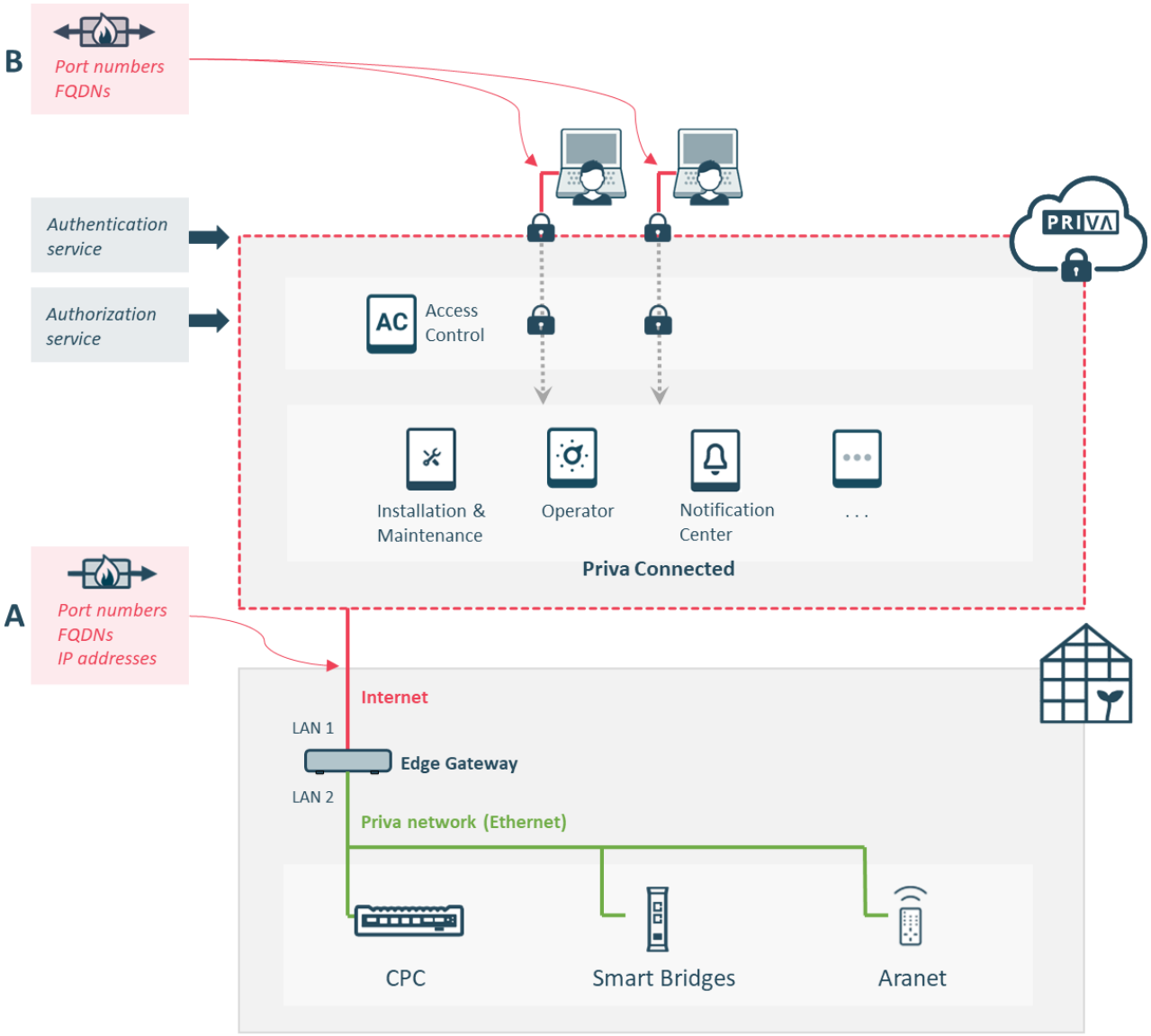
> ICT INFORMATION

How does Priva protect your greenhouse's data? And what should you do to enable communication between the Priva hardware and software in a secure way?

Network overview

The image shows the recommended network configuration in which the Priva network is separated from the Internet. Please note that there are security risks involved if the Priva network is not separated from the Internet.



A See: A) Communication between gateway and Priva Cloud (page 3)

B See: B) Communication between browsers and Priva Cloud (page 5)

Function of Edge Gateway / Priva Gateway

Process management systems should never run on a network with Internet access, as this entails security risks. Priva therefore strongly recommends keeping the Priva network and the Internet separate. In order to use cloud services, communication between the management system and the Priva Cloud is, of course, necessary. The Edge Gateway is a gateway that makes this possible in a secure manner. The Edge Gateway is the successor to the Priva Gateway.

