



DIGIFORT CYBER PROTECTED GUIDE



Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from cyber attacks. Effective cyber security reduces the risk of cyber attacks, and protects organisations and individuals from the unauthorised exploitation of systems, networks and technologies.

HERE ARE THE CYBER SECURITY FEATURES WE HAVE IN DIGIFORT



- ▶ Every other password that is required by Digifort is also stored encrypted on the server so even if the configuration from the server is retrieved, the authentication keys are safe.



- ▶ Every other password that is required by Digifort is also stored encrypted on the server so even if the configuration from the server is retrieved, the authentication keys are safe.



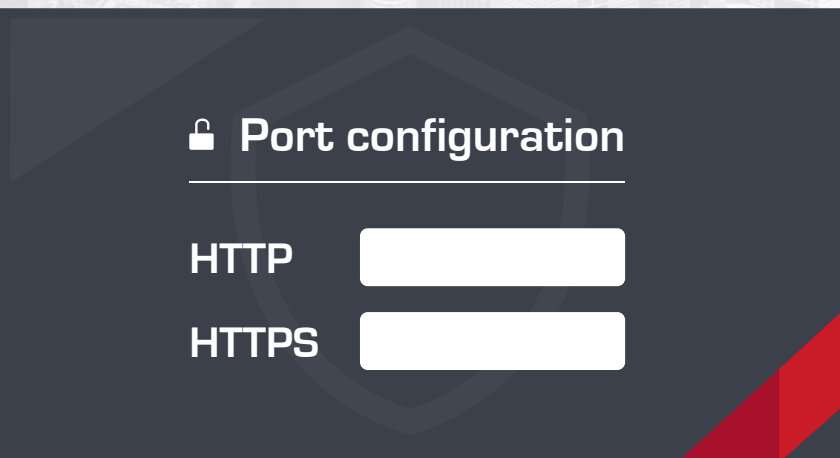
- ▶ All user passwords are stored encrypted on the server.
-



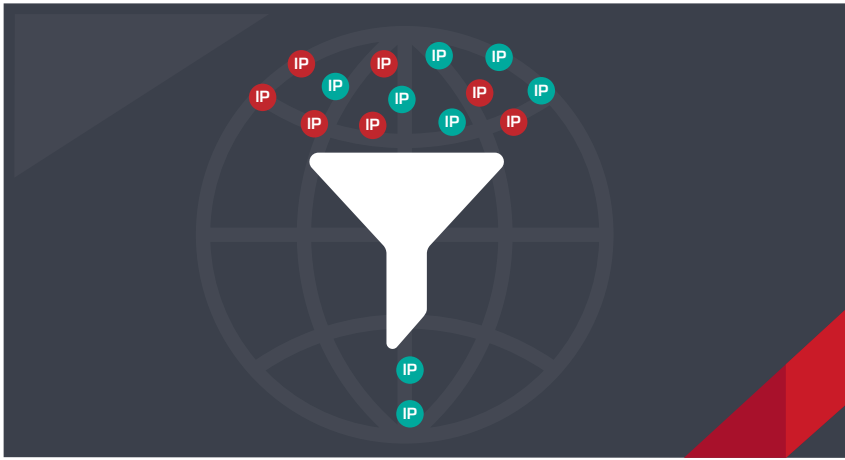
- ▶ All camera passwords are stored encrypted on the server.
-



- ▶ The system has the option to block the user account if the password is wrong (after X tries, configurable by the admin).
-



- ▶ Default ports can be changed (For example HTTP, HTTPS, RTSP), to obscure the open ports for a potential attacker (if the server is open on the internet).
-



- ▶ Global IP filtering. Provides a list of the range of IPs that can access and range of IPs that can't access the server.
-



- ▶ The API and HTTP server supports HTTPS.
-



- ▶ User-specific IP filtering. Provide a list of IPs from where a specified user can access. With user specific IP filtering, a given user can only access the system from a given IP address or the range of IP addresses, protecting their user account since it cannot be used to be accessed from any computer.
-



- ▶ Login times for users. This option allows the creation of a schedule to specify the times of when a given user can log in to the system, preventing unauthorized access at unauthorized times.
-



- ▶ Auto expiry setup for temporary users.
-



- ▶ Use digest authentication to cameras
-



- ▶ Force encryption on exported video
-















- ▶ SSL/TLS for Server to Native Clients communication (7.3)
-







- ▶ SSL/TLS for new Web Server (7.3)
-

TIPS

NETWORK LAYER







-  Buy from reliable sources and brands
-  Firewall
-  Not use default IP ports
-  Separate IT network from IP Surveillance network
-  Use VLAN's
-  Use MAC address filters to lock down your network
-  Avoid Cloud based services
-  Avoid remote accessing from public WiFi
-  Disable common access on switches
-  Create unique subnet and IP address range for CCTV
-  Use domain(s)
-  Use VPN for remote users

SOFTWARE LAYER

-  Use anti-virus
-  Update frequently
-  Force strong password policies
-  Use certificates if possible

END-POINTS

(Cameras, I/O devices, etc)

-  Use strong passwords, delete default password !
-  Change default ports
-  Different password for every device
-  Use HTTPS (SSL certificate)
-  Switch off discovery services such as uPNP
-  Install on physically separated network as the rest of the network

“

The cyber security is also subject to the different network security policy levels using different layers of authentication and protections. Digifort works seamlessly with such secured network environment.

Digifort requiring a limited number of ports to open, it further limits the risk of random cyber attacks.



 DIGIFORT GLOBAL
 DIGIFORT GLOBAL
 WWW.DIGIFORT.COM

Asia, Pacific, Europe, Middle East
Suite 403, Level 4, 79-77 Parramatta Road
Lidcombe NSW 2141
Ph +61 2 9748 6869
info@digifort.com

Americas
Rua Teffe, 334, - Santa Maria
Sao Caetano do Sul - SP, Brazil
+55 11 4226 2386
contato@digifort.com.br

