Network Optix

Nx Witness

Video Management System

Quick Start Guide | Version 6.1.x

Still need help? Visit us at http://support.networkoptix.com

Introduction 3

Site Setup 4

Media Server Setup 5
Connect Site to an Organization 7
Connect Site to a Cloud Account 8
Site Settings 9
Security Settings 10
Merge Server to Local Site 11
User Management 12
User Types 13
User Permissions 15
Create a Cloud Account 19
Add Cameras and Streams 20
Storage and Backup Configuration 21
License Key & Services 24

Operations 25

User Interface 26
Camera Control Icons 27
Layouts and Scenes 28
Timeline Controls 29
Camera Settings 30
Enable Recording 31
Search the Video Archive 32
Smart Motion Search 34
Advanced Object Search 35
Export Recorded Video 37

Introduction

Platform Overview

Nx Witness is a lightning-fast, easy-to-use, cross-platform IP video management system (VMS) and video surveillance software platform designed to discover, view, record, and manage IP video cameras. Operators can monitor, analyze, and react to analytically detected and observed events in real-time using soft-triggers and a customizable set of rules and actions that are always on watch.

This extensible platform consists media servers interconnected as a hive-network that maintains data integrity and provides failover options to each Site. Depending on intent and configuration, Sites can be locally isolated or accessed over the internet using the Nx Cloud portal. A browser-based Web Admin interface is hosted on each media server to facilitate remote management while Mobile clients for iOS and Android deliver video and notifications into the hands of response teams.

The fully featured Desktop Client provides access to all device settings, user management tools, audit logs, alerts, and an extensive ecosystem of integrations from device manufactures and independent, third-party solution providers that extend the power of Nx Witness.

Document Scope

This guide outlines the fundamental steps to set up a media server as a Site and how to access frequently used features and powerful video-search tools. Topics presented are distilled from the complete Nx Witness User Manual that can be accessed from within the Desktop Client and rely on the audience having a fundamental understanding of network topology, IP cameras, data storage technologies, and the broader concept of a VMS.

The set up chapter covers configuring a new Site, activating license keys & subscription services, connecting a Site to an Organization or connect a Site to a Cloud Account, configuring storage, adding cameras, and managing users.

The operations chapter provides abbreviated instructions for navigating the Desktop Client User Interface, creating Layouts and Scenes that display multiple cameras how to enable recording, access Camera Settings, and Search the Video Archive.

Additional References

- The complete Nx Witness User Manual integrated into theDesktop Client.
- Contact your technical support team or authorized reseller.

Site Setup

This chapter covers setting up a new media server, configuring video storage, adding users, and optionally connect it to an existing local Site, an Organization, or an individual Cloud Account.

Key Concepts

- The media server manages devices, network traffic, video archives, and user access.
- A Site can support 2,560 video steams (256 streams per media server and 10 servers per Site).
- Sites are connected together as an Organization to endlessly expand video stream count.
- Only the Desktop Client provides access to every possible settings and configuration option.
- Each media server offers a browser-based (Web Admin) interface to perform common tasks.
- The Nx Cloud can only access cloud-connected or Enterprise Sites.
- Professional Edition Sites can only record to media servers that have license keys.
- Enterprise Edition Sites use Subscription Services that are transferable between media servers.
- A Professional Edition Site can easily be upgrade to an Enterprise Edition Site.
- An Enterprise Edition Site cannot be converted into a Professional Edition Site.
- Site performance is influenced by hardware selection, network capacity, and optional settings.
- Some devices features depend on having compatible integrations and plugins installed.
- Video Wall enables HD Witness to remotely control or span accessible displays.

NOTE: For the media server application to continuously process data, the host server must remain running and cannot be enter a state that pauses the media server application.

Media Server Setup

Launch a Client

Start the media server setup process by launching the Desktop Client or the Web Admin interface:

- Desktop Client: Launch the client using the installed shortcut and wait for the Welcome Screen.
- Web Admin: Enter the Server address (e.g. https://172.16.0.112:7001) into an internet browser.

NOTE: A prompt to update graphics drivers or enable alternate rendering services may be presented based on workstation configuration.

Setup a New Site

1. If using the Desktop Client, first click the **New Site** tile on the Welcome Screen.
2. Select **Setup New Site** in the Get Started dialog box.
3. Enter a name for the new Nx Witness Site.
4. Click the **Advanced system settings** link below the Site Name and configure the following options:
   - Enable device auto discovery.
   - Allow device setting optimization.
   - Send anonymous usage statistics and crash reports.
   - Select the *Security Level* using the menu. The System Security Level cannot be changed once set (see "System Settings and Security").

     Standard:

     - “Encrypt video traffic to desktop and mobile client” is disabled.
     - Camera credentials are shown in the Camera settings dialog.
     - Server IP is shown in API responses.

     High:

     - “Encrypt video traffic to desktop and mobile client” is enabled.
     - Camera credentials are not shown in Camera settings.
     - Server IP is not shown in API responses.
5. Enter a password for the admin account - the preset username "admin" cannot be changed.

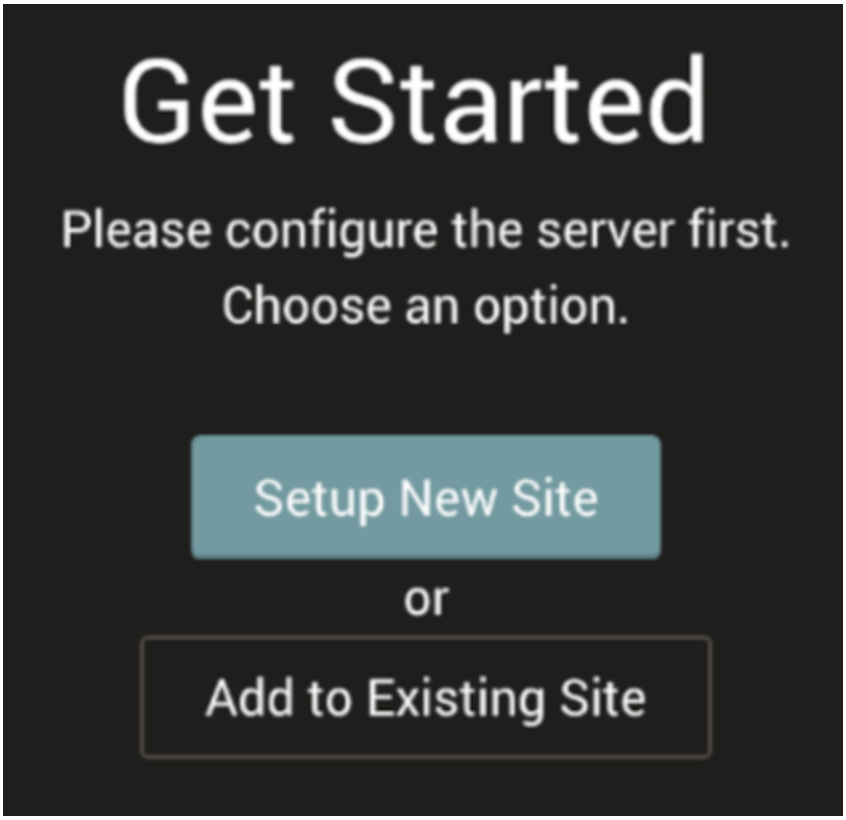
   NOTE: The admin account is the primary System account with all Site privileges.

6. Review the confirmation message and click **Finish**.
   a. The Web Admin interface will refresh to a log in prompt.
   b. The Desktop Client will log in the admin account or return to the Welcome Screen.

Add to Existing Site

1. If using the Desktop Client, first click the **New Site** tile on the Welcome Screen.
2. Select **Add to Existing Site** in the Get Started dialog box.
3. Enter the network address of the existing system; you may need to navigate browser security warnings and manually approve the local connection.
4. Enter the password for the *admin* account on the existing system.

   NOTE: If joining an existing, local site is not successful during media server setup, you can Merge the new Server to Local Site after completing setup.



Connect Site to an Organization

Connecting a new Site to an Organization will define the Site as an Enterprise Edition Site.

Connect a Site to an Organization

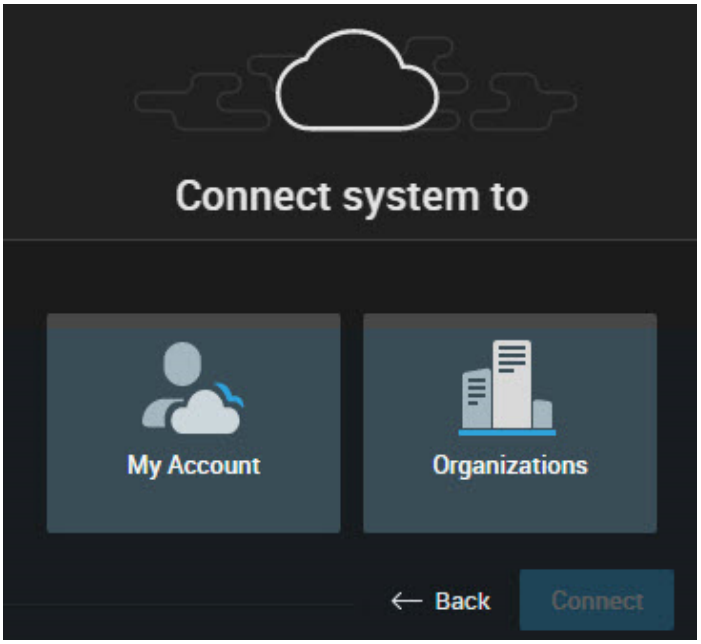
Desktop Client

1. Log in to the Site as an Administrator.
2. Open **Main Menu** > **Site Administration** and go to the **Nx Cloud** tab.
3. Click **Connect Site to Nx Cloud** and log in to Nx Cloud.
4. Click the **Connect Site to Cloud** button; then select the Organization to join.
5. A Site Administrator and an Organization Administrator must authenticate to approve.

