XMS Cloud and (Virtual) Edge Security Whitepaper

DATE 20/09/2021

AUTHOR David Martens | Soumen Mukherjee | Maxim Deboiserie

Table of content

Security at Barco

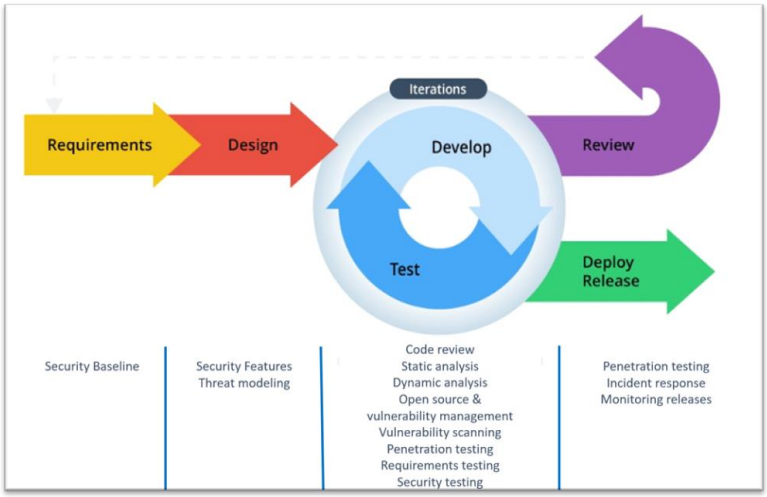
As a technology leader that develops devices capable of connecting to the internet and related software solutions, Barco is fully aware of the growing importance of corporate security. In addition, we set great store by proper data governance, in order to protect our data and that of our customers and comply with regulations like GDPR and similar data privacy legislation outside the EU.

Barco has an information security management system (ISMS) which complies with the ISO 27001 standard, covering policies, management involvement, business processes, technology, compliance with local laws, security awareness and security best practices. In collaboration with the data protection officer, we assess a growing number of high-risk third parties based on security and privacy requirements. In addition, we continuously monitor our key vendors' external security activities. We are gradually working to contain all processes, locations and products within the scope of our ISMS and ISO/IEC 27001:2013 certification. The products and locations in scope are specifically mentioned on our certificate, which can be found on https://www.barco.com/en/about-barco/legal/certificates

More information can be found in Barco's **integrated annual report**, which can be found on our corporate website: https://www.barco.com

Barco's Secure Software Development Lifecycle

Our secure software development lifecycle follows the shift-left security approach: we aim to integrate security controls as early as possible in the design and development phases of our products. This is industry best practice and becoming increasingly important in complying with regulations that focus on security by design, such as the United States Health Insurance Portability and Accountability Act (HIPAA) and Medical Device Regulation (MDR). To integrate these security controls, Barco uses source code management platforms, bug tracking systems, threat modeling, static application security testing, opensource security and compliance management tools, dynamic application security testing and vulnerability scanners. Furthermore, we work together with independent security experts to train our developers and test the security of our products. Thanks to these efforts, we increasingly embrace the 'security by design' principle.