The gateway only permits outgoing connections. In this way, the Priva network protects the system from access by unauthorised persons via the Internet. The gateway does not permit incoming connections. If the gateway sets up the connection to the outside, incoming traffic within that active session will be permitted. This makes it possible to adjust values from outside with an application/service.

The data transferred between the gateway and the cloud is secured by means of encryption. By contrast with other means for access to the Priva network, such as a VPN, this architecture makes use of a system based on reports, so there is no complete datalink between the Priva network and the world outside. Data is exchanged only to a highly restricted degree.

Updates of Linux on the Edge Gateway are implemented in Installation & Maintenance (FirmwareUpdater module).

Support from Priva

When using the Priva Gateway, Priva can conveniently provide remote support via TeamViewer. Port 5938 has to be open for this.

When using the Edge Gateway, Priva can provide remote support via Remote Monitor. Remote Monitor is available from firmware version 2.13.1. No additional ports have to be opened for Remote Monitor, because the communication process uses HTTPS and WebSocket Secure (WSS) (port 443). Please note that FQDN edge-status.priva.com is required.

What is Remote Monitor?

Remote Monitor is a Priva service that consists of two elements:

- a service which runs on Edge Gateway,
- a server in Microsoft Azure.

Remote Monitor has two functions:

- Priva can monitor which gateways are online. The gateway periodically sends a message to the server via an API. This API returns a list of all online gateways as well as all offline gateways that were previously online.
- Priva can provide support for your gateway via an encrypted SSH connection.

Communication with the gateway is completely secure and protected:

- Communication between the gateway and the cloud is initiated by the gateway.
- All communication is protected by TLS.
- Gateways require a client certificate issued by Priva to authenticate with the cloud server. This ensures that only genuine Priva Edge Gateways can connect to the server.
- All communication is protected with specific passwords and tokens per gateway that are only accessible to specific Priva employees.
- Passwords and tokens are generated by Azure KeyVault.

Remote Monitor operates as a separate service independent of IoT Edge and will therefore continue to run in case of issues with IoT Edge.

Security measures by Microsoft

All Digital Services have been designed based on the Microsoft Azure cloud platform. Priva's services use the standard Microsoft Azure components IoT hub and Service Bus for the communication between the Priva network and the cloud. You can find detailed information on Microsoft's security in the Microsoft Trust Center.

A) Communication between gateway and Priva Cloud

To enable communication between the gateway and the Priva Cloud, specific ports must be open in the firewall. In addition, communication with the Priva Cloud must be permitted, based on the FQDNs or based on the IP addresses.

See **A** in the picture in Network overview (page 1).

Port numbers (gateway - Priva Cloud)

The table below lists the port numbers that are required for communication between the Edge Gateway or Priva Gateway and the Priva Cloud. All ports only use outgoing communication.

Port	Details	Transport protocol	
123	NTP	UDP	[1]
443	HTTPS	TCP	[1]
5671	AMQP	TCP	[1]
5672	AMQP	TCP	[1]
8883	MQTT	TCP	[1]

= outgoing [1] LAN port connected to internet

FQDNs (gateway - Priva Cloud)

The tables below show the Fully Qualified Domain Names (FQDNs) required for communication between the gateway and the Priva Cloud. You can choose between using wildcards (addresses starting with *) or releasing the complete FQDNs. The list of complete FQDNs is, however, dynamic; FQDNs may be added or changed in the future. Using wildcards is more maintenance-friendly, because the list of wildcards will change less often than the list of complete FQDNs.

We recommend whitelisting at least the wildcard *.priva.com for the sake of future developments.