Web Admin

1. Login to the Site as an Administrator
2. Open the Web Admin and login.
3. Go to **Settings** > **Site Administration** > **General**.
4. Click **Connect to Nx Cloud** and login as an Organization Administrator
5. Select the **Organizations** tile; then select the Organization the Site will be connected to.
6. The Site Administrator and the Organization Administrator must authenticate to approve .

The Site will be displayed in the **Nx Cloud** Portal accessible by approved users.



Connect Site to a Cloud Account

Connecting a Site to a user-specific cloud account will enable access to Site through the Nx Cloud Portal by all authorized cloud users and enable many cloud-only features, but not all the features available with the Enterprise Edition. See the full User Manual for additional information.

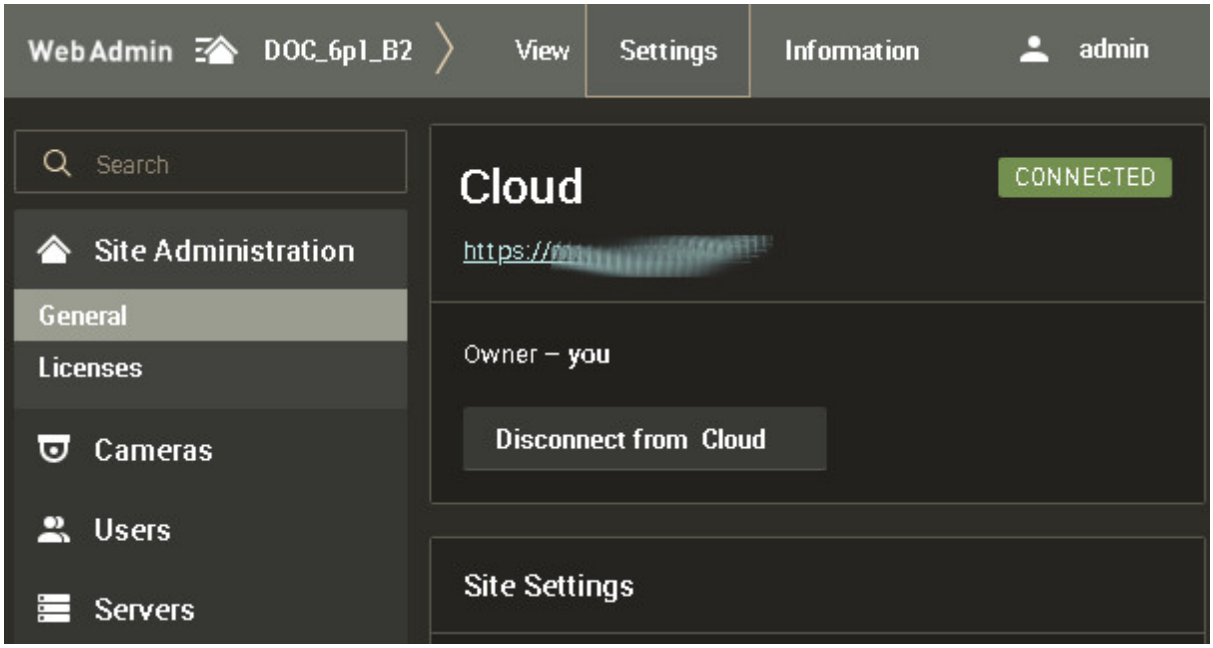
Connect a Site to a a Cloud Account

Desktop Client

1. Log in to the Site as an Administrator.
2. Open **Main Menu** > **Site Administration** and go to the **Nx Cloud** tab.
3. Click **Connect Site to Nx Cloud** and log in to Nx Cloud.
4. If the Connect System To dialog is presented, select the **My Account** tile and **Continue**.
5. Enter the Site Administrator (admin) password to complete the operation.

Web Admin

1. Open the Web Admin and login as an Administrator.
2. Select **Settings** in the heading menu and **Site Administration** > **General** in the left menu.
3. Click **Connect to Nx Cloud** button under the Site name.
4. Log in to the Cloud account that Site will be connected to.as an Organization Administrator
5. If the Connect System To dialog is presented, select the **My Account** tile and **Connect**.
6. Enter the Site Administrator (admin) password and click the **Connect** button.



Site Settings

Use caution and consult the full User Manual before changing any Site settings as they apply to all Servers and User equally.

Open Site Settings

Desktop Client

1. Log in to the Site as an Administrator or Power User.
2. Open **Main Menu** > **Site Administration** and open the **General** tab.
3. Find the Site Settings below the row of icons.

Web Admin

1. Open a web browser and connect to a Server in the Site (**http://<ip>:<port>**)
2. Navigate any the security warnings and enable local access.
3. Log in to the Site as an Administrator or Power User.
4. Select the **Settings** tab in header menu and the **General** tab in the left menu.

Nx Cloud *Portal*

1. Log into the Portal as an Administrator or Power User and select the Site to configure.
2. Select the **Settings** tab in header menu and the **General** tab in the left menu.

Available Site Settings

Selecting or deselecting any of the following in one client will soon be reflected in all other clients.

- *Enable cameras and servers autodiscovery and automated camera status check.*
  - When enabled, the Site will continuously scan for cameras and Servers on the network.
  - When disabled, cameras must be manually added and may report as being offline.

  NOTE: Multicast must be enabled on your network for autodiscovery to work.
- *Send anonymous usage and crash statistics to software developers.*
  - When enabled, the Site will automatically sends anonymous Site data to developers.
- *Allow System to optimize camera settings.*
  - When enabled, cameras will send two streams at the optimal resolution; individual camera settings can be changed through the Camera Settings dialog.

Security Settings

The Nx Cloud Portal and Web Admin interface provide access to the primary security settings with a few additional options accessible only when using the Desktop Client.

Open Security Settings

Desktop Client

1. Log in to the Site as an Administrator or Power User.
2. Open **Main Menu** > **Site Administration** and open the **Security** tab.

Web Admin

1. Open a web browser and connect to a Server in the Site (**http://<ip>:<port>**)
2. Navigate any security warnings and log in to the Site as an Administrator or Power User.
3. Select the **Settings** tab in header menu and the **General** tab in the left menu.
4. Scroll down to find the box containing the Security options.

Nx Cloud Portal

1. Log into the Portal as an Administrator or Power User and select the Site to configure.
2. Select the **Settings** tab in header menu and the **General** tab in the left menu.
3. Scroll down to find the box containing the Security options.

Available Security Settings

Selecting or deselecting any of the following in one client will soon be reflected in all other clients.

- *Force servers to* accept only encrypted connections protects API and Web Admin packets.
- Encrypt video traffic to desktop and mobile clients protects video streams.
- Mandatory 2FA for cloud users requires two factory authentication. Set in the Cloud Portal.
- Enable audit trail tracks and logs all user actions into a historical, time-stamped record.
- Limit session duration will be automatically logged out users a session exceeds the limit.
- Display servers *in tree for non-administrator users* allows all users to see Site Servers.

Functions only available when using the Desktop Client.

- *Use only* HTTPS to connect to cameras protects against intercepted video streams.
- *Display watermark* with username over video can deter leaks and provide traceability.
- *Archive Encryption* encrypts the archive data to prevent viewing without a password.
- *Remote Access Tool* provide automatic port forwarding for remote access to Site clients.

Merge Server to Local Site

Merging Sites is a powerful method to increase fail-over capacity and operational efficiency by placing servers, devices, archives, and users within a single Site entity.

NOTE: This Quick Start Guide only covers merging two local Sites as resolution when it was not possible to add a newly installed server to an existing Site during Server Setup. See the full Nx Witness User Manual for guidance on the other types of Site mergers available and a detailed explanation of the Site merger process.

Merge Server to Existing Site

Desktop Client

1. Launch the client and connect to any Server in the primary Site, this Site will remain.
2. In the resource panel, right-click the Site joining the primary site and choose **Merge Sites.**
3. Enter the URL of the secondary server **http://<ip>:<port>**, to be merged (any Server in the Secondary Site, or a remote server), or select a local site from the drop-down menu.

   <ip> = IP address of Server (the active client must be able to connect to this server).

   <**port>** = network port of Server (default **7001**).
4. Enter the Secondary Site / remote server **Password**; click **Check** to validate the merger.
5. Select the which Site to take the name and settings from.
6. Click the **Merge with <Site Name>** button.

Web Admin

1. Open a web browser and enter the address of the primary site (http://<ip>:<port>).

   <ip> – IP address of Server in primary Site.

   <port> – network port of Server (default 7001).
2. Log in with a Local Admin username and password.
3. Go to the **Site** tab and click **Merge Sites**.
4. Choose a secondary Site from the drop-down list, or enter the address for the secondary Site (http://<ip>:<port>) and click **Find Site,** then click **Next** after Site is found.
5. Authenticate as Site administrator on the secondary Site.
6. Select which Site's name and administrator password will be kept.
7. Click **Merge Sites**.

User Management

Key Concepts

- Know the User Type to add before starting the process it cannot be changed once set.
- A User must be deleted and added again to change their User Type.
- Only Administrators and Power Users can add users.
- Regular Users and Temporary Users can be added at the Desktop Client only.
- Cloud Users can be added at the Web Admin, Cloud Portal or Desktop Client.
- User permissions can be assigned at the Desktop Client only.
- Permission Groups can be assigned using the Desktop Client, Web Admin, and Cloud Portal.

NOTE: Users are added without access to resources unless they are granted User Permission.

Adding a User using the Desktop Client

1. Open the *Add User* dialog by selecting **Main Menu > Add > User**.
2. Select to add the new User in with an Enabled or Disabled status.
3. Choose the User Type.
   - *Cloud*: Enter the Email address of the User to add. Cloud Users cannot be Temporary Users.
   - *Local*: Enter the Login ID, Full Name, and Email address.
4. Select access type:
   - Set time limitations when Adding Temporary Users
   - Provide and confirm a Password when Adding Regular Users.
5. Optional – Select the Permission Groups the Added User will be a member of.
6. Click the **Add User** button to complete the process. Re-authentication may be required.