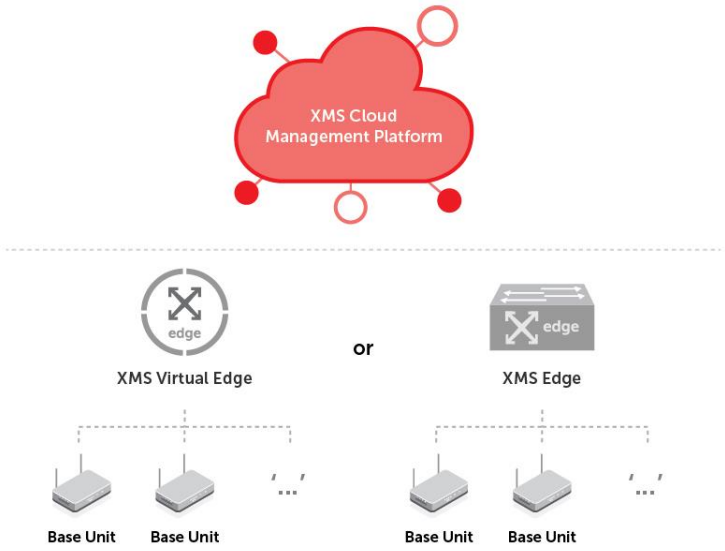
Product introduction

The **XMS Cloud** Management Platform offers the ultimate solution for IT managers deploying or owning a large install base of ClickShare and/or wePresent wireless collaboration devices. It provides an easy-to-use interface for remote and reliable device management to guarantee the most optimal user experience and brings useful analytics to drive the Digital Workplace.
The XMS Cloud Management Platform allows to monitor and manage the latest ClickShare devices within your environment. XMS Cloud is your ideal companion to get worldwide access to your install base.

ClickShare Conference and Present devices (CX-20, CX-30, CX-50, C-5 and C-10) can be accessed directly from within XMS Cloud.
ClickShare's wireless presentation and collaboration devices (CS-100 Huddle, CS-100, CSE-200, CSE-200+, CSE-800) and wePresent devices require a cloud gateway to be accessible from XMS Cloud. Two solutions are available that can act as a gateway:

- **XMS Edge**, a plug & play hardware appliance
- **XMS Virtual Edge**, a free software download in the form of an OVA file

IT or facility managers can easily deploy the XMS Virtual Edge onto a local server or install the plug & play XMS Edge and use them as a gateway to the XMS Cloud management platform.



Product security

XMS Cloud

Authentication

Authentication on XMS cloud is offered through Barco's Customer Identity and Access Management (CIAM) https://auth.barco.com/. Barco's CIAM is built on top of Microsoft Azure B2C where user passwords are stored in hashed format. Barco CIAM enforces a minimum password length of 12 characters as an additional safeguard and brute force attack prevention is in place via defined lockout threshold and lockout duration.

Session management

Sessions on XMS Cloud make use of Open ID Connect (OIDC). OIDC is an identity layer built on top of the OAuth 2.0 protocol, which allows clients to verify the identity of an end user based on the authentication performed by an authorization server or identity provider (IdP), Barco's CIAM.

The following token lifetimes are configured by Barco's CIAM:

- Identity token: 10 minutes
- Access token: 10 minutes
- Refresh token: 2 weeks

Additionally, authentication and authorization in the entire XMS Cloud microservice architecture is secured by sidecars which implements the security principle of zero trust network and principle of least privilege to enforce security controls at every component endpoint.

Role based access control (RBAC)

The first user who creates the tenant is assigned the **admin role** and is the tenant admin. XMS Cloud provides options to define granular role-based access control. It is strongly recommended to define roles based on needs and in line with your organization's information security policies. XMS offers the following default role at tenant creation:

- ***admin role***: This role has full access rights to manage the complete tenant. This role cannot be modified or deleted.

The tenant admin can create additional roles with specific access rights to tailor role-based access control to the needs of the organization.

Security recommendation: Ensure continued admin access to your tenant on XMS Cloud by configuring a second administrator as a fallback option.

Security recommendation: It is the responsibility of the tenant admin to regularly review users and roles to keep them aligned with employee migrations and changes in the

organization.

Audit log

Users with the admin role have access to the XMS Cloud tenant audit logs. All actions executed by users inside the tenant are logged and should be reviewed for irregularities.

Security recommendation: The tenant admin has to regularly review the audit logs for any unintended changes done to role-based access controls or user management.

Secure IoT connectivity

The direct connections from ClickShare Conference and Present devices (CX-20, CX-30, CX-50, C-5 and C-10), and the connection through XMS (Virtual) Edge are based on **Azure IoT Hub technology** to securely connect, monitor and manage the ClickShare and wePresent install base.

