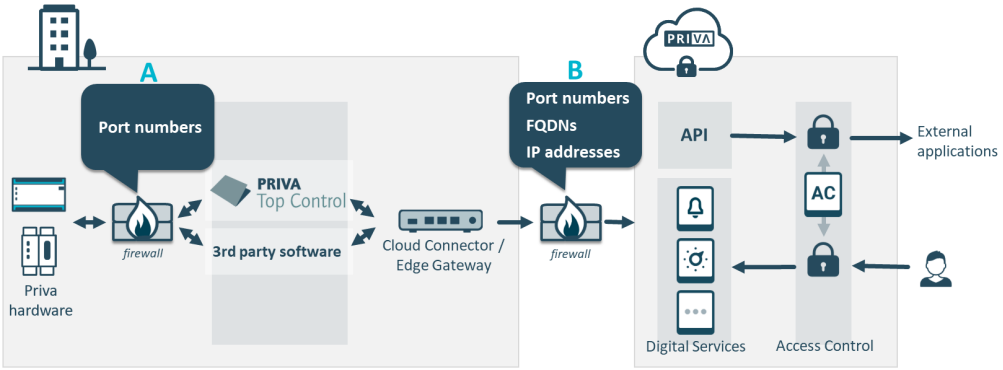
> INFORMATION DE TIC

Priva Blue ID, Top Control, Digital Services

Comment Priva protège-t-il les données de votre bâtiment ? Et que devez-vous faire pour permettre la communication entre le matériel et le logiciel Priva de manière sécurisée ?



A Pour permettre la communication au sein du réseau local, des ports spécifiques doivent être ouverts dans le pare-feu (si un pare-feu est présent).
Voir : Communication au sein du réseau local (page 2)

B Pour permettre la communication avec le Priva Cloud, des ports spécifiques doivent également être ouverts dans ce pare-feu. Il convient en outre d'autoriser la communication avec le Priva Cloud sur la base des noms de domaine FQDN ou sur la base des adresses IP.
Voir : Communication avec le Priva Cloud (page 4)

Fonction Edge Gateway / Cloud Connector

Les systèmes de gestion de bâtiment ne doivent jamais fonctionner sur un réseau avec accès à Internet. Mais pour pouvoir utiliser des services cloud, il faut naturellement qu'une communication soit établie entre le système de gestion et le Priva Cloud. Le Edge Gateway et le Cloud Connector sont des passerelles qui le permettent de manière sécurisée. Edge Gateway est le successeur de Cloud Connector.

La passerelle autorise uniquement les connexions sortantes. Elle protège ainsi le système de gestion de bâtiment contre tout accès non autorisé via Internet. La passerelle n'autorise pas les connexions entrantes. Lorsque la passerelle établit la connexion vers l'extérieur, un trafic entrant sera toutefois autorisé dans le cadre de cette session active. Ceci permet de modifier des valeurs de l'extérieur à l'aide d'une application ou d'un service.

Les données transférées entre la passerelle et le cloud sont sécurisées par cryptage. Contrairement à d'autres méthodes d'accès aux systèmes d'automatisation du bâtiment, tels qu'un VPN, cette architecture utilise un système basé sur des messages, il n'y a donc pas de lien de données complet entre le bâtiment et le monde extérieur. Seule une quantité très limitée de données est échangée.

Les mises à jour de Windows 10 IoT sur le Cloud Connector sont automatiquement téléchargées et installées selon le mécanisme standard de Windows Update. Aucun redémarrage n'est forcé pendant les heures d'activité standard du Cloud Connector (8h00-17h00).

Les mises à jour de Linux sur le Edge Gateway sont effectuées dans Installation & Maintenance (module FirmwareUpdater).

Support de Priva

Priva peut facilement fournir une assistance à distance via TeamViewer sur le Cloud Connector. Le port 5938 doit être ouvert pour cette opération.

