



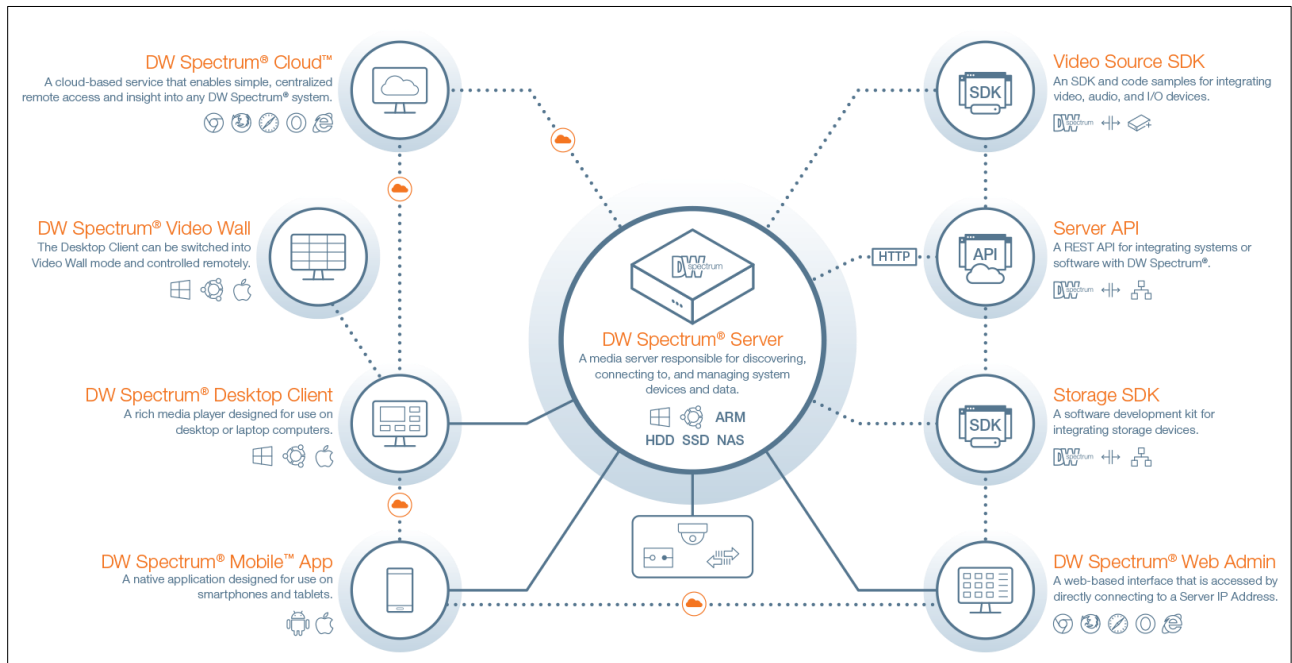
DW Spectrum FAQs and Security Review

Related Digital Watchdog VMS Apps: DW Spectrum IPVMS
Last Edit: September 20, 2024

DW Customer Questions

When shopping for a security hardware and software provider that works best with your budget and practical needs, customers will often have a long list of inquiries regarding our products and services. Primarily, these questions are focused on cyber security and privacy.

While every situation and deployment are unique, this document will provide you with answers to some of the questions that are most frequently asked by our customers and partners.



Frequently Asked Questions

1) Please describe the overall application.

DW Spectrum has a unique hive architecture where servers can automatically discover ONVIF-compliant devices. Administrators can manage users, monitor data, and observe security footage all from a single application.

Designed for scalability, “Owners” can merge multiple servers together into a single system, each with its own set of cameras, recording archives, and license keys.

For more details, you can refer to:

- [Working with DW Spectrum](#)

2) Please provide an overview of the security safeguards.

DW Spectrum is continuously being improved and updated to address cybersecurity threats by using a combination of secure technology and process countermeasures such as user access rights management, two-factor authentication (2FA), SSL certificates, encryption, and more.

For more details, you can refer to:

- [How Secure is DW Spectrum?](#)
- [Cyber Security and DW Spectrum](#)

3) Does DW Spectrum use secure communication protocols?

