



# **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.

“

*The security industry has taken notice of Cyber Security.*

*The only way forward is teamwork and making sure each participant in the security chain plays their role to ensure the most secure solution.*



## AES256 (ADVANCED ENCRYPTION STANDARD)

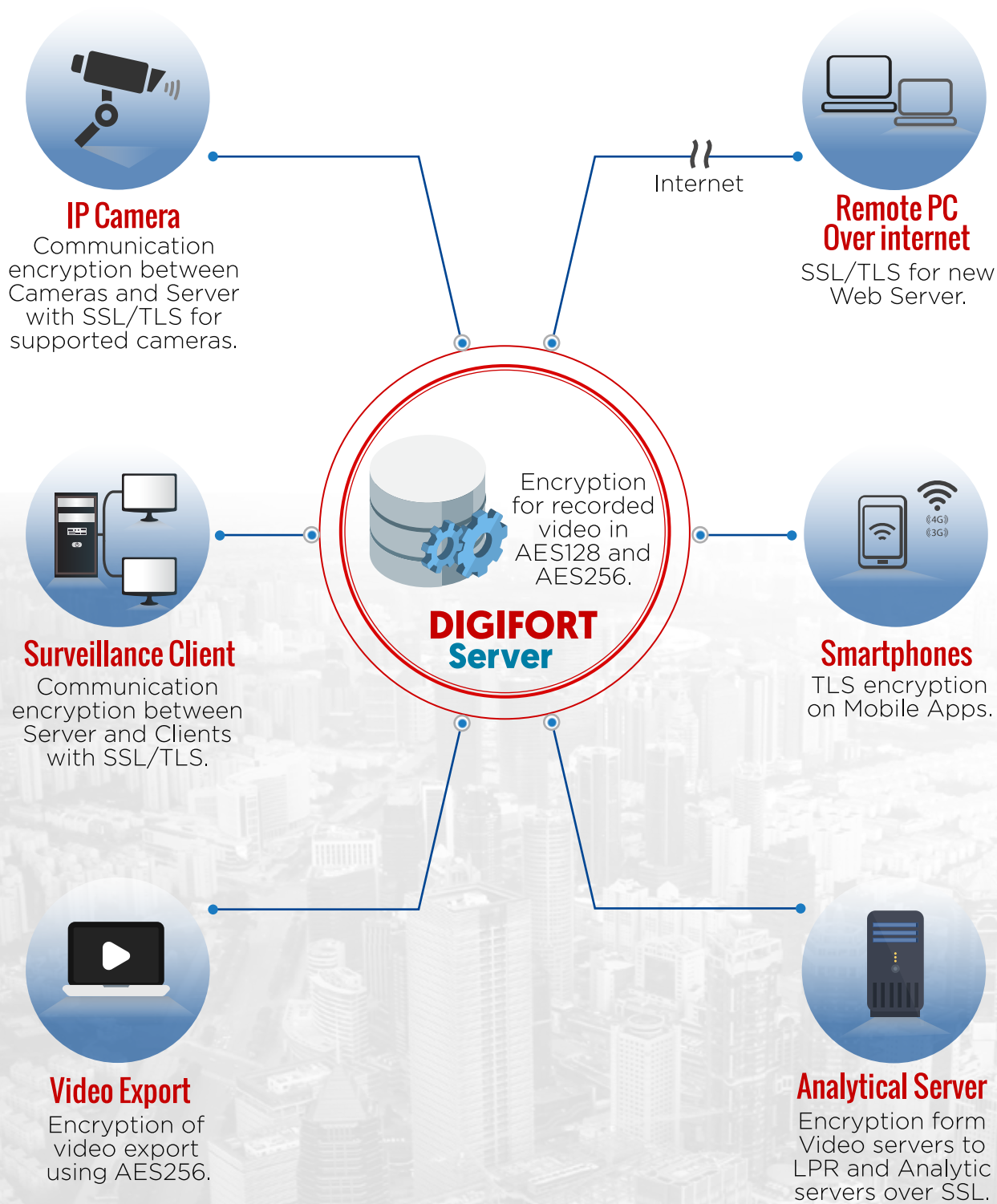
AES256-bit encryption is a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files. It is one of the most secure encryption method.

SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two system.

TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions.



# DIGIFORT CYBER SECURITY AT A GLANCE





# HERE ARE THE CYBER SECURITY FEATURES WE HAVE IN DIGIFORT

---



- ▶ If the connection is unsecure, user authentication in the system (between client and server) is one-way encrypted and cannot be discovered by network sniffing. The transferred data cannot be reversed (to find out the password). This is similar to the very secure HTTP Digest authentication."

- ▶ 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.



- ▶ 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.





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



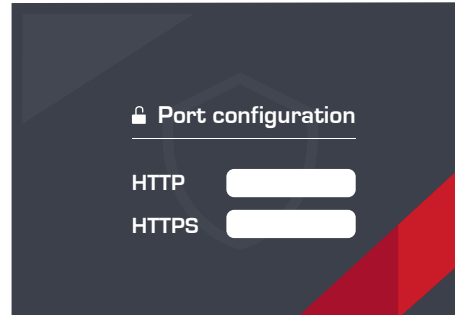
- ▶ All camera passwords are stored encrypted on the server.



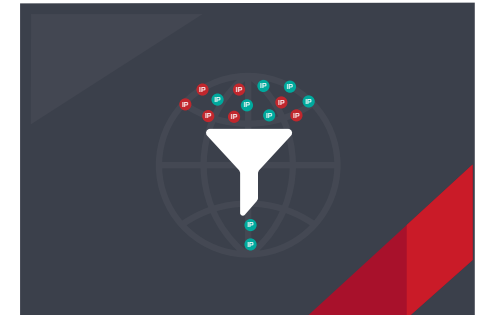
- ▶ Auto expiry setup for temporary users.



- ▶ 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.



- ▶ Use digest authentication to cameras.



- ▶ SSL encryption on Mobile Apps.





- ▶ SSL/TLS for Server to Native Clients communication.



- ▶ SSL/TLS for Webservers.



- ▶ Recorded video encryption with AES128 & AES256.



- ▶ Encryption from Video to LPR & Analytical servers using SSL.



- ▶ Encryption of video export using AES256.



- ▶ Force password protection on exported video.



- ▶ 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.



- ▶ Encryption between cameras and server with SSL/TLS for supported cameras.

