Constantly improving product protection and security

IT environments continue to evolve at a rapid pace, the volume and severity of the potential security threats are ever increasing whilst also becoming more sophisticated and intelligent.

To tackle this problem, a combined holistic approach is required from the industry, starting with the vendors within it leading the way, right through to the end users, deploying the security products and associated network services. The defence against this growing threat will be the right mix of technology, processes, and people.

At Oncam, we keep the importance of physical and cyber security at the forefront during the inception, design, development, testing and maintenance phases of our products and services to minimise the number of potential areas that could be exploited in an attack. We are leading security innovation and providing guidance on best practice, a robust and efficient response to security threats and ongoing threat monitoring, and we are committed to supporting your security needs and those of the whole industry.

These principles have under-pinned the development of the C-Series Cameras and every effort has been made to minimise security risks and address current and potential security threats to the end user.

C-Series cameras have several security features enabled by default to ensure they secure out of the box, whilst more advanced features such as "IP Address Filtering" are user controlled and offer higher levels of protection against potential attacks.

Our firmware is common and updated across our entire C-Series range and we are constantly developing and hardening it with the latest security, to the benefit of current and future products.

SECURE CONFIGURATION

Every effort is made to ensure the product is secure on your network as standard, but we nonetheless recommend enabling and configuring all available security measures. Essentially, these steps involve protecting and controlling access to the camera on the network. We have deployed several measures and features to protect this access:

- **Secure Bootup:** The initial bootup process checks and verifies that the firmware installed on the camera is authorised and signed before proceeding, to ensure only verified firmware is deployed.
- **Secure Password**: During first time access, default user passwords are not supported, Users will be required to set a secure password, which will need to meet a minimum length using a combination of upper- and lower-case letters, numbers and special characters.
- **Secure Authentication:** WS-Username Token and HTTP Digest Authentication are supported to ensure clients access the camera over the network with a hashed password, protecting it from network sniffer attacks. We recommend using HTTPS to ensure network traffic is encrypted.
- **Brute force protection:** Restrictions are in place as part of the authentication process to slowdown the camera's response when multiple incorrect credentials are used to access it, to ensure prevention against automated attacks aimed at guessing the password. Users can also set the maximum number of connection attempts per minute to further restrict access to the camera.

- **User authorization levels**: Three-tiered user levels; Admin, Operator and User are supported to control and restrict access to the camera, its configuration and advanced features.
- **Secured Firmware:** All firmware is digitally signed and authorized by Oncam. During the firmware update process, the camera will check for a digital signature on the firmware and only proceed if it is verified. This prevents tampered firmware that could compromise the camera from being installed.
- **Support Logs**: The camera gathers essential log information during daily operation which can be helpful in support enquiries. As the information can be sensitive it is encrypted, and the downloaded log file can only be viewed by the Oncam Support Team.
- **Access Logs:** Details of the last client to access the camera are available including username, date, time and access level.

The following advanced access features can be applied by the user for additional security:

- **Communication Protocols:** HTTP and HTTPS are both enabled by default. HTTP can be turned off to ensure a secure connection between camera and the client over HTTPS. HTTPS uses TLS, which ensures communication to the camera is encrypted and protected.
- **Secure Certificates:** When using HTTPS, we also recommend downloading the Oncam Certificate into your client work station to ensure communication remains secure from end to end.
- **IP address restrictions:** Create a filter to control which clients can access the camera by allowing or declining access to specified IP addresses only. A Whitelist ensures only listed IP addresses can connect to the camera, alternatively create a blacklist to deny access to listed IP addresses.

SECURE PRODUCTION

C-Series Cameras are manufactured in a secure facility with access control and full auditing. We assure integrity over the complete supply chain, with regular auditing of our suppliers to ensure our high standards are maintained. Products are checked and tested according to our quality standards prior to shipping. All Firmware on the camera is only built and signed by the Oncam engineering team based in the UK.

SECURE PROCESS

At Oncam we have a robust and efficient response in place to manage security threats, this is supported by ongoing threat monitoring as part of our development process. We work closely with our strategic partners to identify and resolve any security issues in a timely manner. As part of our security monitoring activity, the vulnerability scans deployed are constantly updated and are an integral part of our release process.

.

Oncam Global Ltd |6th Floor, 2 London Wall Place | London EC2Y 5AU | United Kingdom
oncamgrandeye.com | +44 (0)20 7371 6640 | info@oncamgrandeye.com