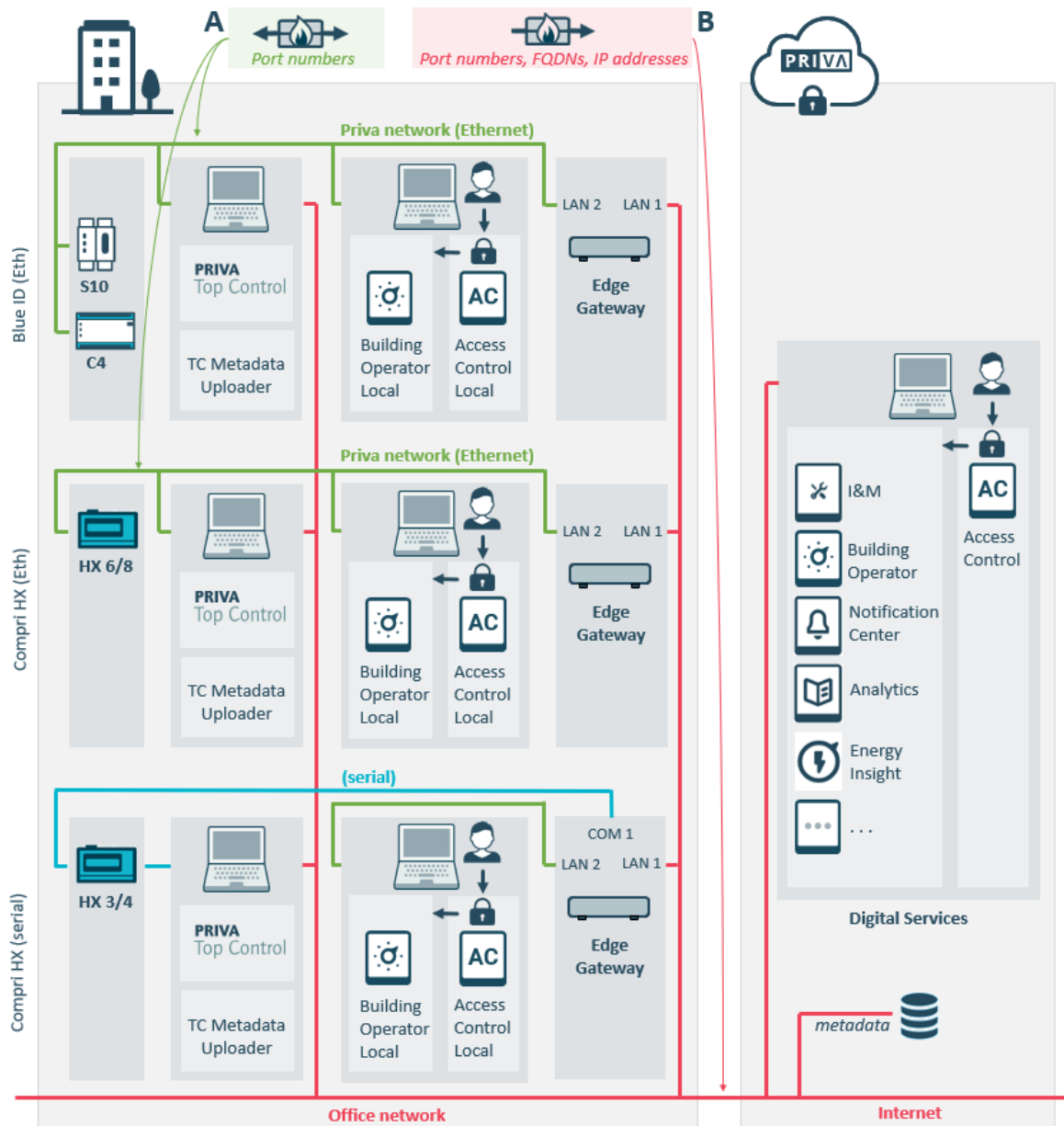


> ICT-INFORMATIE

Priva Blue ID, Top Control, Digital Services

Hoe beschermt Priva de data van uw gebouw? En wat moet u doen om communicatie tussen de Priva hardware en software op een veilige manier mogelijk te maken?