   NOTE: Copy and provide the Temporary link to the intended user.

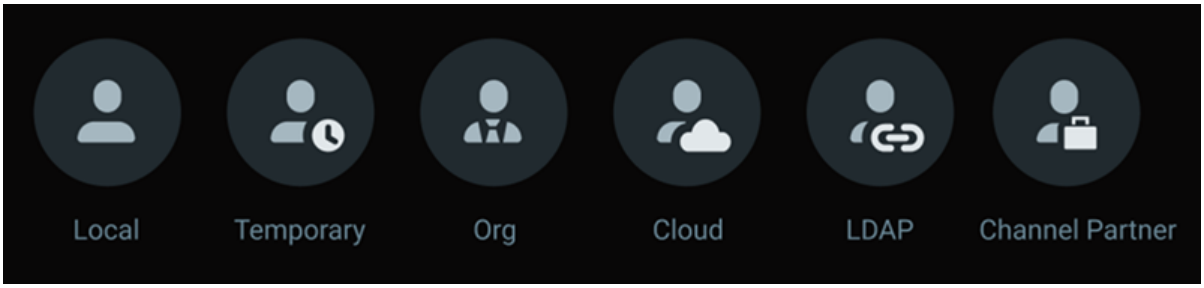
Adding a User using the Web Admin / Cloud Portal

1. Select **Settings** in the header menu and expand **Users** in the left panel navigation.
2. Click the **Add User** button and enter the Email address of the User to add.
3. Optional – Select the Permission Groups the Added User will be a member of.
4. Click **Add User** to complete the process. Authentication may be required.

NOTE: Site will be shown to established Cloud Users and new Cloud Users will receive an email with further instructions to validate and activate their account.

User Types

The following types of Users can be present in the Site and are identified in lists with specific icons.



Local Users:

- Reside in the Site where they were added.
- Connect to the Local Site using the Desktop Client, Mobile Client, or the Web Admin interface.
- Cannot use the Cloud Portal.

Temporary Users:

- Are Local Users with limited permissions, and a preset expiration date or session limit.
- Cannot be a member of any group with Power User permissions.
- Can use the Desktop Client and Web Admin to connect to a Site.
- Cannot use the Cloud portal with the link provided.
- Receive a URL to connect to the Site; no password is required and link can be used by anyone.

Organization (Org) Users

- Are created outside of the Desktop Client, Mobile Client, or the Web Admin interface.
- Are managed at the Organization level by the Organization Administrator.
- Are displayed in User Management dialogs and Site User lists.
- Can be granted access to any combination of Sites, or all Sites, within the Organization.
- Can only have permission changed by an Organization Administrator.
- Site-level permissions are set and revised by authorized Site Administrators and Power Users.
- Cannot be disabled or removed by Site Administrators or Power Users.
- Access Sites using the Desktop Client, Mobile Client, Web Admin, or Cloud Portal.

Cloud Users

- Reside in the Cloud and can exist without having access to a Site.
- Use the Desktop Client, Mobile Client, or the Web Admin interface to access Cloud Connected Sites.
- Can only access Sites that are connected to the Cloud.

LDAP Users

- Retain their username, password, and LDAP Group memberships after imported is complete.
- Connect to Sites using their imported credentials and the Desktop Client or Web Admin.
- Cannot log into a Site when the LDAP Server fails to respond.
- Can be directly granted Permissions and added to both Built-In and Custom Permission Groups.
- Cannot be permanently deleted from a Site as LDAP users are refresh during each LDAP sync.

Channel Partner Users

- Are displayed in User Management dialogs and Site User lists when they have Site-level permissions.
- Inherit permissions from their Channel Partner that cannot be changed by Site-level users.
- Site-level permissions can be set and revised by Site Administrators and Power Users.
- Use the Desktop Client, Mobile Client, Web Admin, and Cloud Portal to access Site.
- Cannot be disabled. However, Channel Partner Users can be removed from a Site.

NOTE: Removing a Channel Partner user from a Site hides the user in the User Management interface while retaining their inherited permissions.

User Permissions

Permissions can be configured for Groups (Custom and LDAP), Channel Partners users, and for individual (local, cloud, organization, and LDAP) users. This topic only covers individual user permissions, please see the full User Manual for additional information.

To configure Permission for a User

1. Open the *User Management* dialog by selecting **Main Menu > User Management** dialog and switching to the **Users** tab.
   - Optionally refine the list of users by using the search box, filters, and column sorting options.
2. Click on the User name in the list, or a select a single checkbox and Click **Edit** to open *User Properties*.
3. Choose the *Groups* tab to assign group membership, *Resources* tab to manage **Resource Permissions,** or the *Global Permissions* tab to manage **Global Permissions**.

Resource Permissions

Granting Permissions to Resources is done by selecting the Permission level (view live, archive, manage bookmarks, etc.) a User or Group will have to a Resource. The Resource configuration panel is the same when configuring Users or Groups

Global Permissions for Users

Use the checkboxes to enable or disable the following:

- If Group members are permitted to View the Event Log.
- If Group members are permitted to generate non-camera events.

Permission Groups

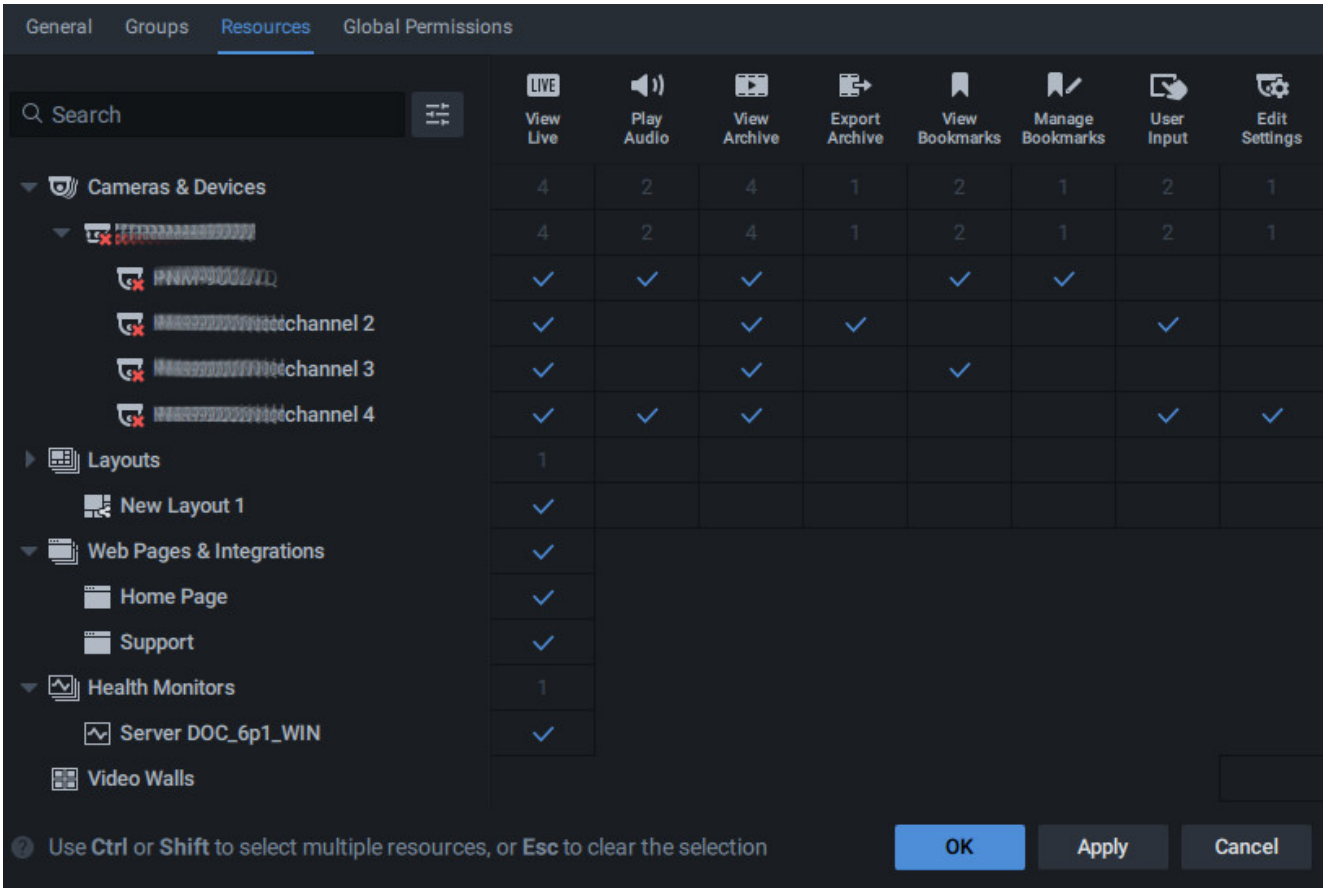
The following able details the Permissions available to each Built-in Group.

- Built-In groups cannot be renamed or modified.
- Custom Groups can be members of any Built-In Group, except for the Administrators Group.
- A Built-In Group cannot be a member of a Built-In Group, a Custom Group, or an LDAP group.