The short answer is yes. DW Spectrum uses encryption for system security using a Secure Socket Layer (SSL) to ensure that connections are authenticated and to prevent interception by unwanted parties.

However, we understand that our customers' needs differ and require varying levels of security. This is why Owners and Administrators have the option to enable or disable HTTPS encryption and other security configurations as needed.

For more details, you can refer to:

- [Using Encryption for System Security](#)

- [Encrypting Video Traffic](#)
- [Configuring Secure Connections](#)
- [Cyber Security and DW Spectrum](#)

4) What operating systems are DW Spectrum compatible with?

DW Spectrum is compatible with Windows, Ubuntu Linux, and Mac OS (Client only).

For more details and OS versions, please visit the [Downloads](#) page in the DW Cloud Web Portal.

5) What devices are DW Spectrum compatible with?

DW Spectrum primarily supports Digital Watchdog cameras and products, but it also supports cameras from a large variety of other manufacturers.

For more details, please visit the [Supported Devices](#) page in the DW Cloud Web Portal.

6) How Many devices does DW Spectrum support on a single server?

The answer to this question can vary depending on the hardware capabilities of the computer hardware that is hosting the program, as well as the network throughput of the devices. There is a recommended limit of no more than 128 video streams per DW Spectrum Server. This includes considering cameras that use dual-streaming technology and cameras that house more than one lens.

Digital Watchdog provides an online storage calculator to help customers determine the type of server model and cameras to deploy, while staying within the recommended safeguards.

For more details:

- [DW Rapid Review – DW IP Storage Calculator \(video\)](#)
- [DW IP Storage Calculator](#)
- [DW Spectrum IPVMS Maximum System Size](#)

7) How is DW Spectrum licensed?

DW Spectrum is free to install and use for live streaming camera footage to your desktop and mobile clients. However, to record video to the DW Spectrum Server's archive, unique recording licenses will need to be activated for your system.

Digital Watchdog does not hold customers hostage with a subscription service. License keys are unique and yours to own for life. All Digital Watchdog brand recording servers (DW Blackjack series) come with complimentary license keys. Additional license keys can also be purchased in packs of licenses keys of varying sizes from DW Sales representatives.

For more details, you can refer to:

- [DW Spectrum Licenses](#)
- [DW Spectrum – License Types](#)
- [DW Spectrum – Activating License Keys](#)

8) How often are new software versions released?

Digital Watchdog works closely with its software developers to ensure that our products are vigorously tested and confirmed stable prior to public release. These updates can include security updates, quality of life improvements, compatibility updates and bug fixes.

Major versions of the DW Spectrum software are typically released every 1 – 2 years.

Various build versions of the DW Spectrum software are typically released every 1 – 2 months.

For more details, you can refer to:

- [DW Spectrum Release Timeline & Release Notes](#)

9) How is DW Spectrum updated?

DW Spectrum offers one-click update options and can be configured to automatically download available updates over the Internet or can be manually prompted to download updates. However, DW Spectrum will not

force updates to install once downloaded. Confirmation by an Administrator is required to apply all updates to prevent the installation of an unwanted update. Once approved, the program will apply the update to all software components within your system.

For offline systems kept within a private network, Administrators can download and transport updates from a computer with Internet access using a USB storage device.