Netwerkoverzicht



- A** Om de communicatie binnen het lokale netwerk mogelijk te maken, moeten specifieke poorten open staan in de firewall (indien een firewall aanwezig is).
Zie: Communicatie binnen het lokale netwerk (pag. 3)
- B** Om de communicatie met de Priva Cloud mogelijk te maken, moeten ook in deze firewall specifieke poorten open staan. Daarnaast moet de communicatie met de Priva Cloud toegestaan worden op basis van FQDN's of op basis van IP-adressen.
Zie: Communicatie met de Priva Cloud (pag. 5)

Functie Edge Gateway / Cloud Connector

Gebouwbeheersystemen mogen nooit op een netwerk met internettoegang draaien. Om cloud services te kunnen gebruiken, is natuurlijk wel communicatie tussen het beheersysteem en de Priva Cloud nodig. De Edge Gateway en de Cloud Connector zijn gateways die dit op een veilige manier mogelijk maken. De Edge Gateway is de opvolger van de Cloud Connector.

De gateway staat alleen uitgaande verbindingen toe. Zo beschermt het het gebouwbeheersysteem tegen toegang door onbevoegden via het internet. Inkomende verbindingen staat de gateway niet toe. Als de gateway de verbinding naar buiten toe opzet, zal inkomend verkeer binnen die actieve sessie wel worden toegestaan. Dit maakt het mogelijk om met een applicatie/dienst van buitenaf waarden aan te passen.

De data die wordt overgedragen tussen de gateway en de cloud is beveiligd aan de hand van versleuteling. In tegenstelling tot andere methoden voor toegang tot gebouwautomatiseringssystemen, zoals een VPN, maakt deze architectuur gebruik van een systeem op basis van berichten, dus is er geen volledige datalink tussen het gebouw en de buitenwereld. Er wordt slechts in heel beperkte mate data uitgewisseld.

Updates van Windows 10 IoT op de Cloud Connector worden automatisch gedownload en geïnstalleerd volgens het standaard Windows Update mechanisme. Er wordt geen herstart geforceerd binnen de standaard actieve uren van de Cloud Connector (8.00-17.00 uur).

Updates van Linux op de Edge Gateway worden uitgevoerd in Installation & Maintenance (module FirmwareUpdater).

Support van Priva

Priva kan eenvoudig support op afstand leveren via TeamViewer op de Cloud Connector. Hiervoor moet poort 5938 open staan.

Bij de Edge Gateway is support via TeamViewer niet van toepassing omdat deze gateway extern niet direct benaderbaar is.

Beveiligingsmaatregelen van Microsoft

Alle Digital Services zijn vormgegeven op basis van het cloudplatform van Microsoft Azure. De services van Priva maken gebruik van de standaardcomponenten IoT-hub en Service Bus van Microsoft Azure voor de communicatie tussen het gebouw en de cloud. Gedetailleerde informatie over de beveiliging van Microsoft vindt u in het Microsoft Trust Center.

Communicatie binnen het lokale netwerk

Om de communicatie binnen het lokale netwerk mogelijk te maken, moeten specifieke poorten open staan in de firewall (indien een firewall aanwezig is).

Zie **A** in de afbeelding in Netwerkoverzicht (pag. 1).

Poortnummers (communicatie binnen lokale netwerk)

In de tabel hieronder staan de poortnummers die nodig zijn voor de communicatie tussen de Priva Blue ID-hardware en Top Control-applicaties en de Cloud Connector of Edge Gateway. Ook staat hierin aangegeven of de poorten gebruik maken van ingaande of uitgaande communicatie. De configuratie van de poorten in de firewall is afhankelijk van de gebruikte Top Control-applicaties en de gemaakte netwerkconfiguratie in het project.