Action	Built In Groups					
	Administrators (Owner in 5.x)	Power Users (Administrator in 5.x)	Advanced Viewers	Viewers	Live Viewers	Site Health Viewers
Configure Site Settings						
Edit Site Name	✔	✔				
Configure General Settings	✔	✔				
Install Site Updates	✔	✔				
Activate Licenses	✔	✔				
Deactivate Licenses	✔					
Create, Edit, Delete Regular Users	✔	✔				
Create, Edit, Delete Regular Groups	✔	✔				
Create, Edit, Delete Power Users	✔					
Create, Edit, Delete Administrators						
Configure Email Server Settings	✔	✔				
Configure Security Settings	✔	limited				
Configure Time Synchronization	✔	✔				
Configure Routing Settings	✔	✔				
Configure Plugins	✔	✔				
Create Site Backup	✔					
Restore from Site Backup	✔					
Manage Logs	✔	✔				
Update Site	✔	✔				
Merge Sites	✔					
Connect Site to Cloud	✔					
Disconnect the Site from the Cloud	✔					
Audit Trail	✔	✔				

Action	Built In Groups					
	Administrators (Owner in 5.x)	Power Users (Administrator in 5.x)	Advanced Viewers	Viewers	Live Viewers	Site Health Viewers
Configure Server Settings						
Rename Server	✔	✔				
Auto-detect built-in and USB camera	✔	✔				
Configure Failover (all settings)	✔	✔				
Detach Server (from Site)	✔					
Delete Server from Resource Panel	✔					
Reset to Defaults	✔					
Restart Server	✔	✔				
Add, Edit, Delete Storage	✔	✔				
Manage Analytic DB Storage	✔	✔				
Reindex (Archive + Backup)	✔	✔				
Configure Backup Settings	✔	✔				
Pin Certificate (in case of error)	✔					
Cameras and Devices						
View Live all Camera and Devices	✔	✔	✔	✔	✔	
View Live Web Pages & Integrations	✔	✔	✔	✔	✔	
View Live all Server Health Monitors	✔	✔	✔	✔	✔	✔
Play Audio	✔	✔	✔	✔	✔	
View Archive	✔	✔	✔	✔		
Manage Bookmarks	✔	✔	✔			
User Input (PTZ, Audio, Soft Triggers)	✔	✔	✔			
Generate Events	✔	✔	✔			
Edit Settings all Cameras and Devices	✔	✔				
Edit Setting all Video Walls	✔	✔				
View Event Log	✔	✔	✔			
Edit Event Rules	✔	✔				
Edit Device Settings	✔	✔				
View Bookmarks	✔	✔	✔	✔		
Export Archive	✔	✔	✔	✔		

Action	Built In Groups					
	Administrators (Owner in 5.x)	Power Users (Administrator in 5.x)	Advanced Viewers	Viewers	Live Viewers	Site Health Viewers
Other Resources						
View, Edit, Rename, and Delete Shared Layouts	✔	✔				
Create new Shared Layouts	✔	✔				
Configure and access Video Walls	✔	✔				
Web Admin / Cloud Portal						
View Metrics & Alerts	✔	✔				✔
View Monitoring & Graphs	✔	✔				✔
View Monitoring & Logs	✔	✔				



Create a Cloud Account

Create a Nx Cloud Account

1. Open the Nx Cloud account registration page.
2. Enter the account registration information requested and click **Create Account**.
3. Open the account activation email and following the included instructions.

Log in to the Nx Cloud Portal

The Nx Cloud portal homepage displays tiles, and each tile represents a cloud-connected system to which the user has access.

1. Open the Nx Cloud portal homepage and click **Log In**.
2. Enter your account email and click **Next**; enter your account password and click **Log In**.
3. Click on a tile to access a Cloud connected site - menus shown are defined by User Permissions.

Enable Two-Factor Authentication (2FA)

1. Install Google Authenticator, Microsoft Authenticator, or Duo Mobile on a compatible device.
2. Open Nx Cloud portal homepage and log in to your account.
3. Click your email address to open account settings sub-menu, then select **Security**.
4. Enable **Two-factor authentication** by clicking on the switch.
5. Enter your Nx Cloud account password.
6. Open your chosen mobile authentication application and scan the QR code.
7. Enter the TOTP verification code generated by the mobile authentication app.
8. Click **Verify** to complete the setup process.

   NOTES:

   - Enable *Ask for verification code on every login* to increase security.
   - Securely store single-use backup codes for use without the mobile app.

Log in to Nx Cloud with the Desktop Client

1. Click the Nx Cloud icon ( ) on the Navigation Panel.
2. Enter your Nx Cloud account email and click **Next**.
3. Enter your Nx Cloud account password and click **Log in**.

Add Cameras and Streams

Key Concepts

- Compatible cameras are detected during setup as auto-discovery is enabled by default.
- Discovered cameras will be shown in the resource panel of the Site after model identification.
- A video stream is added using the same method as manually added cameras.
- Many cameras must be authenticated before settings and video streams will become available.
- Device discover errors may be reported when a camera is on a network with multiple Servers.
- Removed cameras may be re-discovered, after removal, while auto-discovery is enabled.

Manually add a Device

Cameras and streams can be added individually or in bulk when multiple cameras are present on the network. Either open the main menu and select **Add > Device** or right-click on the Serve and click **Add** to open the add devices dialog.

- To add a single camera or stream, enter the device network address into the Known Address tab, include any port or authorization credentials, and then click Search to query the specific network address provided.
- To add multiple camera or stream on the same network, click the Subnet Scan tab and enter the subnet to search. Include any port number or authorization credentials, and click Scan to scan the network IP range for cameras.
- To add a video stream, follow the method to manually add a single device and enter the stream protocol (rtsp, udp) followed by the full address where the stream is hosted, and include any authentication that may be required.

Authorization Credentials

Cameras that require authorization credentials to access their stream are shown with a lock icon.

1. Right-click on a Camera and click **Camera Settings**.
2. In the *General* tab, click **Edit Credentials**.
3. Enter the login and password. Click **OK**.

Storage and Backup Configuration

Key Concepts

- Each media server can use an unlimited number of local, network, and cloud storage solutions.
- The media server will automatically balance space and consumption across available drives.
- Each media server only performs backups for it's own (archive) storage.
- External storage must use one of the supported storage protocols: CIFS, SMB, NFS, or iSCSI.
- Storage backup duplicates the footage in an archive and saves it to another available location.
  - Backups can be performed in real-time or as scheduled function.
  - Backups can be configured to copy captured low-resolution streams, or all streams.
  - Backups can be configured for specific cameras.
  - Every media server in sites with multiple media server must specify a backup location.

Add Storage

Each accessible local and network drive should automatically be detected as a separate storage. Network drives can be added manually if not detected automatically:

1. Right-click on a media server to open the context menu and select **Server Settings**.
2. Go to the *Storage Management* tab.
3. Click **Add External Storage** and enter the storage location and credentials. Click **OK**.
4. Choose which locations should be used for **Main** and **Backup** storage.
5. To store analytics data, hover over the desired drive and click *Use to store analytics data*.

NOTE: It is not recommended to store analytics data on the Main drive as analytics data cannot be moved and takes up large amounts of space.

Read-Write Policies

1. **Exclusive**: The media server can read all folders, erase old data from all folders, and write only to its own folder.
   - This is default setting for all local storage.
2. **Shared**: The media server can read all folders, but can only write or erase old data within it's own folder.
   - This setting can not be applied to local storage.
3. **Isolated**: The media server can only read, write, or erase data in its own folder.
   - This is the default option for all non-local storage locations.

NOTES:

a. Local storage cannot use the Shared policy.
b. Cloud storage can only be configured with the Isolated policy.
c. The read-write policy for reserved storage makes the location available for editing.
d. A warning message and alert icon is displayed when non-local storage has conflicting read-write policies applied by different servers in the Site.

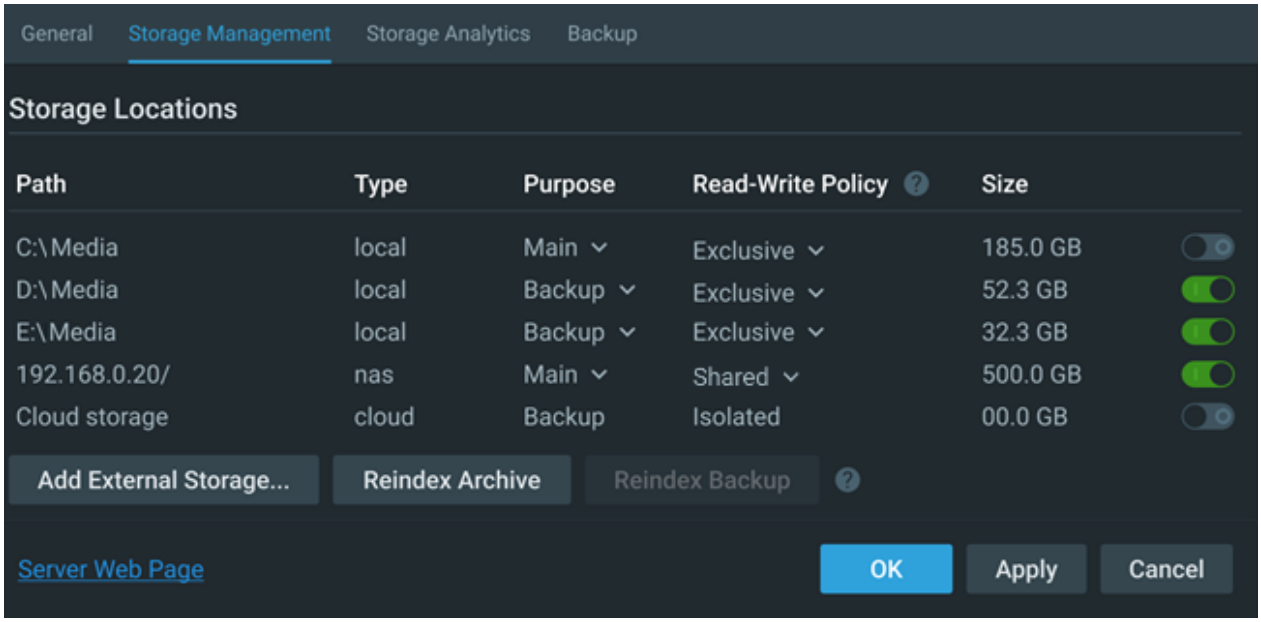
Manually Add Network Storage

Make sure the NAS is available and accessible by the workstation where the media server is installed.

