# uniview

### Better Security, Better World.

# OTHER TUTORIALS



## UNIVIEW SECURITY

#### SECURITY BREFING

Security should be your number one priority with your surveillance system. Recently in the surveillance industry some manufactures have not been providing enough security features for users to use, this has been resulting in hacked devices and stolen networks. Devices that have been accessed can also be used in DDoS attacks to bring networks down completely.

Uniview has an extensive list of features that can be utilized to greatly improve security of their surveillance devices. Here we will go over the 3 most secure features that are offered.

TELNET DISABLE ABILITY							
uniview		📮 Live View	III Playback	ŧ Settings			
Client	*	IP Control	HTTPS		ONVIF Auth	Telnet	ARP Protection
System	~						
Basic		Telnet	⊖On ⊚Off				
Preview		Save					
Time							
DST							
Holiday							
Security							

The first main security feature is the ability to turn Telnet on and off. All recorders and cameras come with telnet off by default. When Telnet is off no connections via telnet will be able to be made to the device.



Once Telnet is turned on the device will then allow Telnet connections. The Telnet login username and passwords are secured and only know by Uniview and their direct partners. This information is not available online or given to installers.

uniview		🖳 Live View 🛛	III Playback	🌣 Settings			
Client	~	IP Control	HTTPS		ONVIF Auth	Telnet	ARP Protection
System	~						
Basic		Telnet	● On ○ Off				
Preview		Save					
Time		ourc					
DST		Telnet 192.168.1.1	167		- 0 X		
Holiday		1			^		
Security		LOBIUL -					
Camera	~						

								_
WHITELIST								
uniview		📮 Live View	🅅 Playback 🏟 Settings					ogou
_								
Client	$\otimes$	IP Control	HTTPS	ONVIF Auth	Telnet	ARP Protection		
System	*							
Basic		IP Control	P Control Off ○Blacklist @Whitelist					
Preview		Start IP:	IP:					
Time		End IP:						
DST								
Holiday		Add						
Security		No.	Start IP	End IP		Edit	Delete	
Camera	8	1	192.168.1.100	192.168.1.11	5	Ø	<b></b>	
VCA		2	50.193.145.82	50.193.145.8	2	Ø	曲	
VCA	~							

The second main security feature is Whitelisting of IP address. Users can Whitelist local network IP address and External IP address. Once Whitelisting is turned on and IP address ranges are set users on a device with and IP address that is not Whitelisted will not be able to login, they will receive a "The user does not have permission"

uniview	
The	user does not have permission.
Username	
Password	
	Login Reset

#### WEB ACCESS VIA STRONG PASSWORD

Weak password. Please reset before accessing via Internet.

The third top offered security feature is not being able to access a recorder or camera via a remote access web browser if the password of the device is default or considered "weak". The device will allow access via a local (LAN) web browser and prompt the user that the password is weak and that it will need to be changed before accessing via the internet.

If a user does not changed the password to a "Strong" password before accessing via a remote network the device will deny access to the device and prompt the user to go to the local area network and change the device password.