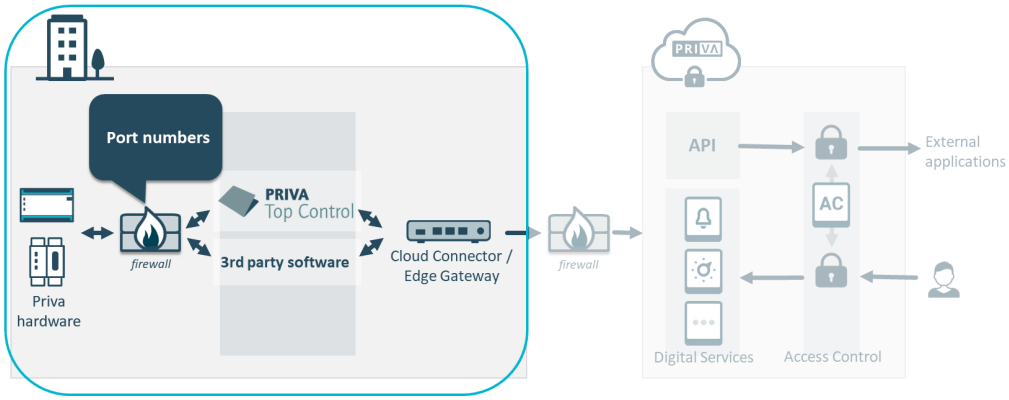
L'assistance via TeamViewer ne s'applique pas au Edge Gateway, car celui-ci n'est pas directement accessible de l'extérieur.

Mesures de protection de Microsoft

Tous les Digital Services s'appuient sur la plateforme de cloud de Microsoft Azure. Les services de Priva utilisent les composants standard IoT-hub et Service Bus de Microsoft Azure pour la communication entre le bâtiment et le cloud. Les informations détaillées de protection de Microsoft sont disponibles dans le Microsoft Trust Center.

Communication au sein du réseau local

Pour permettre la communication au sein du réseau local, des ports spécifiques doivent être ouverts dans le pare-feu (si un pare-feu est présent).



Numéros de port (communication au sein du réseau local)

Le tableau ci-dessous indique les numéros de port requis pour la communication entre le matériel Priva Blue ID et les applications Top Control et le Cloud Connector ou Edge Gateway. Celui-ci précise également si les ports utilisent une communication entrante ou sortante. La configuration des ports dans le pare-feu dépend des applications Top Control utilisées et de la configuration du réseau créée dans le projet.

Port	Détails	Protocole transport	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	►	►	►	►	►	►	►	►	► 9,10,11	► 10
80	HTTP	TCP	◄►	► 1	► 1	►	► 1	► 1	► 1	► 1	◄► 11	
123	NTP	TCP/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	

Port	Détails	Protocole transport	Priva Blue ID	TC Engineer	TC Operator	TC Manager	TC ServeCenter	TC History proxy	TC History	TC LAN Manager	Edge Gateway	Cloud Connector
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				↔		↔				
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	↔									

↔ = entrant
↔ = sortant
↔ = entrant et sortant

[1] Aide en ligne uniquement

[2] Numéro de port standard, peut être modifié

[3] Lors de la communication locale

[4] TC LAN Manager recherche un numéro de port libre

[5] Protocole propre à Priva

[6] Ports réservés, réglables en TC Engineer

[7] En cas d'utilisation d'une connexion Compri HX

[8] Seul SNMP Trap est supporté dans Top Control 8

[9] Port LAN connecté à internet
(Edge Gateway : LAN 1, Cloud Connector : LAN 3)

[10] Port LAN connecté au réseau Priva
(Edge Gateway : LAN 2, Cloud Connector : LAN 1)

[11] Port de service
(Edge Gateway : LAN 3, Cloud Connector : LAN 2)