FQDNs: from Edge Gateway to cloud

FQDN	Service
***.blob.core.windows.net** (HTTPS)	
coprdfrontend2sawe.blob.core.windows.net	Gateway services[1]
edgegatewayfirmware.blob.core.windows.net	Gateway services[1]
prddevicemetadatasa.blob.core.windows.net	Gateway services[1]
prdfileuploadersa.blob.core.windows.net	Gateway services[1]
prdhdptsgwtelemetrysa.blob.core.windows.net	Cloud History
prdprivaauditlogs.blob.core.windows.net	Gateway services[1]
***.priva.com** (HTTPS)	
cr.priva.com	Gateway services[1]
cr-data-westeurope.priva.com	Gateway services[1]
data-gateway-fileuploader.priva.com	Gateway services[1]
edge-remote.priva.com	Gateway services[1]
edge-status.priva.com (HTTPS, WSS)	Gateway service Remote Monitor
local-auth-provisioning.priva.com	Gateway services[1]
***.pool.ntp.org** (NTP)	
Country dependent, i.e.: 0.uk.pool.ntp.org	NTP server
***.oms.opinsights.azure.com** (HTTPS)	Gateway services[1]
Miscellaneous	
aka.ms [2] (HTTPS)	Gateway services[1]
global.azure-devices-provisioning.net (HTTPS)	Gateway services[1]
mcr.microsoft.com (HTTPS)	Gateway services[1]
prd-priva-generic-ih.azure-devices.net (HTTPS, MQTT, AMQP)	Gateway services[1]
priva.azurecr.io (HTTPS)	Gateway services[1]
priva.westeurope.data.azurecr.io (HTTPS)	Gateway services[1]

FQDN	Service
westeurope.data.mcr.microsoft.com (HTTPS)	Gateway services[1]

[1] Services of the gateway (configuration of the gateway, gateway updates, authorisation, metadata and so on)
[2] When running the connectivity check (in the local configuration application), aka.ms will redirect to other end points: raw.githubusercontent.com/* (subject to change).

FQDNs: from Priva Gateway to cloud

FQDN	Service
***.priva.com** (HTTPS)	
accesscontrolapi.priva.com	Gateway services[1]
assetapi.priva.com	Gateway services[1]
auth.priva.com	Gateway services[1]
authorization.priva.com *(out of date)*	Gateway services[1]
connect.priva.com *(out of date)*	Gateway services[1]
gps.priva.com	Gateway services[1]
state.priva.com	Gateway services[1]
tenantapi.priva.com	Gateway services[1]
Miscellaneous	
prdinstallupdatesa.blob.core.windows.net (HTTPS)	Gateway services[1]

[1] Services of the gateway (configuration of the gateway, gateway updates, authorisation, metadata and so on)

IP addresses (gateway - Priva Cloud)

Priva uses the "EuropeWest" and "EuropeNorth" IP address ranges from Microsoft that are required for Priva Digital Services. These series are used dynamically by Microsoft and therefore can not be mentioned specifically. The series that Microsoft uses, can be found on their website: go to https://www.microsoft.com/en-us/download/details.aspx?id=56519 and download the json file.

This file is updated weekly. New ranges added in the file will not be used in Azure for at least one week. If you are using the IP address restriction list, download the new json file every week and perform the necessary changes at your site to correctly identify services running in Azure.

Do not use IP address range 172.23.105.0/24. This range is already used internally in the Edge Gateway.

Internet connection

All Priva Digital Services require a broadband Internet connection with a minimum upload and download speed of 10 Mbps.

B) Communication between browsers and Priva Cloud

To enable communication between user browsers Priva Digital Services and the Priva Cloud, port 443 must be open in the firewall and communication with the Priva Cloud must be permitted based on FQDNs.

See **B** in the picture in Network overview (page 1).

Port numbers (browser - Priva Cloud)

The table below shows the port number required for communication between Priva Digital Services users' browsers and the Priva Cloud.

Port	Details	Transport protocol	
443	HTTPS, WSS[1]	TCP	

[1] WSS stands for WebSocket Secure. Unlike HTTP, the WebSocket protocol enables full-duplex communication between browsers and Priva Cloud (which is used to get real-time values without HTTP polling).

 = incoming and outgoing

FQDNs (browser - Priva Cloud)

The table below shows the Fully Qualified Domain Names (FQDNs) required for communication between Priva Digital Services users' browsers and the Priva Cloud. The table shows only the wildcard (address starting with *).

FQDNs: from browser to cloud

FQDN wildcard	Service
***.priva.com** (HTTPS, WSS[1])	Priva Digital Services
***.azurewebsites.net** (HTTPS, WSS[1])	API Access

[1] WSS stands for WebSocket Secure. Unlike HTTP, the WebSocket protocol enables full-duplex communication between browsers and Priva Cloud (which is used to get real-time values without HTTP polling).

Internet connection

All Priva Digital Services require a broadband Internet connection with a minimum upload and download speed of 10 Mbps.

Priva (head office)
Zijlweg 3
2678 LC De Lier
The Netherlands

See www.priva.com for contact information of a Priva office or partner for your region.