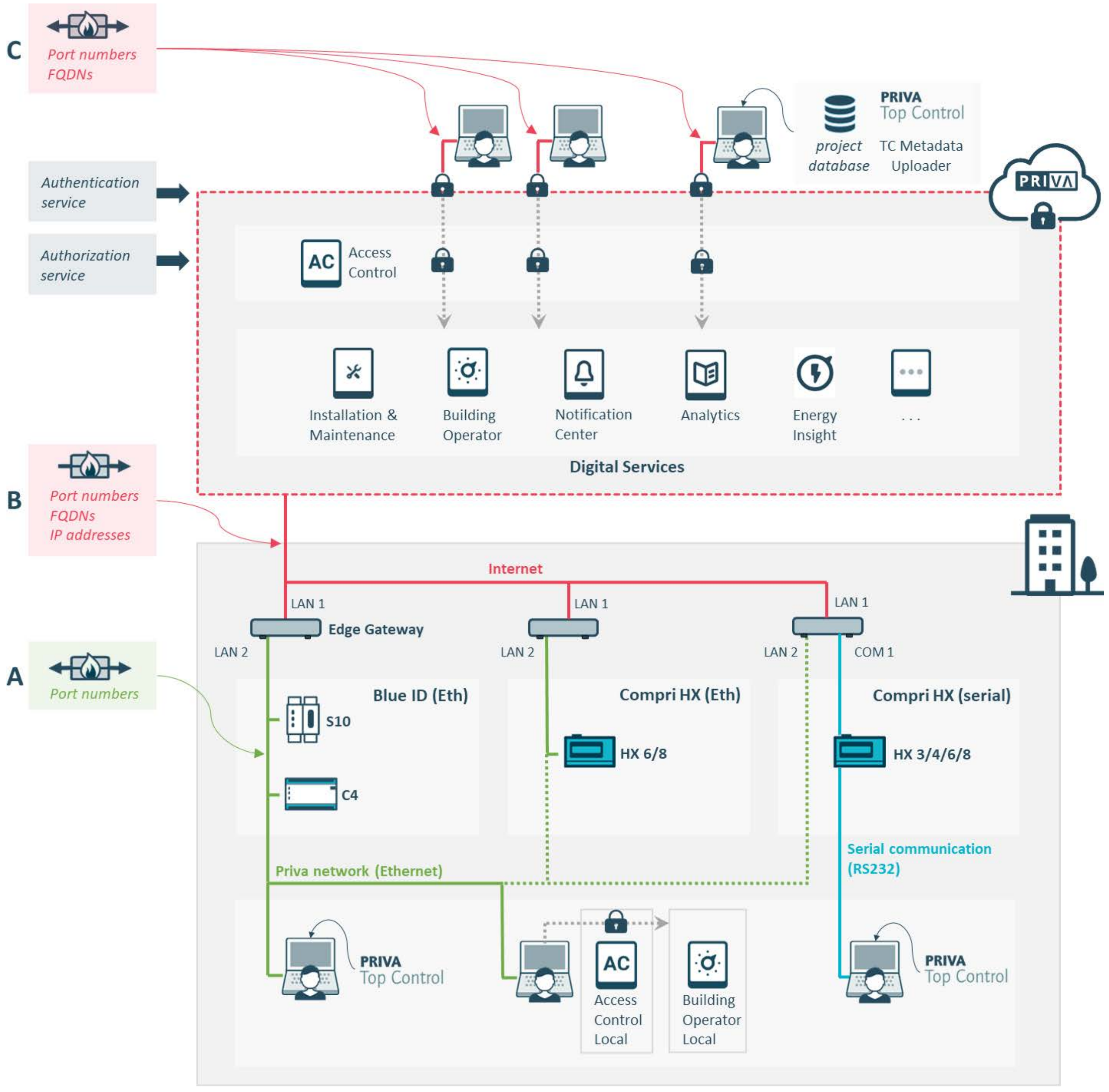
> ICT INFORMATION

Priva Blue ID, Top Control, Digital Services

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

Network overview

The illustration shows the recommended network configuration where the Priva network is separated from the Internet. Keep in mind that it poses security risks if the Priva network is not separated from the Internet.



A See: A) Communications within the local network (page 3)

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

C See: C) Communication between browsers and Priva Cloud (page 8)

Function Edge Gateway / Cloud Connector

Building management systems should never run on a network with Internet access. To use cloud services, communication between the management system and the Priva Cloud is, of course, necessary. The Edge Gateway and the Cloud Connector are gateways that securely make this possible. The Edge Gateway is the successor to the Cloud Connector.

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

The data transferred between the gateway and the cloud is secured utilizing encryption. In contrast to some other methods of accessing building automation systems such as VPN, this architecture uses a message-based system, so there is no full data link between the building and the outside world. Only very limited relevant data is exchanged.

Updates from Windows 10 IoT to the Cloud Connector downloaded and installed automatically in accordance with the default Windows Update mechanism. There is no forced restart of the Cloud Connector during normal business hours (8.00 am - 5.00 pm).

