SECURITY INFORMATION
for Pharos Cloud

SUMMARY

- Devices that are connecting with Pharos Cloud will only tunnel out via port over HTTPS via port 443
- All data is encrypted during transit and at rest
- No inbound connection is required, no ports to be opened
- Granular user permissions
- Optional to enable mandatory 2 factor authentication

ABOUT PHAROS AND SIXEYE

Pharos has been making ground-breaking lighting control solutions, that are both reliable and robust, for the best part of two decades. Designed and manufactured in-house, our multi award-winning products are trusted to run day and night, illuminating iconic installations around the world.
SixEye is a sister company to Pharos, and created as a manufacturer independent company that provides remote management of devices in the lighting and AV world. Using industry standard security to ensure this solution can be trusted in any environment has been at the heart of our development.
Pharos has embraced the SixEye technology to deliver the Pharos Cloud solution.

WHY CONSIDER PHAROS CLOUD

The reasons to support remote management are among others

- Decreased downtime
- Improved service levels
- Reduced travel time (including environmental benefits and reduced time and costs)
- Allow remote control of an installation by multiple users managed by granular permissions

NETWORK SECURITY

SixEye technology has been created with security in mind, and we are confident that using our technology will not put your network at risk. Our system allows devices with the SixEye SDK communicate with our cloud based back-end, and share status information. The tunnel between the device and our back end allows relevant actions to be run specifically on that device, or allow a device to pull in new firmware or configuration settings.

Does Pharos Cloud expose my network.

No. The SixEye technology will only establish communication between the specific device(s) that includes the SixEye SDK, and our back end. User cannot get access to your network. The devices that include our SDK will only support the features and files supported by the manufacturer of that device. For example, a lighting controller will only support its proprietary firmware and project files and cannot be loaded with generic scripts or executables.

What connectivity do devices require?

Devices need a valid gateway IP address with Internet access and **a DNS server IP address** – just like any computer needs to access the Internet. Devices make secure outbound connections to remote servers using TLSv1.2. To perform its initial authentication, a device must make a handful of short-lived connections to AWS servers in London, UK. Once authentication is complete, the device creates and holds one TLS connection to an AWS server in London, UK, allowing 2-way communication with the device.
For reference, the list of addresses the device will need to access:

1) a33z5x8196i4vy-ats.iot.eu-west-2.amazonaws.com
2) sixeye-firmware-files-production.s3.eu-west-2.amazonaws.com
3) sixeye-file-uploads-production.s3.eu-west-2.amazonaws.com
4) cognito-idp.eu-west-2.amazonaws.com
5) cognito-identity.eu-west-2.amazonaws.com
6) primary.sixeye-api.com
7) dl.pharoscontrols.com (only required for accessing Pharos Controls Remote Device Firmware files)

Please note that the URLs listed above are accurate at time of publishing, during ongoing development some of these may be retired or new additions may be made. We're unable to provide specific IP addresses for these services as the systems we use rely on dynamic IP addressing for load balancing purposes.

In all cases, HTTPS is used – the connection is to port 443 on the remote server. All other connections are closed. No inbound connections are required. In fact, **we'd recommend that all inbound connections are blocked** by a properly configured firewall.

Does Pharos Cloud support encryption of data in motion?

Yes. Encryption for data in motion is always on and cannot be disabled. We use HTTPS, which is to say that all connections are made to port 443 on remote servers, using TLSv1.2. This applies both to connections made by devices and connections to our API server from any web client.

I don't want 'AV Data' on my network

We agree that keeping your audio / lighting / video network data separate from other traffic is good practice. Configuring your AV network with a dedicated VLAN, or using an additional router to connect the AV network to your company network is recommended. As mentioned earlier, there only needs to be an outbound connection. A router can be configured to block all AV protocols, all incoming data and only allow outbound internet traffic via port 443.

Isn’t it easier if a mobile modem is used?

The solution is designed to be very light weight and robust, and works well over 3G, 4G and 5G connections, making this a viable option. A separate modem will need additional subscription, monitoring, and configuration.
For an IT professional, we would advise to support supporting compatible devices on your network, and see that as a lower risk then allowing a by 3rds configured router on your premises.

What is the internet usage of these devices?

Because our back-end knows about devices that can connect, limited data is needed to update values. The SDK on the device will only send data changes, keeping the data usage to an absolute minimum. As guideline a device being interacted with a reasonable amount uses approximately 2-5KB/minute, or roughly 250Mb/month per device.
File transfers (firmware, project files or content) will be responsible for the most data usage. File size and frequency of transfer having the largest impact. File transfers in SixEye are extremely stable, and will continue partial transfers on a restored connection, preventing unnecessary data use.