1. Do one of the following:
   - *Desktop Client:* Right-Click on a server to open the context menu and select **Server Settings**; open the **Storage Management** tab.
   - *Web Admin / Cloud Portal:* Open **Settings** > **Servers** and select a server.
2. Click **Add External Storage**.
3. Choose the desired option from the **Protocol** menu, and enter the storage path (**URL**), **Login**, and **Password** for the external storage device.
4. Click OK to accept the entries and add the new device to the list of storage locations.
5. Use the button at the end of the row to toggle the storage location on or off.

Configure Server Storage

1. Do one of the following:
   - Desktop Client: Right-Click on a server, select **Server Settings** > **Storage Management** tab.
   - Web Admin / Cloud Portal: Open Settings > Servers and select a server.
2. Use the drop-down menu to select the purpose and policy for each storage location.
3. Use the switch to enable or disable each storage location.
4. Example:
   - The server has three local partitions (C:, D:, E:).
   - Disk C (operating system) is currently disabled.
   - Disk D and Disk E are backup partitions with an exclusive policy.
   - The NAS is used as main storage using the shared policy.
   - Cloud storage is an isolated backup location (shown as disabled).



NOTES:

a. There must always be at least one Main storage location.

b. At least one drive must be defined as Backup for archive backup to be possible.

c. A warning is displayed when a drive is not available or has insufficient space.

d. Nx Witness will periodically download from a camera's internal storage.

e. All recycling bins and similar services (Trashboxes, trash bins) must be disabled.

See the full User Manual for additional information related to storage, archives, and backups.

License Key & Services

Key Concepts

- Users can create layouts displaying multiple video feeds and perform Site configuration tasks immediately after installation.
- Recording services, support for certain accessory devices, and some advanced analytical tools require either a License Key or a Subscription Service.
- Subscription Services are pooled within an Organization and can be easily moved between Servers and Cameras running the Enterprise Edition of Nx Witness.
- A Professional Site can be upgrade to an Enterprise Site to gain additional features and options; this cannot be undone and an Enterprise Site cannot be converted into a Professional Site.
- Perpetual License Key are attached to an uniquely identifiable Server ID and only operate with the Professional Edition of Nx Witness.
- The Professional Edition includes a fixed duration demonstration key that is activated over the internet or by email relay.

NOTE: Live streams that are not connected to either a subscription service (Enterprise Edition) or a perpetual recording key (Professional Edition) will be interrupted every 10 minutes by a banner displaying "Live Streaming Time Limit Reached" and a 30-second countdown timer.

To activate a License

1. Open the **Main Menu** and click **Site Administration**.
2. Go to the *Licenses* tab.
3. Activate a Trial licenses, or
4. Enter a Professional License Key and click **Activate** License.
5. Recording can be enabled once a valid key is activated.

NOTE: Use the manual activation method for Site that do not have internet connectivity.

To allocate a Subscription Service

Services are made available by Organization Administrators or Channel Partners.

1. Open the **Main Menu** and click **Site Administration.**
2. Go to the *Services* tab to see all Sites services with in use and available totals.
3. Available Services can be allocated to camera where Recording will be enabled.

Operations

This chapter provides a summary of how to navigate the user interface and perform common tasks.

Key Concepts

- The graphical user interface consists of four panels (navigation, resources, notifications, timeline.
- Layouts are dynamic grids where cameras, devices, and integrations are placed, moved, and sized.
- The video timeline includes tools to navigate the archive and scan for events and objects.
- An control panel is available for each camera and embedded tools are easily accessible.
- Record modes include continuous and motion based; either continuous or time scheduled.
- Video archives can be searched using motion detection or advance analytical integrations.
- Exported video can be watermarked, password protected, and bundled with playback software.

User Interface

1. Navigation Panel – Access the Main Menu, create and organize layouts, log in to Nx Cloud, and use the context-sensitive user manual.
2. Resource Tree – Organize all servers, cameras, layouts, webpages, and other resources. Use Keyword Search to find resources quickly. Right-click on a resource and choose Rename to change its name.
3. Notification Panel – Access the following tabs:
   - Notifications – Displays information about the system's state and triggered event rules.
   - Motion – Displays detected motion events from cameras with recording enabled.
   - Bookmarks – Displays bookmarks that were manually created or triggered by an event rule.
   - Events – Provides a list of recently triggered event rules.
   - Objects – Displays detected objects from plugin or camera analytics.
4. Timeline – Playback controls are to the left (Play/Pause, Last/Next Frame, Last/Next Video Segment), and stream toggles are to the right (Live, Sync, Thumbnail, and Calendar). Recorded video appears as a solid green bar. If the Motion tab is open, motion recordings appear as red segments. If the Bookmarks tab is open, bookmarks appear as blue segments.
5. Viewing Grid – Displays up to 64 items (e.g. cameras, webpages, etc.). Items are easily adjustable (drag-and-drop to move, drag corner to resize).

Camera Control Icons

The camera control icons are located in the upper right hand corner of a camera or video stream; icons shown are device, mode, and user-permission dependent.

Icon	Title	Description
	Object Search	Click to open the object search panel.
	Motion Search	Click to open Smart Motion Search.
	Snapshot Image	Open dialog to capture a screen image.
	Dewarp or Fisheye	Access the dewarp controls and settings.
	Hotspots	Configure hotspots on current camera.
	Zoom Window	Draw a zoom area to add to layout.
	Rotate Image	Freely rotate the image using the mouse.
	Pan, Tilt, Zoom	Click and drag to pan - mouse scroll to zoom.
	Information Panel	Display the camera information panel.
	Close WIndow	Removes camera from layout.

Layouts and Scenes

Key Concepts

- On initial Site launch, the default view is an empty layout tab named "**New Layout***"
- An asterisk at the end of the layout name indicates that the layout has unsaved changes.
- A Layout can contain up to 64 video streams, Web Pages, and integrations on the Viewing Grid.
- Multiple layouts exist as individual tabs; clicking the tab title to quickly change the active layout.
- Depending on Site configuration, layouts can be shared with other users or opened by an event.
- To lock a layout, right click in layout open space, select layout settings, and activate the lock.
- Right-click an existing layout to create a layout group, groups can be nested and moved.

Types of Layouts

- *Local Layouts* can only be accessed by the user who created the Layout.
- *Shared Layouts* can be shared with other Site users.
- *Cloud Layouts* may contain devices from multiple Cloud-Connected Sites.
- *Intercom Layouts* are created to support the unique nature of intercom events.
- *Alarm Layouts* will open when a specific event happens or an analytical condition is met.

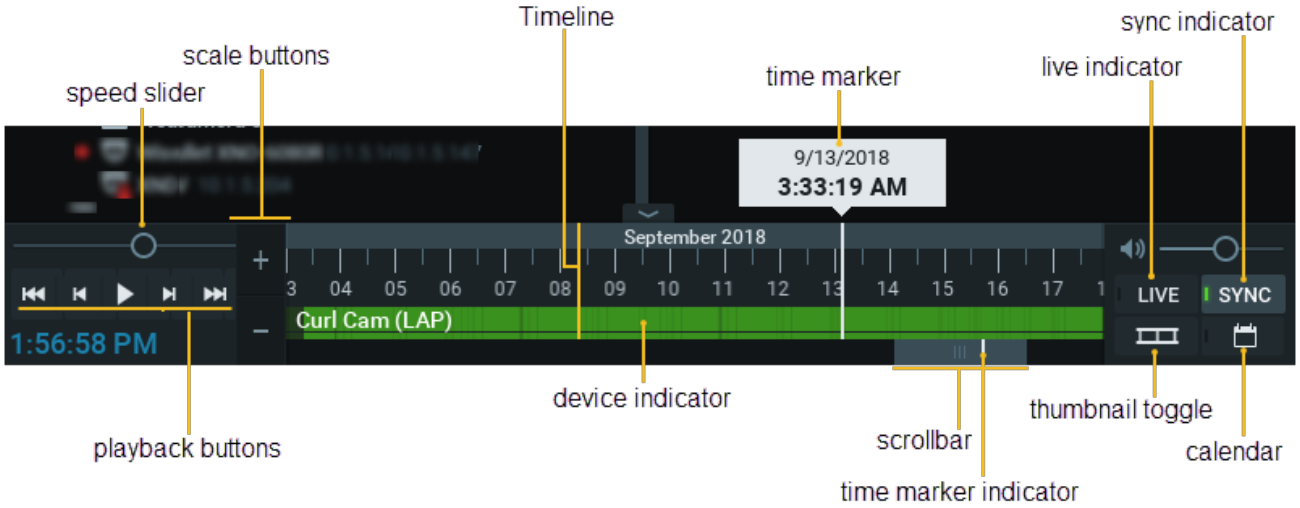
Working with Layouts

- Click on the plus (+) icon in the window header to open a new tab and (x) to close a tab
- Click and Drag layout tabs to change its order across the top of the window.
- Use the right-click contextual menu to rename, save as, or change layout type.
- Right-Click on the layout grid to access cell spacing, aspect ratio, resolution, and other options.
- Drag and Drop cameras, web pages, and devices from the Resource Panel onto the layout grid.
- Grab the corner of an item on the grid to re-size it while other items on the dynamically shuffle.
- Reposition items by dragging them to a new grid location within the active layout.

NOTE: Save layout changes to the current, or a new name, so they are available in the future.

Timeline Controls

The Timeline is used to navigate through live or archived video and control the playback speed. Timeline controls and behavior are similar, yet slightly different between live and archived video.