Updates of Linux on the Edge Gateway will be implemented in Installation & Maintenance (Module Firmware Updater).

Support from Priva

Priva is easily able to provide support remotely on the Cloud Connector. Port 5938 must be open for this.

With Edge Gateway support via TeamViewer is not applicable, because this gateway cannot be approached directly from outside.

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) Communications within the local network

To enable communication within the local network, specific ports must be open in the firewall (if there is a firewall).

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

Port numbers (communication within local network)

The table below lists the port numbers that are required for communication with the Priva Blue ID/Compri HX hardware and Top Control applications and the Cloud Connector or Edge Gateway. The table also specifies whether the ports use incoming or outgoing communication. The configuration of the ports in the firewall depends on the Top Control applications used and the network configuration created in the project.

Port	Details	Transport protocol	Priva Blue ID, Compri HX	TC Engineer	TC Operator	TC Manager	TC ServeCenter	TC History proxy	TC History	TC LAN Manager	Edge Gateway	Cloud Connector
25 465 587[16]	SMTP(S) 16	TCP	→				→					
53	DNS	TCP/UDP	→	→	→	→	→	→	→	→	→ 9,10,11	→ 10
67	DHCP	TCP									→	
80	HTTP	TCP	←	→ 1	→ 1	→	→ 1	→ 1	→ 1	→ 1	← 10,11	
123	NTP	UDP	↔								→ 9.10	→ 10
161	SNMP[8]	TCP/UDP	→									
502[2]	Modbus	TCP	↔									
514	Rsyslog	UDP									→ 10	
1883	MQTT	TCP									→ 10	
1900	SSDP	UDP									→ 10	
5000	LOAS[12]	TCP									→ 10	
5001	LOUM[13]	TCP									→ 10	
5002	LOU[14]	TCP									→ 10	
5003	LOAS[15]	TCP									→ 10	
5353	mDNS	TCP/UDP	↔	↔	↔	↔					→ 10	→ 10
7650	DDS	UDP									→ 10	
7651	DDS	UDP									→ 10	
7660	DDS	UDP									→ 10	
7661	DDS	UDP									→ 10	
8080[2]	HTTP	TCP				→		←				

Port	Details	Transport protocol	Priva Blue ID, Compri HX	TC Engineer	TC Operator	TC Manager	TC ServeCenter	TC History proxy	TC History	TC LAN Manager	Edge Gateway	Cloud Connector
9093	XML	TCP	←									
9354	SBMP	TCP (TLS 1.2)										↔
9508	PTP	UDP									→ 10	
15000	Priva [5,7]	UDP	↔								↔ 10	↔ 10
15001	Priva [5]	UDP	↔	→ 3	→ 3		→ 3		→ 3	→	↔ 10	↔ 10
23456 24690 25924 27158[17]	Priva [4]	TCP		→	→		→	→	↔	↔		
23457 24691 25925 27159[17]	Priva [4]	UDP		→	→		→	→	↔	↔		
47808 through 47817[16]	BACnet [6]	UDP	↔									

← = incoming
→ = outgoing
↔ = incoming and outgoing

[1] Only online help

[2] Default port number, can be changed

[3] For local communication

[4] TC LAN Manager looks for a free port number to use

[5] Priva own protocol

[6] Reserverd ports, adjustable in TC Engineer

[7] When using a Compri HX connection

[8] Only SNMP Step is supported in Top Control 8

[9] LAN port connected to internet
(Edge Gateway: LAN 1, Cloud Connector: LAN 3)

[10] LAN port connected to Priva network
(Edge Gateway: LAN 2, Cloud Connector: LAN 1)

[11] Service port
(Edge Gateway: LAN 3, Cloud Connector: LAN 2)

[12] Local Operator Authorization Service

[13] Local Operator User Management UI

[14] Local Operator UI

[15] Local Operator API

[16] Select one of the stated port numbers

[17] Select one of the stated port numbers. The selected port numbers from the two rows with note 17 must succeed each other (e.g. 23456 and 23457).

B) 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 **B** 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 gateway and the Priva Cloud. All ports only use outgoing communication. Port 5938 is required for support from Priva with TeamViewer (only on the Cloud Connector).

