Unique Identifier.
Downlink messages	Messages sent from Gateways to devices lower down in the hierarchy; for example, messages sent from the Silvanet Cloud to Border Gateways, Border Gateways to Mesh Gateways or Mesh Gateways to sensors are downlink messages. SWARM satellites do not send downlink messages to Border Gateways.

E

Term	Description
End device	In Silvanet, it is a sensor that sends LoRa-modulated wireless messages to Gateways (Border or Mesh) and receives messages from Gateways.

F

Term	Description
FUOTA	*Firmware Update Over the Air*. LoRa allows sensor firmware to be updated over the Mesh Network.

G

Term	Description
Gateway, Mesh	See Mesh Gateway.

Gateway, Border	See Border Gateway.

H

I

Term	Description
IoT	Internet of Things. Silvanet devices are IoT devices.
ISM radio band	Industrial, Scientific, Medical. A license-free radio spectrum limited to certain bands of frequencies. These frequencies must tolerate interference generated by ISM applications.

J, K

L

Term	Description
LoRa	LoRA is a wireless modulation technique at the PHY layer based on Chirp Spread Spectrum (CSS) where a CHIRP (Compressed High Intensity Radar Pulse) is a signal that carries data.
LoRaWAN	LoRaWAN is built on top of LoRa in the MAC layer. It defines how devices use the LoRa hardware, such as when the devices can transmit and receive messages, as well as the format of the messages.
LTE-M	Radios in Silvanet Border Gateways use LTE-M which is a type of 4G cellular network. It is designed for IoT devices to connect to mobile networks. Dryad Border Gateways use Cat M1 version. It is designed to allow IoT devices to go into Power Saving Mode to reduce energy consumption. It also allows FUOTA without draining the supercapacitors in the Border Gateway.

M

Term	Description
Mesh Gateway	Dryad proprietary device. Receives messages from sensors and forwards the messages to the Border Gateway using a LoRaWAN mesh network. Messages sent from sensors hop through all Mesh Gateways within range.
Mesh network	A LAN topology in which nodes can connect directly in a non-hierarchical way to as many other nodes as possible to find the most efficient route to end nodes. Silvanet implements mesh networking.
ML Model	A ML (machine learning) model is a program that has been trained to recognize certain types of patterns.
MQTT	Client Server publish/subscribe messaging transport protocol used by third parties to communicate with a Silvanet Network.

N

Term	Description
Network Server	Software that manages the entire network. In the Silvanet System, the Network Server is the Silvanet Cloud. If it receives multiple copies of the same message, it keeps a single copy of the message and discards the others (preventing message deduplication).

O

Term	Description
OTAA	Over The Air Activation. FUOTA (Firmware Update Over the Air) uses OTAA to update sensor firmware.

P

Term	Description
Packets, (ISO model)	According to the ISO model, packets are data units within the Network Layer. It includes the source and destination IP addresses, as well as other information. Packets are essentially a connection-oriented protocol. It ensures each single packet is not dropped or compromised. It is considered reliable communication. An ACK packet is usually sent as a reply. If no ACK packet is received, the packet is simply resent.
Packets, Silvanet Deployment	Created in the Site Management app and assigned to users for deploying devices in a Site.
PoE	Power over Ethernet. The Border Gateway requires a PoE Injector (Adapter) that provides a voltage range of between 36V and 57V. The PoE must be IEEE 802.3af compliant

Q, R

S

Term	Description
Supercapacitor	A supercapacitor is a high-capacity capacitor that can accept and deliver charges faster than batteries and tolerates many more charge and discharge cycles than rechargeable batteries.

T

U

Term	Description
Uplink Messages	Transmissions sent by end-devices to the Network Server relayed by one or many gateways. SWARM satellites only receive Phase 2 Alerts messages from Border Gateways.

V

Term	Description
VOC	A VOC (Volatile Organic Compound) is an organic chemical compound that evaporates easily at room temperature. The gas sensor in the Silvanet Sensor detects VOCs.

W, X, Y, Z

Silvanet FAQs (Frequently Asked Questions)

Silvanet Suite FAQs

What is a Deployment Packet?

A *Packet* defines the Silvanet sensors and gateways that are to be deployed in a Site. Silvanet Deployment Packets are created in the Site Management app and assigned to users for deploying devices in a Site. Each Packet includes a list of Silvanet devices to be deployed and the location (GPS coordinates) where each device is to be deployed. When a device is deployed to a location, a user scans in the device's QR Code which then syncs the device's actual location to the corresponding entry in the Silvanet Cloud.

Note
Several Packets can be created within each Site. Each Packet can consist of the devices expected to be deployed per day / per forest worker.

What is a Silvanet Site?