Timeline Scale and Position Controls

- *Speed slider* – Provides additional control for playback speed.
- *Playback buttons* – Start, stop, and control playback speed - click arrows to jump 10 seconds.
- *Scale buttons* – Use to scale date/time display from increments of 100ms to 1 month.
- *Timeline* – Provides timestamp markers and currently playhead position.
- *Device indicator* – Displays the name of the selected device and archive markers.
  - Bright green is a recorded segment; blue are a Bookmarks, and Gray is no archive.
- *Time marker* – Indicates the current date and time of the selected video.
- *Scrollbar* – Use to quickly move backwards and forwards along the timeline.
- *Time marker indicator* – Indicates where you are on the Timeline relative to the time marker.
- *Thumbnails* – Click the thumbnail icon to toggle a display of thumbnails above the timeline.
- *LIVE* – Click to switch the selected camera(s) to live playback mode.
- *SYNC* – Click to toggle synchronization of all items displayed in the current layout..
- *Calendar* – Opens a calendar option for Timeline navigation.

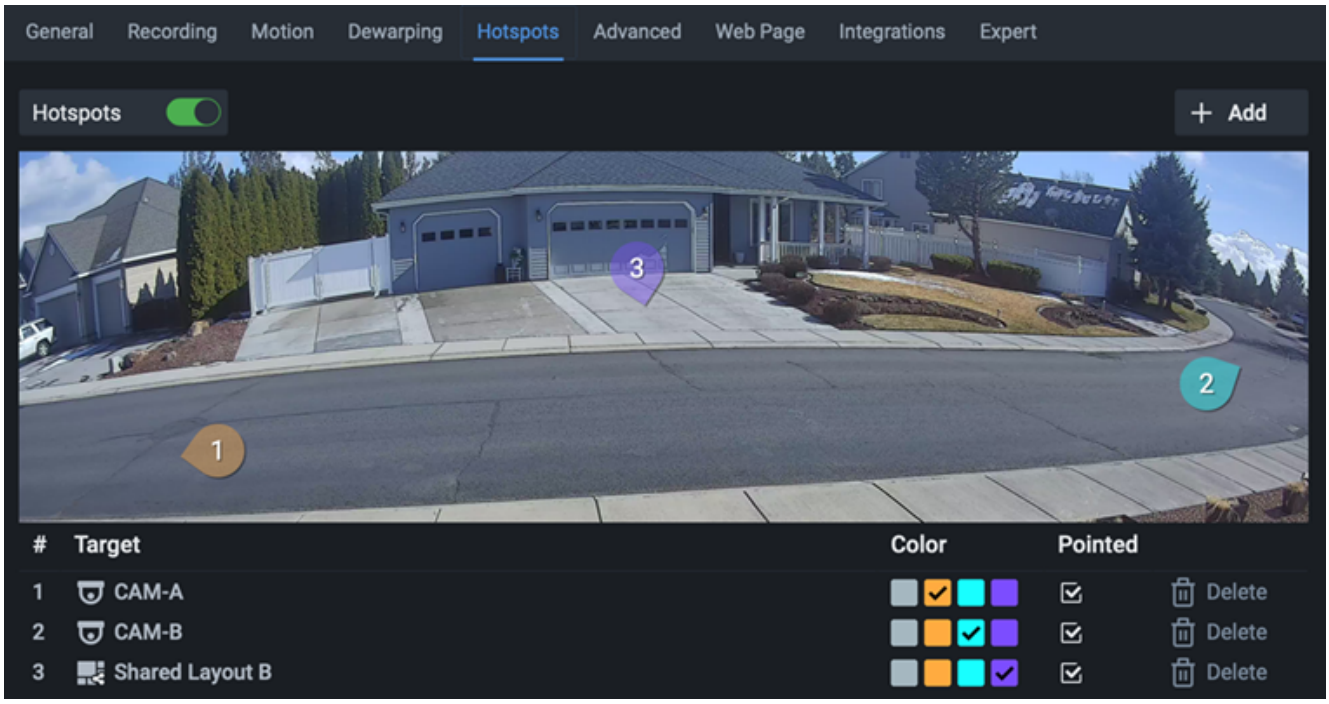
NOTE: When a layout contains multiple devices, the combined archive status for unselected cameras is shown as a very thin, color-coded bar beneath the larger device indicator.

Camera Settings

To edit camera setting:

1. Right-Click a camera on the active layout, or a camera displayed in the Resource Panel.
2. Select **Camera Settings** from the contextual menu.
3. Click on any of the Camera Settings tabs to open specific dialogs:
   a. General tab contains the camera name, model, authentication, image and audio options.
   b. Recording tab is used to configure recording schedule, resolution, and archive duration.
   c. Motion tab provides a detection overlay grid where a region of interest can be drawn.
   d. Hotspots are icons displayed on one camera that open a different camera when clicked.
   e. Advanced tab varies by camera to perform camera hardware resets or stream tuning.
   f. Web Page tab opens the any browser-based configuration tools embedded in the camera.
   g. Integrations tab provides access to any available camera plugins or analytical services.
   h. Expert tab provides device specific overrides for streams, time synch, and web page port.

Hotspot Configuration Example



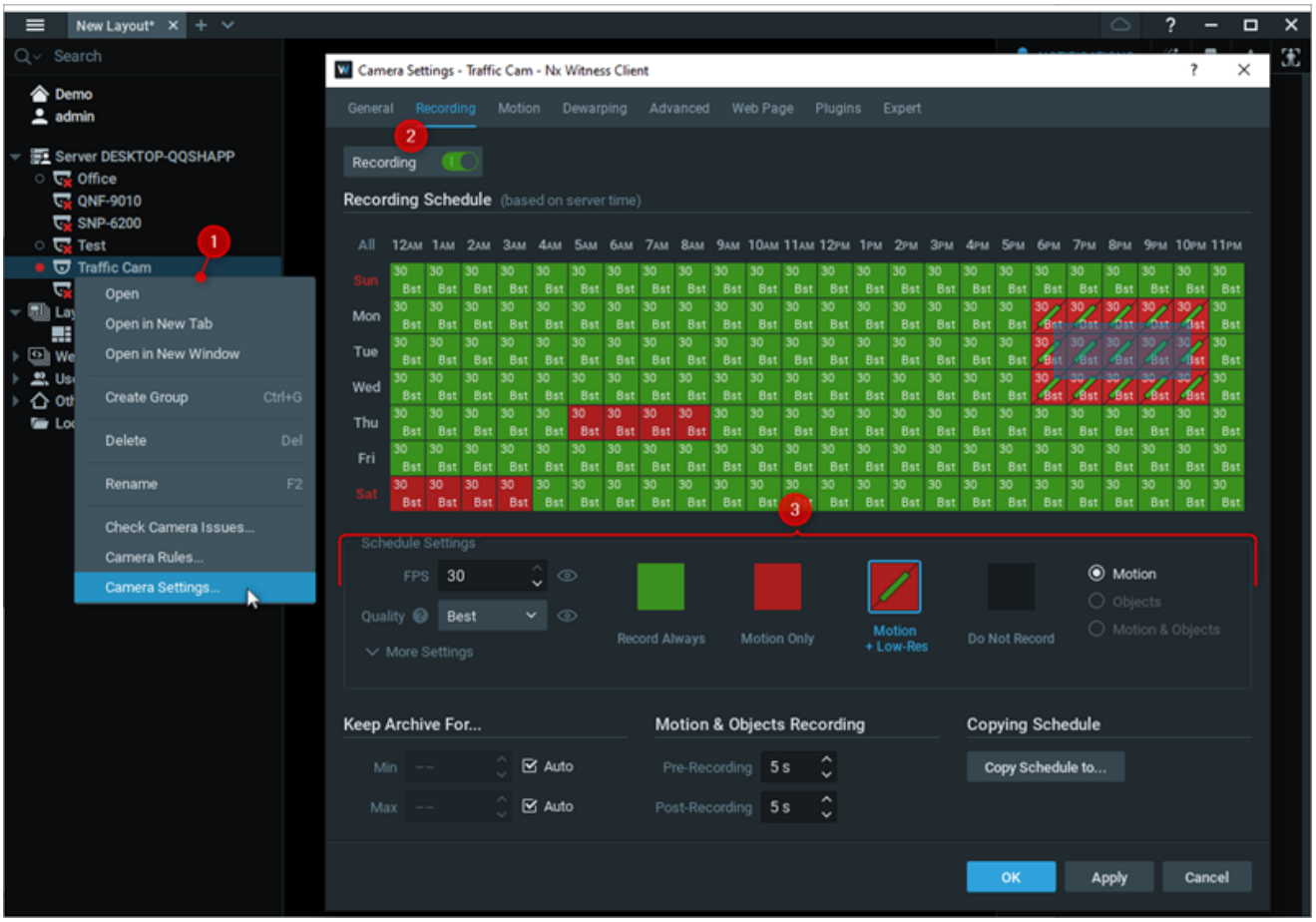
Enable Recording

To enable recording

1. Right-click on a Camera and click **Camera Settings**.
2. Go to the *Recording* tab and enable Recording using the slider control.
3. Select the recording schedule settings: dates/times, recording mode, FPS, and Quality. Click **OK**.

Recording Modes

- Record always – Records the stream all the time.
- Motion Only / Objects Only / Motion & Objects Only – Records the stream only when Motion, Objects, or both are detected.
- Motion + Lo-Res / Objects + Lo-Res / Motion & Objects + Lo-Res – Records the stream in low resolution all the time and high resolution only when Motion, Objects, or both are detected.
- Do Not Record.