Port	Details	Transport protocol	Edge Gateway	Cloud Connector
123	NTP	UDP	→ [1]	
443	HTTPS	TCP	→ [1]	→ [1]
5671	AMQP	TCP	→ [1]	→ [1]
5672	AMQP	TCP	→ [1]	→ [1]
5938	Team-Viewer	TCP		→ [1]
8883	MQTT	TCP	→ [1]	→ [1]
9354	SBMP	TCP (TLS 1.2)		→ [1]

→ = outgoing

[1] LAN port connected to internet
(Edge Gateway: LAN 1, Cloud Connector: LAN 3)

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
***.servicebus.windows.net** (HTTPS)	
priva-lwe-prod-gateway-master-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition2-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition3-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition4-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition5-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition6-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition7-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition8-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition9-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition10-weu.servicebus.windows.net	Remote Management, Cloud History
***.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]
prdhdptsgwtelemetrysa.blob.core.windows.net	Cloud History
prdprivaauditlogs.blob.core.windows.net	Gateway services[1]
***.priva.com** (HTTPS)	

FQDN	Service
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]
local-auth-provisioning.priva.com	Gateway services[1]
***.pool.ntp.org** (NTP)	
Country dependent, e.g.: 0.uk.pool.ntp.org	NTP server
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]

[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 endpoints: raw.githubusercontent.com/* (subject to change).

FQDNs: from Cloud Connector to cloud

FQDN	Service
***.servicebus.windows.net** (HTTPS, SBMP)	
priva-lwe-prod-gateway-master-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition2-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition3-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition4-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition5-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition6-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition7-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition8-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition9-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition10-weu.servicebus.windows.net	Remote Management, Cloud History
***.priva.com** (HTTPS)	
accesscontrolapi.priva.com	Gateway services[1]
assetapi.priva.com	Gateway services[1]
auth.priva.com	Gateway services[1]
authorization.priva.com *(obsolete)*	Gateway services[1]
connect.priva.com *(obsolete)*	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 1 Mbps.

C) Communication between browsers and Priva Cloud

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

See **C** in the figure 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 wildcards (addresses starting with *).

FQDNs: from browser to cloud

FQDN wildcard	Service
***.priva.com** (HTTPS, WSS[1])	Priva Digital Services
***.erbis.one** (HTTPS, WSS[1])	Energy Insight by ErbisOne

[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 1 Mbps.

Priva Blue ID communication specifications

Ethernet	
Network standard used	IEEE 802.3 (37 ... 57 VDC) 10BASE-T (10 Mbps) 100BASE-TX (100 Mbps) auto negotiation auto-MDIX IPv4
DHCP	not supported
Baud rate	10 Mbps and 100 Mbps
Connection of third-party equipment permitted	yes
Cable type required	UTP or STP, minimum category 5E
Maximum cable length	100 m
Connector type	RJ45

Power over Ethernet is only applicable to Priva Blue ID S-Line.

Power over Ethernet	
Network standard used	IEEE 802.3af (37 ... 57 VDC) Powered Device (PD) Class 0

Cables (Priva Blue ID S-Line)

Module	Specifications of cable to be used
Priva Blue ID S-Line SN1 Network module, Priva Blue ID S-Line SN2 Network module and Priva Blue ID S-Line SN3 Network module	• type: UTP or STP, minimum category 5E • maximum length: 100 m • connector type: RJ45
Priva Blue ID S-Line SN3t Network module *The SN3t module is no longer supplied. You can use the ORing Network module for 2-wire.*	In addition to the above-mentioned cable, the following cable can be used: • type: twisted pair (telephone or data cable) • cross section: 0.2 ... 2.5 mm² without ferrule connector 0.25 ... 2.5 mm² with ferrule connector • maximum length between two controllers: 500 m nominal[1] • maximum total length: 1000 m nominal[1] • connector type: two-pin screw connector (polarity-insensitive connection)
ORing Network module	• 2-wire (telephone or data cable) CAT5/6 is also permitted • maximum cable length between two ORing modules: 500 m • connector type: 2-pin terminal block (polarity insensitive connection)
Priva Blue ID TouchPoint	• type: UTP or STP, minimum category 5E • maximum length: 100 m • connector type: RJ45

[1] The maximum cable length is based on test results with twisted pair cable category 5E and Alpha Wire 5261C; for other types of cable, the maximum length may be less.

Cables (Priva Blue ID C-Line)

Module	Specifications of cable to be used
Priva Blue ID C4 C-MX34(m) - Ethernet	• type: UTP or STP, minimum category 5E • maximum length: 100 m • connector type: RJ45
ORing Network module	• 2-wire (telephone or data cable) CAT5/6 is also permitted • maximum cable length between two ORing modules: 500 m • connector type: 2-pin terminal block (polarity insensitive connection)
Priva Blue ID TouchPoint	• type: UTP or STP, minimum category 5E • maximum length: 100 m • connector type: RJ45

Compri HX communication specifications

Ethernet connection (only Compri HX 6E/8E)	
Supported network classes	A, B and C
Baud rate	10 Mbit/sec
Network type	10BASE-T as per the IEEE 802.3 standard
NE2000 Compatible	Yes
Connector type	RJ45
Cable type	UTP or STP, minimum category 5E
Maximum cable length	100 m
Connection with switched on Compri HX	Permitted

Cables (Compri HX 3/4/6E/8E)

RS232 Connection	
Maximum transmission speed	38k4 bps
Connector type	RJ45 in accordance with EIA-561
Connection with switched on Compri HX	Permitted

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.