Secure Azure AD integration

XMS Cloud can be used to display the availability of the meeting room on the screen using ClickShare (optional feature). This is done securely using **Azure Enterprise Applications** that integrate with Azure AD. To mitigate security risks that might arise while integrating Azure Enterprise Applications in Azure AD, this feature makes use of 2 separate Azure Enterprise Applications, the 'ClickShare Meeting Room Discovery' and the 'ClickShare Calendar Sync'. The 'ClickShare Meeting Room Discovery' is a multi-tenant application while the 'ClickShare Calendar Sync' is a single tenant application, only hosted in the customer's Azure AD. The ClickShare Base Units access the calendars only through the single tenant 'ClickShare Calendar Sync' using a per customer unique and random client secret. The client secret is created by Microsoft with the following properties: randomly generated and expires automatically after 24 months.

The table below provides an overview of the permissions that each Azure Enterprise Application requests and the purpose. For each requested permission, least-privilege principles were considered.

Resource permission	Type	Purpose
'***ClickShare Meeting Room Discovery***' *multi-tenant application*		
Application.ReadWrite.OwnedBy	Application permission	Used to create the 'ClickShare Calendar Sync' in the customer tenant, once during installation. Used during operations to interact with the 'ClickShare Calendar Sync'.
Place.Read.All	Application permission	Used during operations to help the tenant admin selecting the correct meeting room linked to a ClickShare Base Unit.
User.Read	Delegated permission	Used once during installation to sign-in to the app and grant consent.

'ClickShare Calendar Sync' *single tenant application*		
Calendars.Read	Application permission	Used during operations to read calendar invites of a particular room-account in the organization. This helps to show room availability status on the Base Unit associated with a particular room-account.
User.Read	Delegated permission	Used once during installation to sign-in to the app and grant consent.

More details regarding these permissions in Azure AD can be found on https://docs.microsoft.com/en-us/graph/permissions-reference#user-permissions

Security recommendation: Verify the publisher (Barco) of the Enterprise Application before adding it to your tenant.

Security recommendation: Limit the access of the Enterprise Application 'ClickShare Calendar Sync' to only the needed meeting rooms (and no other calendars) using an *ApplicationAccessPolicy* on *Microsoft Exchange Online.*

Privacy by design

The amount of personal data which is collected is limited to the absolute minimum. At registration time only name, email address and company name will have to be provided. The system administrator can add users to the XMS Cloud Management Platform via specifying their email address.

The data of the managed devices (ClickShare and wePresent) which is uploaded to XMS Cloud does not contain any personal data.

Data categories, Backup & Retention

The data is generally classified in three categories, as shown in the table below.

Barco does perform backups ensuring disaster recovery and business continuity of the application (not specific tenants). Backup restore testing is done periodically and adequate controls are in place to guarantee the confidentiality, integrity and availability of the data backup. Please note that the XMS Cloud user interface does not provide to the tenant admin the feature to export and import local backups.

For all data categories daily backups are taken. The data retention period varies per data category. The following table summarizes the data retention period for the different data

categories:

Data Category	Description	Backup Retention Period
Customer Data	This is generally the data generated by devices, data generated by users of XMS Cloud and the tenant configuration itself.	3 Months (daily backup)
Functional Audit Logs	This is the audit trail data which is generated when any XMS Cloud user makes changes to the any of the application data being managed by XMS Cloud and contains logs of the last 365 days.	1 Year (daily backup)
Backend Services Logs	This data contains the logs of the last fortnight generated by the running microservices of the platform.	45 Days (daily backup)

Encryption at rest and in transit

All customer data in XMS Cloud is encrypted at rest (disk/volume encryption) using AES-256. The cryptographic keys are managed by Barco, it is not possible for the customer to configure their own keys for encryption at rest.

Communication to XMS Cloud is encrypted in transit using TLS 1.2 or above.