A Site is a geographical area (defined in Km2 or square miles) where a network of sensors and gateways are deployed to monitor the forest environment. Sites are set up by Dryad administrators (currently, Dryad only) and assigned to registered users. Within a Site, the number and location of sensors and gateways are defined. The Site Management app (dryad.app) displays all Sites that Dryad has created and administered for you. Using your username and password, you are granted access to all Sites to which you are registered. After deployment, a Site can be monitored within the Site Management app.

Note
Sites are currently added by Dryad internal Admins. In the future, a Site Admin will be allocated to specific users who will be able to create sites for clients and to create users.

Why are supercapacitors used in Silvanet Devices?

A *supercapacitor* is a high-capacity capacitor that can accept and deliver charges faster than batteries and tolerates many more charge and discharge cycles than rechargeable batteries. It provides a large amount of power for a relatively short time. It is best suited for applications where a very high number of charge/discharge cycles or longer lifetime is required. They also have low risk of spark hazard. This makes them ideal for energy storage for Silvanet devices which are installed in forests. They are used because the sensors and gateways should not themselves be a source of fire ignition.

Silvanet Sensor FAQs

How long does a sensor need to calibrate to a new deployment location?

Once deployed, the Silvanet sensor needs to perform a calibration to determine a value for normal air in the environment around the sensor. This is critical for allowing the sensor to detect a smoldering fire. The calibration period is approximately 14 days after deployment and during this period the sensor does not detect smoldering fires.

Why do I get false Fire Alerts during calibration period?

During the calibration period and up to one month after deploying, the sensor may trigger false Fire Alerts. This is normal behavior and expected.

What happens if a deployed sensor is handled while on a tree?

If a Silvanet sensor is touched or moved while deployed on a tree, it causes interference with the calibration. The gas sensor in the Silvanet sensor is very sensitive to outdoor changes. Consequently, moving, touching or interacting with the sensors beyond what is necessary influences the sensor readings and also the sensor calibration settings.

For the sensor to return to normal values, the sensor needs at least 1 hour to stabilize and return to its base readings. Consequently, the sensor does not measure any changes in the environment if a test is run during this stabilization period.

We strongly advise leaving the sensors alone once they are deployed.

What is meant by interacting with a deployed sensor?

Interacting with sensors includes:

- Touching the sensors in any way

- Moving the sensors in any way
- Being in proximity to the sensors
- Having running vehicles nearby the sensor
- Bringing any source near the sensor that could trigger the Phase 1 alert such as cigarettes, running machinery (especially with diesel motors) and even breathing on the sensor.

How high should a sensor be attached to a tree?

If possible, install the Silvanet sensor at least 3 meters above the forest floor, depending on available sunlight in the location. At this height, the device has less interference from human or animal interactions.

Silvanet Mesh Gateway FAQs

What is a Mesh Gateway?

Mesh Gateways receive messages from sensors and forward them using the LoRaWAN mesh network to other Mesh Gateways within range and finally to one or more Border Gateways. Messages sent from sensors hop through all Mesh Gateways within range.

How high should a Mesh Gateway be attached to a tree?

If possible, install the Silvanet Mesh Gateway at least 3 meters above the forest floor, depending on available sunlight in the location. At this height, the device has less interference from human or animal interactions.

Silvanet Border Gateway FAQs

What is a Border Gateway?

Border Gateways receive messages from Mesh Gateways and Silvanet Wildfire sensors (if they are in range) using the LoRaWAN mesh network and forwards them using one of three services - 4G, Ethernet or SWARM satellite to the Silvanet Cloud.

How is the Border Gateway connected to the Solar Panel

The solar panel is pre-connected to the Border Gateway. If it needs to be disconnected for any reason, the wiring is as follows:

- Negative: Brown wire
- Positive: White wire

How long does it take for the solar panel to charge the Border Gateway supercapacitors?

When the Border Gateway is connected to the solar panel, the Border Gateway requires 3 to 4 hours before it comes online after the solar panel begins charging the supercapacitors in the Border Gateway. If the Border Gateway is moved from using PoE to using the solar panel, the Border Gateway needs 1 to 2 days to begin operating properly.

How do I determine if the solar panel is damaged

First, disconnect the solar panel from Border Gateway (one wire is enough) and measure the voltage. It should be around 20V. If not, then there is not enough light or the solar cell is damaged.

Then Use an 18-24V power supply instead of the solar cell and wait.

Important: The input is protected against reverse voltage from the solar cell but not from a power supply. If you give reverse voltage to the input with a lab power supply, the border gateway will be damaged. Cable color: brown- white+

What type of PoE can be used with the Border Gateway?

The Border Gateway requires a PoE Injector (Adapter) that provides a voltage range of between 36V and 57V. The PoE must be IEEE 802.3af compliant.