USER ACCESS

So I can securely connect a device with SixEye technology on my network to connect to Pharos Cloud. But how is the data it shares with the cloud protected and securely accessed?

How is the data in the back end accessed?

The SixEye backend offers a multi-tenant web API. An integrator can become a tenant who gets access to their data via their own portal. An integrators portal can be branded and can be accessed from their own domain using DNS routing.
Connections from the webclient to our backend are TLSv1.2 encrypted over HTTPS.
A portal provided via Pharos Cloud using SixEye technology can be recognized via the ‘powered by SixEye’ at the right bottom of each page, and an Amazon issued certificate pointing to https://sixeye.live.

Each Portal contains ‘Sites’ which contain one or more ‘Devices’, usually one device per physical device on a project.

How can users get access to connected devices?

Access to a site is granted on invitation via email only.
Users are invited to a ‘Site’ and can be given access to see specific devices in a Site. Other features, from viewing the Control Panel, to executing a Task or rebooting a Device are all provided with their own permissions.
Site owners set permissions of their Site or can grant other users the ability to set specific

permissions.
Users will only see and be able to access the Sites they are invited to.

Do you support Single Sign-on (SSO)

We are working to implement Microsoft 365 SSO, contact us for the current status.

Can you use 2 factor authentication

Each user can optionally turn on 2 factory authentication for their account, based on Time-Based One Time Password (TOTP), using apps like Google Authenticator or LastPass Authenticator. At request of a Portal Owner, Pharos/SixEye can be made mandatory for all users in a Portal to use 2FA.

Portal admins, or users that have received the relevant permission from the Portal admins, will be able to reset the 2FA key for a given user in the Portal.

What about multiple sessions and automatic logout?

Pharos Cloud does allow a user to log in from multiple devices; the nature of the application will sometimes require this. A user that has no activity will be logged out after 7 days.

Are there ‘admins’ that have access too?

At portal level, one or more ‘Portal Admins’ (typically employees of the Portal Owner) can be assigned by Pharos at the request of the Portal Owner. A portal admin can view all Sites and grant themselves access to a Site. At the Pharos / SixEye level there are limited ‘Super Admins’ that can, on request of the integrator, provide themselves access. All activity is logged, see below.

How is a device connected to a specific site?

From a Site a Key is created (max 7 days validity) which is copied onto the device. (The device manufacturer will have provided a way to transfer this key to the device, via its usual configuration application or similar.) This Key contains a set of temporary credentials for the device to connect and contains information for the device to know which Site to connect too. Once the first connection is completed the Key becomes invalid and cannot be used to connect any other devices.

Is data encrypted at rest?

Data in the SixEye database is encrypted using AES-256.

What protection mechanisms are in place?

Any client consuming our API, such as a SixEye-powered portal, creates a TLS connection to a load balancer. We have an AWS VPC (Virtual Private Cloud) for the application servers, with no public access. AWS Shield provides DoS protection. Devices verify the server’s certificate during the TLS handshake to ensure an attacker cannot eavesdrop on communications.

What type of logging is in place for data access?

We log access to infrastructure components – the load balancer, servers & database. We log application errors, events and operations performed by users.

Logging of all activity within a Site is visible for Site owners.

Who owns the data?

Data provided by users of a tenant is owned by the tenant. Data pushed by a device is owned by the manufacturer of the device.

How is data backed up, and can it be restored / recovered?

SixEye has a rolling 7-day backup.

How is data segregated between tenants?

Tenant data is segregated into separate database schemas, with access restricted to users of the initiating tenant. This extends to user data, project data, permissions, etc. Devices are slightly different – the use of devices in a particular project is segregated into separate schemas by tenant; some of the status information pushed by a device is outside tenant scope for the benefit of the manufacturers.

What practices do you follow to identify vulnerabilities that may be present in source code used in the SixEye platform?

- Keeping track of library version dependencies.
- Upgrading libraries early.
- Preferring in-house solution from unknown libraries.
- Automatic tests.
- Test coverage analysis tools.
- Code reviews for every commit.
- Duplicated test environments before release.

Are there browser recommendations for best performance?

The SixEye web app is built using standard web technologies and doesn't require any extensions or plug-ins. A modern web browser for Desktop (e.g.: Firefox 62.0.3+, Chrome 70.0.3538.67+, Edge 44.17763.1.0+ or Safari 10.1+) or mobile (Safari 10.3+, Chrome 70.0.3538.64+) will do. A 3G Internet connection or better is advised. File transfer performance will be faster with higher bandwidth.

For any other questions please contact your integrator, or Pharos via support@pharoscontrols.com