Poort	Details	Transport-protocol	Priva Blue ID	TC Engineer	TC Operator	TC Manager	TC ServeCenter	TC History proxy	TC History	TC LAN Manager	Edge Gateway	Cloud Connector
22	SSH	TCP										
25 465 587 ¹⁶	SMTP(S) ¹⁶	TCP										
53	DNS	TCP/UDP										
80	HTTP	TCP										
123	NTP	TCP/UDP										
161	SNMP ⁸	TCP/UDP										
502 ²	Modbus	TCP										
514	Rsyslog	UDP										
1883	MQTT	TCP										
1900	SSDP	UDP										
5000	LOAS ¹²	TCP										
5001	LOUM ¹³	TCP										
5002	LOU ¹⁴	TCP										
5003	LOAS ¹⁵	TCP										
5353	mDNS	TCP/UDP										
7650	DDS	UDP										
7651	DDS	UDP										
7660	DDS	UDP										
7661	DDS	UDP										
8080 ²	HTTP	TCP										

Poort	Details	Transport-protocol	Priva Blue ID	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 t/m 47817 ¹⁶	BACnet ⁶	UDP										

- = ingaand
- = uitgaand
- = in- en uitgaand

¹ Alleen online help

² Standaard poortnummer, kan gewijzigd worden

³ Bij lokaal communiceren

⁴ TC LAN Manager zoekt een vrij te gebruiken poortnummer

⁵ Priva-eigen protocol

⁶ Gereserveerde poorten, instelbaar in TC Engineer

⁷ Bij gebruik van een Compri HX connectie

⁸ Alleen SNMP Trap wordt ondersteund in Top Control 8

⁹ LAN-poort aangesloten op internet
(Edge Gateway: LAN 1, Cloud Connector: LAN 3)

¹⁰ LAN-poort aangesloten op Priva-netwerk
(Edge Gateway: LAN 2, Cloud Connector: LAN 1)

¹¹ Servicepoort

(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 Kies één van de genoemde poortnummers

¹⁷ Kies één van de genoemde poortnummers. De gekozen poortnummers uit de twee rijen met opmerking 17 moeten elkaar opvolgen (bijv. 23456 en 23457).













Communicatie met de Priva Cloud


Om de communicatie met de Priva Cloud mogelijk te maken, moeten specifieke poorten open staan in de firewall. Daarnaast moet de communicatie met de Priva Cloud toegestaan worden op basis van FQDN's of op basis van IP-adressen.

Zie **B** in de afbeelding in Netwerkoverzicht (pag. 1).

Poortnummers (communicatie met Priva Cloud)

In de tabel hieronder staan de poortnummers die nodig zijn voor communicatie met de Priva Cloud. Alle poorten maken alleen gebruik van uitgaande communicatie. Poort 5938 is nodig voor support van Priva met TeamViewer (alleen op de Cloud Connector).

Poort	Details	Transport-protocol	Edge Gateway	Cloud Connector
67	DHCP	TCP	 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	 1

 = uitgaand

¹ LAN-poort aangesloten op internet
(Edge Gateway: LAN 1, Cloud Connector: LAN 3)

FQDN's voor Digital Services

In de lijst hieronder staan de Fully Qualified Domain Names (FQDN) weergegeven die nodig zijn voor Digital Services. U heeft de keus om wildcards (adressen startende met *) te gebruiken of de volledige FQDN's vrij te geven. De lijst van volledige FQDN's is echter wel dynamisch; er kunnen in de toekomst FQDN's toegevoegd worden en ze kunnen gewijzigd worden. Het gebruik van wildcards is meer onderhoudsvriendelijk omdat de lijst van wildcards minder vaak zal wijzigen dan de lijst van volledige FQDN's.