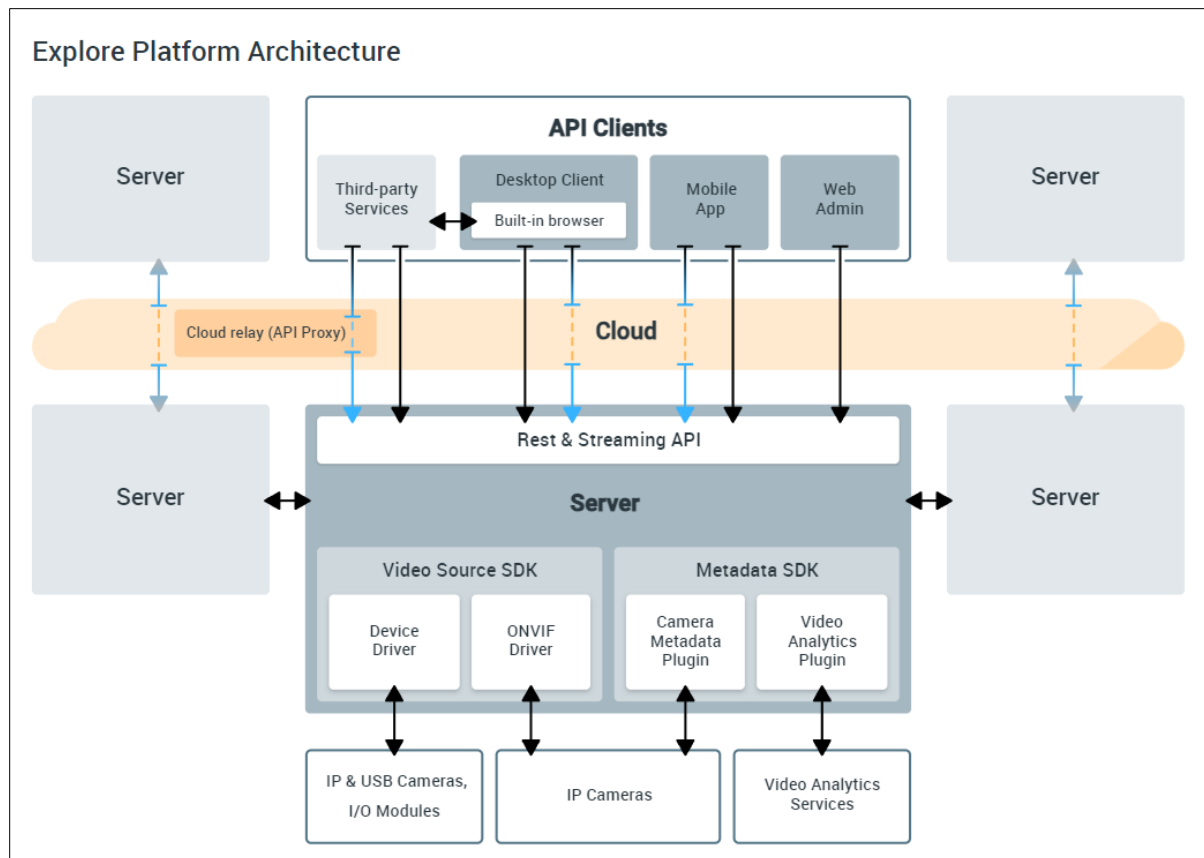
For more details, you can refer to:

- [DW Spectrum – Updating DW Spectrum Software](#)
- [DW Rapid Review - Updating DW Spectrum \(video\)](#)

10) How does DW Spectrum scale?

DW Spectrum allows multiple servers to work together within a single or more Systems. Individual servers within the same local network can be merged so that all components can constantly synchronize data and view video from any camera within your DW Spectrum System.

- [Configuring Multi-Server Environment](#)



11) Please describe your high availability approach.

DW Spectrum will automatically create a database backup of your system once every seven (7) days, when the software version is updated, and before a system merge. Administrators can also manually prompt a database backup at will.

Over time, the system will create up to six (6) database backups. Once the server has six (6) database backups, it will overwrite the oldest backup file. As a result, there will always be at least one backup database file available to restore your system.

Regarding video footage, Administrators can configure backup and redundant storage to ensure that select portions of the video archive remains available in preparation for the unforeseen event of a server going offline, hardware failure, or data corruption.

For more details, you can refer to:

- [Backing Up and Restoring the System Database](#)

- [DW Spectrum – Creating a Database Backup](#)
- [Configuring Server and NAS Storage](#)
 - [Configuring Backup and Redundant Storage](#)
 - [DW Spectrum – Redundant Storage](#)
 - [Background: Archive Distribution and Retention](#)
 - [Background: Archive Indexing](#)
 - [Background: Archive Backup](#)
- [Configuring Failover](#)
 - [DW Spectrum – Automatic Camera Failover](#)

12) Does DW Spectrum provide system activity logs?