Search the Video Archive

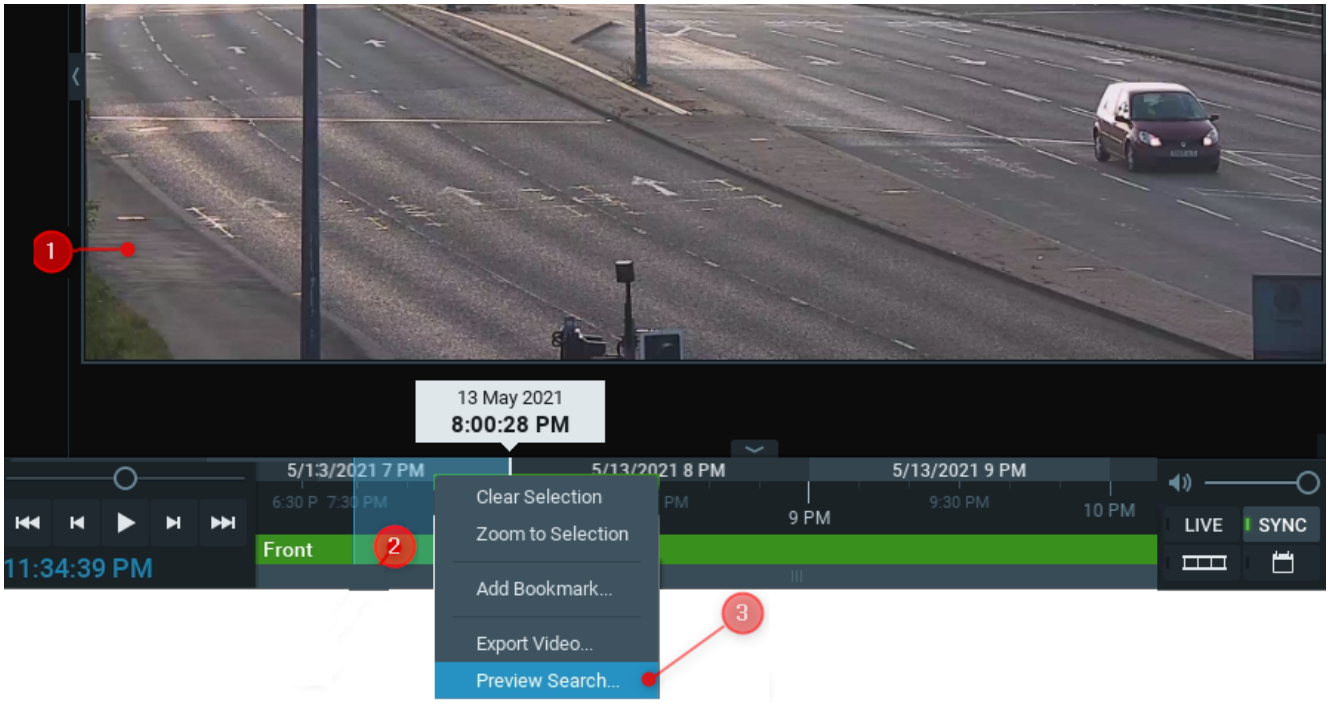
Multiple search methods are provided to optimize results and accommodate user preferences.

Archive Search Methods

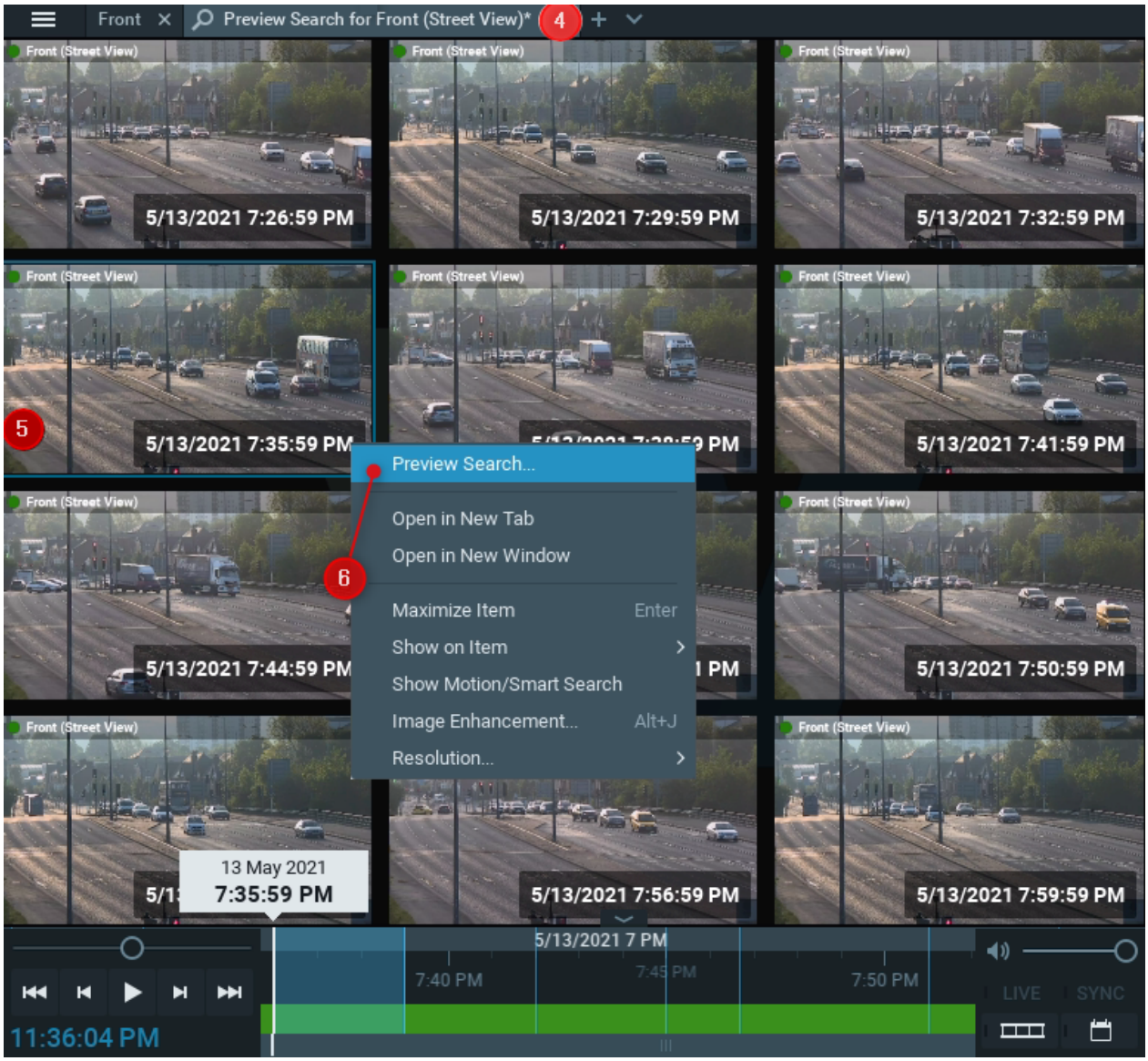
- *Timeline* is the traditional method of manually searching through video footage.
- *Calendar* widget is access by clicking the icon and provides a way to jump between dates.
- *Smart Motion Search* defines a region of interest to scan for changes between frames.
- *Thumbnail Navigation* is opened on top of the timeline to aiding visual search.
- *Bookmarks* are segments of footage that have been tagged with metadata.
- *Preview Search* parses a selection of the timeline to produce small video with timestamps.
- Advanced Object Search employs analytical Integrations to scan for defined objects.

Using Preview Search

1. Select a Camera on the Viewing Grid.
2. Click and drag the position slider along the Timeline to highlight the desired segment.
3. Right-click the highlighted segment and click **Preview Search...**



4. A new Layout will be created that contains the selected time automatically be divided into several equal segments, each with a thumbnail.
5. Click on a Preview Search Thumbnail to see the corresponding segment in the Timeline.
6. Preview Search thumbnails can be divided into smaller time segments by right-clicking on the desired thumbnail and choosing **Preview Search**. The smallest time segment that Preview Search will process thumbnails for is 15 seconds.

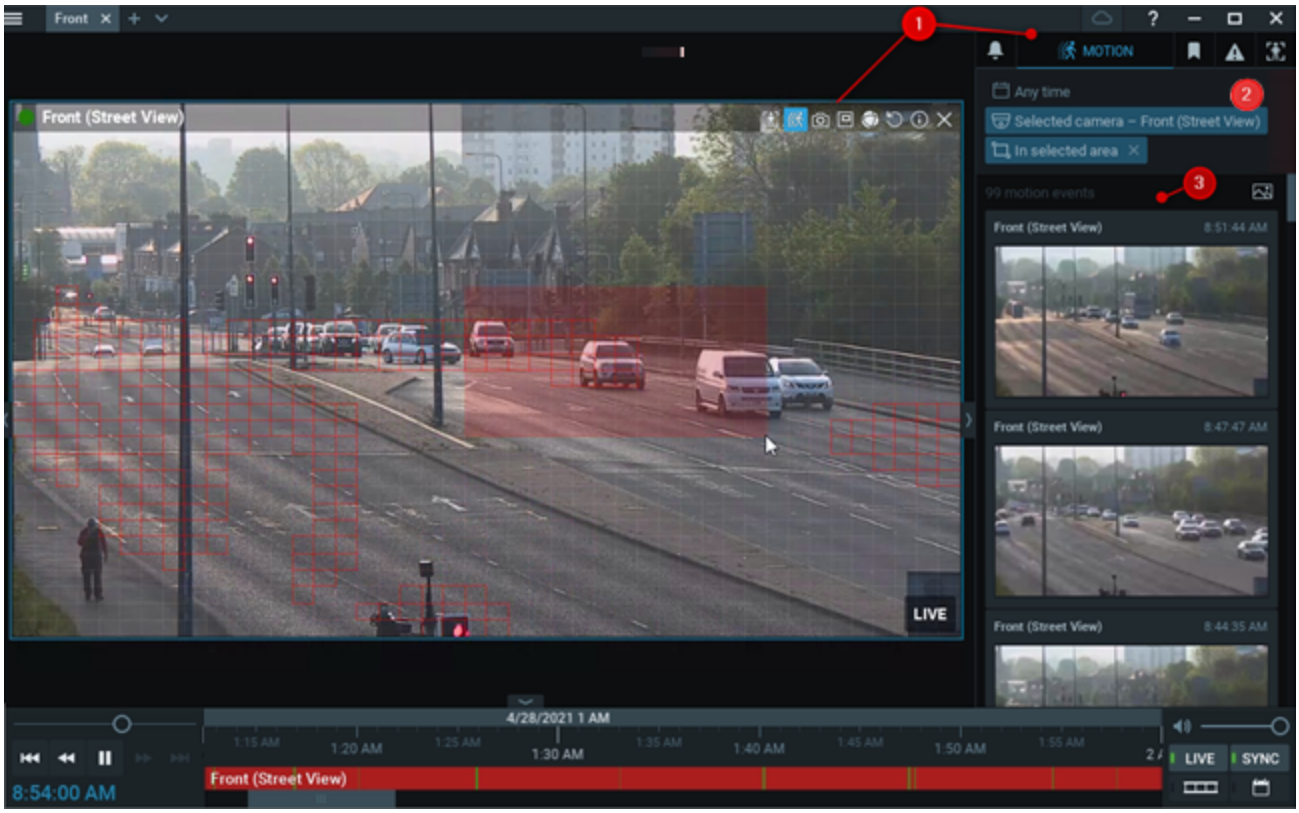


Smart Motion Search

Smart Motion Search must be enabled and configured for the device-archive to be searched.