Usage of open source

XMS Cloud makes use of multiple open-source software packages. Barco closely monitors both for any open-source licenses violating our own policies which would impact cloud deployment and for new vulnerabilities detected in the used open-source packages. If a vulnerability is detected or reported, it will be analysed and depending on the criticality and impact, planned in for a future release.

Data localization

The XMS Cloud services, including backups and database services, are running in datacenters located in Ireland (Amazon AWS and Microsoft Azure). The infrastructure used for running the service is time synced by the 3rd party cloud service provider. All the container-based services, part of the XMS Cloud ecosystem and running on top of that infrastructure, are time synced with the underlying host environment provided by the 3rd party cloud service provider.

Data segregation

XMS Cloud is a multitenant cloud service where every customer has a dedicated share of the instance, this dedicated share is called a tenant. The data is structured per tenant and each tenant (including data, configuration, user management, …) is logically segregated. This is achieved by means of logical separation enforced at the application and at the source code level.

Transparency

Barco's product privacy statement is outlining more details regarding privacy, including which personal data is collected for which purposes and Data Subject Rights. You can find the Product Privacy Statement of XMS Cloud on the following website: https://www.barco.com/en/about-barco/legal/privacy-policy/product-privacy-statement.

Removal of customer tenant's assets

Due to security considerations a customer is not given the option to delete the full tenant configuration and assets from the system. In case a customer may want to purge the tenant and its assets, a support ticket has to be raised via our corporate service portal (https://www.barco.com/en/support). The request will be handled by our service team and the tenant and its corresponding information assets will be purged appropriately. Please be aware that customer tenant information will stay present in the backups until their retention period expires (cfr. Back-up & Data Retention).

User accounts are not managed in XMS Cloud, but in Barco's Customer Identity and Access Management (CIAM). If anyone wants to remove their account from Barco's CIAM a request should be sent to Barco's Data Protection Officer (cfr. Data Subject Rights). You can reach out to the Data Protection Officer via mail: dataprotection@barco.com.

XMS (Virtual) Edge

Signed firmware updates for XMS (Virtual) Edge

Regular updates are offered for XMS (Virtual) Edge. Each update is signed to guarantee the Barco's origin are verified during the update process. A firmware update of XMS (Virtual) Edge will cause unavailability of its services for a couple of minutes.

Latest firmware/software images with their release notes are available on Barco's corporate website: https://www.barco.com/en/clickshare/support/xms-edge/drivers

Keep ClickShare/wePresent device firmware up-to-date

Regular firmware updates are offered for ClickShare and wePresent devices. By default, these updates will not be installed automatically by XMS (Virtual) Edge, it is the responsibility of the XMS (Virtual) Edge administrator to download the latest releases on the XMS (Virtual) Edge instance and deploy the updates to the applicable devices. More details about this process can be found in the XMS (Virtual) Edge user guide available on www.barco.com. Keep in mind that a firmware update on the ClickShare and wePresent devices includes a reboot resulting in unavailability of their services for a couple of minutes.

Security recommendation: Manage the ClickShare and wePresent Base Unit firmwares and keep them in sync with the latest releases via XMS (Virtual) Edge.

Network connectivity

There is no inbound communication in XMS (Virtual) Edge, only outbound communication. The following table gives on overview of the used URL's and the corresponding port.

URL + port + protocol	Purpose
Inbound communication to XMS (Virtual) Edge	
:80 (TCP)	XMS Edge Web UI over HTTP *(not available when connected to XMS Cloud)*
:443 (TCP)	XMS Edge Web UI over HTTPS *(not available when connected to XMS Cloud)*
Outbound communication from XMS (Virtual) Edge	
:25 (TCP/UDP)	Accessing SMTP server, mandatory for sending emails to register new users and send out notifications via mail
:53 (TCP/UDP)	Accessing DNS server in customer's premises as configured by the customer
:80/8080 (TCP)	Proxy server for outbound communication (if necessary)
:123 (TCP/UDP)	NTP time synchronization
:443 (TCP)	Communication to: • Azure IoT Hub (sil-xms-prd01-iothub.azure-devices.net) and XMS Cloud (xms.cloud.barco.com and auth.barco.com) • Barco firmware update services for Base Units and XMS (Virtual) Edge (*.barco.com)