Wildcard	FQDN
*.servicebus.windows.net	priva-lwe-prod-gateway-master-weu.servicebus.windows.net priva-lwe-prod-gateway-partition-weu.servicebus.windows.net priva-lwe-prod-gateway-partition2-weu.servicebus.windows.net
*.azurewebsites.net	prd-gps-service-wa.azurewebsites.net prd-gps-state-wa.azurewebsites.net prd-safefiletransferapi-we.azurewebsites.net
*.blob.core.windows.net	edgegatewayfirmware.blob.core.windows.net coprdrfrontend2sawe.blob.core.windows.net prddevicemetadatas.blob.core.windows.net prdinstallupdatesa.blob.core.windows.net prdprivaauditlogs.blob.core.windows.net
*.azure-devices.net	prd-priva-generic-ih.azure-devices.net
*.b2clogin.com	privaid.b2clogin.com
*.priva.com	accesscontrolapi.priva.com alarms.priva.com analytics.priva.com assetapi.priva.com auth.priva.com authorization.priva.com apps.priva.com catalogapi.priva.com comfortmanagement.priva.com connect.priva.com cr.priva.com cr-data-westeuropa.priva.com gps.priva.com iam.priva.com installationandmaintenance.priva.com local-auth-provisioning.priva.com my.priva.com notificationcenter.priva.com operator.priva.com scheduler.priva.com tenantapi.priva.com
*.erbis.one	erbis.one
n.v.t.	mcr.microsoft.com priva.azurecr.io priva.westeurope.data.azurecr.io global.azure-devices-provisioning.net

IP-adressen voor Digital Services

Priva gebruikt bij de 'EuropeWest' IP-adres reeksen van Microsoft die nodig zijn voor Digital Services. Deze reeksen worden dynamisch gebruikt door Microsoft en kunnen daarom niet specifiek genoemd worden. De reeksen die Microsoft gebruikt, zijn te vinden op hun website onder 'Microsoft Azure Datacenter IP Ranges' <https://www.microsoft.com/en-us/download/details.aspx?id=41653>



Maak geen gebruik van IP-adresreeks 172.23.105.0/24. Deze reeks wordt namelijk al intern in de Edge Gateway gebruikt.

Internetverbinding voor Digital Services

Alle Digital Services vereisen een breedband-internetverbinding met een minimale upload- en downloadsnelheid van 1 Mbps.



De *Priva Cloud Connectivity Check*-tool (snelkoppeling op bureaublad van de Cloud Connector) controleert hierop.

De internetverbinding heeft bij voorkeur een zo hoog mogelijke uploadsnelheid. Hoe groter het project, hoe hogere uploadsnelheid u nodig zult hebben.

Aanvullende vereisten TC Manager Connect



TC Manager Connect wordt vervangen door Building Operator. Priva adviseert u om gebruik te maken van Building Operator.

U kunt TC Manager op afstand gebruiken via TC Manager Connect via het internet. Een VPN-verbinding is dan niet nodig.

Voor het gebruik van TC Manager en TC Manager Connect gelden de volgende eisen:

- Ondersteunde browser: Internet Explorer 10.0 of hoger
- Microsoft Silverlight 5

Specificaties communicatie Priva Blue ID

Ethernet	
Toegepaste netwerkstandaard	IEEE 802.3 (37 ... 57 Vdc) 10BASE-T (10 Mbps) 100BASE-TX (100 Mbps) auto negotiation auto-MDIX IPv4
DHCP	niet ondersteund
Transmissiesnelheid	10 Mbps en 100 Mbps
Aansluiten apparatuur van derden toegestaan	ja
Vereist kabeltype	UTP of STP, minimaal categorie 5
Maximale kabellengte	100 m
Connectortype	RJ45, afgeschermd
Kabeldiameter (bij gebruik van Priva Blue ID TouchPoint Flush Afdekkap (voor paneelmontage))	4 - 6,5 mm

Power over Ethernet is alleen van toepassing op Priva Blue ID S-Lijn.