To search for motion events in the archive

1. Select to the *Notification Panel* and click the *Motion* tab, or hover over a Camera on the Viewing Grid and click the **Smart Motion Search** icon.
2. Configure the following filters:
   - *Area* (required) – Click and drag over the camera to define the Smart Motion Search area. This limits the results to motion events that occurred within a specified zone of the camera's stream.
   - *Camera* (required) – Limits the results to motion events from the selected camera.
   - *Time* (optional) – Limits the results to motion events that occurred within the selected time interval: **Last day**, **Last 7 days**, **Last 30 days**, and **Any time**.
3. View the search results in the Notification Panel.



Advanced Object Search

Key Concepts:

- Advanced Object Search provides filters and options that enable the viewing of specific results.
- Available plug-ins and integrations are listed across the dialog header in a tab-style selection control.
- The left side panel contains all of the Advanced Object Search parameters for the active plugin or integration.
- Additional panels in the Advanced Object Search Dialog include the results panel (center) and the preview panel (right side).
- The results presented in the center panel can be either a card view (image and metadata) or a table view that removes the images makes room for additional results.
- The preview panel includes available metadata provided by the plugin or integration service.
- Data and columns in the table view can be organized by using the Settings (gear) icon on the table view.
  - Settings/Gear icon is only available when Object Type is selected
  - Choices for Table view and Card view are independent (you may show “Color” in Card view, but not in Table)
  - Only shows Attributes that are available for the currently selected Object Type. When 2 object types share some attribute (i.e both Vehicle and Animal have “Color”) - the attribute will be visible for both.
- Hover over a card to display additional playback options (speed, jump points) that may be available.
- The preview panel will play the entire duration that the object is visible, including 4 seconds before and after the after object was detected.
- Left side panel can be re-sized to present an alternate view of the filter and tiles/

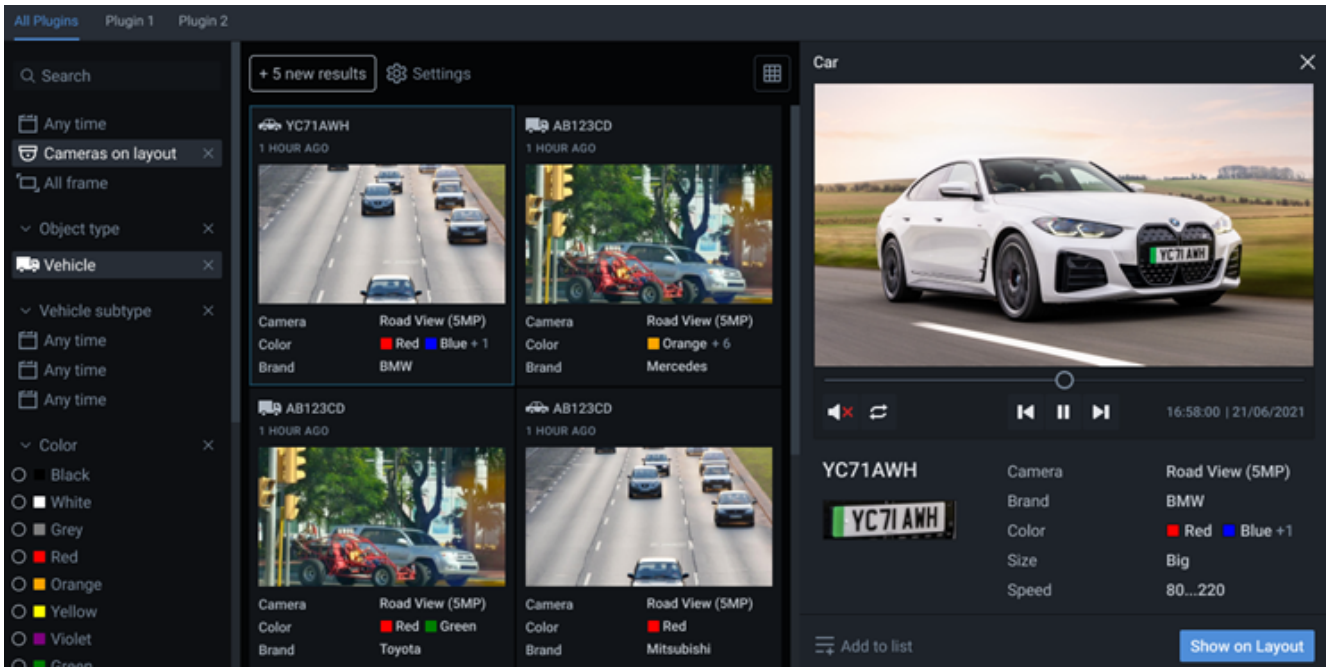
Using the Advanced Search:

1. Select the Objects Tab from within the Notification Panel.
2. Click on the **Advanced** button to open the Advanced Object Search dialog.
3. Select the active plug-in from header menu or select **All Plugins** – all plugins may not support all select object attributes.
4. Configure the search and filter parameters – results will update as parameters are adjusted.

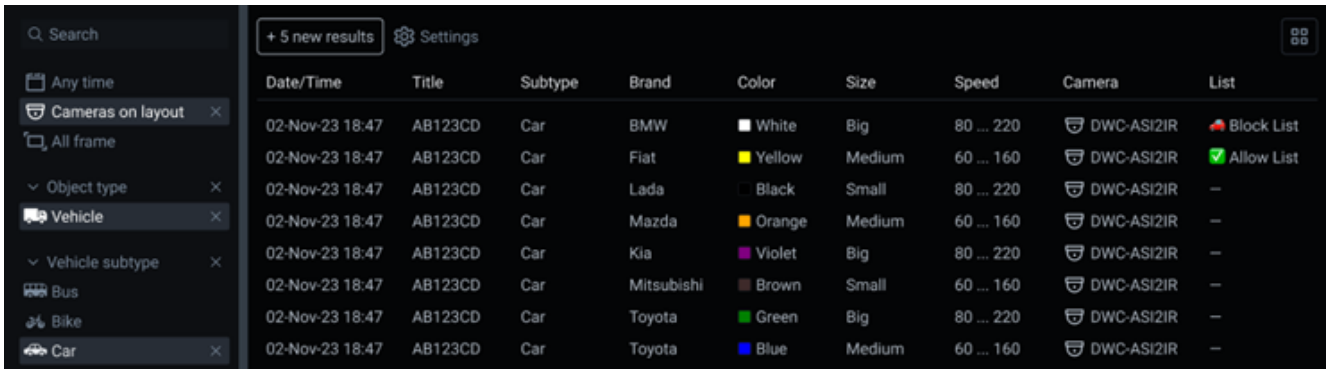
Viewing Advanced Search Results:

1. Toggle the viewing option between Card (image based) and List (text based) formats.
2. Click on the Settings (gear icon) to adjust the fields shown in the results panel.
3. Select a card or list item to open the preview panel.
4. Click **Show on Layout** to return to the main view and align the playback with the search result.

Card View:



List View:



Export Recorded Video

Key Concepts

- Files from a single device, Bookmarks, and files from multiple devices that are synchronized for simultaneous playback can be can be exported to a file.
- Export tasks are performed in the background to enabling continuous client usage.
- The exported video file will be available under Local Files in the Resource Panel.
- Exporting motion-only video ignores all gaps between events and stitches the events together.
- Existing bookmarks are also included in exported video.
- Always save exported files secure location as they are discarded when the Client closes.
- Exported video can locked as read-only or protected with a password (.NOV or.EXE formats).
- Video can be exported as: .MKV, .AVI, .MP4, .EXE, or a .NOV for use with the Client.
  - Exporting as .EXE will package the video with a Microsoft Windows compatible player.
- An optional watermark can be applied to the exported video file.

To Export a Video Segment from the archive

1. Select a Camera on the Viewing Grid.
2. Click and drag the position slider on the Timeline to select the segment to export.
3. Right-click the highlighted segment and click **Export Video**.
4. Configure optional Export Settings:
   - Expert Settings – Apply image correction filters and transcoding options.
   - Add Timestamp – Select format and font size of Timestamp.
   - Add Image – Browse for an Icon to scale and overlay.
   - Text – Enter and scale custom text to be applied.
   - Info – Toggle display of Camera name and date.
   - Rapid Review – Adjust speed and frame interval.
5. Select the file type and export location. Click **Export**.

Nx Witness

Still need help? Visit us at http://support.networkoptix.com