:465 (TCP)	Accessing SMTP server over TLS for sending emails
<ClickShare Base Unit IP>:4001 (TCP)	Communication to ClickShare Base Unit REST API over HTTPS (CS(E) range and CSC-1, CSM-1)
<ClickShare Base Unit IP>:4003 (TCP)	Communication to ClickShare Conference ***or*** Present Base Unit REST API over HTTPS
<wePresent Base Unit IP>:4001 (TCP)	Communication to wePresent Base Unit REST API over HTTPS

Usage of open source

XMS (Virtual) Edge makes use of multiple open-source software packages. The list of these packages is available on https://www.barco.com/en/opensourcesoftware/xms. Barco closely monitors for new vulnerabilities detected in the used open-source packages. If a vulnerability is detected or reported, it will be analysed and depending on the criticality and impact, planned in for a future release.

Physical system interfaces (XMS Edge only)

Externally accessible

- Ethernet
- USB
- External serial port
- Display

Internally accessible

- USB
- SATA/M.2
- PCI-e

Hardware security features (XMS Edge only)

Data stored on the device is protected via hard disk encryption. Protection of the boot stage is a responsibility of the customer and depending on their internal security policies the below security recommendation should be taken into account:

Security recommendation: Locate the XMS Edge hardware appliance in a secured and managed environment (e.g. the datacenter of a company).

Security recommendation: Disable USB boot in the BIOS and protect the BIOS with a strong password.

Shared Responsibility Model

Security is a shared responsibility between Barco and the customer. The complete end-to-end security of communication, infrastructure, data and business flow can only be ensured through a series of actions and responsibilities owned by both parties. In short Barco is responsible for the security of the application, while the customer is responsible for security in the application. The following matrix tries to outline the shared responsibility model between Barco and its customer.

Responsibility	Owner	
XMS Cloud		
	Customer	**Barco**
Install latest ClickShare/wePresent Base Unit firmwares	**X**	
User management (registration, removal, review)	**X**	
Role management	**X**	
Monitoring audit logs	**X**	
Secure access to web portal (browser security, …)	**X**	
Protection of credentials	**X**	
Evaluate and implement security recommendations	**X**	
Adhere to company's internal policies regarding uploading data to XMS (e.g. information in wallpapers)	**X**	
Securing data in motion, server-side encryption, maintaining data integrity		**X**
Customer data & other information assets		**X**
Platform and application updates		**X**
Provide secure and timely ClickShare/wePresent Base Unit firmware updates		**X**
Backup and restore data		**X**
XMS (Virtual) Edge		
	Customer	**Barco**
Protection of the BIOS	**X**	
Protection of credentials	**X**	
Secure physical location *(XMS Edge only)*	**X**	
Install XMS (Virtual) Edge updates	**X**	
Provide secure and timely XMS (Virtual) Edge updates		**X**
Provide secure and timely ClickShare/wePresent Base Unit firmware updates		**X**

Product Security Incident Response

As a global technology leader, Barco is committed to deliver secure solutions and services to our customers, while protecting Barco's intellectual property. When product security concerns are received, the product security incident response process will be triggered immediately. To address specific security concerns or to report security issues with Barco products, please inform us via contact details mentioned on https://www.barco.com/psirt. To protect our customers, Barco does not publicly disclose or confirm security vulnerabilities until Barco has conducted an analysis of the product and issued fixes and/or mitigations.

Closing

XMS Cloud and XMS (Virtual) Edge were designed with security in mind during all stages of the Software Development Lifecycle. We hope this security whitepaper was able to provide the information you were looking for. If any questions might have been left unanswered, please let us know via clickshare@barco.com. For specific application support, please contact Barco Support via https://www.barco.com/support.