[12] Service d'autorisation d'opérateurs locaux

[13] IU de gestion des opérateurs locaux

[14] IU des opérateurs locaux

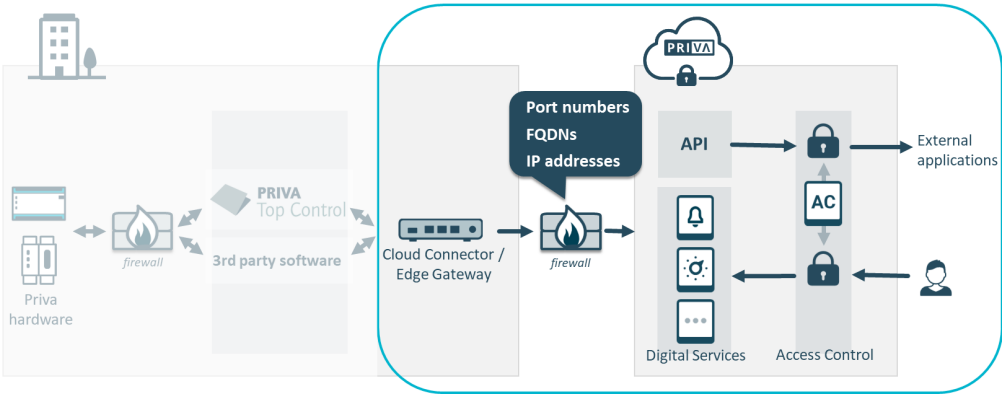
[15] API des opérateurs locaux

[16] Composez l'un des numéros de port répertoriés

[17] Composez l'un des numéros de port répertoriés. Les numéros de port sélectionnés dans les deux lignes de la remarque 17 doivent se suivre (p. ex. 23456 et 23457).

Communication avec le Priva Cloud

Pour permettre la communication avec le Priva Cloud, des ports spécifiques doivent être ouverts dans le pare-feu. Il convient en outre d'autoriser la communication avec le Priva Cloud sur la base des noms de domaine FQDN ou sur la base des adresses IP.



Numéros de port (communication avec Priva Cloud)

Le tableau ci-dessous répertorie les numéros de ports nécessaires pour communiquer avec le Priva Cloud. Tous les ports utilisent uniquement la communication sortante. Le port 443 est le minimum requis pour la communication avec le cloud. Les autres ports permettent une connexion plus rapide et plus stable au cloud. Le port 5938 est requis pour le support de Priva avec TeamViewer (uniquement sur le Cloud Connector).

Port	Détails	Protocole transport	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

= sortant

[1] Port LAN connecté à internet
(Edge Gateway : LAN 1, Cloud Connector : LAN 3)

FQDN pour Digital Services

La liste suivante reprend les noms de domaines complets (Fully Qualified Domain Names ou FQDN) nécessaires pour les Digital Services. Vous avez la possibilité d'utiliser des caractères génériques (adresses commençant par *) ou d'indiquer le FQDN complet. La liste des noms de domaines complets est dynamique ; il est possible d'y ajouter des FQDN ultérieurement et de les modifier. L'utilisation de caractères génériques facilite la maintenance du fait qu'une liste comportant des caractères génériques changera moins souvent qu'une liste de FQDN complets.

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**	prdinstallupdatesa.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 iam.priva.com installationandmaintenance.priva.com my.priva.com notificationceter.priva.com operator.priva.com scheduler.priva.com tenantapi.priva.com
***.erbis.one**	erbis.one

Addresses IP pour les Digital Services

Priva utilise pour l'adresse IP 'EuropeWest' des séries de Microsoft requises pour les Digital Services. Ces séries sont utilisées de manière dynamique par Microsoft et ne peuvent donc pas être mentionnées spécifiquement. Les séries utilisées par Microsoft sont disponibles sur leur site Web sous "Microsoft Azure Datacenter IP Ranges".
https://www.microsoft.com/en-us/download/details.aspx?id=41653

Connexion Internet pour Digital Services

Tous les Digital Services nécessitent une connexion Internet à haut débit avec une vitesse d'au moins 1 Mbps en liaison montante et en liaison descendante.

L'outil *Priva Cloud Connectivity Check* (raccourci présent sur le bureau de Cloud Connector) permet de vérifier ce point.
La connexion Internet aura de préférence une vitesse de transmission montante aussi élevée que possible. Plus le projet est étendu, plus vous aurez besoin d'une vitesse de transmission montante élevée.

Exigences complémentaires pour TC Manager Connect

TC Manager Connect est remplacé par Building Operator. Priva vous recommande d'utiliser Building Operator.