DW Spectrum will automatically create an Event Log that lists and tracks system events as they occur. Administrators can check this log to identify a record of system errors, triggered event rules, and more.

For more details, you can refer to:

- [DW Spectrum – Viewing Event Log](#)
- [DW Spectrum – Exporting Event Logs](#)
- [Collecting Logs](#)

13) Is there a log of user activity?

DW Spectrum does provide an Audit Trail for administrators to track and monitor individual user activity. This includes seeing when a user profile has logged in or logged off, when edits are made to settings, and what cameras and playback have been called for viewing.

For more details, you can refer to:

- [Audit Trail of User Actions](#)
- [DW Spectrum – Audit Trail](#)

14) Who owns the data in the system?

The system Owner maintains control over the surveillance site and of all user data. Digital Watchdog does not have access to users' private data, video archives, or system information at any time. Your system is your system.

For more details, you can refer to:

- [DW Cloud - How Secure is DW Spectrum?](#)

15) Is archive data encrypted?

DW Spectrum provides an Archive Encryption feature to enhance the security of your system by ensuring that video archive files are protected while stored in the storage volume. This protective measure prevents unauthorized access and ensures that video archives remain exclusively accessible within the confines of your DW Spectrum System.

For more details, you can refer to:

- [Enabling Archive Encryption](#)
- [DW Spectrum – Server Archive Encryption](#)

16) How is video data exported?

If an Administrator or an approved user must export video files from DW Spectrum, they can use the Video Export feature to extract video from an individual camera or multiple cameras in different file formats (.MKV, .AVI, .MP4, .NOV, .EXE), variable viewing speeds and with embedded system-generated information (timestamps, custom logos/images, custom text, operator information, etc.).

For more details, you can refer to:

- [Exporting Video](#)
- [DW Spectrum – Exporting Video](#)

17) What development tools are available for DW Spectrum?

Development tools and documentation are built into DW Spectrum including Server API, SDK, Cloud API, and more.

For more details, you can refer to:

- [DW Spectrum for Developers](#)
- [DW Technology Partners](#)

18) How are users authenticated using DW Spectrum?

Users can be managed by the Owner and their Administrators to limit access to specific resources, video archives, and other areas of the system that you may want to safeguard against internal threats. This includes local user profiles, DW Cloud users, and users added from an LDAP Server.

DW Spectrum also uses Bearer Authentication as the default authentication method for user connections, previously using Digest Authentication.

For more details, you can refer to:

- [Creating a New User](#)
- [User Management](#)
- [Adding Users from LDAP Server](#)
- [Resetting DW Cloud User Passwords](#)
- [DW Spectrum – Adding New Users and Assigned Roles](#)
- [DW Spectrum – DW Cloud Account Setup and Management](#)
- [DW Spectrum – Enabling Digest Authentication](#)

19) Is Two Factor Authentication (2FA) available?

Yes, DW Spectrum has a Two Factor Authentication (2FA) security feature that can be implemented as an additional layer of security. When someone tries to gain access to a DW Spectrum System enabled with 2FA, they will be required to enter a password when initially connecting (1st factor) and will additionally be required to enter a pin code (2nd factor) that has been generated from a separate authentication application (Google Authenticator, Microsoft Authenticator).

For more details, you can refer to:

- [Setting Up 2 Factor Authentication](#)

- [DW Cloud – Enabling Two Factor Authentication \(2FA\) for DW Spectrum IPVMS](#)
- [DW Cloud – Using Two Factor Authentication \(2FA\) Backup Codes](#)

20) How are user roles managed within DW Spectrum?

DW Spectrum provides administrative users with the ability to assign roles and organize users together into specific groups. Both premade and custom roles can be applied to limit user access to specific resources and settings, as well as controlling what cameras and recorded video can be viewed.

For more details, you can refer to:

- [Predefined User Roles](#)
- [User Role Management](#)
- [DW Spectrum – Adding New Users and Assigning Roles](#)

21) Is it possible to limit user session duration?

