

Title:	PAN Wi-Fi Camera Security	Version:	Date:	11/29/17
Product:	Hikvision Wi-Fi Cameras		Page:	1 of 5
Action Required:	Upgrade to latest firmware posted, as required			

Summary

It is always a cybersecurity best practice to disable any features that you are not using. If you have a Hikvision Wi-Fi camera and are managing that camera using an Ethernet cable rather than Wi-Fi, it is recommended that you disable the Wi-Fi function (see "Disabling Wi-Fi," below).

NOTE: Under certain conditions, a threat actor could potentially establish Wi-Fi connections with Hikvision Wi-Fi cameras that are being managed with a wired Ethernet connection.

If you are using Wi-Fi, this document explains how to enable data encryption for the camera for heightened security (see "Enabling Wi-Fi Data Encryption," below).

Details

For the threat actor to establish a Wi-Fi connection, they would have to be within Wi-Fi range and set up a Wi-Fi access point (AP) with the default SSID of "davinci."

In a hypothetical situation where a threat actor successfully establishes a Wi-Fi connection, the connection would not give the attacker privileged access or access to the device interface and video feed. Privileged access and access to the device interface and video feed would still need to be gained through proper authentication.

While this finding does not constitute a vulnerability, it does increase the attack surface. It is another reminder to all those who own or manage Hikvision Wi-Fi cameras to ensure that they are running the latest firmware.

Hikvision believes education and outreach are of paramount importance in an effective cybersecurity program, and it recognizes the important role that security researchers play in our ongoing cybersecurity efforts.

Recommended Actions

As always, Hikvision highly recommends that users ensure they are using the most updated firmware for all Hikvision devices, including Wi-Fi cameras.

 DS-2CD2xx2FWD-IW(S) Cameras (DS-2CD2522FWD-IWS, DS-2CD2542FWD-IWS, DS-2CD2422FWD-IW, DS-2CD2442FWD-IW)

All firmware after version 5.4.0 for these cameras allows for disabling the Wi-Fi interface. Factory default is "Enabled."

DS-2CD2xx2-IW(S) Cameras

 (DS-2CD2112F-IWS, DS-2CD2132F-IWS, DS-2CD2412-IW, DS-2CD2432F-IW)

PRODUCT ADVISORY NOTICE



Title:	PAN Wi-Fi Camera Security	Version:	Date:	11/29/17
Product:	Hikvision Wi-Fi Cameras		Page:	2 of 5
Action Required:	Upgrade to latest firmware posted, as required			

Use the following link to download special firmware that can turn off the Wi-Fi function for these cameras.

ftp://hikfirmware:T3C\$18639Hik@ftp.hikvisionusa.com/Hikvision IP Camera Firmware/Raptor 2xxx Series/ Value%20Series/DZ20170605 048 R0 EN STD WiFi Setting 5.4.5 170718.zip

Disabling Wi-Fi

To disable Wi-Fi on a Hikvision Wi-Fi camera (DS-2CD2xx2FWD-IW(S) w/firmware v5.4.0 or later) or (DS-2CD2xx2-IW(S) w/firmware v5.4.5), perform the following steps:

- 1. Log on to your system through your NVR or a Web browser.
- 2. Go to Configuration > Network > Advanced Settings > Wi-Fi.
- 3. Uncheck the Enable checkbox.
- 4. Click Save.

Н	KVISION	Live	View		Playba	ick	Pict	ture	Conf	guration					
Ģ	Local	SI	IMP	FTP	Email	Platform	Access	HTTPS	QoS	Wi-Fi	Integration Proto	col			
	System	(🗌 Enab	ole											
G	Network		Wireless List								Search				
	Basic Settings		No.		SSID		Workin	ng Mode	Secur	ity Mode	Channel	Signal Strength	Speed(Mbps)	Connection Status	
	Advanced Settings		1		Technol	ogy	Mai	nage	not-er	ncrypted	3	96	150	Disconnected	~
Q.	Video/Audio		2		HIK-Gu	est	Mai	nage	WPA2	personal	1	80	150	Disconnected	
1	Image		3		Hik-Offi	се	Ma	nage	WPA2	personal	1	77	150	Disconnected	

Figure 1, Configuration > Network > Advanced Settings > Wi-Fi Page "Enable" Checkbox



Title:	PAN Wi-Fi Camera Security	Version:	Date:	11/29/17
Product:	Hikvision Wi-Fi Cameras	Page:	3 of 5	
Action Required:	Upgrade to latest firmware posted, as required			

Enabling Wi-Fi Data Encryption

Hikvision strongly recommends enabling data encryption when using its Wi-Fi cameras over Wi-Fi. The following steps explain how to enable data encryption. Factory default is "Not-Encrypted."