Vous pouvez utiliser TC Manager à distance via TC Manager Connect en passant par Internet. Aucune connexion VPN n'est requise.

L'utilisation de TC Manager et TC Manager Connect suppose de satisfaire aux exigences suivantes :

- Navigateur pris en charge : Internet Explorer 10.0 ou au-delà
- Microsoft Silverlight 5

Spécifications de la communication Priva Blue ID

Ethernet	
Norme réseau appliquée	IEEE 802.3 (37 ... 57 Vcc) 10BASE-T (10 Mbps) 100BASE-TX (100 Mbps) auto-négociation auto-MDIX IPv4
DHCP	non pris en charge
Vitesse de transmission	10 Mbps et 100 Mbps
Le raccordement d'appareils tiers est autorisé	oui
Type de câble requis	UTP ou STP, catégorie minimum 5
Longueur de câble maximum	100 m
Type de connecteur	RJ45, blindé
Diamètre du câble (en cas d'utilisation Priva Blue ID TouchPoint Flush Back Cover (pour d'encastrement dans porte d'une armoire électrique))	4 - 6,5 mm

Power over Ethernet s'applique uniquement sur Priva Blue ID S-Line.

Power over Ethernet	
Norme réseau appliquée	IEEE 802.3af (37 ... 57 Vcc) Powered Device (PD) Classe 0

Câbles (Priva Blue ID S-Line)

Module	Spécifications du câble à utiliser
Module de réseau Priva Blue ID S-Line SN1 , Module de réseau Priva Blue ID S-Line SN2 en Module de réseau Priva Blue ID S-Line SN3	• type : UTP ou STP, catégorie minimum 5 • longueur maximale : 100 m • type de connecteur : RJ45, blindé
Module de réseau Priva Blue ID S-Line SN3t	Outre le câble susmentionné, le câble suivant peut également être utilisé : • type : paire torsadée (câble de téléphone ou de données) • section du fil : 0,2 ... 2,5 mm² sans embout de câblage 0,25 ... 2,5 mm² avec embout de câblage • longueur maximale entre deux régulateurs : 500 m nominale[1] • longueur totale maximale : 1000 m nominale[1] • type de connecteur : connecteur à vis et à 2 broches (connexion insensible à la polarité) [1] La longueur maximale du câble est basée sur les résultats d'essais avec un câble à paire torsadée de catégories 5E et Alpha Wire 5261C ; la longueur maximale pour d'autres types de câble est probablement inférieure.
TouchPoint Priva Blue ID	• type : UTP ou STP, catégorie minimum 5 • longueur maximale : 100 m • type de connecteur : RJ45, blindé

Câbles (Priva Blue ID C-Line)

Module	Spécifications du câble à utiliser
Priva Blue ID C4 C-MX34(m) - Ethernet	• type : UTP ou STP, catégorie minimum 5 • longueur maximale : 100 m • type de connecteur : RJ45, blindé
TouchPoint Priva Blue ID	• type : UTP ou STP, catégorie minimum 5 • longueur maximale : 100 m • type de connecteur : RJ45, blindé

Spécifications de la communication Compri HX

Connexion Ethernet (uniquement Compri HX 6E/8E)	
Classes de réseau supportées	A, B et C
Vitesse de transmission	10 Mbit/s
Type de réseau	10BASE-T selon la norme IEEE 802.3
Compatible NE2000	Oui
Type de connecteur	RJ45 MDI (Media dependant interface)
Type de câble	Unshielded twisted pair (Paire torsadée non blindée) Cat.5 (UTP)
Longueur de câble maximum	100 m
Raccordement avec Compri HX activé	Autorisé

Câbles (Compri HX 3/4/6E/8E)

Raccordement du RS232	
Vitesse maximale de transmission	38k4 bps
Type de connecteur	RJ45 d'après EIA-561
Raccordement avec Compri HX activé	Autorisé

Priva (siège social)
Zijlweg 3
2678 LC De Lier
Pays-Bas

Votre partenaire Priva:

Pour contacter l'équipe Priva ou l'un de nos partenaires dans votre secteur, vous pouvez vous rendre sur le site web www.priva.com