Yes, administrators can enable a session time limit to automatically disconnect a user after a select amount of time. By default, each user is given a token that lasts 30-days where their client session can remain connected to the DW Spectrum System. Once this period has passed, their user session will automatically close, regardless of user activity level or interaction status within the application. Administrators can set a duration limit of up to 99 days, minutes or hours (initially 30-days by default).

For more details, you can refer to:

- [Automatic Session Timeouts](#)
- [DW Spectrum – Changing the User Session Time Limit](#)

22) Is there a complete user manual available?

Yes, there are multiple locations where you can view the user manual for DW Spectrum IPVMS including an online help manual, a contextual help guide within the desktop client, and a PDF version for offline reading.

For details, you can refer to:

- [DW Spectrum – Online Help Manual \(overview\)](#)
- [DW Spectrum IPVMS Help](#)
- [DW Spectrum IPVMS Product Page \(Documents tab\)](#)

23) What training options are available for DW Spectrum?

Digital Watchdog offers a variety of ways for you to familiarize yourself with using DW Spectrum including online training courses, in-person certification training, a video library and our YouTube channel.

For details, you can refer to:

- [DW University \(online learning\)](#)
- [In-Person Certification Course](#)
- [DW Online Video Library](#)
- [Digital Watchdog YouTube Channel](#)

24) Please provide a description of support options.

There are DW Technical Support Teams located in Florida and California, as well as international customer service support. Additionally, there are a variety of online help options available.

For more details, you can refer to:

- [DW Support Landing Page](#)
- [Digital Watchdog Hours of Operation](#)
- [DW Knowledge Base](#)

25) What warranty options are available?

All Digital Watchdog hardware is covered by warranty and varies by product type.

Recording servers, analog cameras, and specialized cameras (E.S.T. thermal camera) will have a 2-year warranty period for labor and parts. Meanwhile, hard drives and the majority of the DW MEGApix IP camera series are typically covered for up to 5-years.

There are certain models that are excluded from the limited warranty coverage.

For more details, you can refer to:

- [DW RMA Landing Page](#)
- [DW RMA Warranty Status Tool](#)
- [Digital Watchdog Model SKUs and Warranty](#)

26) What is the company background of Digital Watchdog?

Digital Watchdog is the industry leader in security compliant digital recorders, surveillance cameras, and IP video management software. Founded in 1988, the company has rapidly expanded across regions in the Americas and Asia-Pacific and has experienced 12 consecutive years of strong revenue growth.

DW's established reputation within the security industry has led to 60% of the Top 20 global brands in retail, finance, enterprise, healthcare, government, education, and other vertical markets.

For more details, you can refer to:

- [Meet DW Webpage](#)
- [DW Management Team](#)
- [DW Contacts](#)
- [Cyber Security at DW](#)

27) Has DW Spectrum been reviewed by an independent third-party testing agency?

Yes, Letters of Attestation can be found here:

- [DW Spectrum Application and Client Platform Security Assessment](#)

28) Has DW Cloud been reviewed by an independent third-party testing agency?

Yes, Letters of Attestation can be found here:

- [DW Cloud Backend Platform Security Assessment](#)

- [DW Cloud Portal Platform Security Assessment](#)

29) Please provide an overview of the DW Cloud Service.

DW Cloud is a cloud connect service that allows users to remotely connect with their DW Spectrum Systems through an Internet connection from onsite and offsite locations. Using UDP hole punching to maintain cloud connections, the conventional need to forward TCP ports in your network is unnecessary. However, enterprise Firewall and SonicWall network security will require assistance from your IT department's Network Administrator with allowlisting the service.

The connection services include private peer-to-peer (P2P) communication between connecting clients and the DW Spectrum Servers, encrypted relay servers for optimized network traffic, and the cloud status is constantly monitored and managed to address any regional availability issues.

For more details, you can refer to:

- [DW Cloud Overview](#)
- [DW Cloud Web Portal Interface](#)
- [DW Cloud Landing Page](#)
- [DW Cloud Status Monitoring Portal](#)

30) Does Digital Watchdog have access to private user data?