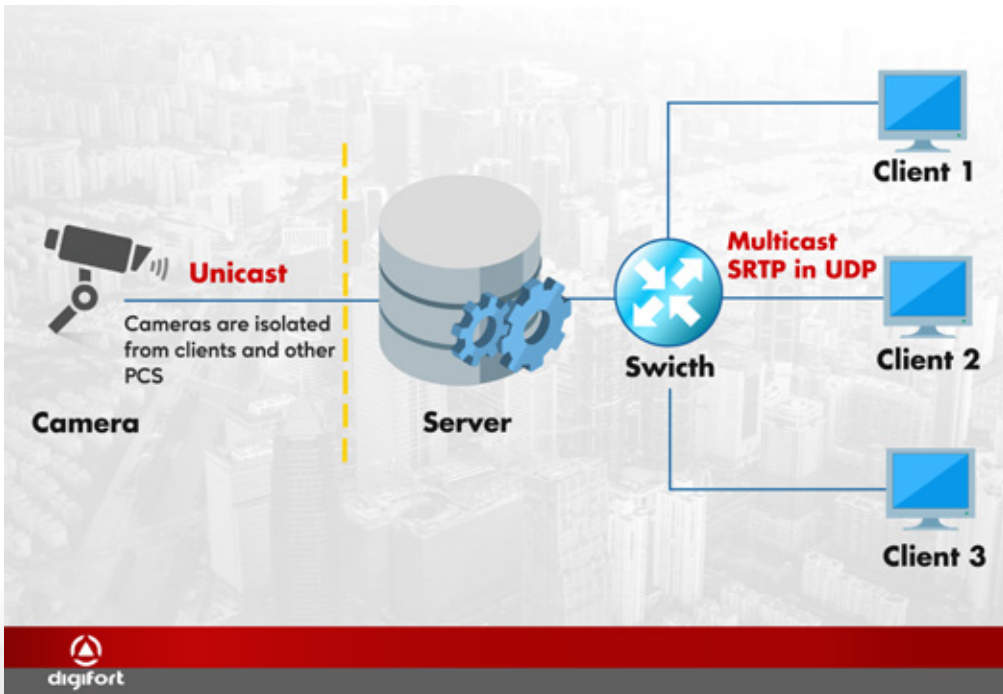






- Support for two-factor authentication, with one-time password token provided by 2fa apps like Google authenticator.

This ensures an even higher level of security in accessing secure and private data.



- SRTP (Secure Real-Time Transport Protocol). It is a protocol to encrypt video and audio.

From server to client Digifort now support SRTP in Multicast (UDP).

This ensures a true end to end encryption

- Encryption from cameras to server in TCP using SSL/TLS.
- Server to clients in unicast with encryption via SSL/TLS or multicast with SRTP encryption in UDP.

### ► **Note:**

#### **Multicasting from Cameras to Server**

The camera will send 1 stream into the network, accessible by everyone (server and clients). This is fine, as it reduces bandwidth.

However, it leaves the camera open in the network, so clients can receive multicast data, leaving it vulnerable to attacks and hacker to try and take down a camera to make it stop recording.

Servers, on the other hand, are much harder to take down.

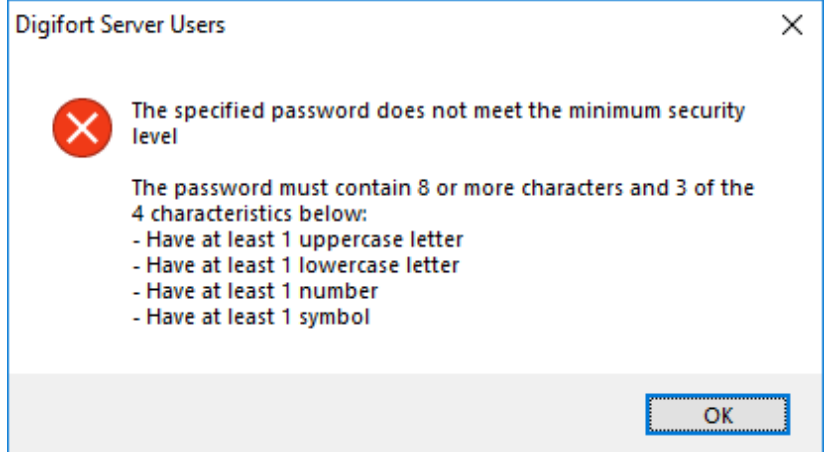
Digifort, in our architecture, cameras are isolated, on a separated LAN or VLAN that only the server can access, not by clients or any other computers, so cameras are protected against any attacks.





# UPDATE YOUR WEAK PASSWORD

We have the option to enforce strong password for users. The system can also force the user to update a previous weak password. For strong passwords the following rules apply :















Besides all security features implemented in the system, the environment also must be protected:

- ✓ Disabling of unused protocols and services (For example, disable RTSP server, disable HTTP server if they are not used)
- ✓ Use VLANs
- ✓ Prevent physical access to the servers







# 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
-  When using public WiFi make sure to always use connection encryption
-  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.*



**Asia, Pacific, Europe, Middle East**

Suite 403, Level 4, 79-77 Parramatta Road  
Lidcombe NSW 2141  
Ph +61 2 9748 6869  
[info@digifort.com](mailto:info@digifort.com)

**Americas**

Rua Teffe, 334, - Santa Maria  
Sao Caetano do Sul - SP, Brazil  
+55 11 4226 2386  
[contato@digifort.com.br](mailto:contato@digifort.com.br)