- 1. Log on to your system through your NVR or a Web browser.
- 2. Go to Configuration > Network > Advanced Settings > Wi-Fi.
- 3. Configure the Wi-Fi settings with the following values (refer to figure on next page):
 - **1 Enable:** Check this checkbox to enable Wi-Fi.
 - 2 Wireless List (Read Only): This list displays all of the Wi-Fi cameras in the system.
 - **3 SSID:** Input **davinci** (default).

NOTE: We recommend changing the default SSID to one of your choosing.

- 4 Network Mode (Read Only): This radio button is clicked (default).
- 5 Security Mode: Use pull-down menu to select WPA2-personal.
- 6 Encryption Type: Use pull-down menu to select AES.
- 7 **Key 1:** Input a large (12 characters minimum recommended) random string of upper case characters, lower case characters, numbers, and special characters.
- 8 Enable WPS: Uncheck this checkbox.
- 9 Save: Click to save settings when done.

PRODUCT ADVISORY NOTICE



-				
Title:	PAN Wi-Fi Camera Security	Version:	Date:	11/29/17
Product:	Hikvision Wi-Fi Cameras		Page:	4 of 5
Action Required:	Upgrade to latest firmware posted, as required			

HI	KVISION	Live	Live View Playback Picture		Configura	ation							
	local	s	NMP	FTP Email	Platform	Access HTTPS	QoS \	Vi-Fi	Integration Proto	col			
	System	(1)	Enab	le									
6	Network		Wisels	an Lint								Coorch	1
V	Basic Settings		Wirele	ess List	`	Working Mode	Security M	odo	Channel	Signal Strength	Speed(Mbps)	Connection Statu	
1	Advanced Settings		140.	331	,	Working Mode	Security W	Jue	Cildiniei	Signal Strength	Speed(mpps)	Connection Statu	10
Q.	Video/Audio		7	HIK-Gu	est	Manage	WPA2-pers	onal	6	72	150	Disconnected	^
	Image		8	HIK-MO	Dile	Manage	WPA2-pers	onal	0	72	150	Disconnected	
一	Event		9	Hik-Off	ice	Manage	WPA2-pers	onal	6	64	150	Disconnected	
	Storage		10	Hik-Warel		Manage	WPA2-pers	onal	6	62	150	Disconnected	11
	otolage		12	HIK-Gu	est	Manage	WPA2-pers	onal	6	60	150	Disconnected	
		(2)	13	Hik-Mo	bile	Manage	WPA2-pers	onal	6	60	150	Disconnected	
			14	The Wal	12.4	Manage	WPA2-pers	onal	2	59	150	Disconnected	
			15	Yotri	D	Manage	WPA2-pers	onal	1	44	150	Disconnected	
			16	NVR5221	37089	Manage	WPA2-pers	onal	1	43	150	Disconnected	
			17	Yotrio M	obile	Manage	WPA2-pers	onal	1	43	150	Disconnected	
			18	qwert	У	Manage	WPA2-pers	onal	1	43	150	Disconnected	~
			40	potaoor a	00014	Managa	MDA0 para	anal	0	47	450	Disconnected	
			Wi-Fi										
			SSID		davinci								
		4	Network	Mode	Manage								
			Security I	Node	wrAz-personal V								
			Encryptio	n Type									
		\cup	Key 1 🖲		8 to 63 ASCII characters or 8 to 64								
					hexadeci	mal characters							
			WPS										
		(8)	Enab	le WPS									
			PIN Code	9	123456	78	Gen	erate					
			PBC	connection	Connec	t							
			O Use r	outer PIN code	Connec	CT							
			SSID Bouter B	Nicodo	davinci								
			Nuller P	IN COUR									
		٣		≡ Save									

Figure 2, Configuration > Network > Advanced Settings > Wi-Fi Page Settings



Title:	PAN Wi-Fi Camera Security	Version:	Date:	11/29/17
Product:	Hikvision Wi-Fi Cameras		Page:	5 of 5
Action Required:	Upgrade to latest firmware posted, as required			

Resources

Links to the updated firmware, and many other cybersecurity resources, are available at the <u>Hikvision Security</u> <u>Center, http://www.hikvision.com/us/securitycenter_10636.html.</u>

Questions

If you have questions or concerns, please contact your Hikvision representative, or contact us at <u>support@hikvision.com</u>. In addition, Hikvision has launched a dedicated Cybersecurity Hotline that integrators, clients, and technology partners can reach directly by calling 626-723-2100.