Absolutely not. Digital Watchdog and its staff, including agents, technicians, developers, and executives, cannot intercept or lookup user video streams, video archives, server databases, or user activity.

In all cases, authentication requests are handled uniformly – through the DW Spectrum Server computer itself, located onsite at the Owner user's location, and never by relay or mediator.

The only way that anyone from DW would be able to access that information is when directly working with you to resolve a troubleshooting issue. You will know when this is happening as onsite authentication will be required so that the assisting DW Support personnel can connect through a limited-permission remote access software (TeamViewer).

For more details, you can refer to:

- [How Secure is DW Cloud?](#)

31) Does DW Cloud provide health monitoring?

Yes, DW Cloud and DW Spectrum monitor the various metrics and parameters of different components within your DW Spectrum System (servers, cameras, storage, etc.) and can give you valuable information about the state of different component types.

Alerts can also be set to notify users when such metrics exceed thresholds in an otherwise healthy system.

For more details, you can refer to:

- [Health Monitoring](#)
- [Metrics](#)
- [Alerts](#)

32) How does DW Spectrum communicate with DW Cloud?

Video management systems (VMS) will generate Internet traffic if a system is provided with Internet access. Because of this, some port management may be needed to allow access through network security for systems to communicate with each other, especially if a DW Spectrum System is comprised of merged servers between different locations.

DW Cloud is part of a Peer-to-Peer (P2P) network that allows DW Spectrum users to easily connect with individual servers and merged systems but there may be instances where an enterprise Firewall prevents communication.

When a user attempts to connect with a camera remotely, the connection will first be routed to the DW Cloud server, which will then direct the connection to the DW Spectrum Server using the already established socket that was previously initiated. Authentication and connection will then be established between the connecting DW Spectrum Client and DW Spectrum Server, providing access to the camera.

For a detailed information:

- [DW Spectrum – FQDN or Allowlist for DW Cloud Access](#)
- [DW Cloud Overview](#)

33) Is there a public monitoring portal for DW Cloud?

Yes, there is a real-time reporting service that monitors the availability of DW Cloud's global mediator and relay servers.

For more details, you can refer to:

- [DW Cloud Monitoring Portal](#)
- [DW Spectrum – Cloud Service is Unreachable or Offline](#)
- [DW Spectrum – Reporting DW Cloud Issues](#)

34) Please provide any third-party code used in DW Spectrum and DW Cloud.

The use of third-party code in DW Spectrum and DW Cloud are licensed for use and redistribution under open-source licenses.

For a list of disclosures and disclaimers in connection with DW Spectrum and DW Cloud, you can refer to:

- [Open-Source Software Disclosure for DW Spectrum and DW Cloud](#)

35) Does Digital Watchdog have a published privacy policy?

Yes, you can find the privacy statement here:

- [Digital Watchdog Statement of Privacy](#)

36) What are the terms and conditions of DW Spectrum?

You can find the terms and conditions of DW Spectrum here:

- [DW Spectrum Terms and Conditions EULA](#)

37) Do DW products comply with the National Defense Authorization Act (NDAA), Section 889?

Yes, you can find our compliance statement here:

- [Digital Watchdog NDAA Compliance Statement](#)

38) Do DW products comply with the Trade Agreement Act (TAA)?

Yes, you can find our compliance statement here:

- [Digital Watchdog TAA Compliance Statement](#)

39) Does DW comply with the 2020 California SB No. 37 IoT (Internet of Things) law?

Yes, you can find our compliance statement here:

- [Digital Watchdog IoT Compliance Statement](#)

40) Are DW products HIPAA compliant?

DW products and other 3rd party manufacturers are not required to be inherently HIPAA compliant. It is the responsibility of the medical facility's staff and organization to ensure that HIPAA compliance is maintained.

You can find some guidance regarding HIPAA compliance here:

- [HIPAA Compliance Recommendations](#)

For More Information or Technical Support

DW Technical Support: 866.446.3595 (option 4)

<https://www.digital-watchdog.com/contact-tech-support/>

DW Sales: 866.446.3595 sales@digital-watchdog.com www.digital-watchdog.com