Do solar panels need regular maintenance, such as cleaning?

The sensors and gateways are placed vertically (by intention) on the tree, which will minimize the dust buildup and allow rain to wash off any dust easily. This vertical position is intentionally to eliminate manual servicing (cleaning). Finally, the solar panels have been intentionally oversized to allow for performance degradation over time while still maintaining functionality. The software in the sensors and gateways is highly optimized to reduce energy consumption and dynamically adapts to lower energy budgets by prolonging sleep cycles in low light / low energy conditions while minimizing performance impact. We have successfully tested sensors and gateways under real-world (forest) conditions for more than 2 years and performed a series of tests in a climate chamber to simulate impacts of temperature and humidity fluctuations.

We do not anticipate that sensors or gateway panels have to be manually serviced / cleaned, however unusual circumstances (e.g. bird droppings) may present additional challenges for the gateways as they have a higher energy requirement than sensors. However, again, due to the vertical positioning, these effects should be minimized.

Fire detection FAQs

How is a ML model used in Silvanet?

A *Machine Learning (ML) model* is a program that has been trained to recognize certain types of patterns. You can train a model over a set of data, providing it an algorithm that it can use to make predictions and learn from those data. ML models find patterns and make decisions in previously unseen data and make predictions about that data. A ML Model recognizes patterns by having it "trained" with large datasets. Training involves optimizing the machine learning algorithm to find certain patterns or outputs from the dataset. The output - a ML Model - is a computer program with specific rules and data structures.

What are Volatile Organic Compounds (VOC)?

A *VOC (Volatile Organic Compound)* is an organic chemical compound that evaporates easily at room temperature. They vaporize into air and dissolve in water. Organic compounds are chemicals that contain carbon and are found in all living things, especially trees. VOCs are also emitted from oil and gas fields and diesel exhaust. From the US EPA: "Any compound of carbon, excluding carbon monoxide, carbon dioxide," and related chemicals.

How is fire intensity measured?

The most important measure of fire behavior is fire intensity. Fire intensity (I) represents the heat released per meter of fire front (kW/m of fire front). It is a function of (1) heat yield of fuel (kilojoules/kg), (2) amount of fuel per unit area (kg/m2) and (3) the rate of forward spread of fire front (km/h).

LoRa network FAQs

What is LoRa?

LoRA is a wireless modulation technique based on Chirp Spread Spectrum (CSS) where a CHIRP (Compressed High Intensity Radar Pulse) is a signal that carries data. Chirps have two types of signals - an up-chirp and a down-chirp. An up-chirp increases in frequency while a down-chirp decreases in frequency. LoRa is ideal for IOT applications like the Silvanet sensor as they transmit small data packets with low bit rates.

LoRA has an advantage over other techniques such as ZigBee as data can be transmitted at longer ranges. This allows Gateways to be located at greater distances from sensors, thus reducing the number of gateways required per deployment.

What is LoRaWAN?

LoRaWAN is built on top of LoRa in the MAC layer. It defines how devices use the LoRa hardware, such as when the devices can transmit and receive messages, as well as the format of the messages. LoRaWAN is optimized to operate in low power mode and can transmit as far as 10 km in open fields, less in forests and up to 3 km in urban areas with significant interference. LoRaWAN also allows for firmware updates and updates to the ML Model on sensors over the air (FUOTA).

What is a Data Packet?

Data packets are defined by the ISO model and not to be confused with Silvanet Packets. They are data units within the Network Layer. They include the source and destination IP addresses as well as other information.

Data packets are, essentially, a connection-oriented protocol. They ensure each single packet is not dropped or compromised and are considered a reliable form of communication. An acknowledgement (ACK) packet is usually sent as a reply to a received data packet. If no ACK packet is received, the data packet is simply resent.

LoRa uses data packets to communicate between LoRa enabled devices (sensors and gateways) and are part of the definition of a LoRaWAN network.

What is FUOTA?

Firmware update Over the Air (FUOTA) is a standard for distributing firmware updates using unicast or multicast. It allows firmware updates to be delivered to many devices (Silvanet Sensors) at the same time efficiently and securely.

The Silvanet Cloud (Network Server) enables class C in LoRaWAN and prepares to send updates as a multicast distribution. The firmware is chunked into transmittable parts. The Silvanet Cloud schedules each update chunk as a download message to the multicast group. The Network Server then verifies that each device has received all chunks, synthesizes them and verifies the update signature.

The end device (Silvanet Sensor) applies the firmware update and delivers a firmware update complete uplink message to the Network Server.

What is MQTT?

MQTT is a Client/Server publish/subscribe messaging transport protocol that is lightweight, open, simple, and designed to be easy to implement. Typically used for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium. It is used by third parties to communicate with a Silvanet Network.