Power over Ethernet	
Toegepaste netwerkstandaard	IEEE 802.3af (37 ... 57 Vdc) Powered Device (PD) Class 0

Kabels (Priva Blue ID S-Lijn)

Module	Specificaties toe te passen kabel
Priva Blue ID S-Lijn SN1 Netwerkmodule, Priva Blue ID S-Lijn SN2 Netwerkmodule en Priva Blue ID S-Lijn SN3 Netwerkmodule	<ul style="list-style-type: none"> type: UTP of STP, minimaal categorie 5 maximale lengte: 100 m connectortype: RJ45, afgeschermd
Priva Blue ID S-Lijn SN3t Netwerkmodule <i>De SN3t-module wordt niet meer geleverd. U kunt de ORing Netwerkmodule gebruiken voor 2-wire.</i>	<p>Naast de hierboven genoemde kabel kan de volgende kabel toegepast worden:</p> <ul style="list-style-type: none"> type: twisted pair (telefoon- of datakabel) aderdoorsnede: 0,2 ... 2,5 mm² zonder adereindhuls 0,25 ... 2,5 mm² met adereindhuls maximale lengte tussen twee controllers: 500 m nominaal¹ maximale totale lengte: 1000 m nominaal¹ connectortype: tweepolige schroefconnector (aansluiting polariteitsongevoelig)
ORing Netwerkmodule	<ul style="list-style-type: none"> 2-draads (telefoon- of datakabel) CAT5/6 is ook toegestaan maximale kabellengte tussen twee ORing-modules: 500 m¹ connectortype: 2-pins veerdrukklem (aansluiting polariteitsongevoelig)
Priva Blue ID TouchPoint	<ul style="list-style-type: none"> type: UTP of STP, minimaal categorie 5 maximale lengte: 100 m connectortype: RJ45, afgeschermd

¹ De maximale kabellengte is gebaseerd op testresultaten met twisted-pairkabel categorie 5E en Alpha Wire 5261C; bij andere kabeltypen is de maximale lengte mogelijk kleiner.

Kabels (Priva Blue ID C-Lijn)

Module	Specificaties toe te passen kabel
Priva Blue ID C4 C-MX34(m) - ethernet	<ul style="list-style-type: none">• type: UTP of STP, minimaal categorie 5• maximale lengte: 100 m• connectortype: RJ45, afgeschermd
ORing Netwerkmodule	<ul style="list-style-type: none">• 2-draads (telefoon- of datakabel) CAT5/6 is ook toegestaan• maximale kabellengte tussen twee ORing-modules: 500 m¹• connectortype: 2-pins veerdruklem (aansluiting polariteitsongevoelig)
Priva Blue ID TouchPoint	<ul style="list-style-type: none">• type: UTP of STP, minimaal categorie 5• maximale lengte: 100 m• connectortype: RJ45, afgeschermd

¹ De maximale kabellengte is gebaseerd op testresultaten met twisted-pairkabel categorie 5E en Alpha Wire 5261 C; bij andere kabeltypen is de maximale lengte mogelijk kleiner.

Specificaties communicatie Compri HX

Aansluiting Ethernet (alleen Compri HX 6E/8E)	
Ondersteunde netwerkklassen	A, B en C
Transmissiesnelheid	10 Mbit/sec
Netwerktipe	10BASE-T volgens norm IEEE 802.3
NE2000 Compatibel	Ja
Connectortype	RJ45 MDI (Media dependant interface)
Kabeltype	Unshielded twisted pair Cat.5 (UTP)
Maximale kabellengte	100 m
Aansluiten met ingeschakelde Compri HX	Toegestaan

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

Aansluiting RS232	
Maximale transmissiesnelheid	38k4 bps
Connectortype	RJ45 volgens EIA-561
Aansluiten met ingeschakelde Compri HX	Toegestaan

Priva (hoofdkantoor)
Zijlweg 3
2678 LC De Lier
Nederland

Uw Priva partner:

Zie www.priva.com voor contactgegevens van een Priva kantoor of partner voor uw regio.

